

Redes de Computadores I:

Apresentação da Disciplina

Prof. Max do Val Machado



Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Disciplina Redes de Computadores I

Ementa (3812)

- **Redes de Computadores I:** Conceitos básicos de redes de computadores, protocolos e serviços de comunicação. Arquitetura de redes de computadores. Camadas inferiores dos modelos de referência OSI/ISO e TCP/IP: física, enlace, rede e transporte.
- **Redes de Computadores II:** Serviços e protocolos da camada de aplicação. Redes Multimídia. Segurança em redes. Gerência de redes. Redes sem fio e redes móveis.
- **Lab. de Redes e Sistemas Operacionais:** Sistemas operacionais com suporte a redes. Configuração e administração de sistemas de computação em rede. Projeto de redes de computadores. Implementação das camadas inferiores dos modelos de referência OSI/ISO e TCP/IP: física, enlace, rede e transporte. Programação com soquetes. Serviços e protocolos para camadas superiores. Ferramentas de segurança e gerência de redes.

Ementa (3813)

- **Redes de Computadores I:** Conceitos básicos de redes de computadores, protocolos e serviços de comunicação. Modelos de referência de computadores. Pilha de protocolos TCP/IP (**R2, cam. superiores**). Endereçamento IP (**LRSO**). Redes Multimidia (**R2**).
- **Redes de Computadores II:** Projeto de redes locais e de longa distância: topologia, equipamentos e tecnologias (**LRSO**). Arquitetura de Infraestrutura de TI. Redes sem fio. Administração (**LRSO**), gerência e segurança de redes TCP/IP. Virtualização (**novo**). Computação em Nuvem (**novo**). Comunicação entre dispositivos inteligentes (**novo**).
- **Trabalho Interdisciplinar V: Sistemas Computacionais (**novo**):** Desenvolvimento de uma solução computacional envolvendo arquitetura e redes de computadores e sistemas operacionais. Trabalho e avaliação em equipe.

Equivalência

Curso de Ciência da Computação – Currículo 3813

PER	DISCIPLINA DO CURRÍCULO 3812	CH	PER	DISCIPLINA EQUIVALENTE NO 3813	CH
6	Redes de Computadores I	68	5	Redes de Computadores I	80
7	Lab. de Redes e Sistemas Operacionais	34	6	Trab. Interdisciplinar VI: Sist. Paralelos e Distrib.	30
7	Redes de Computadores II	68	7	Redes de Computadores II	80

Curso de Ciência da Computação – Currículo 3813

PER	DISCIPLINA DO CURRÍCULO 3813	CH	PER	DISCIPLINA EQUIVALENTE NO 3812	CH
5	Redes de Computadores I	80	6	Redes de Computadores I	68
5	Trab. Interdisciplinar V: Sistemas Computacionais	30	4	Arquitetura de Computadores III	68
			5	Sistemas Operacionais	68
			6	Redes de Computadores I	68
				COMPLEMENTAÇÃO DE CARGA HORÁRIA	30
7	Redes de Computadores II	80	7	Redes de Computadores II	68
			7	Lab. de Redes e Sistemas Operacionais	34

Métodos Didáticos

- Aulas expositivas com apresentação de conteúdo, discussão de problemas e aplicações
- Trabalhos práticos e exercícios
- Estudos de casos que realcem a importância da disciplina e sua aplicação em problemas reais

Métodos de Avaliação

- Prova P1, P2 e P3 - 15 pontos cada
- ADA - 5 pontos
- Listas de exercício - 5 pontos
- Seminário de Artigo Científico - 15 pontos
- Trabalhos Práticos (30 pontos)
 - Parte 1: Roteamento entre redes - 3 pontos
 - Parte 2: Wireshark - 1 pontos
 - Parte 3: Packet Tracer - 1 pontos
 - Parte 4: Implementação de aplicação usando sockets - 25 pontos
- Reavaliação – 30 pontos para substituir a nota das duas menores provas sendo que o aluno aprovado na reavaliação terá nota igual a 60

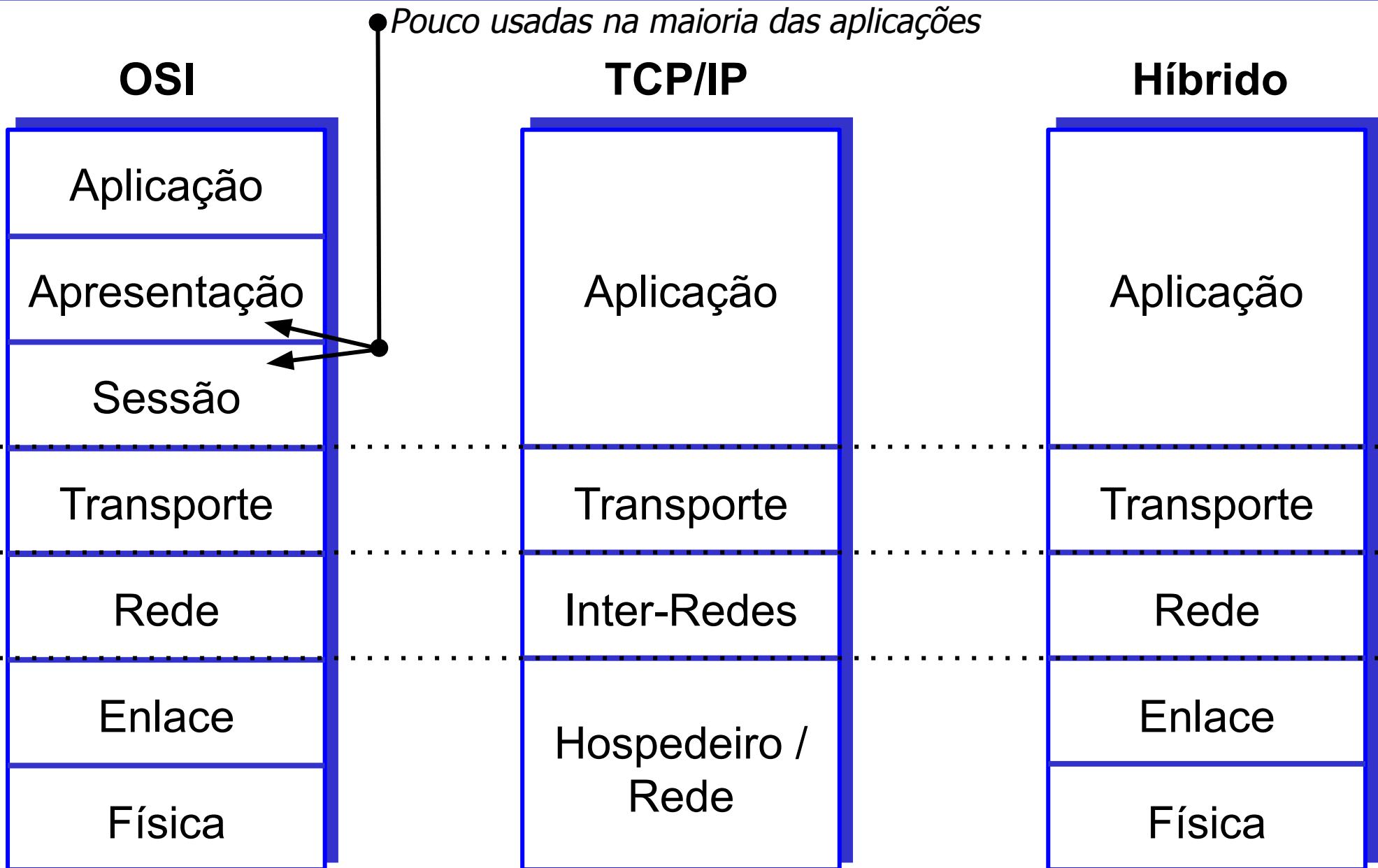
Seminário de Artigo Científico

- Cada grupo deve escolher um artigo em inglês publicado pelo IEEE, ACM ou SBC nos últimos três anos (1 pt, 9/ago)
- Resumo em LaTeX (modelo SBC) com 1 página abordando (5 pts, 23/ago):
 - (i) motivação
 - (ii) objetivos
 - (iii) modelo
 - (iv) resultados de simulação ou experimentação
 - (v) conclusões e trabalhos futuros
- Apresentação de 9 minutos (4 pts slides + 5 pts apresentação): participação de todos os integrantes do grupo; avaliação dos trabalhos pelos alunos; perguntas serão contabilizadas nas notas de cada aluno

Unidades de Ensino

- Impossível falar das unidades de ensino sem introduzir os modelos de referência:
 - Modelo ISO/OSI
 - Modelo TCP/IP (na verdade, Arquitetura)
 - Modelo de Referência Híbrido

Unidades de Ensino



Unidades de Ensino

- Modelo de referência híbrido

CAMADAS

Aplicação

Transporte

Rede

Enlace

Física

Unidades de Ensino

- Modelo de referência híbrido

- **Camada Física:** transmissão de bits e meios de transmissão

CAMADAS

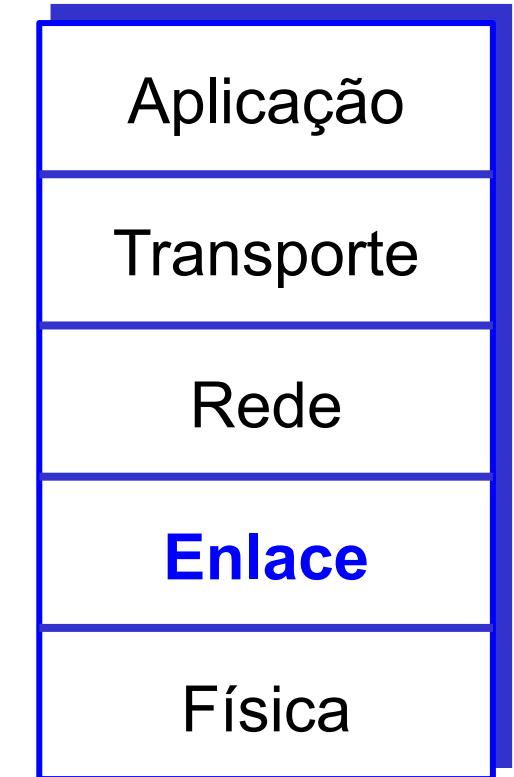


Unidades de Ensino

- Modelo de referência híbrido

- **Camada de Enlace**: transferência de dados entre elementos vizinhos da rede

CAMADAS



Unidades de Ensino

- Modelo de referência híbrido

- **Camada de Rede**: roteamento de pacotes da origem ao destino

CAMADAS



Unidades de Ensino

- Modelo de referência híbrido

- **Camada de Transporte**: transferência de dados processo-processo

CAMADAS

Aplicação

Transporte

Rede

Enlace

Física

Unidades de Ensino

- Modelo de referência híbrido

- **Camada de Aplicação:** suporte a aplicações de rede (e.g., FTP, SMTP, HTTP)

Se necessários, os serviços de **apresentação** e **sessão** do modelo OSI serão implementados na Camada de Aplicação

CAMADAS

Aplicação

Transporte

Rede

Enlace

Física

Unidades de Ensino

- Modelo de referência OSI

- **Apresentação:** permite que as aplicações interpretem significado de dados, por exemplo, criptografia, compactação, convenções específicas da máquina
- **Sessão:** sincronização, verificação, recuperação de troca de dados

Unidades de Ensino

- Unidade I: Conceitos Básicos
 - Conceitos básicos de comunicação de dados
 - Usos de redes de computadores
 - Hardware de rede
 - Software de rede
 - Arquitetura de rede
 - Modelos de referência

Unidades de Ensino

- Unidade II: Camada Física
 - Conceitos básicos
 - Métricas da Rede
 - Meios de transmissão (guiados, sem fio e satélite)

Unidades de Ensino

- Unidade III: Camada de Enlace
 - Questões de Projeto da Camada de Enlace
 - Enquadramento
 - Controle de Fluxo
 - Controle de Erros

Unidades de Ensino

- Unidade IV: Subcamada MAC
 - Alocação de Canais
 - Protocolos de Acesso Múltiplo
 - Padrão IEEE 802 para LANs e MANs
 - LANs Sem Fio

Unidades de Ensino

- Unidade V: Camada de Rede
 - Questões de Projeto da Camada de Rede
 - A camada de rede da Internet
 - Internet Protocol v4 (IPv4)
 - Protocolos de controle da Internet
 - Roteamento
 - Introdução ao Internet Protocol v6 (IPv6)

Unidades de Ensino

- Unidade V: Camada de Transporte

- Serviço de Transporte
- Elementos do serviço de transporte
- Protocolo simples de transporte
- Protocolo UDP
- Protocolo TCP

Cronograma

- Aulas 1 e 2: Apresentação da Disciplina
- Aulas 3 e 4: Unidade I (Introdução)
- Aulas 5 e 6: Unidade II (Física)
- Aulas 7 à 10: Unidade III (Enlace)
- Aula 11: Correção de Exercícios
- **Aula 12: Prova I (8/set)**
- Aula 13: Unidade IV (MAC)
- Aula 14 à 21: Unidade V (Rede)
- Aula 22: Wireshark e Packet Tracer
- Aula 23: Correção de Exercícios
- **Aula 24: Prova II (25/out)**
- **Aula 25 e 26: Seminários (27/out e 1º/nov)**
- Aula 27 à 29: Unidade VI (Transporte)
- Aula 30: Correção de Exercícios
- **Aula 31: Prova III (22 de novembro)**
- Aula 32: Devolutiva e Trabalhos
- **Aula 33: Reavaliação (29 de novembro)**
- Aula 34: Devolutiva e Considerações finais

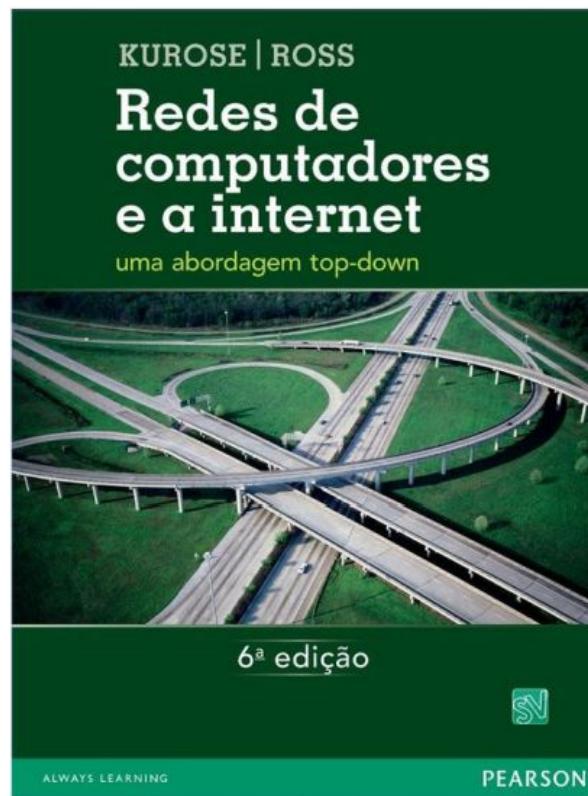
Bibliografia Básica

- TANENBAUM, A. S. Redes de Computadores, 5.^a ed., Ed. Pearson, 2011



Bibliografia Básica

- KUROSE, J. F. e ROSSA, K. W. Redes de computadores e a internet, 6.^a ed. , Ed. Pearson, 2013



Bibliotecas Digitais

- IEEE Xplore - www.ieeexplore.com
- Portal da ACM - portal.acm.org
- Portal da CAPES - www.periodicos.capes.gov.br
- Biblioteca da PUC - portal.pucminas.br/biblioteca/

Biblioteca Digital da PUC Minas



Conta

Idioma



Sair

Ferramentas

Compartilhar

Realçadores

Menu de Aplicativos

Tutorial

Loja

Ajuda

Suporte

Fornecer feedback



Biblioteca Digital da PUC Minas

Sumário

Pesquisar conteúdo

 **Redes de Computadores - Guia Total**
SOUSA, Lindeberg Barros de

20 Capítulo 1 - Fundamentos de Comunicação de Dados >

58 Capítulo 2 - Modems e Interfaces de Conexão de... >

78 Capítulo 3 - Protocolos de Comunicação de Dados >

94 Capítulo 4 - TCP/IP - Arquitetura, Protocolos e Endereçamento IP >

Configurações > 5 - Segurança - Criptografia e Compressão de...

**Redes de Computadores
Guia Total**

Contato do Professor Max do Val Machado



PUC Minas (2o andar, prédio 34), Av. Dom José Gaspar, 500
Coração Eucarístico - Belo Horizonte - MG (**hoje, Teams**)



+55 31 9.9771-3360



maxm@pucminas.br



linkedin.com/in/max-machado

GRUPO
ZAP

<https://chat.whatsapp.com/Ev98Vu4Mit14PzyIURh7gL>



Exercício (1)

- Quais são as funções das sete camadas do modelo de referência OSI?

Exercício (2)

- Qual a diferença de visibilidade entre as camadas de rede e enlace?

Exercício (3)

- Tanto a camada de rede quanto a de transporte, são responsáveis pela transferência de dados, qual a diferença entre elas?

Exercício (4)

- O que significa Broadcasting na camada de rede e na de enlace?

Exercício (5)

- No caso da rede difusão, discuta as vantagens e desvantagens da alocação estática, dinâmica centralizada e dinâmica descentralizada ou distribuída.

Unidade I:

Conceitos Básicos

Prof. Max do Val Machado



Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Disciplina Redes de Computadores I

Agenda

- Introdução
- Hardware de rede
- Software de rede
- Arquiteturas de rede
- Modelos de referência

Agenda

- **Introdução**
- Hardware de rede
- Software de rede
- Arquiteturas de rede
- Modelos de referência

O que é uma Rede de Computadores?



O que é uma Rede de Computadores?

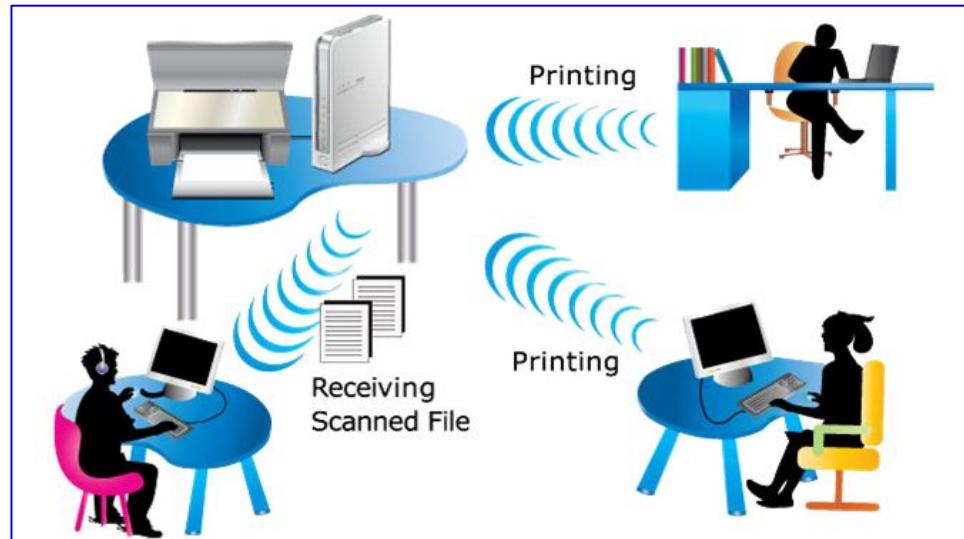
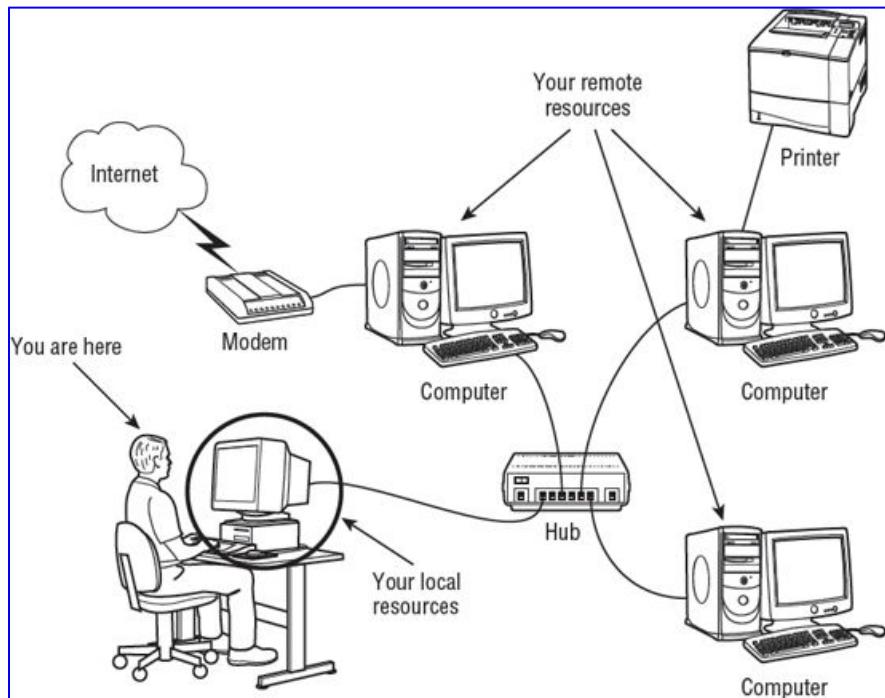
- Conjunto de computadores autônomos interconectados entre si
- Autônomos: não existe uma relação mestre-escravo entre computadores
- Interconectados: capazes de trocar informações entre si através de algum meio (e.g., par trançado, microondas e satélite)

Por que as pessoas estão interessadas em redes de computadores?

Compartilhamento de Recursos

- Disponibilidade de recursos para qualquer usuário
- Recursos podem ser programas, dados, dispositivos físicos, independente da localização geográfica

Compartilhamento de Recursos



Por que as pessoas estão interessadas em redes de computadores?

Compartilhamento de Informações



Comunicação entre Funcionários



Trabalho *Online* Cooperativo



E-Business



NEGÓCIOS

Sua próxima compra online virá diretamente do shopping ao lado

Sistema piloto da rede de shoppings BR Malls passou a vender produtos do shopping Villa Lobos pelo Mercado Livre, com entrega em poucas horas

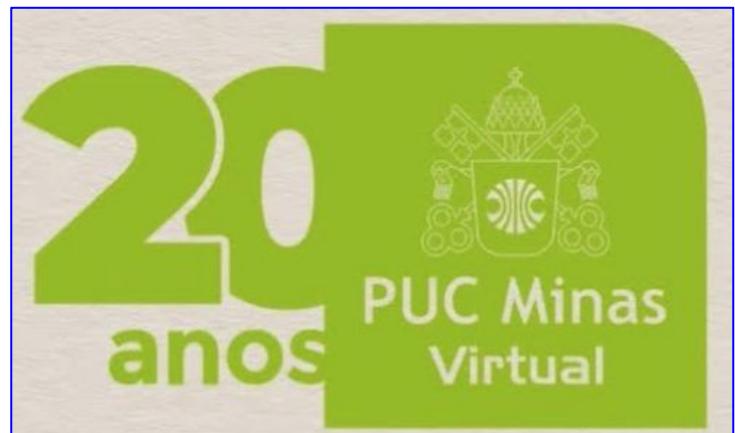
A loja física não vai acabar, afirma Luiza Trajano, do Magazine Luiza

Durante participação no SAS Forum Brazil, executiva destacou também a aposta da rede nas chamadas "lojas físicas virtuais"

Videoconferência



E-Learning



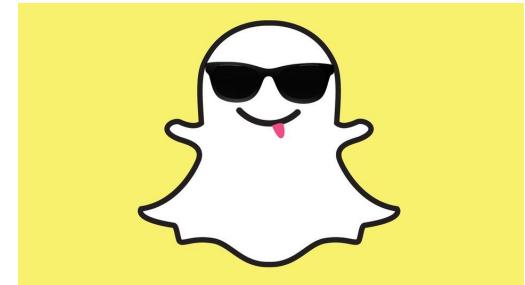
Bancos



banco
inter

The logo for Banco Inter. It features the word "banco" in a small, gray, sans-serif font above the word "inter" in a large, bold, orange, sans-serif font. The "i" in "inter" has a small vertical stroke extending upwards.

Entretenimento



Jogos Online



E-Government



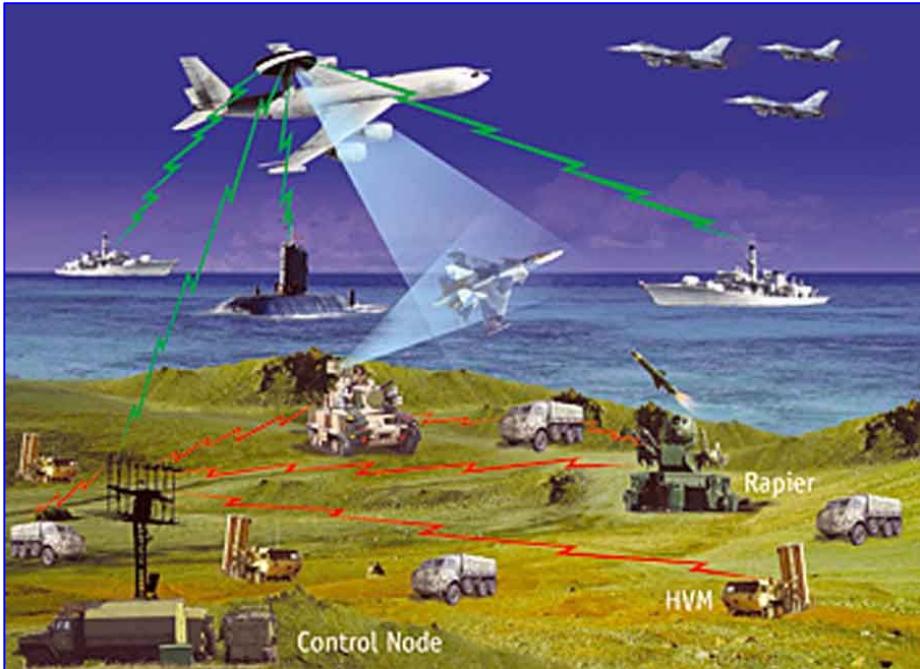
Cartão SUS Digital



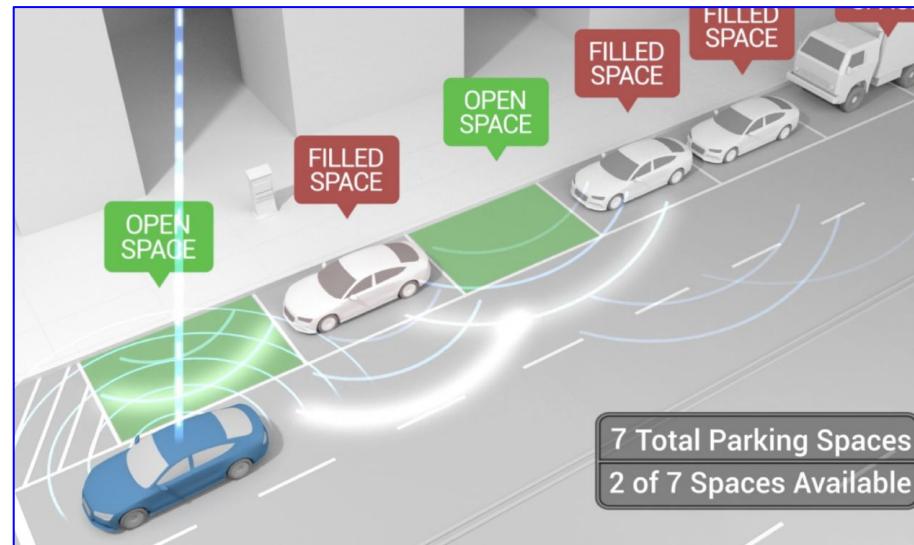
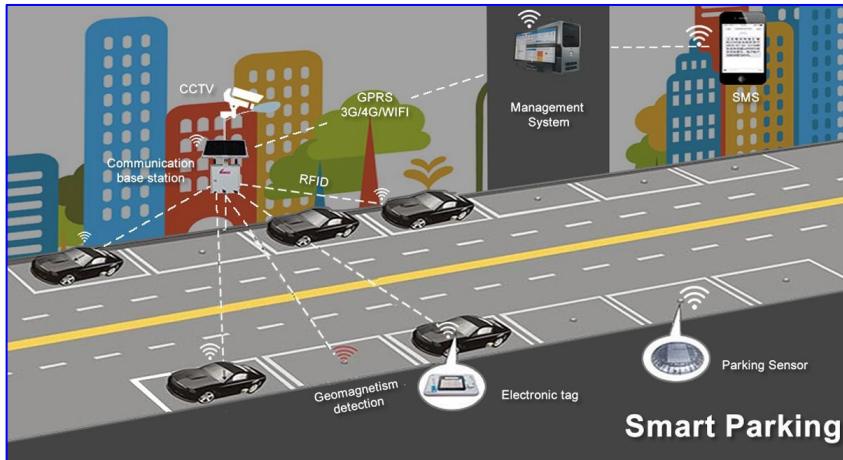
CARTEIRA
DIGITAL DE
TRÂNSITO



Aplicações Militares



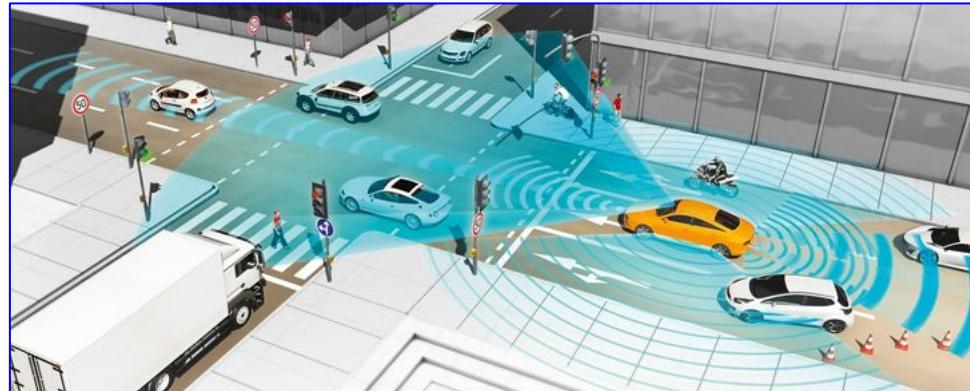
Estacionamento Inteligente



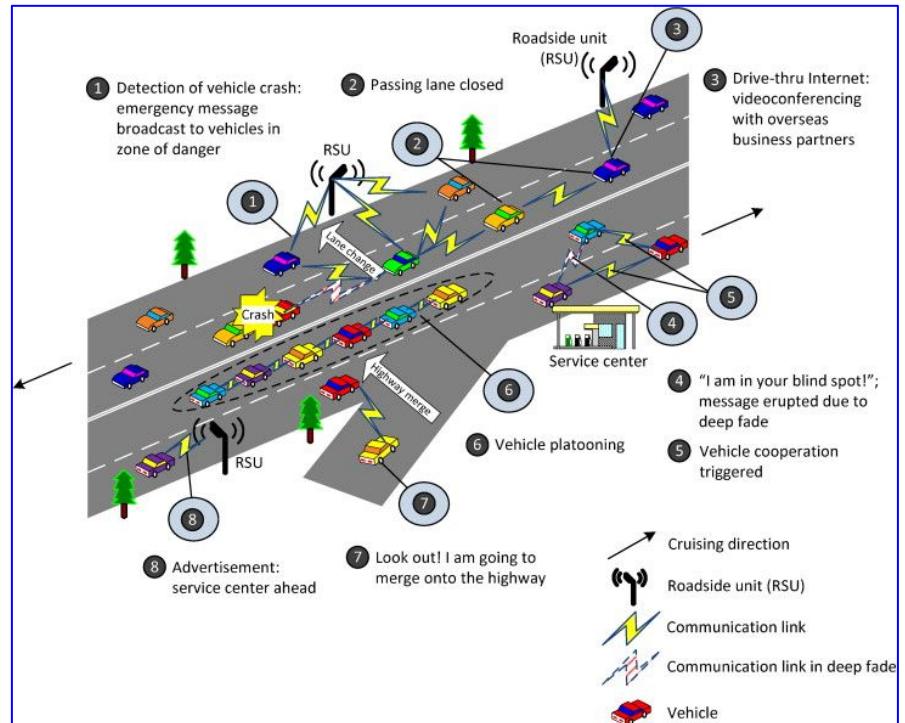
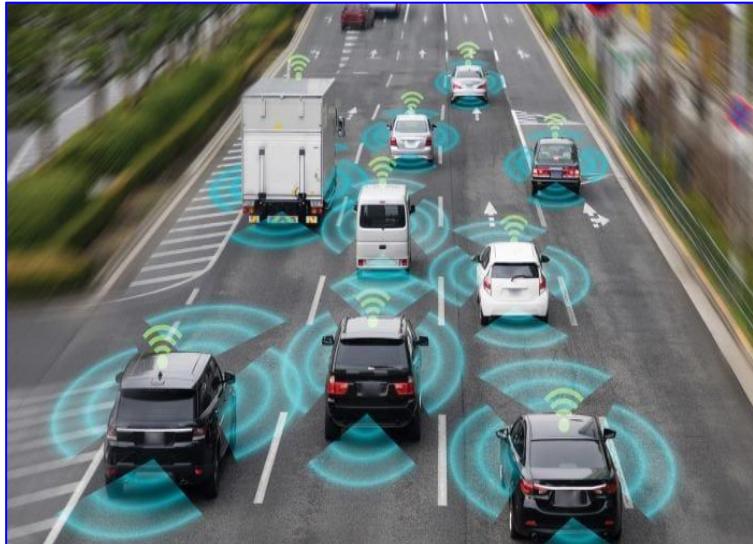
Cidades Inteligentes



©Singapore Press Holdings Ltd



Redes Veiculares



Algumas frases...

“Quatro ou cinco computadores devem ser suficientes para o mundo inteiro até o ano 2000.”

T. J. Watson, 1945 (presidente da IBM)

“Não há razão para qualquer indivíduo ter um computador em casa.”

Ken Olsen, 1977 (presidente da Digital Equipment Corporation)

“640K é mais memória do que qualquer pessoa vai precisar.”

Frase polêmica e teria sido dita por Bill Gates em 1981. Contudo, Gates afirma que “(...) disse coisas estúpidas e erradas, mas não isso. Ninguém envolvido com computadores diria que uma quantidade determinada de memória é suficiente para o todo o tempo (...).”

“A Internet e tudo o que ela habilita é uma vasta fronteira nova, cheia de desafios surpreendentes. Há espaço para grandes inovações. Não fiquem limitados à tecnologia existente hoje. Soltem sua imaginação e pensem no que poderia acontecer e transformem isto em realidade.”

Leonard Kleinrock¹

(1) Professor de Ciência da Computação da UCLA (em 1969, primeiro nó da Internet)

Exercício (1)

- Em breve, teremos um terminal doméstico e seguro conectado a Internet permitindo plebiscitos instantâneos sobre questões importantes. Nesse caso, a política atual será eliminada. Os aspectos positivos dessa democracia direta são óbvios, analise alguns dos aspectos negativos.

Agenda

- Introdução
- **Hardware de rede**
- Software de rede
- Arquiteturas de rede
- Modelos de referência

Classificação das Redes

- Não existe uma taxonomia na qual todas as redes se encaixam
- No entanto, existem dois pontos importantes:
 - Tecnologia de transmissão
 - Escala

Classificação das Redes

- Não existe uma taxonomia na qual todas as redes se encaixam
- No entanto, existem dois pontos importantes:
 - **Tecnologia de transmissão** 
 - Escala

Tecnologias de Transmissão

- Basicamente dois grandes grupos:
 - Redes difusão (*broadcast*) ou acesso múltiplo
 - Redes ponto-a-ponto (*point-to-point*)

Exemplos de Redes Difusão



Redes Difusão

- Canal de comunicação é compartilhado entre os nós da rede
- Mensagens são enviadas por um nó e recebidos por todos os outros
- É necessário um algoritmo para controlar o acesso ao meio
- Toda mensagem possui um campo de endereço

Algoritmo de Recebimento de Mensagens

se endereço da mensagem = meu endereço **então**

processa a mensagem

senão

descarta a mensagem

fimse

Destinatário na Rede Difusão

- Todos computadores da rede (*broadcasting*)
- Um computador (*unicasting*)
- Um subconjunto dos computadores (*multicasting*)

Formas de Alocação do Canal na Rede Difusão

- Alocação Estática
- Alocação Dinâmica (sob demanda)

Alocação Estática

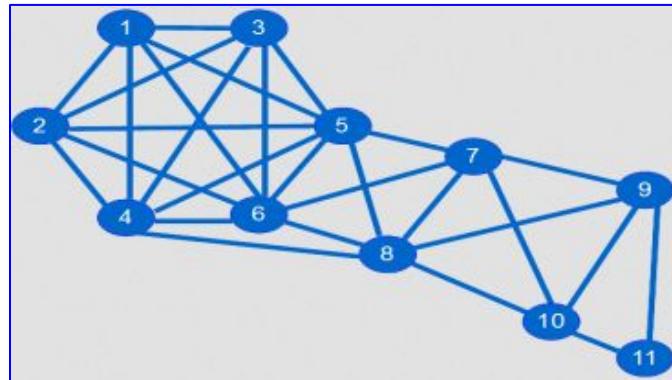
- Tempo dividido em intervalos (*slots*)
- Existe um algoritmo tipo “ciranda” (*round robin*) em que cada nó transmite somente no seu *slot*
- Desvantagem: canal fica vazio se um nó não tem o que transmitir

Alocação Dinâmica

- Centralizada:
 - Uma entidade central escolhe o próximo nó a ter acesso ao meio
 - A entidade recebe requisições e escolhe
- Descentralizada:
 - Cada nó decide se transmite em um determinado momento ou não

Redes Ponto-a-ponto

- As conexões são entre pares de computadores
- Pacotes são enviados na modalidade *store-and-forward*
- Algoritmos de roteamento são importantes



Redes Difusão x Ponto-a-ponto

- Em geral,

Difusão	Ponto-a-ponto
Redes menores	Redes maiores
Localizadas geograficamente	Espalhadas

Classificação das Redes

- Não existe uma taxonomia na qual todas as redes se encaixam
- No entanto, existem dois pontos importantes:
 - Tecnologia de transmissão
 - Escala 

Escala

- É a classificação de processadores interconectados em função da distância entre eles (tamanho da rede)

Distância entre os processadores	Processadores localizados no(a) mesmo(a)	Exemplo
1 m	Metro quadrado	Rede pessoal
10 m	Sala	Rede local
100 m	Edifício	
1 km	Campus	
10 km	Cidade	Rede metropolitana
100 km	País	Rede geograficamente distribuída
1.000 km	Continente	A Internet
10.000 km	Planeta	

Tamanho da Rede

- Normalmente, afeta a tecnologia básica que pode ser utilizada
- Proporciona informações como, por exemplo, o tempo necessário para dados serem propagados entre as ponta da rede

Agenda

- Introdução
- Hardware de rede
- **Software de rede**
- Arquiteturas de rede
- Modelos de referência

Pilha de Camadas

- É a forma como as redes estão organizadas
- É a razão de sucesso das redes de computadores
- Separa tarefas, reduzindo a complexidade do projeto

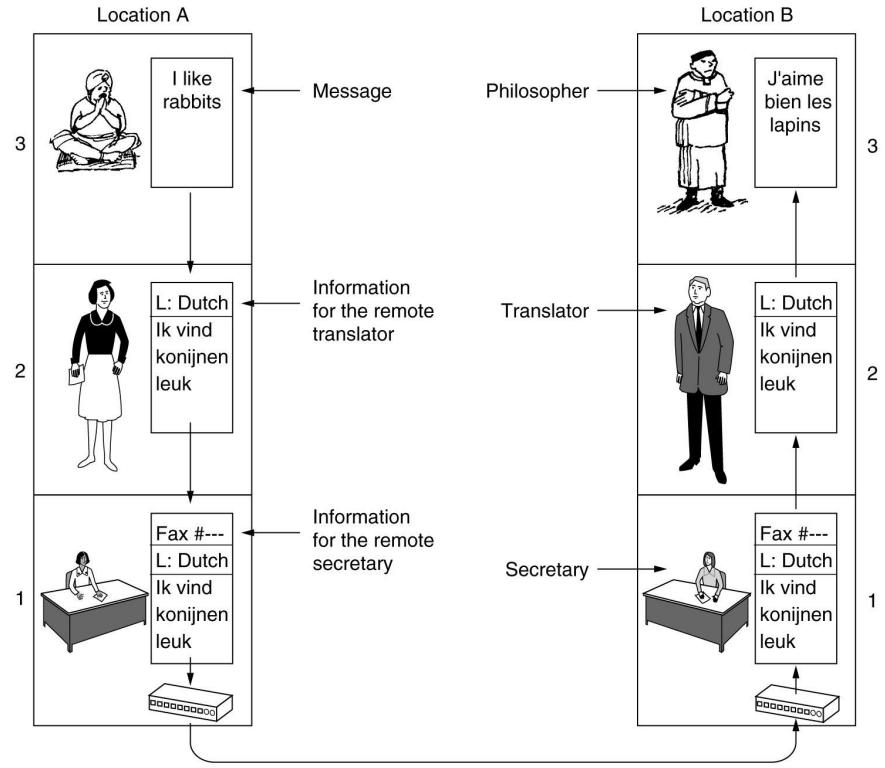
Cada Camada da Pilha

- Oferece serviços para suas superiores, abstraindo detalhes de implementação
- Acredita que se comunica diretamente com seu par na outra máquina

Comunicação Virtual x Real

- Comunicação direta (horizontal) entre entidades pares é virtual e executada através do protocolo da camada n
- Comunicação real (vertical) é feita entre entidades na mesma hierarquia
- Comunicação ocorre efetivamente na camada mais baixa através de um meio físico

Exemplo de Comunicação em Camadas



Quais são as camadas e suas funcionalidades?

Exercício (2)

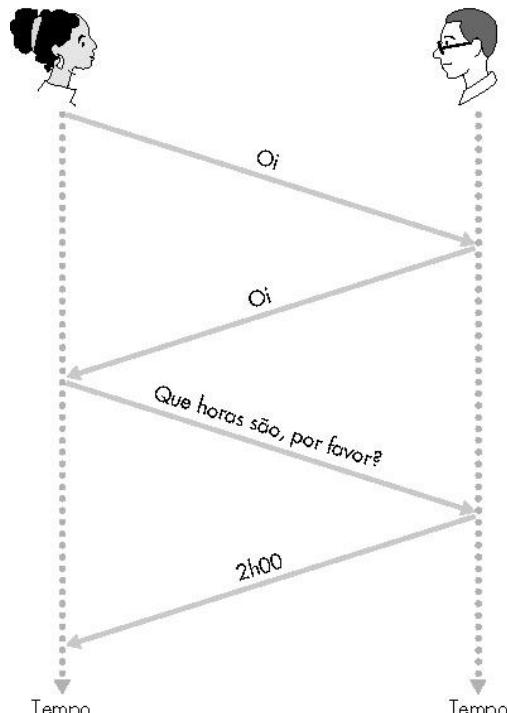
- O presidente da XBeer resolve trabalhar com a YBeer para produzir uma lata de cerveja invisível (medida higiênica). O presidente pede que o jurídico analise a questão. Esse contacta o departamento de Engenharia. Como resultado, o engenheiro-chefe entra em contato com seu par na YBeer para discutirem os aspectos técnicos. Em seguida, os engenheiros enviam um relatório aos departamentos jurídicos, que discutem os aspectos legais. Por fim, os presidentes discutem as questões financeiras do negócio. Esse é um exemplo de protocolo em várias camadas no sentido utilizado pelas redes de computadores? Justifique.

Protocolos de Comunicação

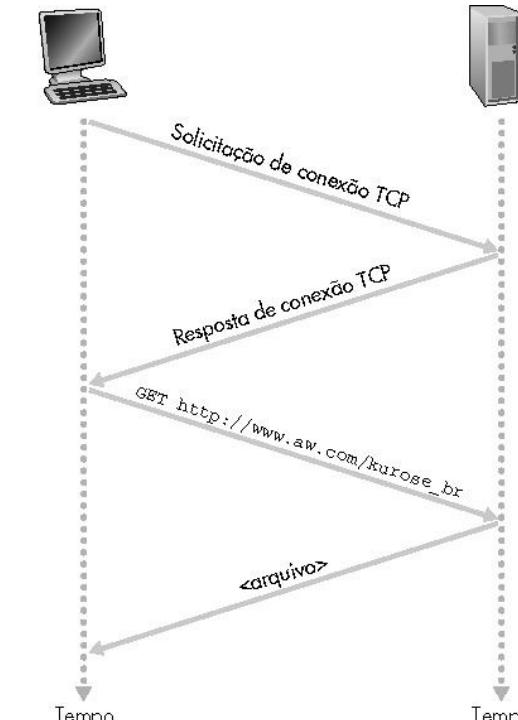
- Conjunto de regras e convenções para troca de informações entre duas ou mais entidades comunicantes
- Define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comunicantes
- Define as ações realizadas na transmissão e no recebimento de uma mensagem ou outro evento

Protocolos de Comunicação

Protocolo humano



Protocolo de rede



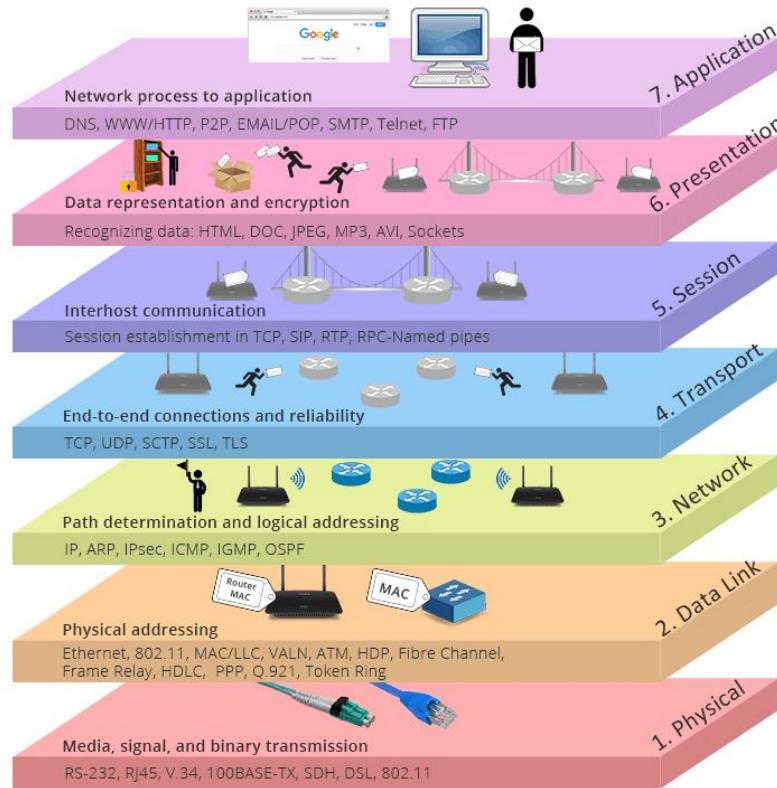
Agenda

- Introdução
- Hardware de rede
- Software de rede
- **Arquiteturas de rede**
- Modelos de referência

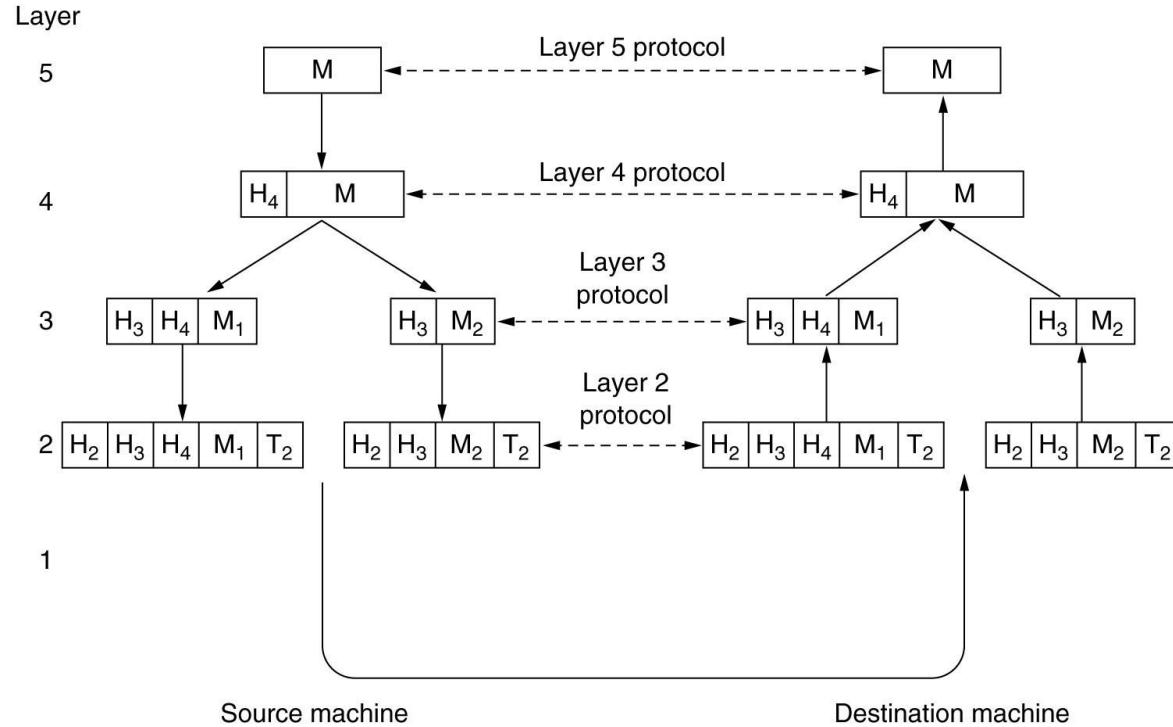
Arquitetura de Rede

- Definição: conjunto de camadas e seus protocolos
- Detalhes de implementação e especificação de interfaces não fazem parte da arquitetura
- Pilha de protocolos (*protocol stack*): protocolos usados em cada camada (um por camada) em um sistema

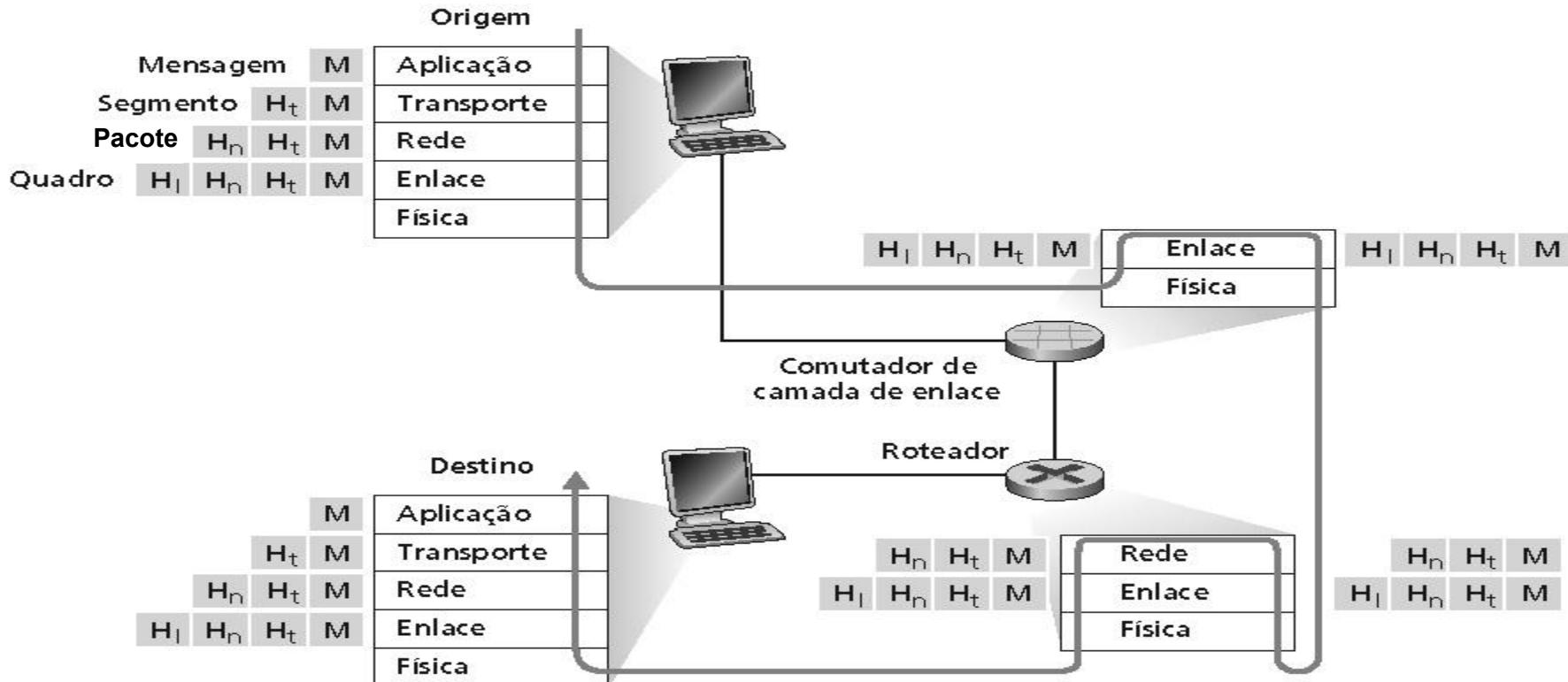
Arquitetura de Rede



Comunicação em Camadas



Comunicação em Camadas



Exercício (3)

- Um sistema tem uma hierarquia de protocolos com n camadas. As aplicações geram mensagens com M bytes de comprimento. Em cada uma das camadas, é acrescentado um cabeçalho com h bytes. Qual é a fração dos dados enviados que corresponde ao tamanho dos cabeçalhos?

Agenda

- Introdução
- Hardware de rede
- Software de rede
- Arquiteturas de rede
- **Modelos de referência**

Modelos de Referência

- São propostas concretas de arquiteturas de rede
- Duas arquiteturas de rede importantes:
 - Modelo OSI - *Open Systems Interconnection* da ISO
 - Não é uma arquitetura em si porque não especifica os protocolos em cada nível
 - Informa apenas o que cada camada deve fazer
 - TCP/IP

Modelos de Referência OSI

- Trata da interconexão de sistemas abertos
- Aberto no sentido que qualquer sistema que seguir os padrões será capaz de se interconectar
- Possui sete camadas



Modelo de Referência TCP/IP

- Usado na “avó” de todas as redes, a ARPANET, e em sua sucessora, a Internet mundial
- Surgiu como um conjunto de protocolos que deveriam ter certas características para uso militar
- Seus protocolos são flexíveis para suportar diferentes aplicações
- Surgiu “oficialmente” com o re-projeto dos protocolos TCP/IP no início da década de 80

Modelo de Referência TCP/IP

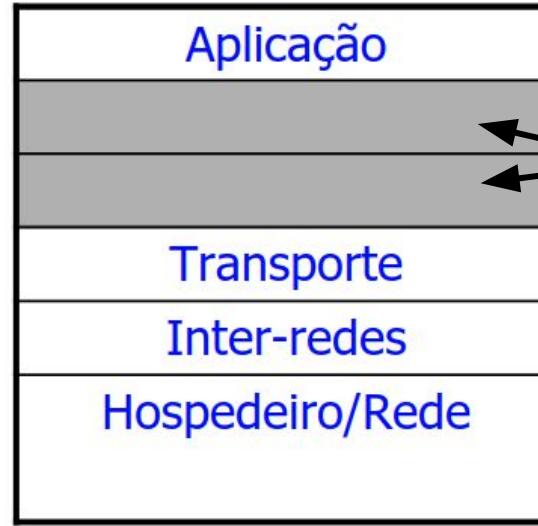
- O Depto de Defesa dos EUA desejava que as conexões ficassem intactas enquanto as máquinas de origem e destino estivessem funcionando. Isso, mesmo que algumas máquinas ou linhas de transmissão intermediárias deixassem de operar repentinamente

Modelo de Referência TCP/IP

OSI



TCP/IP



Não presentes no modelo (são pouco usadas na maioria das aplicações)

Camada Hospedeiro / Rede

- Protocolo não definido pelo modelo TCP/IP
- Responsável por transmitir os pacotes IPs
- Protocolo varia em função do hospedeiro e rede



Camada Inter-redes

- Normalmente, chamada de “camada de rede”
- Sem conexão
- Ponto fundamental da arquitetura
- Define *Internet Protocol* (IP), a “cola” da Internet
- Maiores questões: roteamento e controle de congestionamento



Camada de Transporte

- Nome dado à camada acima do nível IP
- Responsável pela comunicação fim-a-fim
- Dois dos protocolos mais usados são:
 - *Transmission Control Protocol* (TCP)
 - *User Datagram Protocol* (UDP)



Protocolo TCP

- Protocolo orientado à conexão confiável
- Usa *byte stream*
- Normalmente, fragmenta um *byte stream*, pois o pacote IP tem um tamanho máximo
- Hospedeiro destinatário faz o processo contrário
- Faz controle de fluxo

Protocolo UDP

- Protocolo não orientado à conexão e não confiável
- Usado normalmente em aplicações que somente interagem uma única vez com outra aplicação (*one-shot*)
- Exemplo, *request-reply* no paradigma cliente-servidor

Camada de Aplicação

- Protocolos: http, smtp, telnet, ftp, email, etc.



Modelo de Referência Híbrido



Exercício (4)

- Determine qual das camadas do modelo TCP/IP trata de cada uma das tarefas a seguir:
 - a) Dividir o fluxo de bits transmitidos em quadros.
 - b) Definir a rota que será utilizada na sub-rede.

Exercício (5)

- Cite dois aspectos em que os modelos de referência OSI e TCP/IP são similares e dois em que eles são diferentes.

Exercício (6)

- Qual é a principal diferença entre o TCP e o UDP?

Unidade II:

Camada Física

Prof. Max do Val Machado



Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Disciplina Redes de Computadores I

Agenda

- Introdução
- Métricas da rede
- Meios de transmissão (guiados, sem fio e satélite)

Agenda

- Introdução
- Métricas da rede
- Meios de transmissão (guiados, sem fio e satélite)

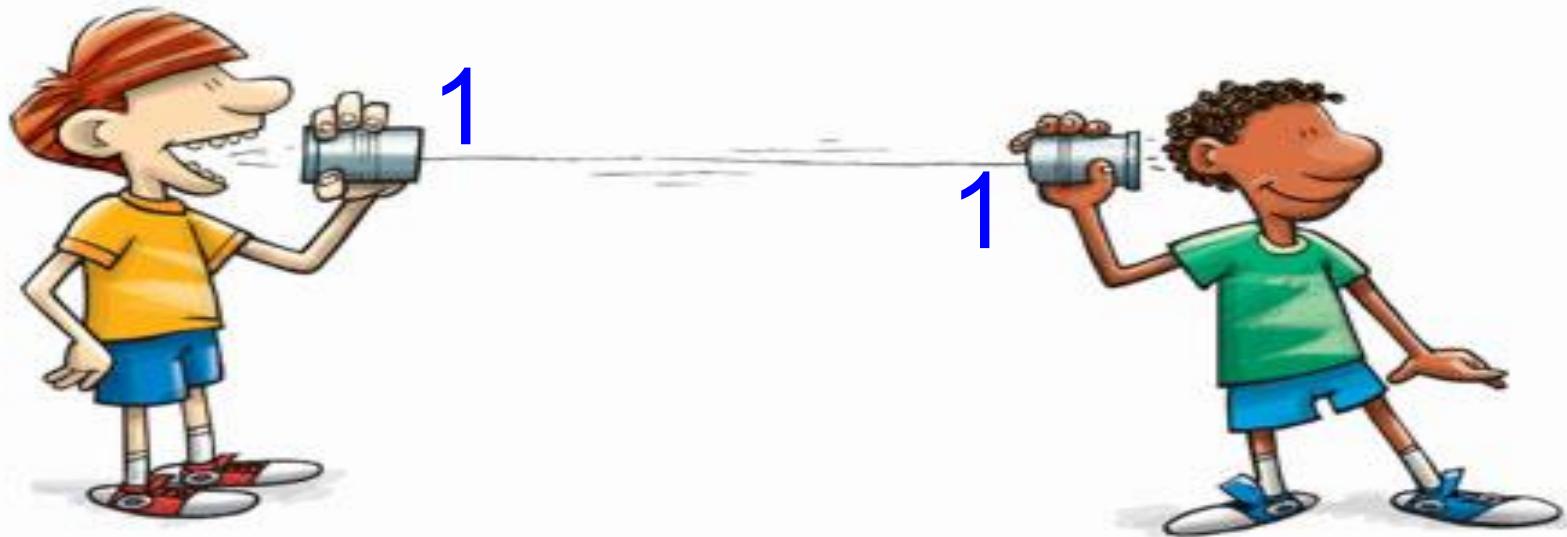
Introdução

- A camada física é o alicerce sobre o qual a rede é construída

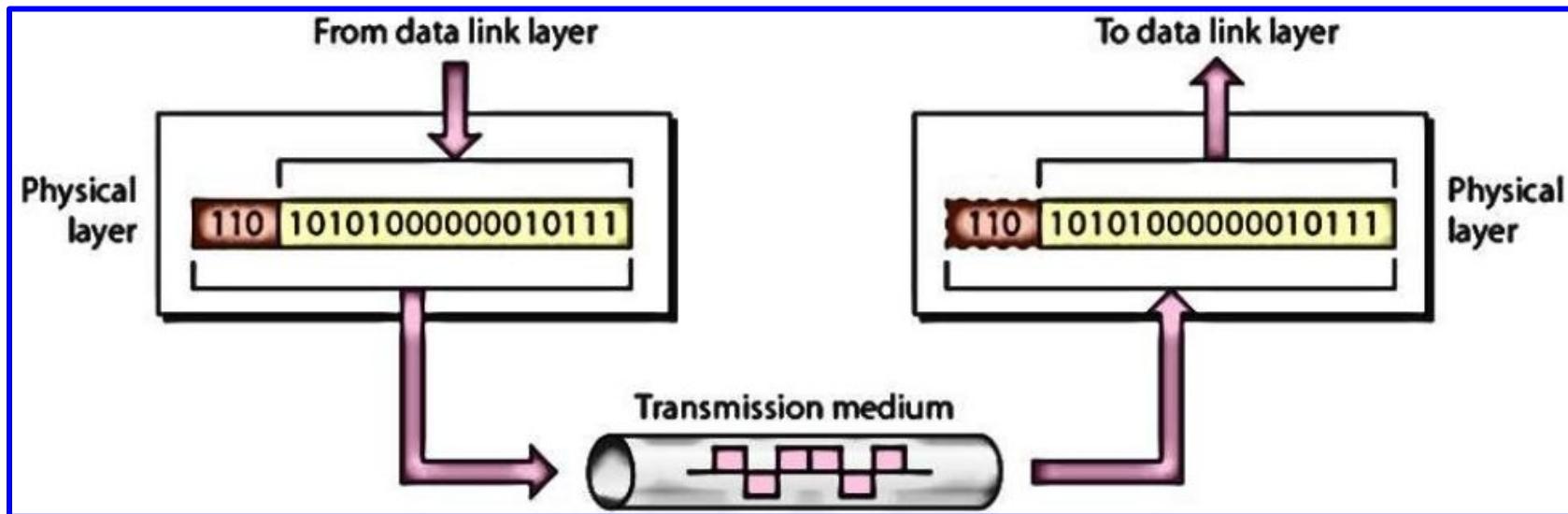


Introdução

- A camada física trata da transmissão de bits através do canal, garantindo que quando um lado enviar um bit 1, o outro o receberá o bit 1 (não um 0)



Introdução



- Questões a serem consideradas na Camada Física

- Quais sinais elétricos serão usados para representar cada bit (0 e 1)
- Quantidade de nanossegundos que um bit deve durar
- Transmissão pode ser realizada simultaneamente nos dois sentidos
- Como uma conexão será estabelecida/terminada
- Quantos pinos o conector de rede terá e qual é a finalidade de cada pino

Introdução

- A camada física define interfaces elétrica, de sincronização e outras, pelas quais os bits são enviados como sinais pelos canais
- As propriedades dos diferentes tipos de canais físicos determinam o desempenho (e.g., latência^(?), throughput^(?) e taxa de erros) e, consequentemente, o projeto da rede

Agenda

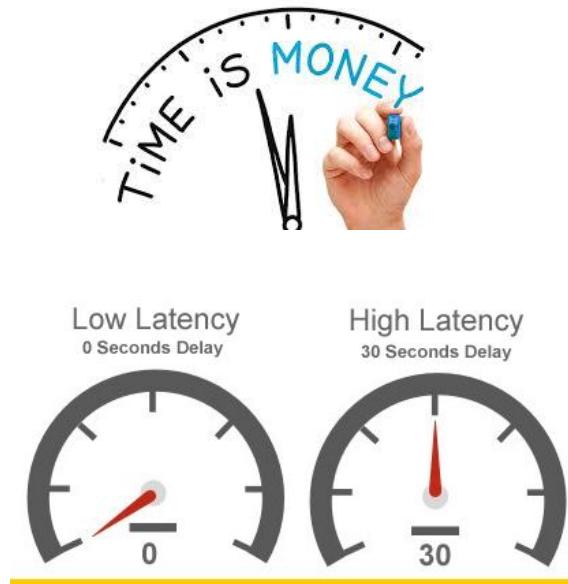
- Introdução
- **Métricas da Rede**
- Meios de Transmissão

Métricas da Rede

- Custo
- Facilidade de instalação e manutenção
- Taxa de Erros
- *Latency* (Latência)
- *Bandwidth* (Largura de Banda)
- *Troughput* (Taxa de Dados)

Latency (Latência)

- Também conhecida como atraso (*delay*) ou retardo



Tipos de Atraso

- Decorrente de processamento (por exemplo, CPU)
- Decorrente de enfileiramento (por exemplo, FIFO)
- Decorrente de serialização
- Decorrente de propagação fim a fim. Por exemplo, um enlace entre Belo Horizonte e Contagem será mais rápido que outro entre BH e São Luís (MA)

Bandwidth (Largura de Banda)

- Quantidade **máxima** de dados que pode ser transmitida em um canal durante um intervalo de tempo
- Propriedade física do canal
 - Depende, por exemplo: da construção, espessura e comprimento do meio

Bandwidth (Largura de Banda)

- Para o Engenheiro Eletricista, a largura de banda (análogica) é uma quantidade medida em Hz
- Para o Cientista da Computação, a largura de banda (digital) é a taxa de dados máxima de um canal, uma quantidade medida em bits/s
- Na verdade, a taxa de dados (do Cientista da Computação) é o resultado final do uso da largura de banda

Lei de Shannon-Hartley

$$C = B \times \lg\left(1 + \frac{P}{N}\right) [bits/s]$$

C, capacidade do canal

B, largura de banda do canal em Hz

P, potência do sinal transmitido

N, potência do ruído adicionado ao sinal no canal

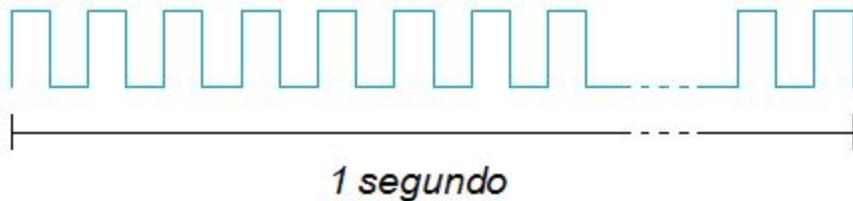
Troughput (Taxa de Dados)

- Número de bits transmitidos por unidade de tempo
- Unidades básicas: bps, Kbps, Mbps, Gbps ou *packets per seconds* (pps)

Troughput (Taxa de Dados)

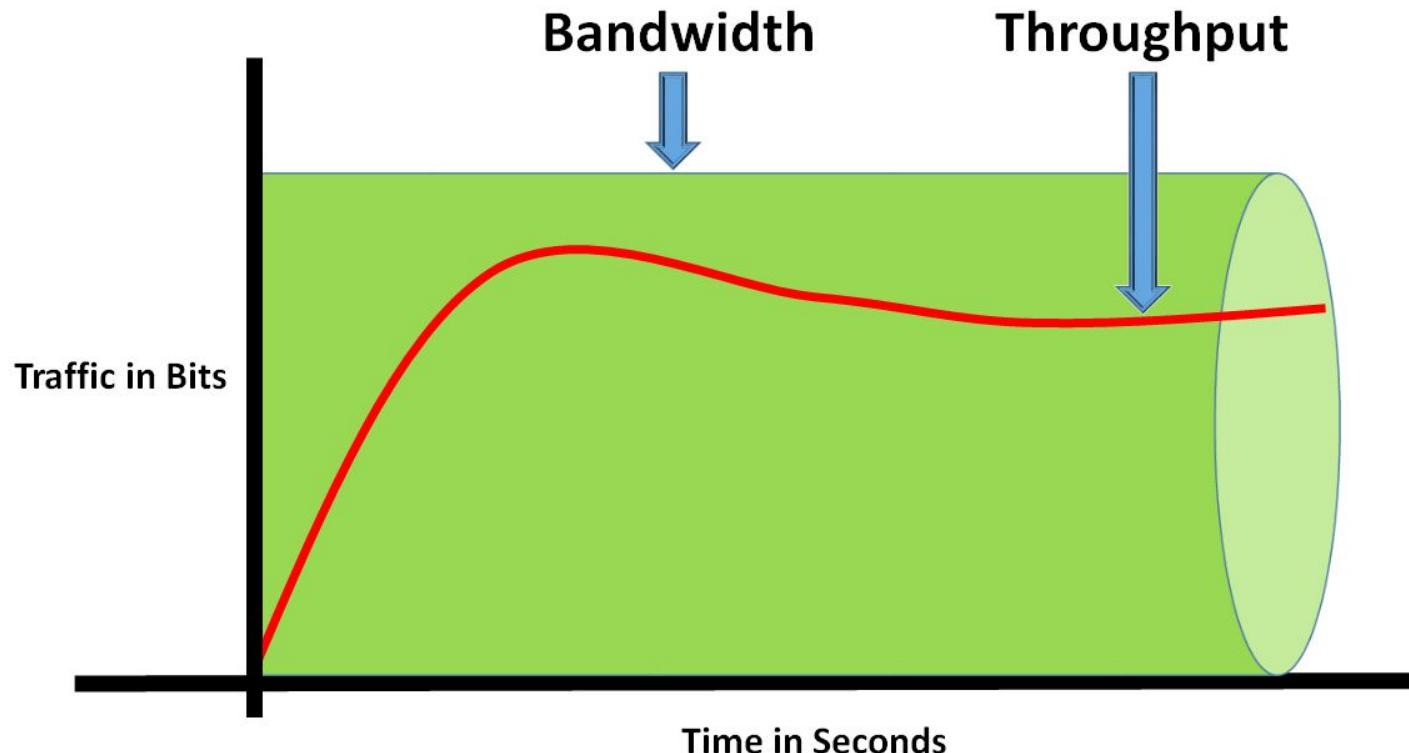


1 Mbps: 1 milhão de bits por segundo (1 μ s para transmitir cada bit)

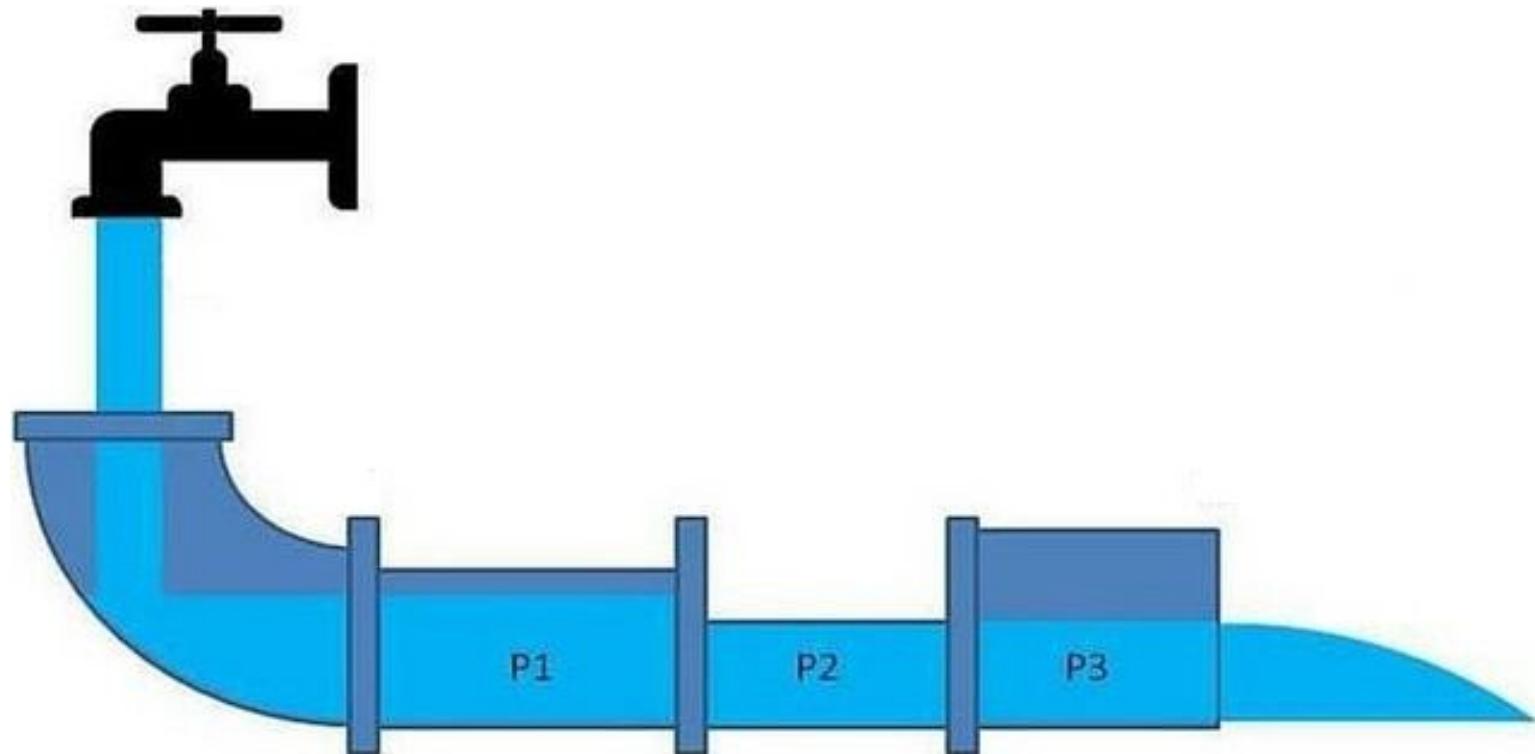


2 Mbps: 2 milhões de bits por segundo (0.5 μ s para transmitir cada bit)

Troughput x Bandwidth

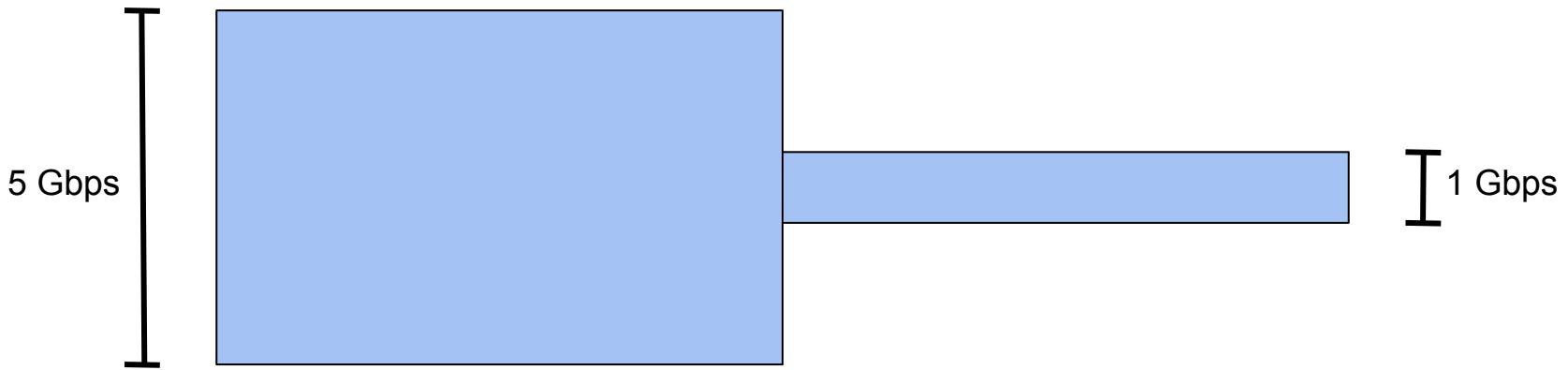


Troughput x Bandwidth

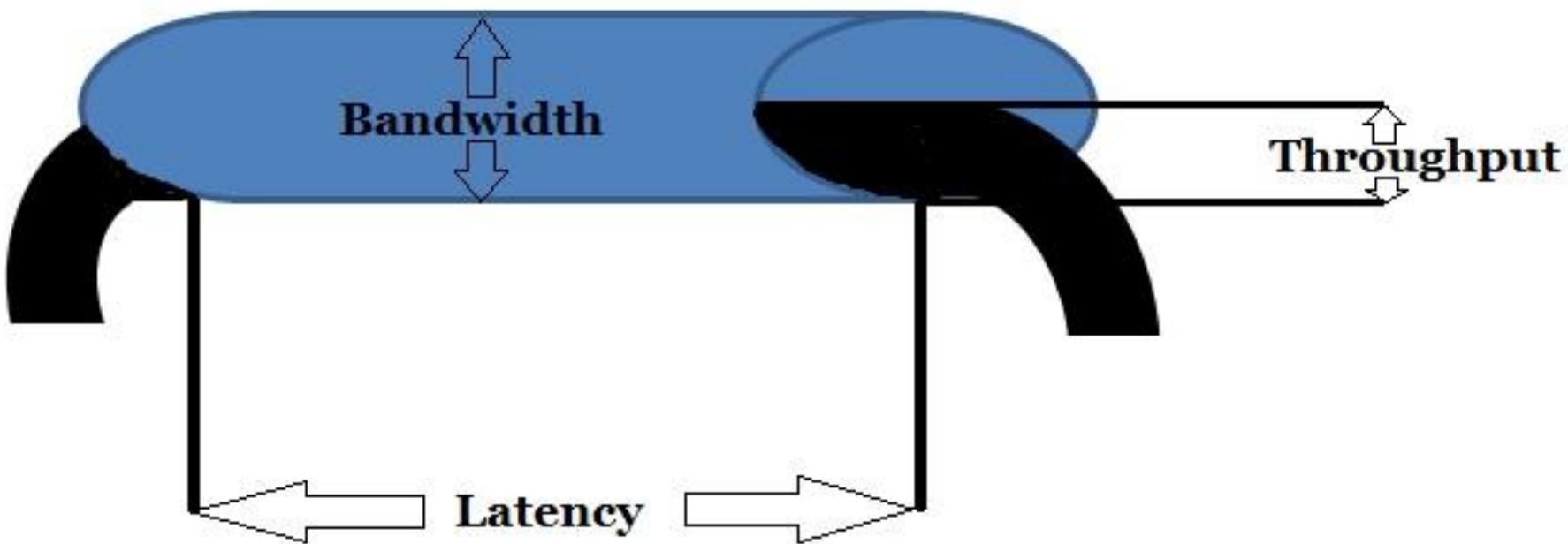


Troughput x Bandwidth

- Por exemplo, se dois pontos da rede tem *bandwidth* de 5 Gbps e 1 Gbps, o *throughput* será, no máximo, 1 Gbps



Throughput x Bandwidth x Latency



MB, Mbps, KB, Kbps

- **b** significa bits e **B** bytes
- Na Computação, Kilo significa 2^{10} , não, 10^3
- Na Computação, Mega significa 2^{20} , não 10^6
- Largura de banda
 - Está relacionada com velocidade de clock (Hz)
 - Mbps significa 10^6 bits por segundo
- Mensagem a ser transmitida: armazenada na memória e medida em potência de 2

Unidades Métricas

Agenda

- Introdução
- Métricas da Rede
- **Meios de Transmissão**

Meios de Transmissão

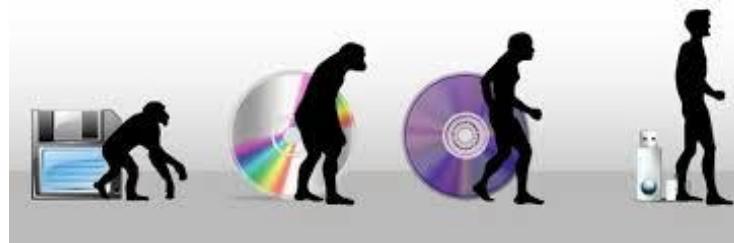
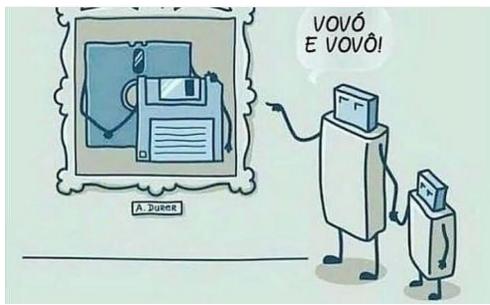
- **Guiados:** Meios magnéticos, pares trançados, cabo coaxial, linha de energia elétrica e fibra óptica
- **Sem fio:** Rádio, micro-ondas, infravermelho e luz
- **Satélites de Comunicação:** Geoestacionários e terrestres

Meios de Transmissão

- **Guiados:** Meios magnéticos, pares trançados, cabo coaxial, linha de energia elétrica e fibra óptica
- **Sem fio:** Rádio, micro-ondas, infravermelho e luz
- **Satélites de Comunicação:** Geoestacionários e terrestres

Meios de Transmissão Magnéticos

- Uma forma comum de transportar dados é gravá-los em fita magnética ou outra mídia removível



Meios de Transmissão Magnéticos

- Apesar de não ser sofisticado, esse método pode ser eficaz sob o ponto de vista financeiro em aplicações em que a alta largura de banda ou o custo por bit têm importância fundamental
- Vamos fazer um cálculo simples ...

Meios de Transmissão Magnéticos

- Uma fita Ultrium de pode armazenar 800 GB [Tanenbaum, 2011]
- Uma caixa de $60 \times 60 \times 60$ cm pode conter cerca de 1000 fitas desse tipo, ou seja, 800 TB, ou 6.400 Tb (6,4 petabits)
- Nossa caixa pode ser entregue em qualquer parte dos EUA em 24h (86.400 s)
- Largura de banda = $6.400 \text{ terabits} / 86.400 \text{ s} \approx 70 \text{ Gbps}$
- Se o destino estiver a 1 hora, a largura de banda $\approx 1.700 \text{ Gbps}$

Meios de Transmissão Magnéticos

- Nenhuma rede de computadores alcança 1.700 Gbps e ainda podemos melhorar nossa tecnologia



- Logicamente, as redes estão ficando mais rápidas, contudo, a densidade das fitas está aumentando

Meios de Transmissão Magnéticos

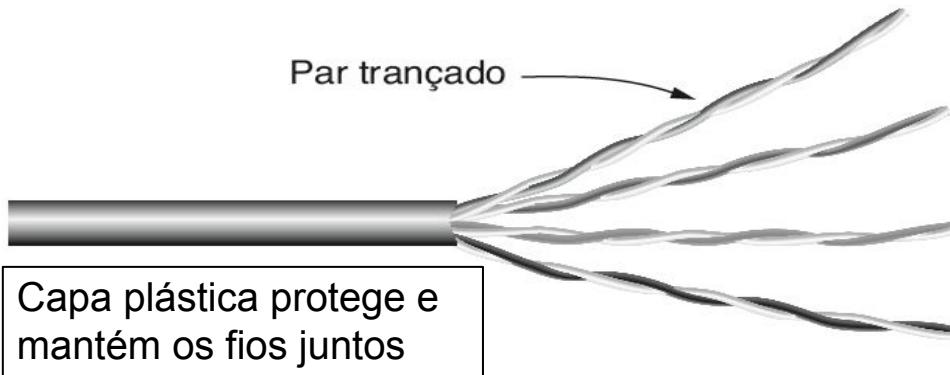
- O resultado financeiro também é interessante
- Fita Ultrium \approx US\$ 40 [compra no atacado] e pode ser reutilizada 10 vezes, logo, US\$ 4 por cada 800 GB
- O custo das fitas passa a ser US\$ 4.000 por caixa mais US\$ 1.000 pelo frete, temos: US\$ 5.000 para transportar 800 TB, ou seja, 1 GB \approx US\$ 0.5

Meios de Transmissão Magnéticos

- Moral da história: Não subestime a largura de banda de uma caminhonete cheia de fitas “voando” na estrada
- Embora as características de largura de banda da fita magnética sejam excelentes, as características de atraso são ruins

Pares Trançados

- Tem 2 fios de cobre encapados ($\approx 1\text{mm}$ de espessura)
- Fios enrolados de forma helicoidal como uma molécula de DNA
- São trançados para que as ondas se cancelam, minimizando interferência



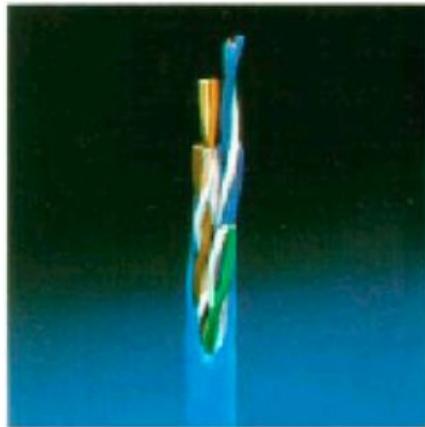
Pares Trançados

- Um dos meios de transmissão mais antigos e comuns
- Usado no sistema telefônico: chamadas e acesso à Internet por ADSL
- Diversos quilômetros sem amplificação (em redes pequenas, 100 metros)
- Transmissão de sinais analógicos ou digitais
- Largura de banda depende do comprimento e da espessura do cabo

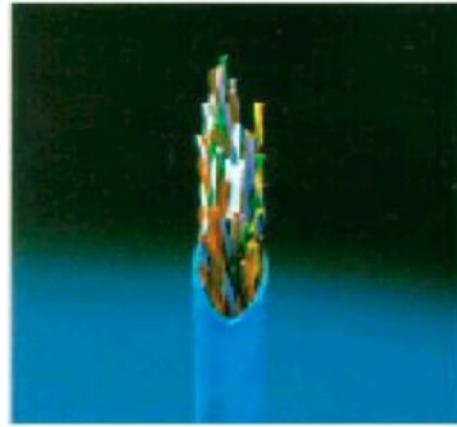
Pares Trançados

- Fácil instalação e baixo custo
- Normalmente, quatro pares agrupados

O padrão Ethernet de 100 Mbps usa dois (dos quatro) pares, um para cada direção. O Ethernet de 1 Gbps usa todos os quatro pares nas duas direções simultaneamente.



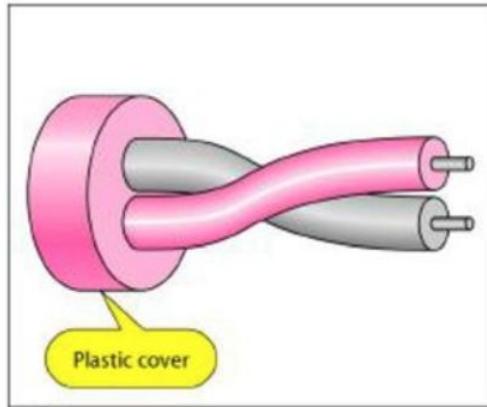
4 pares



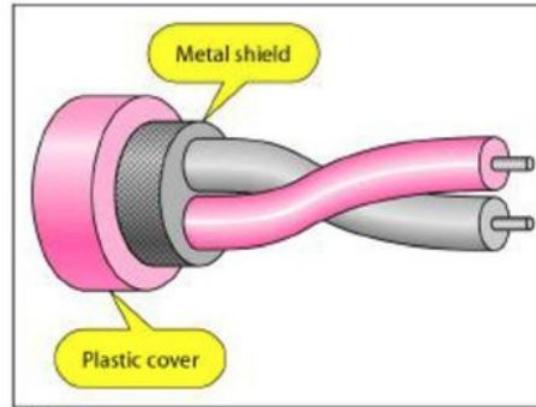
25 pares

Tipos de Pares Trançados

- Não blindados (*Unshielded Twisted Pair*, UTP): melhor custo
 - Categorias 1 a 6 sendo que o Cat 5e é o mais utilizado
- Blindados (*Shielded Twisted Pair*, STP): melhor proteção eletromagnética

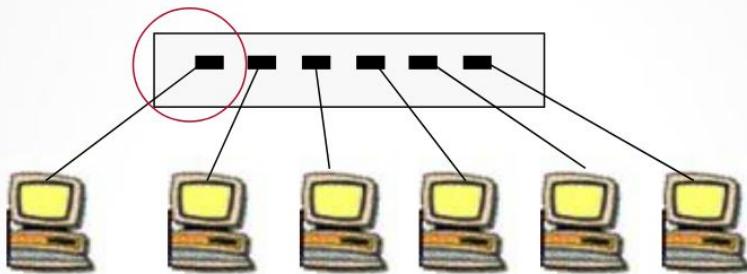


UTP

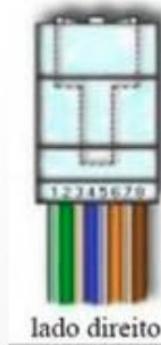


STP

Usando os Pares Trançados

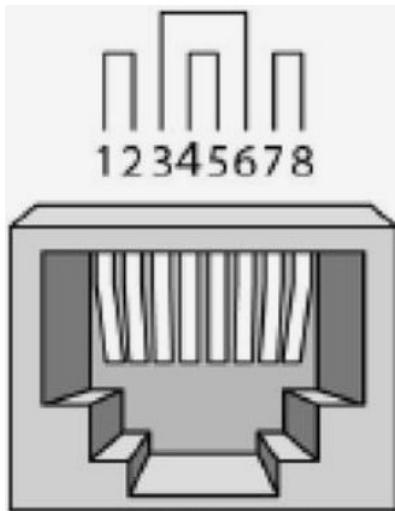


Conector RJ 45

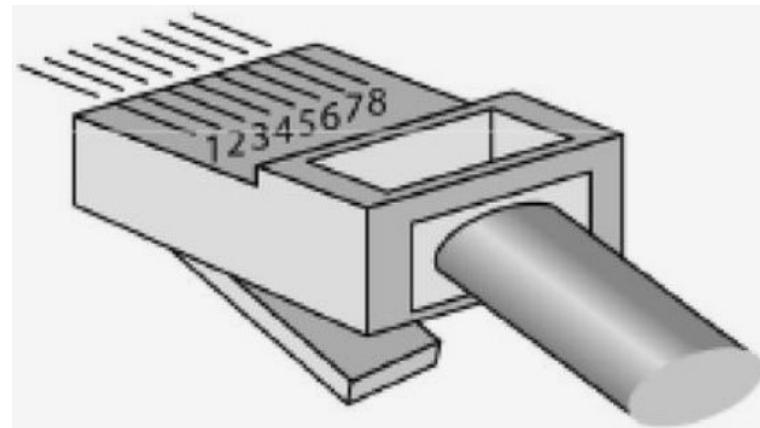


- Conector da direita:
- | |
|-----------------------|
| 1- Branco com Verde |
| 2- Verde |
| 3- Branco com Laranja |
| 4- Azul |
| 5- Branco com Azul |
| 6- Laranja |
| 7- Branco com Marrom |
| 8- Marrom |

Conectores RJ-45



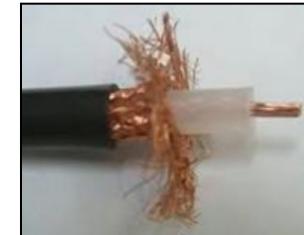
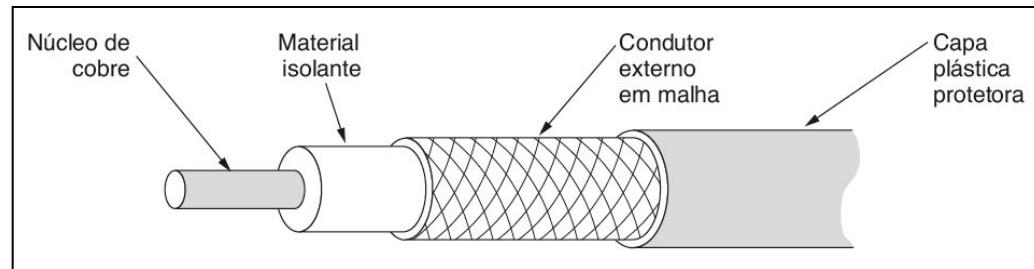
Fêmea



Macho

Cabo Coaxial

- **Blindagem melhor que os pares trançados**, permitindo seu uso em distâncias mais longas e com maior velocidade



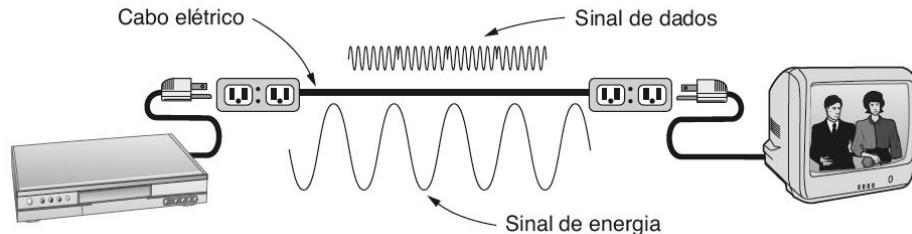
- A construção e a blindagem do cabo coaxial proporcionam a ele uma boa combinação de alta largura de banda e excelente imunidade ao ruído

Cabo Coaxial

- Largura de banda depende da qualidade e do tamanho do cabo
- Atualmente, os cabos têm uma largura de banda de até alguns GHz
- Eram muito usados no sistema telefônico para linhas de longa distância, contudo, estão sendo substituídos por fibras ópticas
- Ainda usados em larga escala pelas redes de televisão a cabo e em redes metropolitanas

Linhas de Energia Elétrica

- Sobreposição de sinais
- Oscilações no sinal de dados: a rede não foi projetada para isso e pendente das propriedades elétricas da fiação e dos aparelhos ligados
- Inexistência do “trançado” perde a proteção contra ruídos
- Largura de banda: até 100 Mbps



Fibra Óptica

- A Lei de Moore previu a duplicação do número de transistores por chip a cada dois anos e, nas últimas décadas, observamos:
 - “essa” evolução no aumento do poder computacional
 - algo próximo na largura de banda dos enlaces
 - além da redução na taxa de erros para algo próximo a zero

Fibra Óptica

- Atualmente, as CPUs estão próximas do seu limite físico, causando o aumento do número de CPUs por chip
- Atualmente, a largura de banda das fibras ópticas pode ultrapassar 50 Tbps, contudo, por restrições de velocidade na conversão entre sinais elétricos e ópticos nosso limite é próximo de 100 Gbps

Vantagens da Fibra Óptica

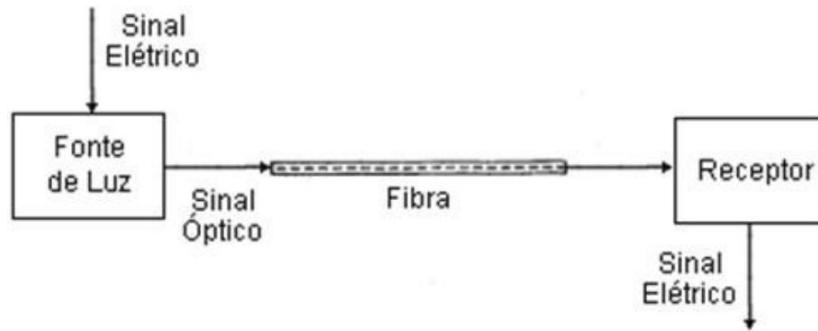
- Leve e pequena
- Baixa perda de sinal e grande banda passante
- Livre de interferências eletromagnéticas

Desafios da Fibra Óptica

- Dificuldade de conexão
- Acopladores do tipo T geram perdas
- Padronização dos componentes óticos
- A produção dos cabos é cara e complexa
- Conexões: atenuação de 10 a 20% da luz
- Junções mecânicas: atenuação de 10% da luz
- Fusão: pequena atenuação

Componentes do Sistema de Transmissão Óptico

- Fonte de luz
- Meio de transmissão: fibra de vidro ultrafina
- Detector/Receptor: gera um pulso elétrico quando a luz incide sobre ele

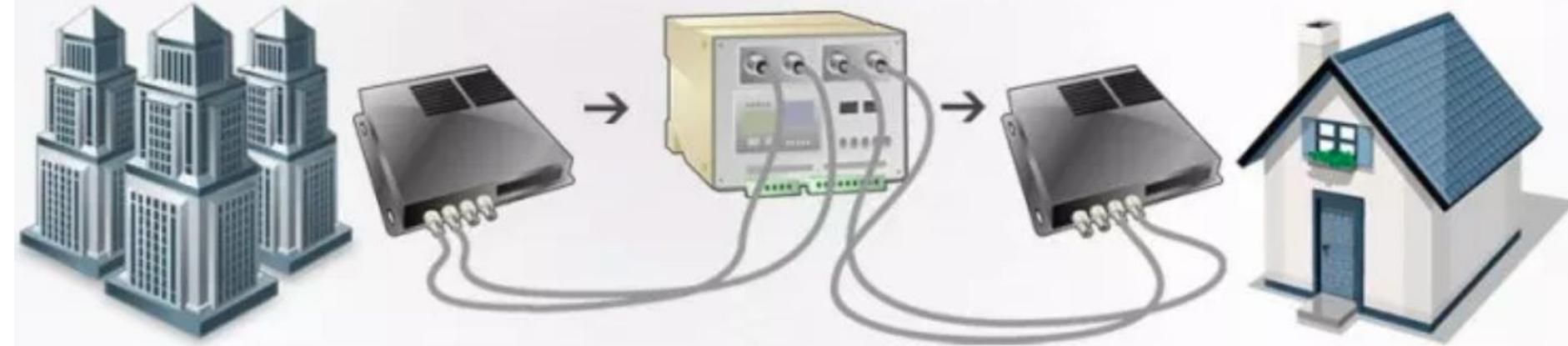


Componentes do Sistema de Transmissão Óptico

Transmissor
(converte o sinal de dados em luz)

Retransmissor
(necessário em grandes distâncias)

Receptor
(converte a luz em sinal de dados)

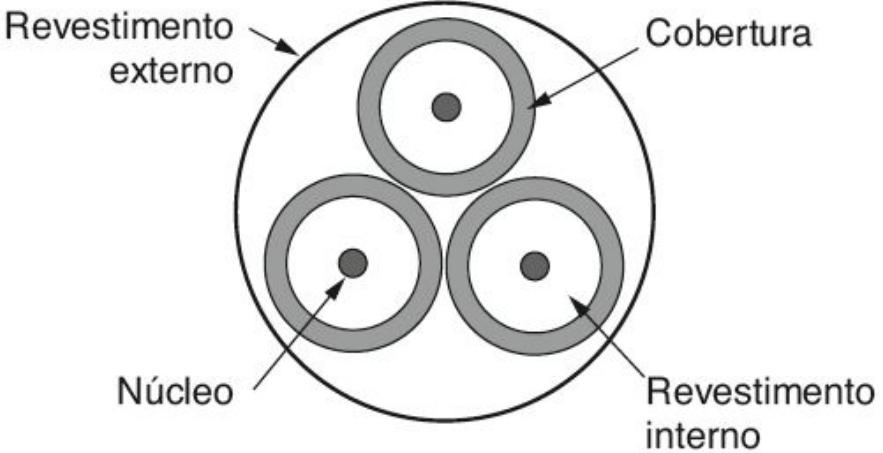
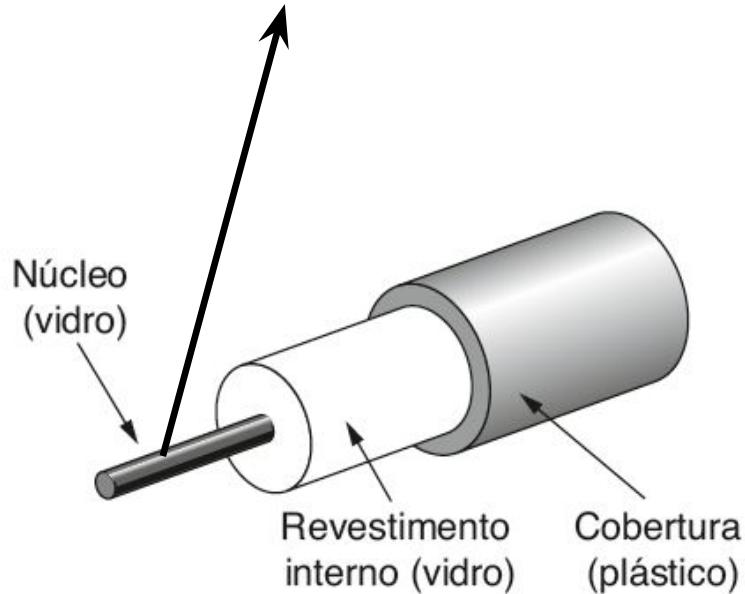


Estrutura do Cabo



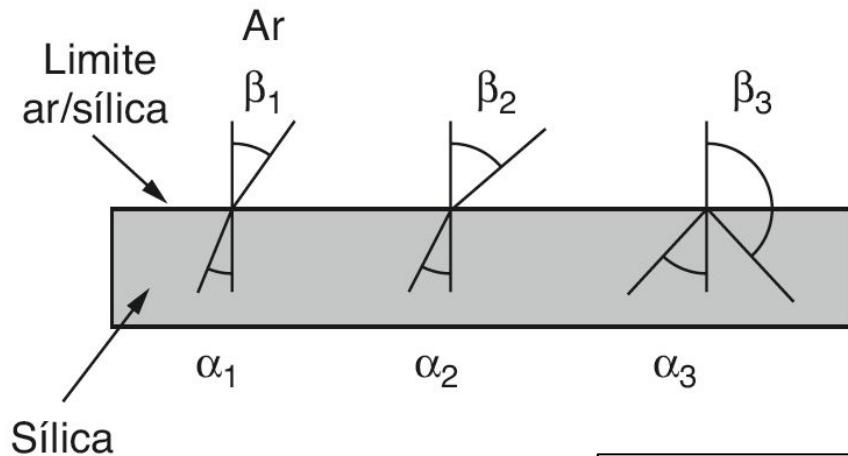
Estrutura do Cabo

Pode ser menor que um fio de cabo



Princípio Físico de Refração

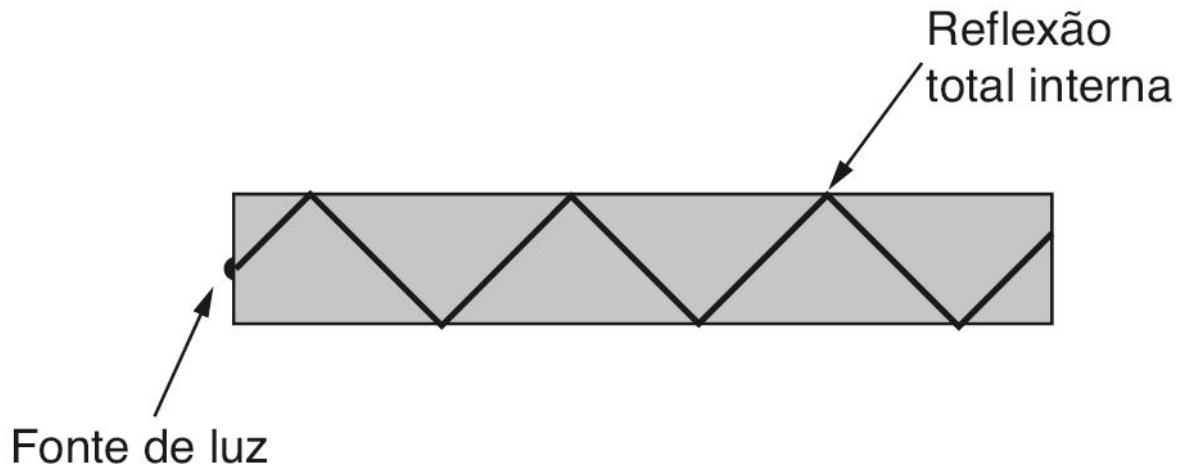
- Três exemplos de raios de luz incidentes internamente em diferentes ângulos na fronteira sílica/ar



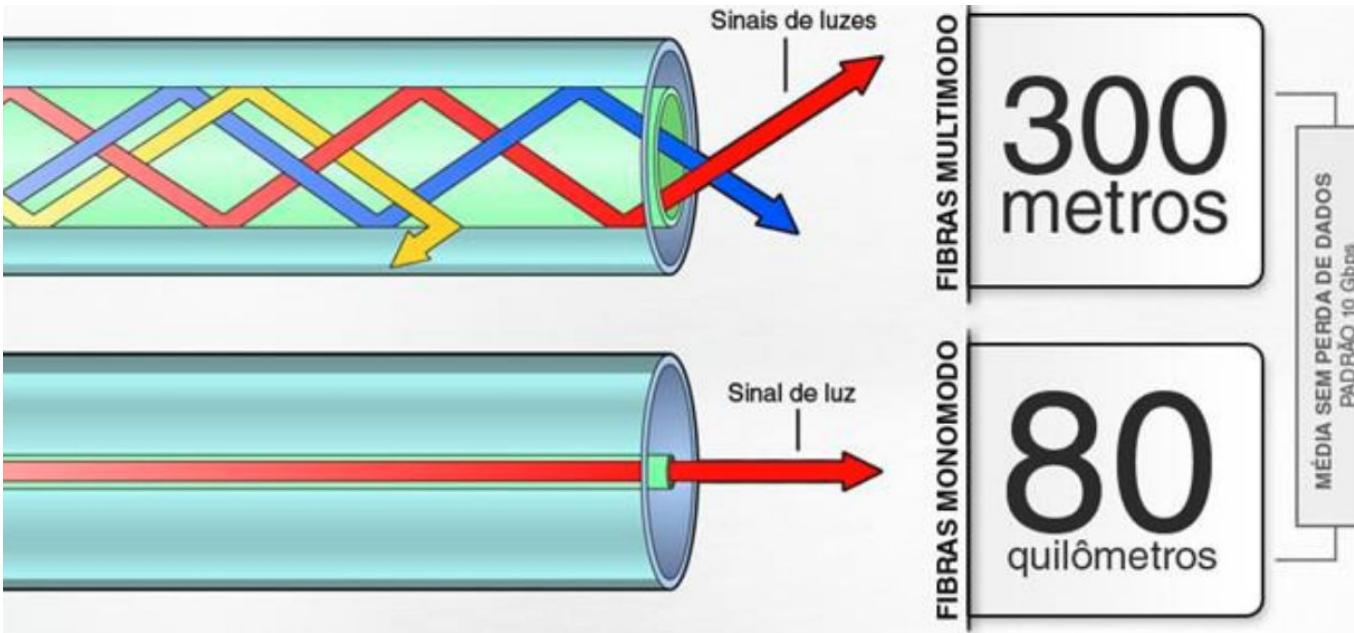
A quantidade de refração depende do índice de refração das duas mídias ar/sílica

Princípio Físico de Refração

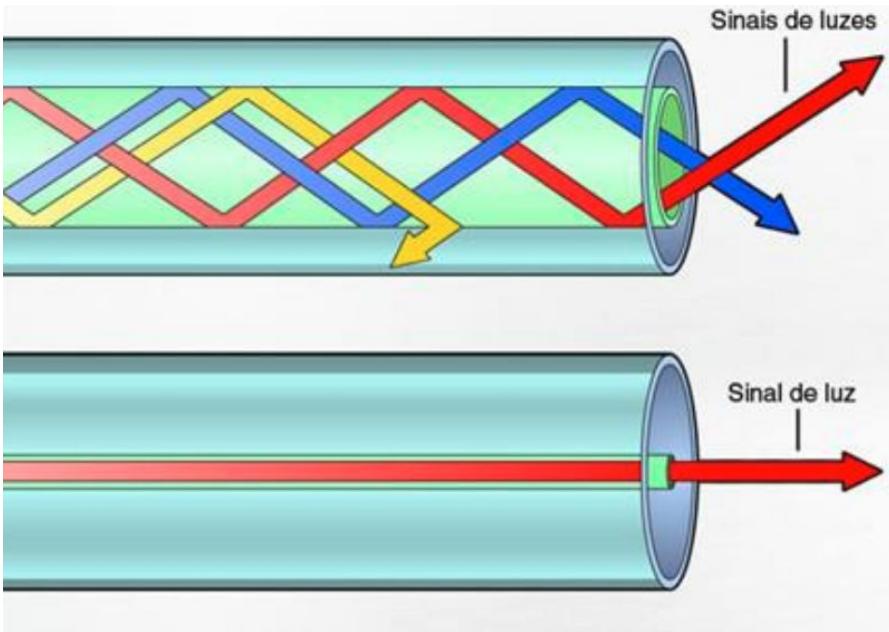
- Luz confinada pela reflexão total interna



Fibra Multimodo vs Fibra Monomodo



Fibra Multimodo vs Fibra Monomodo



A Multimodo pode ter vários raios

A monomodo tem diâmetro reduzido para que a luz propague em linha reta

A monomodo é mais cara, precisa e usada em longas distâncias

Fibras Ópticas vs Fios de Cobre

- A largura de banda das fibras é maior
- Os repetidores das fibras são necessários a cada 50 km e, no cobre, a cada 5 km
- A fibra não é afetada por picos de tensão, interferência eletromagnética ou quedas no fornecimento de energia
- A fibra é imune à ação corrosiva de elementos químicos que pairam no ar, despertando mais atenção em ambientes industriais

Fibras Ópticas vs Fios de Cobre

- A fibra é fina e leve sendo que muitos dutos de cabos estão lotados, despertando mais a atenção das empresas telefônicas
- A substituição do cobre por fibras pode esvaziar os dutos e o cobre ainda tem um excelente valor de revenda para as refinarias especializadas
- A fibra é mais leve. Por exemplo, 1000 pares trançados (1 km) pesam 8 toneladas sendo que duas fibras têm mais capacidade e pesam 100 kg

Fibras Ópticas vs Fios de Cobre

- Nas novas rotas, as fibras são preferidas por terem um custo de instalação muito mais baixo
- Por fim, as fibras não desperdiçam luz e dificilmente são interceptadas
- Desvantagens das fibras:
 - Tecnologia menos familiar (será que isso ainda é verdade?)
 - Danificada com mais facilidade
 - As interfaces de fibra são mais caras que as interfaces elétricas (será que isso ainda é verdade?)

Meios de Transmissão

- Guiados: Meios magnéticos, pares trançados, cabo coaxial, linha de energia elétrica e fibra óptica
- **Sem fio: Rádio, micro-ondas, infravermelho e luz**
- Satélites de Comunicação: Geoestacionários e terrestres

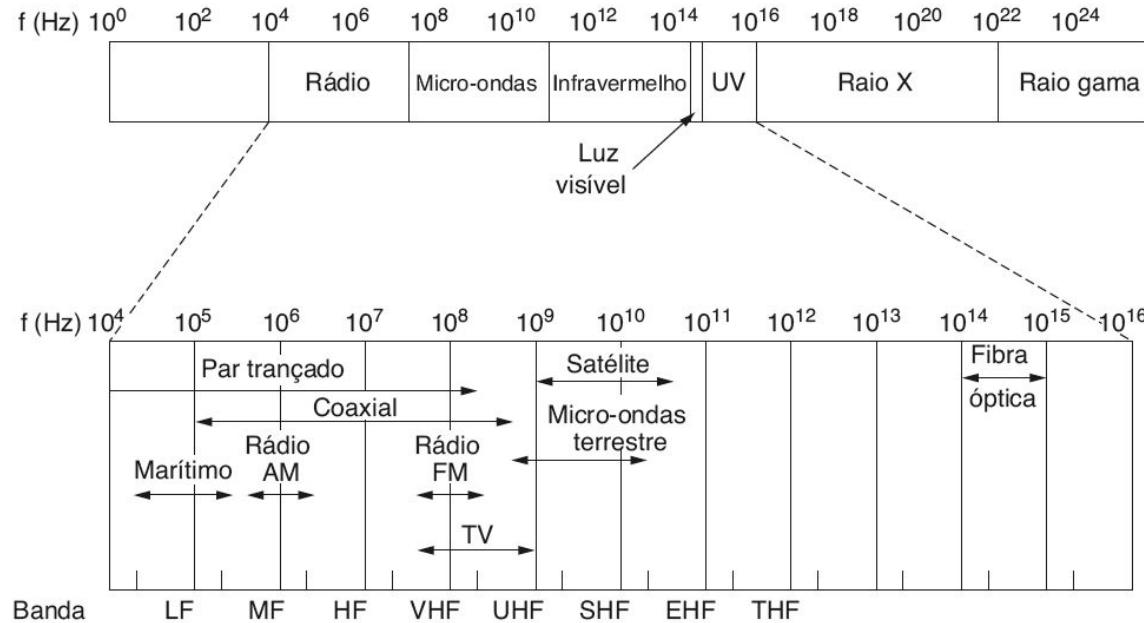
Princípio da Comunicação Sem Fio

- O movimento dos elétrons cria ondas eletromagnéticas que podem se propagar pelo espaço livre
 - Frequência (f): Número de oscilações por segundo de uma onda eletromagnética (Hz)
 - Comprimento de onda (λ): Distância entre dois pontos máximos (ou mínimos) consecutivos
- Quando se instala uma antena em um circuito elétrico, as ondas eletromagnéticas podem ser transmitidas e recebidas com por um receptor

Velocidade da Luz (c)

- Velocidade de todas as ondas eletromagnéticas no vácuo $\approx 3 \times 10^8$ m/s
- No cobre ou na fibra, cai para cerca de 2/3 desse valor e se torna ligeiramente dependente da frequência
- Limite máximo que se pode alcançar
- Relação fundamental (no vácuo) é: $\lambda f = c$

Espectro Eletromagnético



* A UV, raios X e raios gama são difíceis de produzir e modular, não se propagarem bem através dos prédios e são perigosos para os seres vivos

Transmissão de Rádio

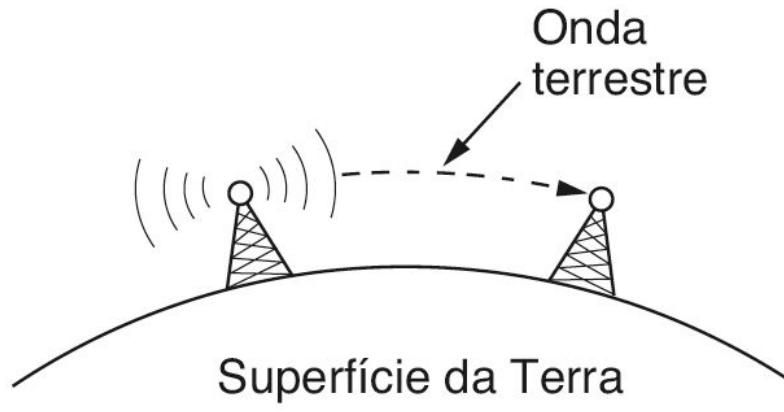
- Ondas fáceis de gerar, podem percorrer longas distâncias e penetrar facilmente nos prédios
- Amplamente utilizadas para comunicação
- Ondas omnidirecionais (viajam em todas as direções a partir da origem)
- Transmissor e receptor não precisam estar alinhados ponto a ponto

Freios Controladores dos Cadillacs em 1970



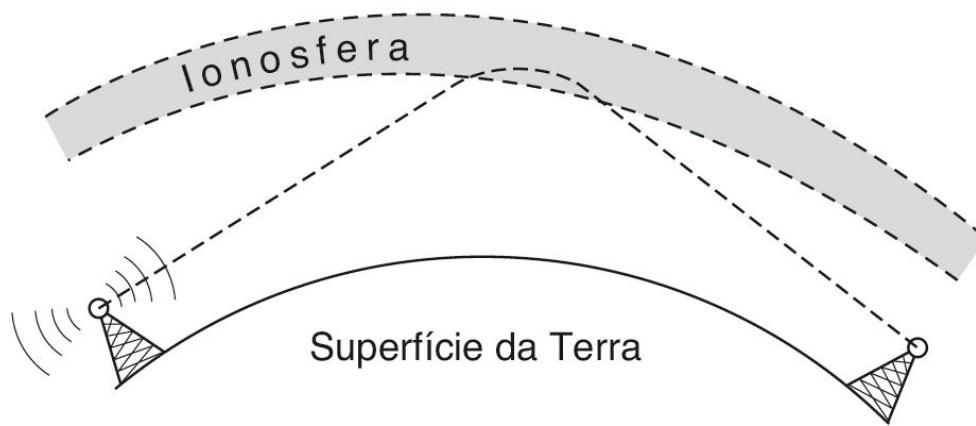
Ondas de Rádio

- Nas bandas VLF, VF e MF, as ondas obedecem à curvatura da Terra



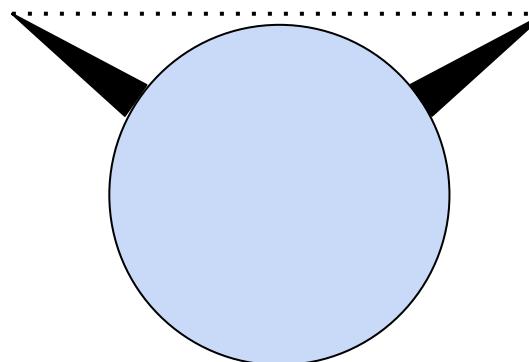
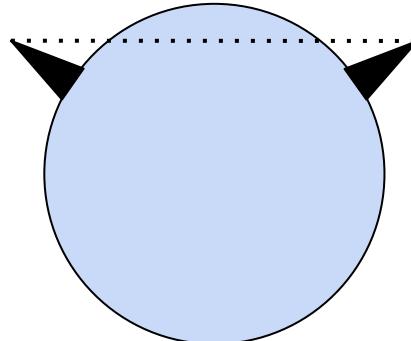
Ondas de Rádio

- Na banda HF, as ondas ricocheteiam na ionosfera



Micro-ondas

- Acima de 100 MHz, as ondas trafegam praticamente em linha reta
 - Antenas direcionais
 - Se duas torres estiverem muito afastadas, a Terra fica entre elas
 - Usa-se repetidores em intervalos periódicos. Quanto mais altas as torres, mais distantes elas podem estar umas das outras.



Micro-ondas

- Susceptíveis a interferência e atenuação, em especial, obstáculo e chuva
- Telefonia de longa distância, celular e sinais de televisão

Vantagens das Micro-ondas sobre as Fibras

- Dispensa a necessidade de se ter direitos sobre um caminho
- Com lotes/antenas a cada 50 quilômetros, é possível ignorar o sistema telefônico e se comunicar diretamente
- Enterrar 50 quilômetros de fibra em uma área urbana congestionada ou em uma região montanhosa não é uma tarefa simples

Políticas do Espectro Eletromagnético

- Para evitar o caos total, existem acordos nacionais e internacionais a respeito de quem terá o direito de usar cada uma das frequências
 - Governos nacionais alocam
 - International Telecommunication Union (ITU) - www.itu.int
 - Agencia Nacional de Telecomunicações (ANATEL) - www.anatel.gov.br

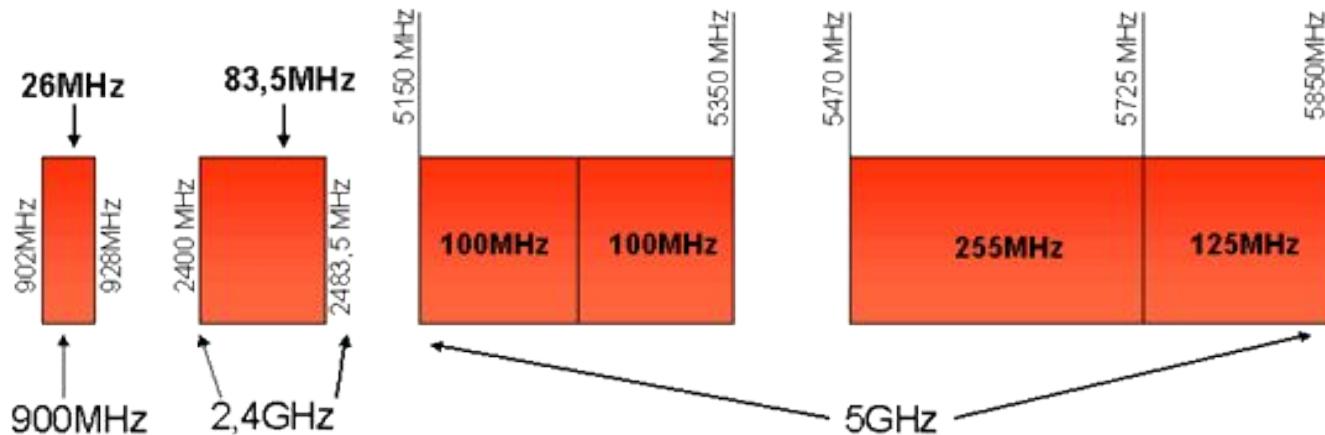
Políticas de Alocação

- Concurso de beleza: suborno, corrupção, nepotismo e crimes piores
- Sorteio: revenda
- Leilão: disputa frenética e irresponsável

Políticas de Alocação

- Não alocar
- Não existe restrição para transmissões
- Existe regulação de potências para que uma estação não interfira na outra
- A maioria dos governos reserva as bandas de frequência ISM (Industrial, Scientific, Medical) para uso sem licença (garagens, telefones sem fio, brinquedos que usam rádio, mouse sem fio e outros aparelhos domésticos)
- Técnicas para evitar interferência

Bandas ISM no Brasil

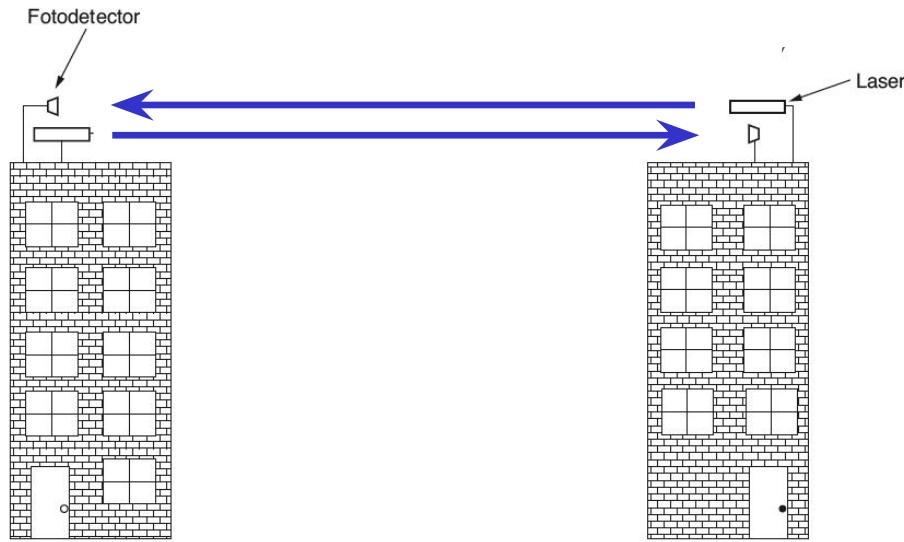


Infravermelho

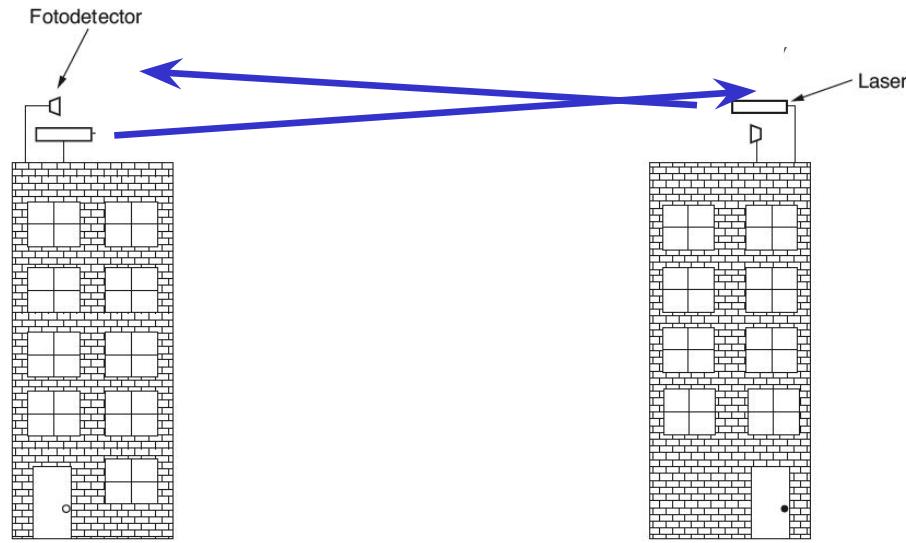
- Utilizadas na comunicação de curto alcance
- Indicado para conexão de dispositivos próximos (e.g., mesmo ambiente)
 - Por exemplo, dispositivos de controle remoto e conexão com periféricos
- Direcionais, econômicos e fáceis de montar
- Não atravessa objetos sólidos (por exemplo, parede)
 - Vantagens: segurança, sem interferência e não necessidade de licença governamental

- A transmissão óptica não guiada ou em espaço livre é utilizada há séculos
- Exemplo: conexão entre dois prédios usando lasers instalados nos telhados
 - Unidirecional; assim, cada prédio precisa de seu próprio raio laser e fotodetector
 - Largura de banda muito alta
 - Relativamente seguro (laser estreito), fácil de ser instalado e difícil de ser calibrado
 - Não precisa de uma licença governamental
 - Suscetível a vento, temperatura, chuva, Sol, neblina, ...
 - Muitos desses fatores não são problemas para se conectar duas naves espaciais

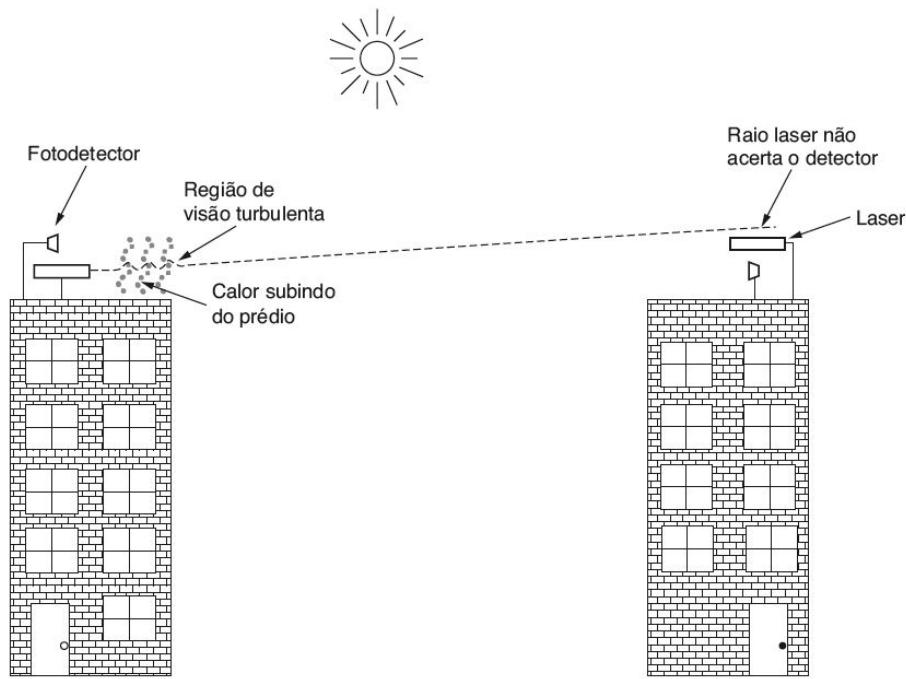
Exemplo da Conferência



Exemplo da Conferência



Exemplo da Conferência

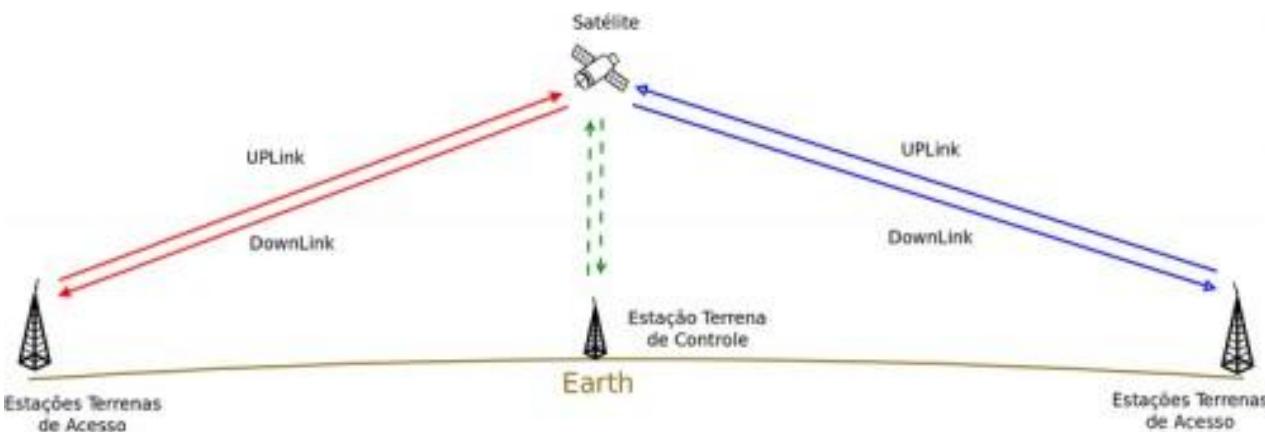


Meios de Transmissão

- Guiados: Meios magnéticos, pares trançados, cabo coaxial, linha de energia elétrica e fibra óptica
- Sem fio: Rádio, micro-ondas, infravermelho e luz
- **Satélites de Comunicação: Geoestacionários e terrestres**

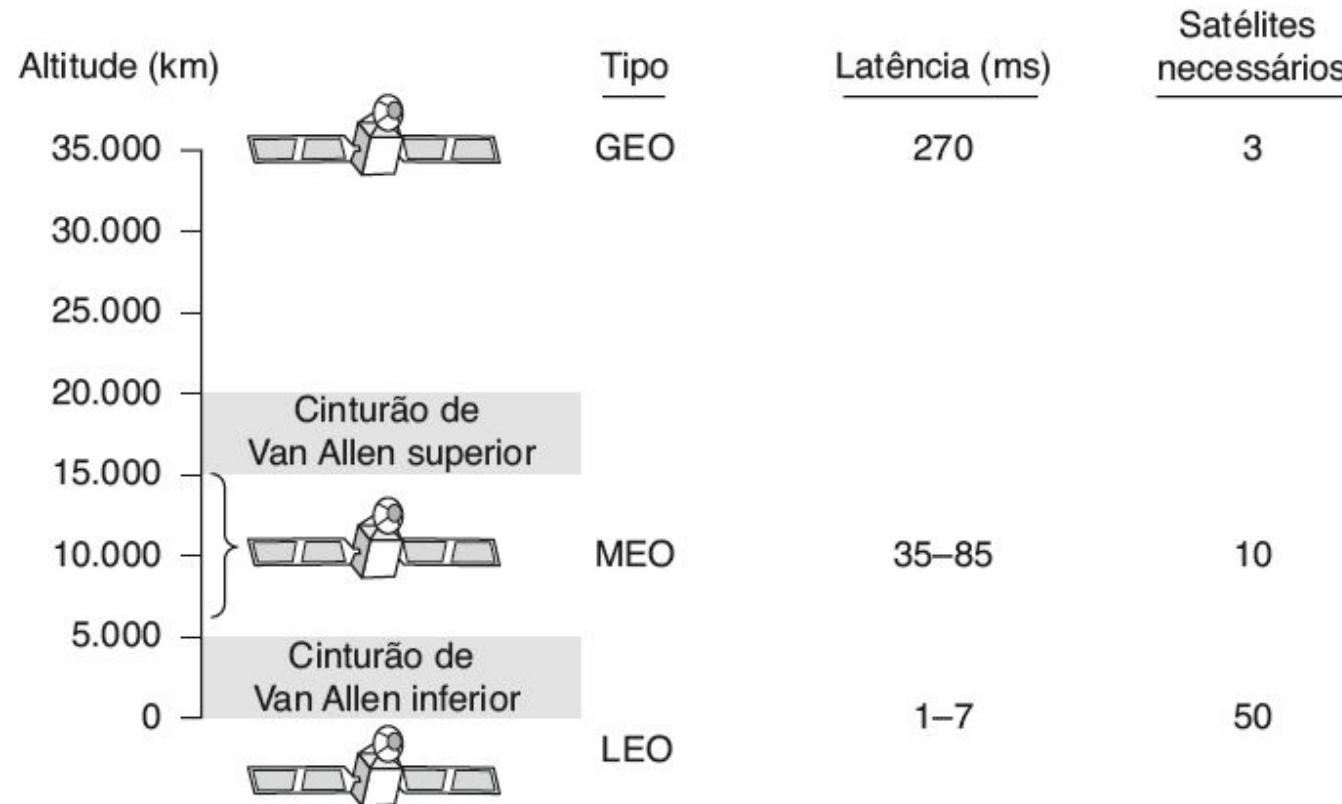
Satélite de Comunicação

- Pode ser considerado um grande repetidor de micro-ondas no céu
- Amplifica os sinais de entrada e os transmite novamente em outra frequência, para evitar interferência com o sinal de entrada



- Os satélites são basicamente meios de difusão
- Enviar uma mensagem para milhares de estações (na área de cobertura) não custa mais do que enviá-la para apenas uma estação
- Interessante para algumas aplicações, por exemplo, a transmissão de páginas web comuns para diversos *caches*
- A criptografia é essencial quando é necessário segurança

Algumas Propriedades dos Satélites

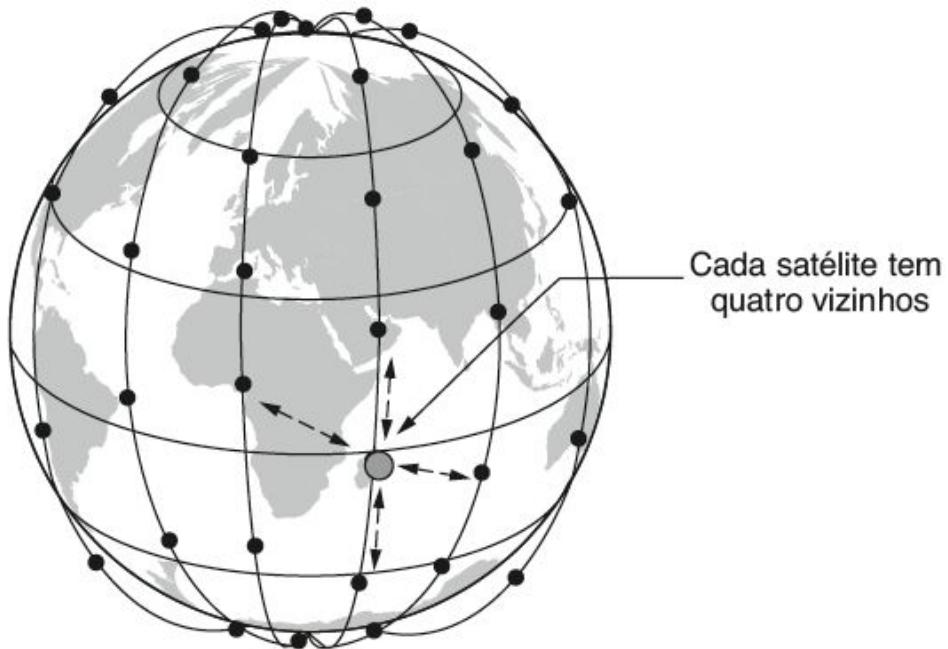


Exemplos de Satélites

- Satélites geoestacionários (GEO): VSATs
- Satélites terrestres de órbita média (MEO): Sistema de GPS
- Satélites terrestres de órbita baixa (LEO): Iridium e Globalstar

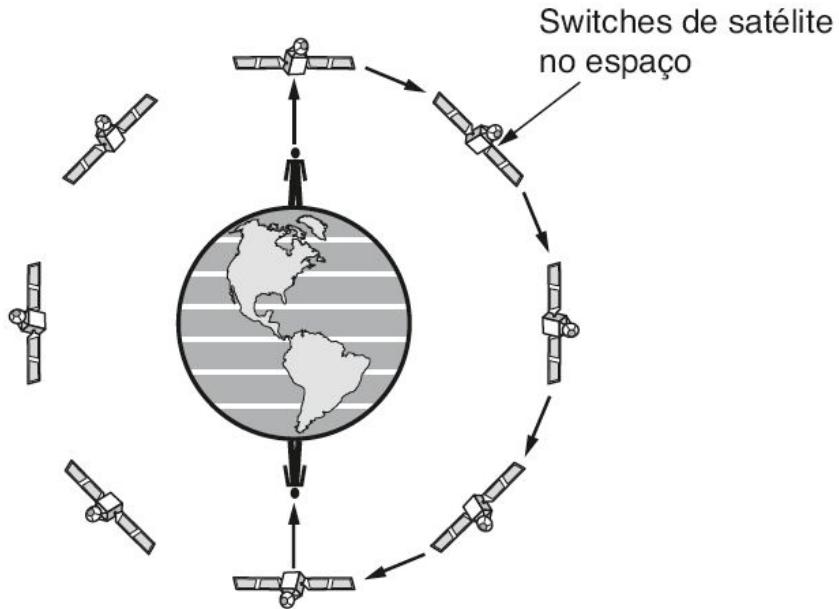
Satélites Iridium

- Formam seis cinturões em torno da Terra



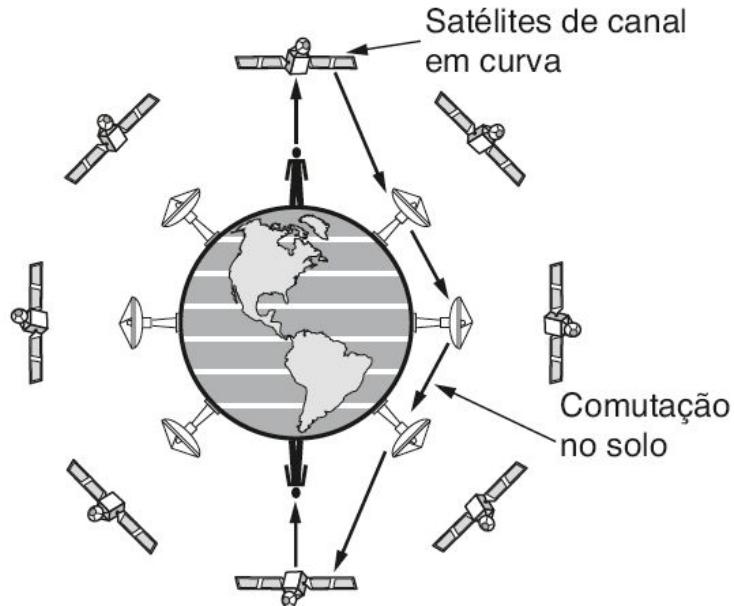
Satélites Iridium

- Emissor (Polo Norte), Destino (Polo Sul) e roteamento via satélites



Satélites Iridium

- Emissor (Polo Norte), Destino (Polo Sul) e roteamento via torres na Terra



Algumas Questões Políticas

- ITU aloca os slots de órbitas para evitar o caos total no céu
 - Alguns países se acham donos da “Terra/Espaço”, sustentando que os direitos nacionais de propriedade não se estendem para cima
 - Outros querem vantagens sobre “seus” slots de órbitas
- Para aumentar a disputa, as telecomunicações comerciais não são a única aplicação. Emissoras de TV, governos e instituições militares também querem ter uma fatia dessa torta orbital

Satélites de Comunicação Atuais

- Peso: até 5.000 kg
- Consumo de energia produzido por painéis solares
- Órbita afetada (gravidade Sol, Lua, e Terra) e ajustada (motor de foguetes)
- Término do combustível dos motores: órbita decai, reentrada na atmosfera e destruição total (raramente existe colisão com a Terra)
- Outra discórdia: as frequências do *downlink* interferem nas micro-ondas

Algumas Bandas de Satélites Alocadas pelo ITU

Banda	Downlink	Uplink	Largura de banda	Problemas
L	1,5 GHz	1,6 GHz	15 MHz	Baixa largura de banda; lotada
S	1,9 GHz	2,2 GHz	70 MHz	Baixa largura de banda; lotada
C	4,0 GHz	6,0 GHz	500 MHz	Interferência terrestre
Ku	11 GHz	14 GHz	500 MHz	Chuva
Ka	20 GHz	30 GHz	3.500 MHz	Chuva; custo do equipamento

Vantagens dos Satélites sobre as Fibras Ópticas

- Quando a implantação rápida é crítica, os satélites ganham facilmente. Uma resposta rápida é útil para sistemas de comunicação militares em tempos de guerra e resposta a desastres em tempos de paz
- Lugares onde a infraestrutura terrestre é pouco desenvolvida
- Difusão, pois uma mensagem enviada por satélite pode ser recebida por milhares de estações terrestres ao mesmo tempo

Exercício (1)

- Explique os termos Latência, Largura de Banda e Taxa de Dados

Exercício (2)

- Faça um paralelo entre o par trançado, cabo coaxial e fibra óptica

Exercício (3)

- Faça um paralelo entre fibra óptica e a comunicação via satélite

Exercício (4)

- Faça um paralelo entre fibra óptica e os meios de comunicação sem fio

Unidade III:

Camada de Enlace

Prof. Max do Val Machado



PUC Minas

Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Disciplina Redes de Computadores I

Agenda

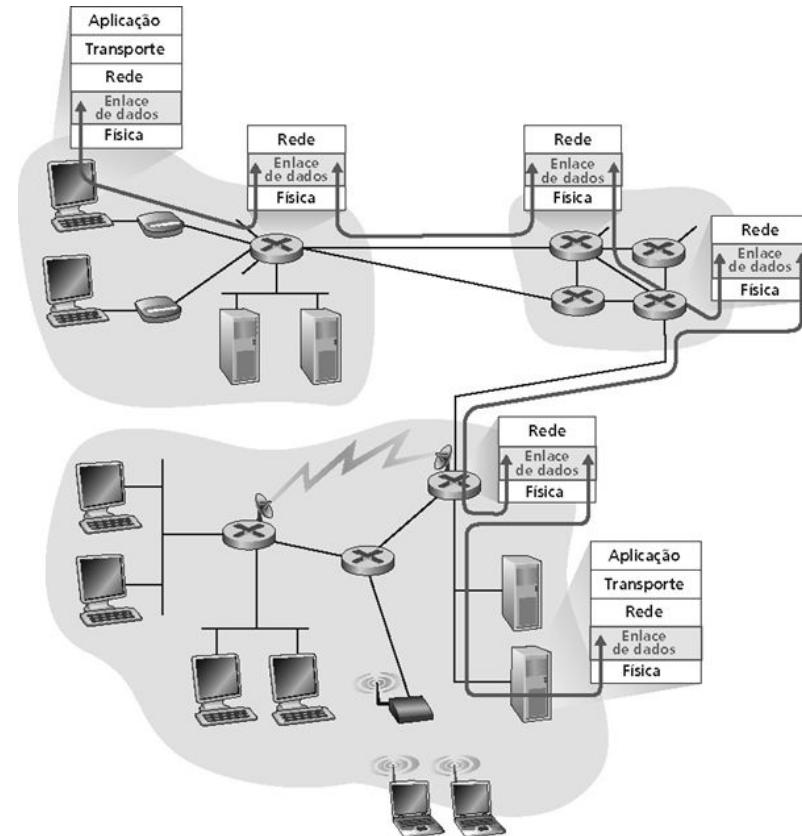
- Introdução
- Orientação à Conexão e Existência de Confirmação
- Enquadramento
- Controle de Fluxo
- Controle de Erro
- Camada de Enlace da Internet

Agenda

- **Introdução**
- Orientação à Conexão e Existência de Confirmação
- Enquadramento
- Controle de Fluxo
- Controle de Erro
- Camada de Enlace da Internet

Conceitos Básicos

- **Nós:** os hospedeiros e os roteadores
- **Enlaces:** os canais de comunicação que se conectam a nós adjacentes pelo caminho de comunicação (por exemplo, os enlaces com fio, os sem e as LANs)

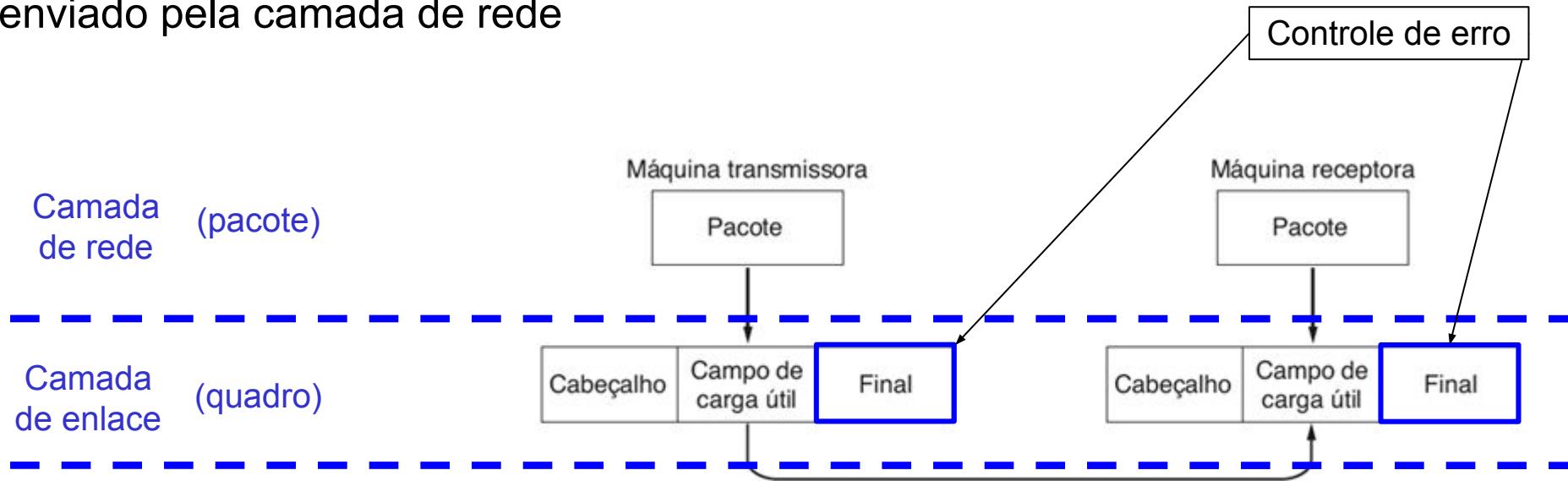


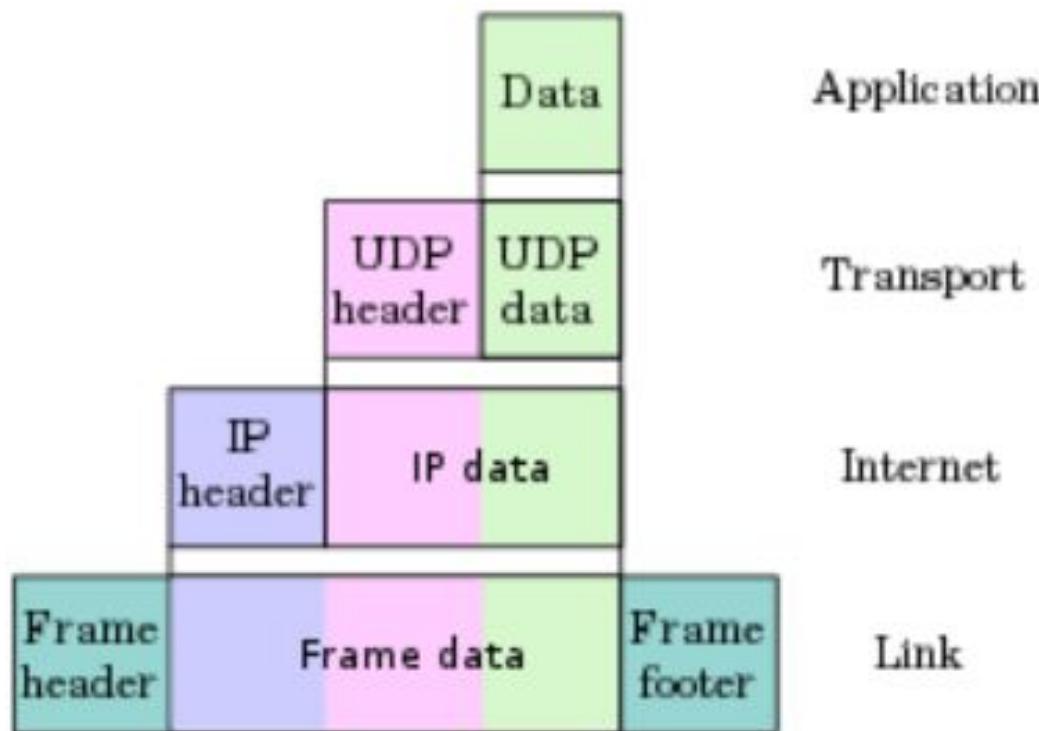
Tipos de Enlaces

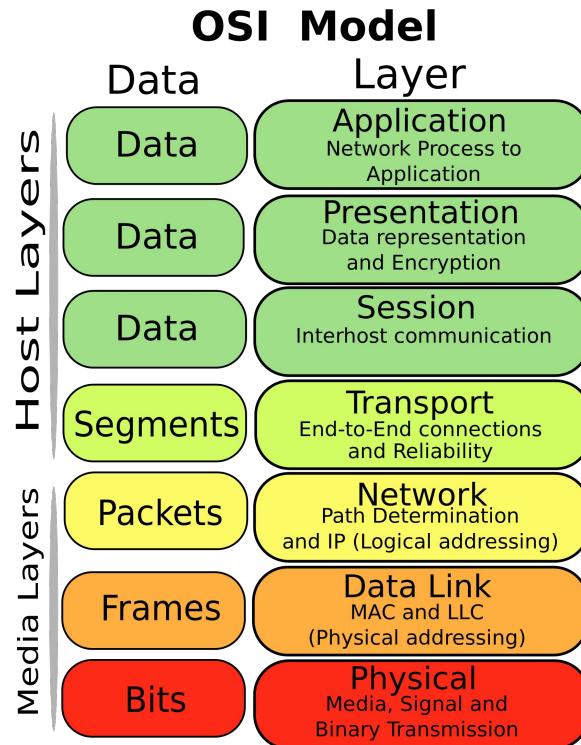
- **Full-duplex**: podem ser usados nos dois sentidos ao mesmo tempo, como uma estrada de mão dupla
- **Half-duplex**: usados em qualquer sentido, mas apenas um deles de cada vez, como uma linha férrea de trilho único
- **Simplex**: permitem o tráfego em apenas uma direção, como uma rua de mão única

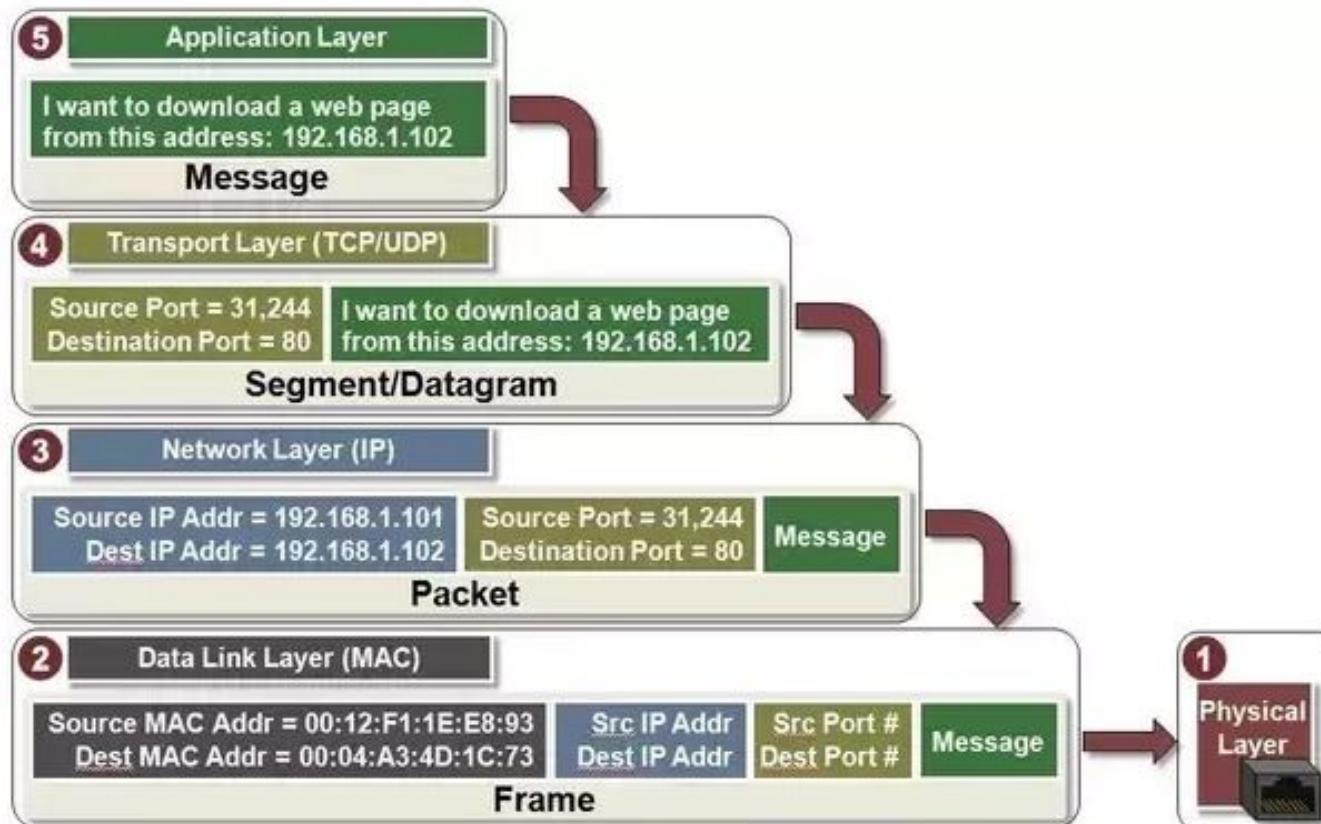
Quadro

- Na camada de enlace, a mensagem é chamada de quadro e encapsula o pacote enviado pela camada de rede









Relação entre as Camadas de Física e de Enlace

- A física fornece um fluxo de bits bruto para a de enlace
- Se o canal tiver ruído, a física pode inserir alguma redundância para reduzir a taxa de erro para um nível tolerável
- A enlace transforma o fluxo de bits bruto em quadros
- A enlace pode detectar e, eventualmente, corrigir erros

Motivação

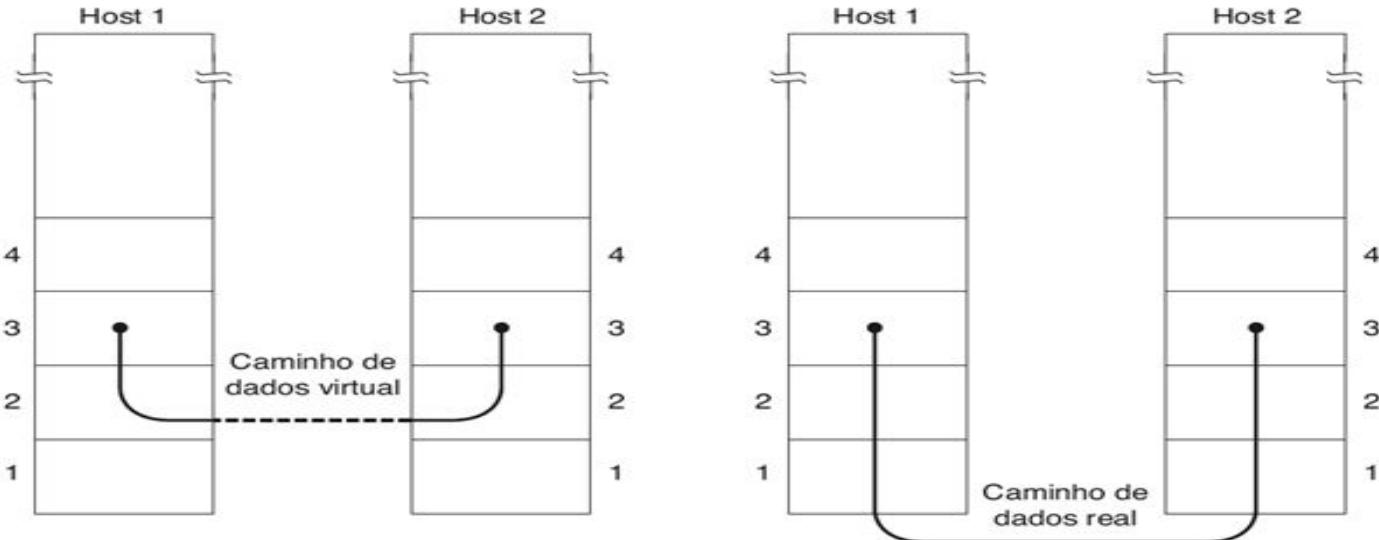
- Dado duas máquinas conectadas diretamente através de um canal de comunicação, podemos ter algumas limitações:
 - Os canais podem produzir erros
 - A taxa de dados é finita
 - O atraso de propagação é diferente de zero

Questões de Projeto da Camada de Enlace

- Fornecer uma interface de serviços bem definida para a camada de rede
- Tarefas da camada de enlace
 - Enquadramento
 - Controle de erros: detecção ou correção
 - Controle de fluxo, permitindo que receptores mais lentos não sejam atropelados por transmissões rápidas

Principal Serviço da Camada de Enlace

- Transferência de dados da camada de rede de uma máquina origem para a mesma camada de uma máquina de destino



(a) Comunicação virtual

(b) Comunicação real

Agenda

- Introdução
- **Orientação à Conexão e Existência de Confirmação**
- Enquadramento
- Controle de Fluxo
- Controle de Erro
- Camada de Enlace da Internet

Serviços Oferecidos à Camada de Rede

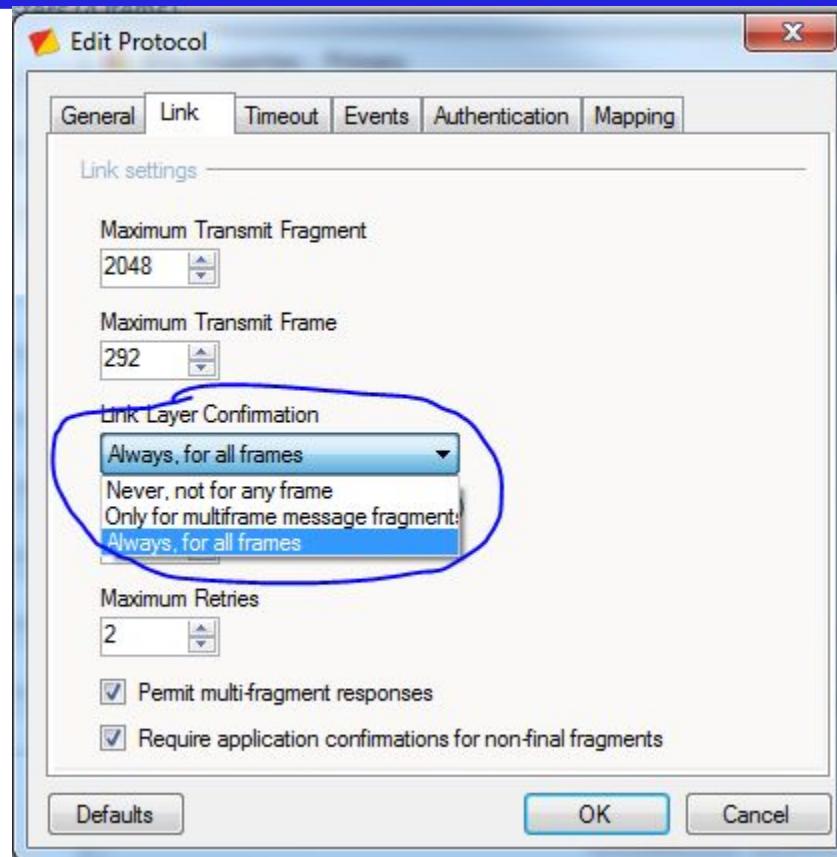
- Classificados quando a:
 - Orientação à conexão
 - Existência de confirmação

Orientação à Conexão

- A origem pode enviar quadros de forma numerada, garantindo a entrega e a ordem de entrega de cada um deles
- Apropriada para canais longos ou não confiáveis (e.g., satélite ou circuitos telefônicos interurbano)
- Três fases:
 - estabelecimento da conexão
 - transmissão de um ou mais quadros
 - término da conexão

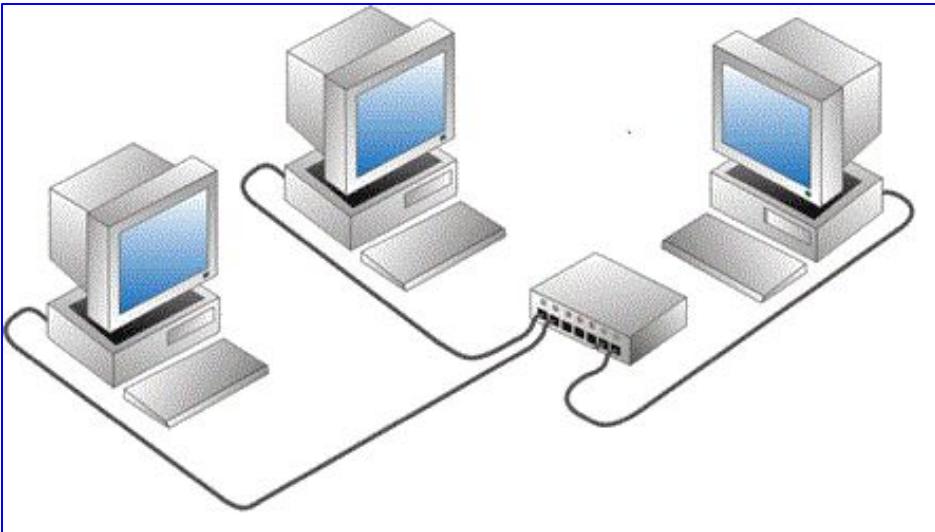
Existência de Confirmação

- Confirmação quadro a quadro



Existência de Confirmação

- É um *overhead* em canais confiáveis (e.g., fibra óptica) e interessante em não confiáveis (e.g., canais sem fio)



Existência de Confirmação

- Relacionada à questão de otimização (nunca uma exigência)
- As camadas de rede ou transporte podem efetuar a confirmação, contudo, um pacote pode ser dividido em vários quadros
- Por exemplo, se um pacote é dividido em 10 quadros e 20% dos quadros são perdidos, o tempo para reenviar o pacote é maior que o de dois quadros

Existência de Confirmação

- Conhecendo o tamanho dos quadros e parâmetros de atraso, a confirmação pode evitar a transmissão de dados já comprometidos



Serviços Oferecidos à Camada de Rede

- Serviço sem conexão nem confirmação
- Serviço sem conexão com confirmação
- Serviço com conexão e confirmação
- ~~Serviço com conexão e sem confirmação (não)~~

Serviço sem Conexão nem Confirmação

- Conexão não é estabelecida à priori
- Origem envia quadros independentes para o destino que não os confirma
- Quadros perdidos são ignorados

Serviço sem Conexão nem Confirmação

- Classe de serviço apropriada quando:
 - taxa de erros é “baixa”
 - alguma camada superior faz o processo de recuperação de erros
 - dados atrasados são piores que falhas (e.g., sistemas de tempo real (voz))
- Serviço normalmente usado em LANs

Serviço sem Conexão com Confirmação

- Conexão não é estabelecida a priori
- Destino confirma os quadros recebidos
- Origem usa mecanismo de temporização para reenviar quadros não confirmados
- Uma confirmação perdida pode acarretar diversas retransmissões de um quadro e, consequentemente, faça com que ele seja recebido várias vezes
- Serviço apropriado para canais não são confiáveis (e.g., comunicação sem fio)

Serviço com Conexão e Confirmação

- Serviço mais sofisticado
- Origem e destino estabelecem uma conexão antes da transmissão de dados
- Quadros recebidos corretamente
- Camada de enlace pode entregar os quadros em ordem para a rede

Agenda

- Introdução
- Orientação à Conexão e Existência de Confirmação
- **Enquadramento**
- Controle de Fluxo
- Controle de Erro
- Camada de Enlace da Internet

Enquadramento

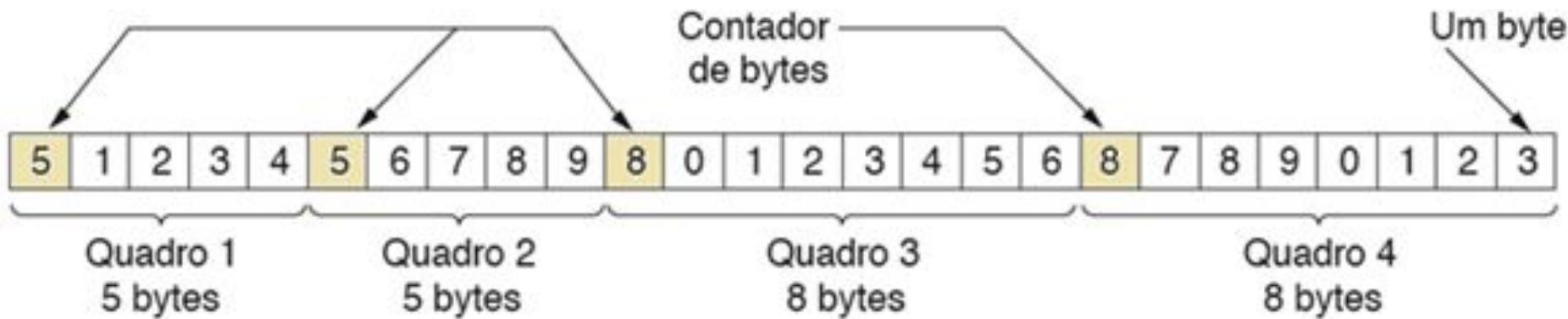
- É a divisão do fluxo de bits em quadros
 - Quando um nó envia um quadro, ele calcula e insere seu *checksum* no quadro
 - Quando um nó recebe um quadro, ele verifica o *checksum* desse quadro
- Permite que o receptor identifique o início de novos quadros consumindo pouco *overhead*

Técnicas para Enquadramento

- Contagem de *bytes*
- *Byte stuffing*
- *Bit stuffing*
- Violação de código da camada física

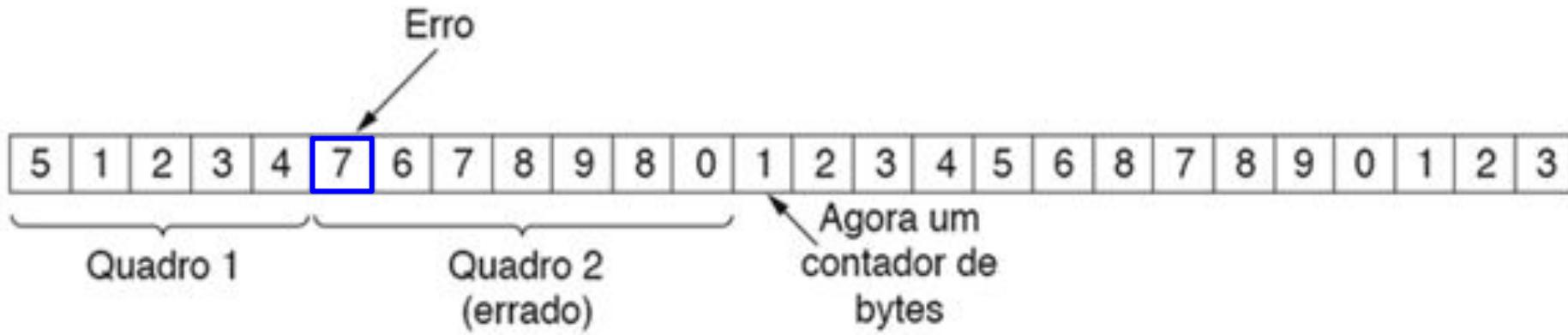
Contagem de Bytes

- Cada quadro terá um campo indicando seu número de bytes



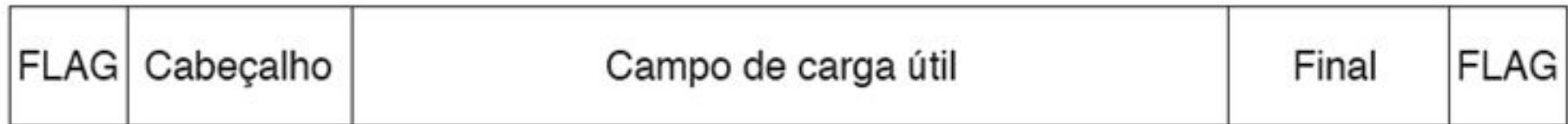
Contagem de Bytes

- Desvantagem: fortemente sensível a erros
 - No exemplo, um erro no contador do segundo quadro (se tornou 7), faz com que o receptor não identifique o início dos demais quadros



Byte Stuffing

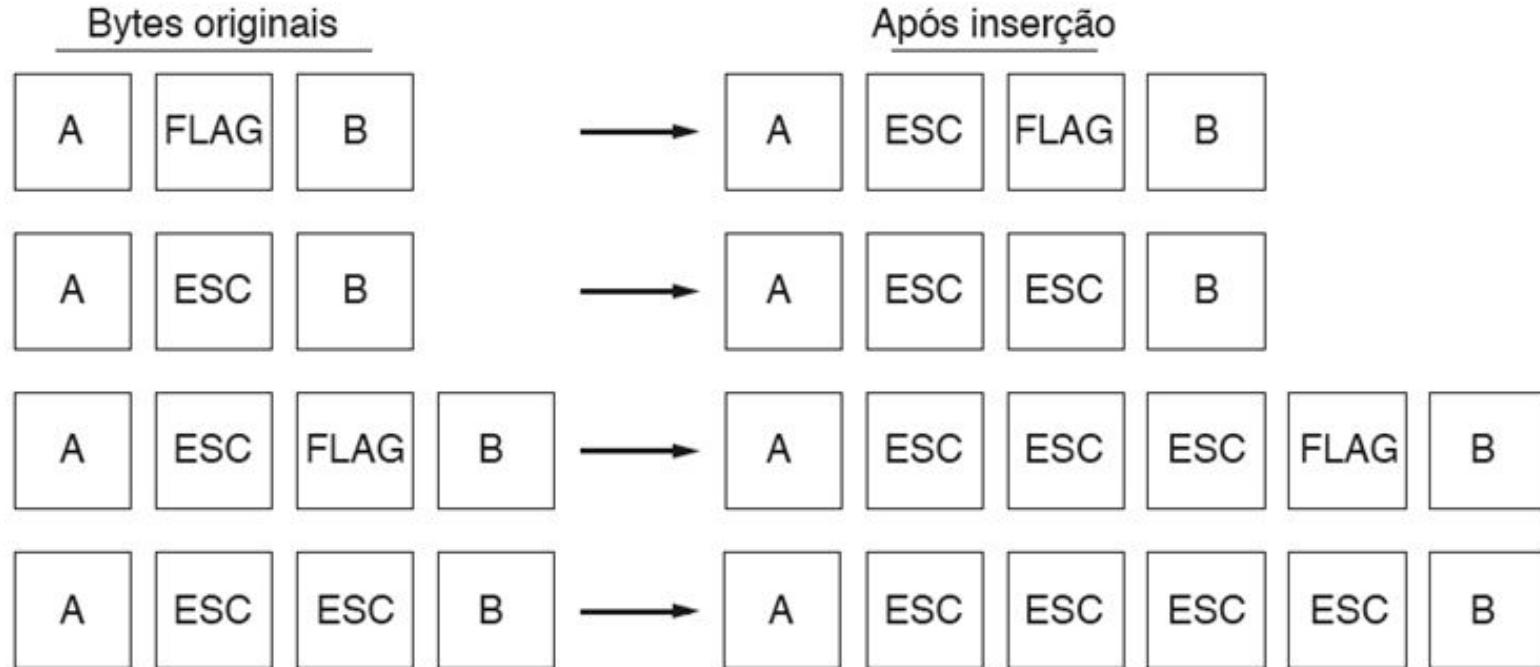
- Contorna o problema de ressincronização dos quadros (no caso de erros), inserindo bytes de flag para delimitar o início e fim dos quadros



Quadro limitado com bytes de flag

Byte Stuffing

- Quatro exemplos de sequências de bytes antes e depois do *byte stuffing*



Byte Stuffing

- Desvantagens:
 - *overhead* com a inserção de bytes que pode ser minimizado inserindo caracteres menos frequentes
 - depende da utilização de caracteres de 8 bits sendo que existem sistemas diferentes (e.g., o UNICODE emprega caracteres de 16 bits)

Exercício (1)

- Sabendo o caractere de flag é o @ e o de escape, #, quais serão as mensagens resultantes da aplicação do *byte stuffing* em:
 - a) ABC
 - b) A@C
 - c) @@A@@
 - d) @##A
 - e) @DC##

Bit Stuffing

- Minimiza o *overhead* do *byte stuffing*, permitindo flags com número arbitrário de bits
- Cada quadro começa e termina com o padrão 0111 1110 (0x7E)
- Quando o emissor identifica cinco bits com 1, ele insere um bit com 0 e o receptor efetua o processo contrário
- O comprimento do quadro depende de sua carga útil

Exemplo da Técnica de *Bit Stuffing*

Dados originais: 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Dados com
bit stuffing **7E** 0 1 1 0 1 1 1 1 **0** 1 1 1 1 **0** 1 1 1 1 **0** 1 0 0 1 0 **7E**

↑ ↑
Bits inseridos

Dados
armazenados
pelo receptor

0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Violação de Código da Camada Física

- Uma das técnicas da camada física é a inserção de redundância, fazendo com que alguns sinais não ocorram em dados regulares
- Esses sinais podem ser explorados para início e fim de quadro pela camada de enlace
- Usado no padrão IEEE 802.11

Observações sobre as Técnicas de Enquadramento

- Protocolos de enlace, por segurança, podem usar uma ou mais técnicas
- O IEEE 802.11 e o Ethernet fazem com que cada quadro tenha um preâmbulo e seja seguido por um campo de comprimento

Agenda

- Introdução
- Orientação à Conexão e Existência de Confirmação
- Enquadramento
- **Controle de Fluxo**
- Controle de Erro
- Camada de Enlace da Internet

Controle de Fluxo

- O que fazer quando um transmissor é mais rápido que o receptor?
- Protocolos de enlace normalmente consideram técnicas baseadas em:
 - *Feedback*: o receptor envia *feedbacks* sobre sua capacidade de processamento de quadros
 - Velocidade: o protocolo tem um mecanismo interno que limita a velocidade de transmissão sem usar *feedback*

Agenda

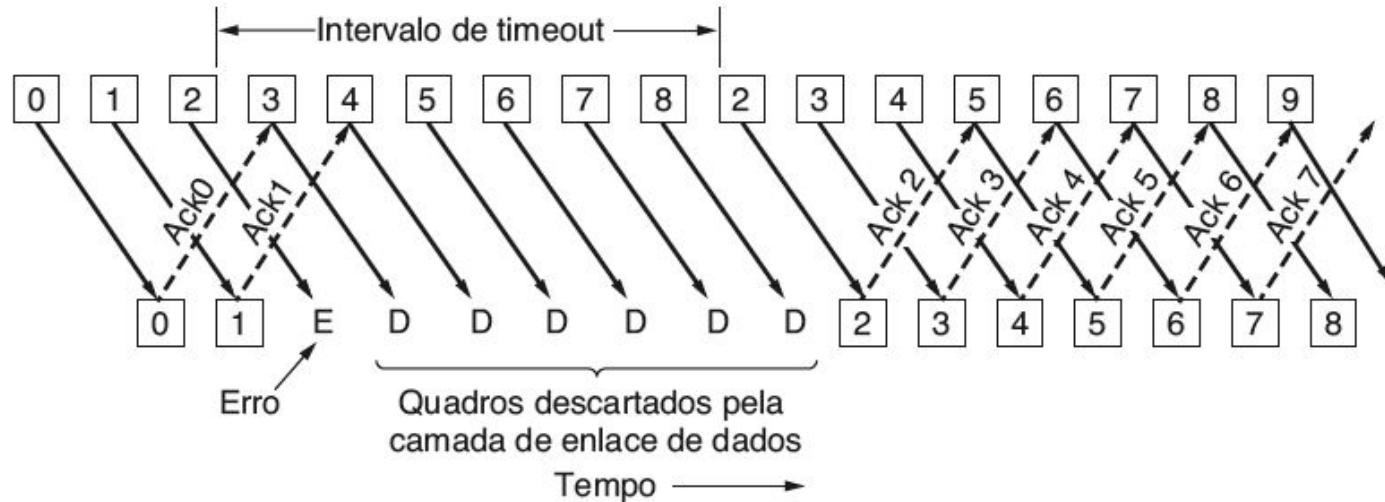
- Introdução
- Orientação à Conexão e Existência de Confirmação
- Enquadramento
- Controle de Fluxo
- **Controle de Erro**
- Camada de Enlace da Internet

Controle de Erros

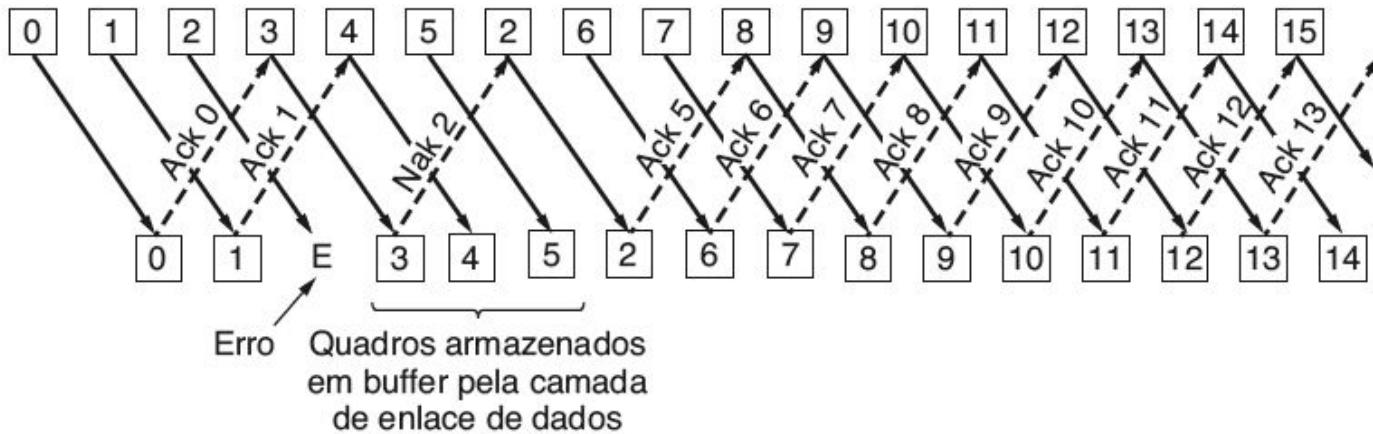
- Como garantir que os quadros serão entregues na camada de rede do destino e na ordem/forma correta?
 - Uma solução é não garantir
 - Outra é dar um *feedback* ao emissor

- Enviado pelo receptor, pode ser uma confirmação positiva ou negativa
 - Positivo: quando o receptor recebe um quadro, ele envia um ACK. Se o emissor não receber o ACK após um tempo, ele retransmite o quadro
 - Negativo: quando um nó recebe o quadro n sendo que ele não recebeu o $(n-1)$, o receptor envia um NACK (n)

Recuperação de Erros com ACK



Recuperação de Erros com NACK



Algumas Considerações

- Não existe mundo perfeito
- Os erros normalmente acontecem em rajadas o que minimiza a quantidade de blocos com erro, contudo, dificulta a detecção ou a correção dos erros
- A correção de erros é chamada de Correção Adiantada de Erros ou *Forward Error Correction* (FEC)

Inserção de Redundância nos Quadros

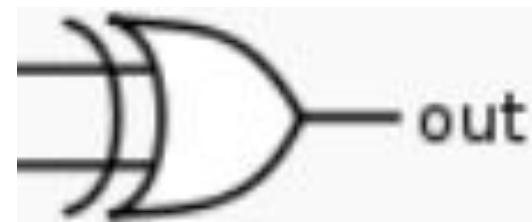
- Permite que o receptor seja capaz de detectar ou corrigir erros
- A correção normalmente demanda mais redundância que a de detecção
- Cada quadro é composto por $n = m + r$ bits, onde temos m bits de dados e r bits de redundância sendo r calculado a partir de m
 - Taxa de código: fração da palavra que representa os dados não redundantes

Estratégias para Inserção de Redundância

- Estratégia sistemática: os próprios m bits de dados são enviados
- Estratégia linear: os r bits de redundância são calculados como uma função (popularmente, a operação XOR) dos m de dados

Operação XOR

p	q	$p \oplus q$
F	F	F
F	V	V
V	F	V
V	V	F



Dependência do Meio

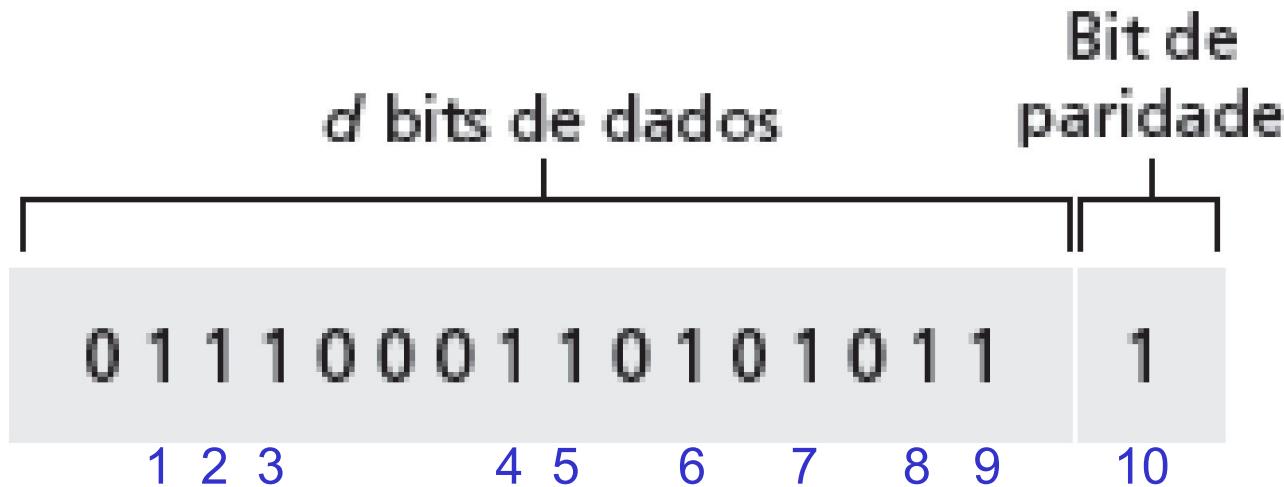
- Códigos de detecção de erros:
 - Usados em canais altamente confiáveis, como as fibras
 - Bloco defeituoso é retransmitido
- Códigos de correção de erros:
 - Usados em canais como enlaces sem fio que geram muitos erros

Algumas Técnicas para Detecção de Erros

- Verificação de paridade
- Checksum
- Verificação de redundância cíclica (CRC, *Cyclic Redundancy Check*)

Verificação de Paridade

- Insere um bit de paridade no quadro para garantir que o número total 1s seja par. No exemplo, o valor desse bit é 1, pois os dados têm um número ímpar de 1s



Esquemas de Paridade

- **Esquema de paridade par:** quando o número total 1s é par
- **Esquema de paridade ímpar:** quando o número total 1s é ímpar

Verificação Bidimensional de Paridade

- Enxerga o fluxo de bits como uma matriz e verifica a paridade de cada linha / coluna, aumentando o *overhead* e qualidade da verificação, e permitindo a correção de 1 bit

Nenhum erro	Erro de bit único corrigível
1 0 1 0 1 1	1 0 1 0 1 1
1 1 1 1 0 0	1 0 1 1 0 0
0 1 1 1 0 1	0 1 1 1 0 1
----- -----	----- -----
0 0 1 0 1 0	0 0 1 0 1 0

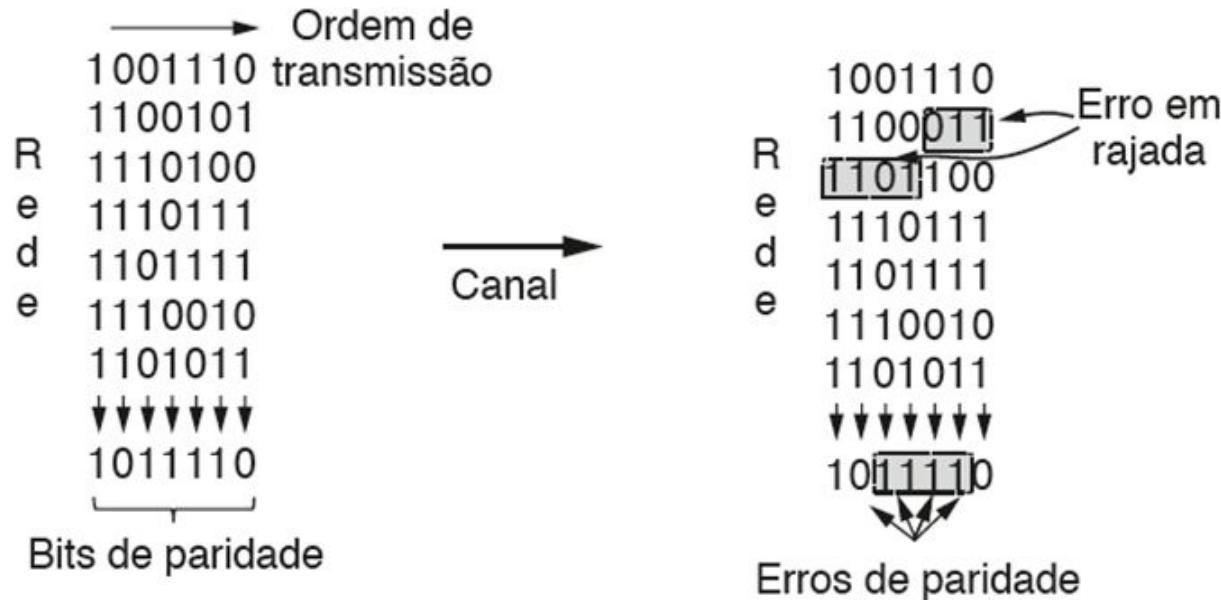
Diagrama ilustrando a verificação bidimensional de paridade:

- Nenhum erro:** A matriz de bits é:

1	0	1	0	1	1
1	1	1	1	0	0
0	1	1	1	0	1
0	0	1	0	1	0
- Erro de bit único corrigível:** Um erro ocorre na 4ª coluna da 1ª linha.
 - O resultado esperado é 1 (paridade ímpar).
 - O resultado obtido é 0 (paridade par).
 - Um erro de paridade é detectado na 4ª coluna.
 - Um erro de paridade é detectado na 1ª linha.

Verificação em Colunas de Paridade

- Solução intermediária entre as duas anteriores e que é robusta para identificar rajadas de erros (situação comum na transmissão de bits)



Checksum

- Termo normalmente usado para indicar um grupo de bits de verificação associados a uma mensagem, independente de como são calculados
- Na literatura, observa-se diversas variações dessa técnica
- Utilizado no protocolo IP (camada de rede)

Cyclic Redundancy Check (CRC)

- Tipo mais forte de detecção de erros
- Tem uso generalizado na camada de enlace
- Efetua a divisão de polinômios e faz com que o resto da divisão seja usado na detecção de erros

Representação usando Polinômio

- Considera que os m bits de dados são os coeficientes de um polinômio com m termos, variando desde x^{m-1} até x^0 (grau $m-1$)
- Exemplo: **110001** representa o polinômio $x^5 + x^4 + x^0$
5 4 3 2 1 0

Polinômio Gerador - G(x)

- Definido antecipadamente por emissor e receptor
- Seus bits de maior e menor ordem sempre serão um (por definição)

Polinômios Geradores Comuns

CRC	$G(x)$
CRC-8	$x^8 + x^2 + x + 1$
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x + 1$
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + 1$
CRC-16	$x^{16} + x^{15} + x^2 + 1$
CRC-CCITT	$x^{16} + x^{12} + x^5 + 1$
CRC-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Fonte: PETERSON; DAVIE, 2004, p.70

Polinômios Geradores Comuns

- Redes Ethernet utilizam CRC-32
- Redes *Asynchronous Transfer Mode* (ATM) utilizam CRC-8, CRC-10 e CRC-32

Exercício (2)

• Mostre a sequência de bits dos polinômios geradores abaixo:

a) CRC-8: $x^8 + x^2 + x + 1$

b) CRC-10: $x^{10} + x^9 + x^5 + x^4 + x + 1$

Ideia Básica do CRC

- O emissor adiciona um conjunto de bits de controle no final do quadro de forma que o quadro (agora, dados + bits de controle) é divisível pelo polinômio gerador $G(x)$
- O receptor efetua a divisão do polinômio representado pelos bits do quadro pelo polinômio gerador $G(x)$ e se o resto dessa divisão for zero, temos sucesso, ou seja, não detecção de erros

Polinômio Dividendo - D(x)

$$\begin{array}{r} \text{dividendo} \quad \longleftarrow \quad \begin{array}{c} 6 \\ | \\ 3 \end{array} \quad \longrightarrow \quad \text{divisor} \\ \text{resto} \quad \longleftarrow \quad \begin{array}{c} 0 \\ | \\ 2 \end{array} \quad \longrightarrow \quad \text{quociente} \end{array}$$

Polinômio Dividendo - D(x)

- Produto da multiplicação do polinômio de dados da mensagem $M(x)$ por x^R onde R representa o maior grau do polinômio gerador (seu número de bits menos um)
- Por exemplo, se $M(x) = 10011010 = x^7 + x^4 + x^3 + x$ e $G(x) = 1101 = x^3 + x^2 + 1$, e $R = 3$ e o polinômio dividendo $D(x) = (x^7 + x^4 + x^3 + x) * (x^3) = (x^{10} + x^7 + x^6 + x^4) = 10011010\textcolor{blue}{000}$
- Ou seja, o polinômio dividendo $D(x) = M(x)$ mais R zeros inseridos à direita

Aritmética Polinomial

- É feita em módulo 2 segundo as regras da teoria algébrica, logo, não há transportes para adição nem empréstimos para subtração
- Nesse caso, tanto a adição como a subtração são como o XOR

$$\begin{array}{r} 10011011 \\ + 11001010 \\ \hline 01010001 \end{array} \quad \begin{array}{r} 00110011 \\ + 11001101 \\ \hline 11111110 \end{array} \quad \begin{array}{r} 11110000 \\ - 10100110 \\ \hline 01010110 \end{array} \quad \begin{array}{r} 01010101 \\ - 10101111 \\ \hline 11111010 \end{array}$$

- A divisão será realizada através de várias subtrações

Polinômio a ser Transmitido $T(x)$

- $T(x) = D(x)$ **or** resto da divisão de $D(x)$ por $G(x)$

Exemplo

- Seja $M(x) = 10011010$ e $G(x) = 1101$, calcule $T(x)$
- 1º passo: calcular o polinômio dividendo $D(x)$
- 2º passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$
- 3º passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

Exemplo

- Seja $M(x) = 10011010$ e $G(x) = 1101$, calcule $T(x)$

- **1º passo: calcular o polinômio dividendo $D(x)$**

$$D(x) = 10011010\textcolor{blue}{000}$$

- 2º passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$
- 3º passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

Exemplo

- Seja $M(x) = 10011010$ e $G(x) = 1101$, calcule $T(x)$

- 1º passo: calcular o polinômio dividendo $D(x)$

$$D(x) = 10011010000$$

- 2º passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$

- 3º passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

Exemplo: Divisão de D(x) por G(x)

10011010000 1101

Exemplo: Divisão de D(x) por G(x)

$$\begin{array}{r} 10011010000 \\ \underline{\text{xor } 1101} \\ 100 \end{array}$$

Exemplo: Divisão de D(x) por G(x)

$$\begin{array}{r} 1001\textcolor{blue}{1}010000 \\ \underline{\text{xor } 1101} \\ 1001 \end{array} \quad \begin{array}{r} 1101 \\ \hline 1 \end{array}$$

Exemplo: Divisão de D(x) por G(x)

$$\begin{array}{r} 1001\textcolor{blue}{1}010000 \\ \underline{\text{xor } 1101} \qquad\qquad\qquad 11 \\ \qquad\qquad\qquad 1001 \\ \qquad\qquad\qquad \underline{\text{xor } 1101} \\ \qquad\qquad\qquad 100 \end{array}$$

Exemplo: Divisão de D(x) por G(x)

$$\begin{array}{r} 10011\textcolor{blue}{0}10000 \\ \underline{\text{xor } 1101} & \quad | \quad 1101 \\ 1001 \\ \underline{\text{xor } 1101} \\ 1000 \end{array}$$

Exemplo: Divisão de D(x) por G(x)

10011 <u>0</u> 10000	<u>1101</u>
<u>xor 1101</u>	111
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
101	

Exemplo: Divisão de D(x) por G(x)

$$\begin{array}{r} 100110\textcolor{blue}{1}0000 \\ \underline{\text{xor } 1101} & \quad 1101 \\ 1001 \\ \underline{\text{xor } 1101} & \quad 111 \\ 1000 \\ \underline{\text{xor } 1101} \\ 101\textcolor{blue}{1} \end{array}$$

Exemplo: Divisão de D(x) por G(x)

$$\begin{array}{r} 100110\textcolor{blue}{1}0000 \\ \underline{\text{xor } 1101} & \quad 1101 \\ 1001 \\ \underline{\text{xor } 1101} & \quad 1111 \\ 1000 \\ \underline{\text{xor } 1101} & \\ 1011 \\ \underline{\text{xor } 1101} & \\ 110 \end{array}$$

Exemplo: Divisão de D(x) por G(x)

1001101 <u>0</u> 000	<u>1101</u>
<u>xor 1101</u>	1111
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
1011	
<u>xor 1101</u>	
1100	

Exemplo: Divisão de D(x) por G(x)

1001101 <u>0</u> 000	1101
<u>xor 1101</u>	11111
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
1011	
<u>xor 1101</u>	
1100	
<u>xor 1101</u>	
001	

Exemplo: Divisão de D(x) por G(x)

10011010 <u>000</u>	1101
<u>xor 1101</u>	111110
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
1011	
<u>xor 1101</u>	
1100	
<u>xor 1101</u>	
001 <u>0</u>	

Exemplo: Divisão de D(x) por G(x)

10011010000	1101
<u>xor 1101</u>	1111100
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
1011	
<u>xor 1101</u>	
1100	
<u>xor 1101</u>	
00100	

Exemplo: Divisão de D(x) por G(x)

10011010000	1101
<u>xor 1101</u>	11111000
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
1011	
<u>xor 1101</u>	
1100	
<u>xor 1101</u>	
001000	

Exemplo: Divisão de D(x) por G(x)

10011010000	1101
<u>xor 1101</u>	111110001
1001	
<u>xor 1101</u>	
1000	
<u>xor 1101</u>	
1011	
<u>xor 1101</u>	
1100	
<u>xor 1101</u>	
001000	
<u>xor 1101</u>	
101	

Exemplo: Divisão de D(x) por G(x)

10011010000 1101
xor 1101 111110001
 1001
xor 1101
 1000
xor 1101
 1011
xor 1101
 1100
xor 1101
 001000
xor 1101
 101 ← resto

Exemplo

- Seja $M(x) = 10011010$ e $G(x) = 1101$, calcule $T(x)$

- 1º passo: calcular o polinômio dividendo $D(x)$

$$D(x) = 10011010000$$

- 2º passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$

resto = 101

- 3º passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

Exemplo

- Seja $M(x) = 10011010$ e $G(x) = 1101$, calcule $T(x)$

- 1º passo: calcular o polinômio dividendo $D(x)$

$$D(x) = 10011010000$$

- 2º passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$

$$\text{resto} = 101$$

- 3º passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

$$T(x) = 10011010101$$

Ideia Básica do CRC

- O emissor adiciona um conjunto de bits de controle no final do quadro de forma que o quadro (agora, dados + bits de controle) é divisível pelo polinômio gerador $G(x)$
- O receptor efetua a divisão do polinômio representado pelos bits do quadro pelo polinômio gerador $G(x)$ e se o resto dessa divisão for zero, temos sucesso, ou seja, não detecção de erros

Exemplo na Recepção

- Como $T(x) = 10011010101$ e $G(x) = 1101$, temos:

Exemplo na Recepção

10011010101 1101
xor 1101 xxxxxxxx
1001
xor 1101
1000
xor 1101
1011
xor 1101
1100
xor 1101
001101
xor 1101
000 ← resto

Exercício (3)

- Seja $M(x) = 111100101$ e $G(x) = 101101$, calcule $T(x)$
- 1º passo: calcular o polinômio dividendo $D(x)$
- 2º passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$
- 3º passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

Exercício (4)

- Seja $R(x) = 11110010101010$ um quadro recebido e o polinômio gerador $G(x) = 101101$, informe se conseguimos identificar algum erro usando CRC

Exercício (5)

- Seja $M(x) = 1101011011$ e $G(x) = 10011$, calcule $T(x)$
- 1o passo: calcular o polinômio dividendo $D(x)$
- 2o passo: encontrar o resto da divisão de $D(x)$ pelo polinômio gerador $G(x)$
- 3o passo: $D(x)$ or com o resto da divisão de $D(x)$ por $G(x)$

Exercício (6)

- Qual é o resto obtido pela divisão módulo 2 de x^7+x^5+1 pelo polinômio gerador x^3+1 ?

Exercício (7)

- Um fluxo de bits 10011101 é transmitido com a utilização do método de CRC padrão descrito no texto. O polinômio gerador é x^3+1 . Mostre o string de bit real transmitido. Suponha que o terceiro bit a partir da esquerda seja invertido durante a transmissão. Mostre que esse erro é detectado na extremidade receptora.

Algumas Técnicas para Correção de Erros

- Código de Hamming
- Código Convolucional Binário
- Outros

Código de Hamming

(1) Recodificamos a mensagem de tal forma que os bits potência de dois (1, 2, 4, 8, 16, ...) serão bits de verificação

Exemplo: mensagem = 10101

b1	b2	b3	b4	b5	b6	b7	b8	b9
—	—	1	—	0	1	0	—	1

Nesse caso, observamos que os bits de verificação são: b1, b2, b4 e b8

Código de Hamming

(2) Na nova mensagem (ainda incompleta), selecionamos os bits com 1 e efetuamos um XOR entre os valores de suas respectivas posições

b1	b2	b3	b4	b5	b6	b7	b8	b9
—	—	1	—	0	1	0	—	1

Como os bits com valor um são b3, b6 e b9:

Pos.	Binário
3	0 0 1 1
6	0 1 1 0
9	1 0 0 1
<hr/>	
XOR	1 1 0 0

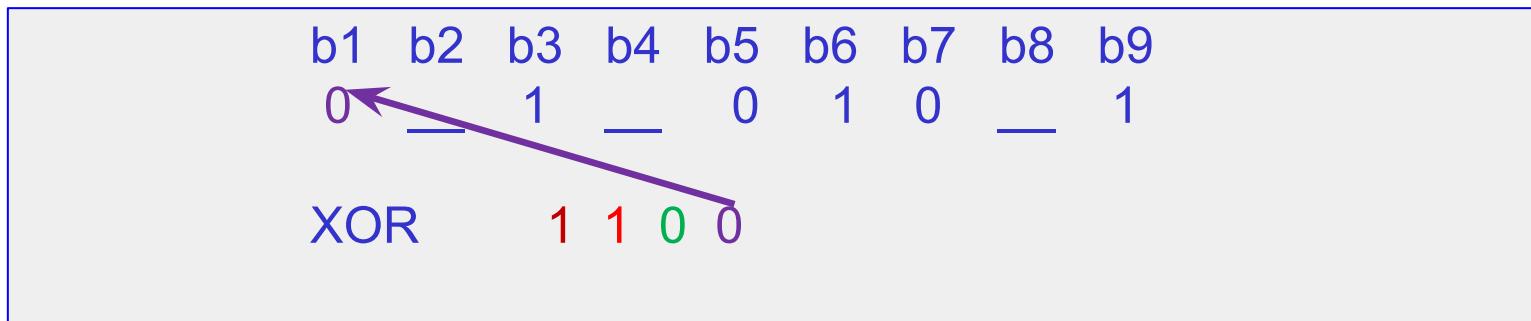
Código de Hamming

(3) Completamos a mensagem a ser enviada com os valores do XOR na ordem inversa

b1	b2	b3	b4	b5	b6	b7	b8	b9
—	—	1	—	0	1	0	—	1
XOR		1	1	0	0			

Código de Hamming

(3) Completamos a mensagem a ser enviada com os valores do XOR na ordem inversa



Código de Hamming

(3) Completamos a mensagem a ser enviada com os valores do XOR na ordem inversa

b1	b2	b3	b4	b5	b6	b7	b8	b9
0	0	1	—	0	1	0	—	1

XOR 1 1 0 0

Código de Hamming

(3) Completamos a mensagem a ser enviada com os valores do XOR na ordem inversa

b1	b2	b3	b4	b5	b6	b7	b8	b9
0	0	1	1	0	1	0		1
XOR			1	1	0	0		

Código de Hamming

(3) Completamos a mensagem a ser enviada com os valores do XOR na ordem inversa

b1	b2	b3	b4	b5	b6	b7	b8	b9
0	0	1	1	0	1	0	1	1

XOR

1 1 0 0

Código de Hamming

(3) Completamos a mensagem a ser enviada com os valores do XOR na ordem inversa

Mensagem a ser enviada:

0 0 1 1 0 1 0 1 1

Código de Hamming

(4) No recebimento da mensagem, efetuamos um XOR com as posições cujo valor seja igual a 1

Mensagem recebida:

0	0	1	1	0	1	0	1	1
b1	b2	b3	b4	b5	b6	b7	b8	b9

Pos.	Binário
3	0 0 1 1
4	0 1 0 0
6	0 1 1 0
8	1 0 0 0
9	1 0 0 1
<hr/>	
XOR	0 0 0 0

Código de Hamming

(5) Se a resposta do XOR for zero, o código de Hamming não detectou qualquer erro

Mensagem recebida:

XOR 0 0 0 0

Código de Hamming

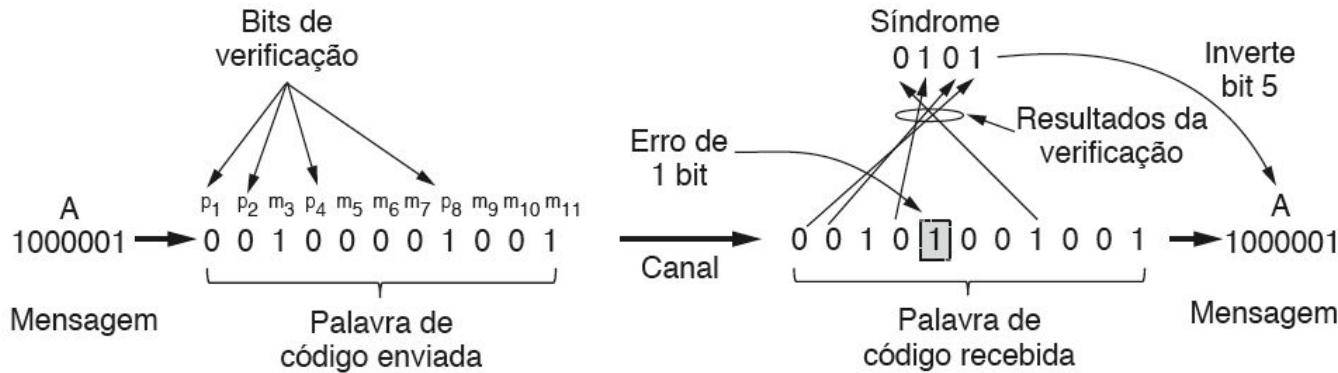
(6) Se a resposta do XOR for diferente de zero, o código de Hamming detectou um erro no bit indicado pelo XOR

Mensagem recebida com erro na posição:

1	0	1	1	0	1	0	1	1
b1	b2	b3	b4	b5	b6	b7	b8	b9
Pos.								Binário
1								0 0 0 1
3								0 0 1 1
4								0 1 0 0
6								0 1 1 0
8								1 0 0 0
9								1 0 0 1
<hr/>								
XOR		0 0 0 1						

Exercício (8)

- Mostre que a figura abaixo está correta



Exercício (9)

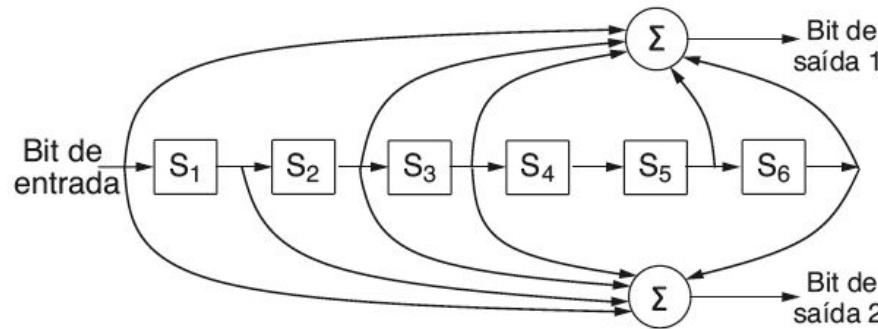
- Um usuário deseja enviar uma mensagem contendo a letra 'G', como ficarão os bits dessa mensagem aplicando o Código de Hamming

Código Convolucional Binário

- Utilizado pela NASA, ele converte cada bit de entrada em dois de saída, conforme a figura abaixo
- Para cada bit de entrada, suas saídas dependem dos últimos seis bits
- Para decodificação, utilizamos algoritmos probabilísticos que encontram a sequência de bits que tem a maior probabilidade de ser a original

Código Convolucional Binário

- Para os primeiros bits, considera-se que os anteriores eram 000000, assim, por exemplo, se a entrada for 111, a saída será 111001



$$\text{Saída 1: } b_1 \oplus b_3 \oplus b_4 \oplus b_6 \oplus b_7$$

$$\text{Saída 2: } b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_7$$

Exercício (10)

- Quais são as funções da camada de enlace. Explique cada uma delas.

Agenda

- Introdução
- Orientação à Conexão e Existência de Confirmação
- Enquadramento
- Controle de Fluxo
- Controle de Erro
- **Camada de Enlace da Internet**

Camada de Enlace da Internet

- A Internet consiste em *hosts* e roteadores conectados através de uma infraestrutura de comunicação
- Boa parte dessa infraestrutura são linhas dedicadas **ponto a ponto**



Point-to-Point Protocol (PPP)

- Protocolo de enlace usado nas comunicações ponto-a-ponto da Internet
- Definido na RFC 1661 e atualizado nas RFCs 1662 e 1663
- Detecta erros
- Aceita vários protocolos
- Permite que endereços IP sejam negociados em tempo de conexão
- Permite a autenticação

Recursos do PPP

- Método de enquadramento não ambíguo
- Protocolo de Controle de Enlace (LCP, *Link Control Protocol*) para ativar linhas, testá-las, negociar opções e desativá-las
- Protocolo de Controle de Rede (NCP, *Network Control Protocol*) para negociar as opções da camada de rede independente do protocolo de rede usado

Exemplo de uma conexão PPP

- Computador A chama o roteador de um provedor através de um modem
- Conexão física é estabelecida
- Quadros LCP são trocados e os parâmetros PPP são selecionados
- Quadros NCP são trocados e os parâmetros de rede são selecionados (e.g., número IP é assinalado a A)
- Conexão definida e A é visto como um computador estático da rede
- Finalização: NCP termina conexão de rede, liberando o número IP
- LCP termina conexão de enlace
- Conexão física é terminada

Exercício (11)

- Explique o funcionamento das técnicas de enquadramento Contagem de bytes, *byte stuffing* e *bit stuffing*.

Exercício (12)

- Explique o funcionamento da técnica de correção de erro denominada matriz de paridade

Exercício (13)

- Explique a recuperação de erros com ACK e NACK

Unidade IV:

Subcamada de Controle e de Acesso ao Meio

Prof. Max do Val Machado

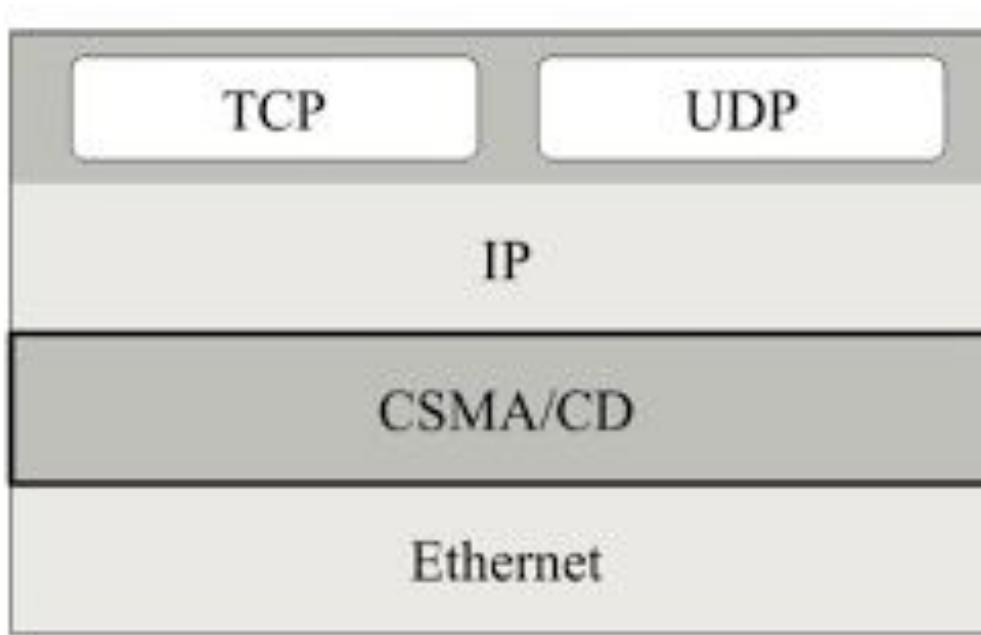


Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Disciplina Redes de Computadores I

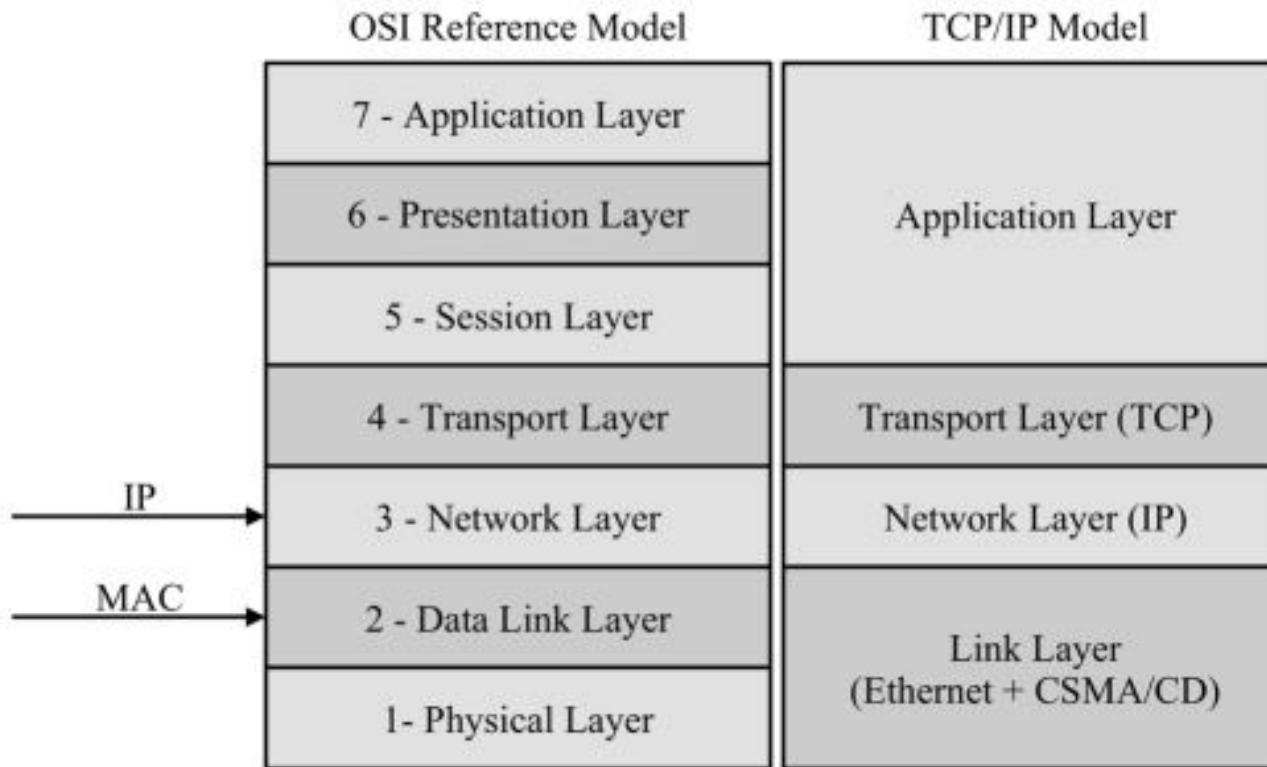
Introdução

- A camada de enlace é dividida em duas subcamadas para redes *broadcast* e uma delas é a MAC
- A MAC fica no nível mais baixo da camada de enlace
- Função da MAC: alocar canais de comunicação no meio físico

Exemplos de Protocolos na Arquitetura TCP/IP



Exemplos de Protocolos na Arquitetura TCP/IP



Introdução

- A camada de enlace é dividida em duas subcamadas para redes broadcast e uma delas é a MAC
- A MAC fica no nível mais baixo da camada de enlace
- Função da MAC: alocar canais de comunicação no meio físico

Conceitos Básicos

- Estações
- Canal único de comunicação
- Tipos de enlaces
- Colisões
- Detecção de colisão
- Políticas de envio de quadros ao longo do tempo
- Detecção de portadora (*carrier sense*)

Estações

- São os pontos de comunicação que transmitem quadros de dados



Estações

- São os pontos de comunicação que transmitem quadros de dados



Estações

- Existem n estações independentes que geram quadros a serem transmitidos
- A estação fica bloqueada até que o quadro seja totalmente transmitido

Canal Único de Comunicação

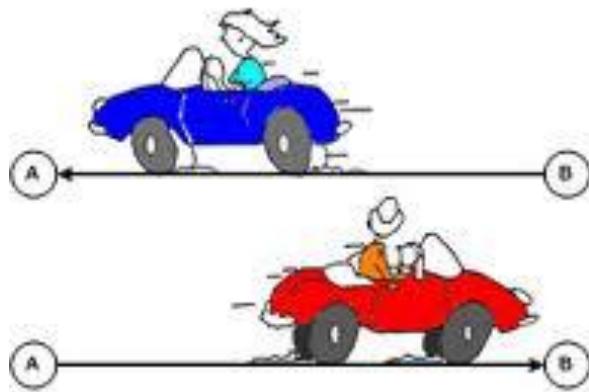


Canal Único de Comunicação

- Todas estações compartilham um único canal de comunicação para transmissão e recepção
- Do ponto de vista de hardware, as estações são equivalentes
- Do ponto de vista de software, as estações podem ter prioridades

Tipos de Enlaces

Full-Duplex



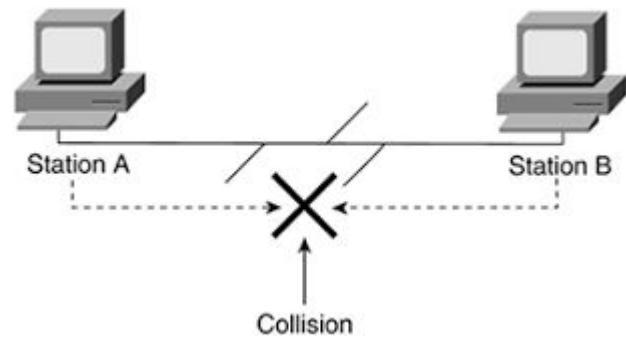
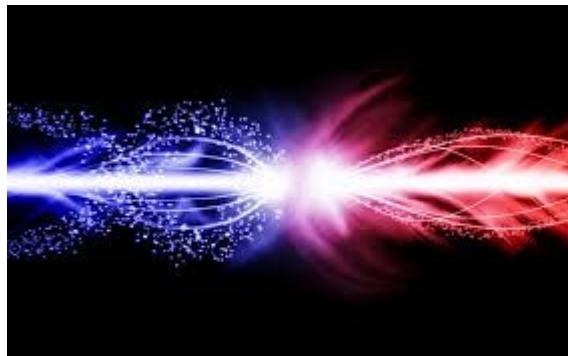
Half-Duplex



Simplex



Colisões



Colisões

- Podem acontecer quando duas ou mais estações transmitem “simultaneamente” quadros
- Afetam o desempenho do sistema
- Na verdade, acontecem na(s) estação(ões) receptora(s) dos quadros
- Quadros envolvidos em colisões são perdidos e devem ser transmitidos posteriormente

Detecção de Colisão

- Estações podem ser capazes de detectar colisões

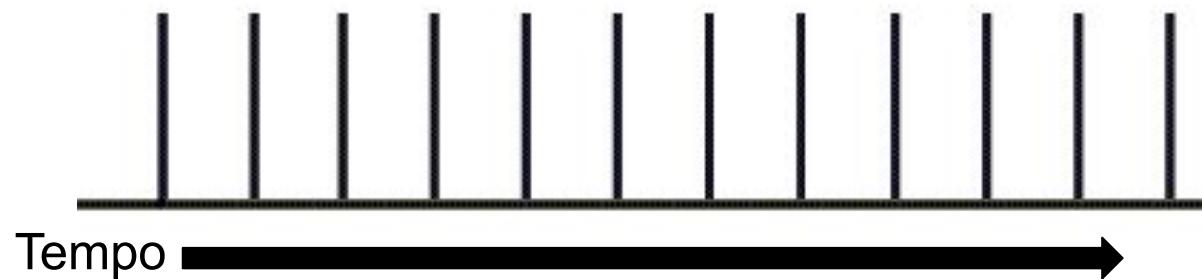


Políticas de Envio de Quadros ao Longo do Tempo

- Qualquer instante (*continuous time*)



- Instantes pré-determinados ou quantizados, segmentados (*slotted time*)



Detecção de Portadora (*Carrier Sense*)

- Antes de uma transmissão, as estações conseguem detectar se o canal está ocupado. Nesse caso, a estação espera a liberação do canal



Não Detecção de Portadora

- Oposto a situação anterior, as estações realizam a transmissão e, depois, verificam o sucesso da operação



Formas de Alocação do Canal

- Alocação Estática
- Alocação Dinâmica

Alocação Estática

- O meio físico é dividido em canais e essa divisão é feita por frequência ou tempo
- Indicada quando existe um número pequeno e fixo de usuários ou cada um possui um tráfego pesado
- Exemplo: sistema telefônico convencional
- Problema (1): os canais são pré-alocados e ficam ociosos quando a estação “dona” do canal não tem o que transmitir
- Problema (2): Em sistemas de computação, o tráfego é tipicamente em rajadas

Alocação Dinâmica

- O controle de acesso ao meio considera a demanda

Protocolos de Acesso ao Meio

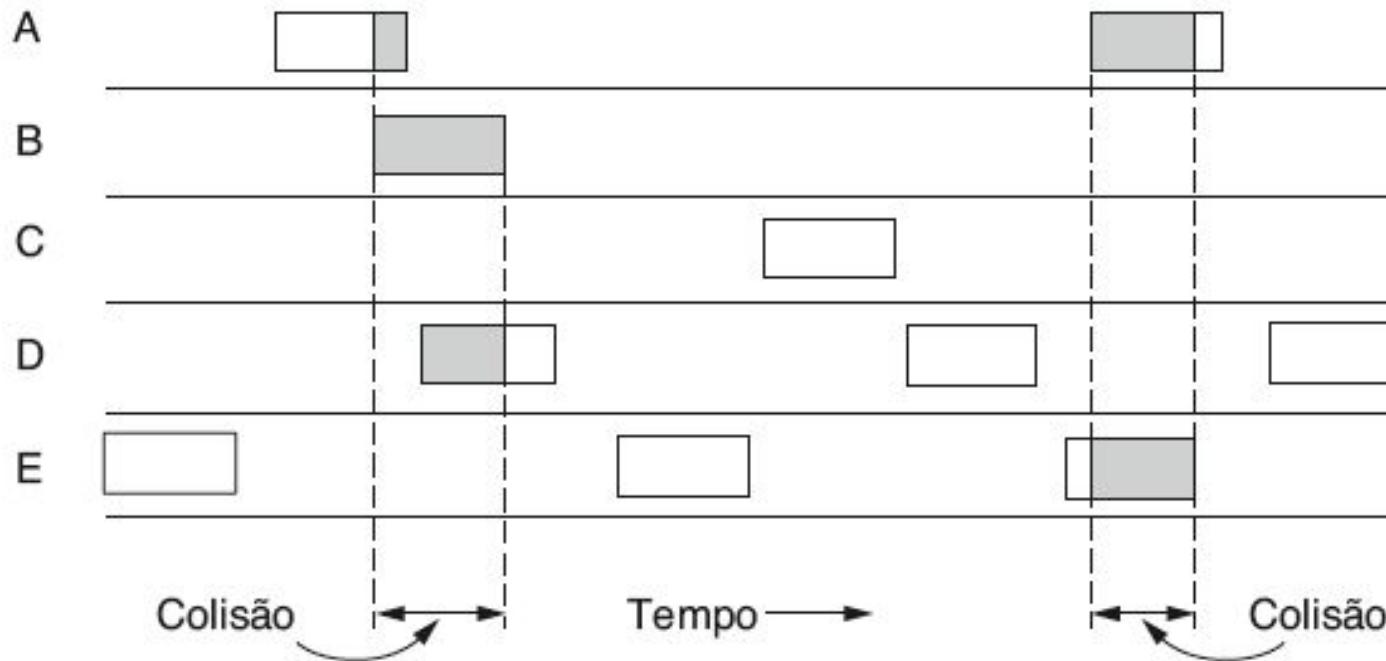
- ALOHA
 - ALOHA Puro
 - Slotted ALOHA
- *Carrier Sense Multiple Access (CSMA)*
 - CSMA 1-Persistente
 - CSMA p-Persistente
 - CSMA Não Persistente
 - CSMA com Detecção de Colisões
- Vários outros

ALOHA Puro: Primeiro Protocolo MAC

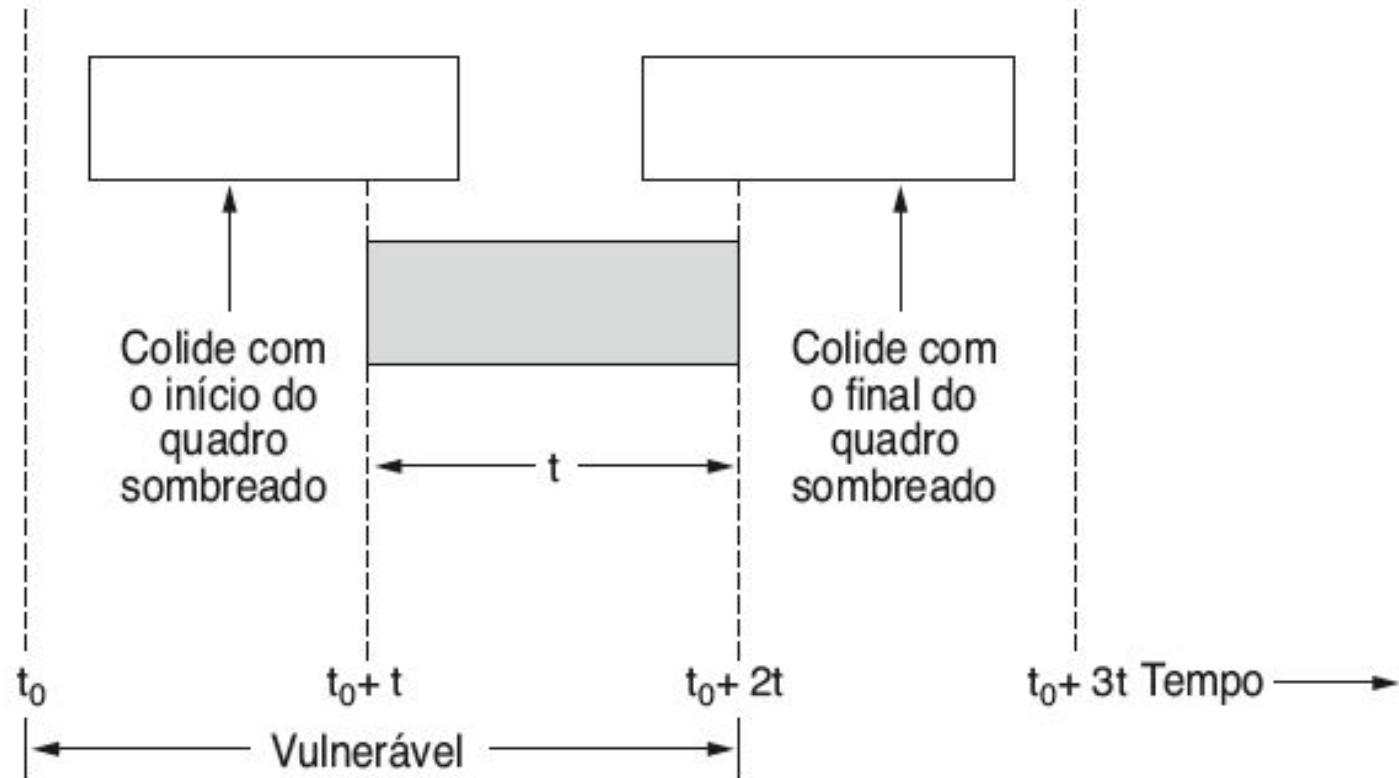
- Sempre que desejado, um nó realiza uma transmissão
- Após a transmissão, ele verifica o canal para identificar se o seu frame foi destruído
- Se sim, o nó espera um tempo aleatório para retransmitir

Tempo Aleatório na Transmissão de Quadros

Usuário



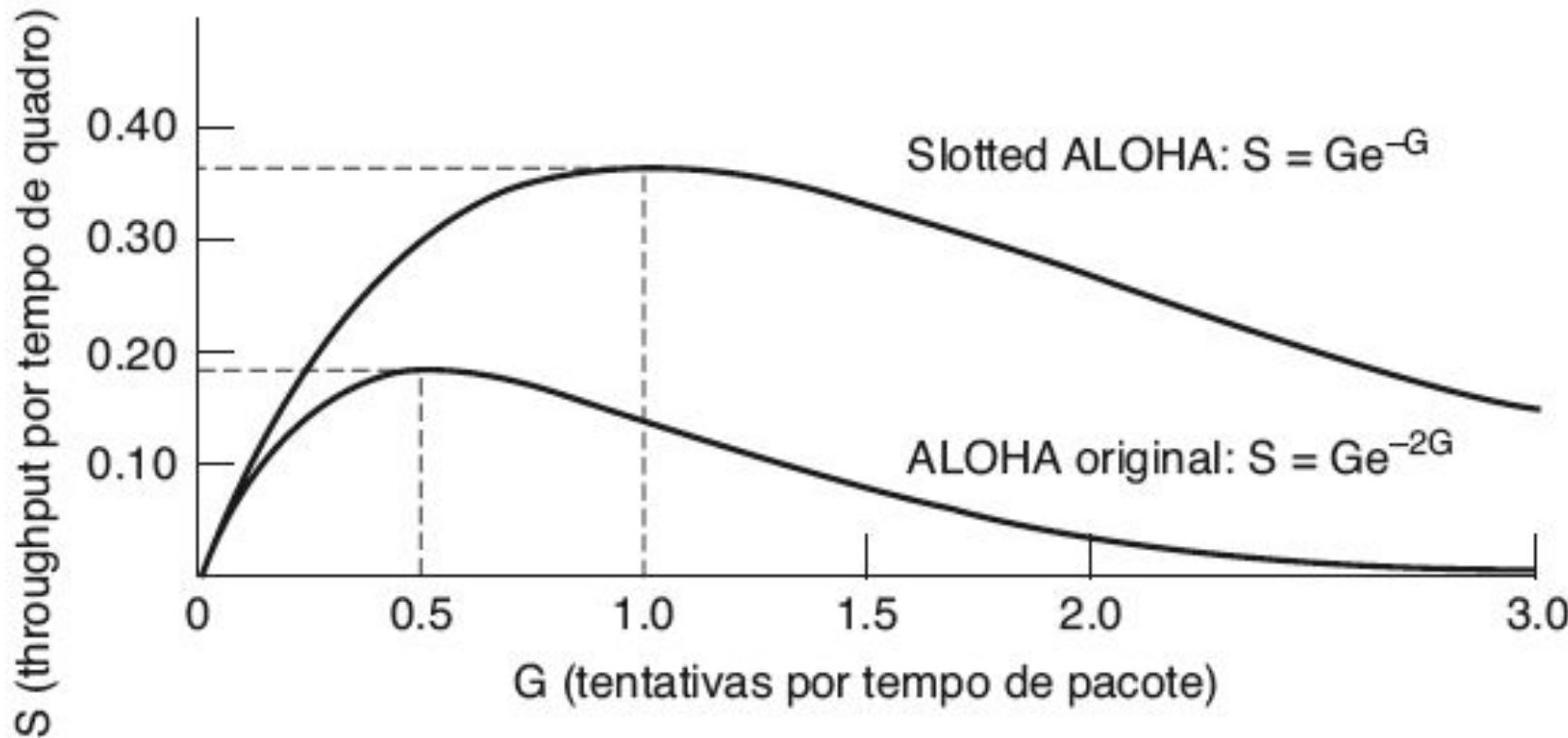
Vulnerabilidade do Quadro (Sombreamento)



Slotted ALOHA

- Mecanismo de sincronização global e tempo é dividido em discretizado em *slots*, onde cada intervalo corresponde a um quadro
- Quando um nó deseja transmitir, ele aguarda início do próximo *slot* de tempo para transmitir
 - Após a transmissão, o nó verifica o canal para identificar se seu quadro foi destruído
 - Se sim, o nó espera um tempo aleatório para retransmitir

ALOHA Puro vs. Slotted ALOHA



Carrier Sense Multiple Access (CSMA)

- Quando uma estação deseja transmitir, ela escuta o canal
- Se estiver ocupado, ela não o utiliza para evitar colisões
- Em caso de colisão, a estação espera um tempo aleatório e recomeça o processo
- O CSMA tem variações para decidir quando a estação deve tentar transmitir novamente
 - 1-persistente
 - p-persistente
 - não persistente

CSMA 1-persistente

- Faz com que a estação continue escutando o canal até que ele fique desocupado
- Inicia a transmissão imediatamente após a desocupação

CSMA 1-persistente

- É chamado 1-persistente porque sempre transmite ao verificar que o canal está desocupado, ou seja, tem probabilidade 1 de transmitir, se canal está livre
- O tempo de propagação tem um efeito importante no desempenho do protocolo

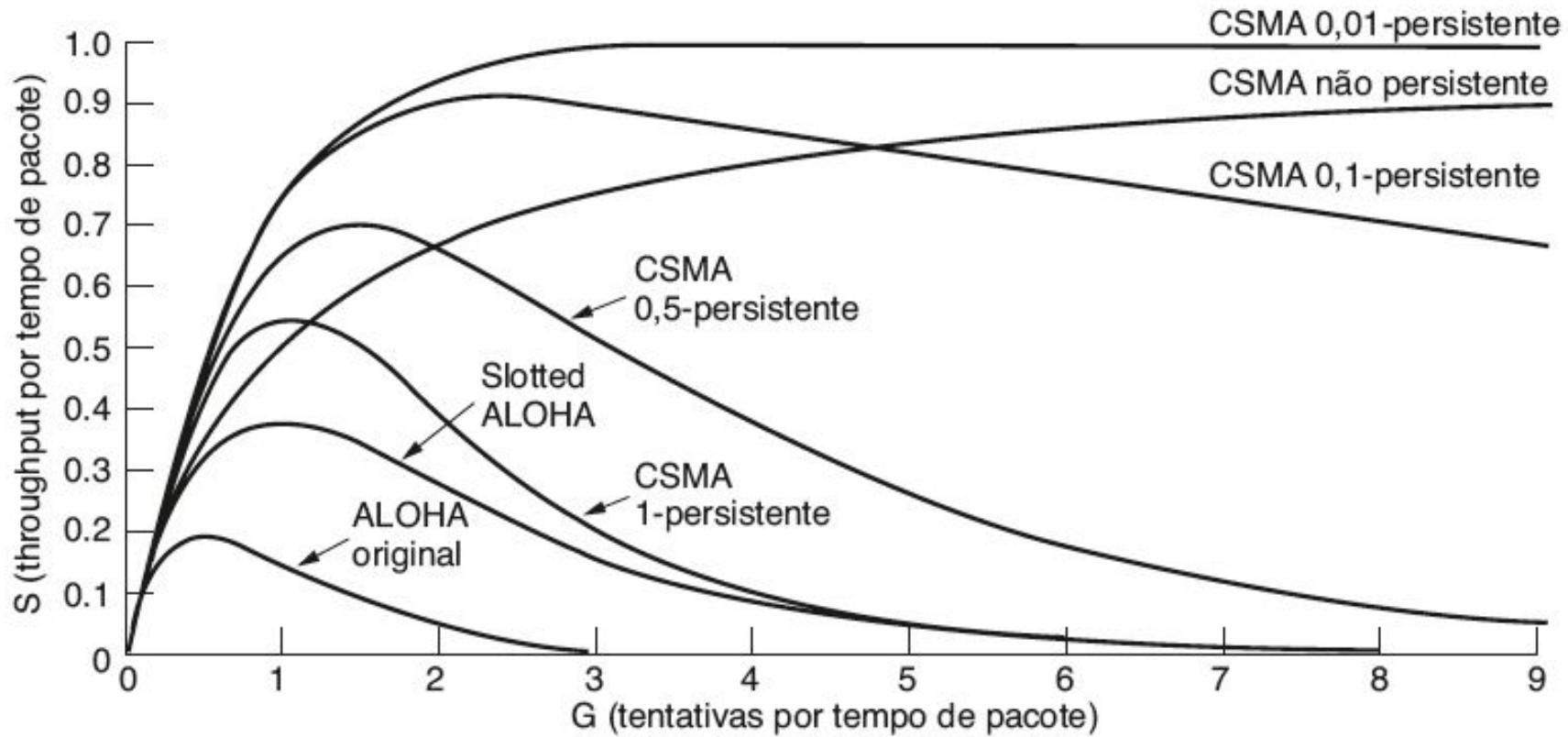
CSMA p-persistente

- Sempre escuta o canal como o 1-persistente
- Quando o canal fica livre, transmite com uma probabilidade p e aguarda um tempo t com probabilidade $(1-p)$
- Após o tempo de espera, o nó repete o passo anterior

CSMA não persistente

- Antes de transmitir, ele analisa o meio físico
- Se estiver livre, ele transmite
- Se estiver ocupado, ele pára de escutar o meio e aguarda um tempo aleatório
- Após o tempo de espera, ele volta ao primeiro passo

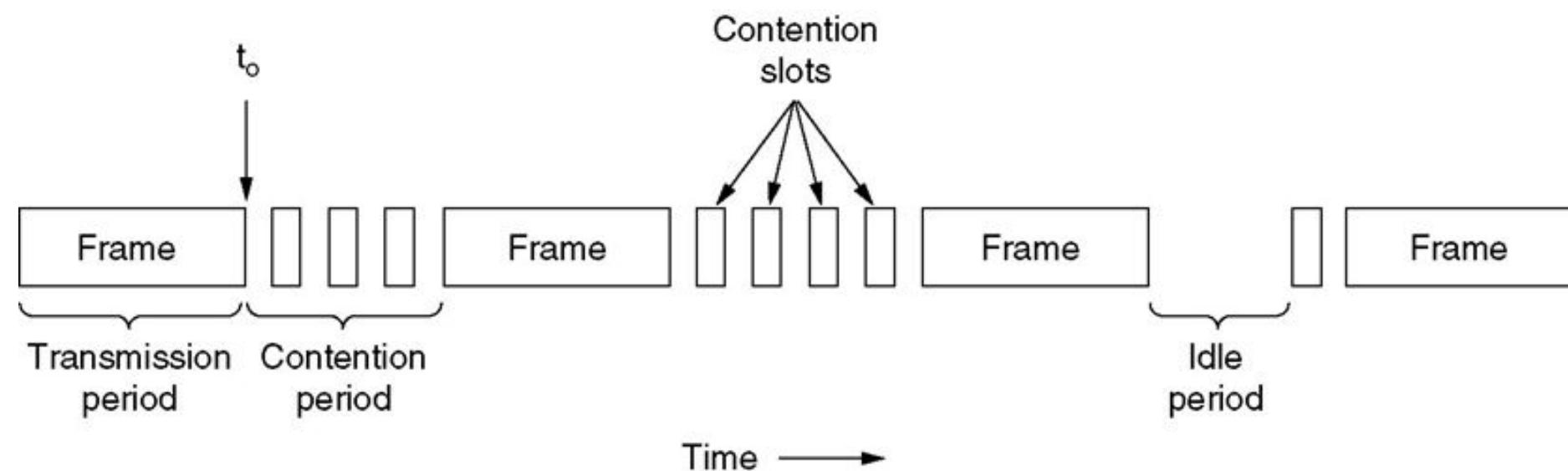
ALOHA * vs. CSMA *



CSMA com Detecção de Colisão

- Como o CSMA 1-persistente, o CSMA/CD sempre escuta o meio físico
- Detecta colisões imediatamente assim que inicia a transmissão e não no final da transmissão como as outras variações anteriores
 - Economia de tempo e de largura de banda
- Em caso de colisão, ele pára a transmissão imediatamente e aguarda um tempo aleatório
- Foi padronizado como IEEE 802.3 (Ethernet)

Etapas do CSMA/CD: Contenção, Transmissão e *Idle*



Considerações sobre o CSMA/CD

- Após uma transmissão, o emissor sabe se houve colisão em, no máximo, o dobro do tempo de propagação no cabo de ponta-a-ponta



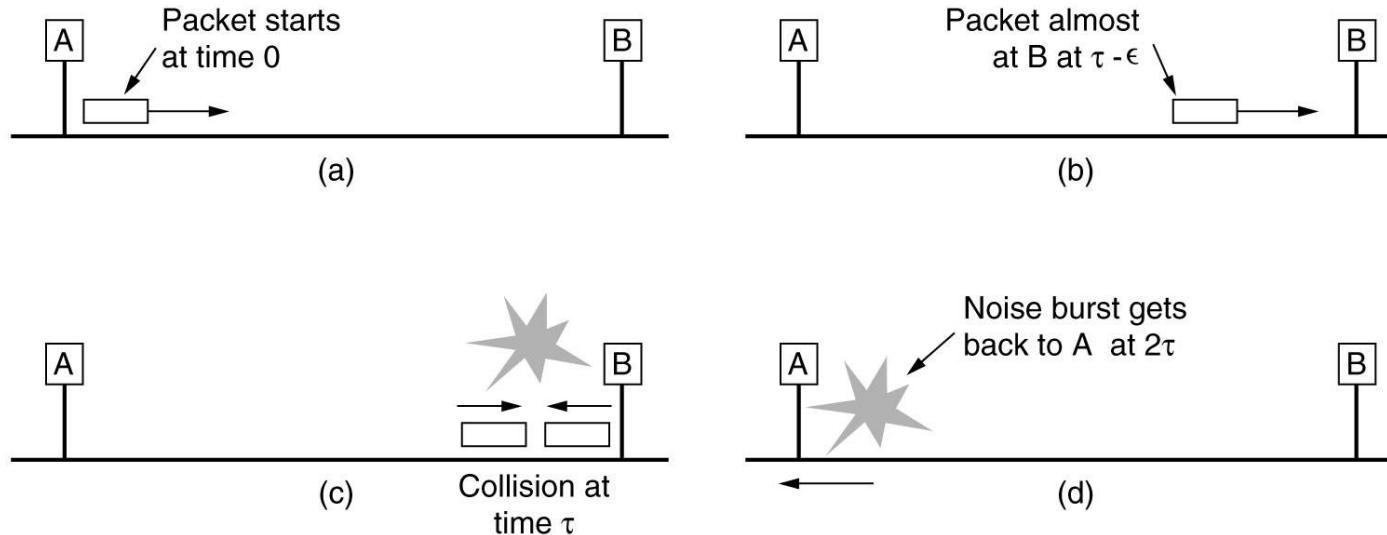
T_0 : A inicia envio do quadro Q_A

T_1 : B inicia envio do quadro Q_B and Q_A chega em B

T_2 : Q_B chega em A

Considerações sobre o CSMA/CD

- Após uma transmissão, o emissor sabe se houve colisão em, no máximo, o dobro do tempo de propagação no cabo de ponta-a-ponta



Padrão IEEE 802 para LANs e MANs



www.ieee802.org

- Conjunto de normas para LANs e MANs
- Padrão adotado pelas seguintes organizações: ANSI, NIST e ISO
- É dividido em partes que são publicados como livros separadamente

Padrão IEEE 802 para LANs e MANs



www.ieee802.org

IEEE 802 LAN/MAN Standards Committee

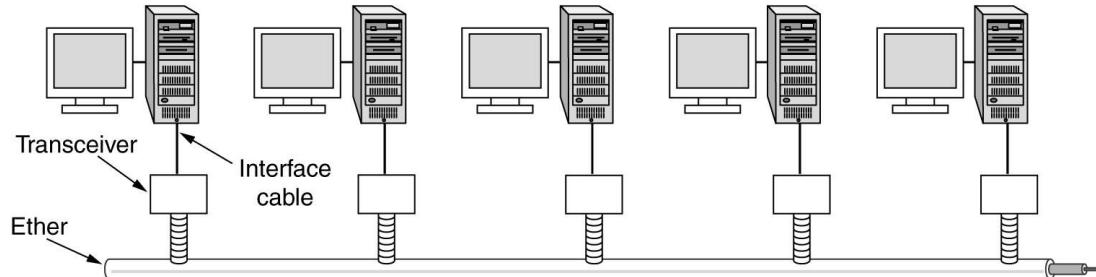
- Get 802 standards
- IEEE 802 Working Groups and Study Groups
- IEEE 802 Session Information
- IEEE 802 General Information
- IEEE 802 Document Repository

Alguns Padrões Importantes do IEEE 802

- IEEE 802.3: Ethernet (LANs)
- IEEE 802.11: WLANs (WiFi)
- IEEE 802.16: (WiMax)



Algumas Topologias com Ethernet



Topologia de barramento

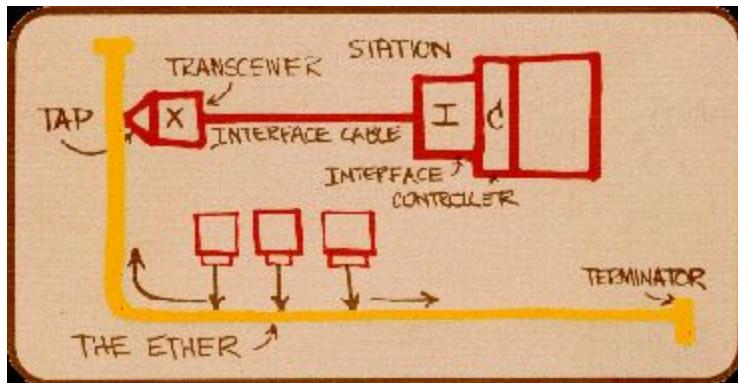


Topologia em estrela

IEEE 802.3: Funcionamento

- Estação escuta o canal antes de transmitir
- Se estiver ocupado espera até ficar livre
- Transmite o quadro se o canal estiver livre
- Se ocorre uma colisão, a estação espera um tempo aleatório e começa o processo todo novamente

IEEE 802.3: História



Baseado no padrão Ethernet de 10 Mbps proposto pela Xerox, DEC e Intel (padrão DIX)

This diagram was hand drawn by Robert M. Metcalfe and photographed by Dave R. Boggs in 1976 to produce a 35mm slide used to present Ethernet to the National Computer Conference in June of that year. On the drawing are the original terms for describing Ethernet.

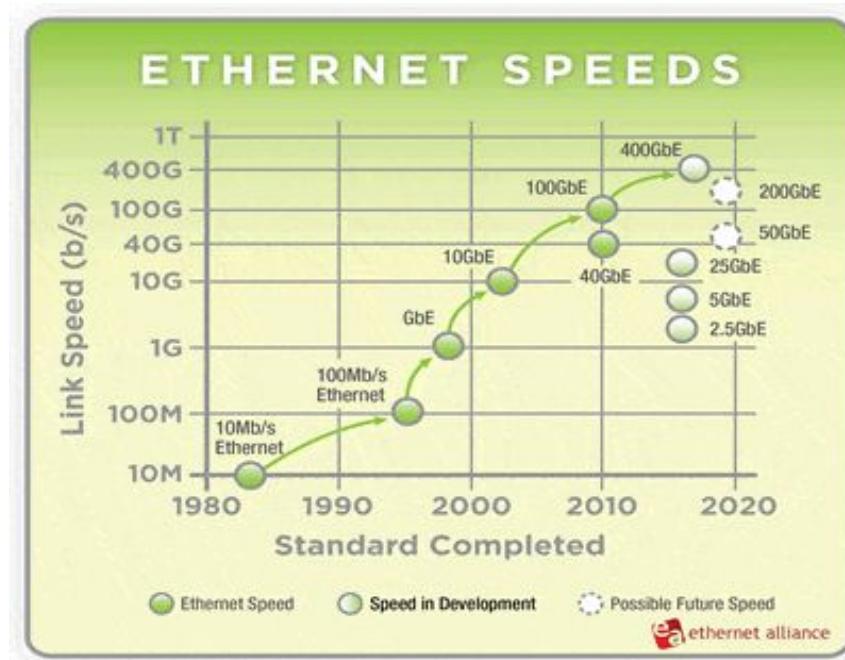
Further information about the origins of Ethernet can be found in the reprinted from "Communications of the ACM" of Ethernet: Distributed Packet Switching for Local Computer Networks by Robert M. Metcalfe and David R. Boggs.

Source:

http://grouper.ieee.org/groups/802/3/ethernet_diag.html
<http://www.acm.org/classics/apr96>

IEEE 802.3: Família de Redes

- 10 Mbps – IEEE 802.3 (Ethernet)
- 100 Mbps – IEEE 802.3u (Fast Ethernet)
- 1 Gbps – IEEE 802.3z (Gigabit Ethernet)
- 10 Gbps – IEEE 802.3a{knnp} (10G Ethernet)
- Hoje (set/2020) - IEEE 802.3d* (400 Gbps)



IEEE 802.3: Quadro

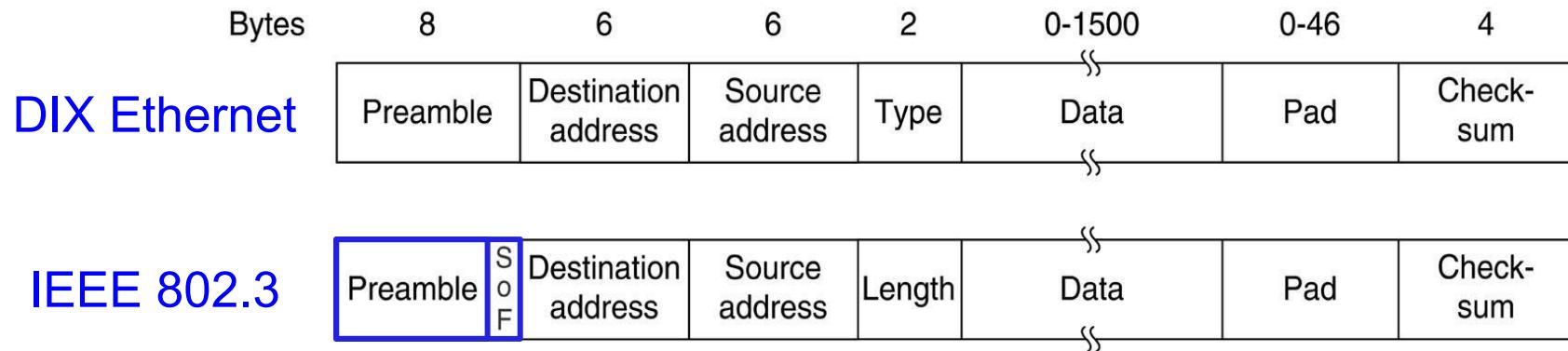
DIX Ethernet

Bytes	8	6	6	2	0-1500	0-46	4
	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum

IEEE 802.3

Preamble	S O F	Destination address	Source address	Length	Data	Pad	Check-sum
----------	-------------	---------------------	----------------	--------	------	-----	-----------

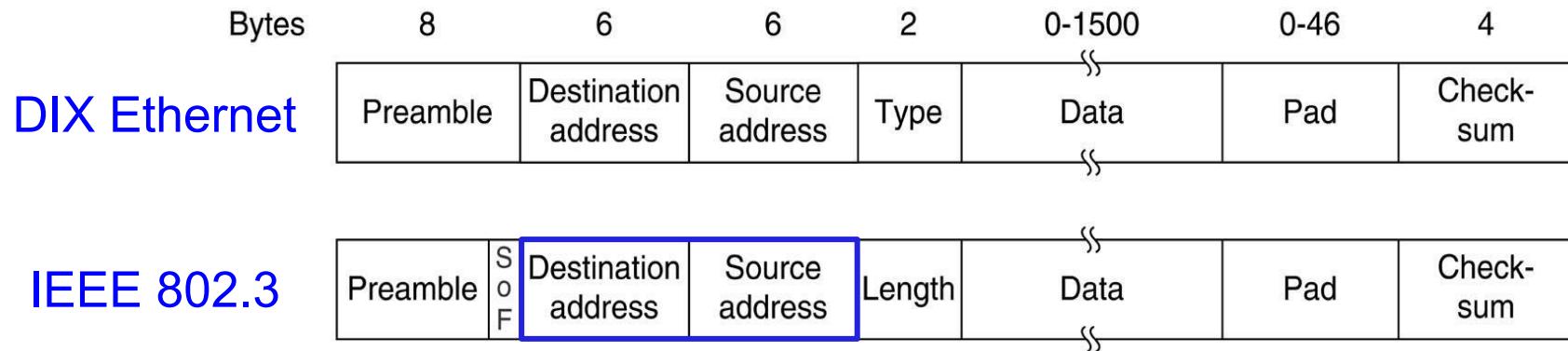
IEEE 802.3: Quadro



- Preâmbulo:

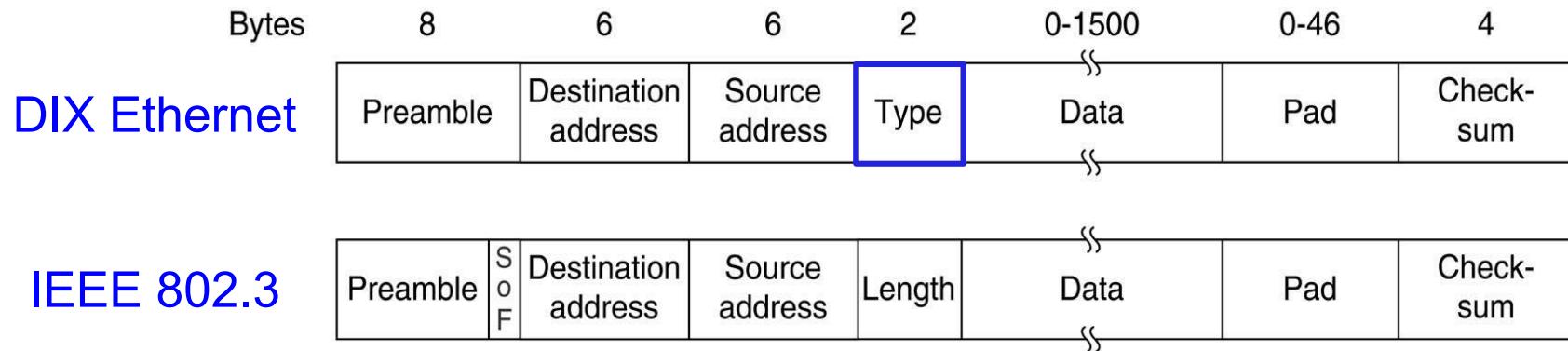
- usado para sincronização entre transmissor e receptor
- 7 bytes 10101010 e 1 byte 10101011

IEEE 802.3: Quadro



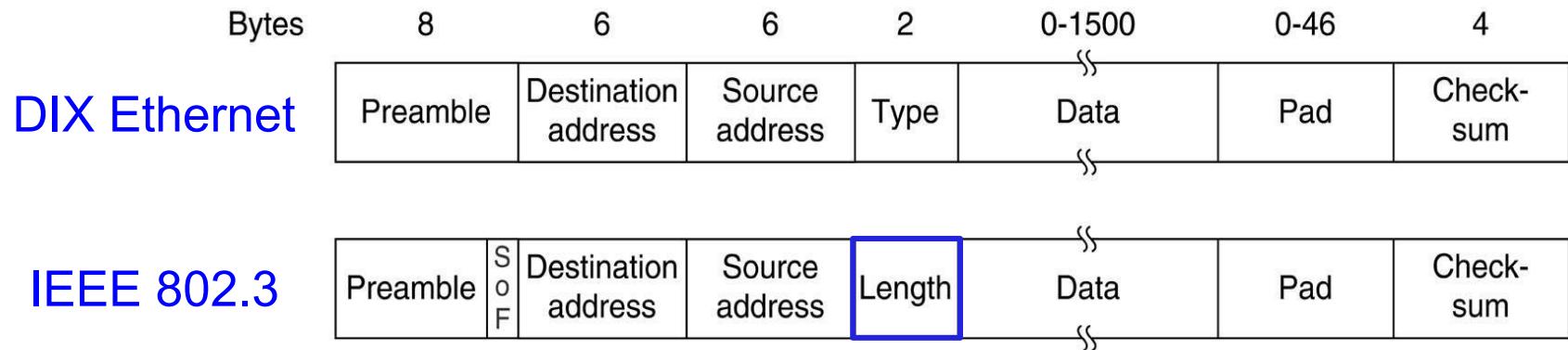
- Endereço LAN dos adaptadores da origem e do destino

IEEE 802.3: Quadro



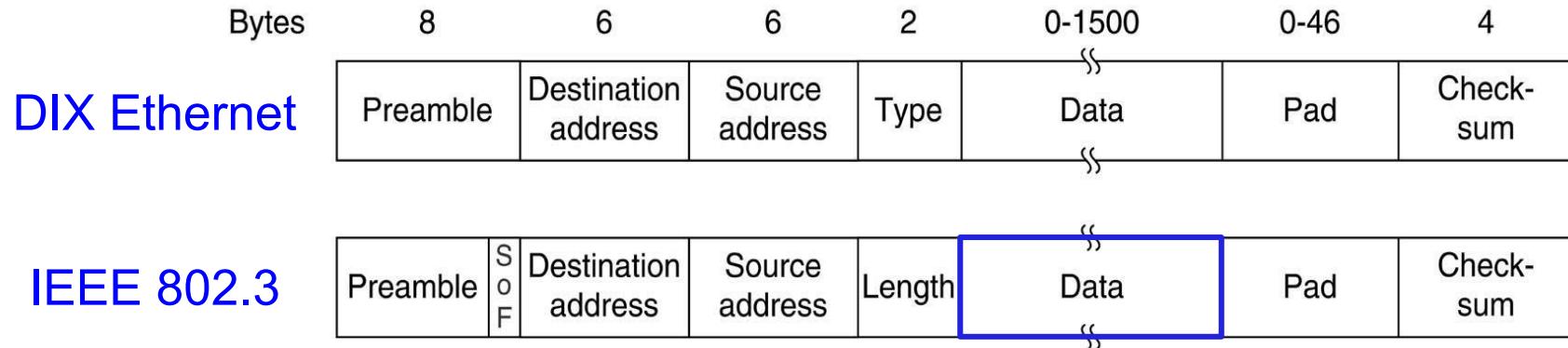
- **Tipo:**
 - Identifica o protocolo da camada de rede que deve receber o pacote
 - Permite que a Ethernet “multiplexe” os protocolos da camada de rede

IEEE 802.3: Quadro



- Comprimento (número de bytes do campo de dados)

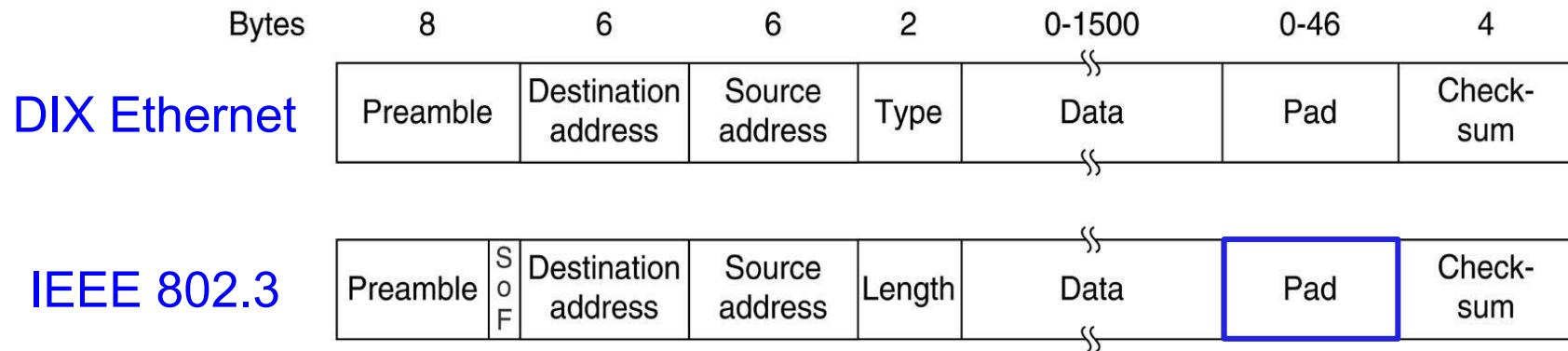
IEEE 802.3: Quadro



• Dados:

- Carrega o datagrama IP
- $46 \text{ bytes} \leq \text{Dados} \leq 1500 \text{ bytes}$
- $64 \text{ bytes} \leq \text{tamanho total quadro} \leq 1518 \text{ bytes}$

IEEE 802.3: Quadro

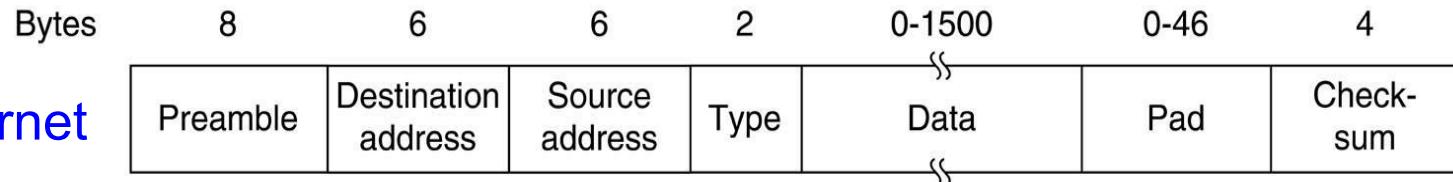


- **Pad (Preenchimento):**

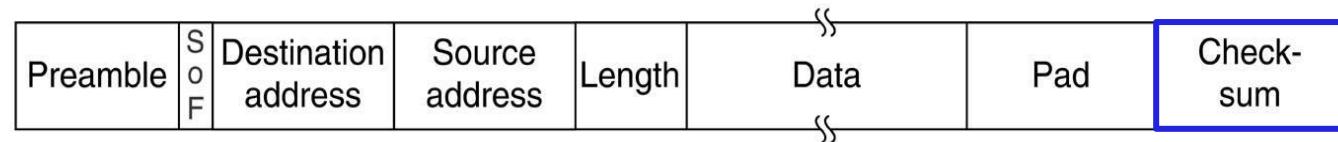
- Campo de dados deve ser ≥ 46
- Caso contrário, pad = 46 – esse valor
- Prevenir que uma estação termine de transmitir um quadro antes do primeiro bit chegar no extremo do cabo e ocorra uma colisão

IEEE 802.3: Quadro

DIX Ethernet

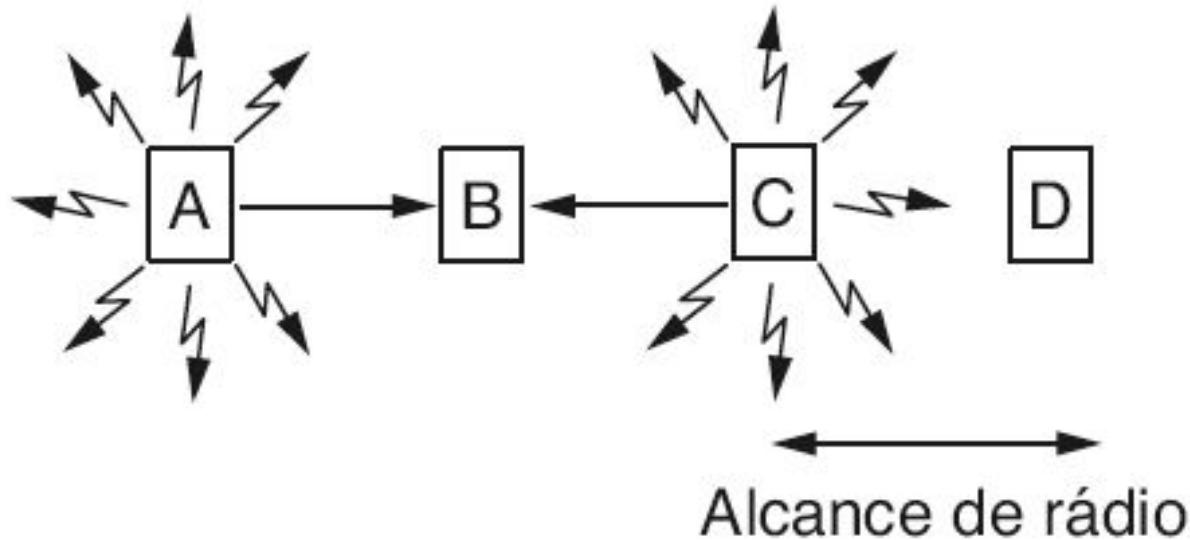


IEEE 802.3



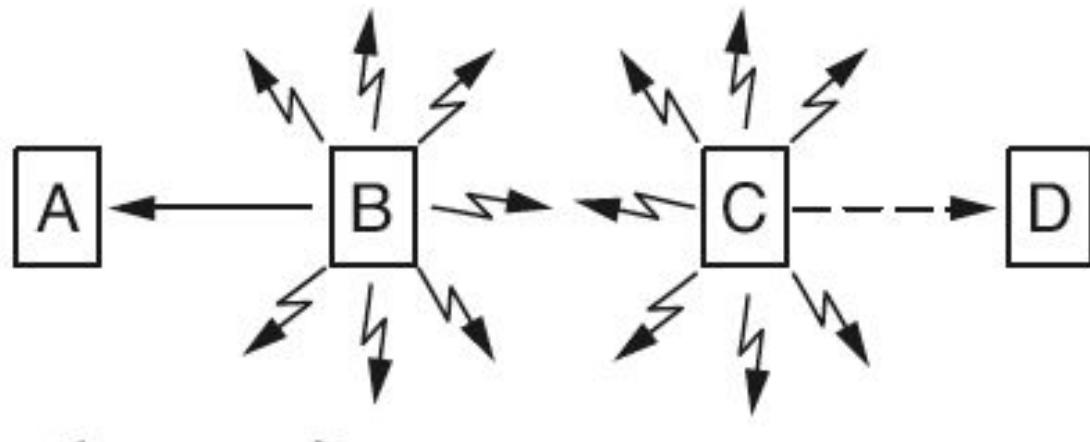
Protocolos para Redes Sem Fio

- Problema do terminal oculto: A e C ocultos ao transmitirem para B



Protocolos para Redes Sem Fio

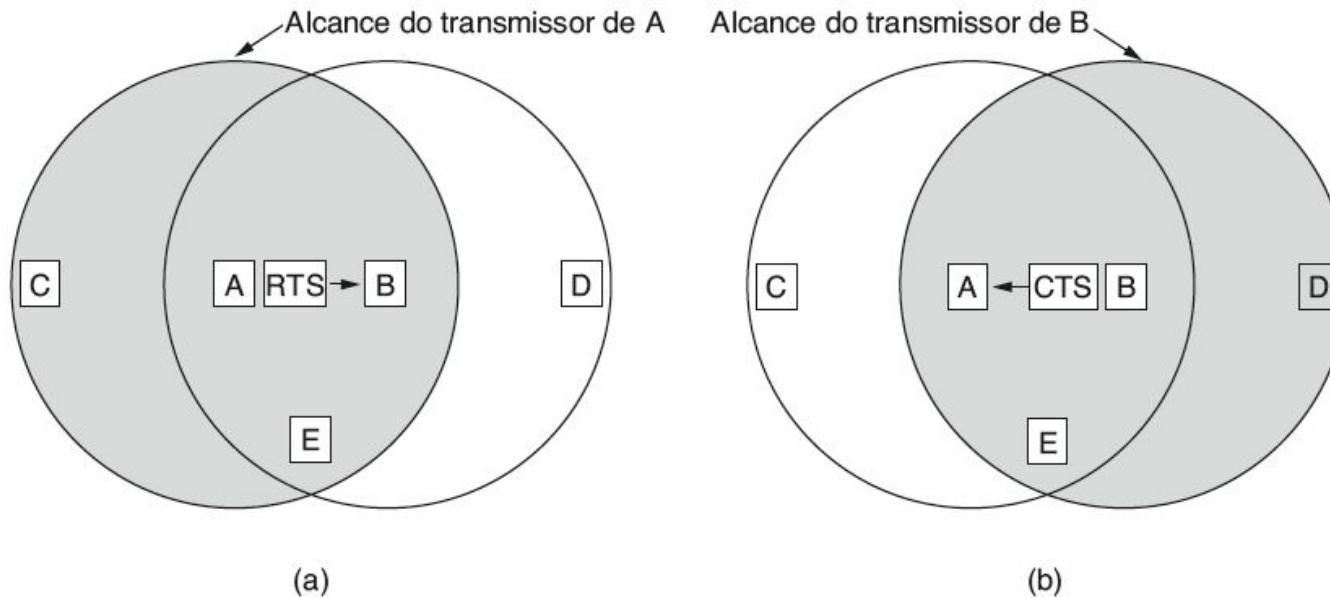
- **Problema do terminal visível:** B e C são visíveis podem transmitir simultaneamente para A e D, respectivamente



Alcance de rádio

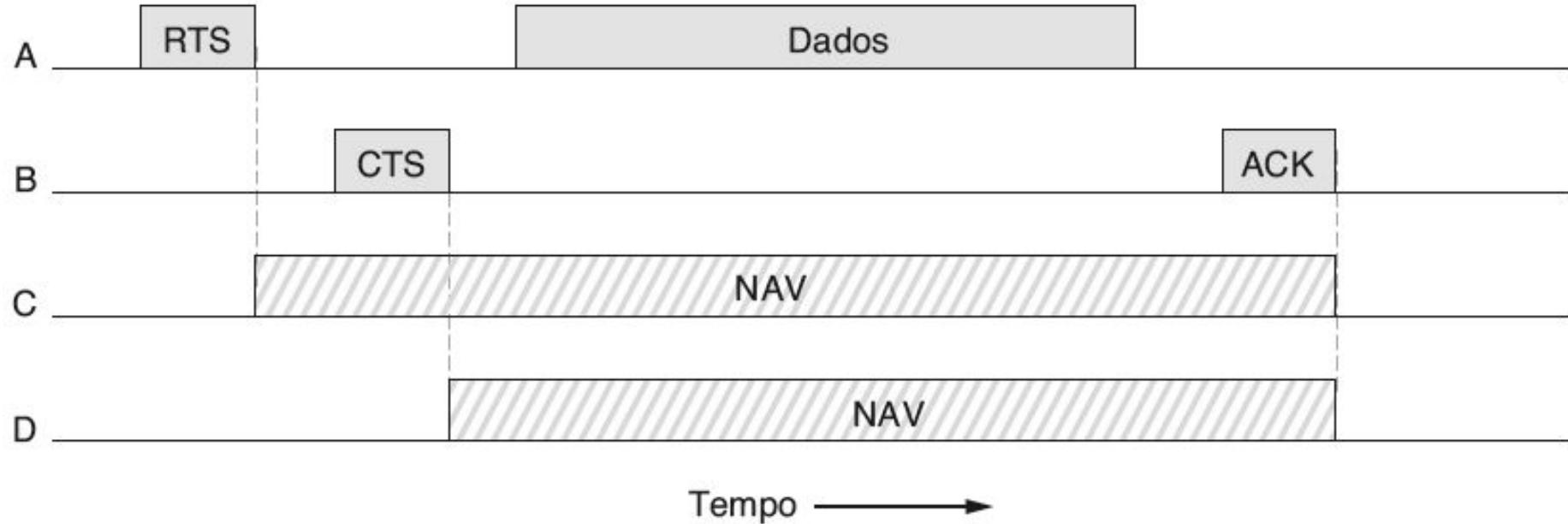
Protocolos para Redes Sem Fio

- Protocolo MACA: (a) A envia um RTS a B; (b) B responde com um CTS para A.



Protocolos para Redes Sem Fio

- Sensoriamento de portadora em um canal com CSMA/CA



Protocolos Sem Colisão

- Para evitar colisões que geram muitos atrasos na transmissão em meios físicos broadcast, alguns protocolos sem colisão foram inventados:
 - Protocolos Bit Map
 - Protocolos de contador binário

Protocolos Bit Map

- O uso do meio físico é alternado entre contenção e dados
- Na fase de contenção cada estação transmite somente um bit indicando se deseja transmitir dados ou não
- Em função da fase de contenção, na fase de dados cada estação transmite os dados na ordem correta (a ordem é pré-definida)

Protocolos de Contador Binário

- Otimizam o Bit-Map que envia 1 bit para cada estação na fase de contenção, enviando um número em binário da estação que deseja transmitir
- Cada estação transmite 1 bit do seu endereço em binário

Protocolos de Contador Binário

- Como o meio físico mantém os bits 1 (faz um OR com os bits enviados), o endereço das estações com mais bits 1s ficarão no meio físico
- As estações que não foram selecionadas param de enviar os bits
- No final da fase de contenção foi transmitido o endereço da estação que transmitirá os dados.

Exercício (1)

- Diferencie o ALOHA Puro, Slotted ALOHA e família CSMA.

Exercício (2)

- Quais são as versões do CSMA? Qual é a diferença entre elas?

Exercício (3)

- Quais são os problemas do terminal oculto e do terminal visível?

Exercício (4)

- Como funciona o *Handshaking* do IEEE 802.11? E como ele evita o problema do terminal oculto e o do visível?

Unidade V: Camada de Rede

Prof. Max do Val Machado



PUC Minas

Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Disciplina Redes de Computadores I

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- *Internet Protocol v6 (IPv6)*

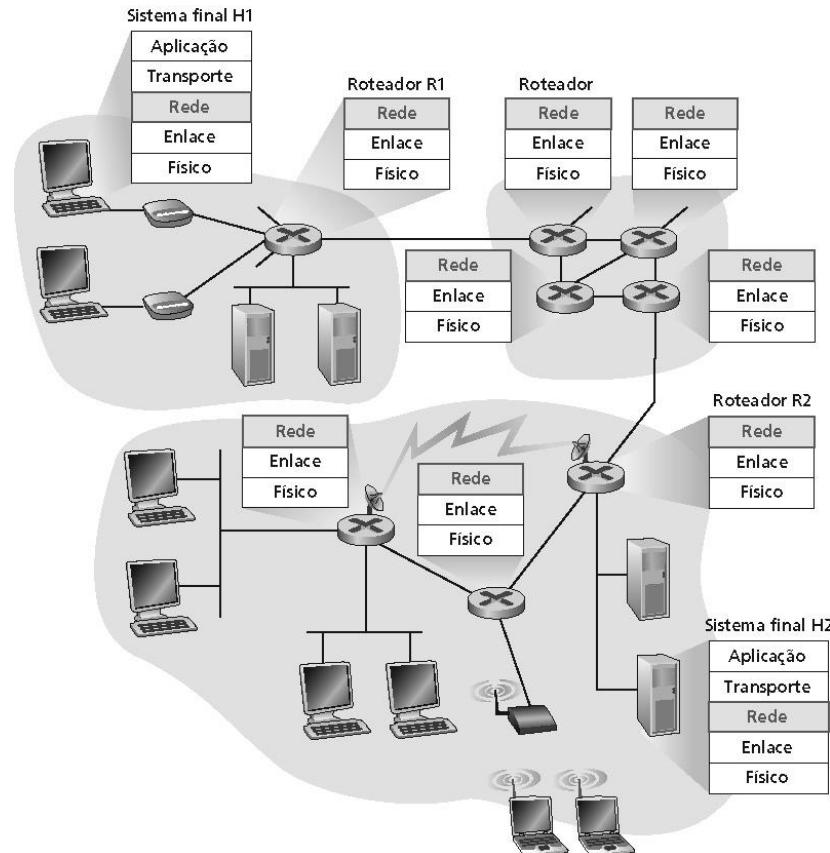
Agenda

- **Introdução**
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- *Internet Protocol v6 (IPv6)*

Introdução

- A camada de rede é responsável por transferir pacotes da origem para o destino
 - Conhecimento da topologia da rede
 - Escolha de rotas: evitar as “piores” e buscar as “melhores”
 - Controle de congestionamento: roteamento baseado em tráfego, controle de acesso e corte de carga

Exemplo da Topologia de uma Rede



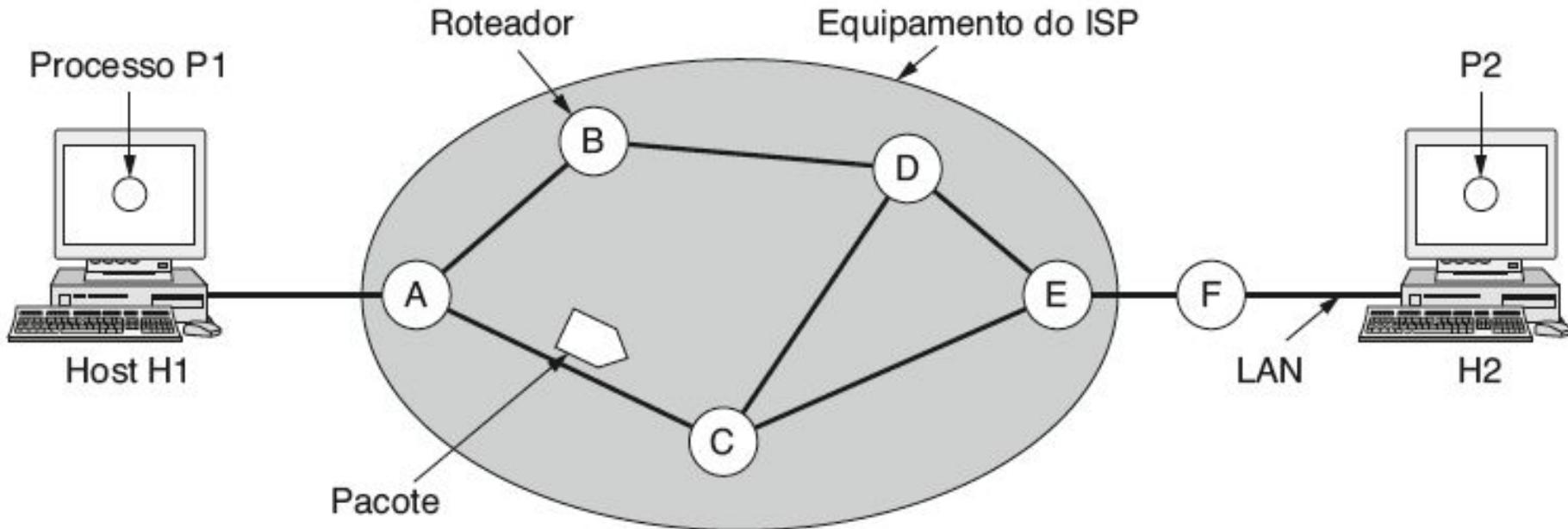
Agenda

- Introdução
- **Questões de projeto da camada de rede**
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- *Internet Protocol v6 (IPv6)*

Questões de Projeto da Camada de Rede

- Comutação de pacotes *store-and-forward*
- Serviços oferecidos à Camada de Transporte
- Serviços orientados (**ou não**) à conexão

Comutação de Pacotes *store-and-forward*



Serviços oferecidos à Camada de Transporte

- Independência em relação à tecnologia presente nos roteadores
- Independência em relação à topologia da rede

Serviços Não Orientados à Conexão

- Uma mensagem pode ser dividida em vários pacotes e cada um deles pode ser roteado por uma rota
- Rede de Datagramas
- Exemplo: Internet Protocol (IP)

Serviços Não Orientados à Conexão

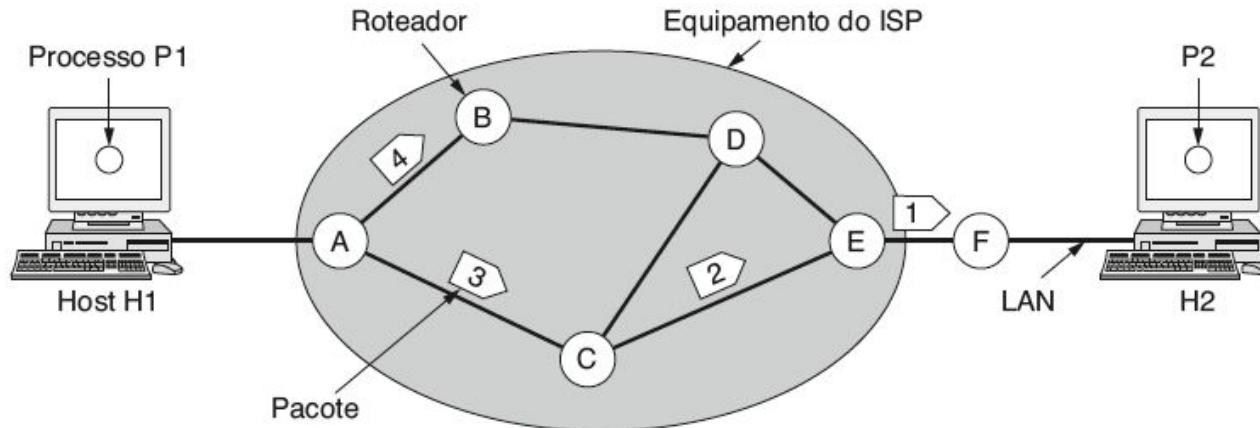


Tabela de A (inicial)

A	-
B	B
C	C
D	B
E	C
F	C

Dest. Interface

Tabela de A (depois)

A	-
B	B
C	C
D	B
E	B
F	B

Tabela de C

A	A
B	A
C	-
D	E
E	E
F	E

A	C
B	D
C	C
D	D
E	-
F	F

Serviços Não Orientados à Conexão

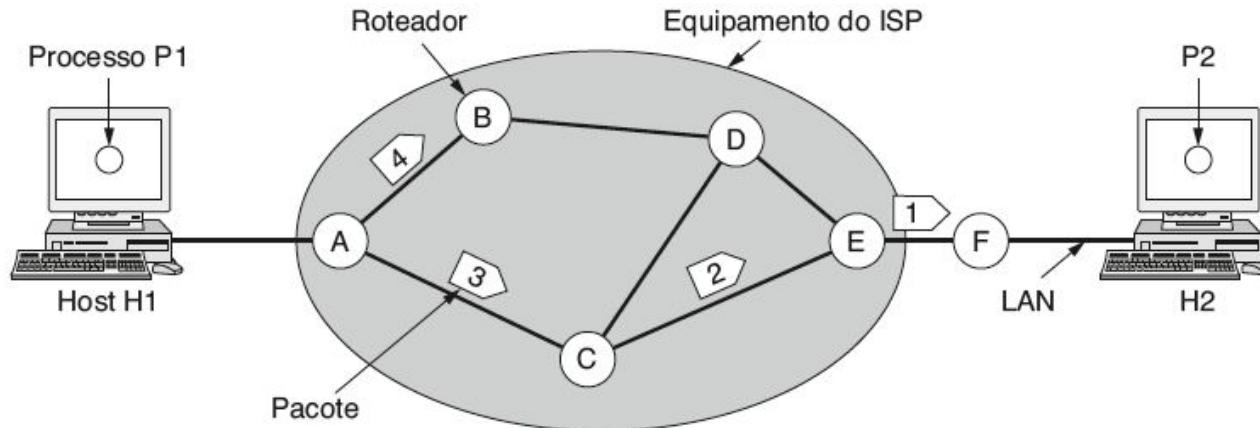


Tabela de A (inicial)

A	-
B	B
C	C
D	B
E	C
F	C

Tabela de A (depois)

A	-
B	B
C	C
D	B
E	B
F	B

Tabela de C

A	A
B	A
C	-
D	E
E	E
F	E

Tabela de E

A	C
B	D
C	C
D	D
E	-
F	F

Dest. Interface

Serviços Orientados à Conexão

- Implementação de serviços orientados à conexão
- Rede de Circuitos Virtuais
- Exemplo: *Multi Protocol Label Switching* (MPLS)

Serviços Orientados à Conexão

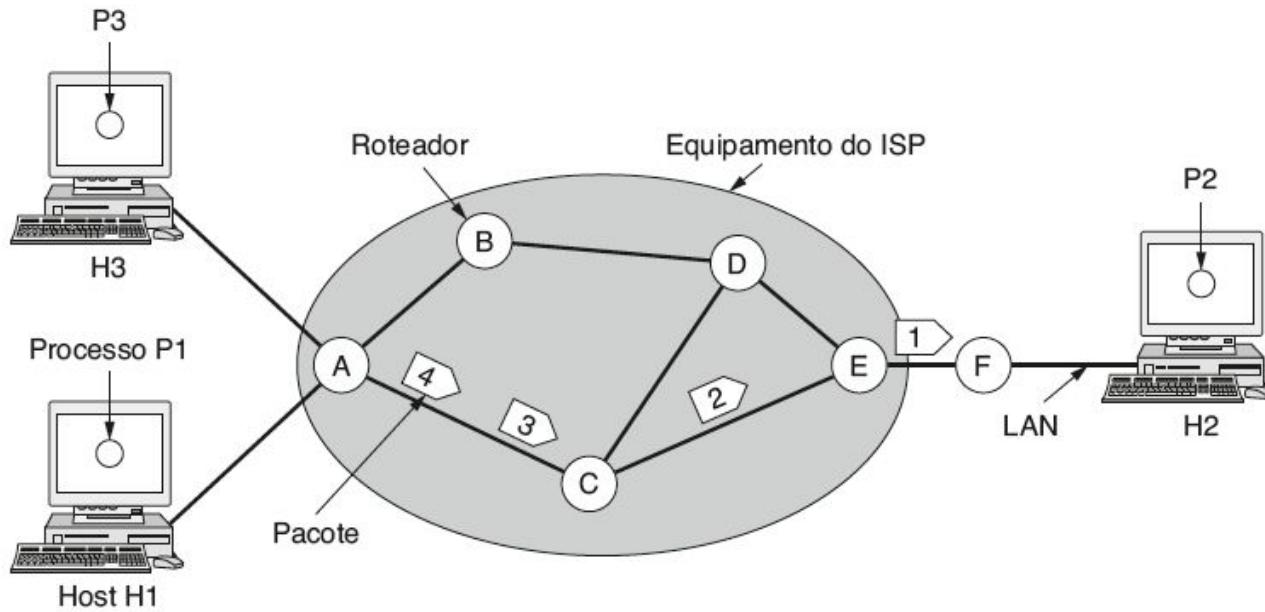


Tabela de A	
Entrada	Saída
H1 1	C 1
H3 1	C 2

Tabela de C	
Entrada	Saída
A 1	E 1
A 2	E 2

Tabela de E	
Entrada	Saída
C 1	F 1
C 2	F 2

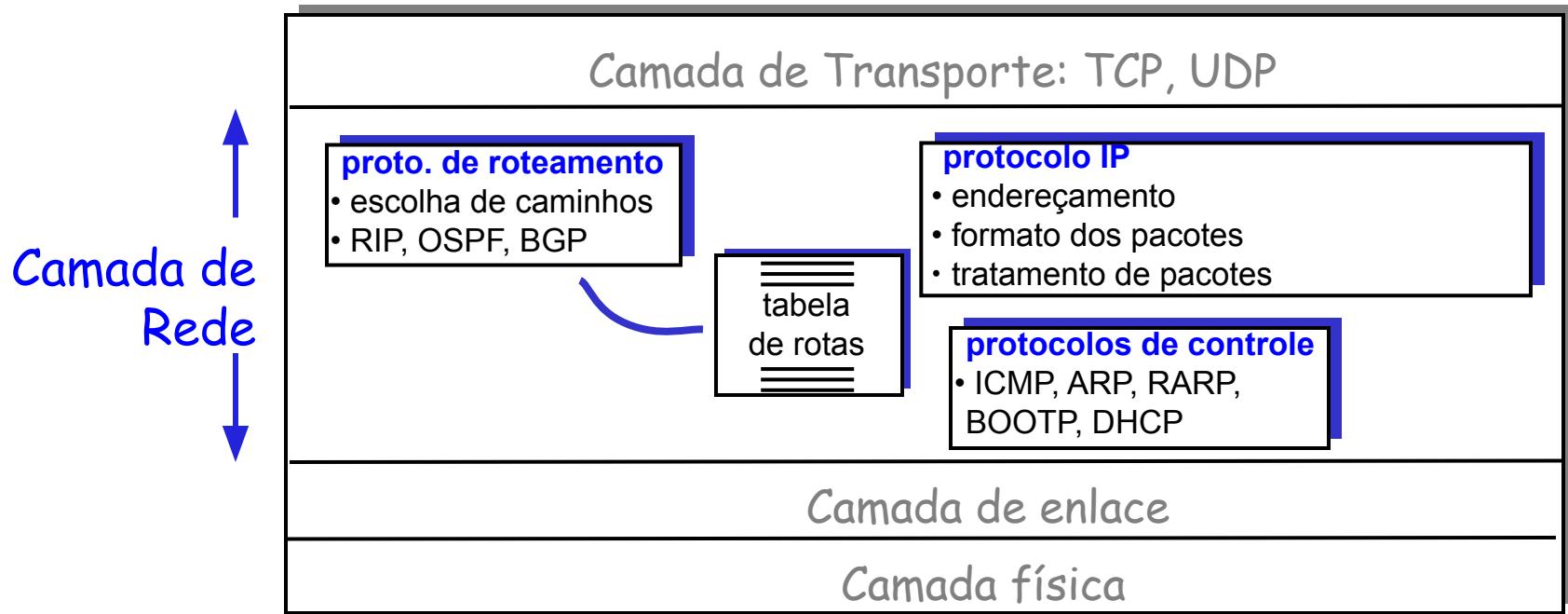
Rede de Datagrama vs de Circuito Virtual

Questão	Rede de datagramas	Rede de circuitos virtuais
Configuração de circuitos	Desnecessária	Obrigatória
Endereçamento	Cada pacote contém os endereços completos de origem e de destino	Cada pacote contém um pequeno número do circuito virtual
Informações sobre o estado	Os roteadores não armazenam informações sobre o estado das conexões	Cada circuito virtual requer espaço em tabelas de roteadores por conexão
Roteamento	Cada pacote é roteado independentemente	A rota é escolhida quando o circuito virtual é estabelecido; todos os pacotes seguem essa rota
Efeito de falhas no roteador	Nenhum, com exceção dos pacotes perdidos durante a falha	Todos os circuitos virtuais que tiverem passado pelo roteador que apresentou o defeito serão encerrados
Qualidade de serviço	Difícil	Fácil, se for possível alocar recursos suficientes com antecedência para cada circuito virtual
Controle de congestionamento	Difícil	Fácil, se for possível alocar recursos suficientes com antecedência para cada circuito virtual

Agenda

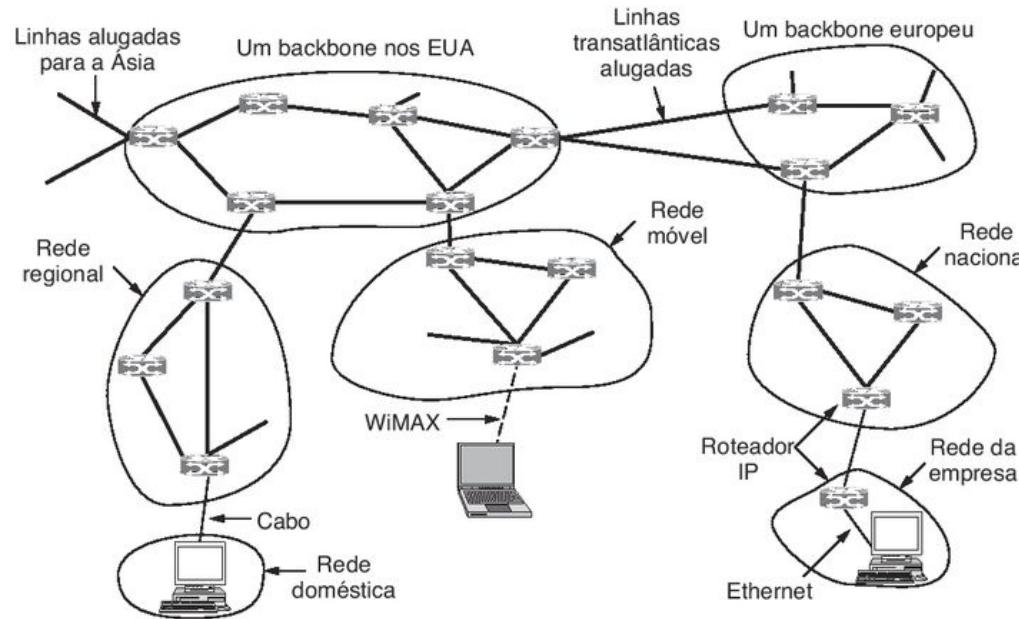
- Introdução
- Questões de projeto da camada de rede
- **A camada de rede da Internet**
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- *Internet Protocol v6 (IPv6)*

A Camada de Rede da Internet



A Camada de Rede da Internet

- Pode ser vista como um conjunto de sub-redes ou sistemas autônomos conectados entre si



Princípios da Camada de Rede da Internet

- Certifique-se de que funciona



Princípios da Camada de Rede da Internet

- Mantenha a simplicidade



Princípios da Camada de Rede da Internet

- Faça escolhas claras



Princípios da Camada de Rede da Internet

- Explore modularidade



Princípios da Camada de Rede da Internet

- Espere heterogeneidade



Princípios da Camada de Rede da Internet

- Evite opções e parâmetros estáticos



Princípios da Camada de Rede da Internet

- Procure excelência de projeto, contudo, não existe mundo perfeito



Princípios da Camada de Rede da Internet

- Seja rígido ao enviar e tolerante ao receber

Enviar pacote



Receber pacote

Princípios da Camada de Rede da Internet

- Escalabilidade



Princípios da Camada de Rede da Internet

- Considere custo e desempenho



Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- *Internet Protocol v6 (IPv6)*

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- *Internet Protocol v6 (IPv6)*

- **Introdução**
 - Cabeçalho
 - Endereçamento
 - Roteamento IPv4
 - Caixa NAT

Internet Protocol (IP)

- Elemento que mantém a Internet unida
- Projetado para a interconexão de redes
- Apresenta a melhor forma para transportar pacotes entre a origem e o destino, independente deles pertencerem à mesma rede, à redes adjacentes ou não

Internet Protocol (IP)

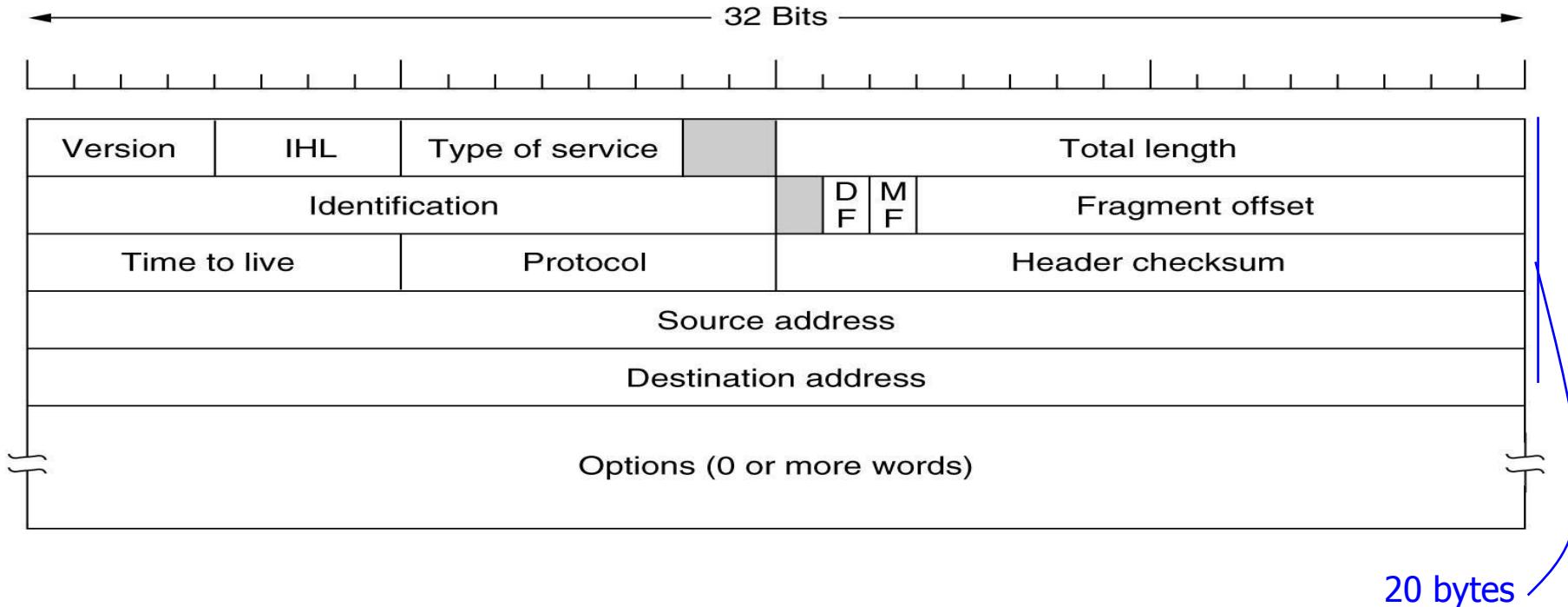
- Entrega pacotes com o “maior esforço” (*best-effort delivery*), contudo, não garante:
 - Duplicação de pacotes
 - Entrega atrasada ou fora de ordem
 - Alteração de dados
 - Perda de pacotes
- Protocolos de outros níveis também devem tratar desses problemas

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - ***Internet Protocol v4 (IPv4)***
 - Protocolos de controle da Internet
 - Roteamento
 - *Internet Protocol v6 (IPv6)*
- Introdução
 - **Cabeçalho**
 - Endereçamento
 - Roteamento IPv4
 - Caixa NAT

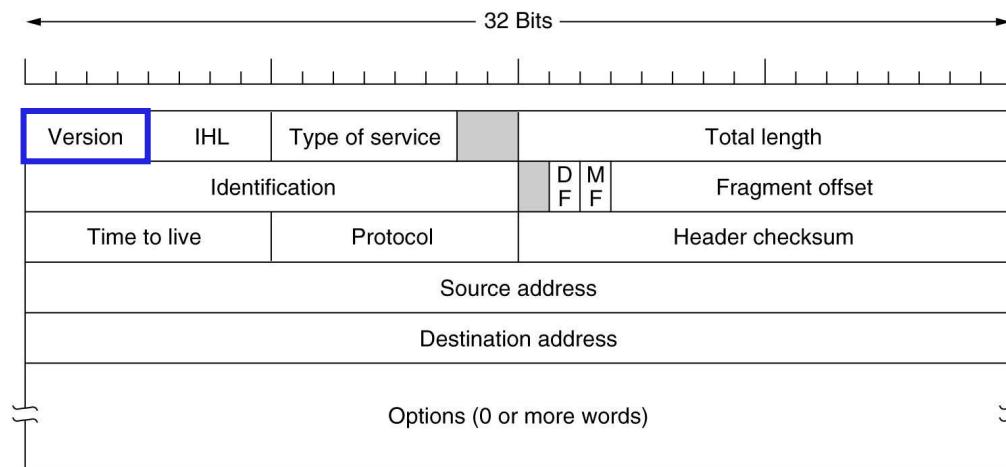
- Permite um pacote de até 64 KBytes
- O cabeçalho tem uma parte fixa de 20 bytes e outra opcional (tamanho variável)

Cabeçalho do IPv4



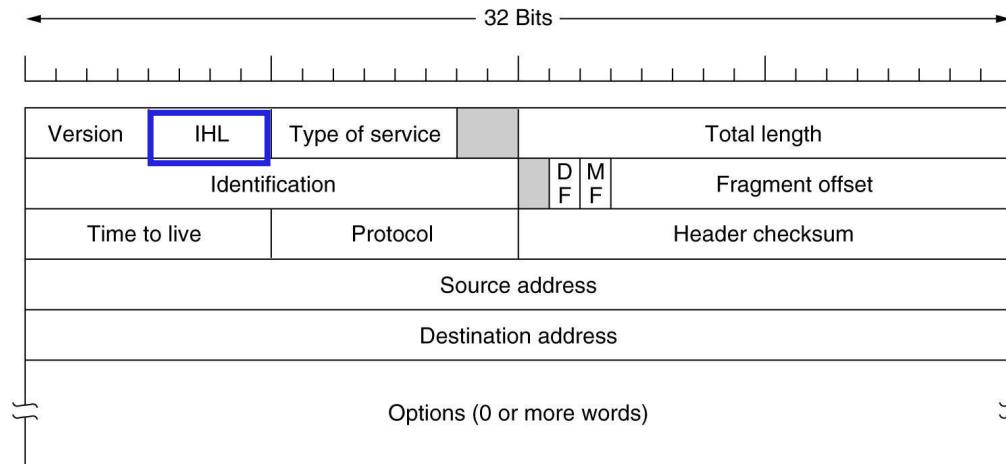
Campo Version (4 bits)

- Indica o número da versão corrente
- Permite uma transição “suave” entre versões



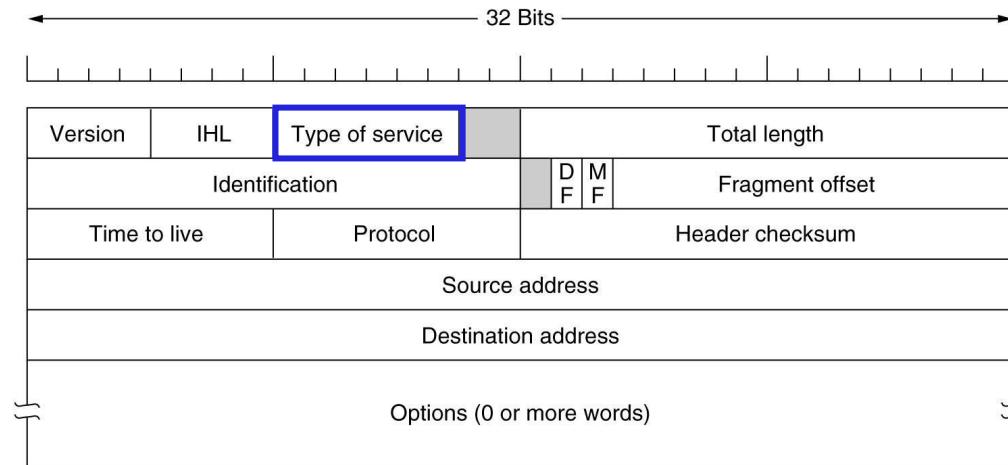
Campo IHL (4 bits)

- Informa o tamanho do cabeçalho em palavras de 32 bits
- Mínimo: 5 (sem nenhuma opção)
- Máximo: 15 (60 bytes sendo 40 bytes no campo *Options*)



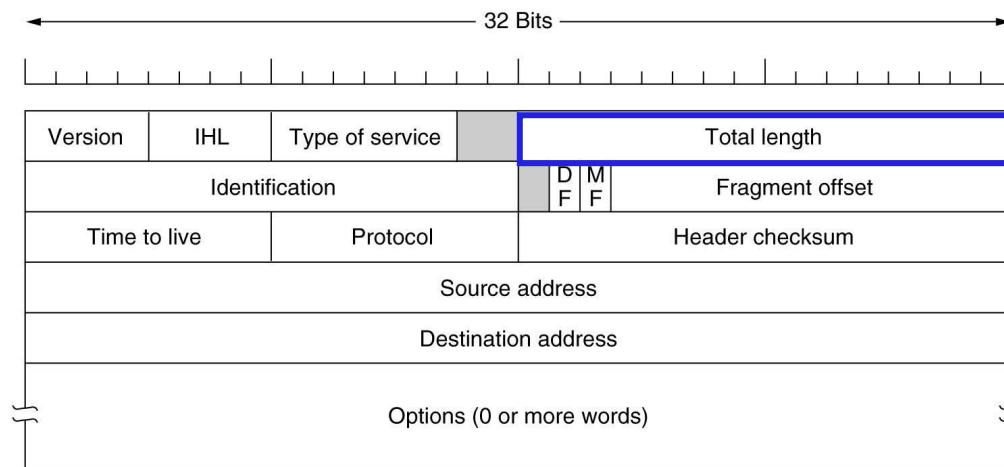
Campo Type of service (6 bits)

- Diferencia as classes de serviço, indicando o que é mais importante para a aplicação: menor atraso, maior vazão, maior confiabilidade
- Na prática, os roteadores tendem a ignorar tal campo



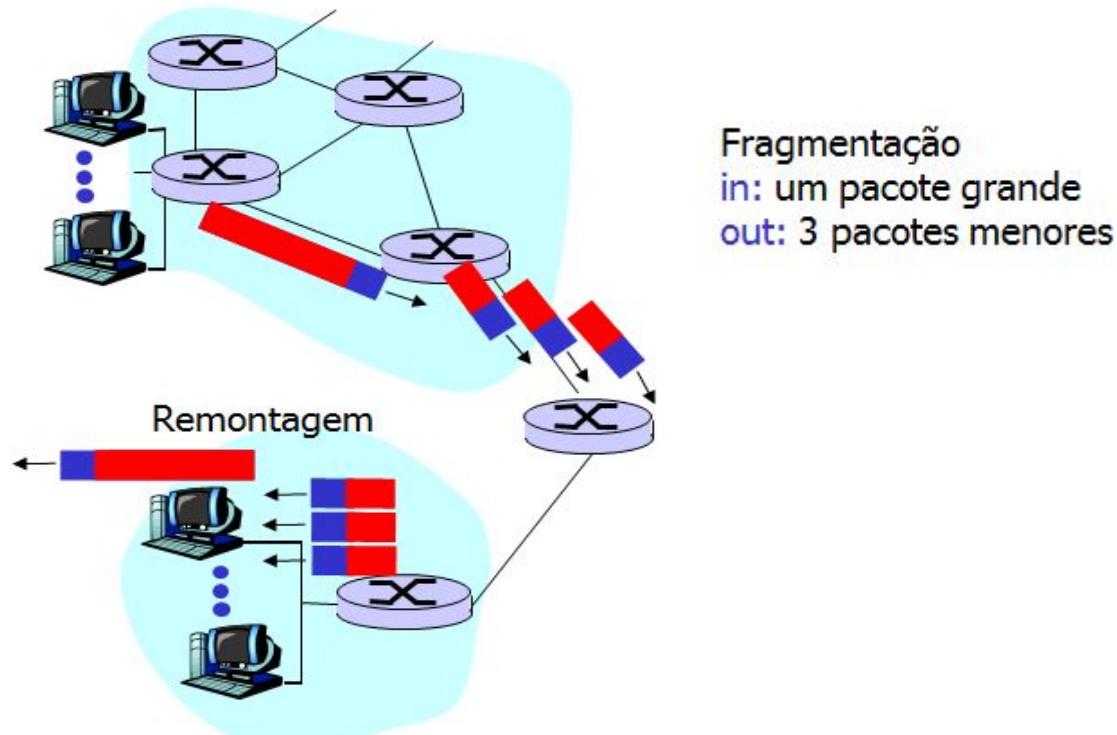
Campo *Total length* (16 bits)

- Tamanho, em bytes, de todo o pacote: cabeçalho e dados
- Valor máximo 65535



Fragmentação e Remontagem de Pacotes

- Pacotes podem ser maiores que os quadros, fazendo com que a camada de rede tenha que fragmentá-los



Fragmentação e Remontagem de Pacotes

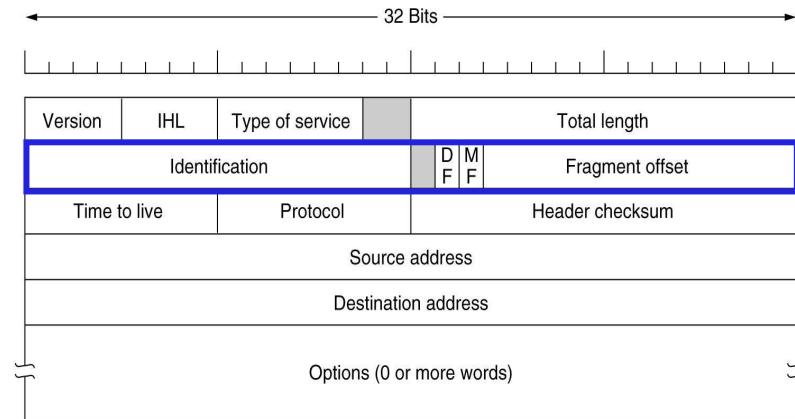
- O cabeçalho é preservado na fragmentação, exceto o campo de *checksum*

Unidade Máxima de Transferência (MTU)

- Do inglês, *Maximum Transmission Unit* (MTU)
- Quantidade máxima de dados que um quadro de enlace pode carregar
- Protocolos de enlace possuem diferentes tamanhos de quadros
 - Por exemplo, a carga útil máxima do Ethernet é 1500 bytes
 - Existem protocolos de enlace cuja carga útil máxima é 576 bytes

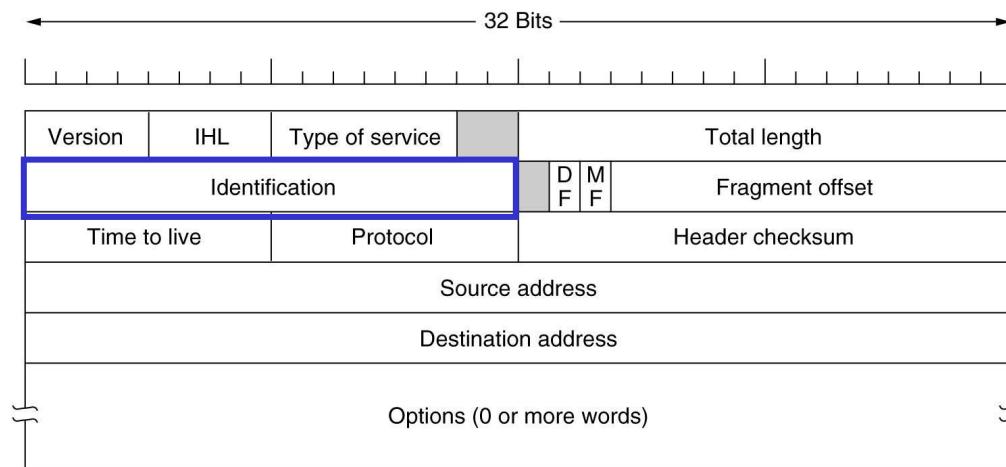
Fragmentação e Remontagem de Pacotes

- A origem ou intermediário fragmenta o pacote e o destino remonta os fragmentos
- O IPv4 permite a identificação e ordenação dos fragmentos
- Se a rede perder um fragmento, o destino descarta o pacote todo
- Seus campos no IPv4 são:
 - *Identification*
 - DF
 - MF
 - *Fragment Offset*



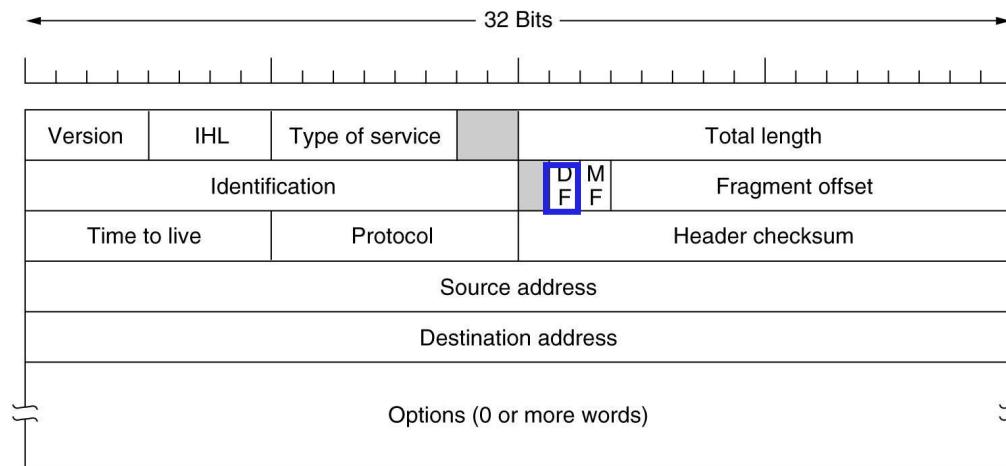
Campo *Identification* (16 bits)

- Identificador de um pacote
- Número auto incremental em cada emissor
- Todos os fragmentos de um pacote têm o mesmo *Identification*



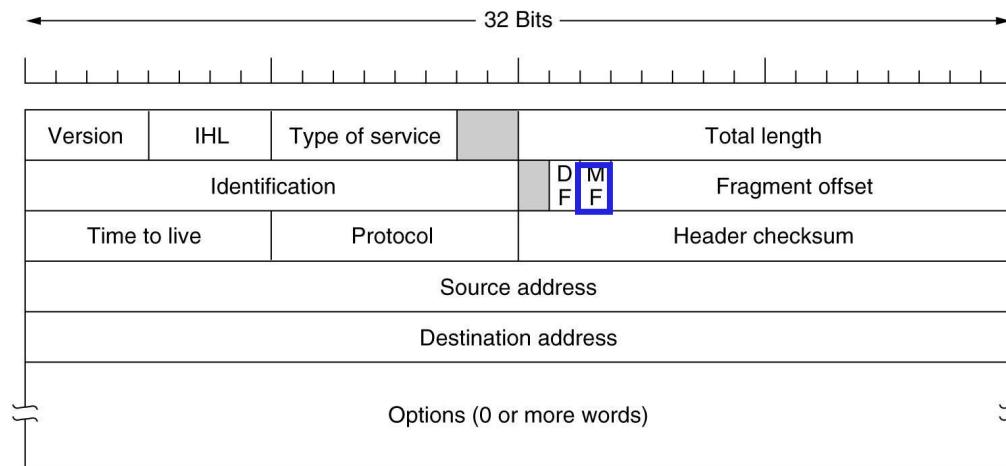
Bit *Don't Fragment* (DF)

- Indica que o pacote não deve ser fragmentado



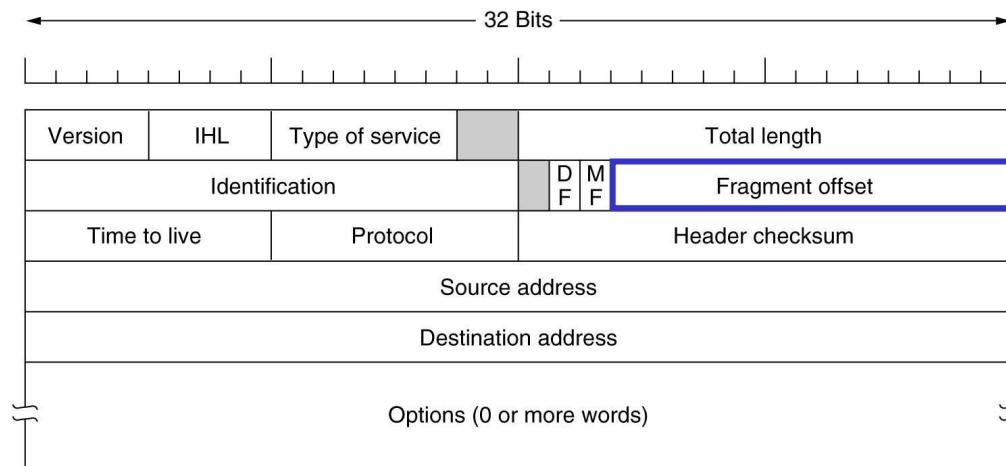
Bit More Fragment (MF)

- Todos os fragmentos de um pacote marcam este bit, exceto o último



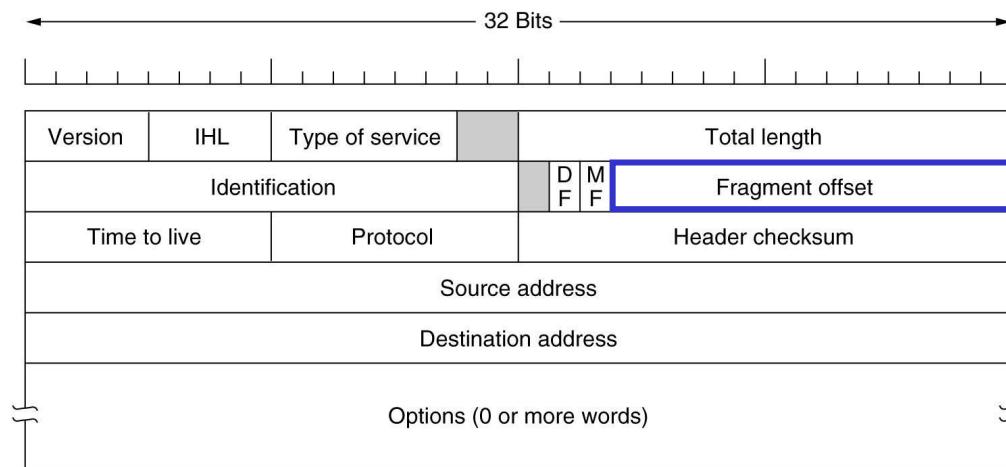
Campo *Fragment Offset* (13 bits)

- Indica onde o fragmento se encaixa dentro do pacote
- A carga útil de cada fragmento, exceto o último, deve ser múltiplo de 8



Campo *Fragment Offset* (13 bits)

- O número máximo de fragmentos é 8192, limitando o tamanho máximo de um pacote em 65.536 bytes



Exemplo para os Campos de Fragmentação

- Segmento de 3980 bytes em uma rede com MTU de 1500 bytes

T.length =4000	ID =x	MF =0	offset =0	
-------------------	----------	----------	--------------	--

Se um pacote:

$$\text{tamanho } 4000 = 3980 + 20 \\ \text{útil} \quad \text{cabeçalho}$$

Exemplo de um datagrama dividido em vários fragmentos

T.length =1500	ID =x	MF =1	offset =0	
-------------------	----------	----------	--------------	--

T.length =1500	ID =x	MF =1	offset =185	
-------------------	----------	----------	----------------	--

T.length =1040	ID =x	MF =0	offset =370	
-------------------	----------	----------	----------------	--

Como MTU = 1500 \Rightarrow três pacotes:

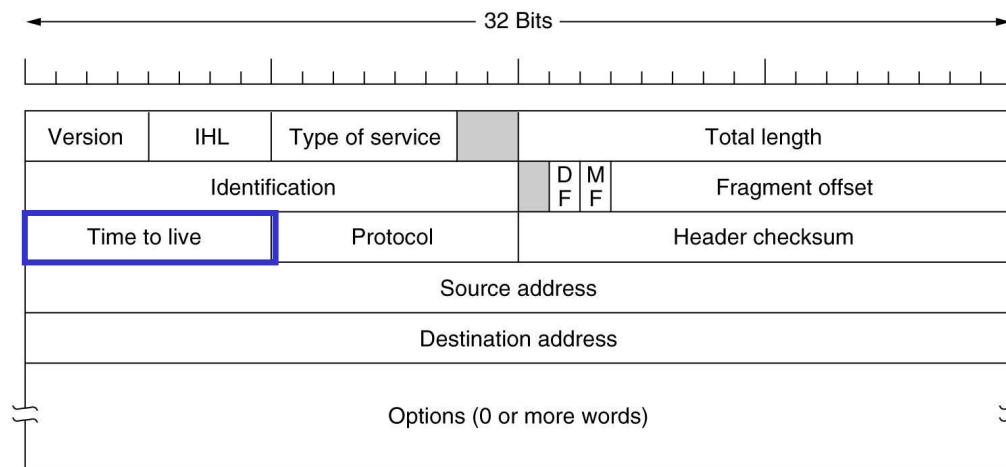
$$\text{tamanho } 4040 = 3980 + 20 \times 3 \\ \text{útil} \quad \text{cabeçalhos}$$

Consideração para os Campos de Fragmentação

- Fragmentação e remontagem são cargas extras sobre os roteadores (fazem a fragmentação) e *hosts* (fazem a remontagem)
 - Logo, a minimização das fragmentações é uma métrica desejável
 - O TCP e UDP limitam o tamanho de seus segmentos para minimizar as fragmentações do IP – na prática esse limite é de 556 bytes
 - Todos os protocolos suportados pelo IP têm MTU mínimo de 576 bytes

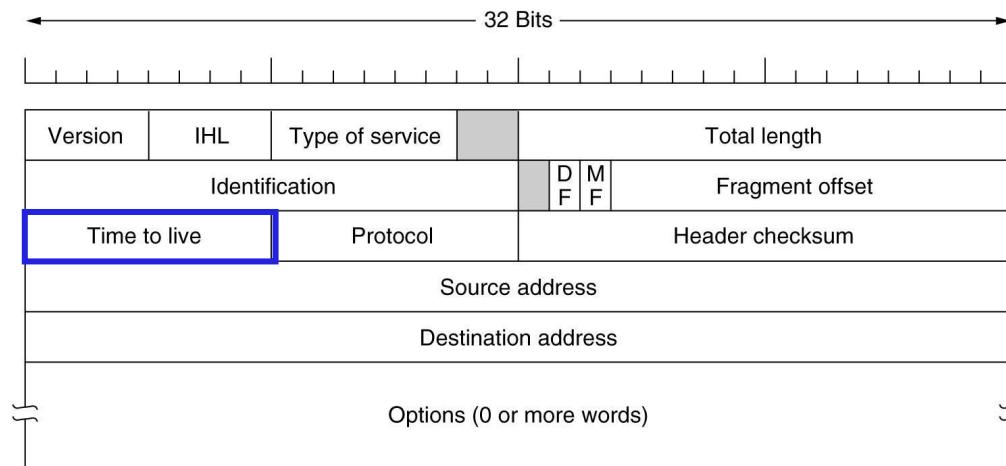
Campo Time To Live (TTL, 8 bits)

- Contador usado para limitar a vida útil dos pacotes
- Indica o número máximo de roteadores (*hops*) que o pacote pode passar



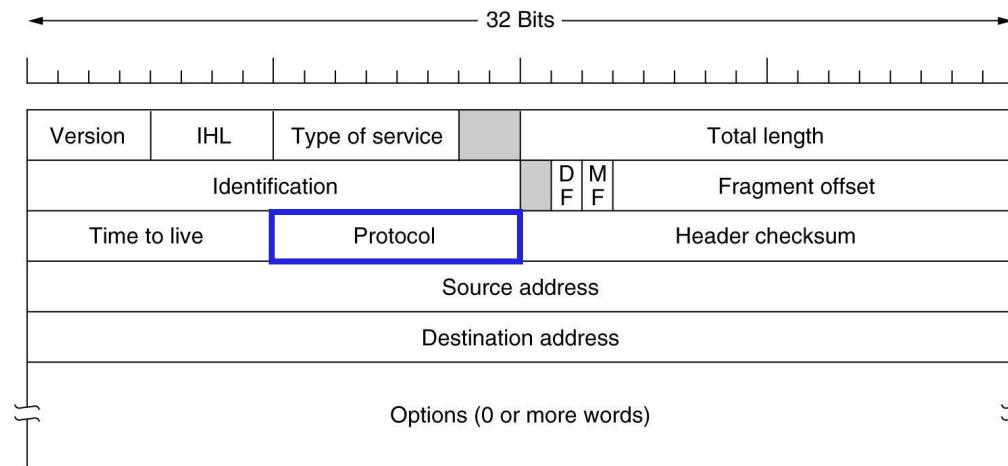
Campo Time To Live (TTL, 8 bits)

- Quando chega a zero, o pacote é descartado e um pacote de advertência é enviado para a origem



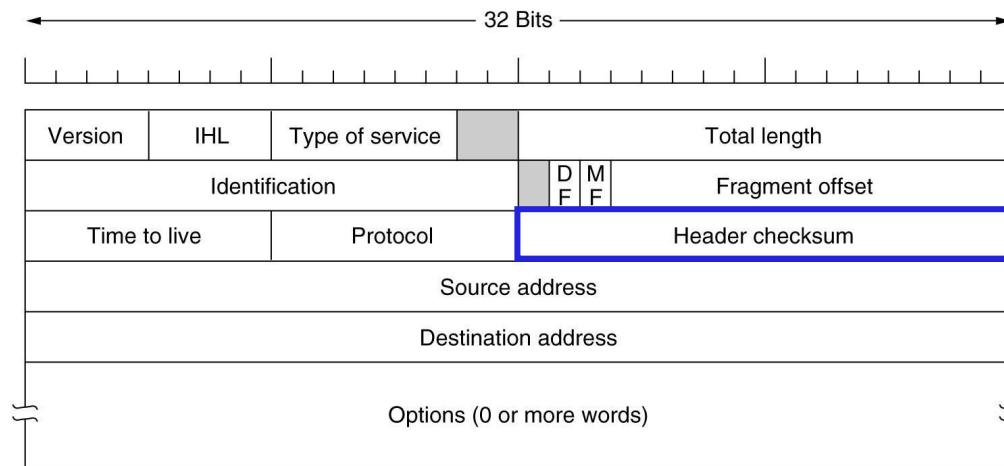
Campo Protocol (8 bits)

- Indica o protocolo de transporte para o qual deve-se passar o pacote (e.g., TCP e UDP)
- O RFC 1700 identifica os protocolos



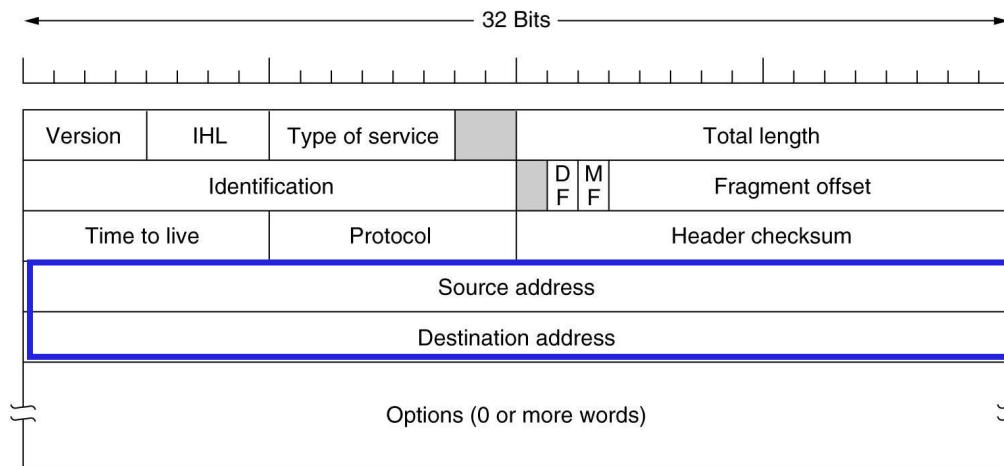
Campo Header Checksum (16 bits)

- Total de verificação do cabeçalho
- Recalculado em cada roteador, pois o TTL é decrementado a cada *hop* (salto)



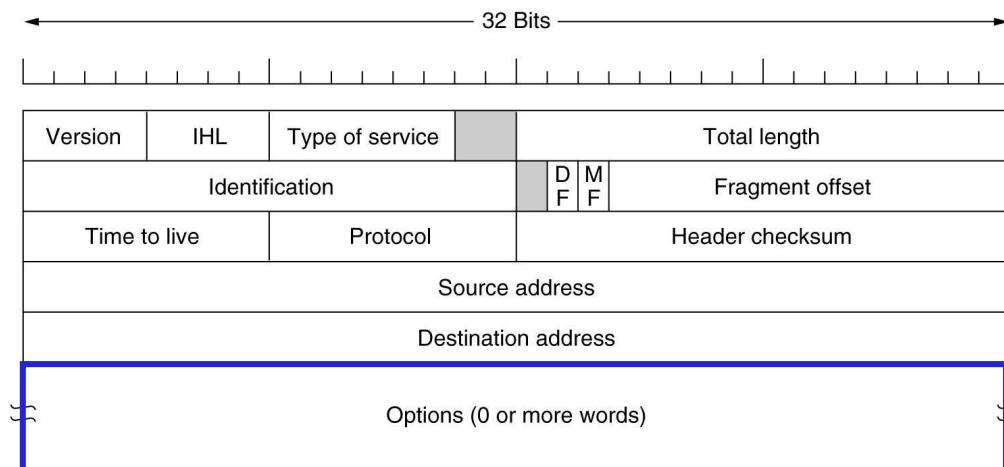
Campos Source e Destination Address (32 bits, cada)

- Endereços IP dos computadores origem e destino



Campo Options

- Forma de incluir informações não presentes na versão



Exercício (1)

- Suponha que o *host A* esteja conectado a um roteador R1, que R1 esteja conectado a outro roteador R2, e que R2 esteja conectado ao *host B*. Suponha que uma mensagem TCP contendo 900 bytes de dados e 20 bytes de cabeçalho TCP seja repassada ao código IP do *host A* para ser entregue a B. Mostre os campos *Total length*, *Identification*, DF, MF e *Fragment offset* do cabeçalho IP em cada pacote transmitido pelos três enlaces. Suponha que o enlace A-R1 possa admitir um tamanho máximo de quadro de 1.024 bytes, incluindo um cabeçalho de quadro de 14 bytes, que o enlace R1-R2 possa admitir um tamanho máximo de quadro de 512 bytes, incluindo um cabeçalho de quadro de 8 bytes, e que o enlace R2-B possa admitir um tamanho máximo de quadro de 512 bytes, incluindo um cabeçalho de quadro de 12 bytes

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - ***Internet Protocol v4 (IPv4)***
 - Protocolos de controle da Internet
 - Roteamento
 - ***Internet Protocol v6 (IPv6)***
- Introdução
 - Cabeçalho
 - **Endereçamento**
 - Roteamento IPv4
 - Caixa NAT

Endereço IPv4

- Número único de 32 bits que identifica cada máquina na Internet
- Na verdade, identifica cada interface de rede sendo que um *hosts* com duas interfaces têm um endereço IP para cada uma delas
- Teoricamente, a Internet tem $2^{32} = 4.294.967.296$ endereços
- Campos *Source* e *Destination Address* no cabeçalho dos pacotes IPv4
- Fundamental para o roteamento

Notação Decimal com Pontos

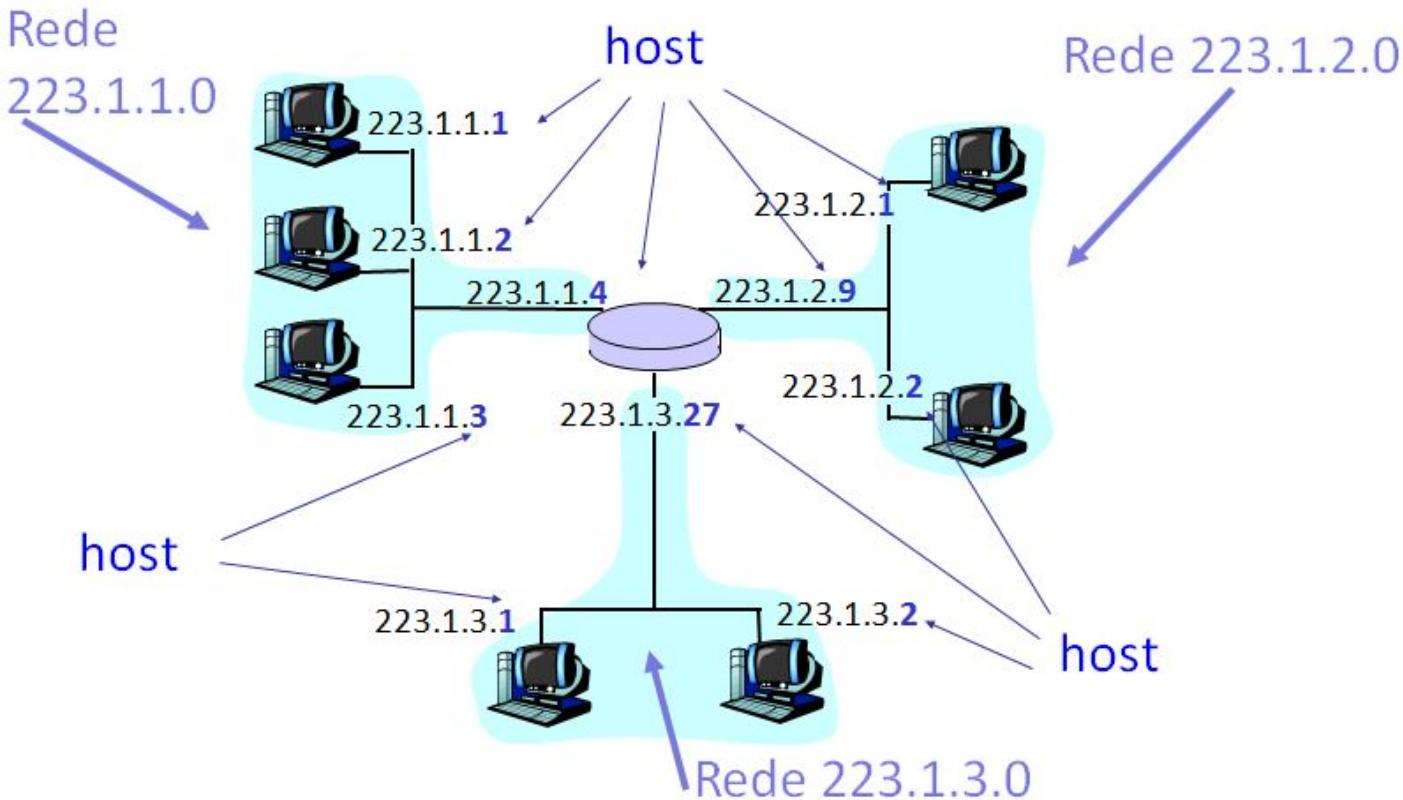
- Os 32 bits são divididos em 4 grupos de 8 bits (1 byte)
- Cada byte pode assumir $2^8 = 256$ valores, em decimal, um número entre 0 e 255
- Por exemplo: 128.208.2.151
- A representação hexadecimal do número acima seria 80D00297 e a binária, 10000000.11010000.00000010.10010111

Organização dos Bits

- A parte mais à esquerda (**prefixo**) identifica a rede que o *host* pertence (número de rede) e esse valor é definido globalmente
- A parte mais à direita (**sufixo**) identifica o *host* na rede e esse valor é definido localmente pelo projetista da rede

Exemplo com 24 Bits de Prefixo e 8, de Sufixo

Todos os *hosts* da rede têm o mesmo prefixo



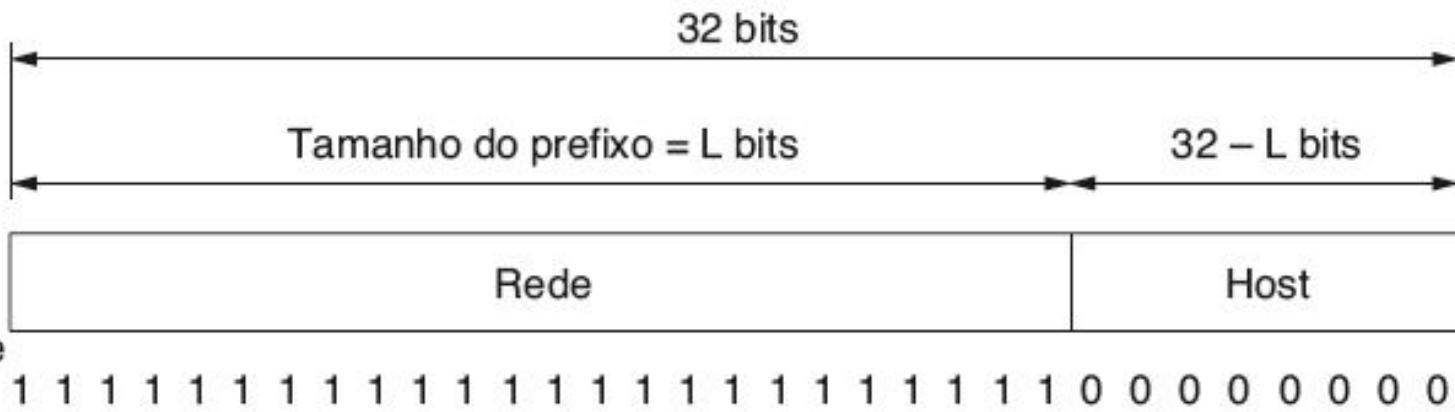
Problema

- Dado um endereço IPv4, não conseguimos deduzir seu prefixo de rede

E agora José?

Máscara de Rede

- Técnica para definir o tamanho do prefixo da rede
- Número com 32 bits onde os bits de rede tem valor um, e os de *host*, zero



Exemplos de Representação da Máscara

- Com barra:

/20

- Em binário:

11111111.11111111.11110000.00000000

- Em hexadecimal:

FF.FF.F0.00

- Em decimal:

255.255.240.0

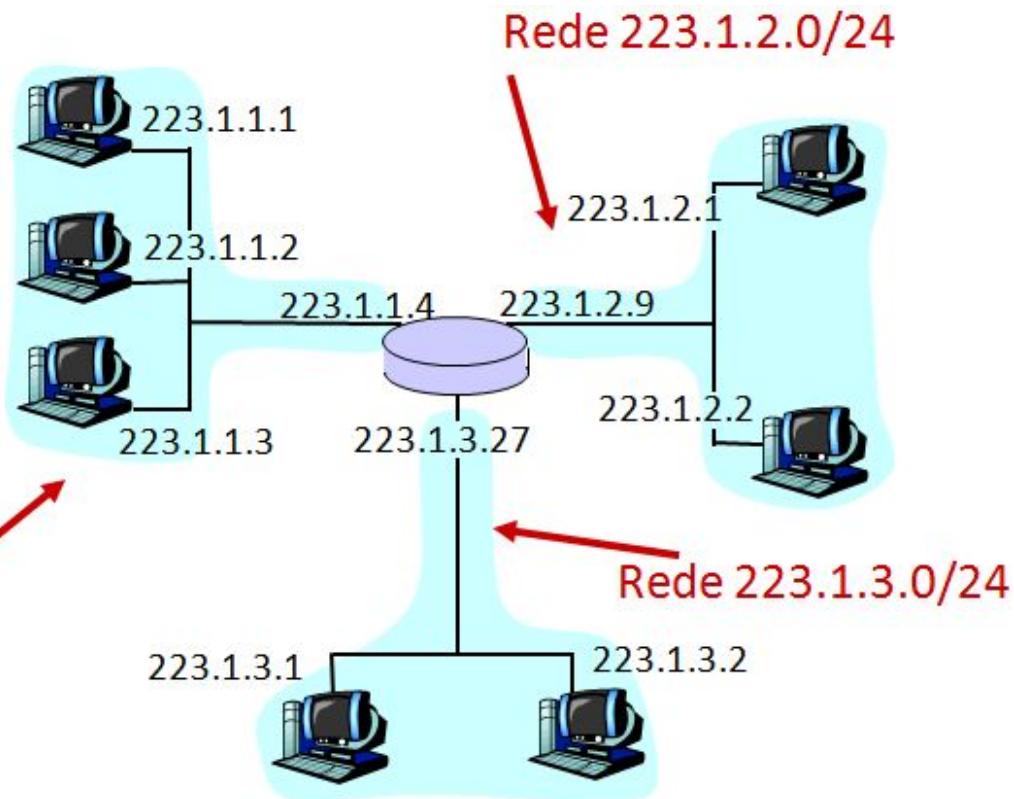
Importância da Máscara

AND (máscara, endereço IP da rede) = prefixo da rede

Máscaras no Exemplo Anterior

Número de bits que definem o endereço de rede

Rede 223.1.0/24 ou
223.1.0 com
máscara 255.255.255.0



Vantagem do Roteamento Hierárquico

- Em sua tabela de rotas, cada roteador pode armazenar somente os endereços de rede (prefixo) uma vez que todos os *hosts* de uma rede estão “próximos”
- Por exemplo, o tamanho da Internet é próximo de um bilhão de *hosts* e os roteadores precisam manter rotas de somente 300 mil redes

Desvantagem do Roteamento Hierárquico

- O endereço IP depende de onde ele está na rede (ao contrário do Ethernet)
- Desperdício de endereços

- *Internet Corporation for Assigned Names and Numbers*
- Corporação não lucrativa que controla os números de redes, evitando conflitos



www.icann.org

- Delegou uma parte dos endereços IP a diversas autoridades regionais que distribuíram endereços IP aos ISPs e a outras empresas
 - Na verdade, as empresas têm uma faixa de IPs
 - O que fazer quando uma empresa precisa de mais IPs?

Sub-redes

- Com o crescimento da Internet, tornou-se necessário a particionar as redes para uso interno, contudo, externamente, as sub-redes funcionam como uma única rede
- Todos os *hosts* de uma rede têm o mesmo endereço de rede
- A alocação de uma nova sub-rede não exige qualquer mudança externa

Exemplo: Sub-rede Universitária

- Suponha uma universidade que começou com o prefixo 128.208.0.0 e a máscara /16 para o uso do Departamento de Ciência da Computação (DCC)
 - Prefixo: **10000000.11010000.00000000.00000000** ou **128.208.0.0**
 - Máscara: /16 ou **11111111.11111111.00000000.00000000** ou **255.255.0.0**
 - IPs: 128.208.x.y ou 10000000.11010000.xxxxxxxx.xxxxxxxx

Exemplo: Sub-rede Universitária

- Um ano mais tarde, os departamentos de Eng. Elétrica (DEE) e o de Artes (DAR) decidiram entrar na rede
 - Quais deveriam ser os endereços desses departamentos?
 - Sair do bloco da universidade não seria uma solução interessante
 - /16 permite alocar mais de 60.000 hosts

Exemplo: Sub-rede Universitária

- A solução adotada foi alocar metade para o DCC, um quarto para o DEE, um oitavo para o DAR e o outro oitavo fica de reserva

Exemplo: Sub-rede Universitária

- A solução adotada foi alocar metade para o DCC, um quarto para o DEE, um oitavo para o DAR e o outro oitavo fica de reserva

DCC: 10000000 11010000 1 | xxxxxxxx xxxxxxxx

DEE: 10000000 11010000 00 | xxxxxx xxxxxxxx

DAR: 10000000 11010000 011 | xxxx xxxxxxxx

: 10000000 11010000 010 | xxxx xxxxxxxx

Exemplo: Sub-rede Universitária

- Assim, o prefixo e máscaras das sub-redes seriam:
 - DCC:
 - Prefixo : **10000000.11010000.10000000.00000000** ou 128.208.128.0
 - Máscara: /17 ou **11111111.11111111.10000000.00000000** ou 255.255.128.0
 - DEE:
 - Prefixo: **10000000.11010000.00000000.00000000** ou 128.208.0.0
 - Máscara: /18 ou **11111111.11111111.11000000.00000000** ou 255.255.192.0
 - DAR:
 - Prefixo: **10000000.11010000.01100000.00000000** ou 128.208.96.0
 - Máscara: /19 **11111111.11111111.11100000.00000** ou 255.255.224.0

Exemplo: Sub-rede Universitária

EE



128.208.0.0/18

Como funciona o
recebimento de pacotes?

CC



128.208.128.0/17

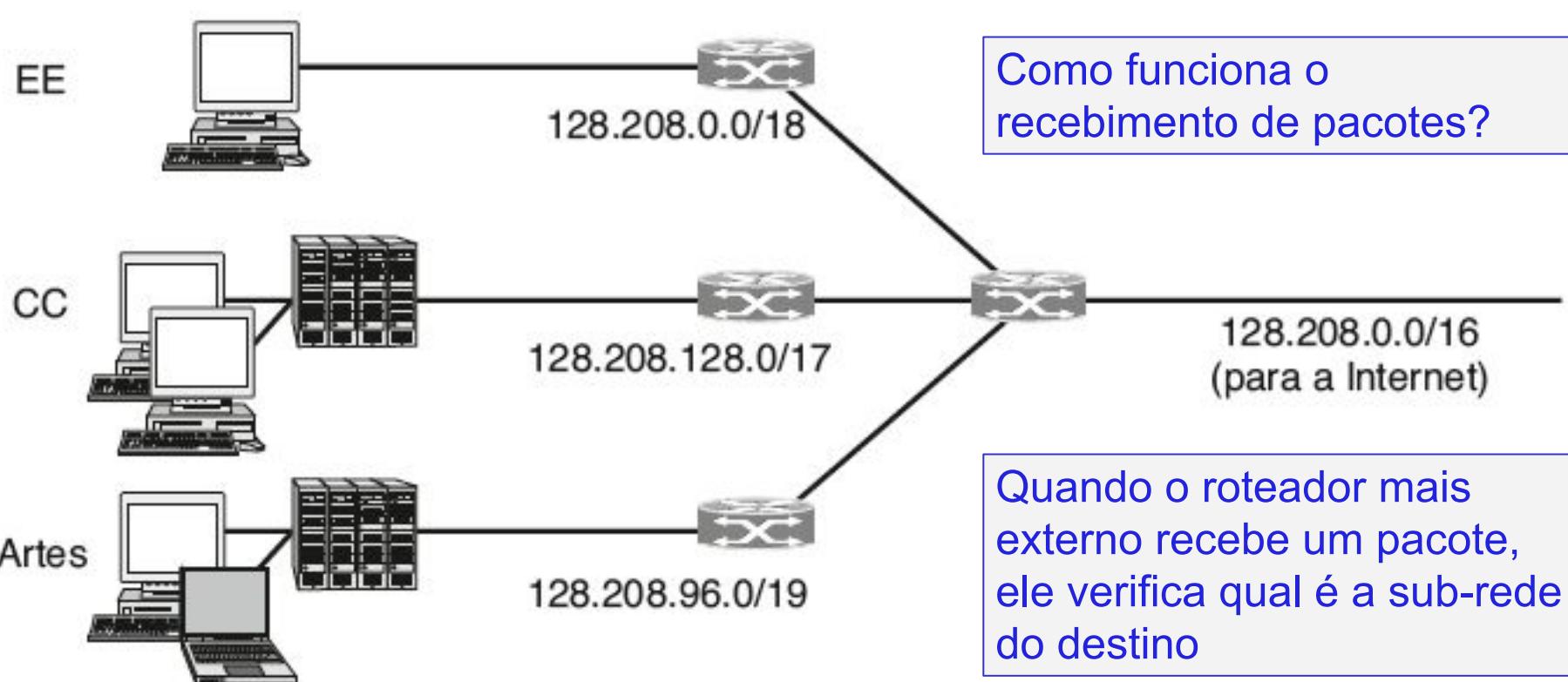
128.208.0.0/16
(para a Internet)

Artes



128.208.96.0/19

Exemplo: Sub-rede Universitária



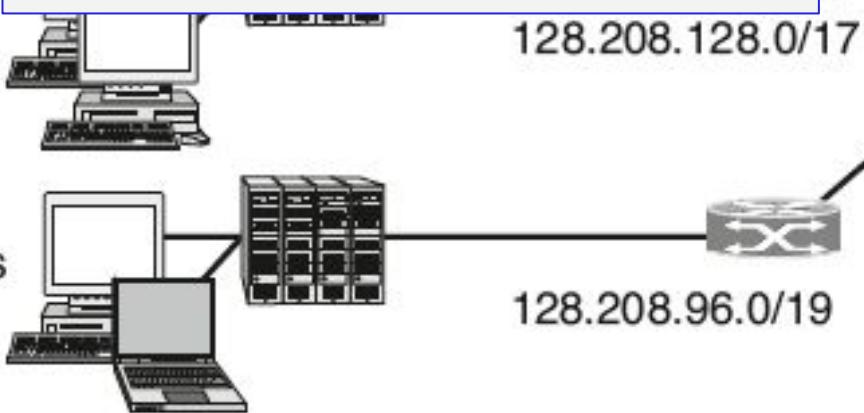
Exemplo: Sub-rede Universitária

EE

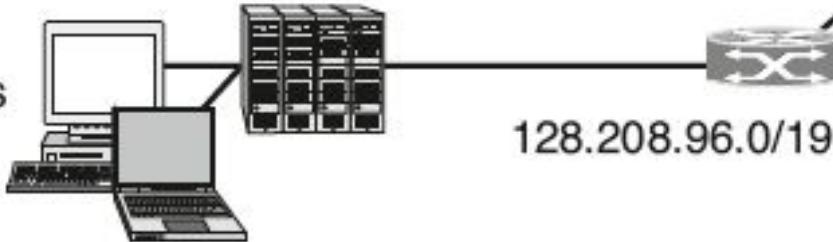


Como funciona o
recebimento de pacotes?

CC



Artes



128.208.0.0/16
(para a Internet)

Quando o roteador mais
externo recebe um pacote,
ele verifica qual é a sub-rede
do destino

Exemplo: Sub-rede Universitária

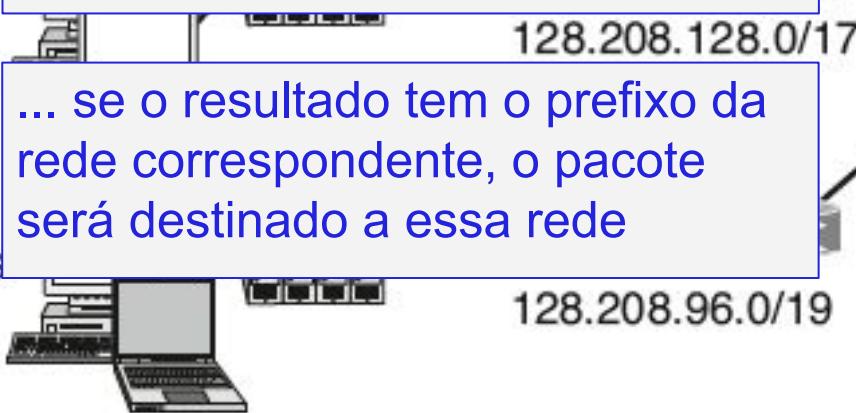
EE



CC

Nesse caso, o roteador faz um AND entre o endereço do destino e a máscara de cada sub-rede ...

Artes



Como funciona o
recebimento de pacotes?

... se o resultado tem o prefixo da rede correspondente, o pacote será destinado a essa rede

Quando o roteador mais externo recebe um pacote, ele verifica qual é a sub-rede do destino

Exercício Resolvido (1)

- Se o roteador mais externo receber um pacote para o IP 128.208.2.151, esse pacote será encaminhado para qual sub-rede?

Lembrete:

Prefixo DCC 128.208.128.0

Máscara DCC: /17 ou 255.255.128.0

Prefixo DEE: 128.208.0.0

Máscara DEE: /18 ou 255.255.192.0

Prefixo DAR: 128.208.96.0

Máscara DAR: /19 ou 255.255.224.0

Exercício Resolvido (1)

- Se o roteador mais externo receber um pacote para o IP 128.208.2.151, esse pacote será encaminhado para qual sub-rede?
 - DCC: 128.208.2.151 and 255.255.128.0 (17 bits) = 128.208.0.0 que é diferente do prefixo do DCC (128.208.128.0)

128.208.**2**.151
and 255.255.**128**.0

128.208.**0**.0
 - DEE: 128.208.2.151 and 255.255.192.0 (18 bits) = 128.208.0.0 que corresponde ao prefixo do DEE.

128.208.**2**.151
and 255.255.**192**.0

128.208.**0**.0

Exercício (2)

• E se o IP do destino for:

- a) 128.208.145.13
- b) 128.208.15.93
- c) 128.208.199.12

Lembrete:

Prefixo DCC 128.208.128.0
Máscara DCC: /17 ou 255.255.128.0

Prefixo DEE: 128.208.0.0
Máscara DEE: /18 ou 255.255.192.0

Prefixo DAR: 128.208.96.0
Máscara DAR: /19 ou 255.255.224.0

Exercício (3)

- Faça um método que receba um IP (String), uma máscara de sub-rede (String) e um prefixo de rede (String) e retorne se o pacote pertence à sub-rede em questão?

Endereçamento na Internet

- Usa o conceito de sub-redes, permitindo que um roteador trate um IP com uma máscara /20 enquanto outro roteador trate o mesmo IP como uma /22
- Chamada de *Classless Inter-Domain Routing* (CIDIR) ou endereçamento sem classes
- Utilizada desde 1993
- Definida nos RFCs 1518 e 1519 e atualizada no RFC 4632

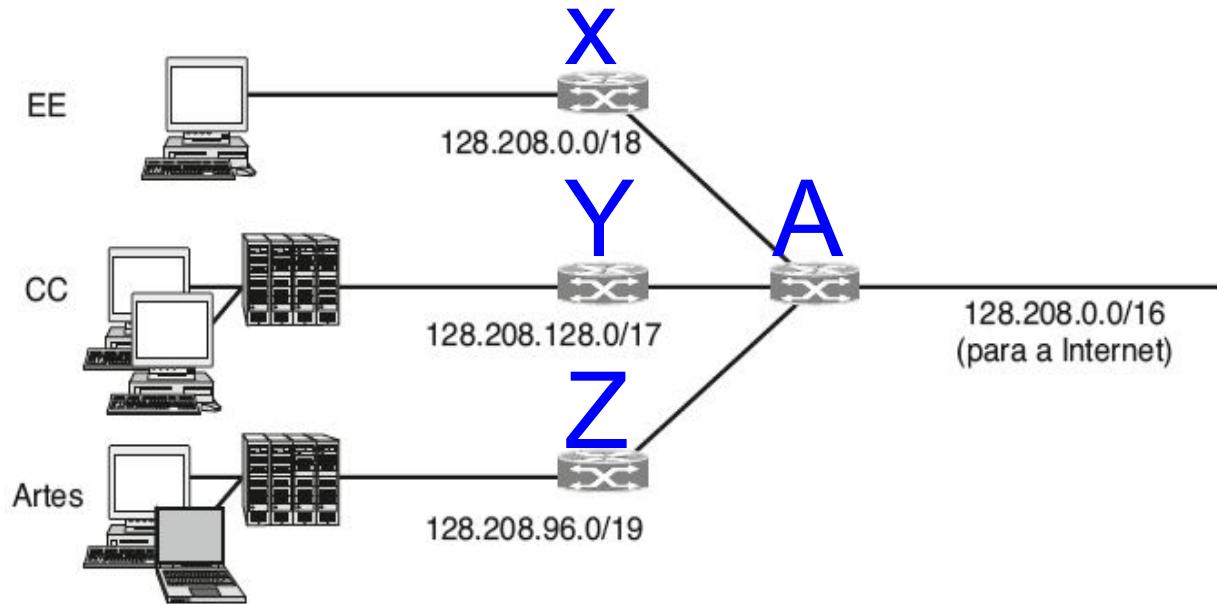
Endereçamento na Internet

- Usa o conceito de sub-redes, permitindo que um roteador trate um IP com uma máscara /20 enquanto outro roteador trate o mesmo IP como uma /22
- Chamada de *Classless Inter-Domain Routing* (CIDIR) ou endereçamento sem classes
- Utilizada desde 1993
- Definida nos RFCs 1518 e 1519 e atualizada no RFC 4632

Funcionamento baseado
em sub-redes

Agregação de Rotas

- Roteadores externos conhecem apenas a sub-rede de A com prefixo 128.208.0.0 e máscara /16, as informações sobre X, Y e Z pertencem ao roteador A



Agregação de Rotas

- Permite uma redução significativa no tamanho das tabelas de roteamento
- Tal redução é fundamental, pois os roteadores nos ISPs e backbones no meio da Internet (roteadores de núcleo ou zona de livre padrão) têm que conhecer um caminho para chegar em cada rede
- Faz com que não saibamos o número de redes totais conectadas à Internet, contudo, estima-se um milhão de redes

Considerações sobre as Tabelas de Rotas

- Um roteador faz uma pesquisa para cada pacote que ele encaminha
- Roteadores de núcleo podem encaminhar até milhões de pacotes por segundo, exigindo uma atenção especial dos fabricantes desses roteadores
- Os algoritmos de roteamento também podem exigir métricas especiais para cada caminho, aumentando o consumo de memória em cada roteador
- Soluções mais hierárquicas poderiam ser implantadas, contudo, isso demandaria IPs com mais de 32 bits

Exemplo de Endereçamento com Agregação de IPs

- Considere que temos 8.192 endereços disponíveis a partir do 194.24.0.0 com máscara /19 e que três universidades solicitam IPs conforme mostrado abaixo

- Universidade de Cambridge solicita 2.048 endereços ($\frac{1}{4}$)
- Universidade de Oxford solicita 4.096 endereços ($\frac{1}{2}$)
- Universidade de Edinburgh solicita 1.024 endereços ($\frac{1}{8}$)

Observações

$$\Rightarrow 2^{13} = 8.192$$

$$\Rightarrow 13 + 19 = 32$$

\Rightarrow Restam 1.024 IPs livres para uso futuro ($\frac{1}{8}$)

Exemplo de Endereçamento com Agregação de IPs

- Atendendo ao pedido das três Universidades, temos a seguinte organização:

Universidade	Primeiro endereço	Último endereço	Quantos	Prefixo
Cambridge	194.24.0.0	194.24.7.255	2.048	194.24.0.0/21
Edimburgo	194.24.8.0	194.24.11.255	1.024	194.24.8.0/22
(Disponível)	194.24.12.0	194.24.15.255	1.024	194.24.12.0/22
Oxford	194.24.16.0	194.24.31.255	4.096	194.24.16.0/20

Prefixos em binário

Cambridge ⇒ 11000010.00011000.000**00**000.00000000

Edimburgo ⇒ 11000010.00011000.000**01**000.00000000

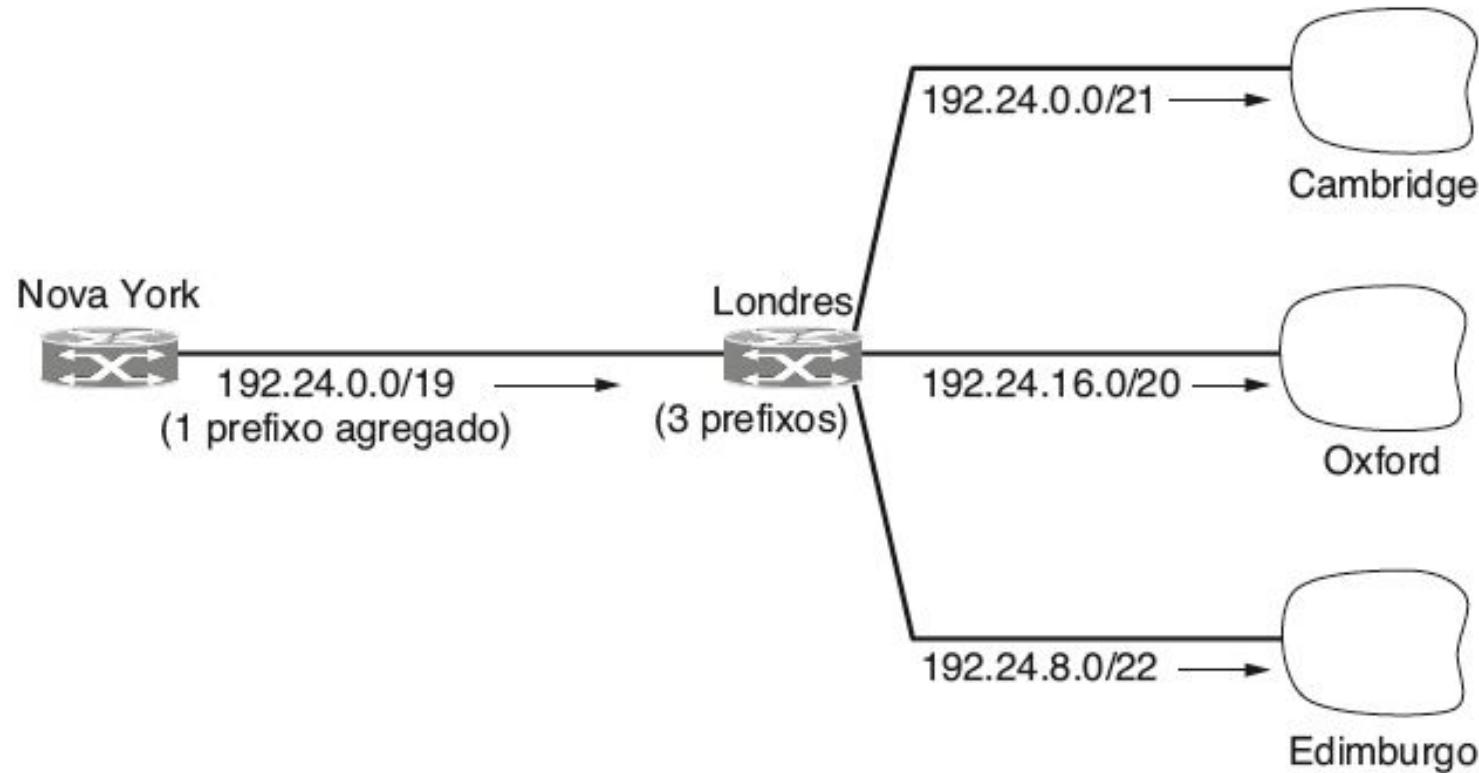
Disponível ⇒ 11000010.00011000.000**01**100.00000000

Oxford ⇒ 11000010.00011000.000**1**0000.00000000

Exemplo de Endereçamento com Agregação de IPs

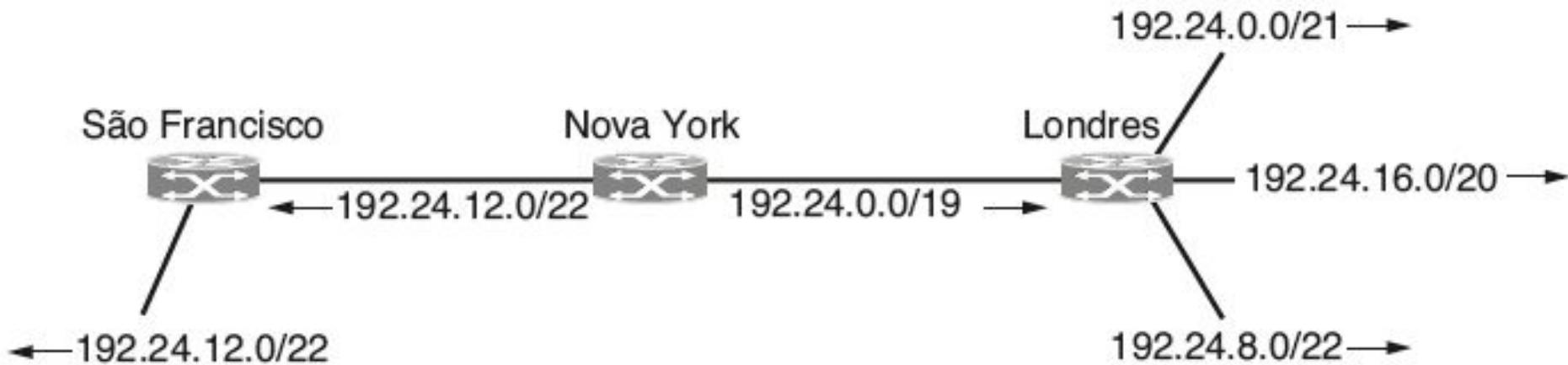
- Todos os roteadores da zona livre-padrão são informados sobre os endereços IPs das três redes
- Um roteador em Londres (próximo às três Universidade), possivelmente, armazenará uma interface de saída diferente para cada uma das Universidades
- Por outro lado, um roteador em Nova York (distante das Universidades), possivelmente, armazenará a mesma interface de saída para as Universidades

Exemplo de Endereçamento com Agregação de IPs



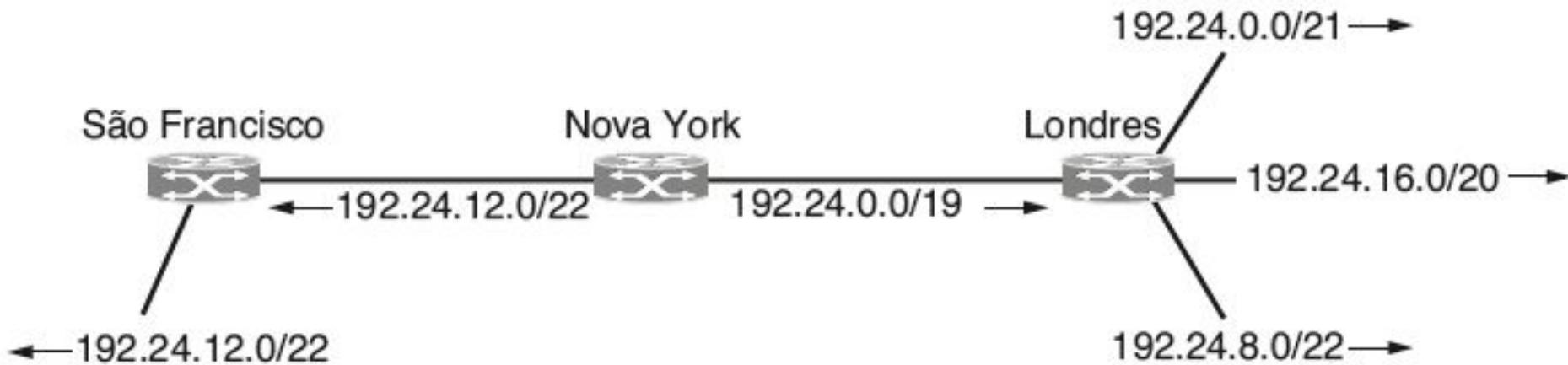
Outro Exemplo com Agregação de IPs

- Suponha que nossa faixa disponível de IPs foi alocada para uma empresa em São Francisco (EUA), como o roteador Nova York saberá para quem enviar dados?



Outro Exemplo com Agregação de IPs

- Quando tivermos uma sobreposição de prefixos, o roteador decide pelo **prefixo com maior casamento**



Exercício Resolvido (2)

- Quando o roteador de Nova York receber um pacote para o IP 192.24.13.13, tal pacote será encaminhado para qual roteador? Justifique.

Exercício Resolvido (2)

- Quando o roteador de Nova York receber um pacote para o IP 192.24.13.13, tal pacote será encaminhado para qual roteador? Justifique.
 - Londres: 192.24.13.13 and 255.255.224.0 (/19) = 192.24.0.0 que corresponde ao prefixo de Londres
 - 192.024.013.013
and 255.255.224.000

192.024.000.000
 - 0000.1101₂ (13₁₀)
and 1110.0000₂ (224₁₀)

0000.0000₂ (0₁₀)
 - São Francisco: 192.124.13.13 and 255.255.252.0 (/22) = 192.24.12.0 que corresponde ao prefixo de S.F.
 - 192.024.013.013
and 255.255.252.000

192.024.012.000
 - 0000.1101₂ (13₁₀)
and 1111.1100₂ (252₁₀)

0000.1100₂ (12₁₀)
 - Maior prefixo (22 > 19) \Rightarrow São Francisco

Exercício Resolvido (3)

- Dada a faixa de endereços de IPs de uma empresa, complete a tabela abaixo

Sub-rede	Prefixo/Máscara	Primeiro End.	Último End.	Número Ends.
0		130.50.0.0	130.50.3.255	
1		130.50.4.0	130.50.7.255	
2		130.50.8.0	130.50.11.255	
3		130.50.12.0	130.50.15.255	
REDE TODA				

Exercício Resolvido (3)

- Dada a faixa de endereços de IPs de uma empresa, complete a tabela abaixo

Sub-rede	Prefixo/Máscara	Primeiro End.	Último End.	Número Ends.
0		130.50.0.0	130.50.3.255	
1		130.50.4.0	130.50.7.255	
2		130.50.8.0	130.50.11.255	
3		130.50.12.0	130.50.15.255	
REDE TODA		130.50.0.0	130.50.15.255	

Exercício Resolvido (3)

- Antes de completar a tabela, vamos ver os endereços em binário

- Sub-rede 0:

130.50.0.0: 10000010.00110010 0000|00|00.00000001 a
130.50.3.255: 10000010.00110010 0000|00|11 11111110

Todas têm 2^{10} IPs

- Sub-rede 1:

130.50.4.0: 10000010.00110010 0000|01|00.00000001 a
130.50.7.255: 10000010.00110010 0000|01|11 11111110

/20: máscara da rede

- Sub-rede 2:

130.50.8.0: 10000010.00110010 0000|10|00.00000001 a
130.50.11.255: 10000010.00110010 0000|10|11 11111110

/22: máscara sub-redes

- Sub-rede 3:

130.50.12.0: 10000010.00110010 0000|11|00.00000001 a
130.50.15.255: 10000010.00110010 0000|11|11.11111110

0, 4, 8 e 12: terceiro octeto do prefixo das sub-redes

Exercício Resolvido (3)

- Dada a faixa de endereços de IPs de uma empresa, complete a tabela abaixo

Sub-rede	Prefixo/Máscara	Primeiro End.	Último End.	Número Ends.
0	130.50.0.0 / 22	130.50.0.0	130.50.3.255	2^{10}
1	130.50.4.0 / 22	130.50.4.0	130.50.7.255	2^{10}
2	130.50.8.0 / 22	130.50.8.0	130.50.11.255	2^{10}
3	130.50.12.0 / 22	130.50.12.0	130.50.15.255	2^{10}
REDE TODA	130.50.0.0 / 20	130.50.0.0	130.50.15.255	2^{12}

Exercício (4)

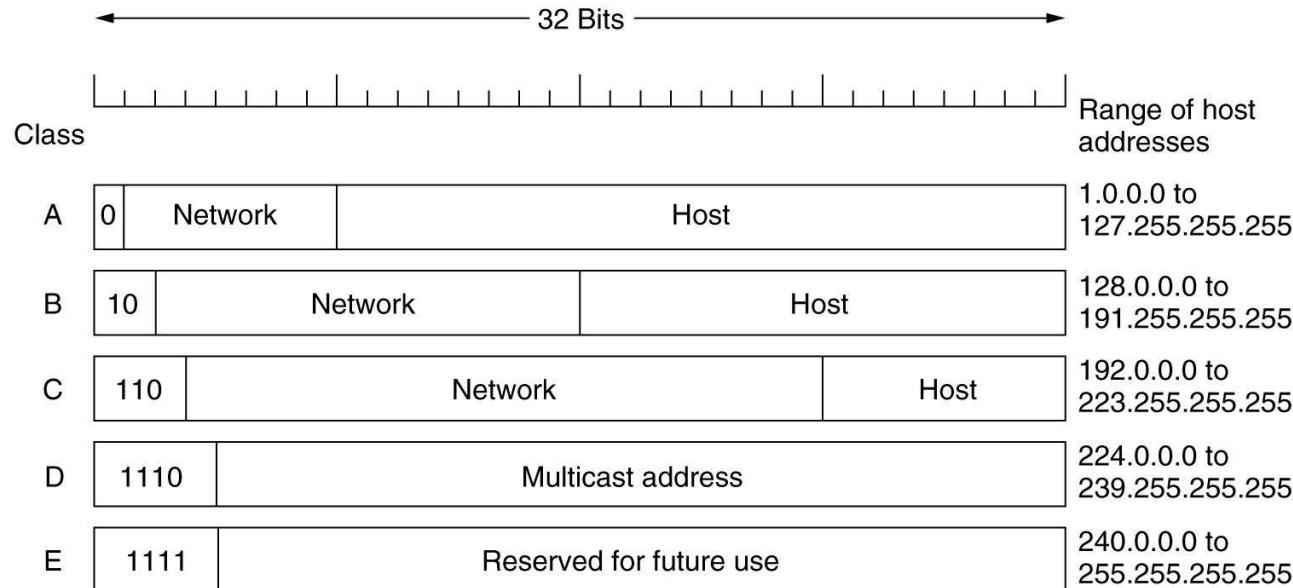
- Um ISP possui o seguinte bloco de endereços: 150.164.192.0/18. Ele deseja dividir esse espaço de endereçamento igualmente entre 6 organizações. Informe a quantidade de endereços IP cada organização terá, o endereço inicial, final e a máscara de cada organização.

Exercício (5)

- Um grande número de endereços IP consecutivos está disponível a partir de 198.16.0.0. Suponha que quatro organizações, A, B, C e D, solicitem 4.000, 2.000, 4.000 e 8.000 endereços, respectivamente, e nessa ordem. Para cada uma delas, forneça o primeiro endereço IP atribuído, o último endereço IP atribuído e a máscara na notação w.x.y.z/s.

Endereçamento com Classes Especiais

- A arquitetura de endereçamento original da Internet definiu classes de endereços (hoje, considera-se o CIDIR)



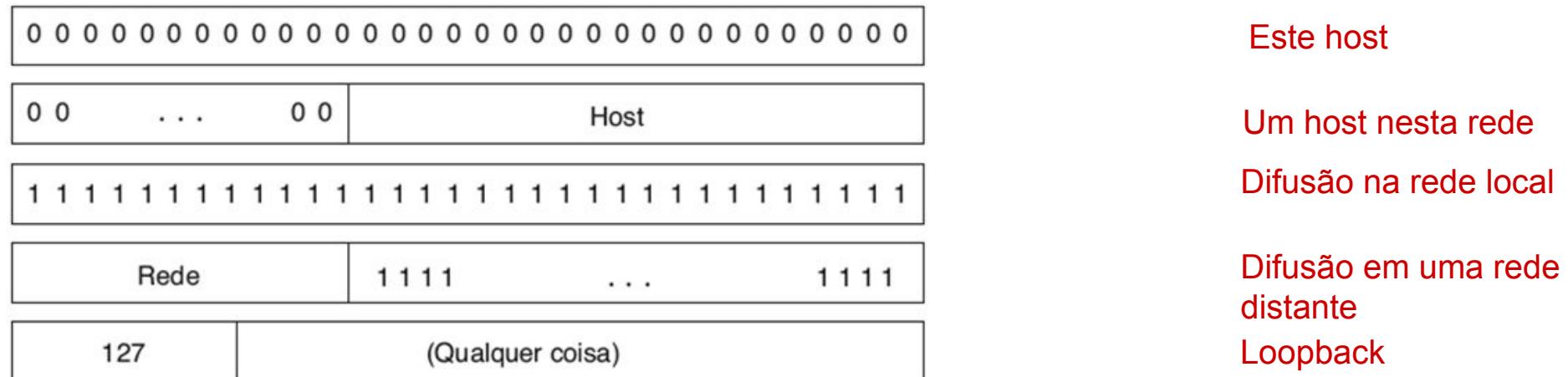
Endereçamento com Classes Especiais

- A arquitetura de endereçamento original da Internet definiu classes de endereços (hoje, considera-se o CIDIR)

Classe	Nº de Bits no Prefixo	Nº Máximo de Redes	Nº de Bits no Sufixo	Nº Máximo de Hosts por Rede
A	7	128	24	16.777.216
B	14	16.384	16	65.536
C	21	2.097.152	8	256

Endereços Especiais

- A arquitetura de endereçamento original da Internet definiu classes de endereços (hoje, considera-se o CIDIR)



Endereços Especiais

- 0.0.0.0 - usado pelos hosts quando eles estão sendo inicializados
- Endereços IP que têm 0 como número de rede se referem à rede atual
- 127.x.y.z - reservados para teste de *loopback*
 - Pacotes enviados para esse endereço não são transmitidos, eles são processados localmente e tratados como pacotes de entrada
 - Desperdício de 16.777.216 endereços IP

Exercício (6)

- Suponha que, em vez de serem utilizados 16 bits na parte de rede de um endereço da classe B, tenham sido usados 20 bits. Nesse caso, quantas redes da classe B existiriam?

Exercício (7)

- A máscara de sub-rede de uma rede na Internet é 255.255.240.0. Qual é o número máximo de hosts que ela pode manipular?

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - ***Internet Protocol v4 (IPv4)***
 - Protocolos de controle da Internet
 - Roteamento
 - ***Internet Protocol v6 (IPv6)***
- Introdução
 - Cabeçalho
 - Endereçamento
 - **Roteamento IPv4**
 - Caixa NAT

Tabela de Roteamento

- Disponível em cada roteador
- Inicializada quando o roteador é ligado e atualizada quando a topologia muda ou temos alguma falha de hardware
- Cada entrada especifica um destino e o próximo nó para alcançar esse destino
- Cada roteador mantém somente entradas para outras redes e *hosts* locais

Algoritmo para Recebimento de Pacote IP

início

 se destino pertence à rede local então

 | enviar o pacote diretamente para o destino

 senão para cada sub-rede cadastrada na tabela de roteamento faça

 | faça um and entre o IP do destino e a máscara da sub-rede

 se resultado igual ao prefixo da sub-rede então

 | enviar o pacote para o próximo nó referente a sub-rede

 fim se

 fim para

fim se

 se pacote não enviado então

 | enviar o pacote para o *default gateway* (possui tabelas maiores)

fim se

fim

Destino x Próximo Nô

- O destino é aquele para quem deve ser entregue o pacote
- O próximo nó é aquele para quem o roteador deve encaminhar o pacote. Esse endereço não aparece no pacote

Exemplo de Roteamento de Pacotes IP

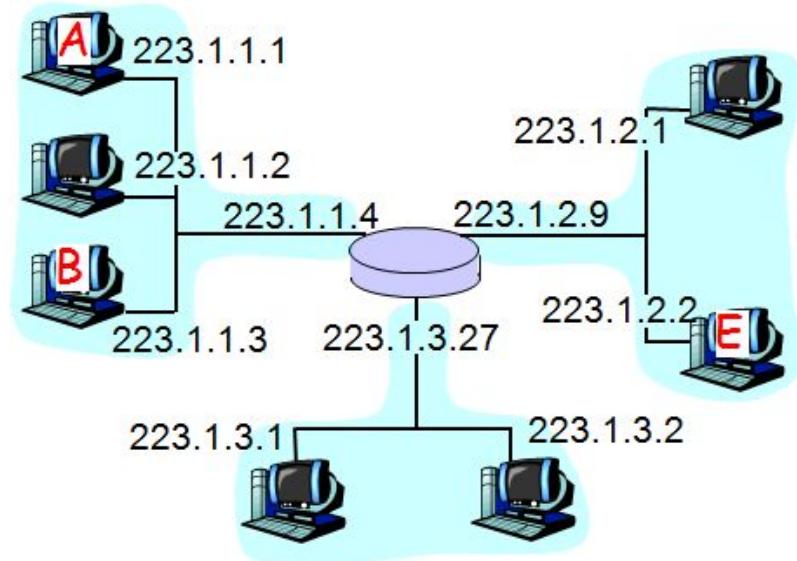
- A deseja enviar mensagens

- pacote IP:

outros campos	endereço IP origem	endereço IP destino	dados
---------------	--------------------	---------------------	-------

- Os endereços da origem e destino

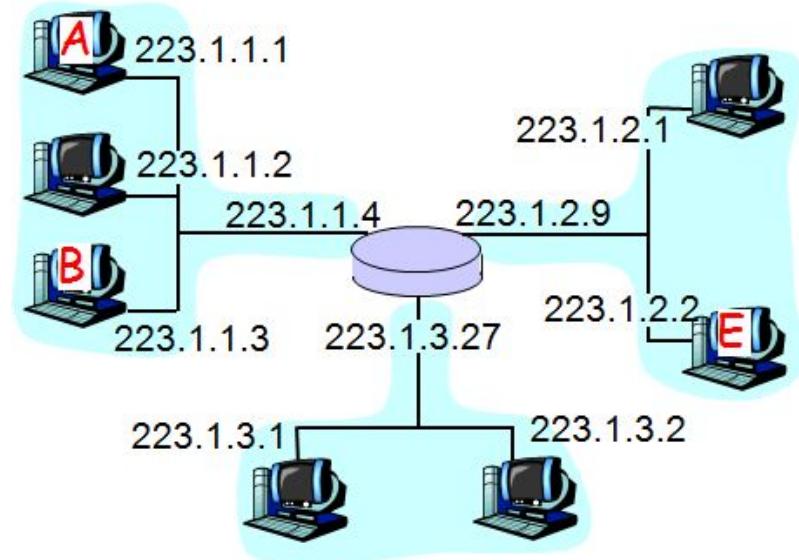
não mudam durante o roteamento



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para B

- pacote IP:



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para B

- pacote IP:



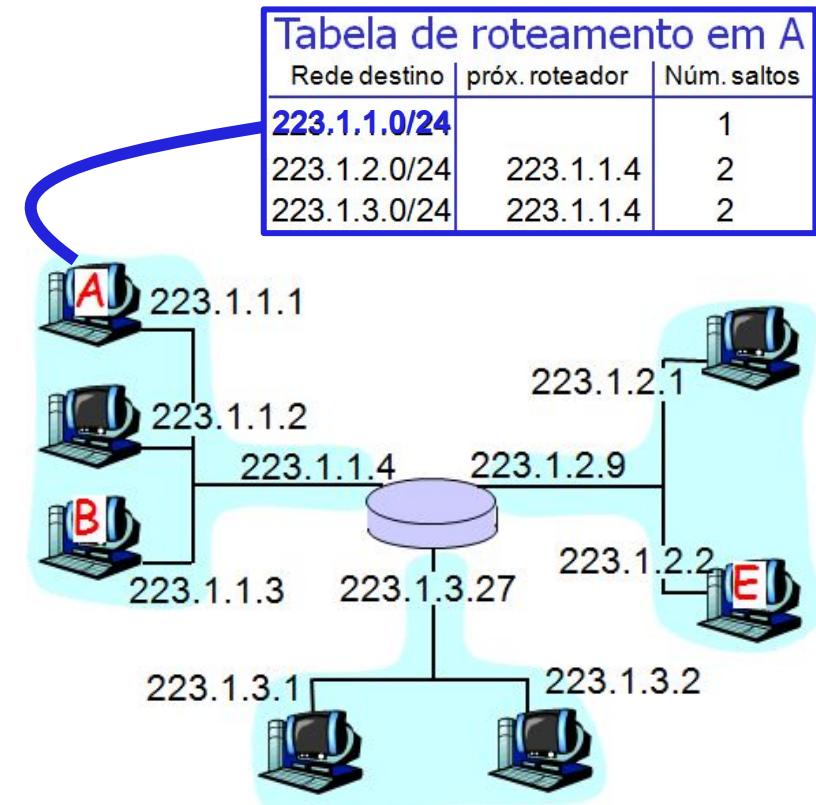
1º) Verificar se o destino pertence à rede local

$$223.1.1.3 \text{ and } 255.255.255.0 = 223.1.1.0$$

IP destino

máscara local
/24

resultado igual
ao prefixo local



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para B

- pacote IP:



1º) Verificar se o destino pertence à rede local

$$223.1.1.3 \text{ and } 255.255.255.0 = 223.1.1.0$$

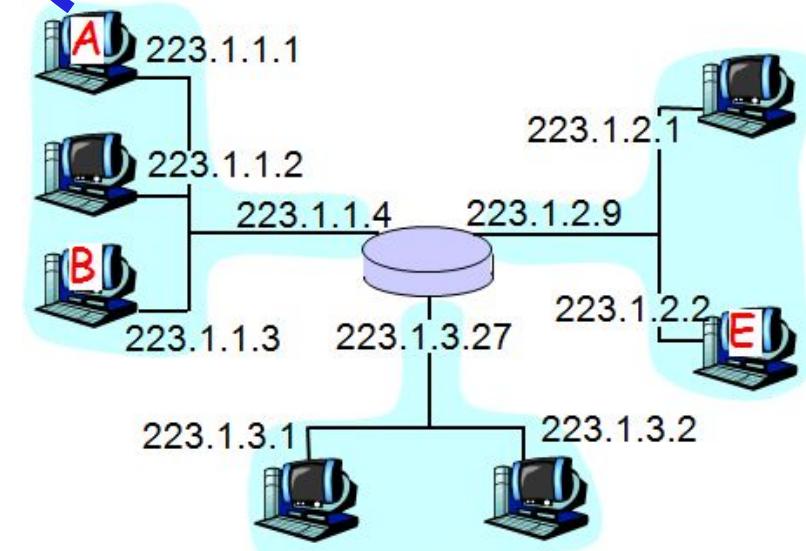
IP destino

máscara local
/24

resultado igual
ao prefixo local

2º) Como é verdadeiro, o pacote é enviado para a camada de enlace

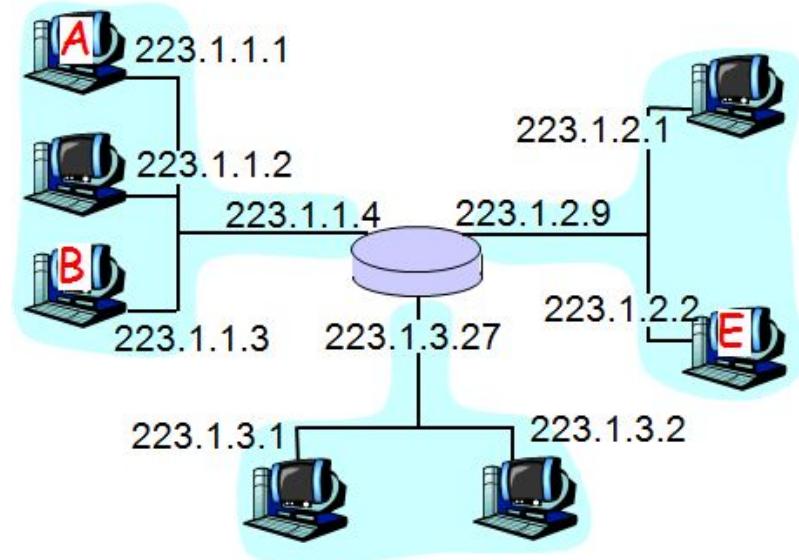
Tabela de roteamento em A		
Rede destino	próx. roteador	N. saltos
223.1.1.0/24		1
223.1.2.0/24	223.1.1.4	2
223.1.3.0/24	223.1.1.4	2



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para E

- pacote IP:



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para E

- pacote IP:



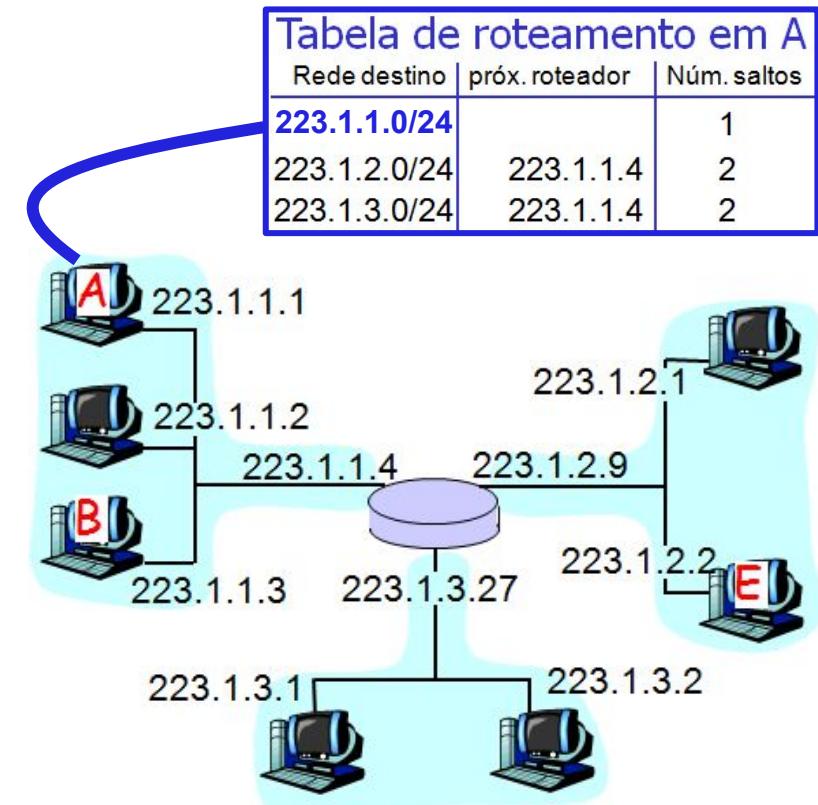
1º) Verificar se o destino pertence à rede local

$$223.1.2.2 \text{ and } 255.255.255.0 = 223.1.2.0$$

IP destino

máscara local
/24

resultado diferente
do prefixo local



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para E

- pacote IP:



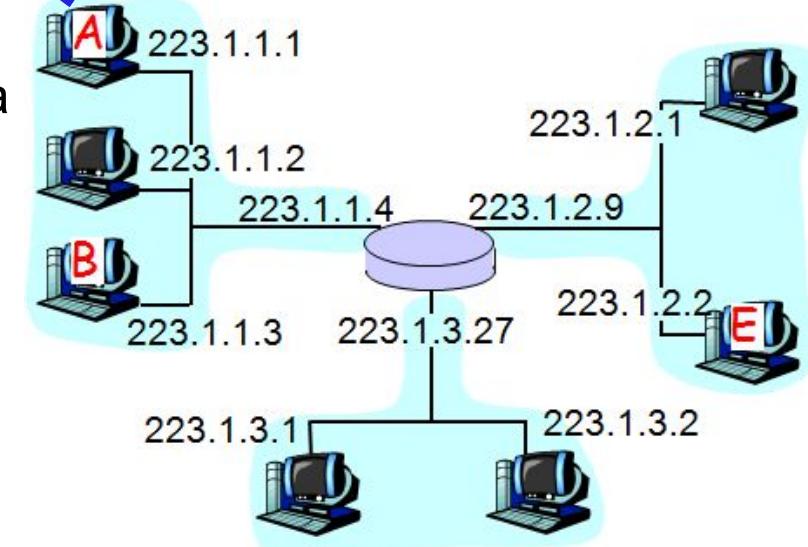
2º) Verificar se o destino pertence a 2ª entrada

$$\text{IP destino} \quad \text{máscara 2a entrada} \quad \text{resultado ao da 2a entrada}$$

$$223.1.2.2 \text{ and } 255.255.255.0 = 223.1.2.0$$

$$/24$$

Rede destino	próx. roteador	N. saltos
223.1.1.0/24		1
223.1.2.0/24	223.1.1.4	2
223.1.3.0/24	223.1.1.4	2



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para E

- pacote IP:



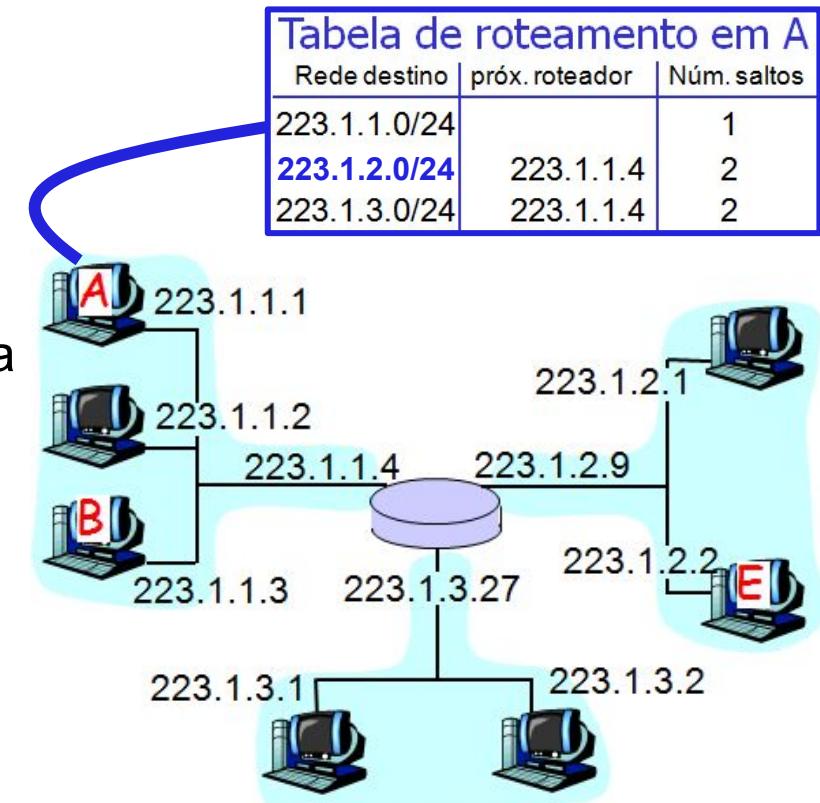
2º) Verificar se o destino pertence a 2ª entrada

$$\text{IP destino} \quad \text{máscara 2a entrada} \quad \text{resultado ao da 2a entrada}$$

$$223.1.2.2 \text{ and } 255.255.255.0 = 223.1.2.0$$

/24

3º) Enviar o pacote para o 223.1.1.4



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para E

- pacote IP:

outros campos	223.1.1.1	223.1.2.2	dados
---------------	-----------	-----------	-------

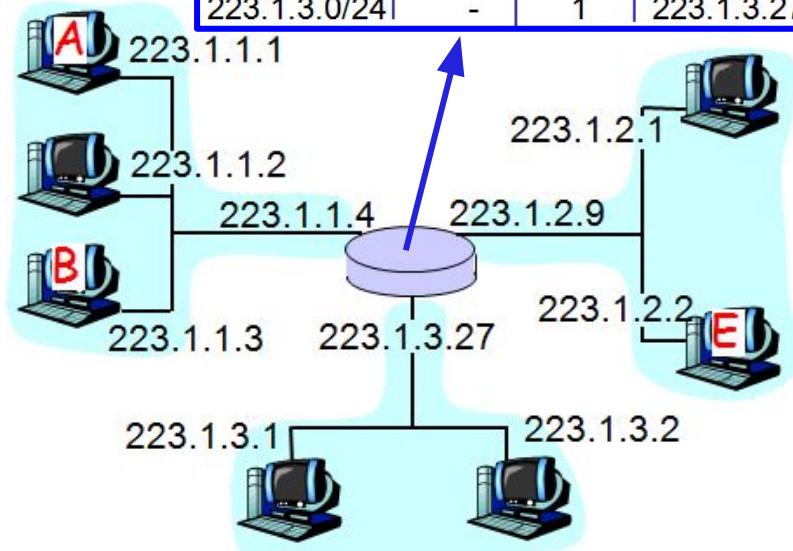
4º) O roteador verifica a 2ª próxima sub-rede

$$\text{IP destino } 223.1.2.2 \text{ and } 255.255.255.0 = 223.1.2.0$$

máscara 2a entrada /24

resultado ao da 2a entrada

Tabela do roteador			
Rede destino	Próx. roteador	Núm. saltos	Endereço Interface
223.1.1.0/24	-	1	223.1.1.4
223.1.2.0/24	-	1	223.1.2.9
223.1.3.0/24	-	1	223.1.3.27



Exemplo de Roteamento de Pacotes IP

- A deseja enviar uma mensagem para E

- pacote IP:

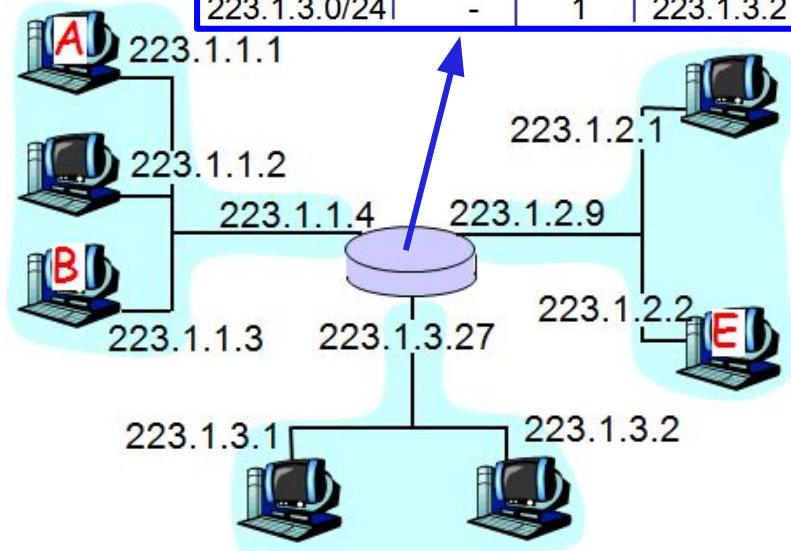
outros campos	223.1.1.1	223.1.2.2	dados
---------------	-----------	-----------	-------

4º) O roteador verifica a 2ª próxima sub-rede

$$\text{IP destino } 223.1.2.2 \text{ and máscara } 255.255.255.0 = \text{resultado ao da 2a entrada}$$

máscara 2a entrada /24

Tabela do roteador			
Rede destino	Próx. roteador	Núm. saltos	Endereço Interface
223.1.1.0/24	-	1	223.1.1.4
223.1.2.0/24	-	1	223.1.2.9
223.1.3.0/24	-	1	223.1.3.27



5º) Enviar o pacote para a interface 223.1.2.9 que pertence à rede local do destino (essa envia para o destino via sua rede local)

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - ***Internet Protocol v4 (IPv4)***
 - Protocolos de controle da Internet
 - Roteamento
 - ***Internet Protocol v6 (IPv6)***
- Introdução
 - Cabeçalho
 - Endereçamento
 - Roteamento IPv4
 - **Caixa NAT**

Escassez de Endereços IPv4

- Os IPv4 estão praticamente esgotados
- Solução: *Network Address Translation* (NAT), descrita no RFC 1631 e atualizada nas RFCs 2993 e 3022

Ideia Básica da NAT

- Cada empresa tem um único IP (ou um intervalo) para comunicação na Internet
- Internamente, cada computador terá um IP exclusivo (privado, interno, falso, *fake*, inválido) dentro de uma faixa pré-definida
- Quando um pacote sai da empresa, ocorre uma conversão de endereços

Intervalos de IPs Privados

- 10.0.0.0 a 10.255.255.255/8
- 172.16.0.0 a 172.31.255.255/12
- 192.168.0.0 a 192.168.255.255/16

Exercício Resolvido (4)

- Quantos *hosts* temos em cada um dos intervalos?
 - a) 10.0.0.0 a 10.255.255.255/8
 - b) 172.16.0.0 a 172.31.255.255/12
 - c) 192.168.0.0 a 192.168.255.255/16

Exercício Resolvido (4)

- Quantos *hosts* temos em cada um dos intervalos?
 - a) 10.0.0.0 a 10.255.255.255/8 → $2^{(32-8)} = 16.777.216$ hosts
 - b) 172.16.0.0 a 172.31.255.255/12 → $2^{(32-12)} = 1.048.576$ hosts
 - c) 192.168.0.0 a 192.168.255.255/16 → $2^{(32-16)} = 65.536$ hosts

Volta da NAT

- Internamente, cada máquina tem um IP privado
- Quando um pacote sai da empresa, ele passa por uma caixa NAT que converte o IP privado (e.g., 192.168.1.2) no IP da empresa (e.g., 198.60.42.12)
- **Na volta, como a caixa NAT sabe qual será o endereço a ser substituído?**

Volta da NAT

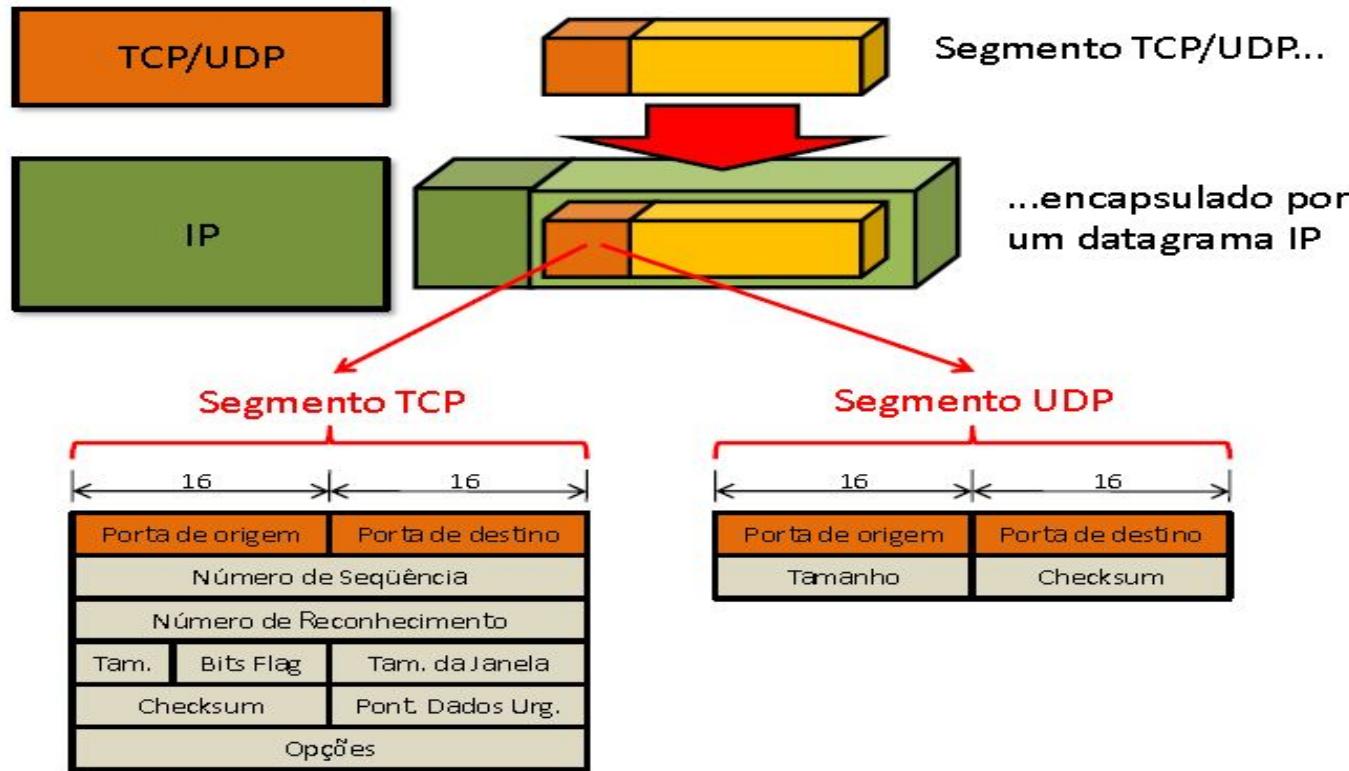
- Internamente, cada máquina tem um IP privado
- Quando um pacote sai da empresa, ele passa por uma caixa NAT que converte o IP privado (e.g., 192.168.1.2) no IP da empresa (e.g., 198.60.42.12)
- Na volta, como a caixa NAT sabe qual será o endereço a ser substituído?

Considerando portas do TCP e do UDP

Portas do TCP e UDP

- Quando um processo deseja estabelecer uma conexão TCP/UDP com outro remoto, ele se associa a uma porta TCP/UDP não usada
 - Portas ⇒ inteiros de 16 bits
 - Essa porta (porta de origem) informa para onde devem ser enviados os pacotes relativos a conexão em questão
 - O processo também fornece uma porta de destino informando para quem deverão ser entregues os pacotes no lado remoto

Portas do TCP e UDP



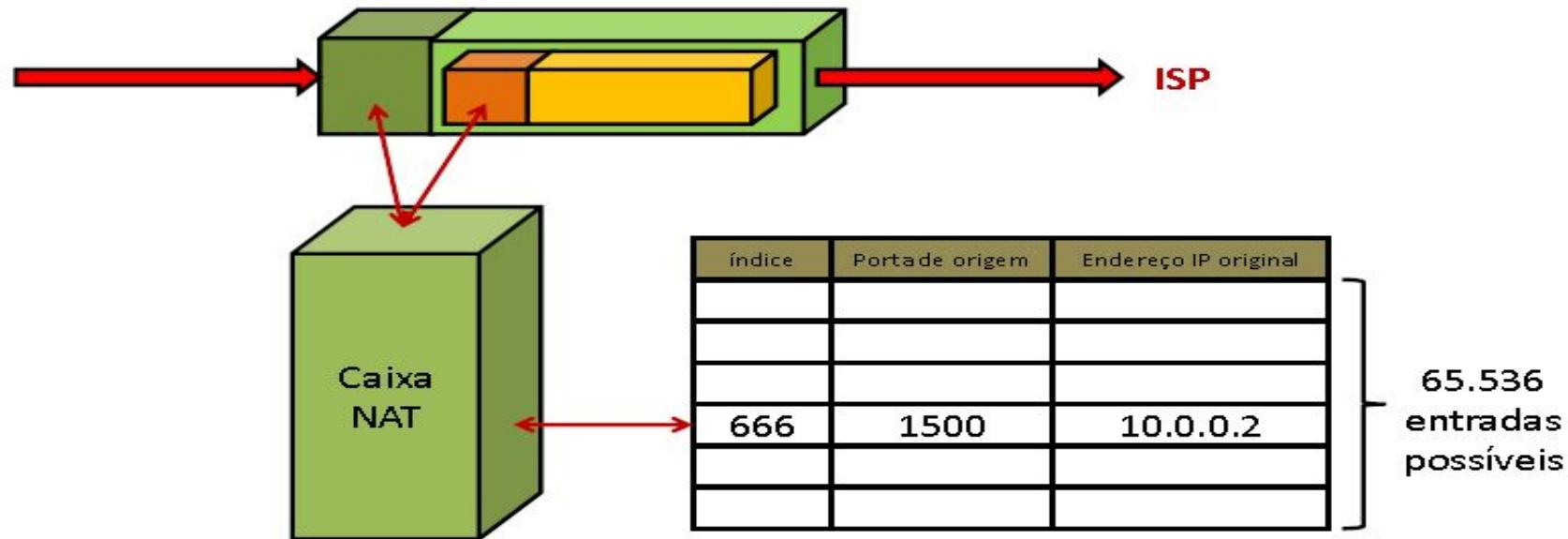
Ideia Básica da NAT

- Cada caixa NAT possui uma tabela de conversão contendo o par porta de origem e IP privado
- Quando um pacote de saída entra na caixa NAT:
 - O IP privado da origem é substituído pelo da empresa
 - O campo porta de origem é substituído por uma das entradas da tabela de conversão da caixa NAT

Ideia Básica da NAT

- Quando um pacote chega ao NAT vindo do ISP, o campo **porta de destino** do cabeçalho do TCP/UDP é extraído e usado como índice para a tabela de mapeamento da caixa NAT
- A partir da entrada localizada, o IP privado e o campo **porta de origem** do TCP/UDP original são extraídos e inseridos no pacote como endereço IP e **porta de destino**

Ideia Básica da NAT



1. Endereço IP original (10.0.0.2) é substituído pelo externo (198.60.42.12)
2. Porta de origem (1500) é substituída por um índice na tabela (666)
3. Checksum do segmento TCP/UDP e do datagrama IP são recalculados

Desvantagens da NAT

- Viola o modelo da arquitetura TCP/IP onde um endereço IP identifica de forma exclusiva uma única máquina em todo o mundo
- Faz a Internet mudar suas características de rede sem conexões para uma espécie de rede orientada à conexão (NAT mantém informações sobre conexões)
- Viola a regra mais fundamental da distribuição de protocolos em camadas em que uma camada não deveria investigar o cabeçalho de outra, garantindo a independência de protocolos

Desvantagens da NAT

- Algumas aplicações inserem endereços IP no corpo do texto (FTP)
- No máximo 2^{16} (65.536) máquinas podem ser mapeadas em um endereço IP
 - Na verdade, temos 61.440 porque 4.096 portas estão reservadas para usos especiais

Exercício (8)

- Tanto o NAT quanto o endereçamento sem classes da Internet (CIDR) foram projetados devido à escassez de endereços IP disponíveis. Explique o funcionamento básico destas duas técnicas e a principal diferença entre elas.

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- **Protocolos de controle da Internet**
- Roteamento
- *Internet Protocol v6 (IPv6)*

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - **Protocolos de controle da Internet**
 - Roteamento
 - *Internet Protocol v6 (IPv6)*
- *Internet Control Message Protocol (ICMP)*
 - *Address Resolution Protocol (ARP)*
 - *Dynamic Host Configuration Protocol (DHCP)*

Internet Control Message Protocol (ICMP)

- Relata eventos inesperados nos roteadores
 - O roteador que detecta o problema envia um pacote ICMP para a origem do pacote com problema
- Mensagens encapsuladas em pacotes IP
- Também é usado para testar a Internet (e.g., no comando *traceroute*)

Cabeçalho IP

Mensagem
ICMP

Mensagens ICMP

- *Destination Unreachable*:
 - Roteador não consegue descobrir um caminho para o destino
 - Pacote com DF não pode ser entregue, pois há um trecho com MTU pequeno
- *Time Exceeded*: Pacote descartado porque seu TTL zerou
- *Parameter Problem*: Valor inválido detectado em um campo de cabeçalho
- *Echo e Echo Reply*: Determinam se um destino está ativo e acessível (e.g., usadas pelo comando ping)
- Outras mensagens: www.iana.org/assignments/icmp-parameters

Exemplo de Aplicação ICMP: Comando *traceroute*

- Mostra por onde um pacote IP trafega quando é enviado
- Não existe um mecanismo disponível nos roteadores para informar o trajeto de um pacote IP pela Internet
- Solução:
 - Origem envia pacotes com TTL a partir de 1 até alcançar o destino
 - Cada vez que um pacote “morre” no caminho até o destino, a origem recebe um pacote *ICMP Time Exceeded* e, assim, consegue traçar a rota

ICMP: Comando *traceroute*

```
:~$ traceroute www.pucminas.br
traceroute to www.pucminas.br (200.229.32.27), 64 hops max
 1  192.168.15.1  1,608ms  1,418ms  1,355ms
 2  179.184.126.85  8,185ms  7,800ms  2,687ms
 3  201.22.79.201  4,534ms  9,966ms  6,485ms
 4  152.255.153.139  36,971ms  31,367ms  30,926ms
 5  *  *  *
 6  *  *  *
 7  186.248.97.170  38,915ms  37,600ms  31,227ms
 8  *  *  *
 9  *  *  *
10  *  *  *
11  *  *  *
12  *  *  *
13  *  *  *
14  *  *  *
15  *  *  *
16  *  *  *
```

■ ■ ■

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - **Protocolos de controle da Internet**
 - Roteamento
 - *Internet Protocol v6 (IPv6)*
- *Internet Control Message Protocol (ICMP)*
 - ***Address Resolution Protocol (ARP)***
 - *Dynamic Host Configuration Protocol (DHCP)*

Endereço Ethernet, Físico ou MAC

- Tem 6 bytes (48 bits) que são representados em hexadecimal e separados por dois-pontos ou hífen (e.g., 00:19:B9:FB:E2:58)
- São únicos, assim, não temos duas *Network Interface Cards* (NICs) com mesmo endereço físico
- Gerenciados pelo IEEE que é responsável por distribuir blocos para os fabricantes de NICs Ethernet

Descubra seu Endereço Físico

- No Linux, use o comando *ifconfig*. No Windows, *ipconfig/all*

```
:$ ifconfig
enp1s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether 74:e6:e2:d0:48:f7 txqueuelen 1000 (Ethernet)
      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

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.15.17 netmask 255.255.255.0 broadcast 192.168.15.255
      inet6 fe80::9b5f:6b9f:d2be:f302 prefixlen 64 scopeid 0x20<link>
      inet6 2804:7f2:288c:de4d:1600:6138:b4b:e3aa prefixlen 64 scopeid 0x0<global>
      inet6 2804:7f2:288c:de4d:996:6cd2:81fe:8cf2 prefixlen 64 scopeid 0x0<global>
      ether 38:b1:db:cc:f7:eb txqueuelen 1000 (Ethernet)
      RX packets 1111856 bytes 840723520 (840.7 MB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 745549 bytes 307200727 (307.2 MB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Qual seu endereço?



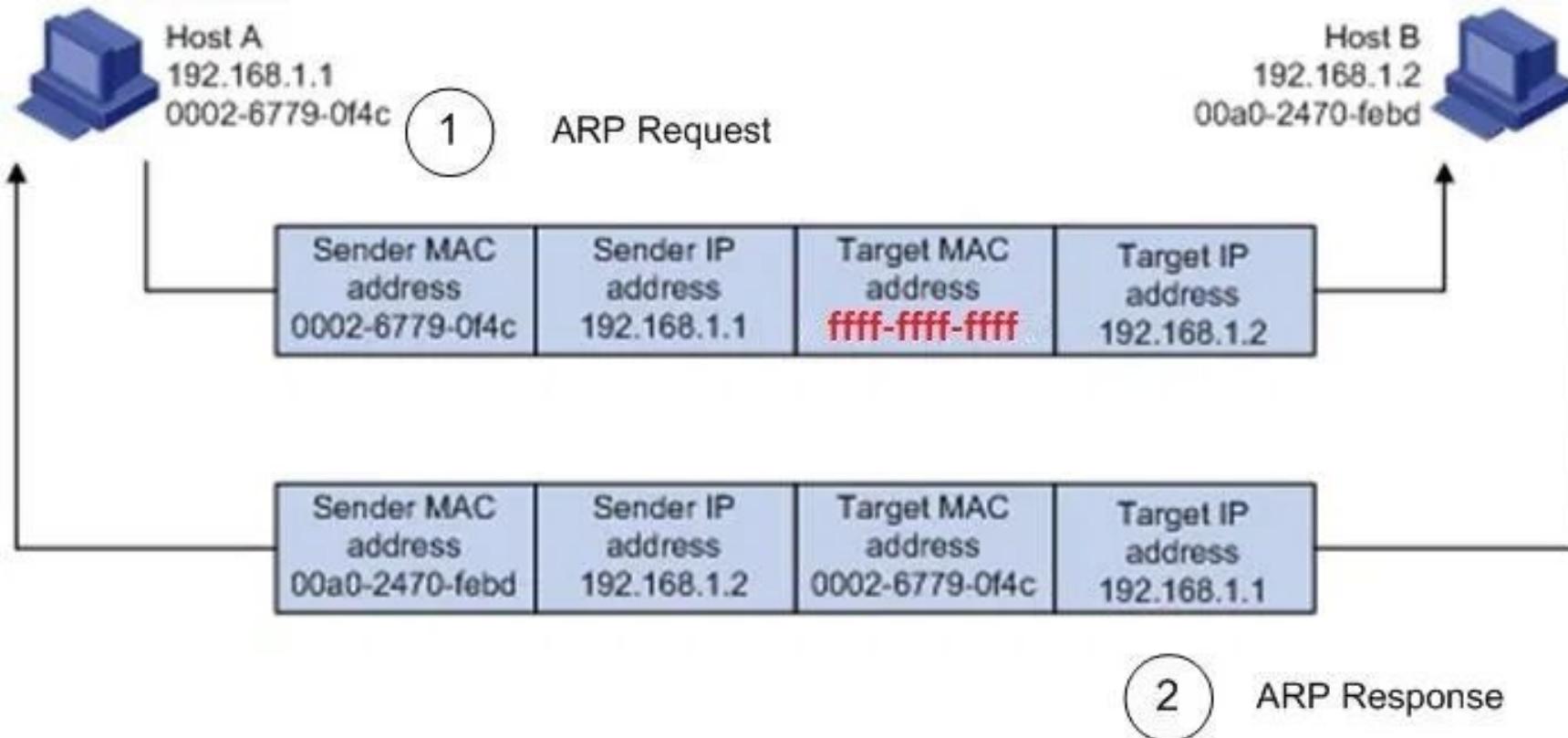
Mapeamento do Endereço IP em Físico

- Quando enviamos uma mensagem, conhecemos o IP e porta do destino
- Acessando a tabela de rotas com o IP do destino, descobrimos o IP do próximo nó
- Como a camada de enlace desconhece endereços IPs, é inútil que a camada de rede apenas informe o endereço IP do próximo nó para a de enlace
- O *Address Resolution Protocol* (ARP) faz o mapeamento de endereços IPs em endereços de enlace (e.g., endereços Ethernet)

Address Resolution Protocol (ARP)

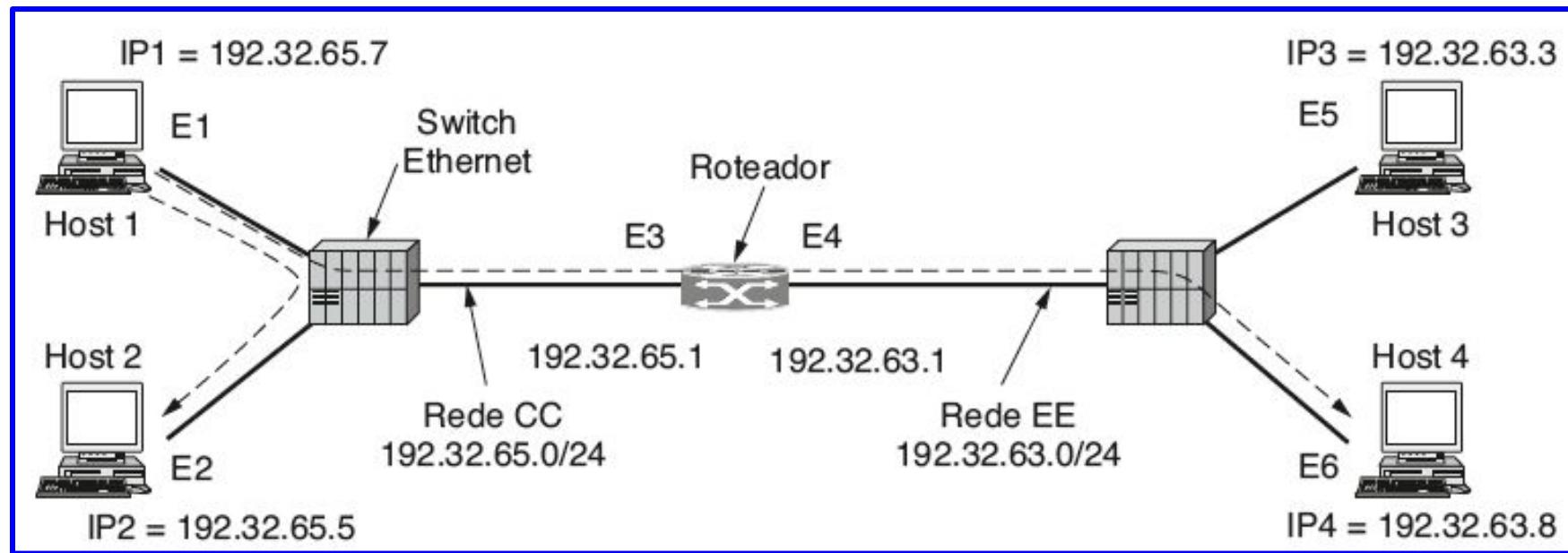
- Quando um nó deseja enviar um pacote e desconhece o endereço físico do próximo nó, ele envia uma mensagem ARP de difusão perguntando qual é o endereço físico do próximo nó
- Todos os nós da rede recebem a mensagem e o próximo nó responde informando seu endereço físico
- Protocolo definido no RFC 826

Address Resolution Protocol (ARP)



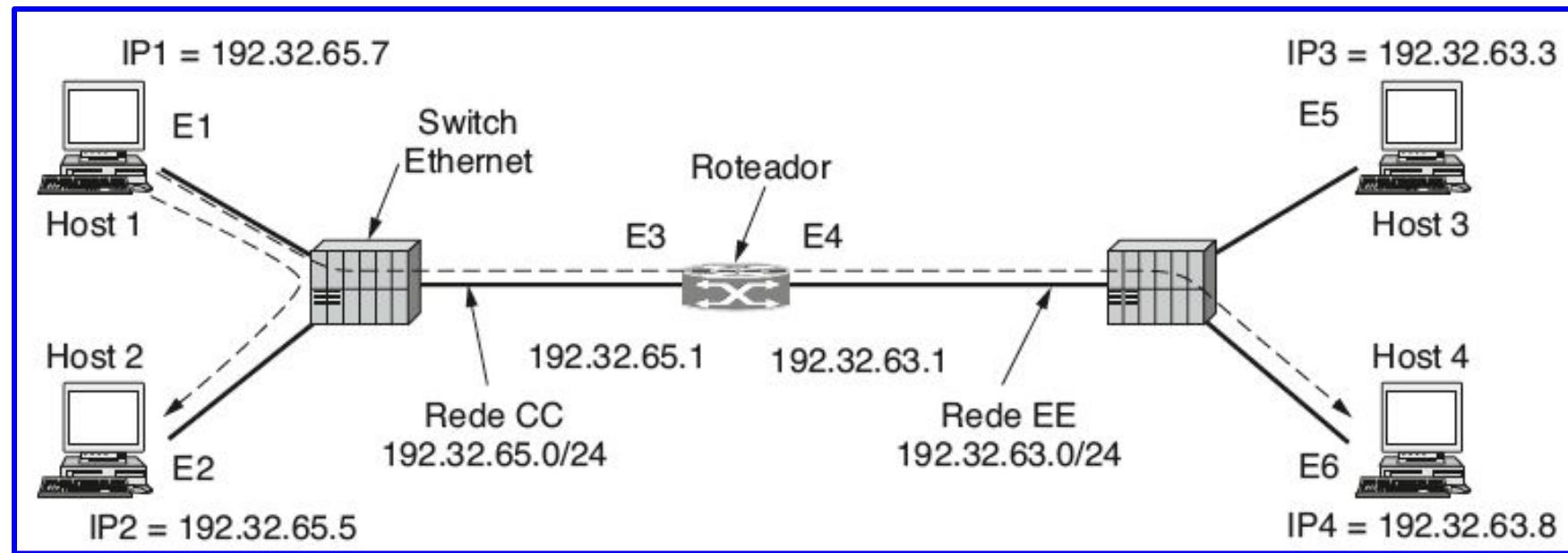
Exemplo do Funcionamento do ARP

- Temos duas redes 192.32.65.0/24 (CC) e 192.32.63.0/24 (EE) com dois *hosts* cada e conectadas por um roteador com duas interfaces de rede. Cada *host* e interface do roteador tem seu endereço IP e físico (E1 a E6)



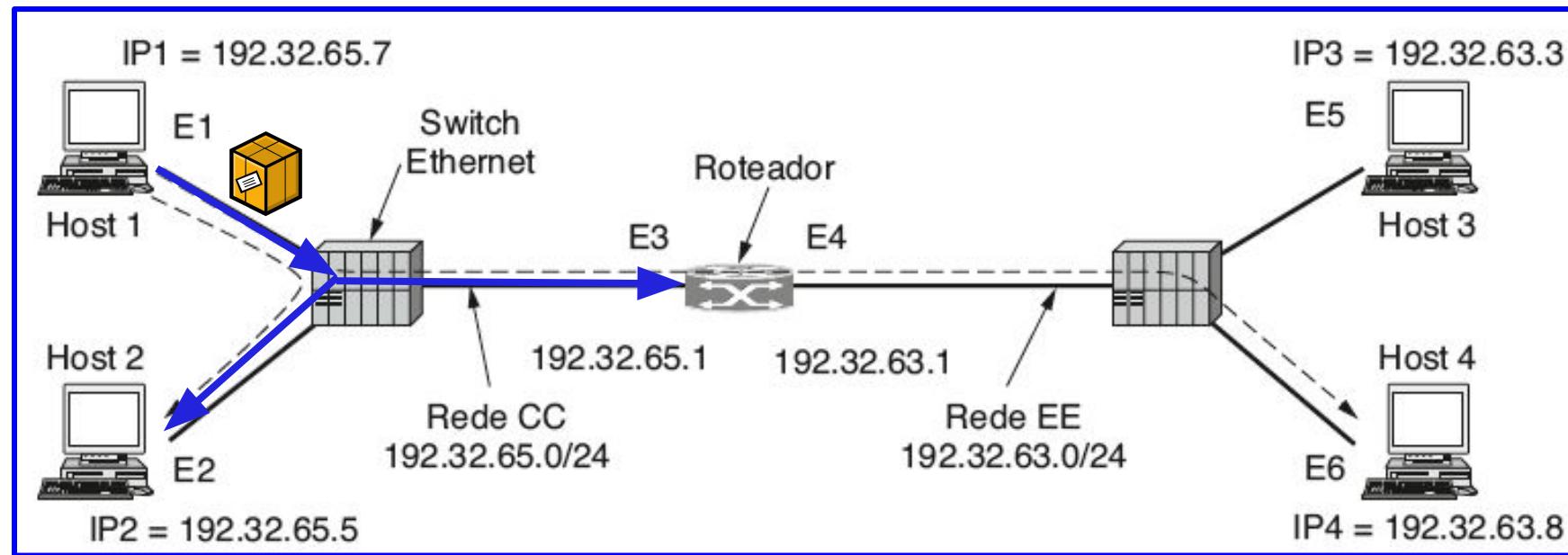
Exemplo (A): Host 1 Deseja Enviar Pacotes para o 2

- O Host 1 sabe o endereço do 2 e que estão na mesma rede, contudo, ele não sabe o endereço físico do host 2



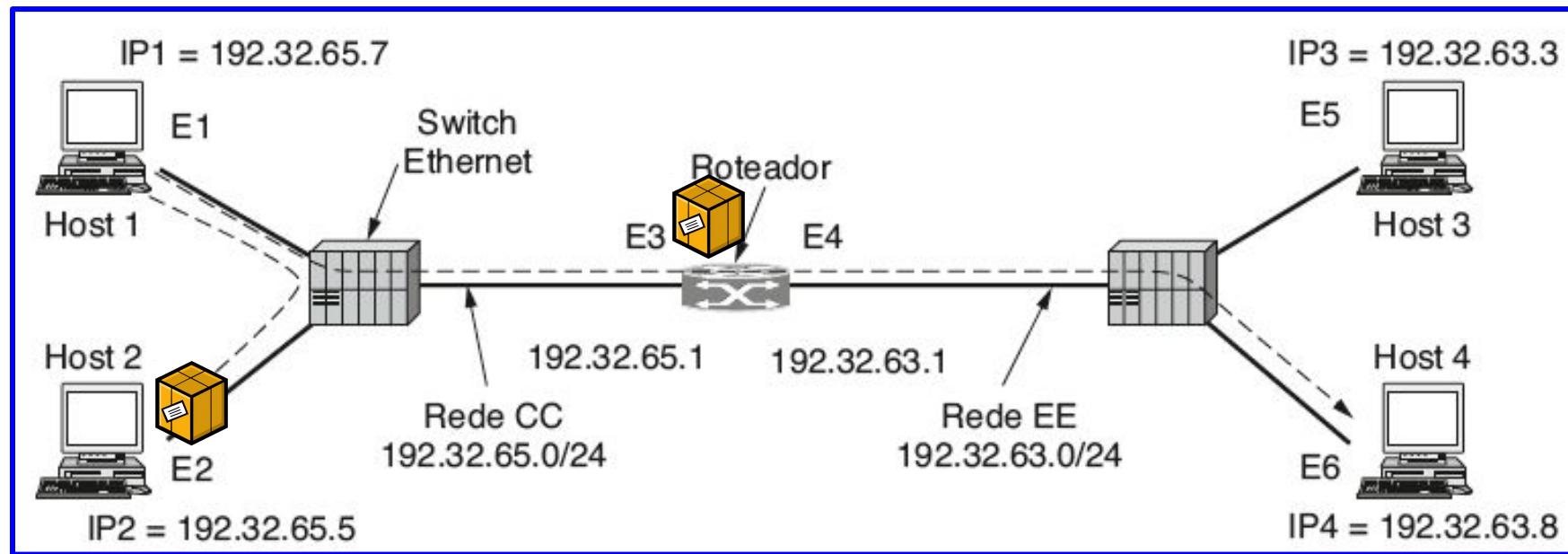
Exemplo (A): Host 1 Deseja Enviar Pacotes para o 2

- Assim, o host 1 envia um pacote ARP de difusão para a Ethernet perguntando quem possui o endereço IP 192.32.65.5



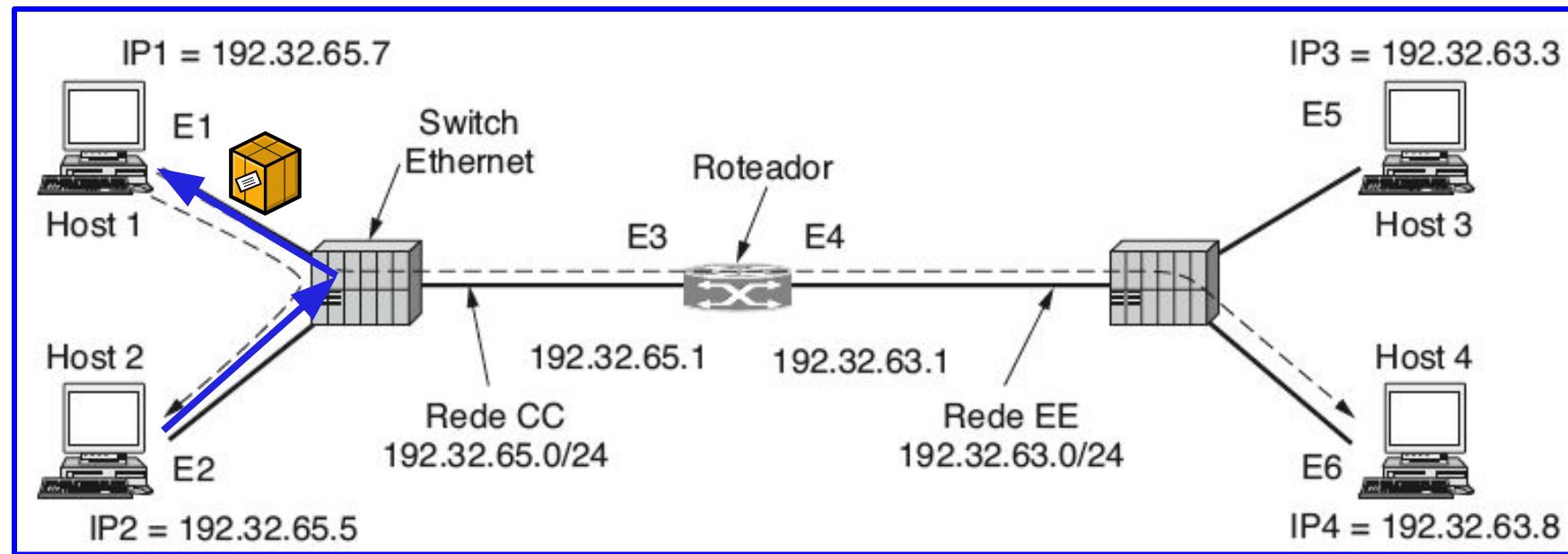
Exemplo (A): Host 1 Deseja Enviar Pacotes para o 2

- A difusão chega em todas as máquinas da rede Ethernet 192.32.65.0/24



Exemplo (A): Host 1 Deseja Enviar Pacotes para o 2

- O *host 2* responde com seu endereço Ethernet (E2) e quando o *host 1* receber essa informação ele inicia o envio desejado



Outra Solução para o Mapeamento de Endereços

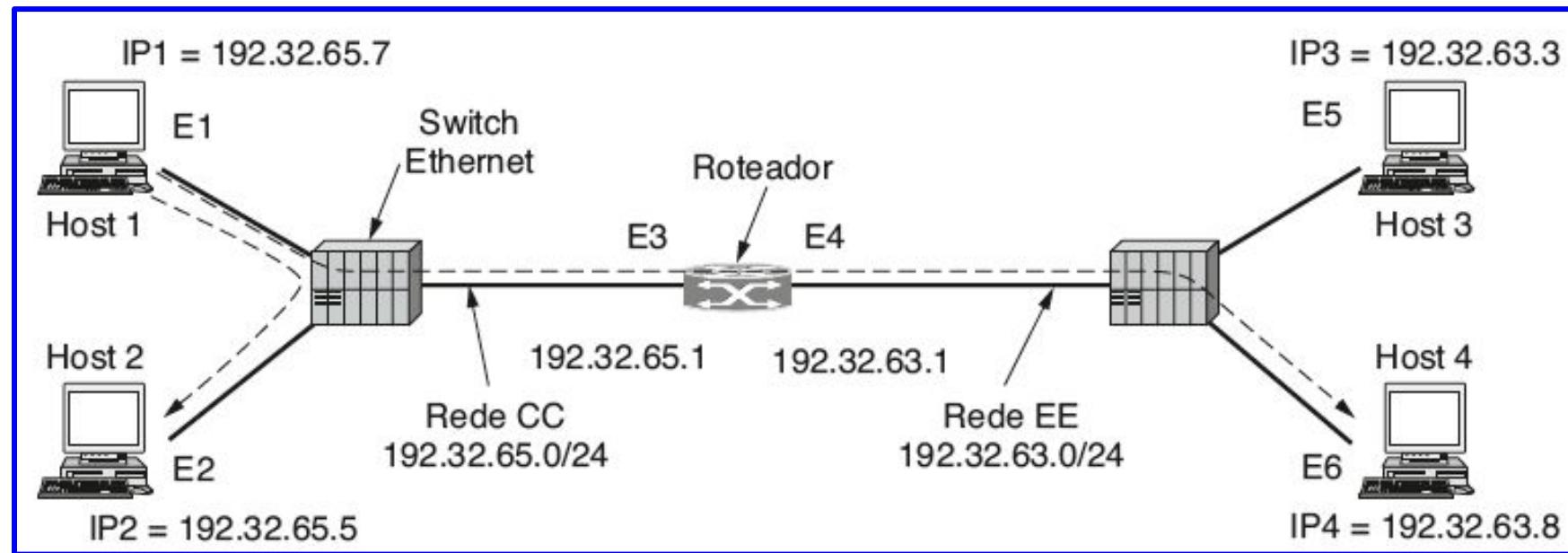
- Existência de um arquivo mapeando endereços IPs em físicos
- Embora possível, essa solução é difícil à medida que aumentamos o número de máquinas e a dinamicidade da rede
- O ARP simplifica o projeto da rede uma vez que o projetista apenas atribui IPs e máscaras e o ARP garante o mapeamento entre os endereços IPs e físicos

Otimizações para o ARP

- Depois que uma máquina executa o ARP, ela armazena o resultado em um *cache*, caso precise entrar em contato com a mesma máquina pouco depois
- *Host 1* inclui o par (IP1,E1) no pacote ARP de difusão para que o 2 insira essa informação no *cache*. Na verdade, todas as máquinas fazem essa inserção
- ARP Gratuito: Cada máquina procura seu próprio endereço Ethernet ao ser inicializada para ter certeza que nenhuma outra possui o mesmo endereço IP
- Para permitir substituições de placas Ethernet, as entradas no *cache* ARP sofrem um *timeout* após alguns minutos

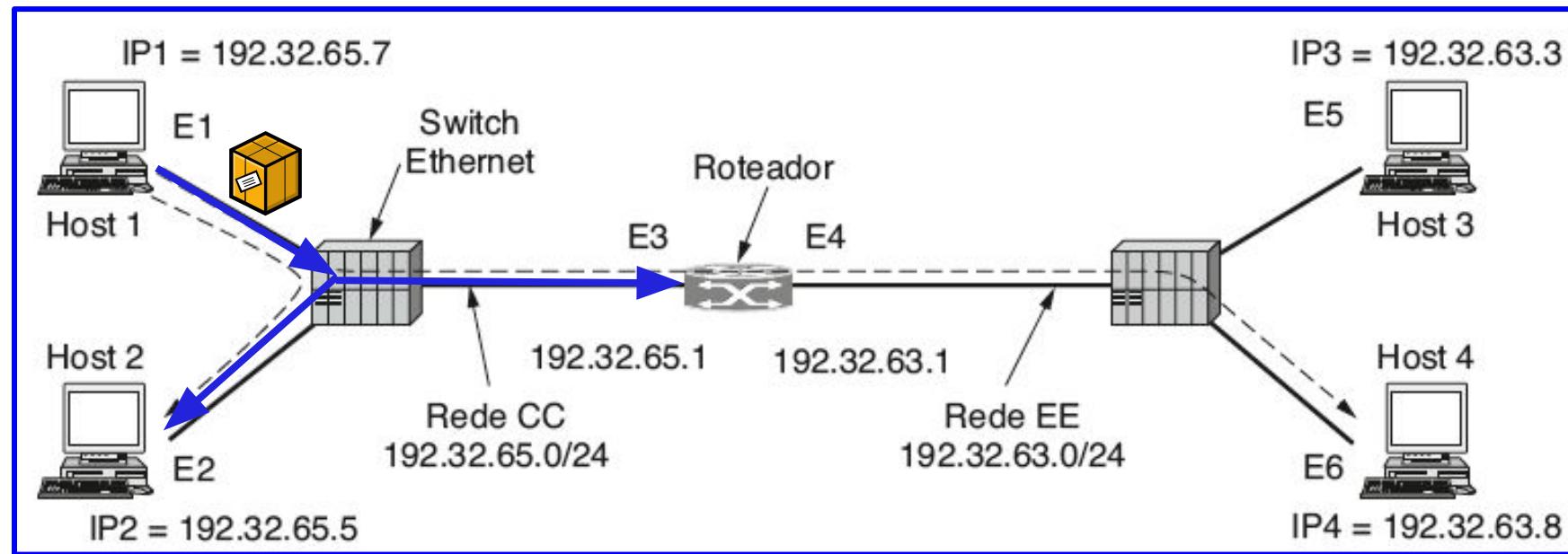
Exemplo (B): Host 1 Deseja Enviar Pacotes para o 4

- O Host 1 sabe o endereço do 4 e que o pacote deve ser enviado para o roteador no IP 192.32.65.1, contudo, ele não sabe o endereço físico do roteador



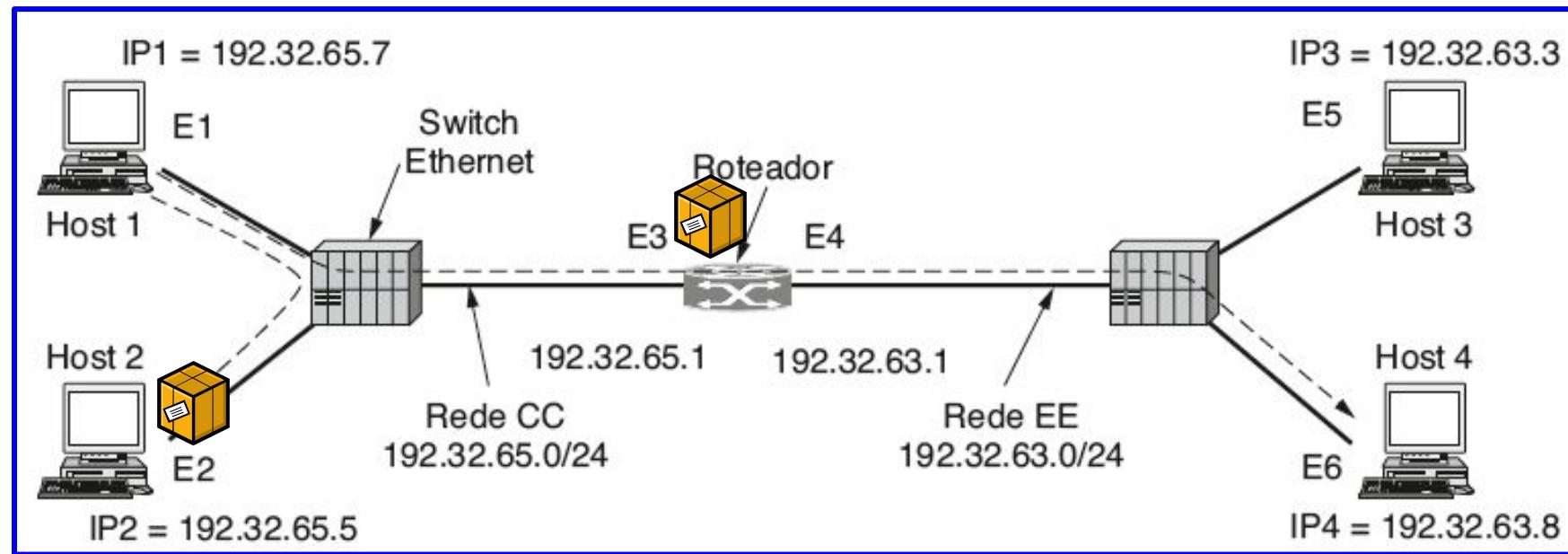
Exemplo (B): Host 1 Deseja Enviar Pacotes para o 4

- Assim, o host 1 envia um pacote ARP de difusão para a Ethernet perguntando quem possui o endereço IP 192.32.65.1



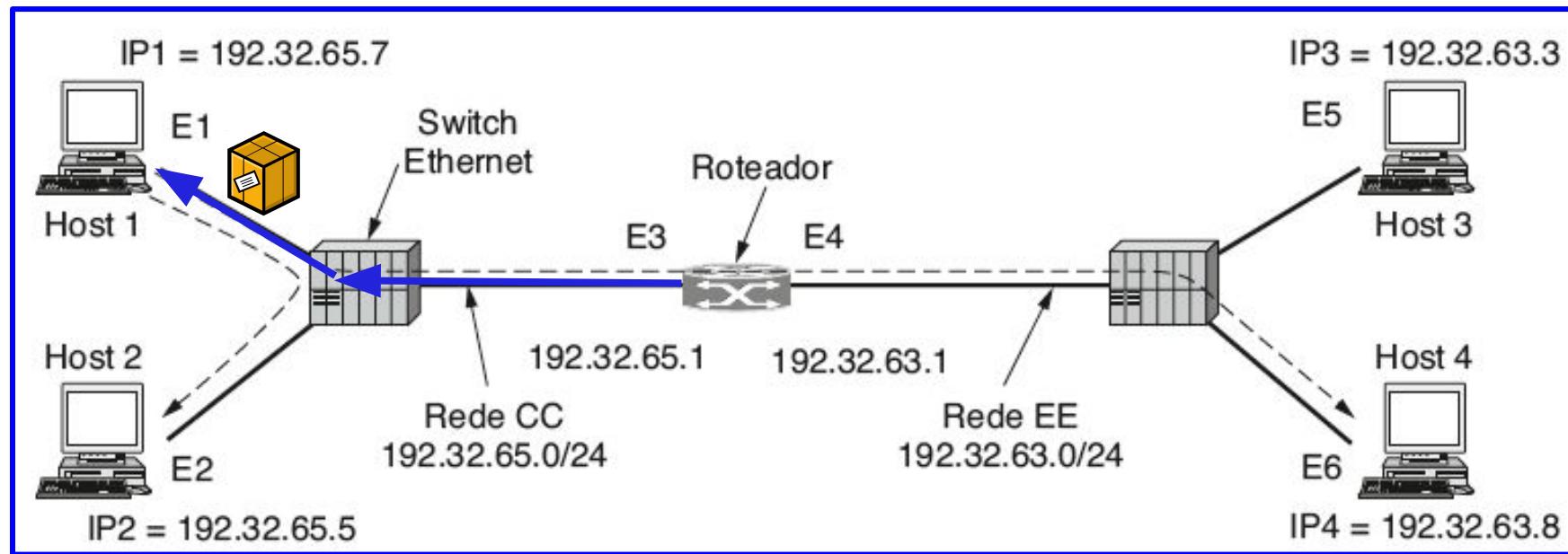
Exemplo (B): Host 1 Deseja Enviar Pacotes para o 4

- A difusão chega em todas as máquinas da rede Ethernet 192.32.65.0/24



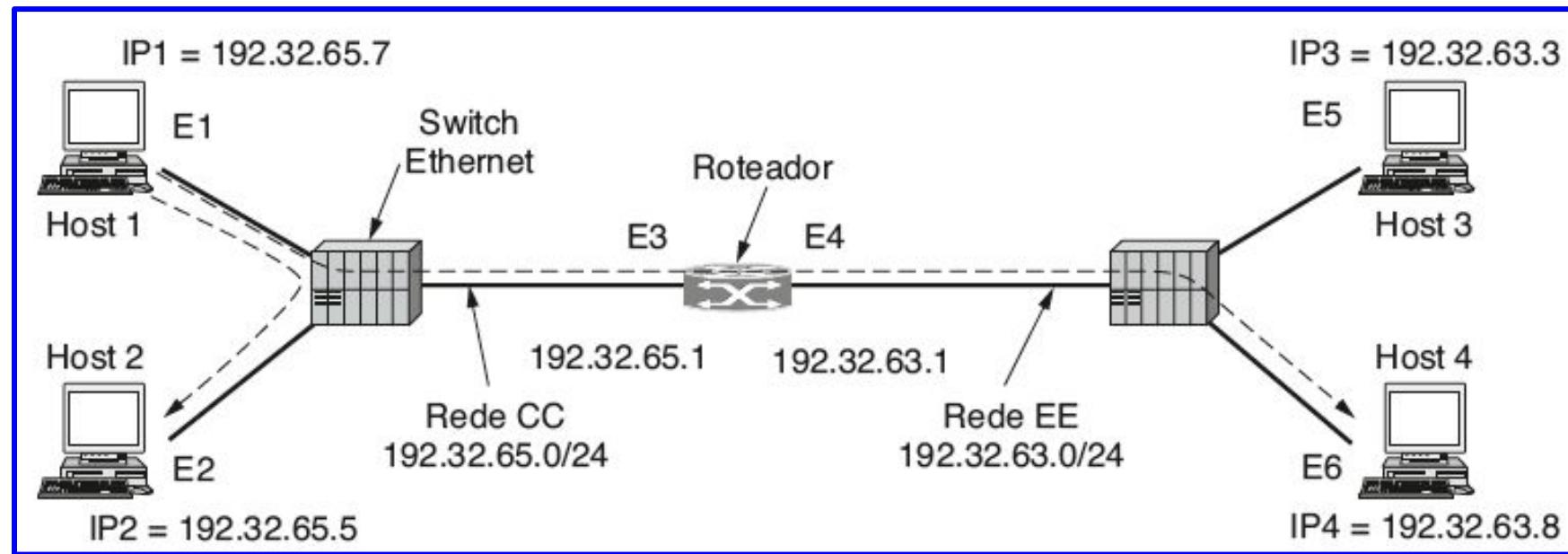
Exemplo (B): Host 1 Deseja Enviar Pacotes para o 4

- O roteador responde com seu endereço Ethernet (E3) e quando o *host* 1 receber essa informação ele inicia o envio desejado



Exemplo (B): Host 1 Deseja Enviar Pacotes para o 4

- Quando o roteador recebe o pacote de dados, ele executa o ARP na outra rede, continuando o roteamento



Comando ARP

```
Mostra as entradas das máquinas especificadas  
Inserir máquina  
Remover máquina
```

```
:$ arp -a  
_gateway (192.168.0.1) em b0:4e:26:0b:50:c4 [ether] em wlp2s0  
:$ sudo arp -s 192.168.0.150 34:8a:7b:56:29:82  
:$ arp -a  
? (192.168.0.150) em 34:8a:7b:56:29:82 [ether] PERM em wlp2s0  
_gateway (192.168.0.1) em b0:4e:26:0b:50:c4 [ether] em wlp2s0  
:$ sudo arp -d 192.168.0.150  
:$ arp -a  
_gateway (192.168.0.1) em b0:4e:26:0b:50:c4 [ether] em wlp2s0  
:$ █
```

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - **Protocolos de controle da Internet**
 - Roteamento
 - *Internet Protocol v6 (IPv6)*
- *Internet Control Message Protocol (ICMP)*
 - *Address Resolution Protocol (ARP)*
 - *Dynamic Host Configuration Protocol (DHCP)*

Dynamic Host Configuration Protocol (DHCP)

- Os protocolos da Internet consideram que os *hosts* estão configurados com seus respectivos IPs
- Uma forma de fazer isso é manualmente, contudo, trata-se de uma tarefa tediosa e passível de erros
- Outra forma é fazendo com que a rede tenha um servidor DHCP responsável pela configuração

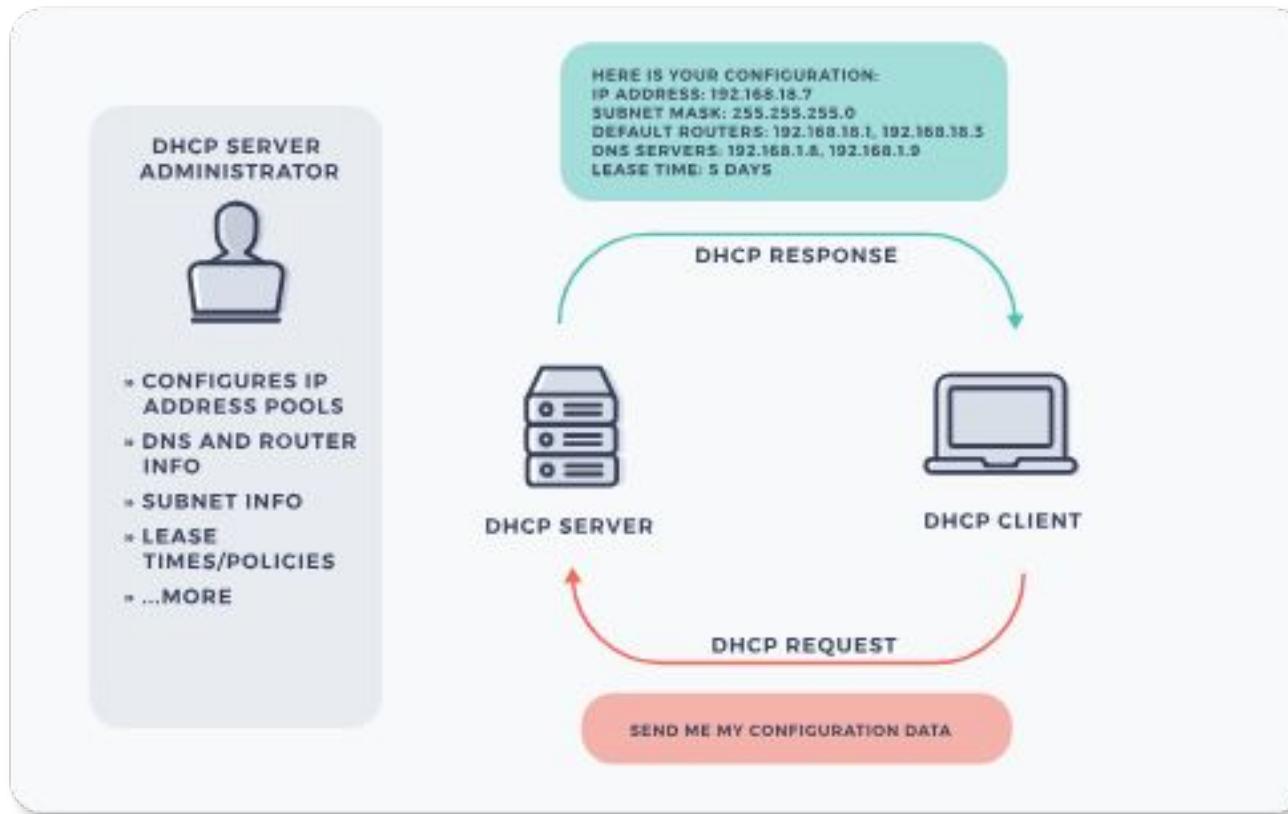
Dynamic Host Configuration Protocol (DHCP)

- Quando um nó entra na rede, ele faz a difusão de um pacote DHCP DISCOVER
- O servidor DHCP responde com um pacote DHCP OFFER contendo um endereço de IP livre e outras informações (e.g., a máscara de rede e os endereços IP do *gateway* padrão e dos servidores de DNS e horas)
- O nó confirma seu desejo enviando um DHCP REQUEST
- O servidor DHCP confirma a alocação enviando um DHCP ACK

Dynamic Host Configuration Protocol (DHCP)



Dynamic Host Configuration Protocol (DHCP)



Dynamic Host Configuration Protocol (DHCP)

- O Servidor de DHCP mantém uma tabela de alocação relacionando os endereços IPs com os físicos dos nós que foram recebidos nos pacotes de DHCP DISCOVER
- *Leasing*: a alocação de IPs acontece por um período de tempo pré-determinado
- Pouco antes do término desse período, o *host* precisa pedir a renovação de seu tempo para o servidor DHCP
- Está descrito nos RFCs 2131 e 2132 e atualizado em 4388 e 6148
- O DHCP é sucessor dos protocolos RARP e BOOTP

Exercício (9)

- Descreva o objetivo e funcionamento básico dos protocolos ICMP, ARP e DHCP?

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- **Roteamento**
- *Internet Protocol v6 (IPv6)*

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- **Roteamento**
- *Internet Protocol v6 (IPv6)*

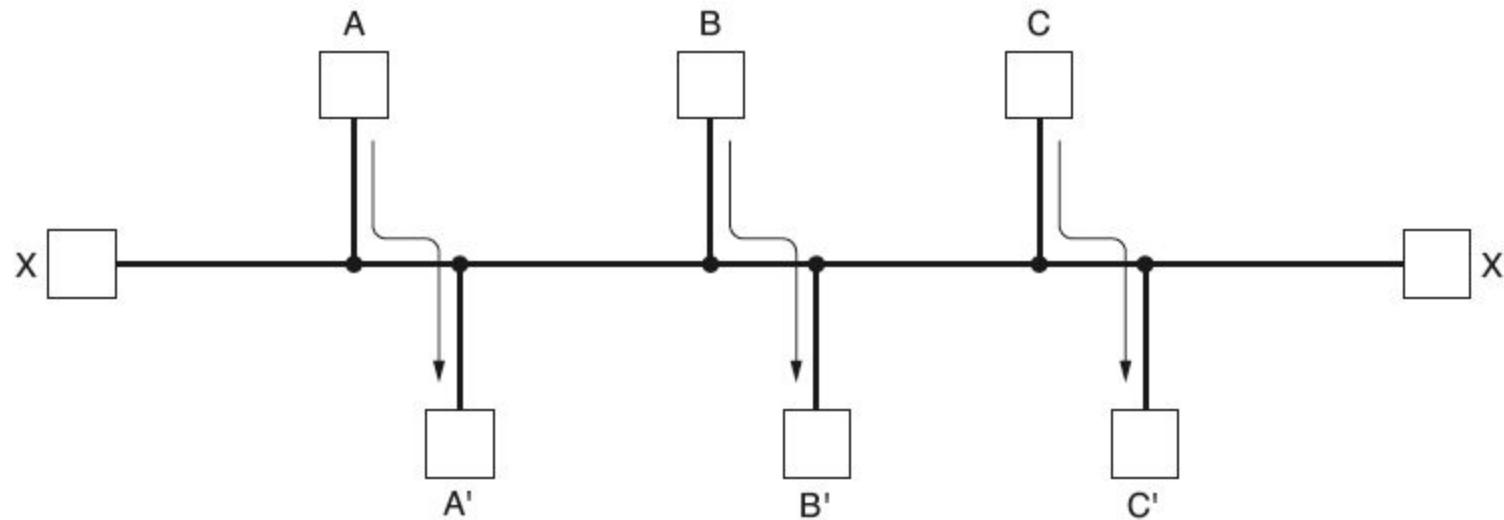
- **Introdução**
- Algoritmos de Roteamento
- Roteamento na Internet

Algoritmo de Roteamento

- É a parte do software da camada de rede responsável pela decisão sobre a interface de saída a ser usada na transmissão do pacote de entrada
- Tem como propriedades desejadas:
 - Exatidão
 - Simplicidade
 - Robustez (pensando em escalabilidade)
 - Estabilidade (convergir para uma rota viável)
 - Equidade
 - Eficiência

Equidade vs Eficiência

- Supondo um tráfego intenso de cada i para i' , a eficiência global máxima acontece desativando completamente o fluxo de x para x' , perdendo equidade. Nesse caso, o ideal é um meio-termo



Roteamento em Redes de Datagrama vs Circuito Virtual

- Em redes de datagrama, a decisão será tomada para cada vez que o pacote de dados recebido
- Em redes de circuito virtual, a decisão será tomada somente quando um novo circuito virtual estiver sendo estabelecido

Algoritmos de Roteamento Estáticos e Dinâmicos

- Estáticos ou não-adaptativos
 - A escolha da rota é previamente calculada off-line, sendo transferida para os roteadores quando a rede é inicializada
 - Desconsidera medidas e estimativas atuais do tráfego, topologia e carga da rede
- Dinâmicos ou Adaptativos
 - Mudam suas decisões de roteamento para refletir mudanças na topologia ou tráfego

Agenda

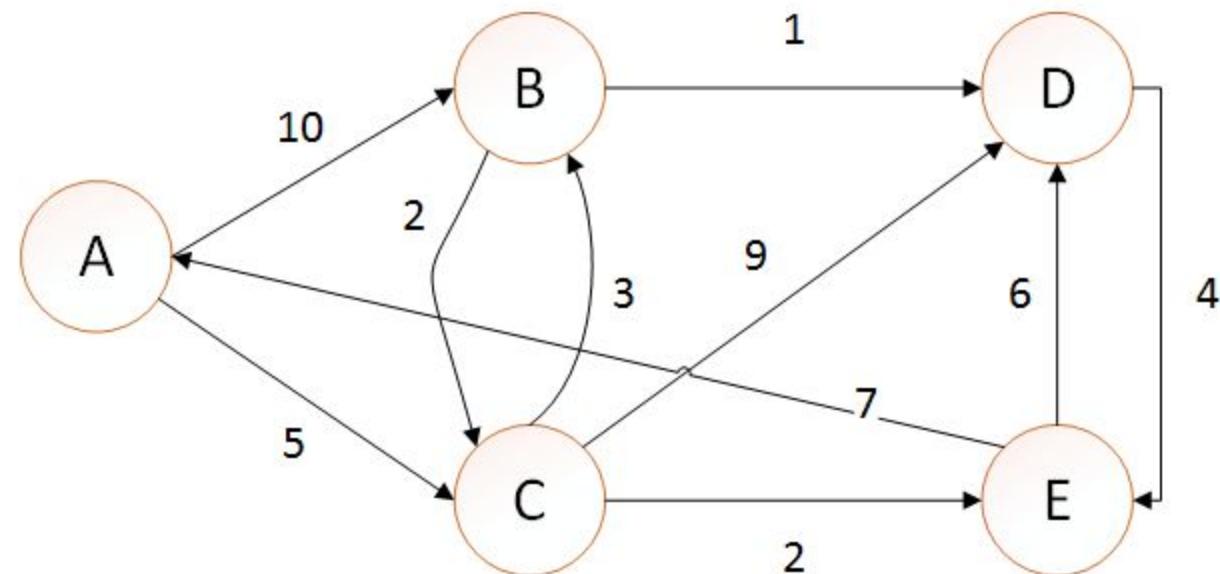
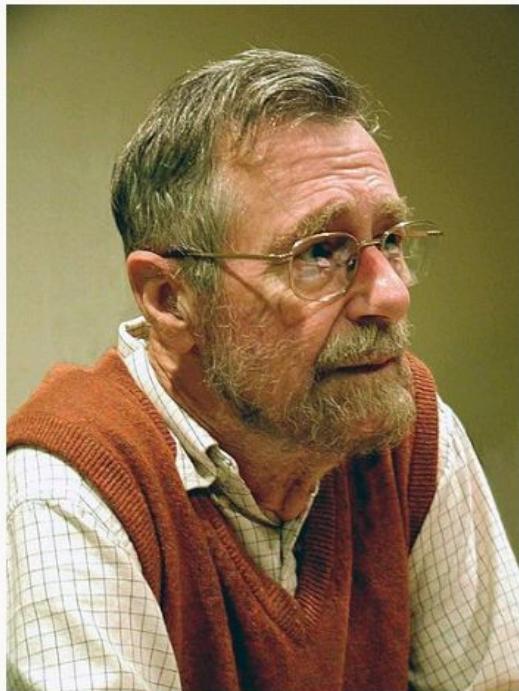
- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- **Algoritmo do caminho mais curto**
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

Algoritmo do Caminho Mais Curto (Dijkstra)

Edsger Dijkstra

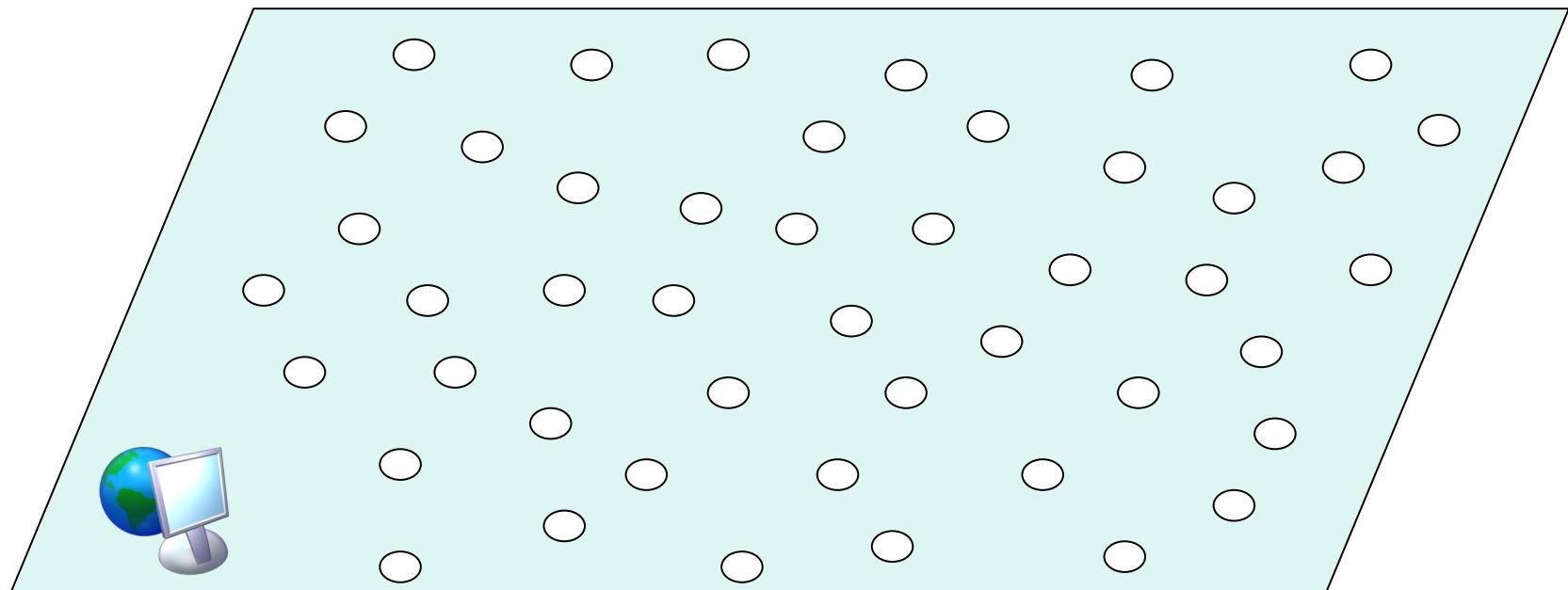


Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - **Flooding**
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

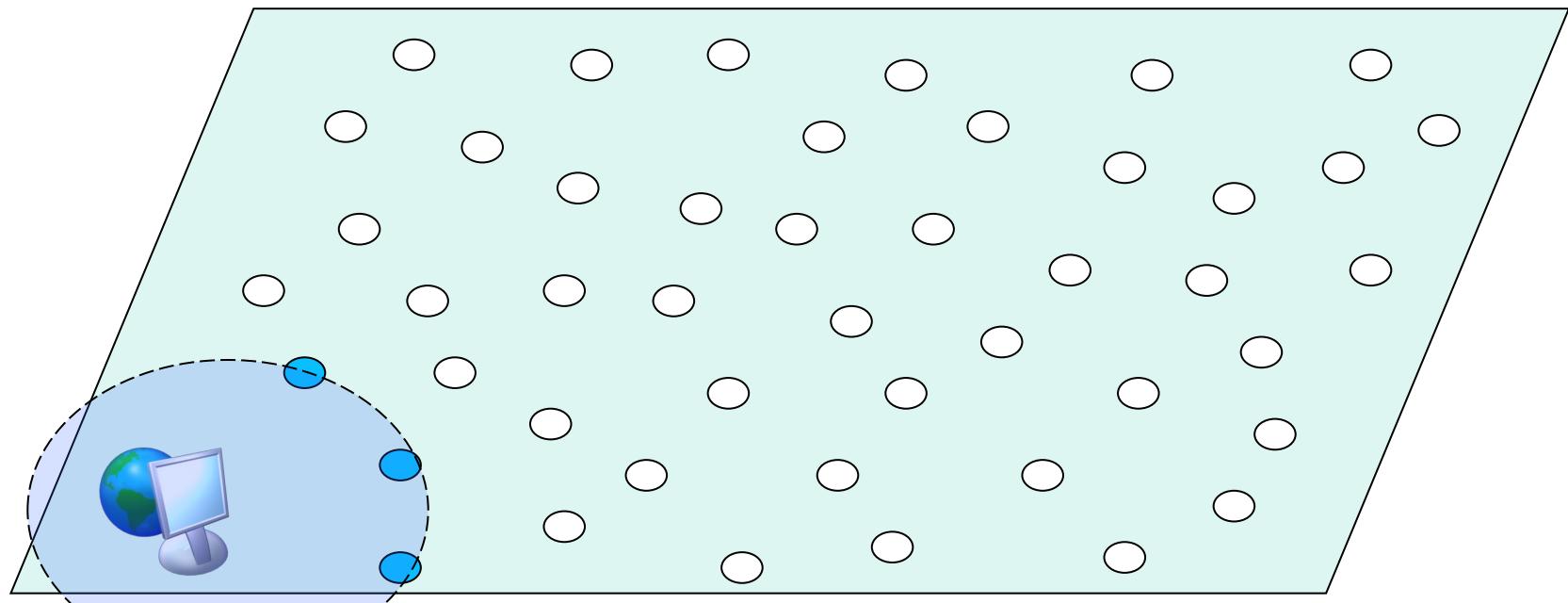
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



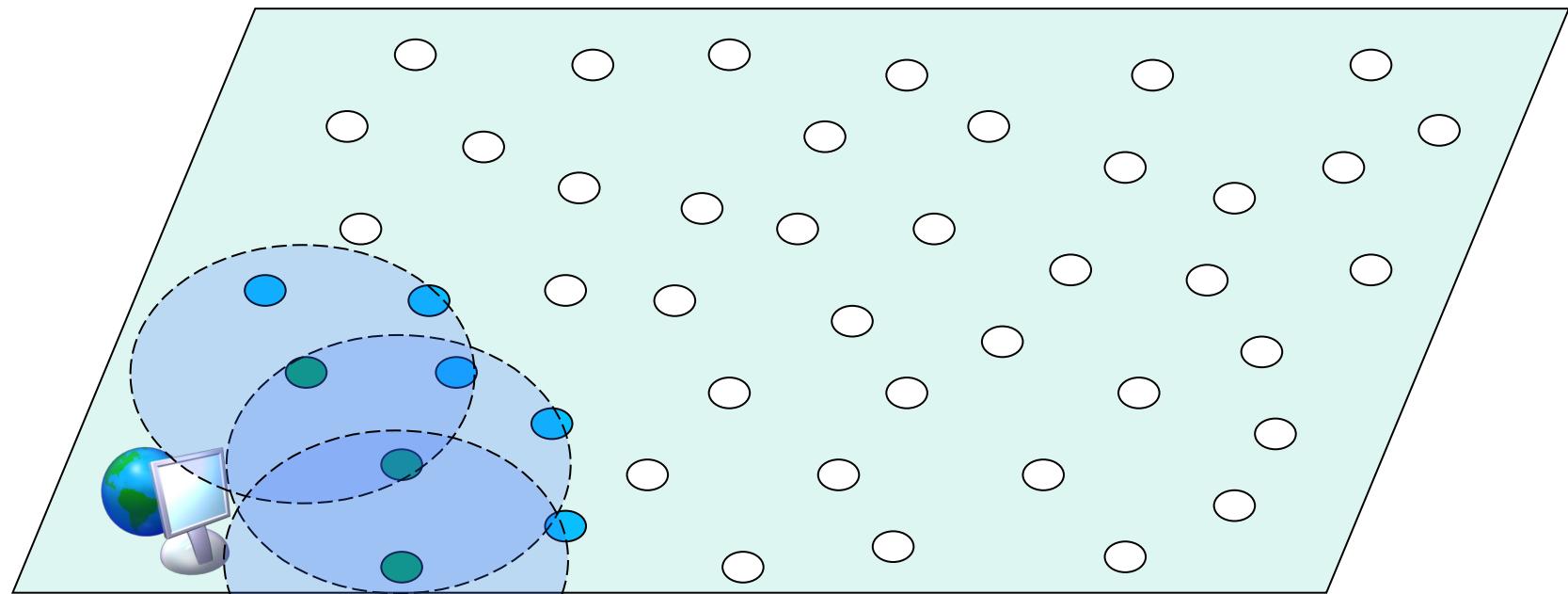
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



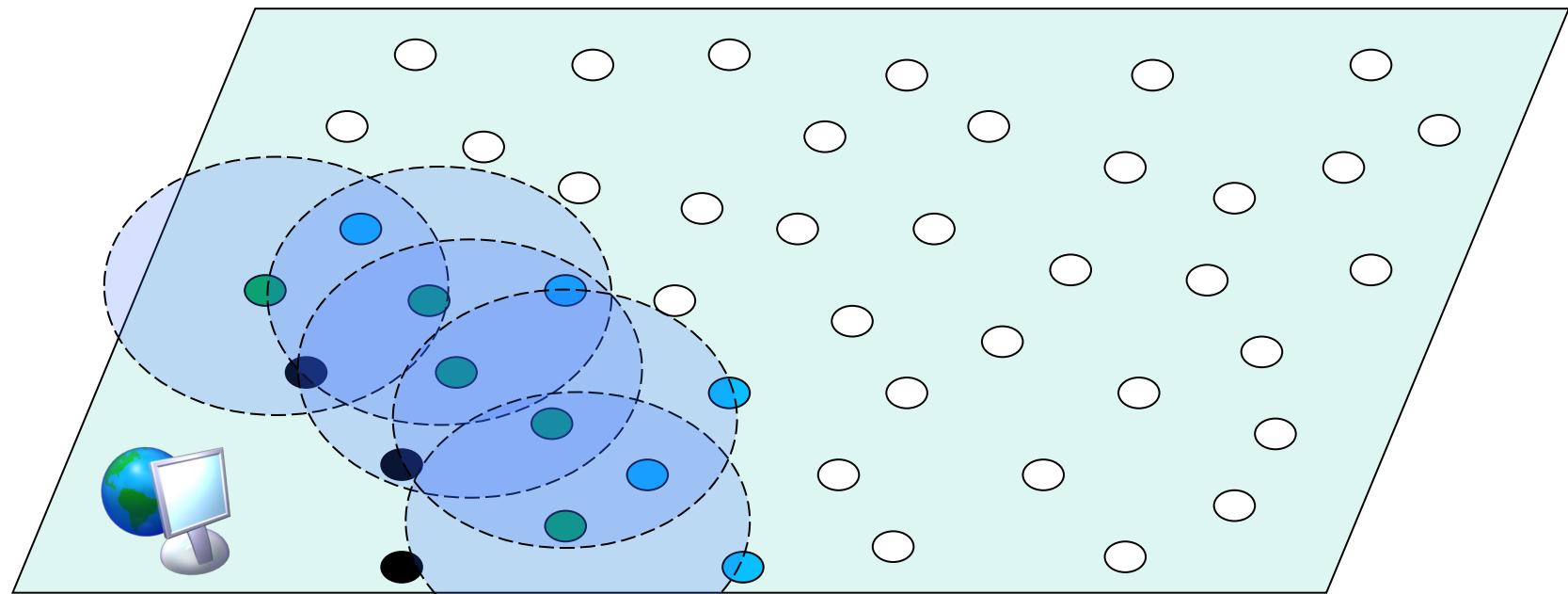
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



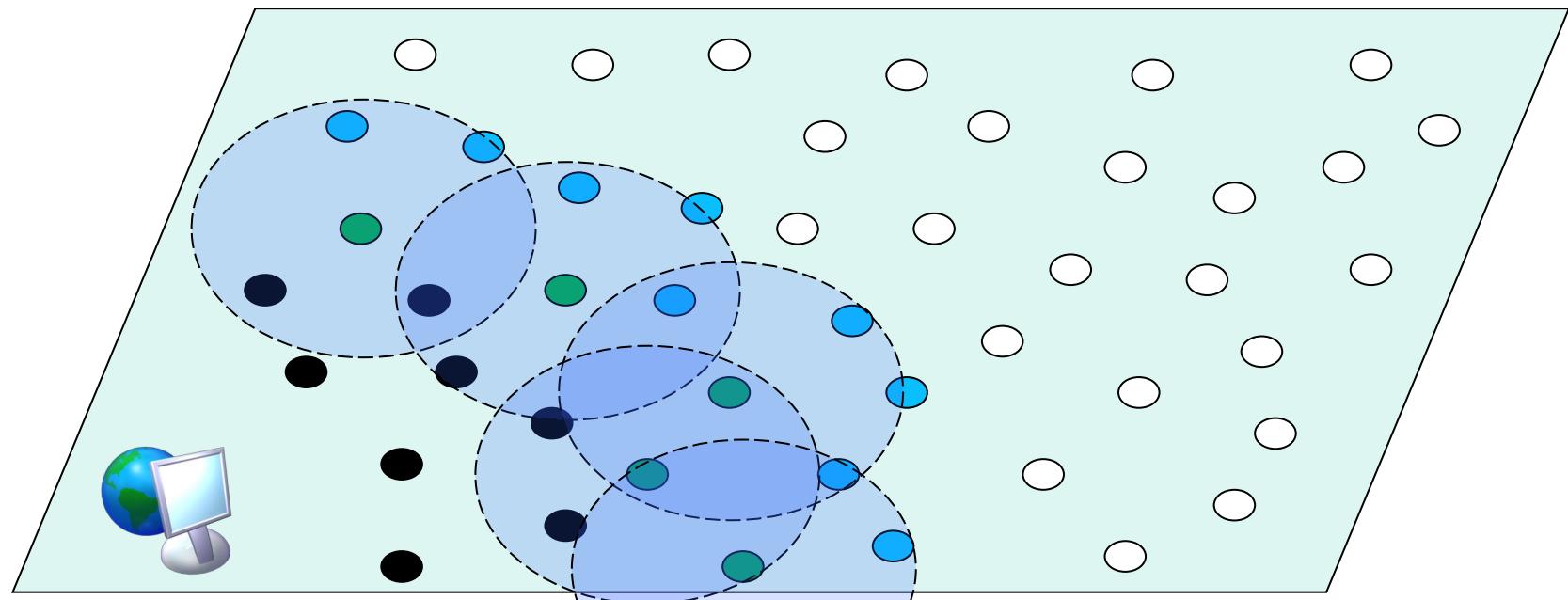
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



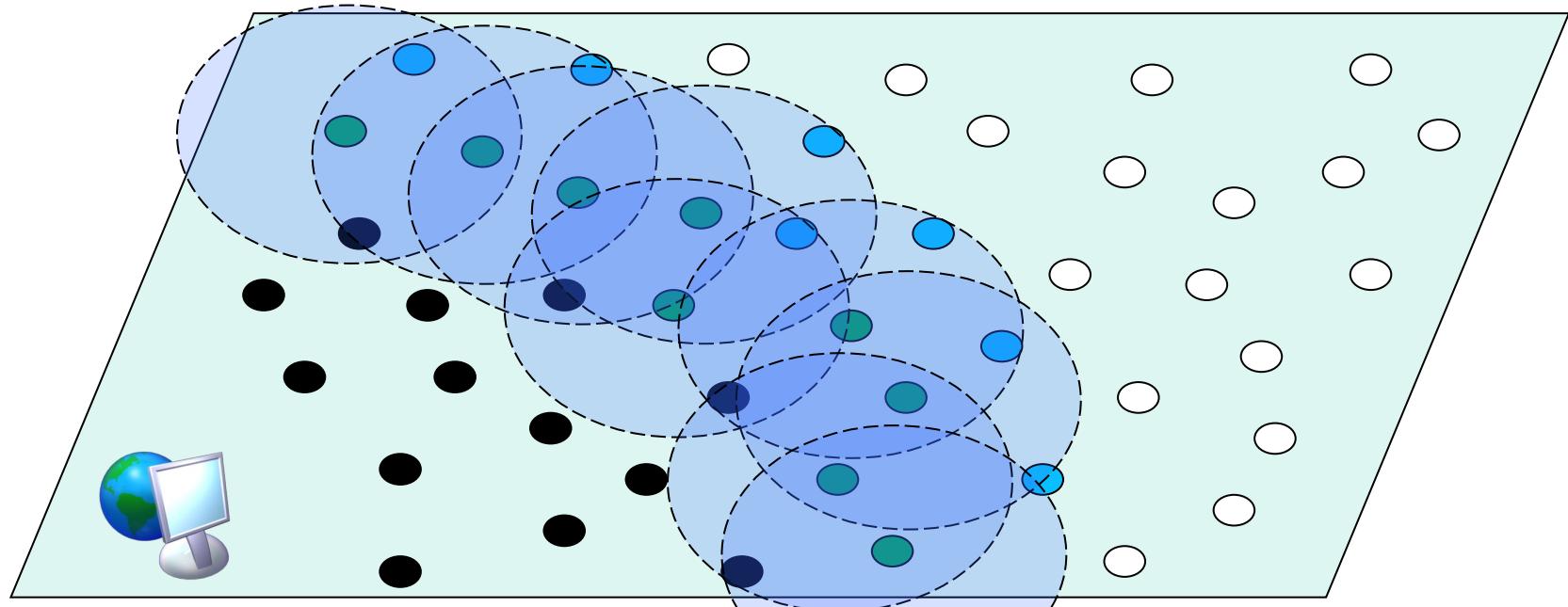
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



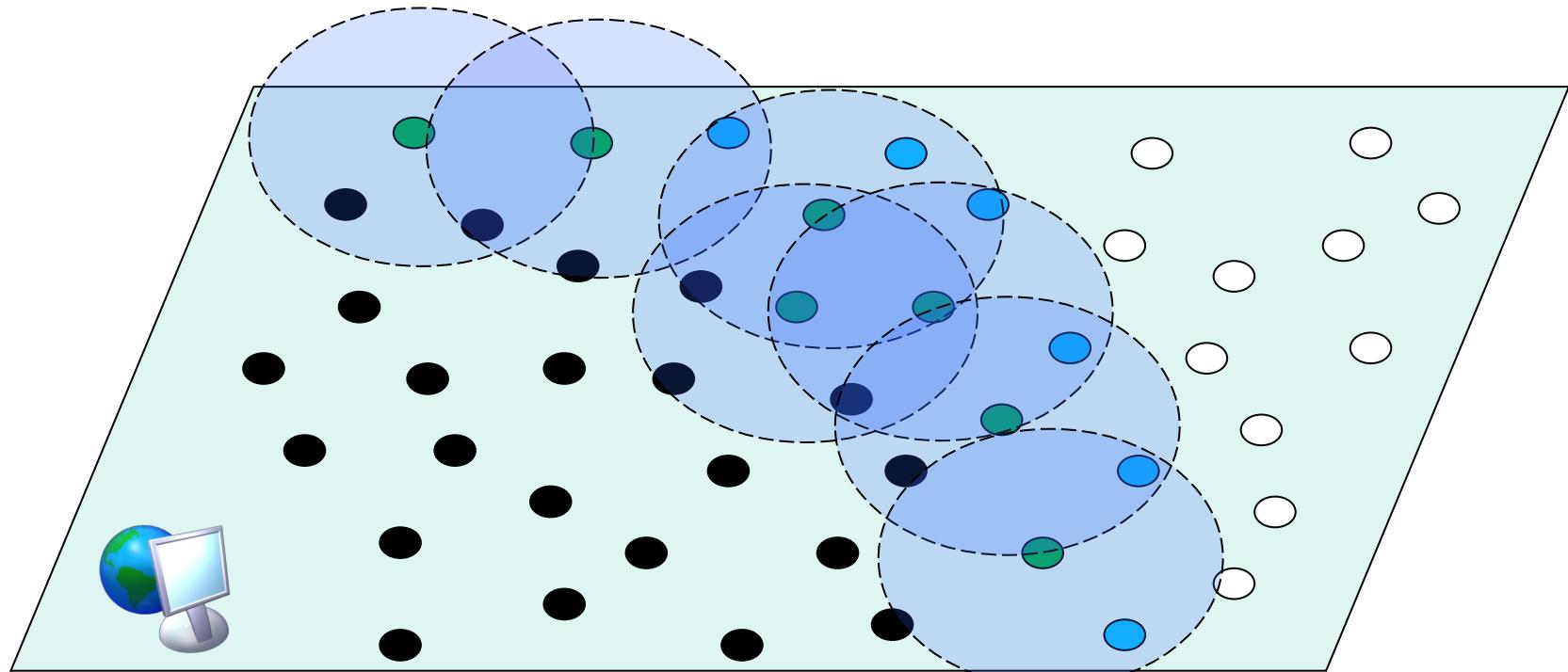
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



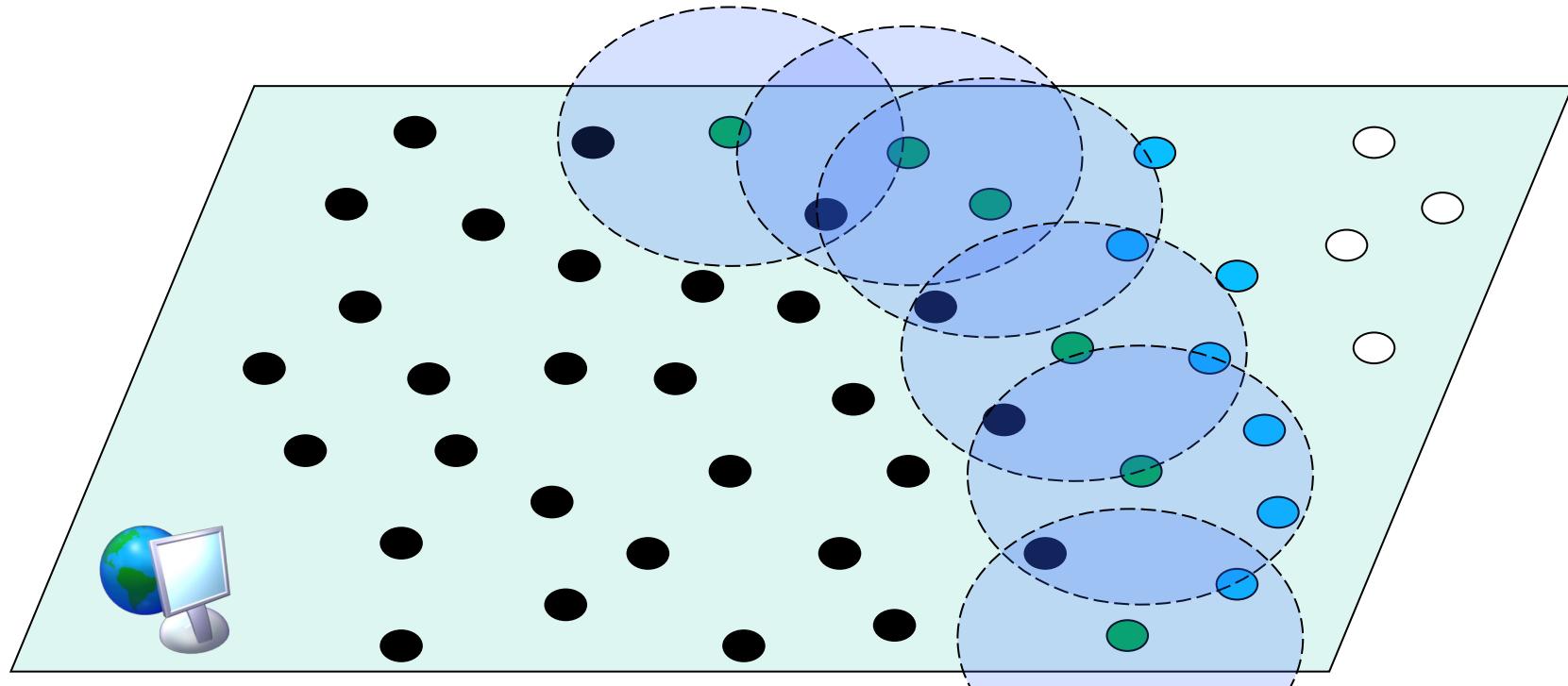
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



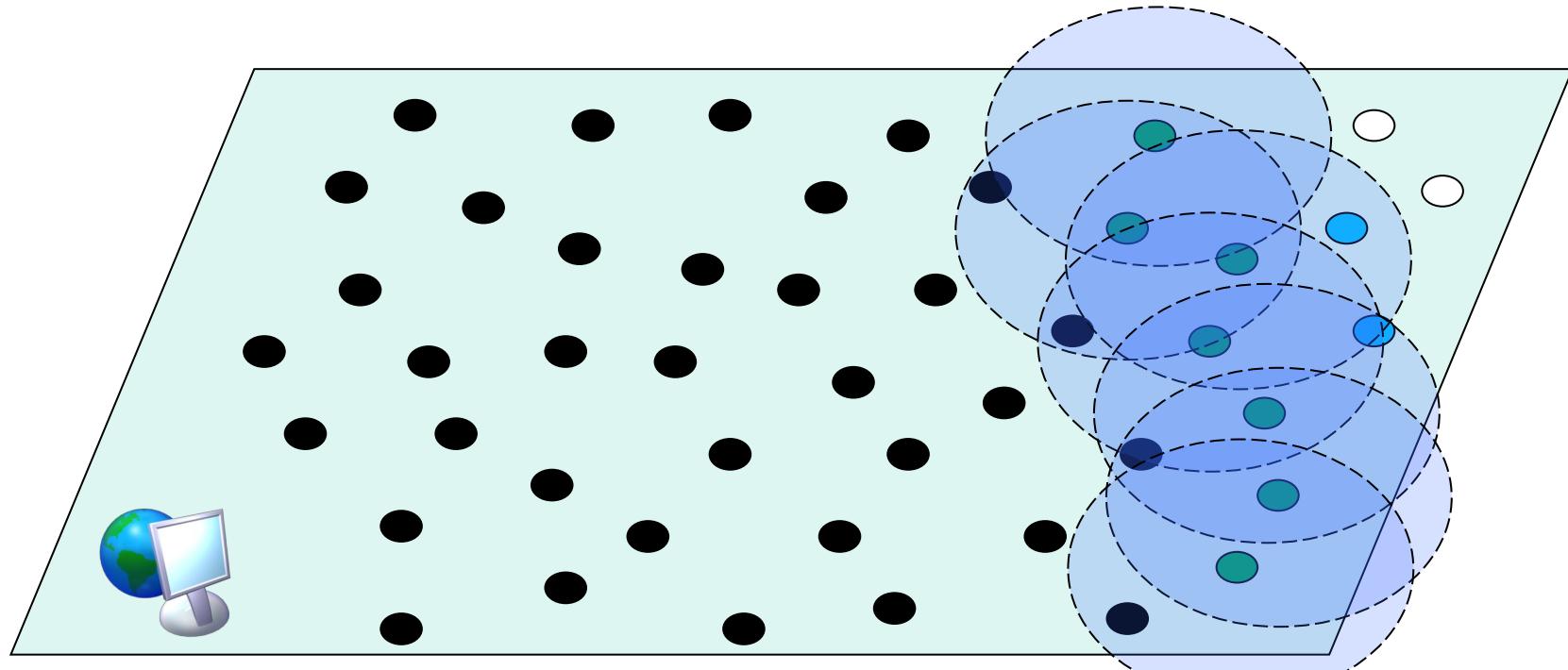
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



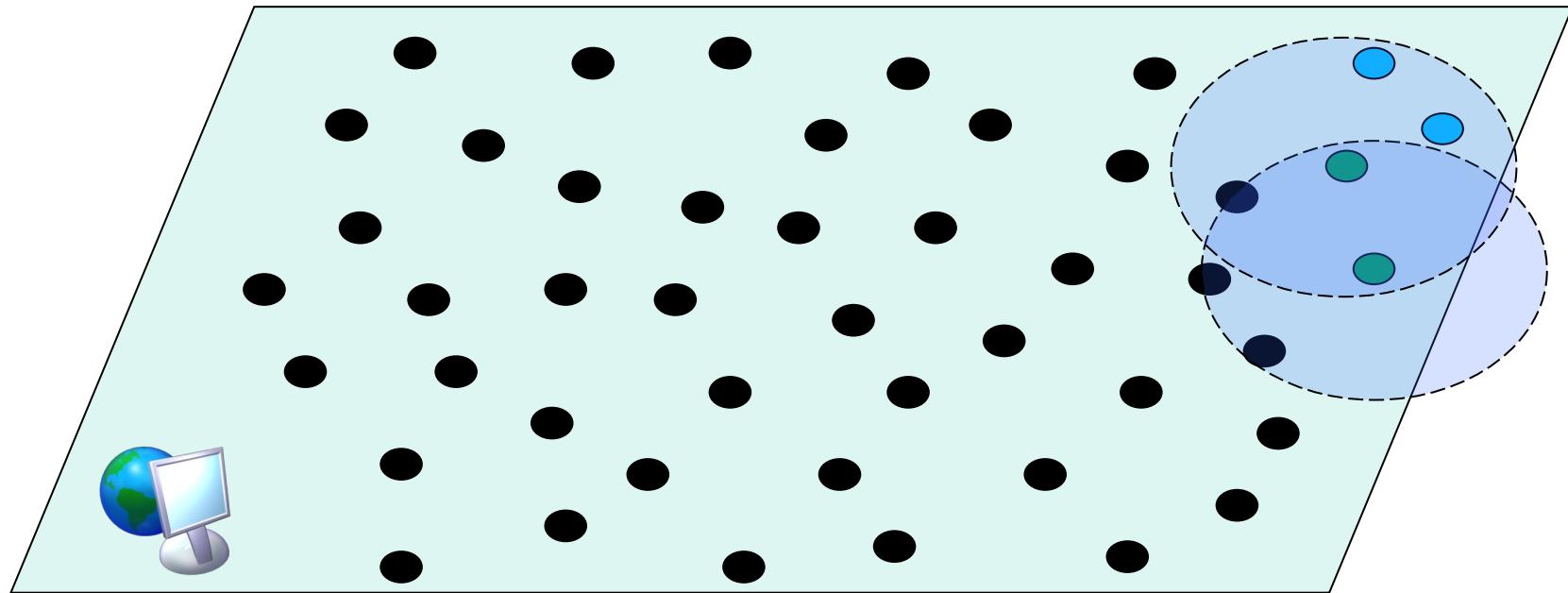
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



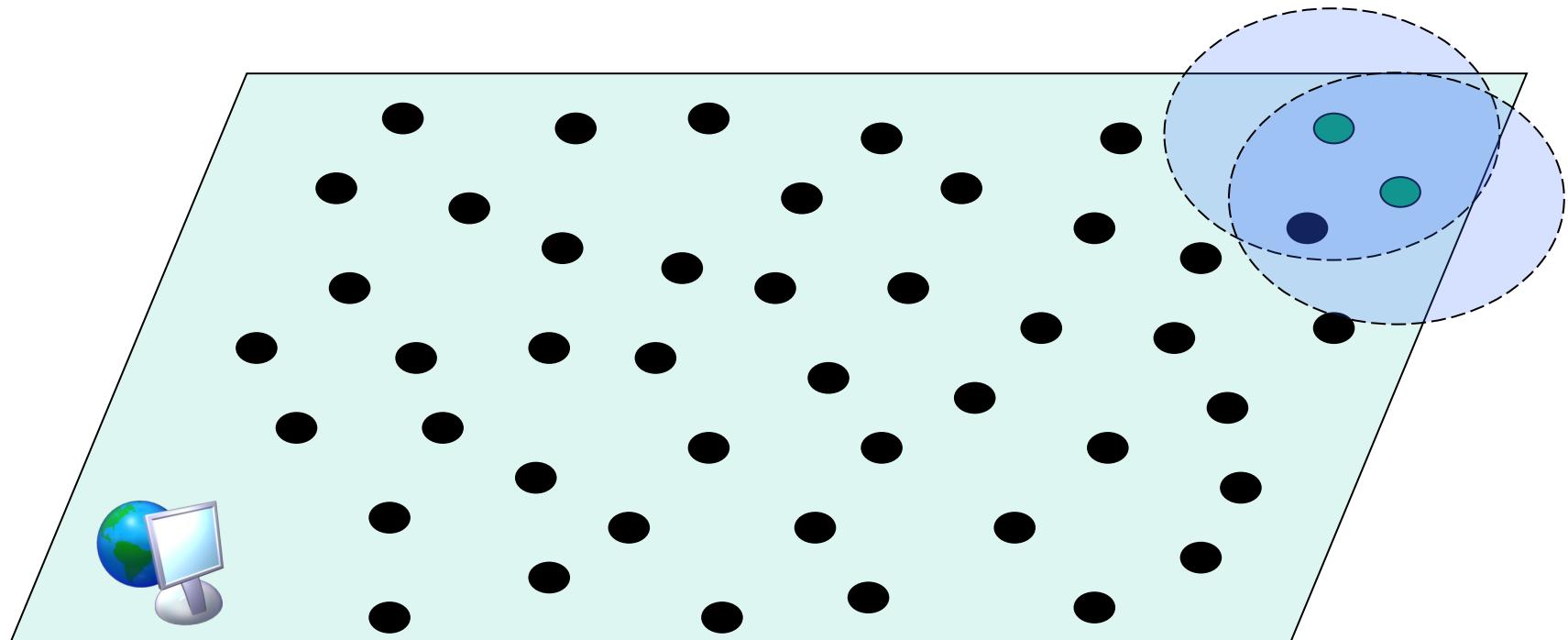
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



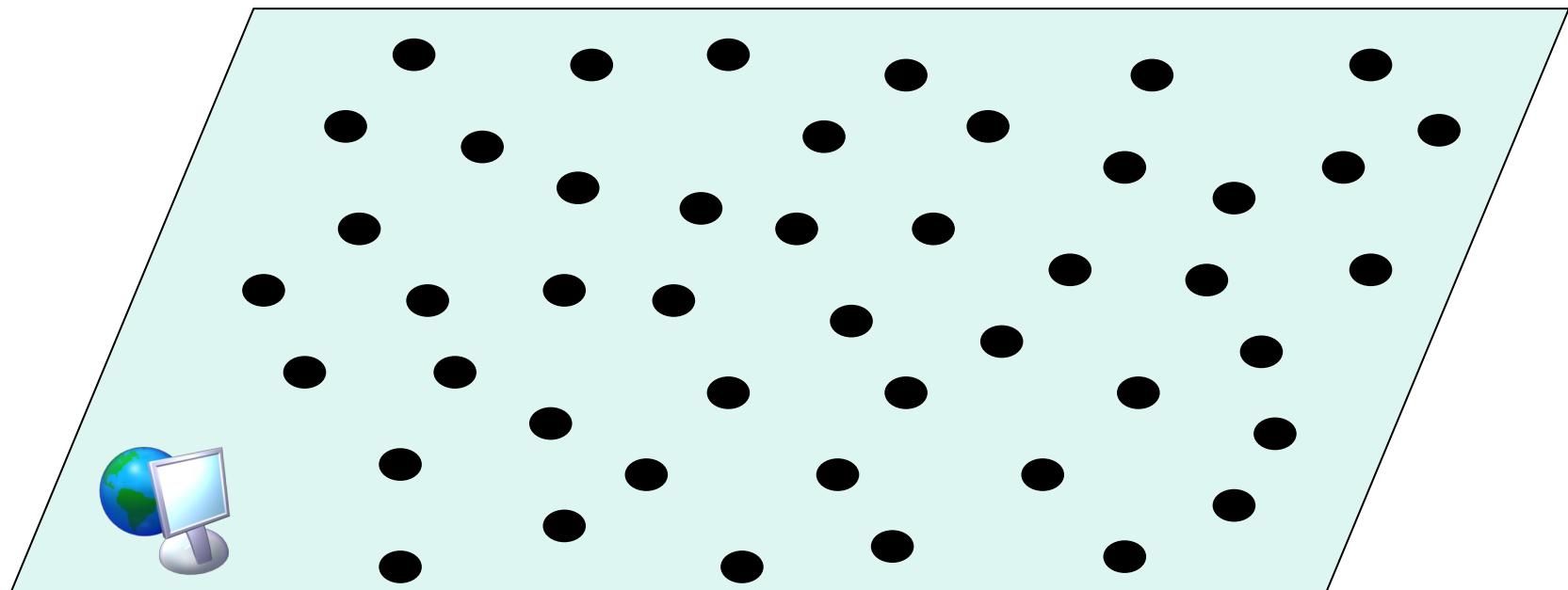
Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa



Flooding (Inundação)

- Quando um nó recebe um pacote pela primeira vez, ele programa

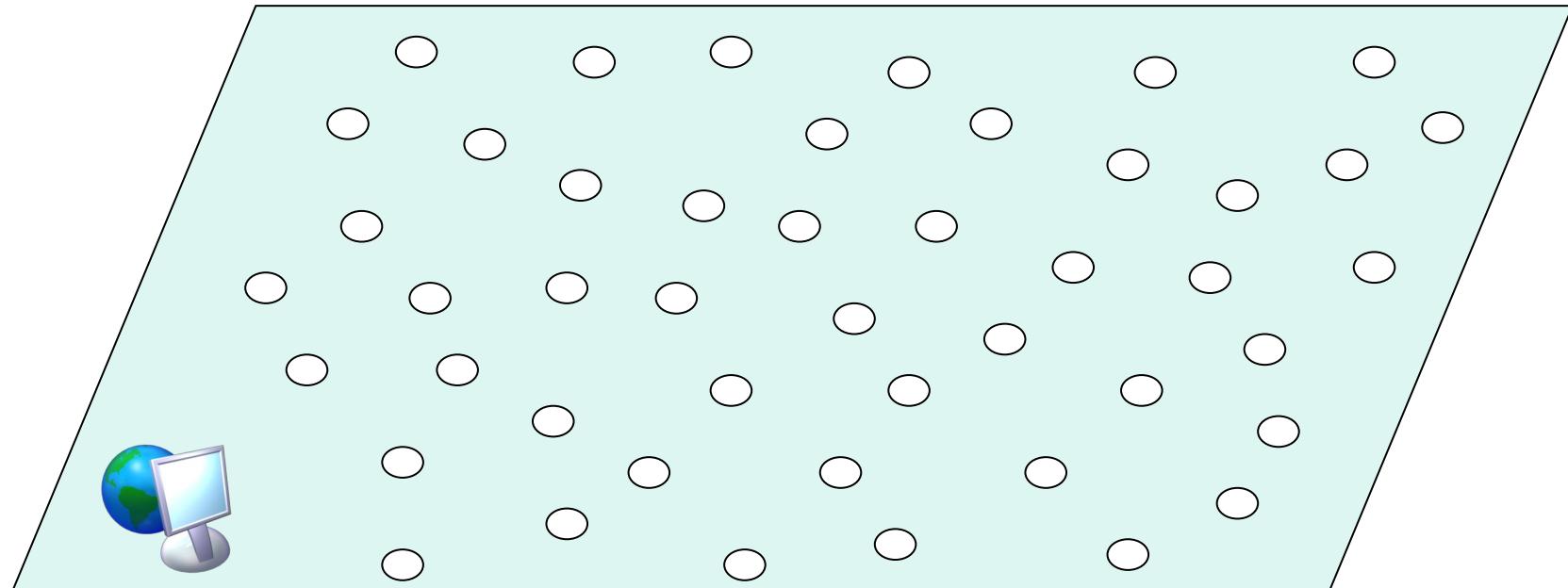


Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - **Gossiping**
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

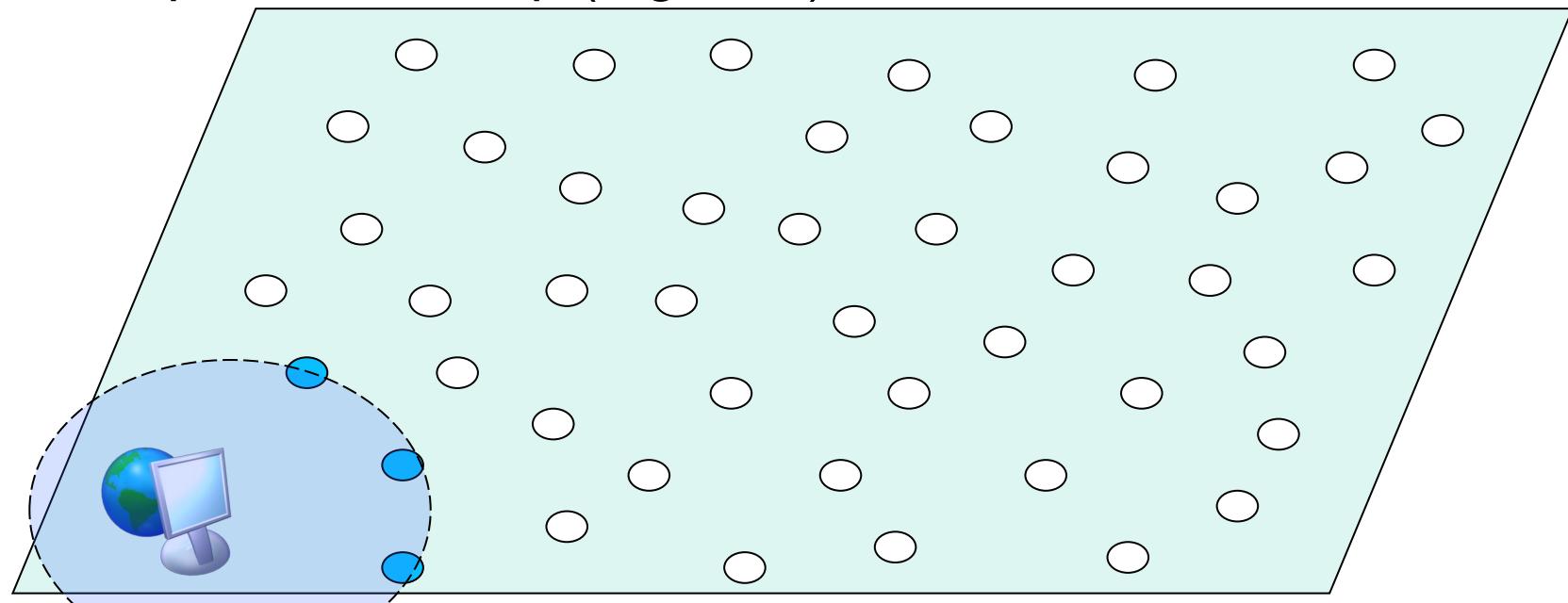
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



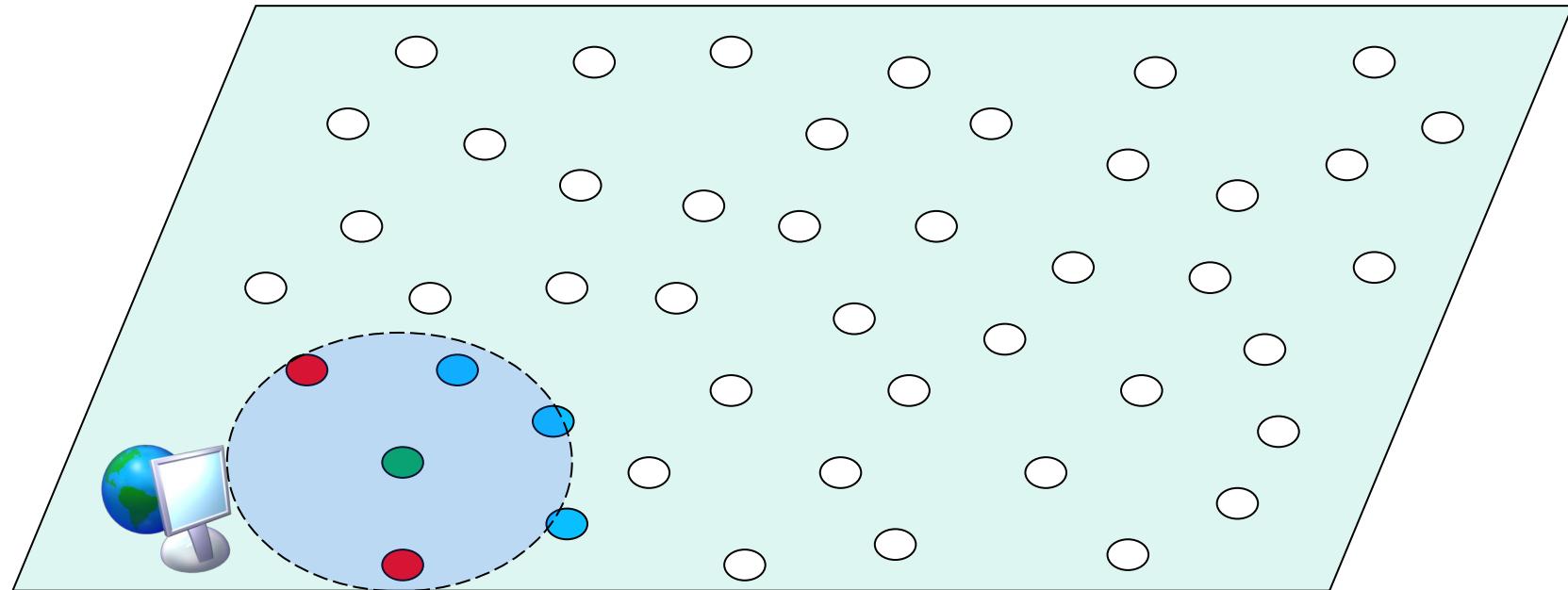
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



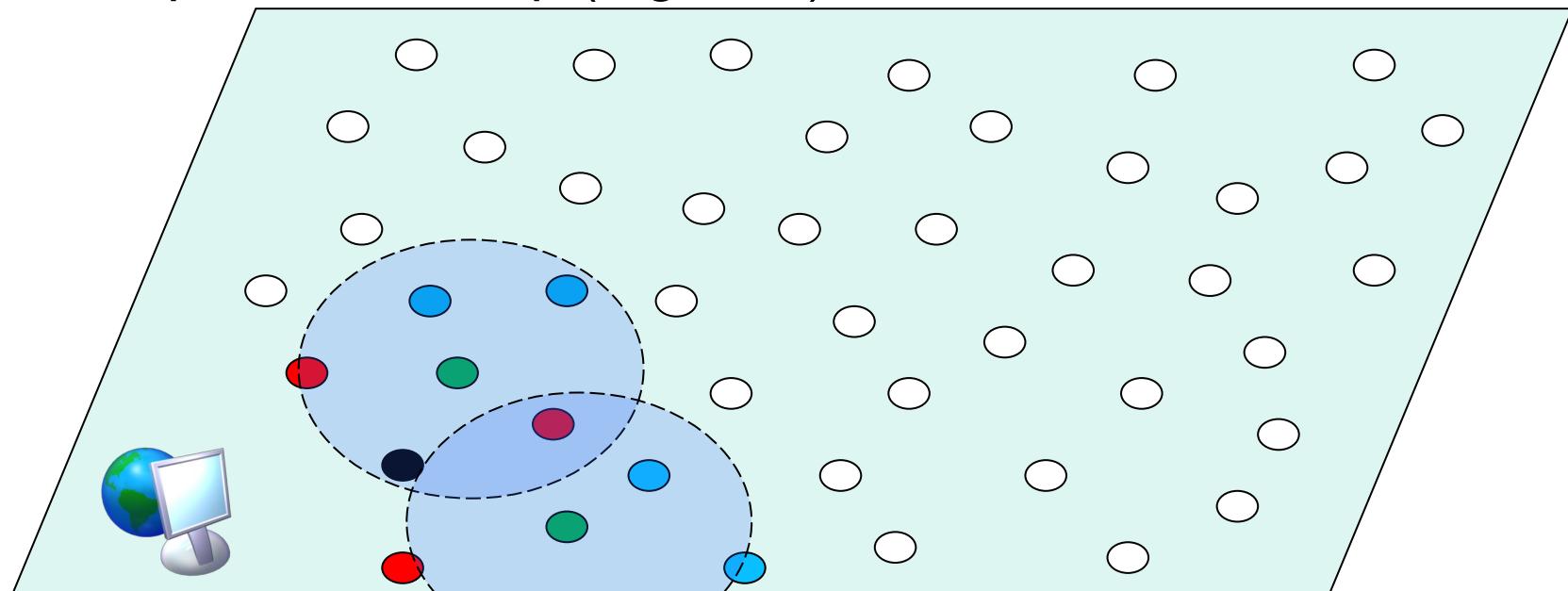
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



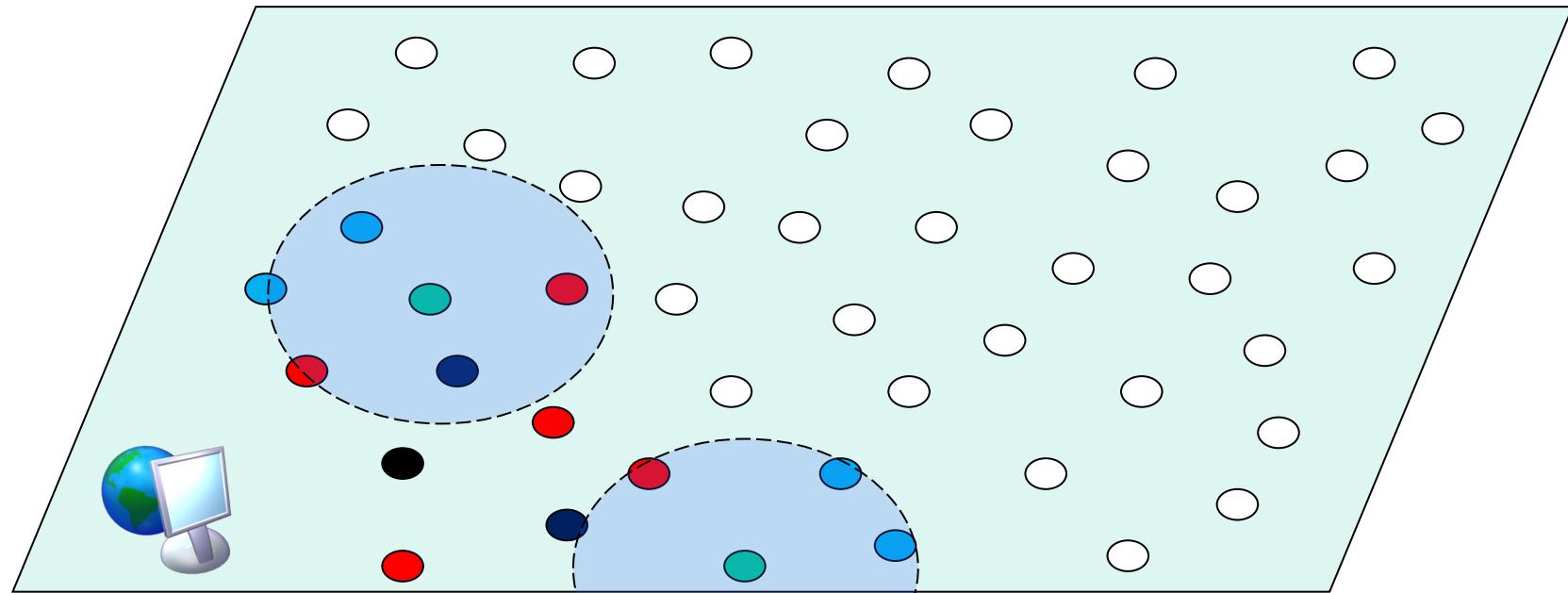
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



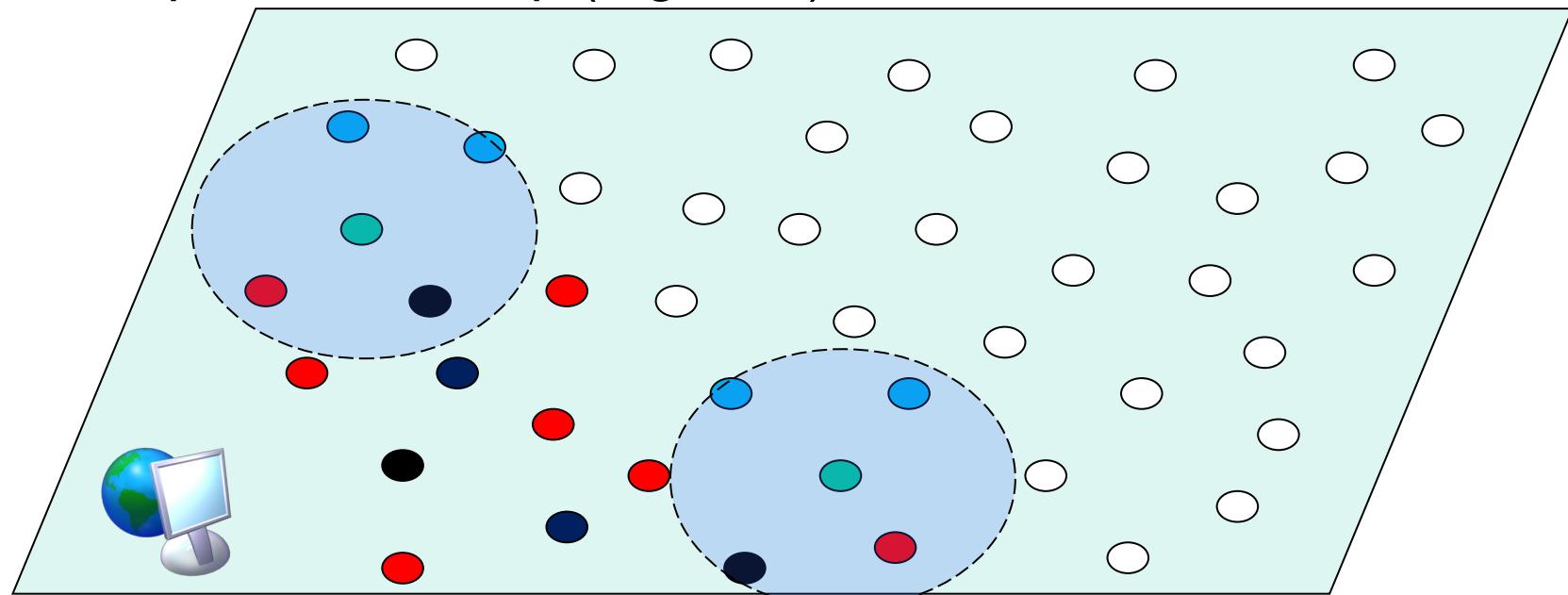
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



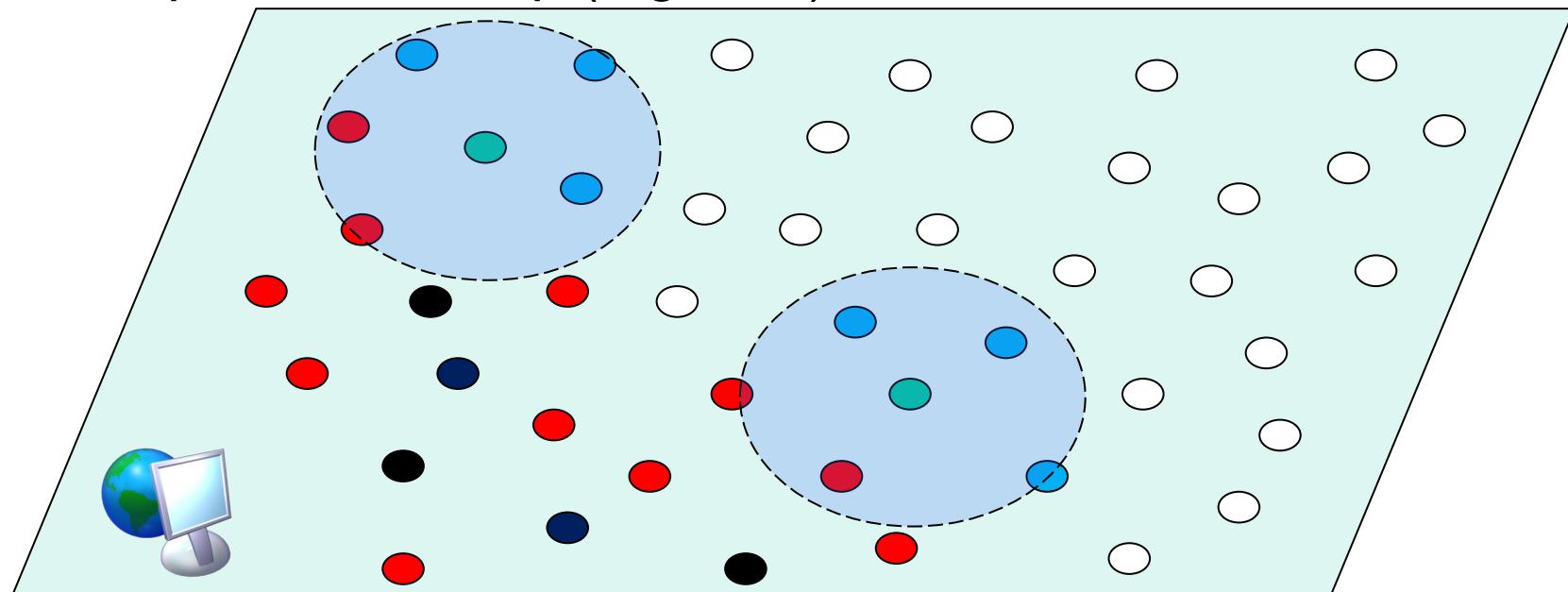
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



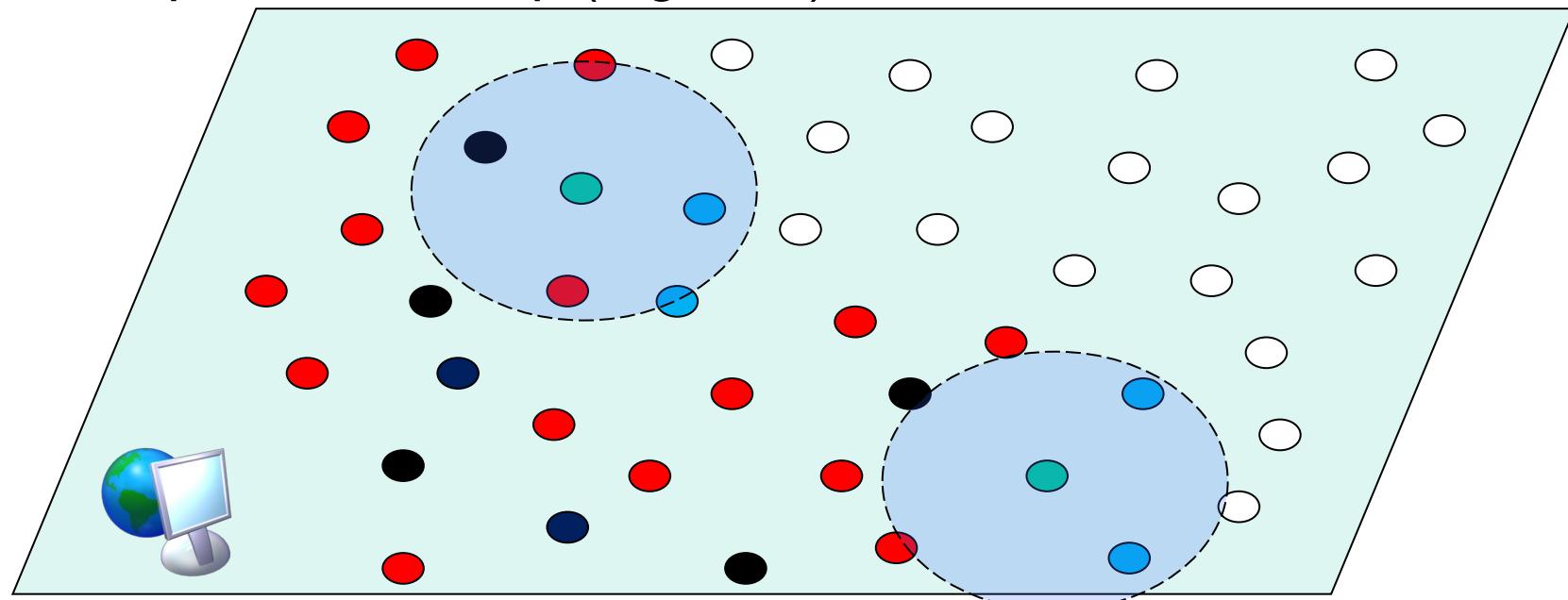
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



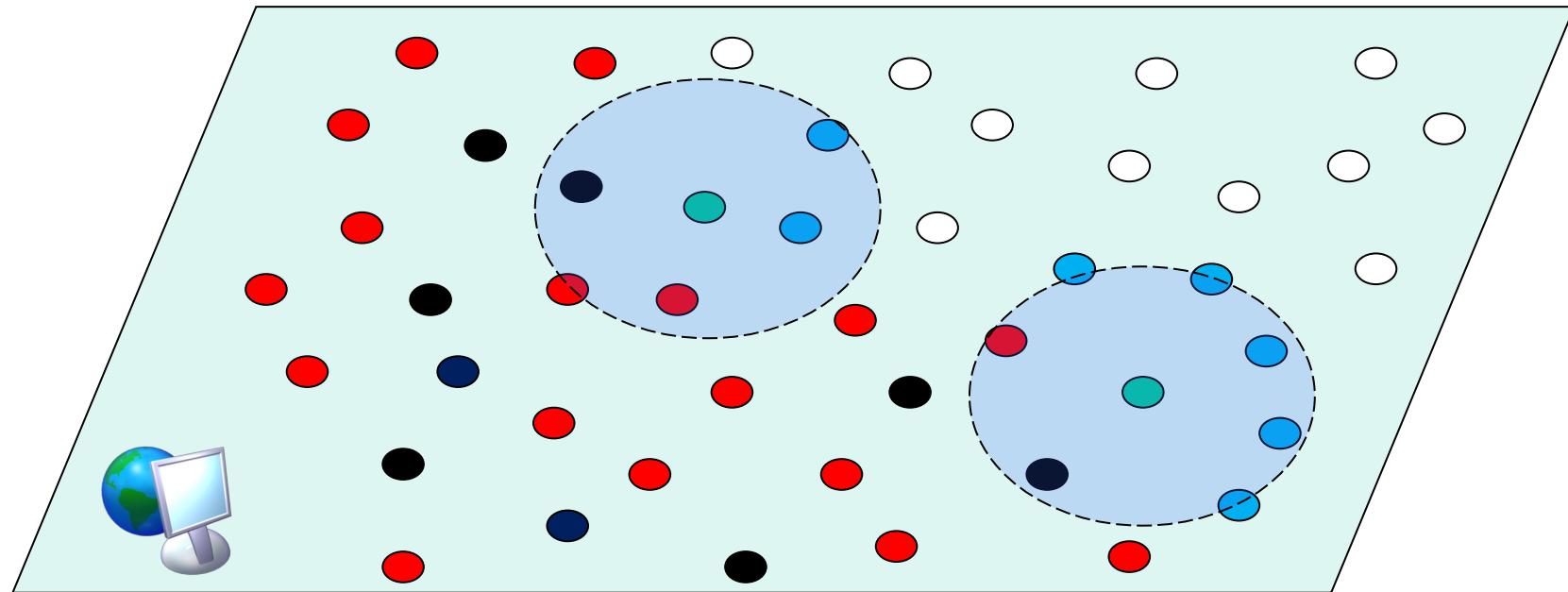
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



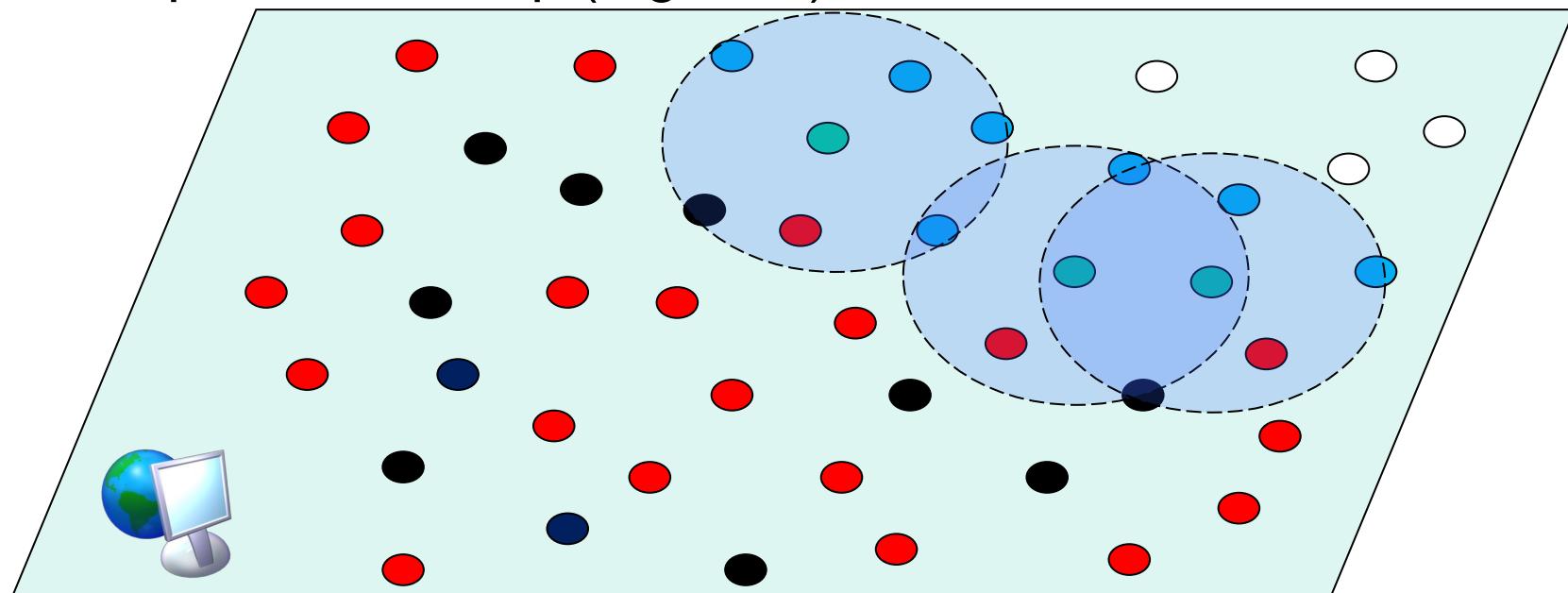
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



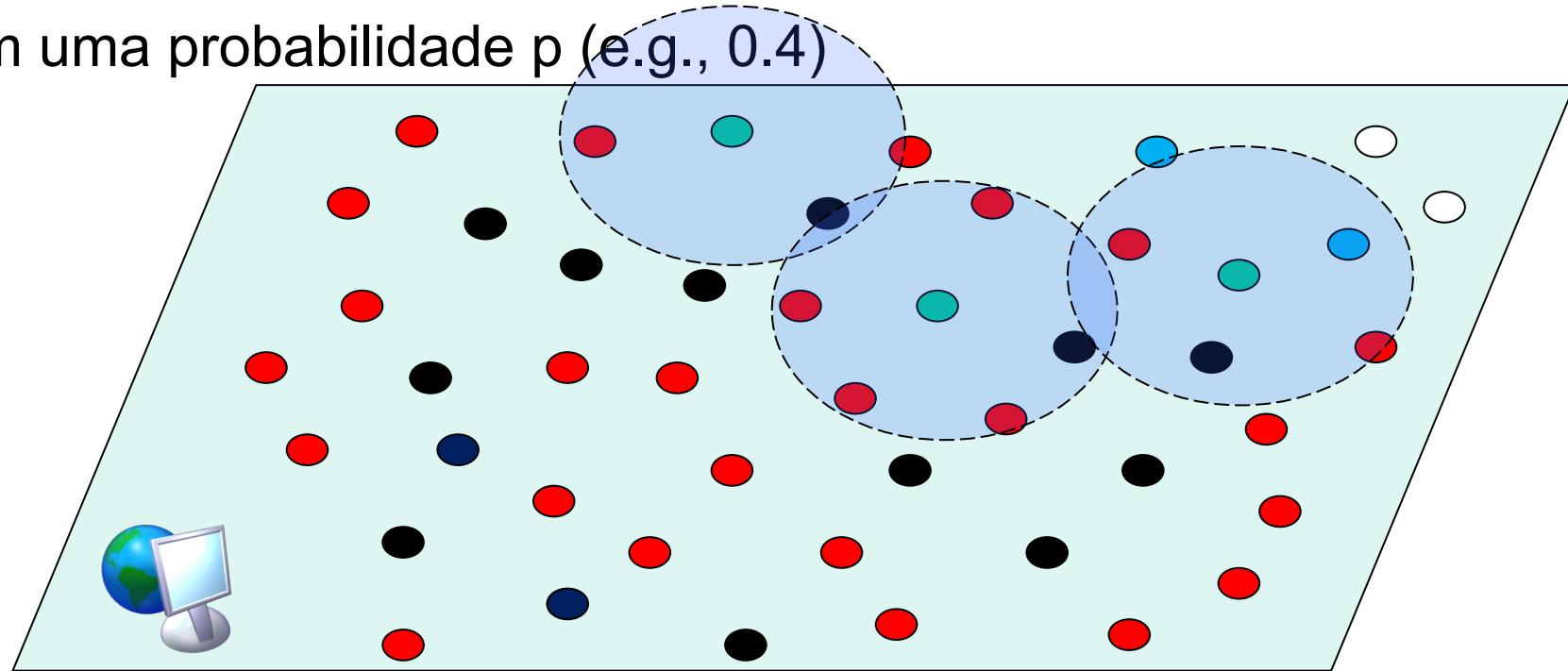
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



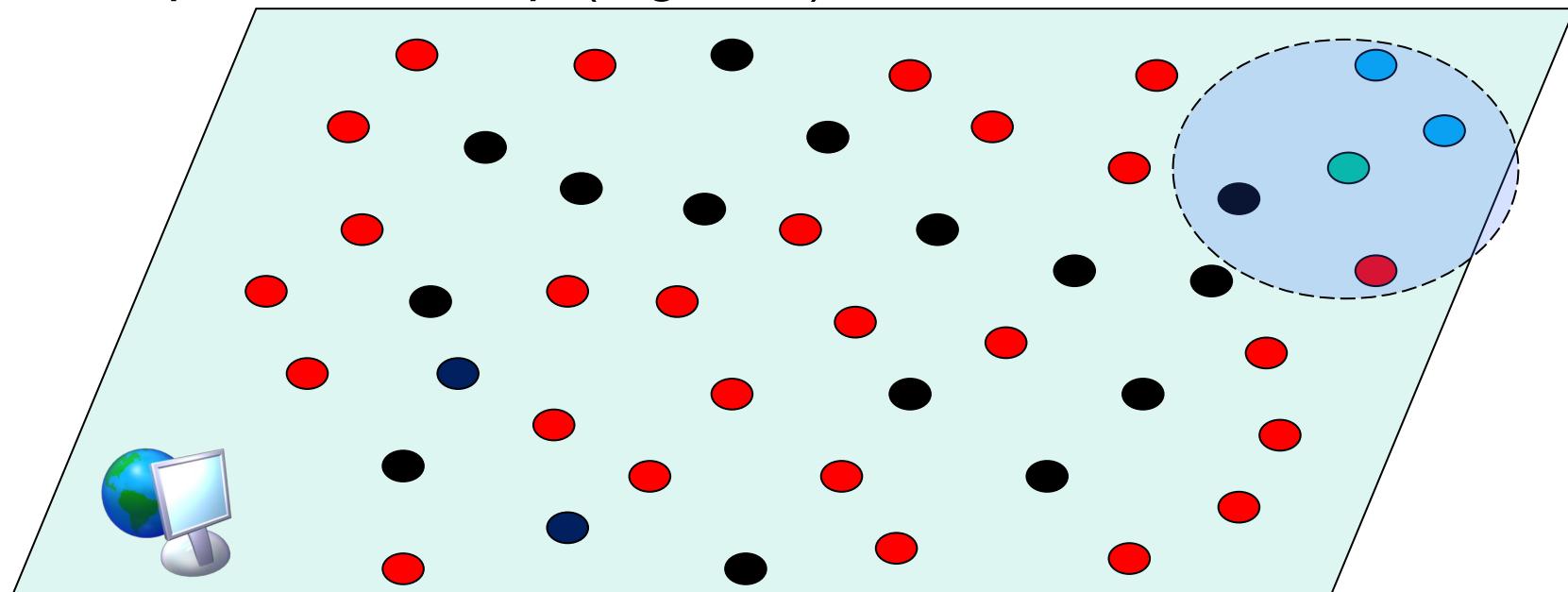
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



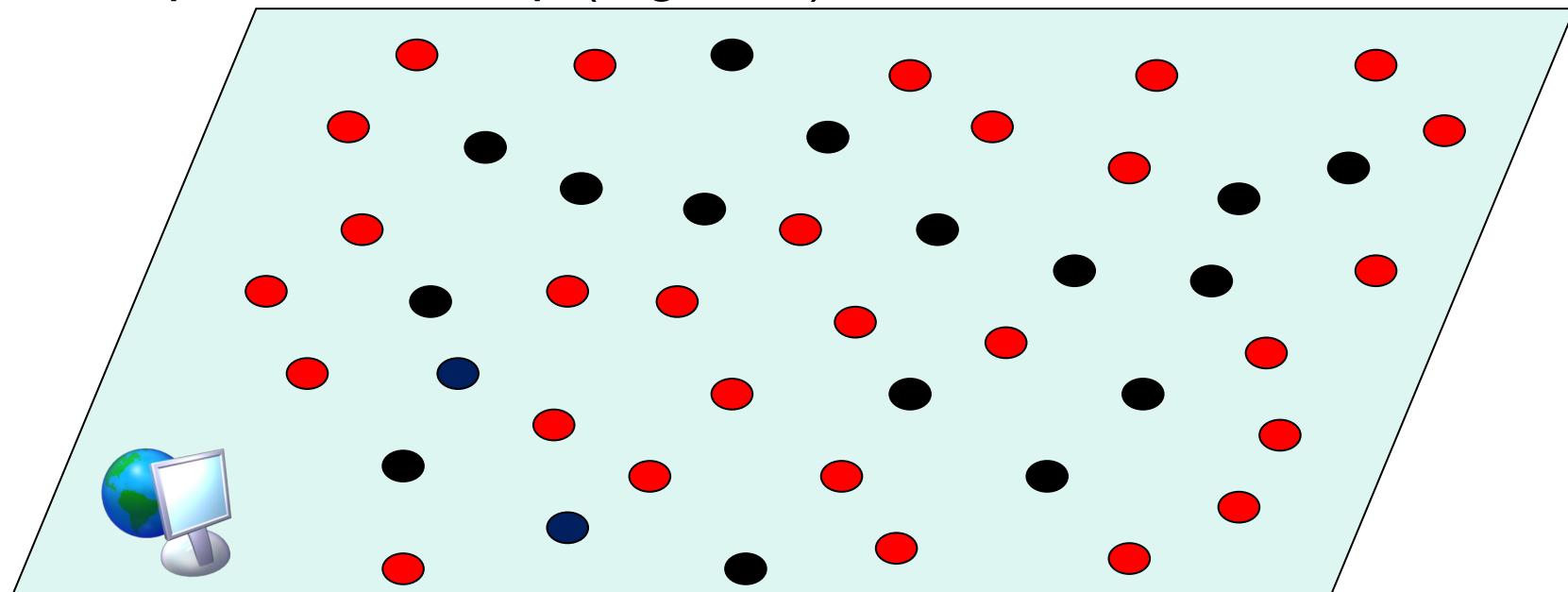
Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



Gossiping (Fofoca ou Flooding Probabilístico)

- Quando um nó recebe um pacote pela primeira vez, ele propaga com uma probabilidade p (e.g., 0.4)



Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - **Roteamento por vetor de distância**
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

Roteamento por Vetor de Distância

- Conhecido também como roteamento distribuído de Bellman-Ford ou Algoritmo de Ford-Fulkerson
- Utilizado na ARPANET até 1979 (*Routing Information Protocol, RIP*)

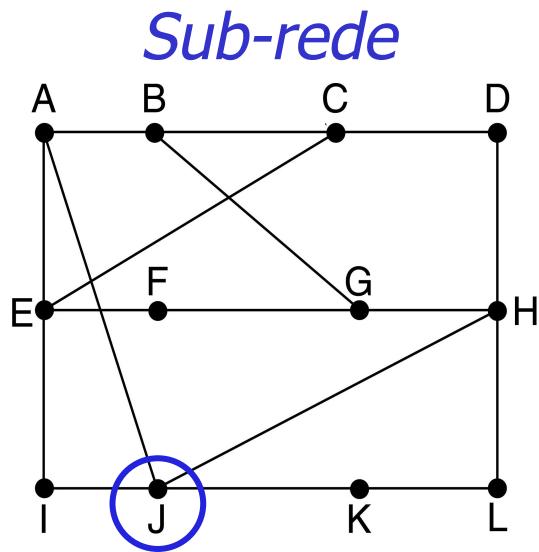
Roteamento por Vetor de Distância

- Cada roteador mantém uma tabela indexada por cada roteador da rede contendo:
 - A linha de saída preferencial a ser utilizada para esse destino
 - Estimativa do tempo ou da distância até o destino
- Cada roteador conhece a distância (e.g., número de saltos, comprimento da fila, Atraso) até cada um dos seus vizinhos

Roteamento por Vetor de Distância

- Periodicamente, cada roteador envia a cada vizinho uma lista de suas distâncias estimadas até cada destino
- Periodicamente, todos os roteadores atualizam suas tabelas utilizando as informações recebidas dos vizinhos
- A antiga tabela de roteamento não é utilizada no cálculo

Exemplo de Atualização da Tabela do Nó J



Listas recebidas

To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
JA delay				
JI delay				
JH delay				
JK delay				
is				
8				
10				
12				
6				

Vetores recebidos de quatro vizinhos de J

**Novo atraso estimado
a partir de J**

↓ Line

$$\begin{aligned} &\min(8+0, 10+24, 12+20, 6+21) \\ &\min(8+12, 10+36, 12+31, 6+28) \\ &\min(8+25, 10+18, 12+19, 6+36) \\ &\min(8+40, 10+27, 12+8, 6+24) \end{aligned}$$

...

8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	-
6	K
15	K

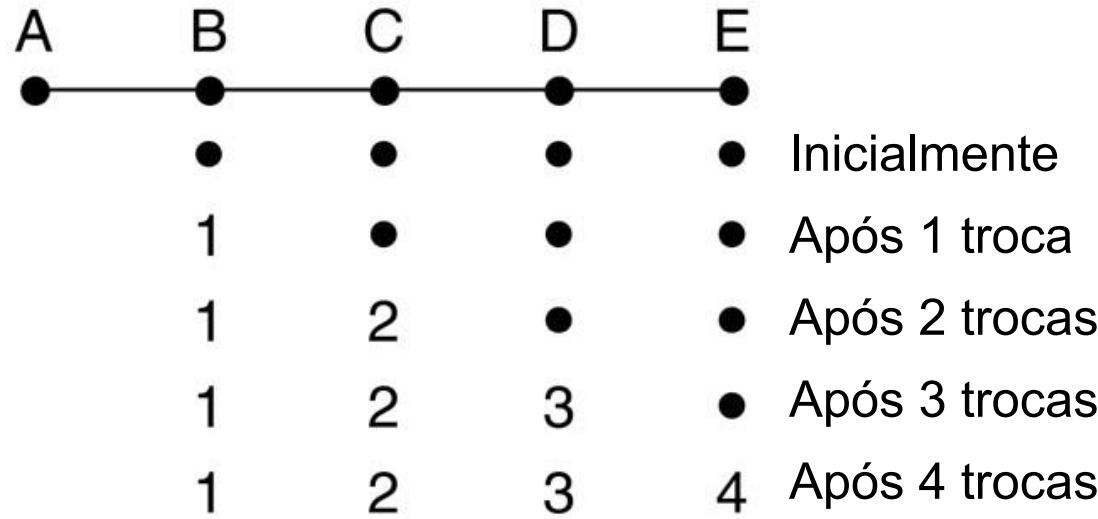
Nova tabela de J

Roteamento por Vetor de Distância

- Reage com rapidez a boas notícias, mas devagar a más notícias
- Boas notícias:
 - Um roteador A possui uma rota grande até o destino X
 - Se um vizinho B relatar uma pequena distância até X, o roteador A passará a enviar o tráfego de X para B
 - Em uma troca de vetores, a boa notícia é sempre processada

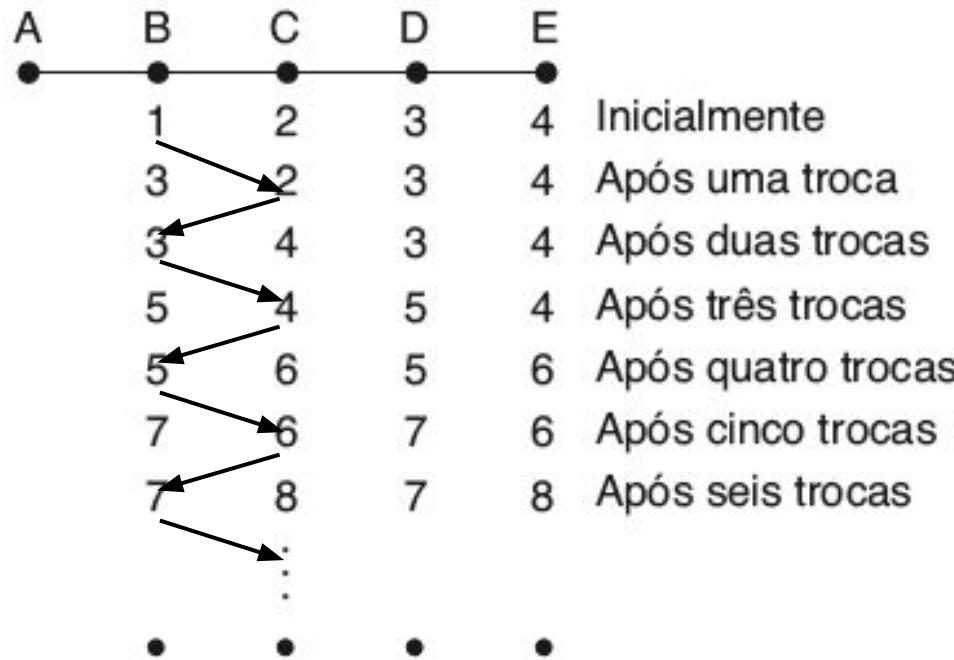
Exemplo de Boas Notícias em um Grafo de Linha

- Métrica de retardo: número de hops
- Inicialmente, A está inativo e todos os roteadores sabem disso



Exemplo de Más Notícias em um Grafo de Linha

- Inicialmente, A está ativo e a primeira linha mostra sua distância para os demais
- De repente, A é desativado e na primeira troca, B atualiza a distância de A por C



*O problema
da contagem
até o infinito*

Problema da Contagem até o Infinito

- Gradualmente, todos os roteadores seguem seu caminho até infinito
- O número de trocas necessárias depende do valor numérico utilizado para infinito
- Quando X informa a Y que tem um caminho em algum lugar, Y não tem como saber se ele próprio está no caminho

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - **Roteamento de estado de enlace**
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

Roteamento de Estado de Enlace

- Motivação: Resolver o problema de contagem até infinito do Roteamento por Vetor de Distâncias
- Substituiu o Roteamento por Vetor de Distâncias na ARPANET a partir de 1979
- Utilizado pelo OSPF

Algoritmo Atualizar Informações sobre Vizinhos

- 1) Descobrir meus vizinhos e aprender seus endereços de rede
- 2) Medir o custo (e.g., atraso) até cada um dos meus vizinhos
- 3) Criar um pacote que informe tudo o que acabei de aprender
- 4) Enviar esse pacote a todos os outros roteadores
- 5) Calcular o caminho mais curto até cada um dos outros roteadores (Dijkstra)

Algoritmo Atualizar Informações sobre Vizinhos

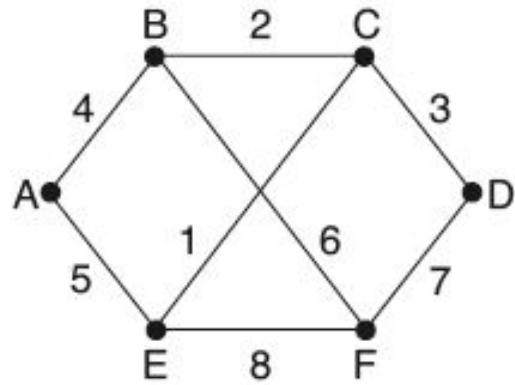
- 1) Descobrir meus vizinhos e aprender seus endereços de rede
- 2) Medir o custo (e.g., atraso) até cada um dos meus vizinhos

Para realizar essas duas etapas, os nós trocam pacotes de HELLO

O atraso pode ser calculado, por exemplo, de forma inversamente proporcional à largura de banda do enlace. Assim, a Ethernet de 1 Gbps tem custo 1 e a de 100 Mbps, custo 10

Algoritmo Atualizar Informações sobre Vizinhos

- 3) Criar um pacote que informe tudo o que acabei de aprender



Uma rede

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
TTL	TTL	TTL	TTL	TTL	TTL
B	4	B	3	A	6
E	5	C	2	C	1
		D	3	F	7
		F	1		

Pacotes de estado de enlace correspondentes a essa rede

Algoritmo Atualizar Informações sobre Vizinhos

4) Enviar esse pacote a todos os outros roteadores

Tarefa difícil e custosa em que cada nó efetua uma difusão

Algoritmo Atualizar Informações sobre Vizinhos

5) Calcular o caminho mais curto até cada um dos outros roteadores (Dijkstra)

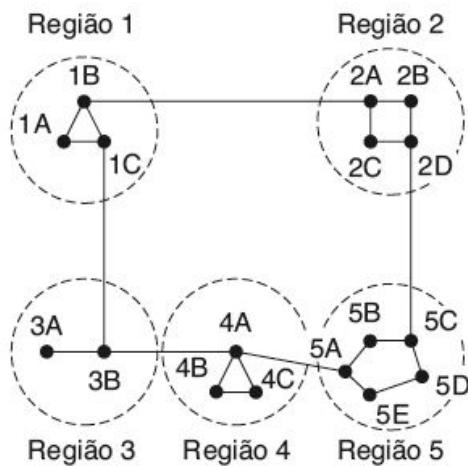
Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - **Roteamento Hierárquico**
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

Roteamento Hierárquico

- Motivação: As tabelas de roteamento crescem proporcionalmente às redes, implicando em aumento de: memória para armazenar as tabelas; CPU para processá-las; e largura de banda para transmiti-las
- As redes são organizadas por regiões e o líder de uma região não conhece a estrutura interna de outras regiões

Exemplo do Roteamento Hierárquico



Uma rede

Tabela para 1A

1A	-	-
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

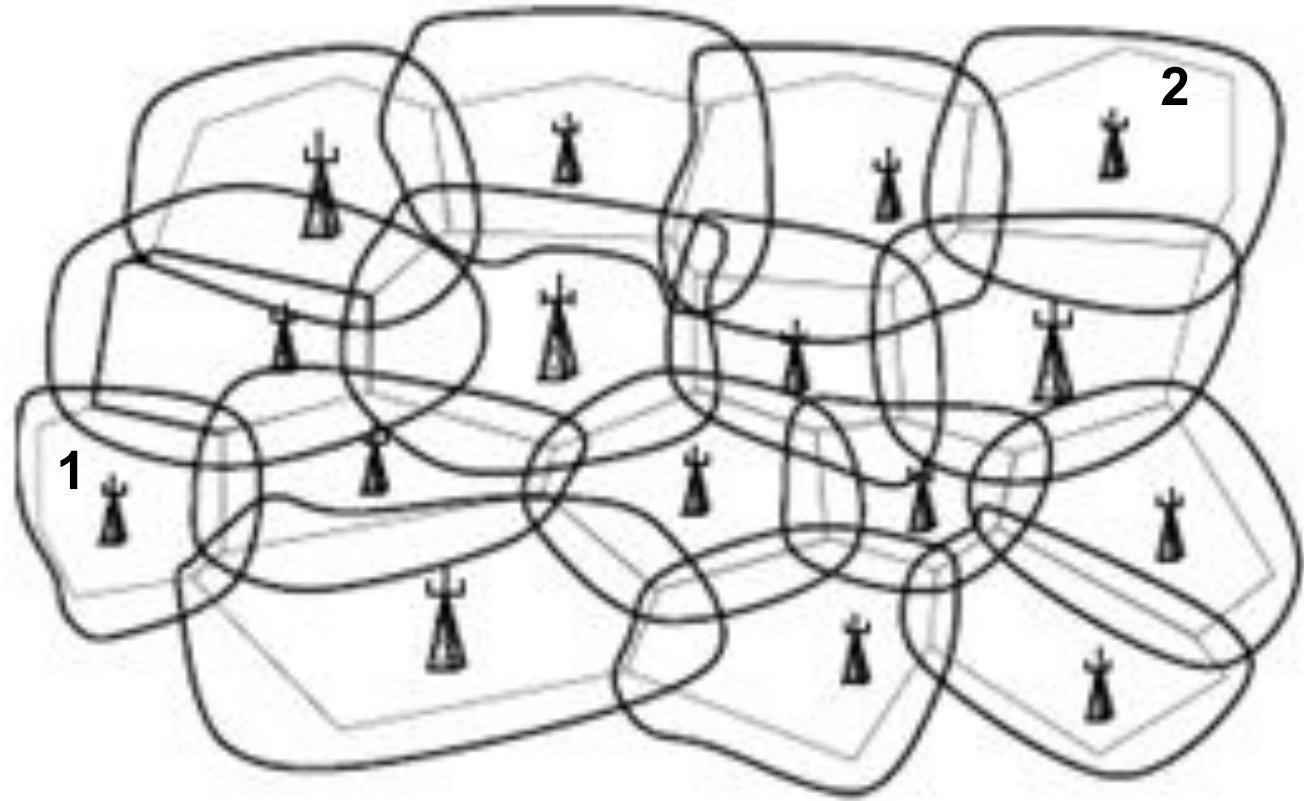
Tabela Hierárquica para 1A

1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - **Roteamento em redes infraestruturadas**
 - Roteamento em redes *ad hoc*
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

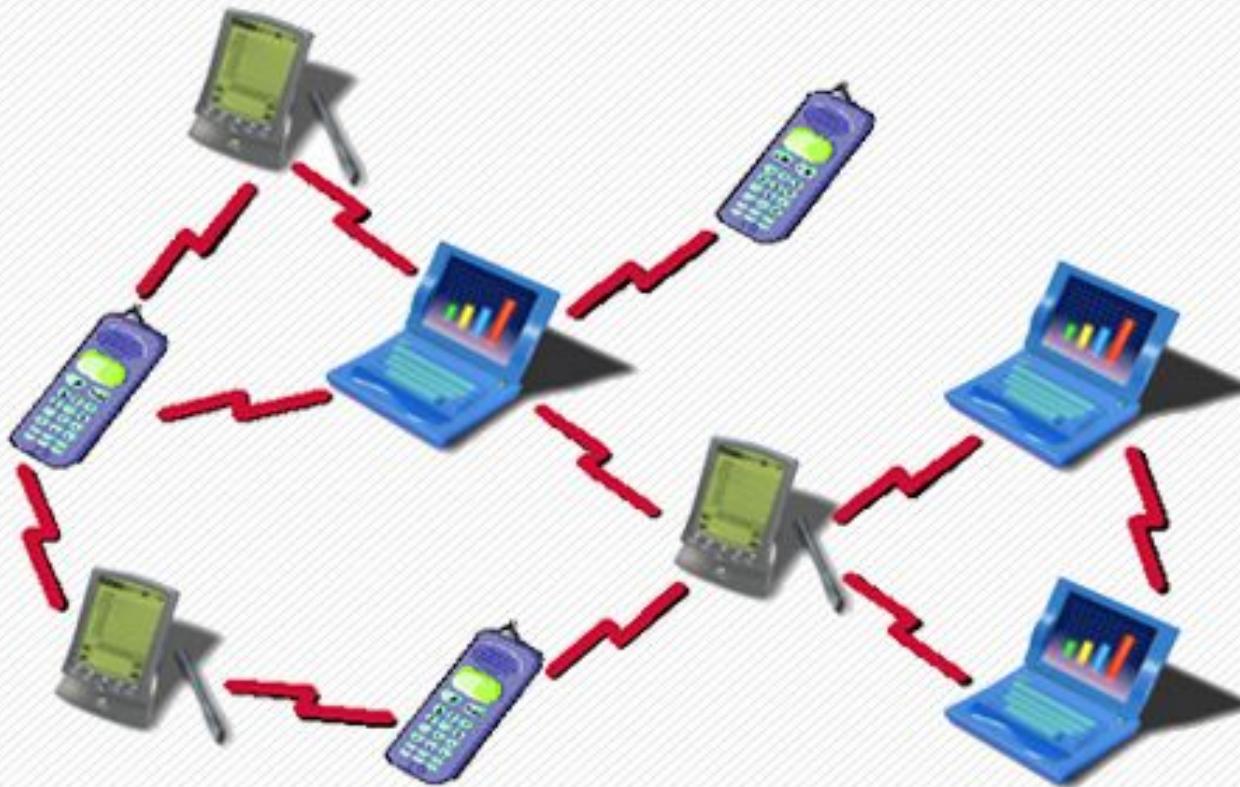
Roteamento em Redes Infraestruturadas



Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - **Roteamento em redes ad hoc**
 - Roteamento em redes *mesh*
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

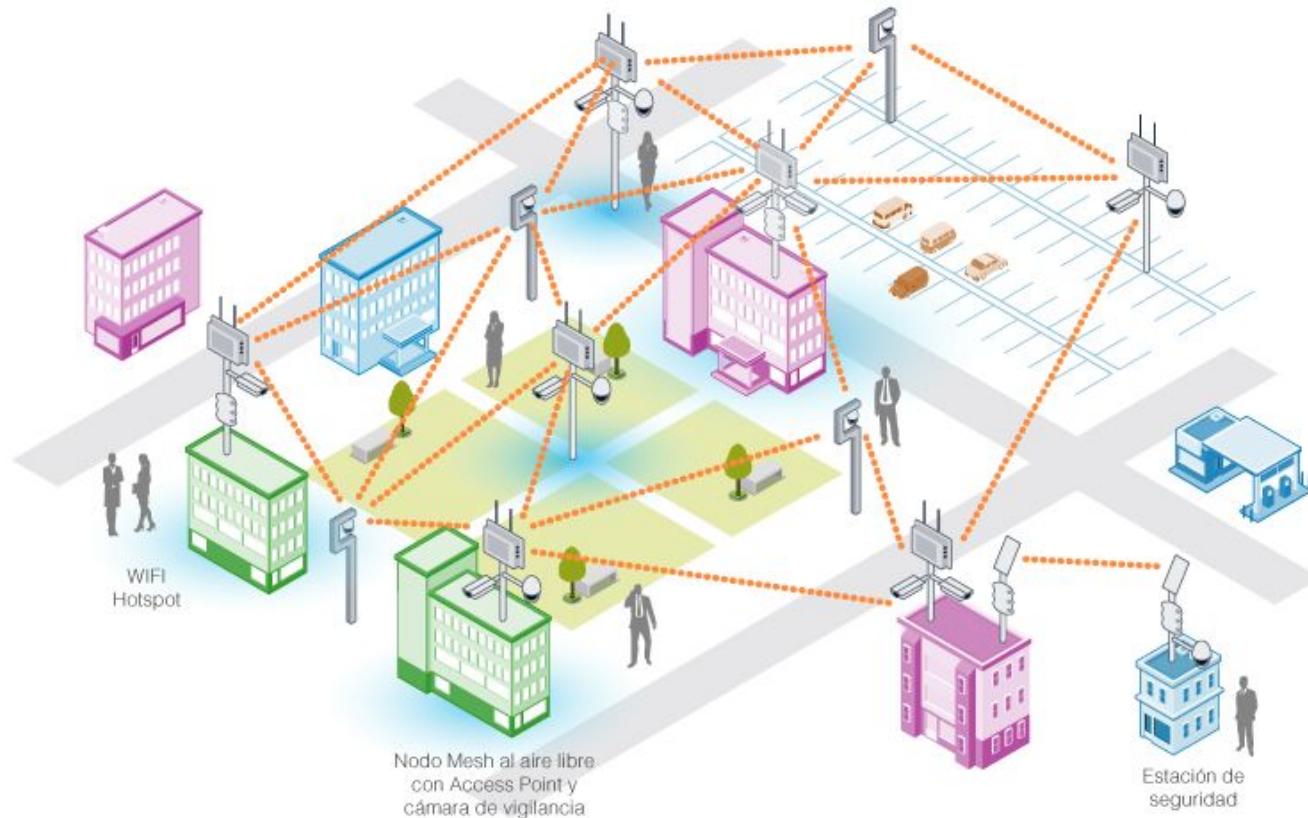
Roteamento em Redes Ad Hoc



Agenda

- Introdução
 - Questões de projeto da camada de rede
 - A camada de rede da Internet
 - *Internet Protocol v4 (IPv4)*
 - Protocolos de controle da Internet
 - **Roteamento**
 - *Internet Protocol v6 (IPv6)*
- Algoritmo do caminho mais curto
 - *Flooding*
 - *Gossiping*
 - Roteamento por vetor de distância
 - Roteamento de estado de enlace
 - Roteamento Hierárquico
 - Roteamento em redes infraestruturadas
 - Roteamento em redes *ad hoc*
 - **Roteamento em redes mesh**
- Introdução
 - **Algoritmos de Roteamento**
 - Roteamento na Internet

Roteamento em Redes Mesh



Exercício (10)

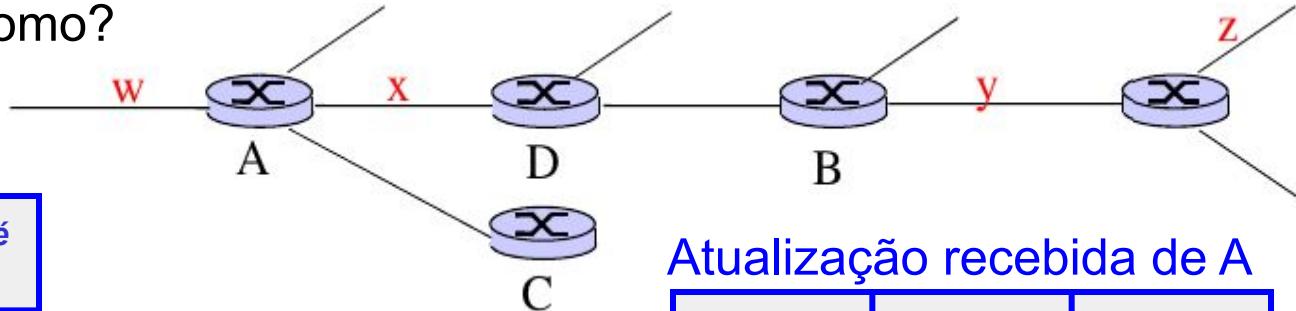
- Descreva o funcionamento básico dos algoritmos de *Flooding* e *Gossiping*

Exercício (11)

- No SA, considere a tabela do nó D e ele recebeu uma atualização de A. A tabela em D mudará? Se sim, como?

Tabela de D

<i>Rede de Destino</i>	<i>Próximo roteador</i>	<i>Saltos até destino</i>
w	A	2
y	B	2
z	B	7
x	--	1
....



Atualização recebida de A

<i>Rede de Destino</i>	<i>Próximo roteador</i>	<i>Saltos até destino</i>
w	--	1
z	C	10
x	--	1
....

Exercício (12)

- Descreva os roteamentos por vetor distância e de estado de enlace

Exercício (13)

- Descreva as redes infraestruturadas, *ad hoc* e *mesh*

Exercício (14)

- Faça um paralelo entre o roteamento em redes infraestruturadas e *ad hoc*

Agenda

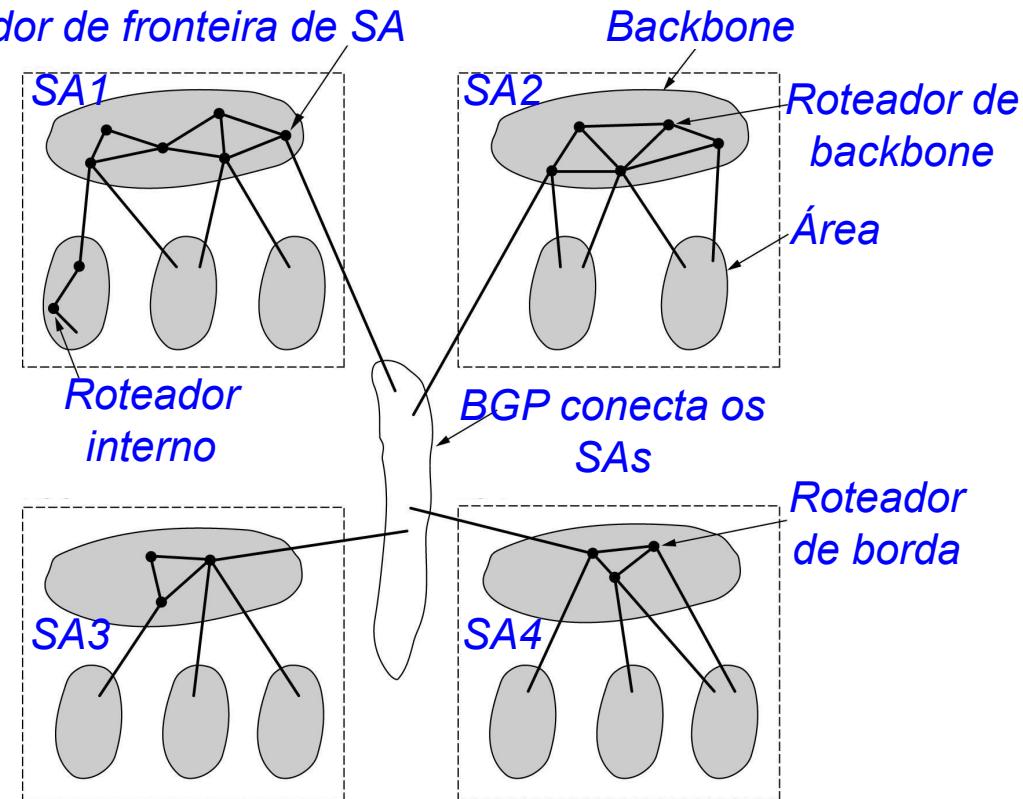
- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- **Roteamento**
- *Internet Protocol v6 (IPv6)*

- **Introdução**
- *Open Shortest Path First (OSPF)*
- *Border Gateway Protocol (BGP)*

- Introdução
- Algoritmos de Roteamento
- **Roteamento na Internet**

Internet, um Conjunto de Sistemas Autônomos (SAs)

- A Internet é formada por um grande número de SAs e cada um deles pode usar seu próprio algoritmo de roteamento interno



Protocolos de Gateway Interior vs. Exterior

- **Protocolos de gateway interior:** usados para comunicação entre roteadores dentro de um mesmo SA, **roteamento intradomínio**. Existem algumas opções de protocolos, contudo, o OSPF é o mais popular
- **Protocolos de gateway exterior:** usados para comunicação entre roteadores de SAs diferentes, **roteamento interdomínio**. Nesse caso, todas as redes usam o mesmo protocolo que, atualmente, é o BGP

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- **Roteamento**
- *Internet Protocol v6 (IPv6)*

- Introdução
- *Open Shortest Path First (OSPF)*
- *Border Gateway Protocol (BGP)*

- Introdução
- Algoritmos de Roteamento
- **Roteamento na Internet**

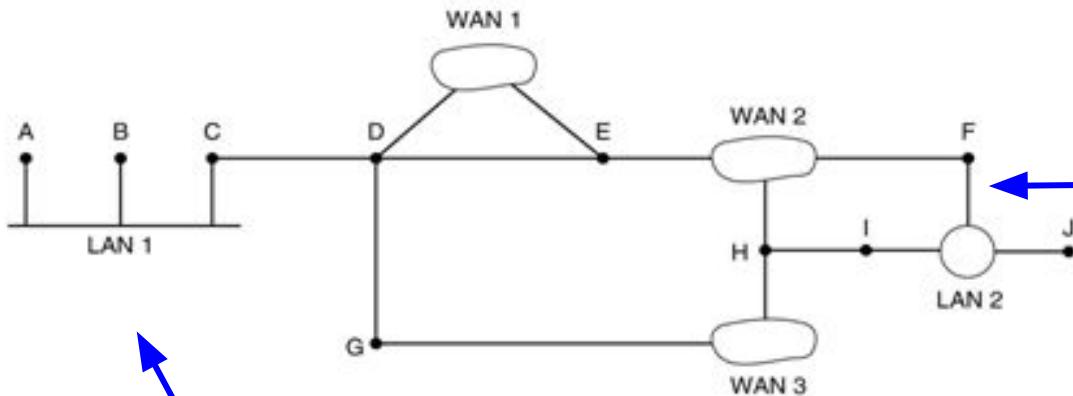
Interior Gateway Routing Protocol

- O protocolo de *gateway* interior da Internet original era um protocolo de vetor de distância, o *Routing Information Protocol* (RIP)
- Os problemas do RIP eram a contagem até infinito e convergência lenta
- Em 1990, o protocolo de estado de enlace *Open Shortest Path First* (OSPF) se tornou o protocolo de *gateway* interior padrão

Características do OSPF

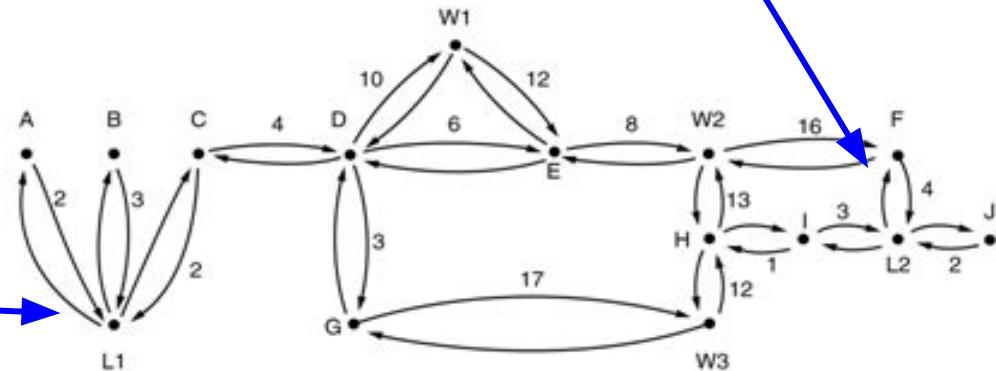
- Amplamente divulgado na literatura especializada (“open”)
- Admite várias unidades de medida de distância (retardo, distância física, etc...)
- Adapta-se de forma rápida e automática a alterações na topologia
- Admite roteamento baseado no tipo de serviço
- Faz balanceamento de carga entre caminhos múltiplos de igual custo
- Possui suporte para hierarquia dentro de um único domínio de roteamento
- Segurança: as trocas entre os roteadores podem ser autenticadas
- Possui suporte para tunelamento

Representação da Rede com Grafo Orientado

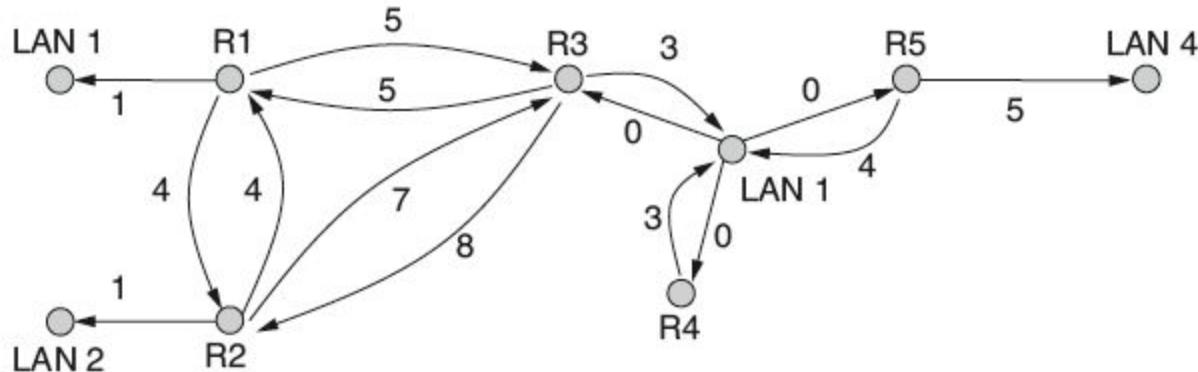
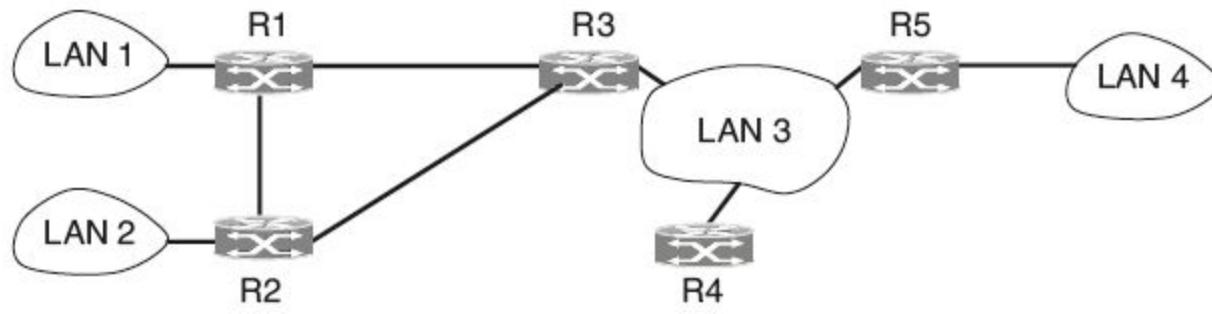


Conexão ponto-a-ponto vira par de arestas bidirecional

Rede difusão vira vértice
conectado com cada *host*



Sistema Autônomo e seu Grafo Representativo

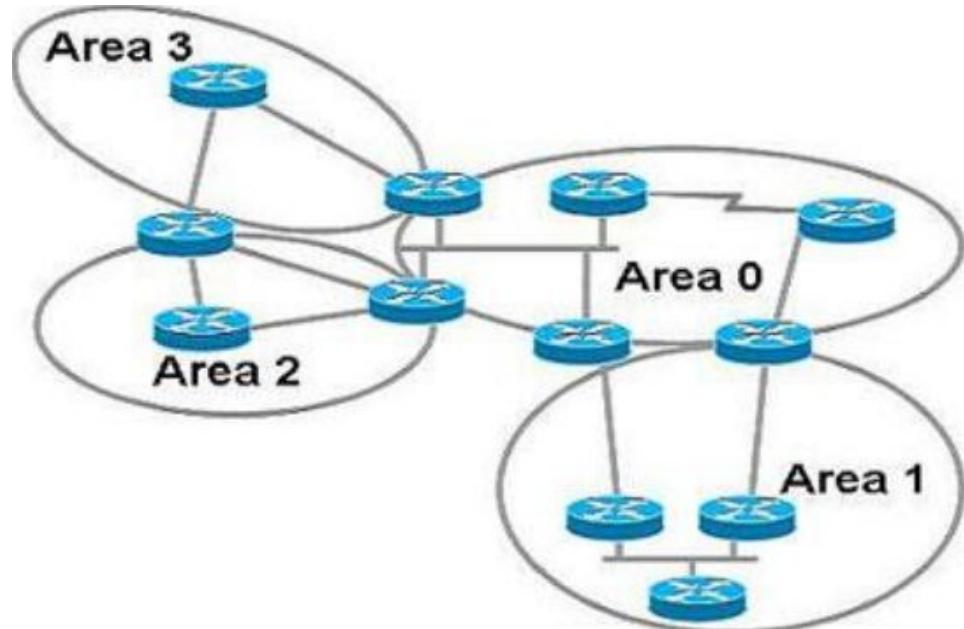


Funcionamento Básico

- Aplica o algoritmo estado de enlace para atualizar as tabelas de vizinhos
 - Cada *host* envia suas informações para todos os outros do SA
 - Atualizações acontecem quando houver uma mudança no estado de enlace ou periodicamente (30 segundos)
- Aplica Dijkstra para encontrar o caminho mais curto
- ***Equal Cost MultiPath (ECMP)***: Quando dois roteadores tiverem múltiplos caminhos mais curtos, todos são lembrados, proporcionando um balanceamento de carga

Hierarquização

- Grandes SAs podem ser divididos em áreas numeradas onde cada área representa uma rede ou mais redes
- Roteadores da mesma área executam o algoritmo de roteamento de estado de enlace



Hierarquização

- Áreas não se sobrepõem nem precisam ser completas
- Eventualmente, um roteador não pertence a uma área
- Fora de uma área, a topologia e os detalhes da sub-rede não são visíveis
- Dentro de cada área, um ou mais roteadores de borda são responsáveis pelo roteamento de pacotes para fora da área
- Um roteador que se conecta a duas áreas armazena o banco de dados de ambas e executa o algoritmo de caminho mais curto para cada uma delas separadamente

Backbone

- Responsável por rotear o tráfego entre as outras áreas do sistema autônomo
- Denominado área 0 do sistema autônomo
- Tem conexão com todas as áreas
- Sempre contém todos os roteadores de borda de área que estão dentro do SA

Roteamento Interárea Dentro do SA

- Pacote é roteado até um roteador de borda de área (roteamento intra-área)
- Em seguida, o pacote é roteado por meio do *backbone* até o roteador de borda de área da área de destino
- Por fim, o pacote é roteado até seu destino final

Cinco Tipos de Mensagens

Tipo de mensagem	Descrição
Hello	Usada para descobrir quem são os vizinhos
Link state update	Oferece os custos do transmissor aos seus vizinhos
Link state ack	Confirma a atualização do estado de enlace
Database description	Anuncia quais atualizações o transmissor tem
Link state request	Solicita informações do parceiro

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- **Roteamento**
- *Internet Protocol v6 (IPv6)*

- Introdução
- *Open Shortest Path First (OSPF)*
- *Border Gateway Protocol (BGP)*

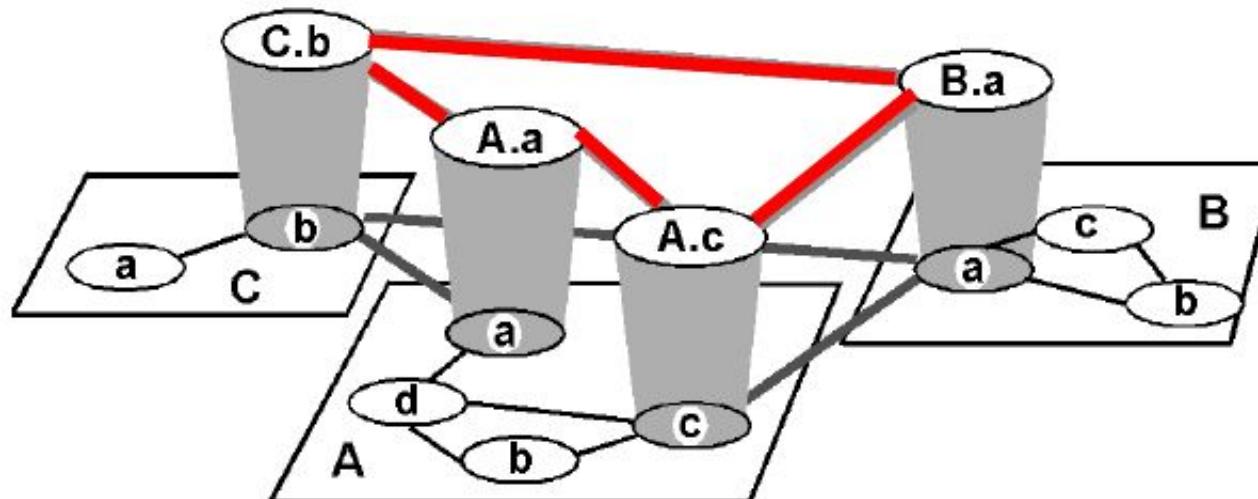
- Introdução
- Algoritmos de Roteamento
- **Roteamento na Internet**

Objetivos de Protocolos de *Gateway* Interior vs. Exterior

- Protocolos de *gateway* interior precisam movimentar pacotes da origem até o destino da forma mais eficiente possível
- Protocolos de *gateway* exterior devem se preocupar com política, por exemplo:
 - Nenhum tráfego deve passar por certos SAs
 - Nunca colocar o Iraque em uma rota que comece no Pentágono
 - Não usar os Estados Unidos para ir da Colúmbia Britânica até Ontário
 - Só passar pela Albânia se não houver outra alternativa para chegar ao destino
 - O tráfego que começar ou terminar na IBM não deve transitar pela Microsoft

Border Gateway Protocol (BGP)

- A Internet consiste de SAs e nas linhas que os conectam
- Dois SAs são considerados conectados se existe uma linha entre roteadores de borda de cada um deles

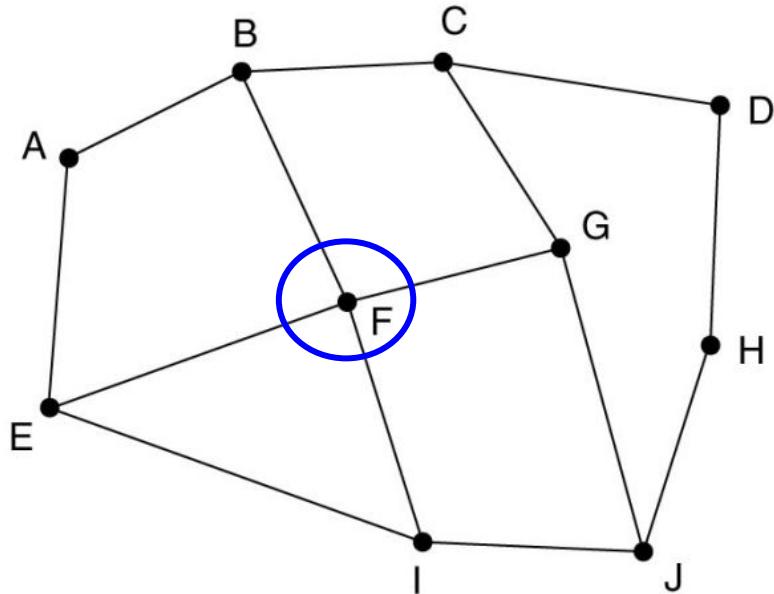


Funcionamento Básico

- Pares de roteadores BGP se comunicam entre si estabelecendo conexões TCP
- Utiliza o Roteamento por Vetor de Distâncias
 - Ao invés de manter apenas o custo para cada destino, cada roteador BGP tem controle de qual caminho está sendo usado
 - Em vez de fornecer periodicamente a cada vizinho apenas o custo estimado para cada destino possível, o roteador BGP informa a seus vizinhos o caminho exato que está usando

Exemplo da Tabela de Roteamento de F

- F descarta caminhos que passam por ele ou que violam alguma restrição política.
Após os descartes, o roteador F adota as rotas mais curtas



*Informações sobre D que F
recebe de seus vizinhos:*

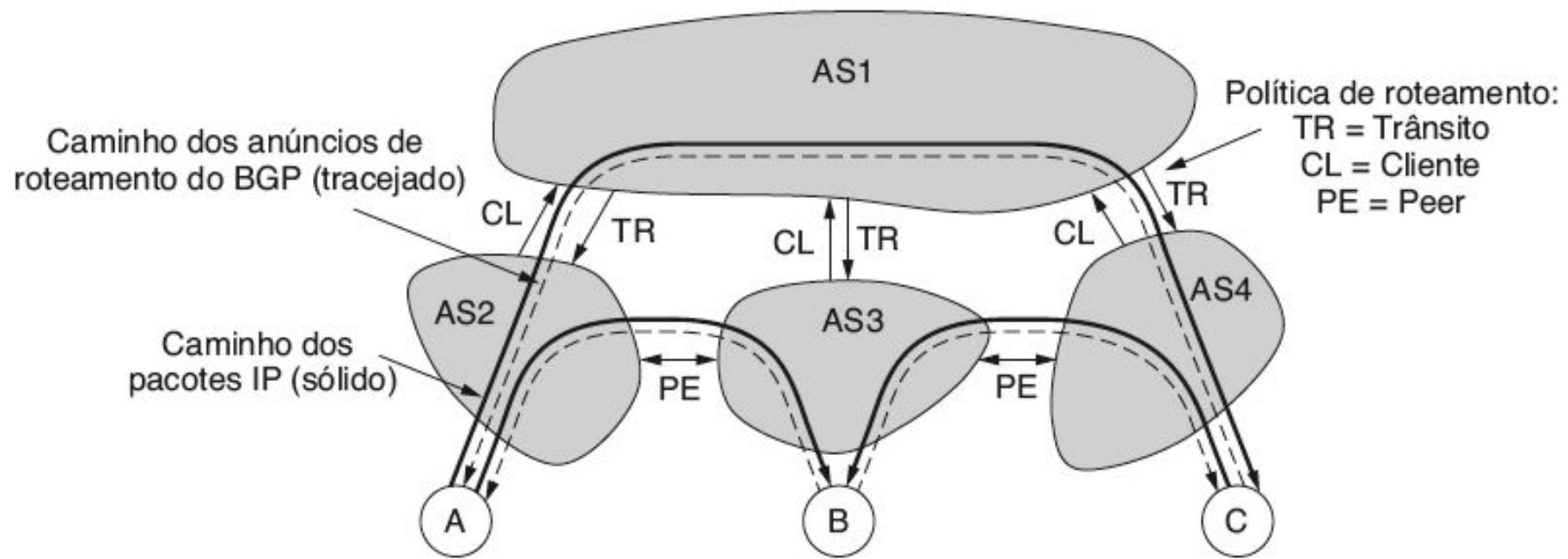
De B: "Eu utilizo BCD"

De G: "Eu utilizo GCD"

De I: "Eu utilizo IFGCD" (descartado)

De E: "Eu utilizo EFGCD" (descartado)

Trânsito e Peering



Classificação das Redes

- **Redes stub**: possuem apenas uma conexão com o grafo BGP, logo, não podem ser usadas para tráfego porque não há “outro” lado
- **Redes multiconectadas**: podem ser usadas para tráfego, a menos que se recusem
- **Redes de trânsito**: tem como objetivo tratar pacotes de terceiros

Exercício (15)

- Como o BGP resolve o problema da contagem até infinito que atinge outros algoritmos de Roteamento por Vetor de Distâncias?

Agenda

- Introdução
- Questões de projeto da camada de rede
- A camada de rede da Internet
- *Internet Protocol v4 (IPv4)*
- Protocolos de controle da Internet
- Roteamento
- ***Internet Protocol v6 (IPv6)***

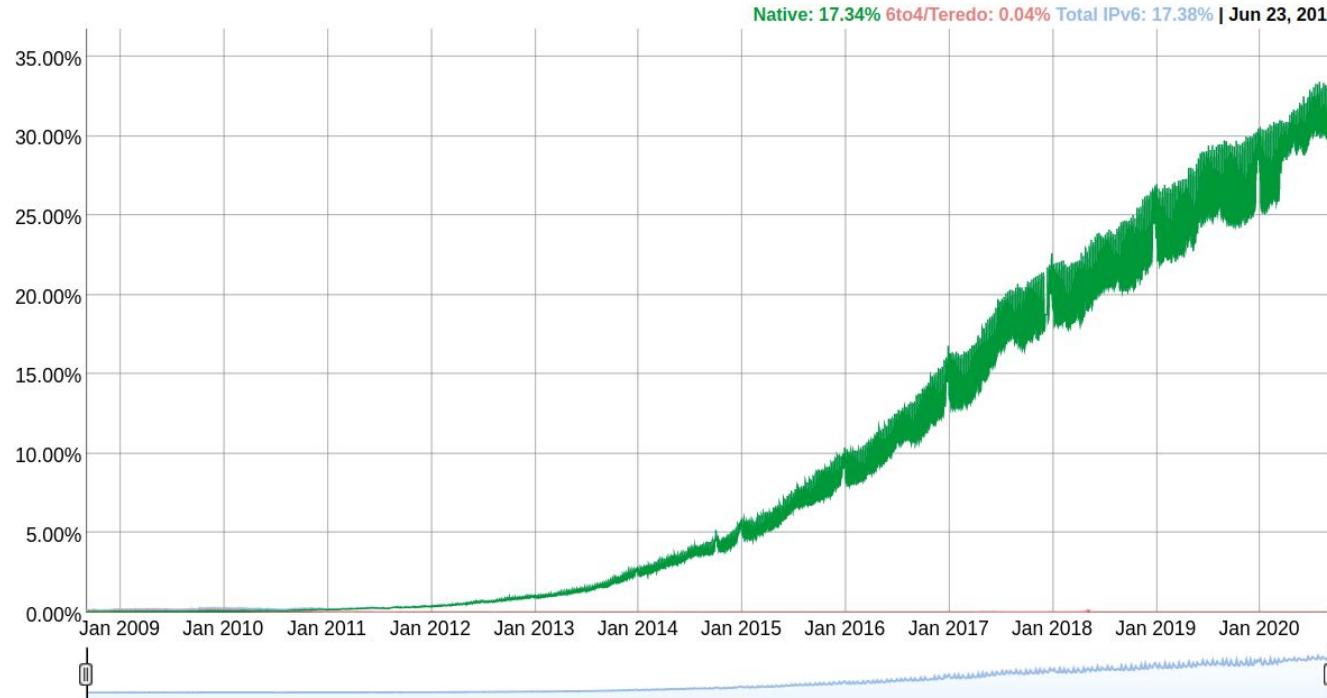
Objetivos do IETF em 1990 para o Sucessor do IPv4

- Aceitar bilhões de *hosts*, mesmo com alocação ineficiente de espaço de endereços
- Reduzir o tamanho das tabelas de roteamento
- Simplificar o protocolo para reduzir o tempo de processamento nos roteadores
- Oferecer mais segurança (autenticação e privacidade)
- Dar mais importância ao tipo de serviço (em especial, dados em tempo real)
- Auxiliar o *multicasting*, possibilitando a especificação de objetivos
- Permitir que um *host* mude de lugar sem precisar mudar de endereço
- Permitir que o protocolo evoluísse no futuro
- Permitir a coexistência entre protocolos novos e antigos durante anos

- ICANN já distribuiu os últimos endereços IPv4 e eles estão sendo alocados pelos autoridades regionais
- Ampla coleção de propostas cuja primeira versão é de 1998
- Utiliza endereços 128 bits e uma nova escassez não deve acontecer
- Difícil de implementar e não se interliga com o IPv4, apesar de serem semelhantes
- Não é compatível com o IPv4, mas o é com os outros protocolos auxiliares da Internet (e.g., TCP, UDP, ICMP, IGMP, OSPF, BGP e DNS)
- Mais informações: RFCs 2460 e 2466

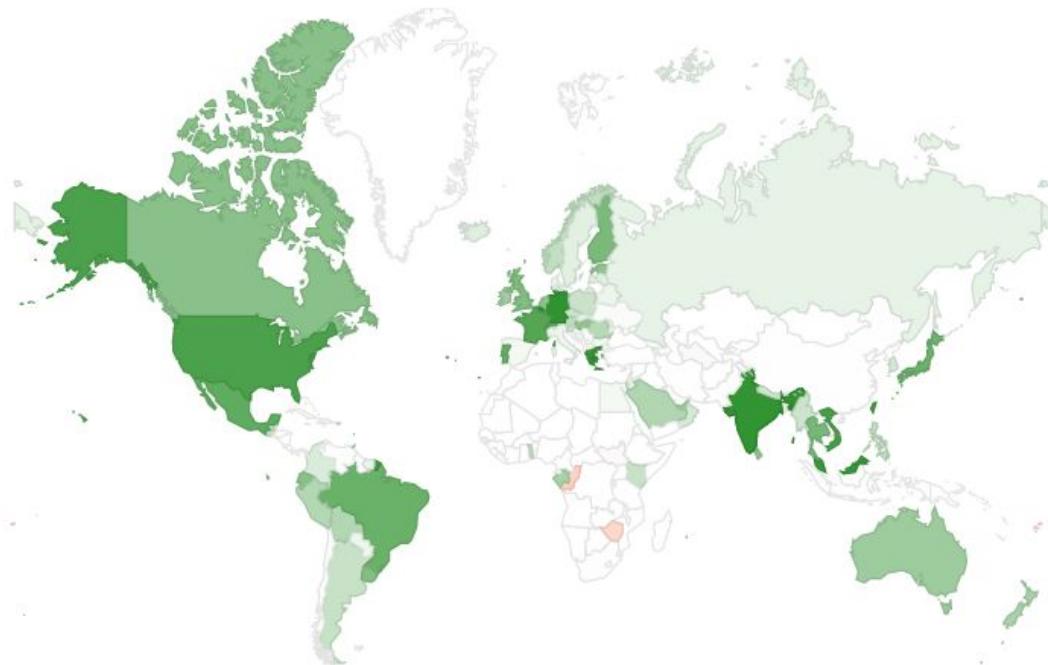
Adoção do IPv6 (set/2020)

www.google.com/intl/pt-BR/ipv6/statistics.html#tab=ipv6-adoption



Adoção do IPv6 por país (set/2020)

www.google.com/intl/pt-BR/ipv6/statistics.html#tab=per-country-ipv6-adoption



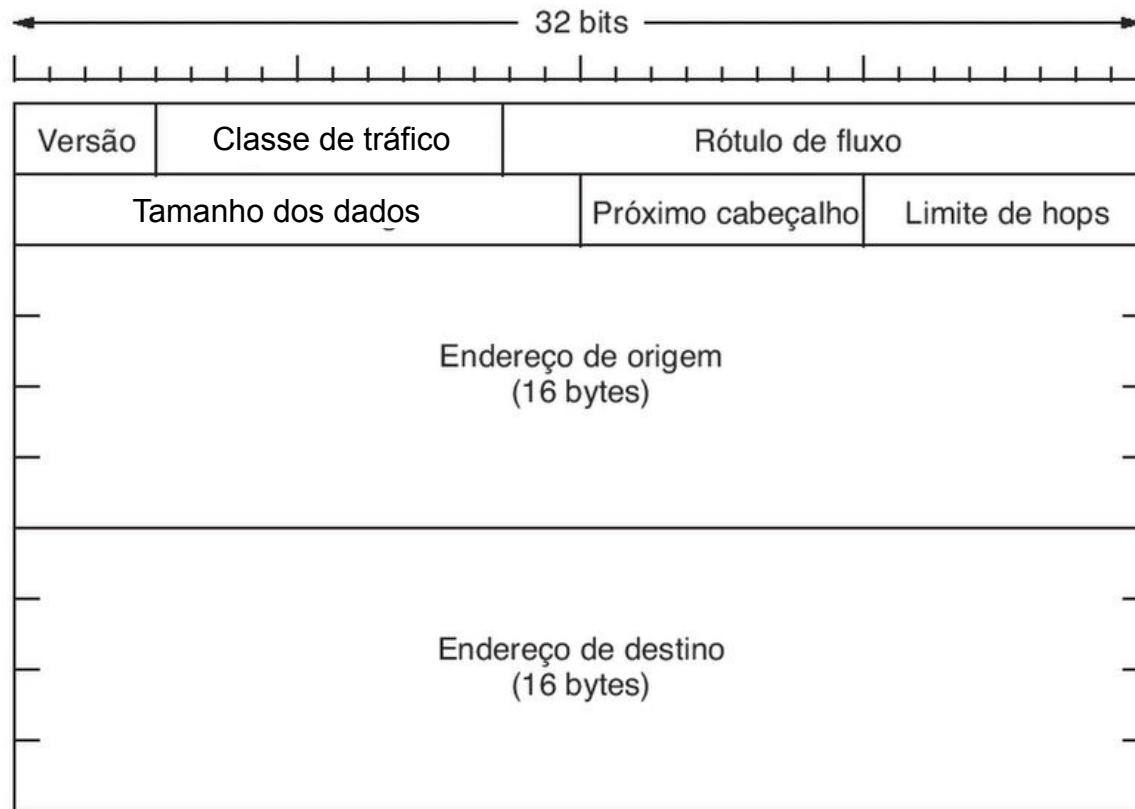
E você?

www.test-ipv6.com

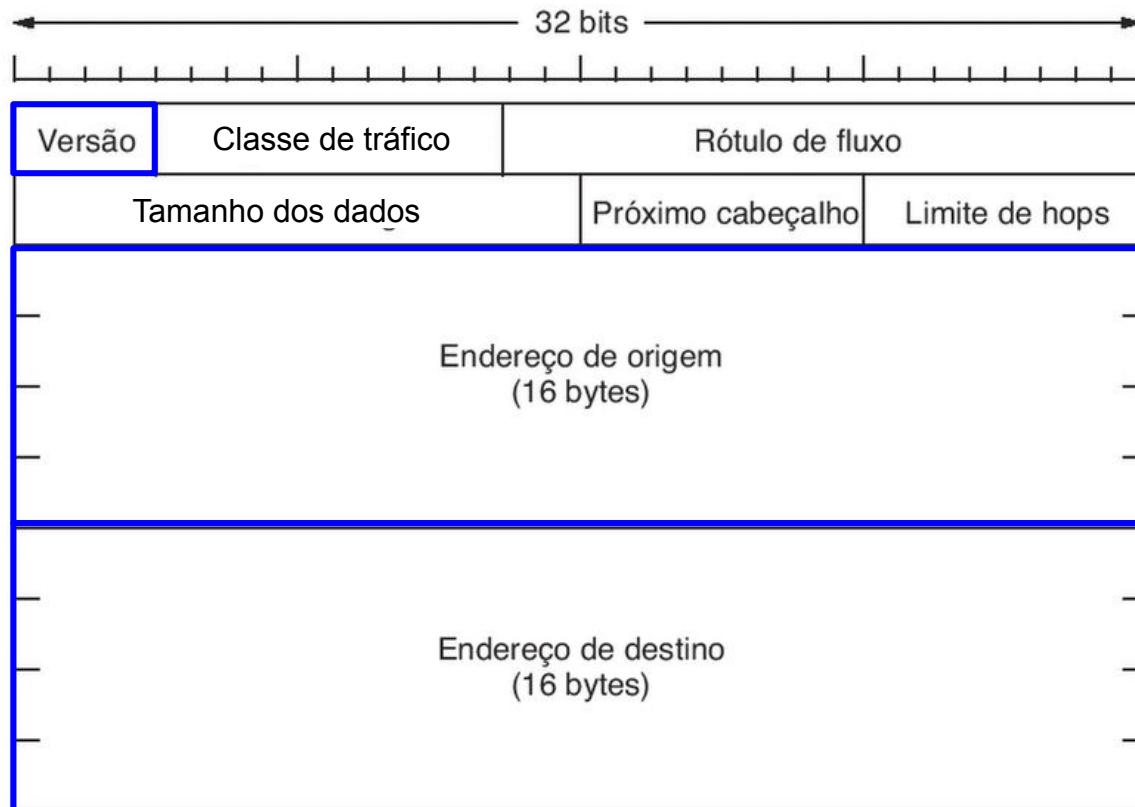
Cabeçalho do IPv6

- Simplificação do cabeçalho do IPv4
- Menos campos que o IPv4, de 14 para 8 campos
- Tamanho fixo de 40 bytes (dobro do IPv4)
- Permite cabeçalhos de extensão não processados por roteadores intermediários
- Espaço de endereçamento 4 vezes maior que o do IPv4

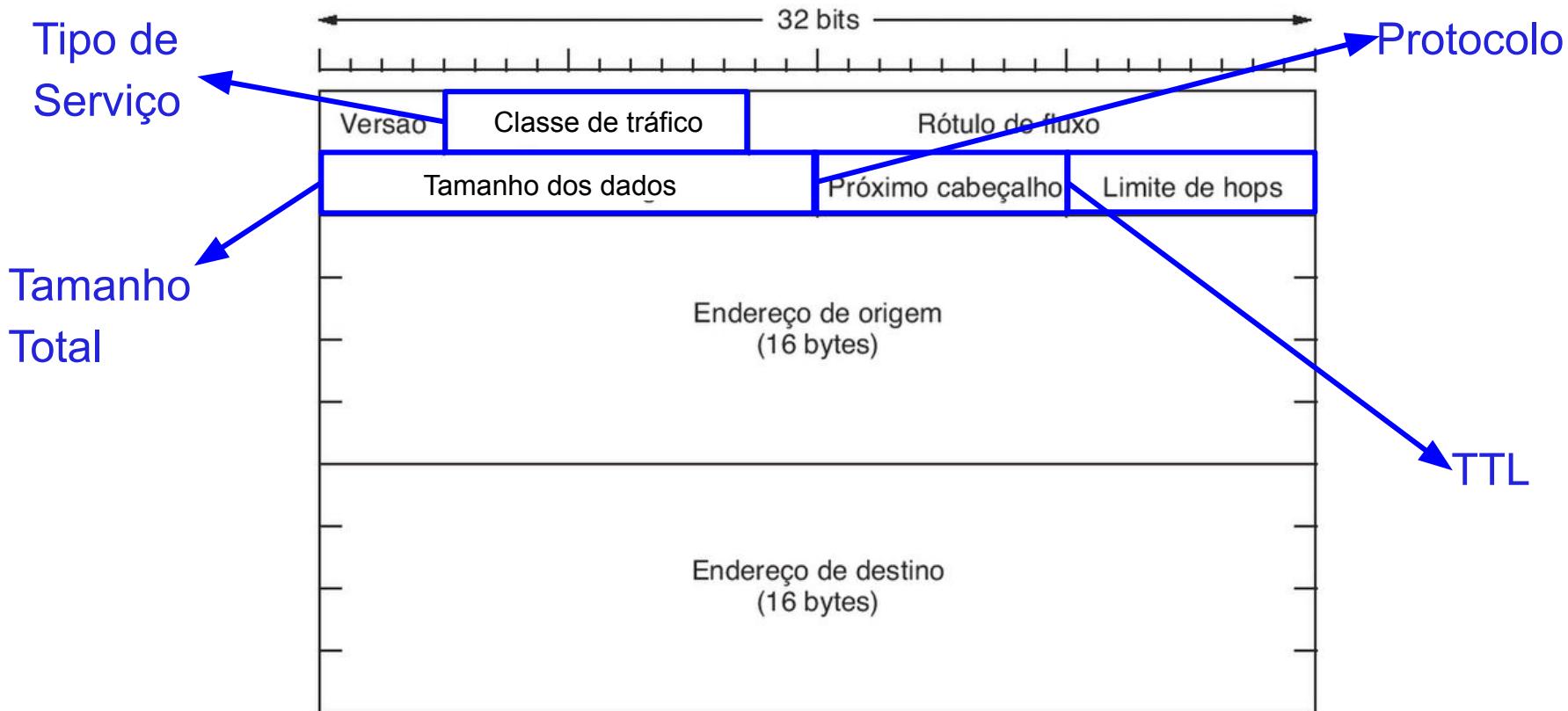
Cabeçalho do IPv6



Campos Similares aos do IPv4



Campos Renomeados ou Repositionados



Campo Classe de Tráfego (8 bits)

- Antigo Tipo de Serviço
- Identifica os pacotes por classes de serviços ou prioridade

Campo Tamanho do Dados (16 bits)

- Antigo Tamanho Total
- Indica o tamanho (em bytes) apenas dos dados enviados
- O tamanho dos cabeçalhos de extensão também são somado neste campo

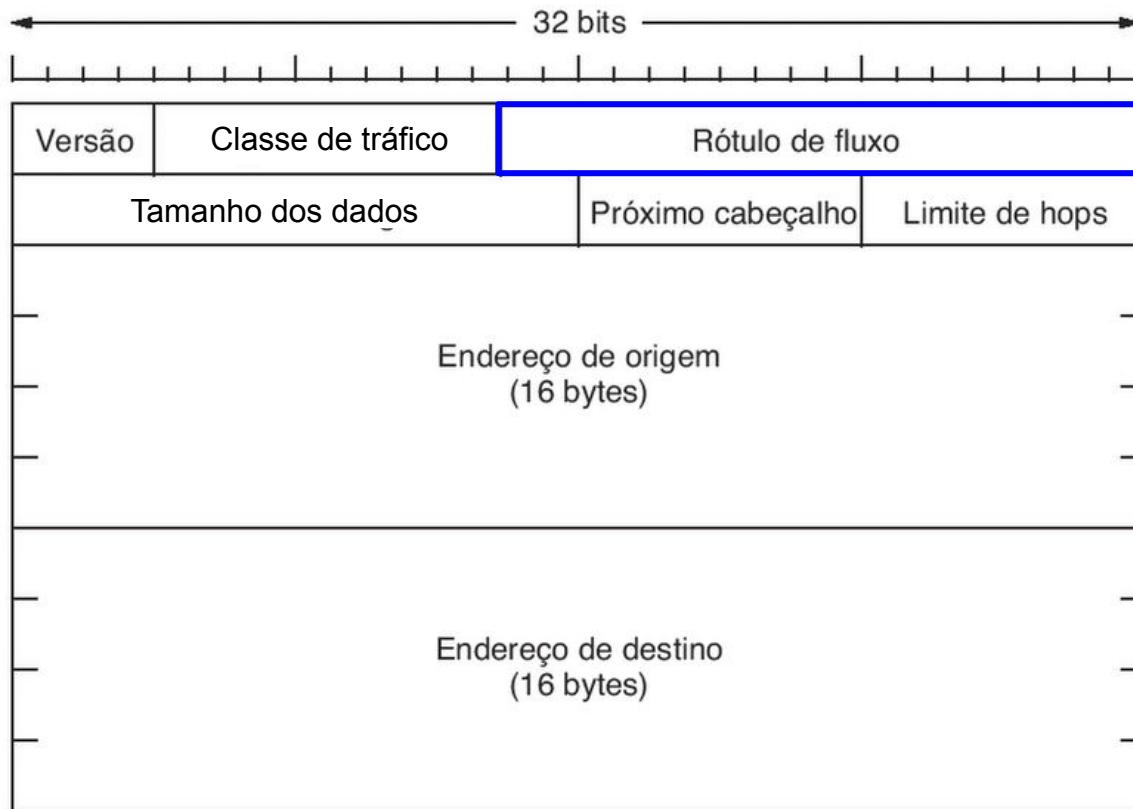
Campo Limite de *Hops* (8 bits)

- Antigo TTL
- Decrementado a cada salto de roteamento e indica o número máximo de roteadores pelos quais o pacote pode passar antes de ser descartado
- Padroniza o modo que o TTL do IPv4 é utilizado uma vez que sua descrição inicial define como o tempo, em segundos, para o pacote ser descartado caso não chegue ao destino

Campo Próximo Cabeçalho (8 bits)

- Antigo Protocolo
- Identifica o cabeçalho de extensão que segue o atual

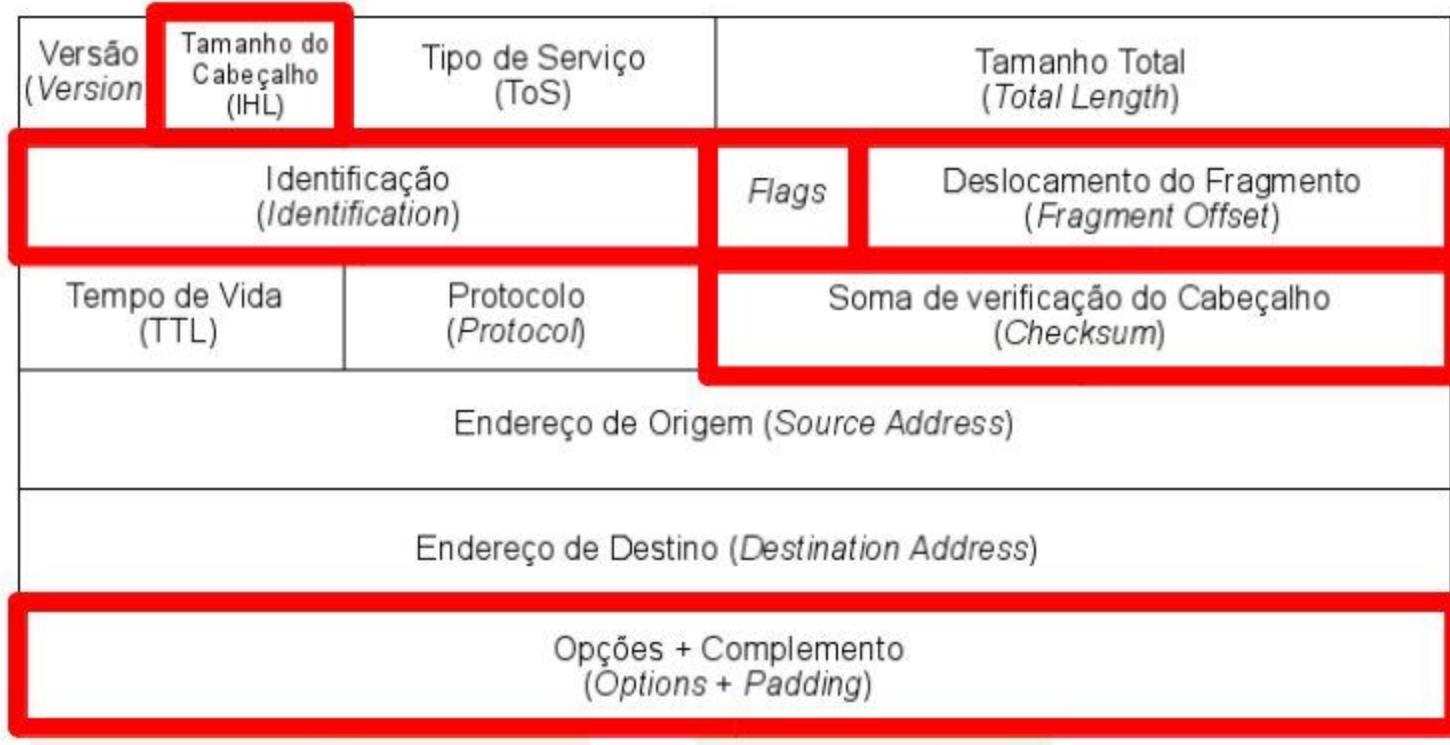
Novo Campo



Campo Rótulo de Fluxo (10 bits)

- Identifica pacotes do mesmo fluxo de comunicação
- Configurado pelo destino para separar os fluxos de cada uma das aplicações e os nós intermediários podem utilizá-lo de forma agregada com os endereços de origem e destino para realização de tratamento específico dos pacotes

Campos Removidos no IPv6

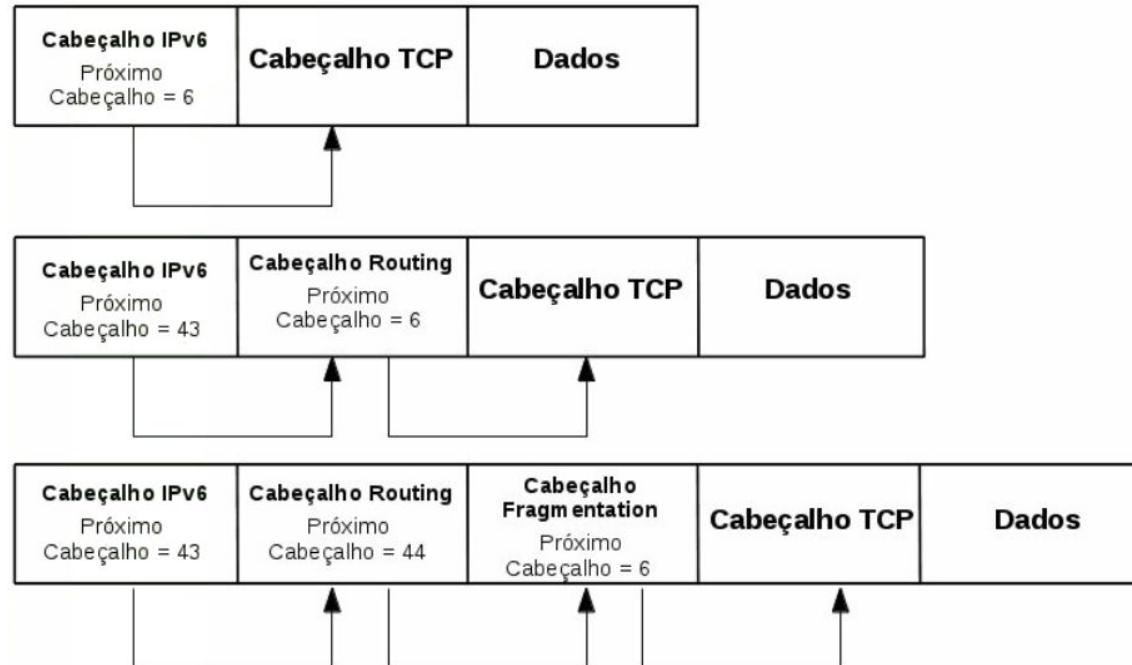


Campos Removidos no IPv6

- **Tamanho do Cabeçalho**: desnecessário uma vez que seu valor foi fixado
- **Identificação, Flags, Deslocamento do Fragmento e Opções**: passaram a ter suas informações indicadas em cabeçalhos de extensão apropriados
- **Soma de Verificação**: descartado, pois camadas superiores também verificam

Cabeçalhos de Extensão

- Localizam-se entre o cabeçalho base e o da camada superior. Se tivermos múltiplos cabeçalhos de extensão, eles formam uma cadeia de cabeçalhos



Os Seis Cabeçalhos Atuais de Extensão

- *Hop-by-Hop Options*: Decisões a serem tomadas durante o roteamento e, por isso, é o único cabeçalho a ser processado por roteadores intermediários
- *Routing*: Suporte a mobilidade
- *Fragmentation*: Campos de fragmentação similares aos do IPv4
- *Authentication Header*: Segurança
- *Encapsulating Security Payload*: Segurança
- *Destination Options*: Suporte a mobilidade

* Por simplificação, essa é a ordem dos cabeçalhos (quando existentes)

Fragmentação no IPv6

- Roteadores intermediários não fazem fragmentações
- Protocolo PMTUD descobre o maior MTU da rota
- Quando um roteador intermediário descobre uma rota com MTU maior que a considerada ele envia ICMP Packet too Big para a origem
- Vídeo sobre Fragmentação (NIC.br): www.youtube.com/watch?v=5OtebbSnwoM

Endereço IPv6

- Número único de 128 bits que identifica cada máquina na Internet
- Teoricamente, $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ endereços, ou seja:
 - $7,9 \times 10^{28}$ vezes a quantidade de endereços IPv4
 - $5,6 \times 10^{28}$ endereços por pessoa (supondo a população 6 bilhões de pessoas)
 - 7×10^{23} endereços por metro quadrado da Terra

Representação de Endereços do IPv6

- Oito grupos de 16 bits separados por “:” e escritos com dígitos hexadecimais (e.g., 0001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1)
- Aceita caracteres maiúsculos e minúsculos
- Para abreviar, podemos omitir os zeros a esquerda de cada bloco de 16 bits ou substituir um ou mais grupos de 16 bits zero por por “::”

Exercício Resolvido (5)

• Abrevie os endereços abaixo:

a) 8000:0000:0000:0000:0123:4567:89AB:CDEF

b) 2001:0DB8:0000:0054:0000:0000:0000:0000

c) 2001:0DB8:0000:0000:130F:0000:0000:140B

Exercício Resolvido (5)

• Abrevie os endereços abaixo:

a) 8000:0000:0000:0000:0123:4567:89AB:CDEF

8000::123:4567:89AB:CDEF

b) 2001:0DB8:0000:0054:0000:0000:0000:0000

2001:DB8:0:054::

c) 2001:0DB8:0000:0000:130F:0000:0000:140B

2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B

A resposta 2001:DB8::130F::140B é errada e ambígua porque gera

2001:DB8:0:0:130F:0:0:140B, 2001:DB8:0:0:0:130F:0:140B ou

2001:DB8:0:130F:0:0:0:140B

Representação de Endereços IPv4 no IPv6

- Endereços IPv4 podem ser escritos empregando um par de sinais de dois pontos e um número decimal tradicional como, por exemplo:

::192.31.20.46

Representação dos Prefixos de Rede

- Como no IPv4, utiliza a notação CIDR
- endereçoIPv6 / tamPrefixo, onde tamPrefixo é um decimal que especifica o número de bits à esquerda que compreendem o prefixo (e.g., 2001:db8:3003:2::/64)
- Possibilita a agregação dos endereços de forma hierárquica, identificando posição geográfica, provedor de acesso, rede, divisão da sub-rede entre outros
- Maximiza agregação, reduzindo as tabelas de roteamento
- Por padrão, utilizamos prefixos /64

Representação de Endereços IPv6 em URLs

- Entre colchetes, evitando ambiguidade com eventuais indicações de portas
- Por exemplo:
 - `http://[2001:12ff:0:4::22]/index.html`
 - `http://[2001:12ff:0:4::22]:8080`

Exercício (16)

- Diferencie redes de datagrama e de circuito virtual

Exercício (17)

- Cite cinco princípios da Camada de Rede da Internet e justifique a razão de cada um deles ser relevante no projeto da rede

Exercício (18)

- Antes do CIDR, os endereços do IPv4 eram organizados em classes. Por que essa mudança aconteceu?

Exercício (19)

- Faça um paralelo entre os cabeçalhos do IPv4 e IPv6

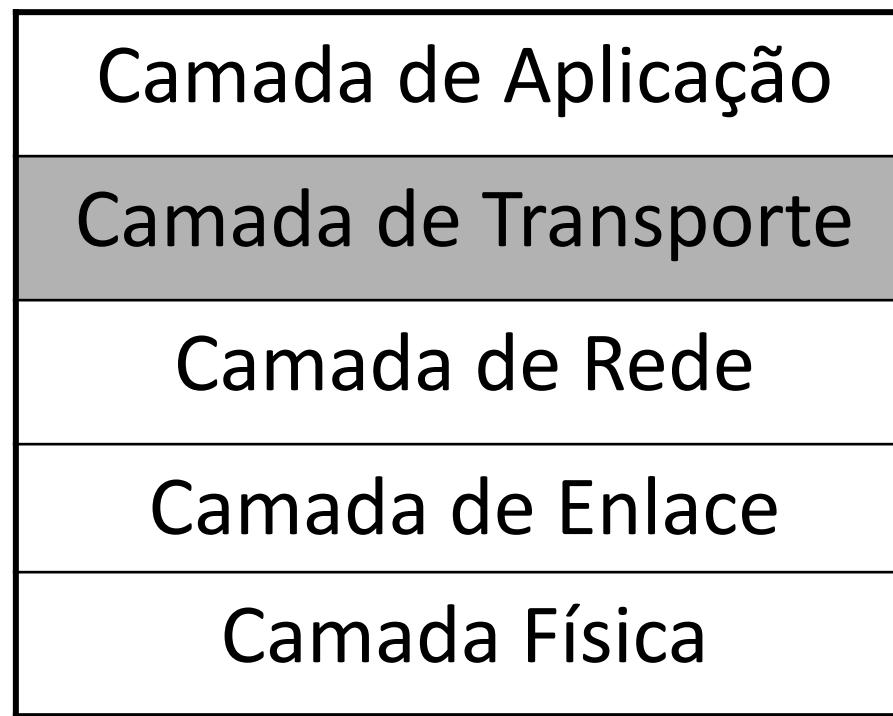
Exercício (20)

- Faça um paralelo entre a fragmentação de pacotes no IPv4 e IPv6

Unidade VI: Camada de Transporte

Prof. Max do Val Machado

Camada de Transporte



Camada de Transporte vs. de Rede

- A camada de rede oferece uma remessa de pacotes fim a fim usando datagramas ou circuitos virtuais
- A camada de transporte se baseia na de rede para oferecer transporte de dados de um **processo** em uma máquina origem para outro em outra de destino
 - ◆ A camada de transporte provê abstrações de que aplicações precisam para usar a rede
 - ◆ A camada de transporte dá sentido a pilha de protocolos

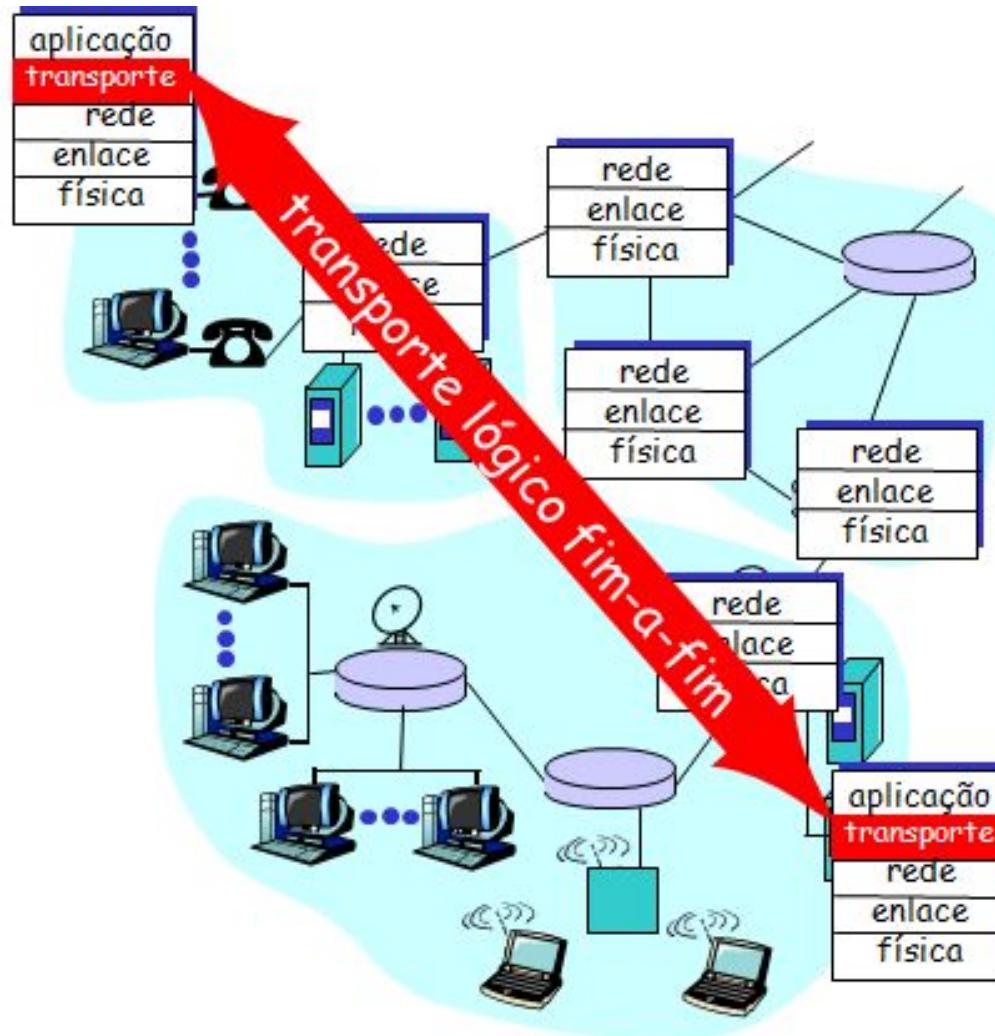
Camada de Transporte vs. de Rede

- Os processos de origem e destino que executam os protocolos de transporte
- A camada de transporte é a primeira a fazer comunicação lógica fim a fim
 - ◆ Fim a fim significa que uma entidade do emissor só se comunica com sua entidade-par do host destinatário
 - ◆ Roteadores, hubs e switches não precisam analisar os cabeçalhos de transporte para executar suas funções nativas

Camada de Transporte vs. de Rede

Camada de Rede	Camada de Transporte
Transferência de dados entre sistemas finais	Transferência de dados entre processos
Funciona principalmente nos roteadores	Funciona inteiramente nas máquinas dos usuários

Camada de Transporte vs. de Rede



Camada de Transporte vs. de Rede

- Se o serviço oferecido pelas duas camadas é tão semelhante por que não unificá-las?
 - ◆ Resposta sutil, mas crucial
 - ◆ Os protocolos de transporte funcionam integralmente nas máquinas de origem e destino e os de rede, principalmente, nos roteadores

Serviços Oferecidos pela Camada de Transporte

- Serviços orientados ou não a conexão que geralmente são semelhantes aos da camada de rede

	Rede orientada a conexão	Rede não orientada a conexão
Camada de Transporte orientado a conexão		
Camada de Transporte não orientado a conexão		

Serviços Oferecidos pela Camada de Transporte

- A combinação de um protocolo de transporte não orientado a conexão com um de rede que seja é normalmente descarta porque é ineficaz estabelecer uma conexão para enviar um único pacote e encerrá-la imediatamente depois do envio

Serviços Oferecidos pela Camada de Transporte

- Serviço confiável, eficiente e econômico a seus usuários que normalmente consistem em processos pertencentes a camada de aplicação
 - ◆ Problemas acontecem e os usuários não possuem qualquer controle real sobre a camada de rede
 - ◆ A camada de transporte pode fazer retransmissões ou restabelecer conexões
 - ◆ A rede não é prefeita e pode ser heterogênea e dinâmica

Função da Camada de Transporte

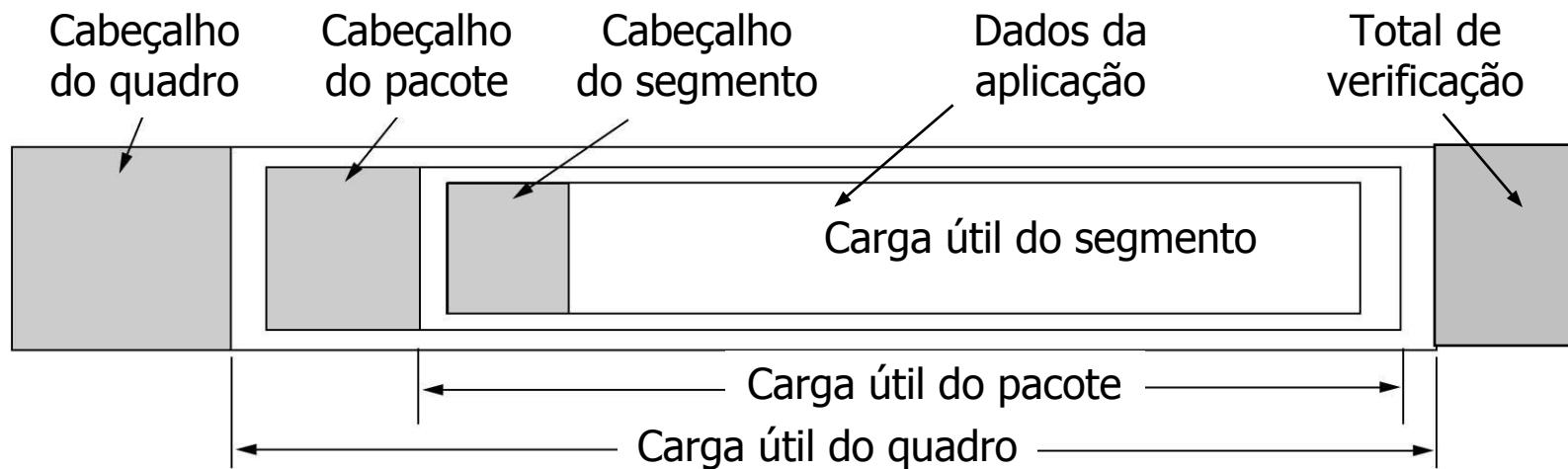
- Tornar as camadas superiores do projeto imunes à tecnologia, ao projeto e às imperfeições da rede

Distinção entre Camadas

- Dada a função da camada de transporte, normalmente fazemos a distinção entre as camadas 1 a 4, por um lado e as superiores, por outro lado
- As quatro primeiras são consideradas como o provedor de serviços de transporte
- As superiores constituem os usuários do serviço de transporte

Segmento

- A unidade de dados trocada entre entidades da camada de transporte é chamada de segmento
- Aninhamento de segmentos, pacotes e quadros:



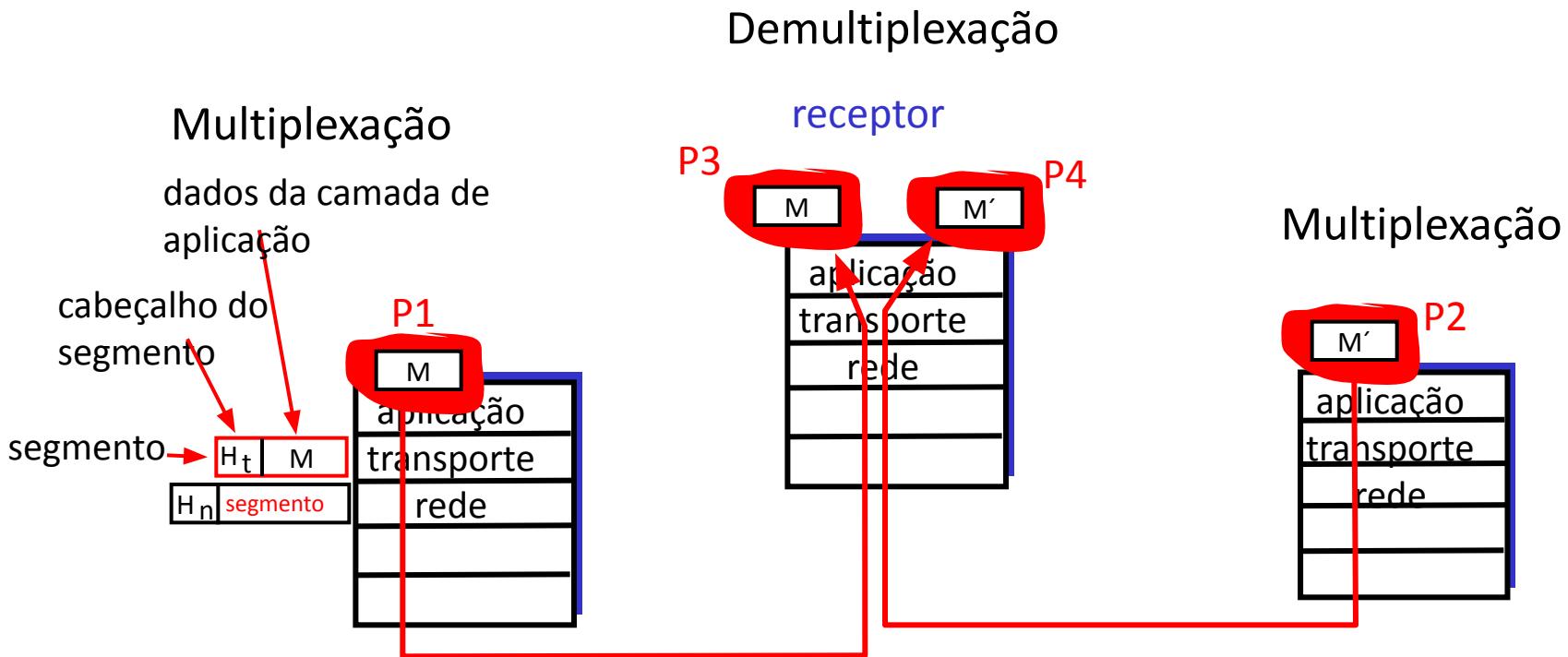
Multiplexação e Demultiplexação de Aplicações

- Fornece comunicação lógica entre processos de aplicação em hospedeiros diferentes (multiplexação / demultiplexação de aplicação)
- Objetivo: Ampliar a entrega hospedeiro a hospedeiro para entrega aplicação a aplicação

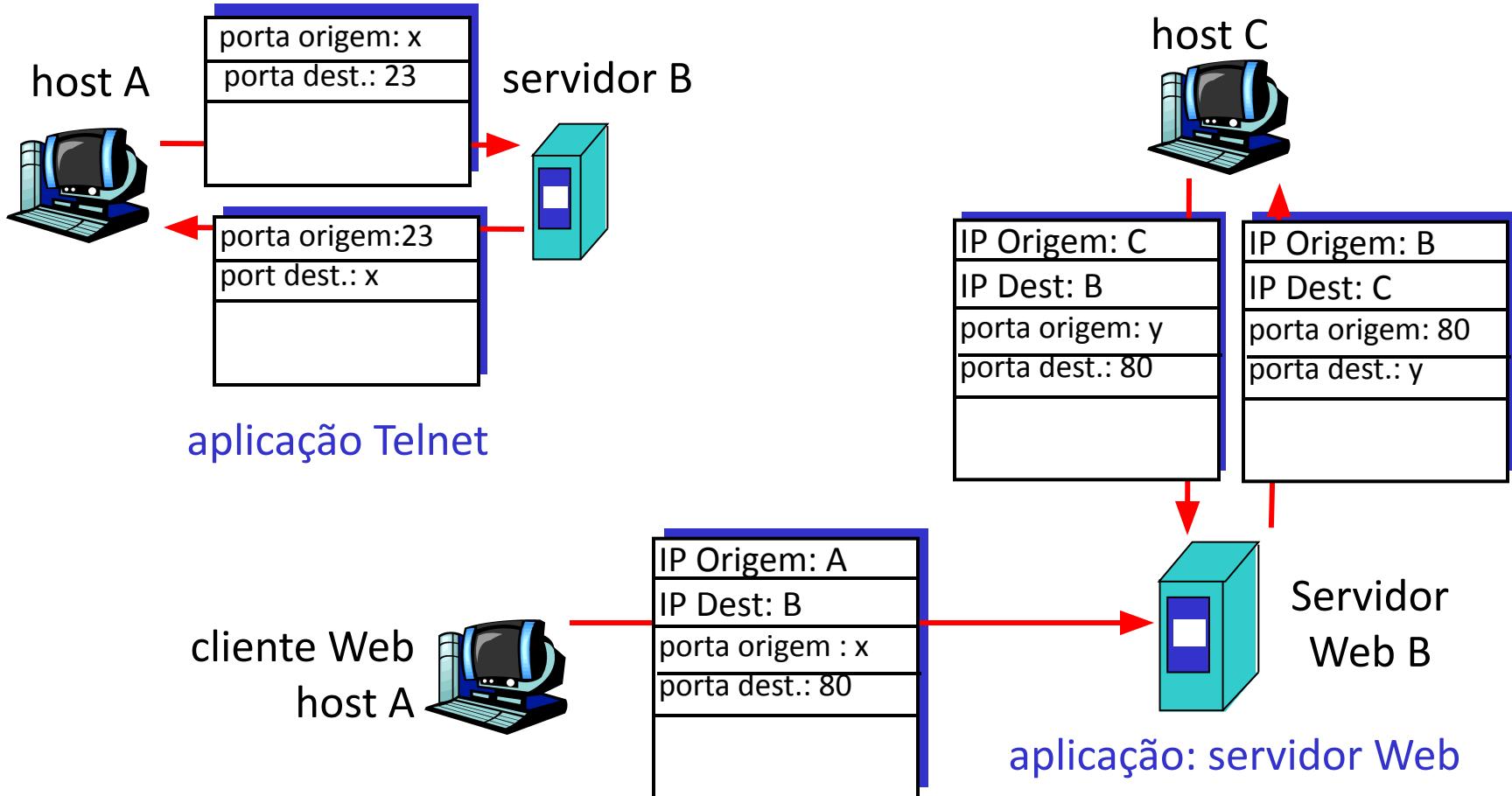
Multiplexação e Demultiplexação de Aplicações

- **Multiplexação:** reunir os dados provenientes de diferentes processos de aplicação
 - ◆ Ocorre no hospedeiro de origem
- **Demultiplexação:** entrega dos dados contidos em um segmento da camada de transporte ao processo de aplicação correto
 - ◆ ocorre no hospedeiro de destino)

Multiplexação e Demultiplexação de Aplicações

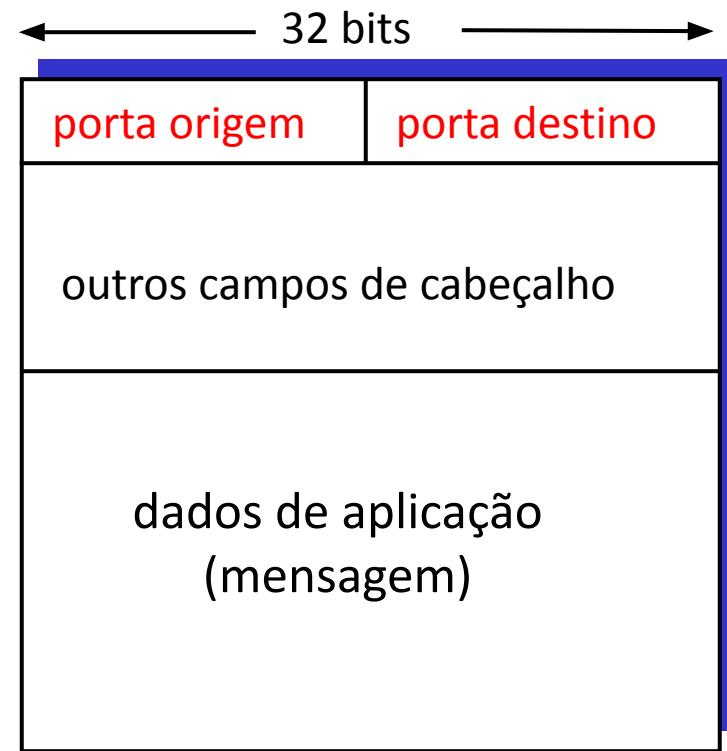


Multiplexação e Demultiplexação de Aplicações: Exemplos



Multiplexação e Demultiplexação de Aplicações

- Baseadas nas portas da origem e do destino e nos endereços IP
- Os números de porta entre 0 e 1023 são chamados de números de porta bem conhecidos e são reservados para protocolos de aplicação tradicionais



formato do segmento TCP/UDP

Alguns Números de Portas

Porta	Descrição
20/TCP	FTP - porta de dados
21/TCP	FTP - porta de controle
22/TCP,UDP	SSH
23/TCP,UDP	Telnet
25/TCP,UDP	SMTP
53/TCP,UDP	DNS
80/TCP	HTTP
81/TCP	HTTP Alternativa
110/TCP	POP3
143/TCP,UDP	IMAP4
194/TCP	IRC
366/TCP,UDP	SMTP
989/TCP,UDP	FTP – porta de dados sobre TLS/SSL
990/TCP,UDP	FTP – porta de controle sobre TLS/SSL
993/TCP	IMAP4 sobre SSL
995/TCP	POP3 sobre SSL

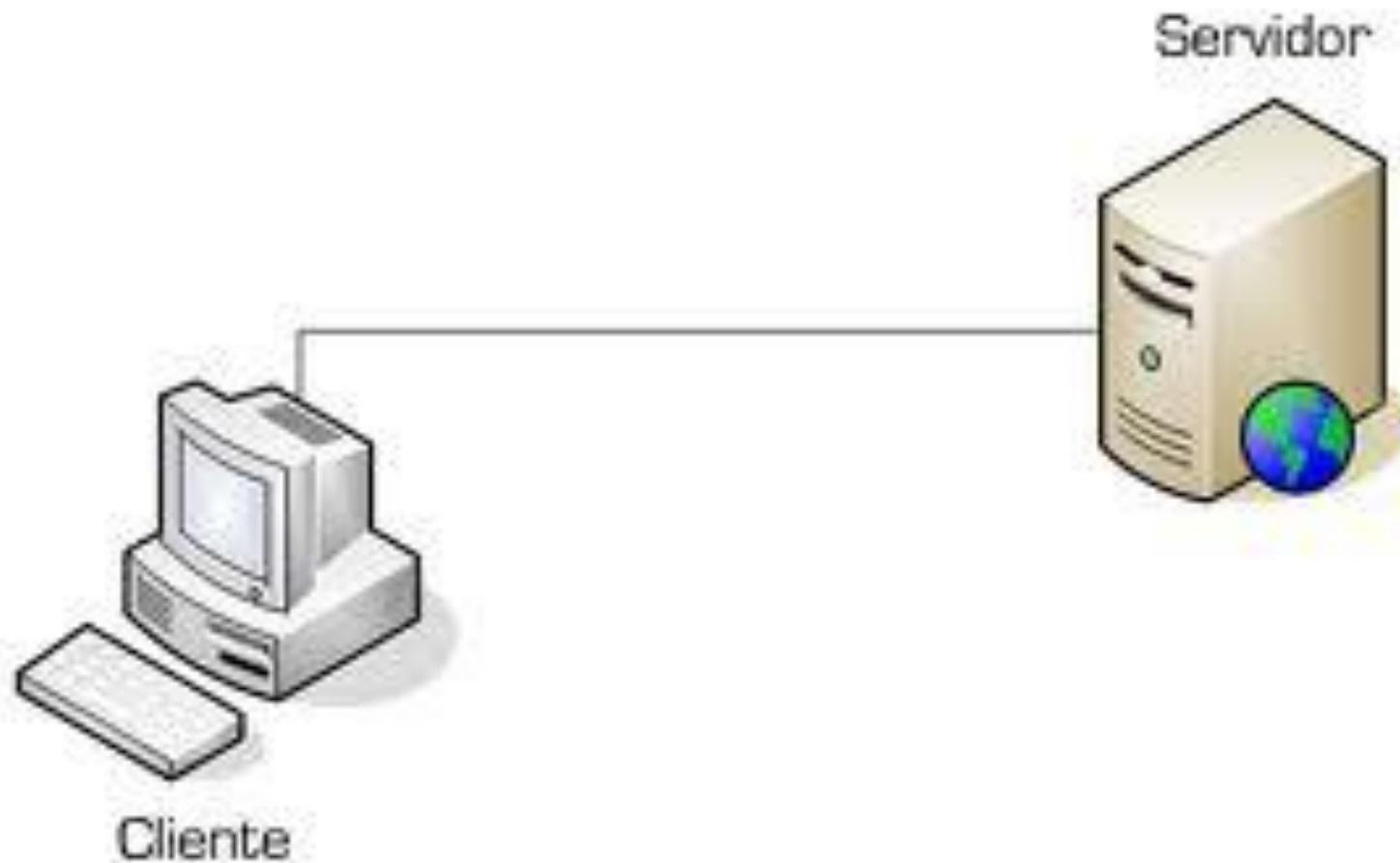
Protocolos da Camada de Transporte da Internet

- A Internet tem dois protocolos principais na camada de transporte
 - ◆ UDP - User Datagram Protocol
 - 4 Sem conexões
 - 4 Transferência não confiável de dados
 - ◆ TCP - Transport Control Protocol
 - 4 Orientado à conexões
 - 4 Transferência confiável de dados
 - 4 Controle de congestionamento
 - 4 Controle de fluxo

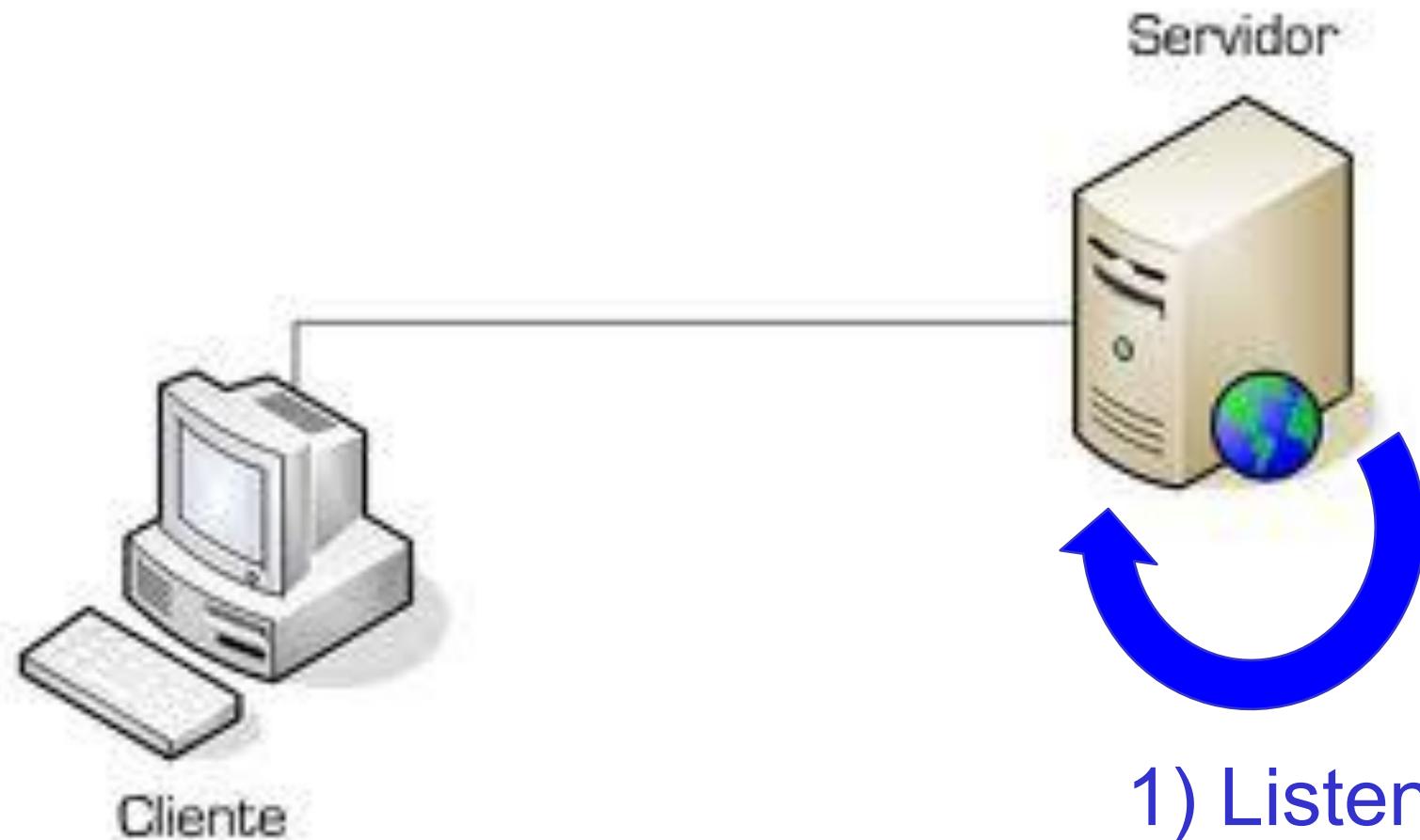
Primitivas para um Serviço de Transporte Simples

Primitiva	Pacote enviado	Significado
LISTEN	(nenhum)	Bloqueia até algum processo tentar conectar
CONNECT	CONNECTION REQ.	Tenta ativamente estabelecer uma conexão
SEND	DATA	Envia informação
RECEIVE	(nenhum)	Bloqueia até que um pacote de dados chegue
DISCONNECT	DISCONNECTION REQ.	Solicita uma liberação da conexão

Primitivas para um Serviço de Transporte Simples

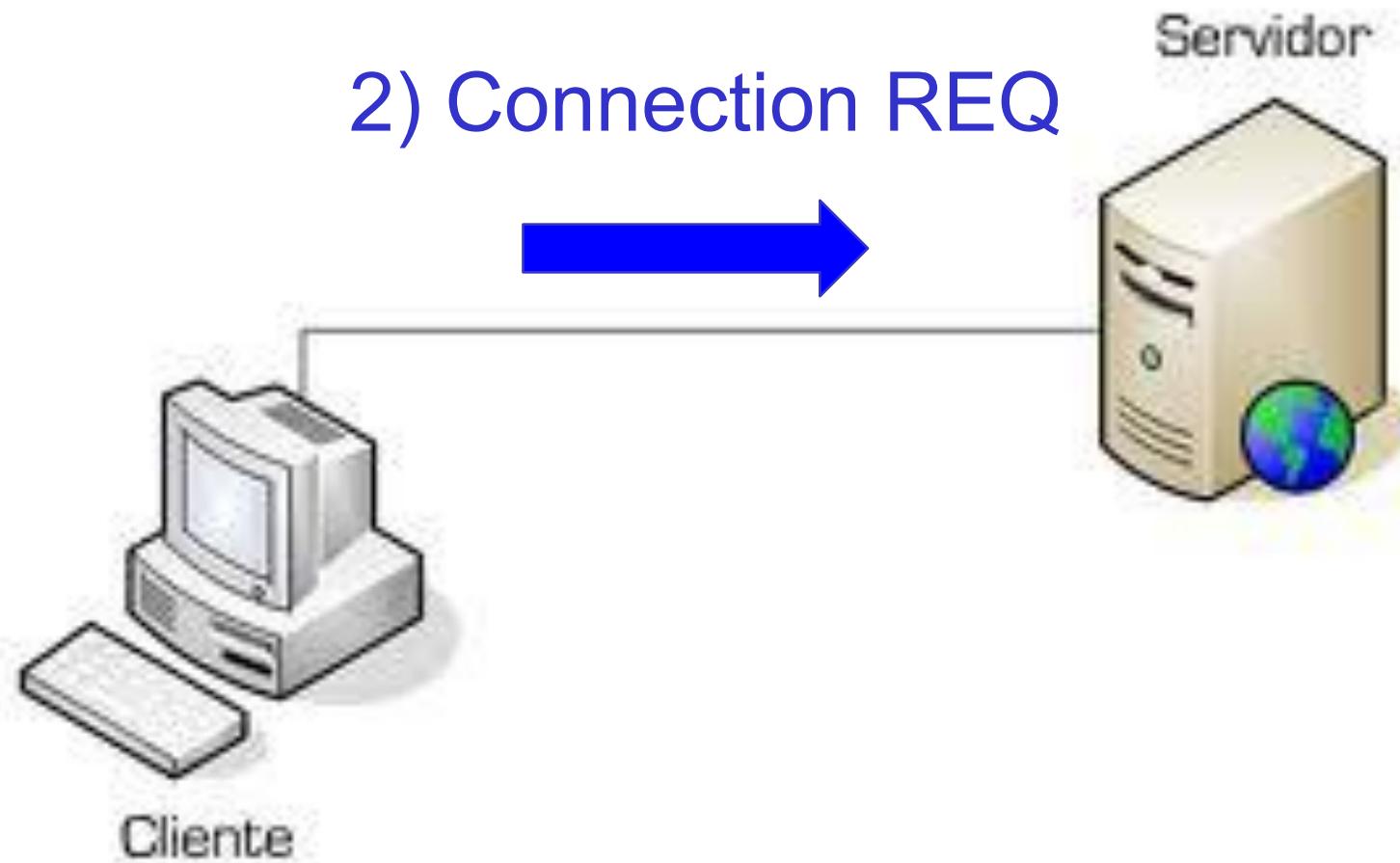


Primitivas para um Serviço de Transporte Simples

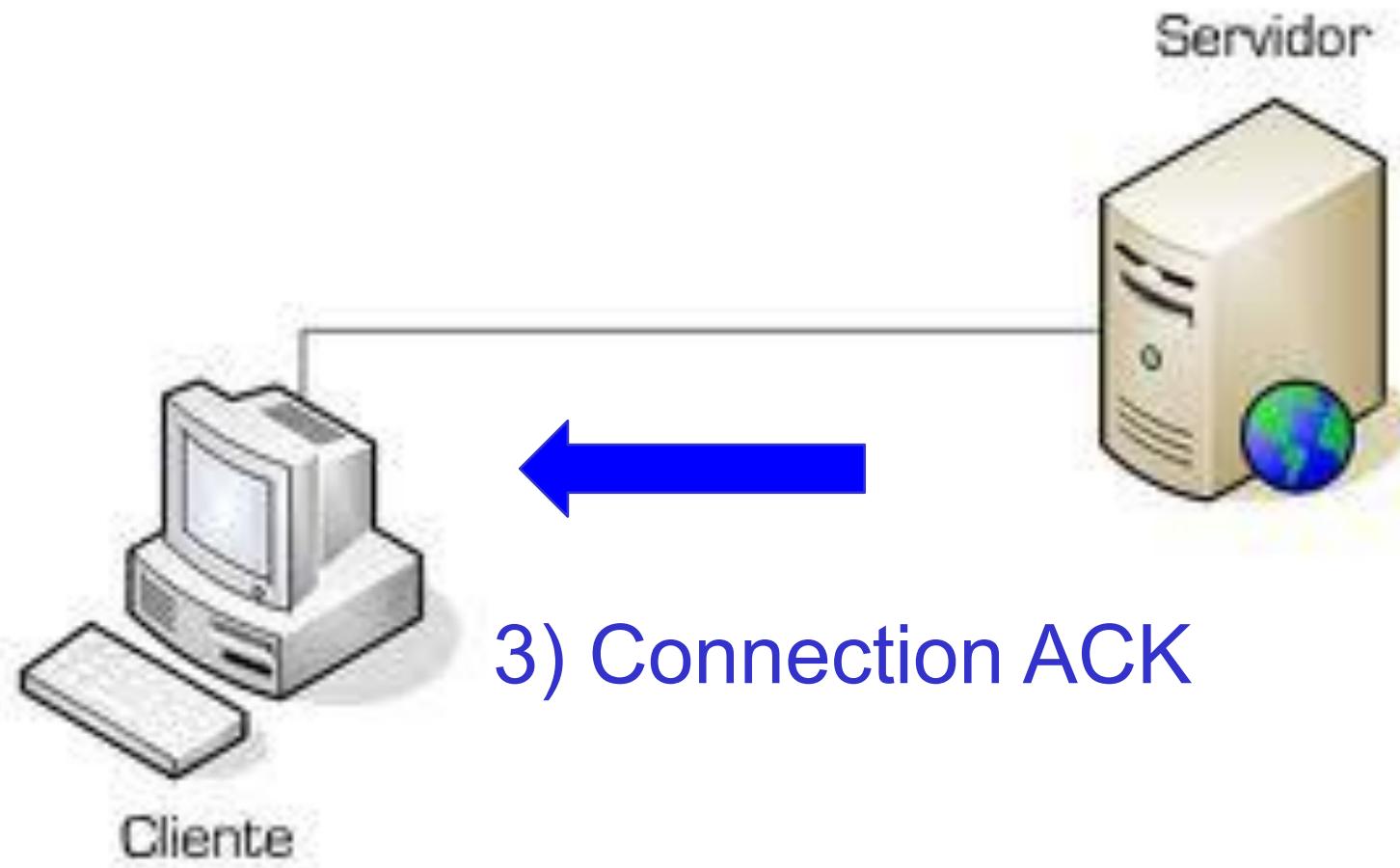


Primitivas para um Serviço de Transporte Simples

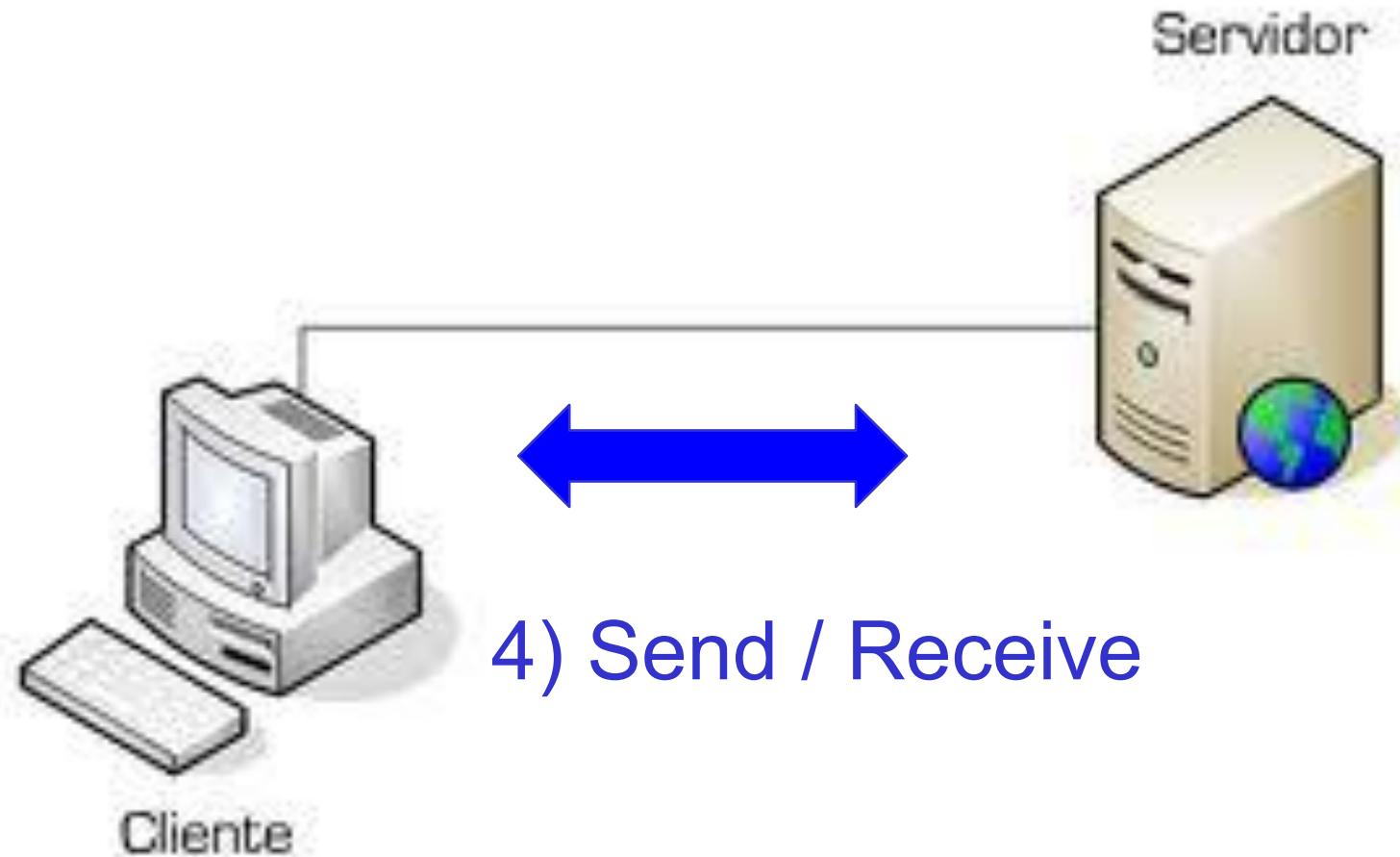
2) Connection REQ



Primitivas para um Serviço de Transporte Simples



Primitivas para um Serviço de Transporte Simples

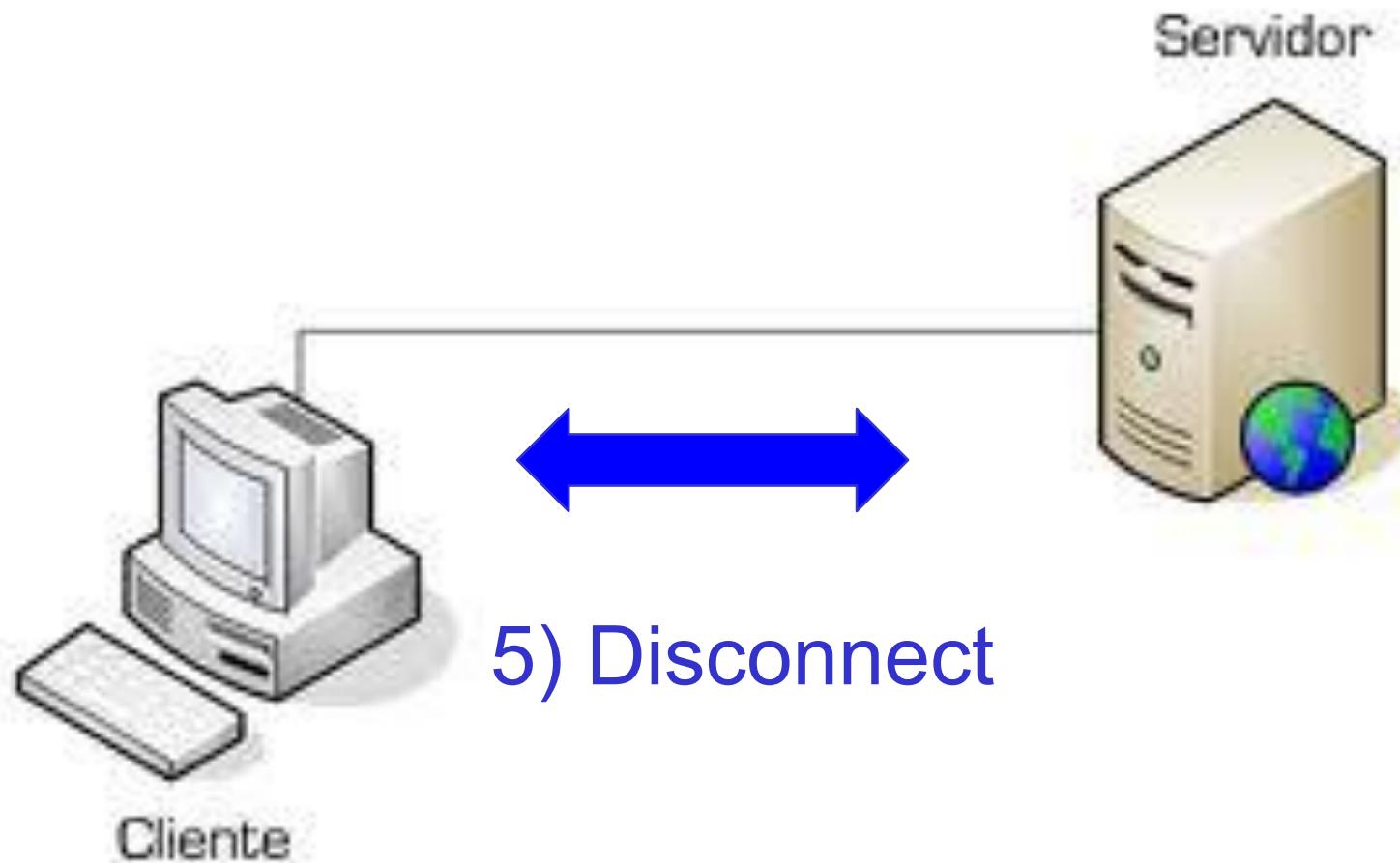


Primitivas para um Serviço de Transporte Simples

As partes devem ter uma política para definir de quem é a vez de enviar dados

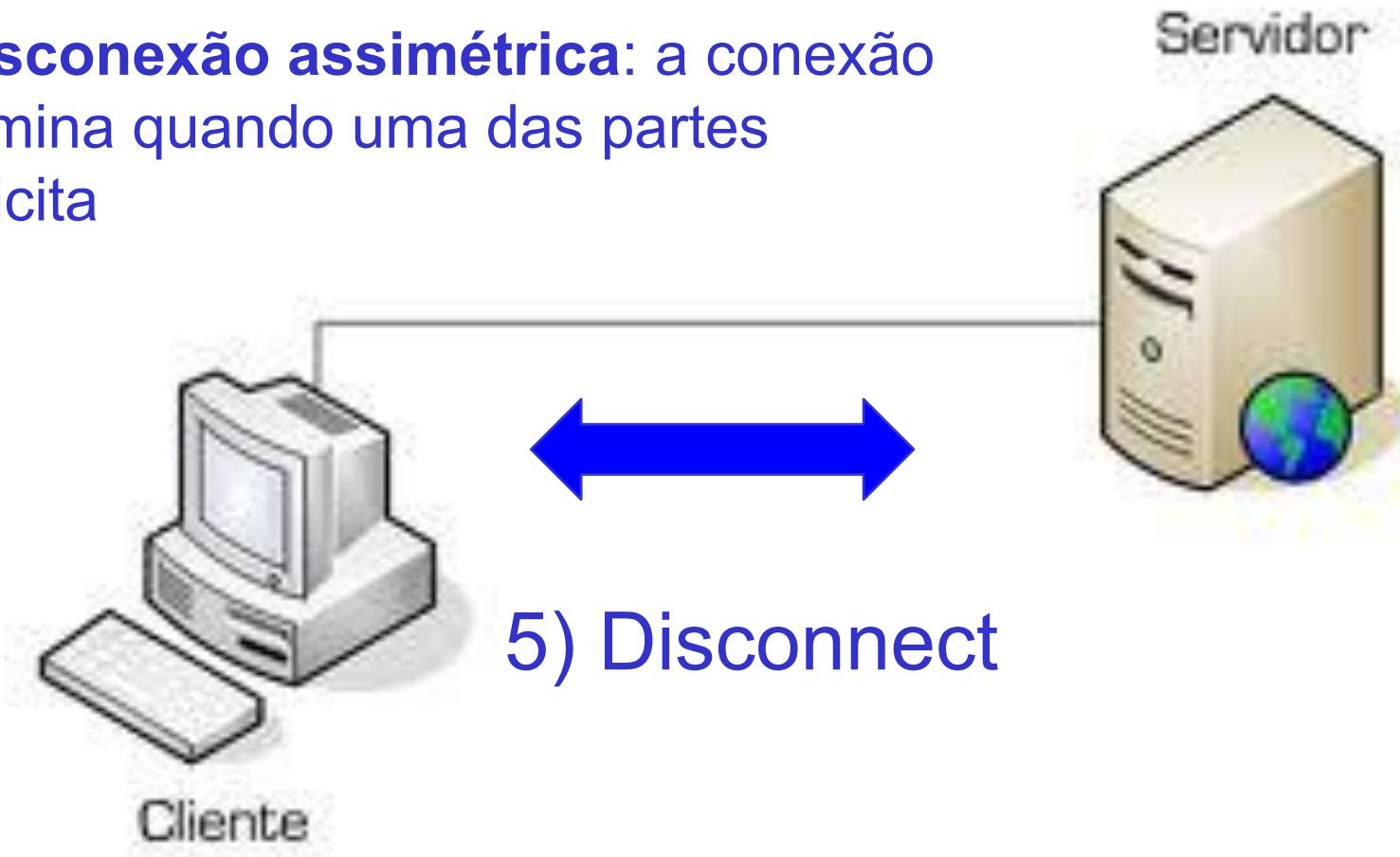


Primitivas para um Serviço de Transporte Simples



Primitivas para um Serviço de Transporte Simples

Desconexão assimétrica: a conexão termina quando uma das partes solicita



Primitivas para um Serviço de Transporte Simples

Desconexão simétrica: cada parte faz sua desconexão para informar que não enviará mais dados



UDP

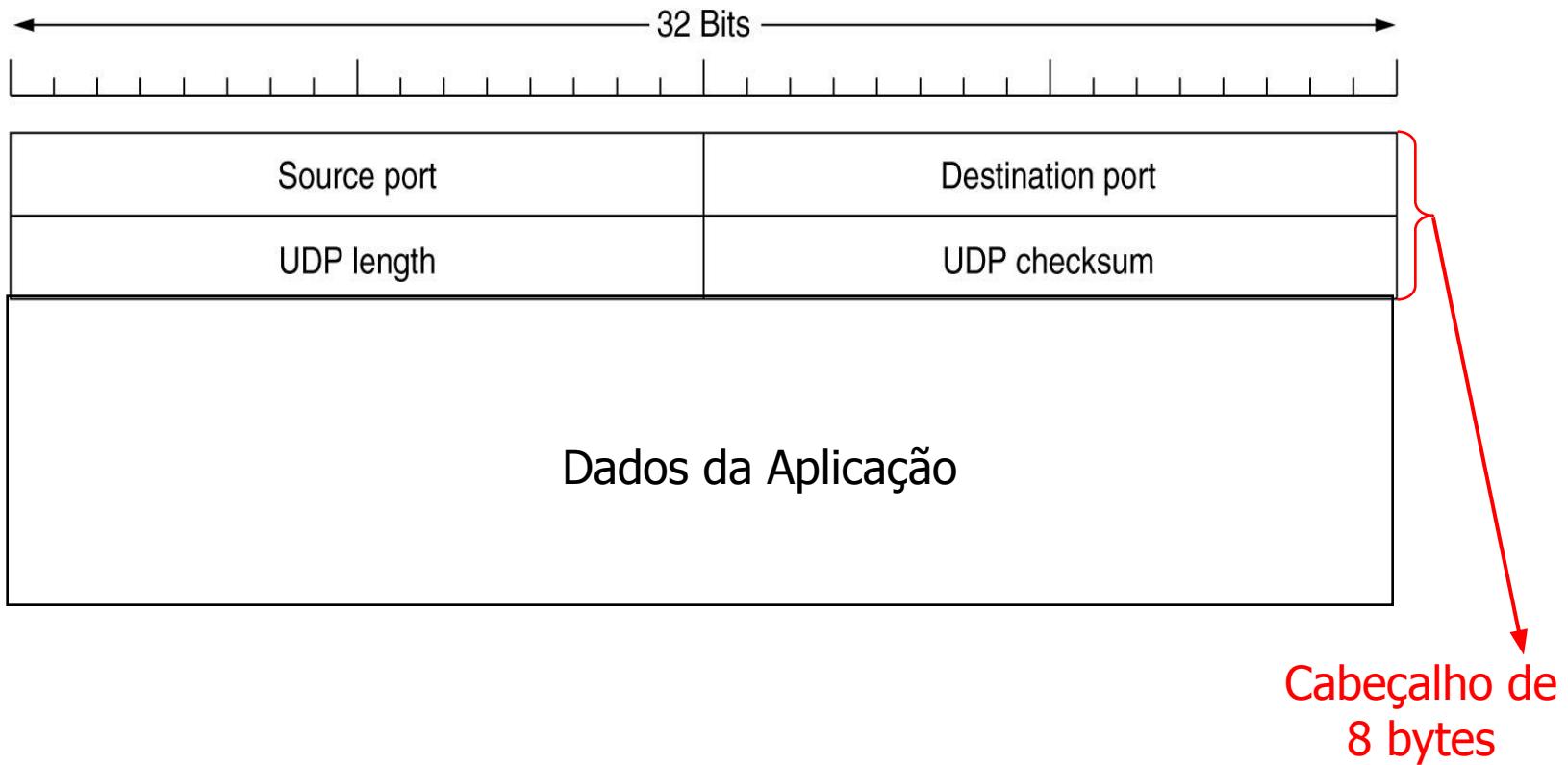
User Datagram Protocol

RFC 768

UDP

- Protocolo de transporte não confiável
- Não há estabelecimento de conexão
 - ◆ Não há apresentação entre o UDP emissor e o receptor
 - ◆ Cada segmento UDP é tratado de forma independente dos outros
- Serviço *best-effort*, segmentos UDP podem ser:
 - ◆ Perdidos
 - ◆ Entregues fora de ordem para a aplicação

Estrutura do Segmento UDP



Estrutura do Segmento UDP

- *Source Port e Destination Port:*
 - ◆ Identificam os pontos extremos (processos) nas máquinas de origem e destino
 - ◆ Quando um pacote UDP chega, sua carga útil é entregue ao processo associado à porta destino
- *UDP length:*
 - ◆ Tamanho total do segmento (incluindo o cabeçalho) em bytes (entre 8 de 65515)
- *UDP checksum:*
 - ◆ Campo opcional, armazenado como 0 se não for calculado

Ações que o UDP Não Realiza

- Controle de fluxo
- Controle de congestionamento
- Controle de erros
- Retransmissão após a recepção de um segmento incorreto

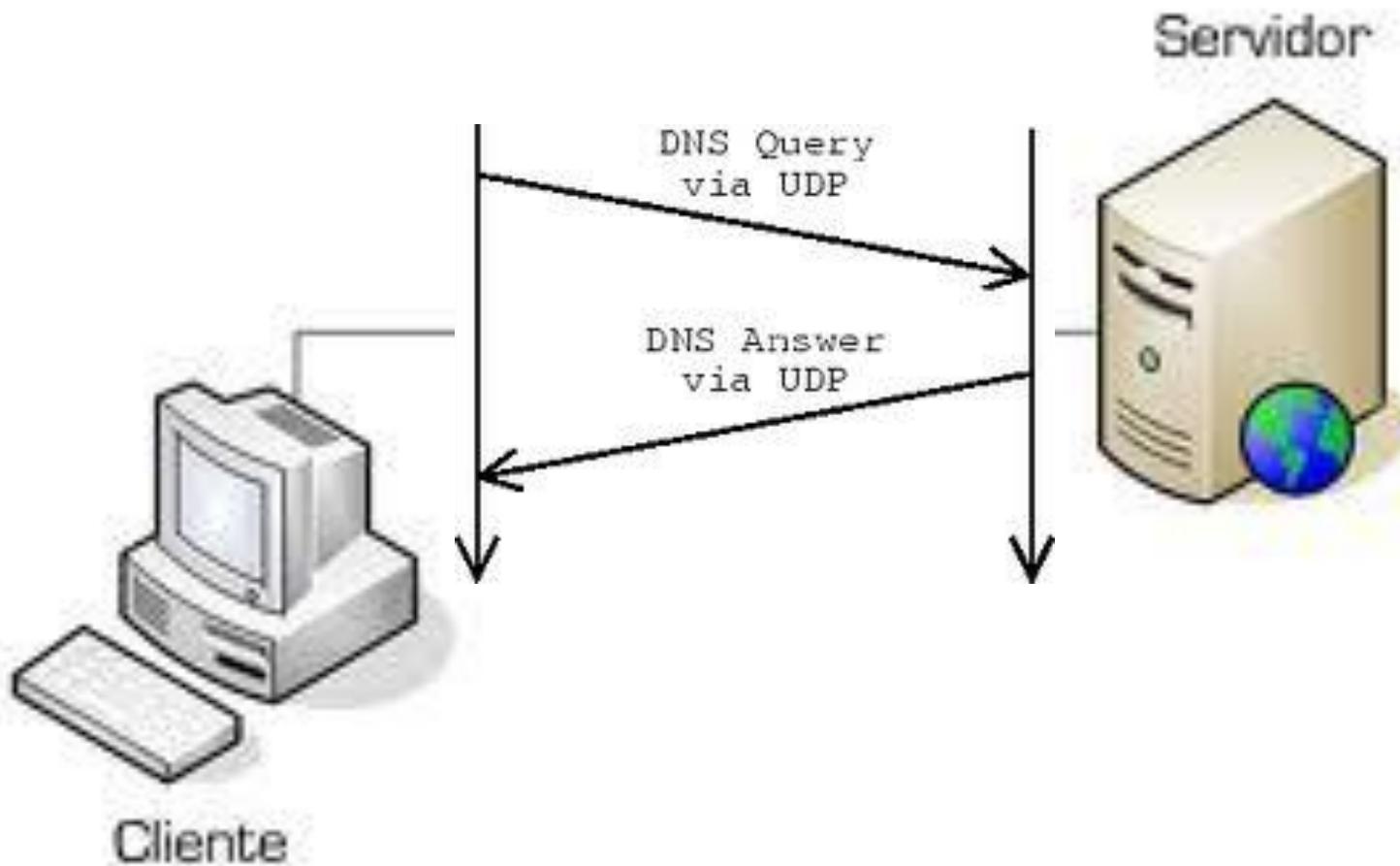
Ação do UDP

- Fornece uma interface para o protocolo IP com o recurso adicional de multiplexação / demultiplexação de vários processos que utilizam as portas

Funcionamento Básico do UDP

- Cliente envia uma solicitação curta para o servidor
- Cliente aguarda por uma resposta curta
- Quando o cliente não recebe a resposta, ele aguarda um timeout e tenta novamente

Exemplo de Aplicação do UDP



Porque existe um UDP?

- Não há estabelecimento de conexão e portanto não introduz atrasos
- Não há estado de conexão nem no emissor e nem no receptor
- Pequeno *overhead* no cabeçalho do pacote
- Taxa de envio não regulada (não há controle de congestionamento)

Onde Usamos o UDP

- Aplicações cliente-servidor em que existe apenas uma requisição e uma resposta
- O custo para estabelecer uma conexão é alto quando comparado com a transferência de dado
- Aplicações de multimídia contínua (*streaming*)
 - ◆ Tolerantes à perda
 - ◆ Sensíveis à taxa

Exemplo de Aplicações UDP e TCP

Aplicação	Protocolo de camada de aplicação	Protocolo de transporte
Correio eletrônico	SMTP	TCP
Acesso a terminal remoto	Telnet	TCP
Web	HTTP	TCP
Transferência de arquivo	FTP	TCP
Servidor remoto de arquivo	NFS	UDP
Recepção de multimídia	proprietário	UDP
Telefonia por Internet	proprietário	UDP
Gerenciamento de rede	SNMP	UDP
Protocolo de roteamento	RIP	UDP
Tradução de nome	DNS	UDP

TCP

Transport Control Protocol

RFCs: 793, 1122, 1323, 2018, 2581

Introdução

- O TCP fornece um fluxo de bytes fim a fim confiável em uma sub-rede não confiável
- O TCP foi projetado para se adaptar dinamicamente às propriedades da sub-rede e ser robusto diante dos diversos tipos de falhas que podem ocorrer
- A principal arquitetura da Internet é o TCP/IP

Características do TCP

- Transferência confiável de dados: o TCP garante que os dados serão entregues da forma que foram enviados
- Orientado à conexões: conexões são gerenciadas nos sistemas finais
- Controle de fluxo: o emissor não esgota a capacidade do receptor

Características do TCP

- Controle de congestionamento: Emissor não esgota os recursos da rede
- Gerenciamento de temporizadores: o TCP necessita de vários temporizadores para realizar seu trabalho

Modelo de Serviço do TCP

- O TCP aceita os fluxos de dados das aplicações e os divide em segmentos de no máximo 65495 bytes
 - ◆ Fluxo de bytes é diferente de fluxo de mensagens
 - ◆ Normalmente, usamos 1460 bytes de dados fazendo com que cada segmento caiba em um único quadro Ethernet

Modelo de Serviço do TCP

- Em seguida, o TCP envia cada segmento para a camada de rede
- Na máquina do destino, os dados são entregues à entidade TCP e essa restaura os fluxos originais

Modelo de Serviço do TCP

- A entidade TCP receptora retorna um segmento (com ou sem dados) com um número de confirmação igual ao próximo número de sequência que espera receber
- Quando o emissor não recebe uma confirmação de um segmento cujo timeout expirou, o emissor retransmite esse segmento

Modelo de Serviço do TCP

- Usa um serviço não confiável para prover um serviço de entrega de dados confiável para as aplicações
- Deve ser capaz de compensar perdas e atrasos na sub-rede de comunicação de tal forma a prover o transporte de dados fim a fim de forma eficiente
- Deve ser capaz de executar essas tarefas sem sobrecarregar a sub-rede de comunicação e os roteadores

Modelo de Serviço do TCP

- O serviço TCP é obtido quando tanto o emissor quanto o receptor criam pontos extremos chamados **soquetes**
 - ◆ Identificação do soquete = endereço IP do host (32 bits) + número de porta (16 bits)
 - ◆ As portas abaixo de 1024 são denominadas portas bem conhecidas (*well-known ports*) e são reservadas para serviços tradicionais

Modelo de Serviço do TCP

- Algumas portas bem conhecidas:

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial file transfer protocol
79	Finger	Lookup information about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

Modelo de Serviço do TCP

- O serviço do TCP é baseado na existência de uma conexão entre um soquete da máquina de origem e outro na de destino
- Fases do TCP
 - ◆ Estabelecimento da conexão
 - ◆ Transferência de dados
 - ◆ Término da conexão

Modelo de Serviço do TCP

- As conexões são identificadas pelos soquetes das máquinas de origem e de destino, ou seja, cada conexão é identificada por:
 - ◆ Endereço IP origem
 - ◆ Porta origem
 - ◆ Endereço IP destino
 - ◆ Porta destino
- Um soquete pode ser utilizado por várias conexões ao mesmo tempo (duas ou mais conexões podem terminar no mesmo soquete)

Modelo de Serviço do TCP

- Todas as conexões TCP são *full-duplex* e ponto a ponto
 - ◆ Tráfego pode ser feito em ambas as direções ao mesmo tempo
 - ◆ Cada conexão possui exatamente dois pontos terminais
 - ◆ O TCP não admite multidifusão e difusão

Primitivas de Sockets para TCP

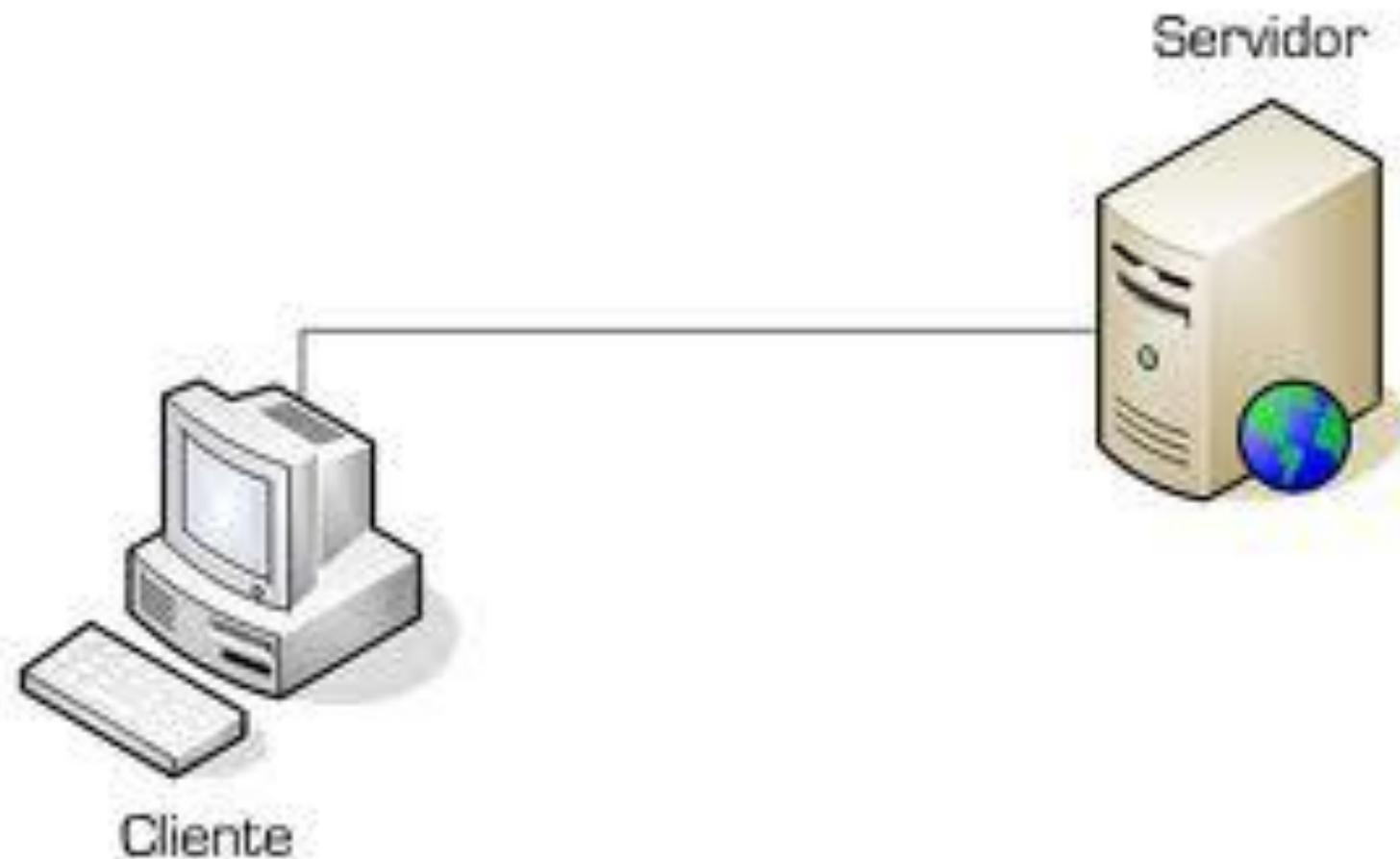
Primitiva	Significado
SOCKET	Criar um novo ponto final de comunicação
BIND	Anexar um endereço local a um soquete
LISTEN	Anunciar a disposição para aceitar conexões; mostrar o tamanho da fila
ACCEPT	Bloquear o responsável pela chamada até uma tentativa de conexão ser recebida
CONNECT	Tentar estabelecer uma conexão ativamente
SEND	Enviar alguns dados através da conexão
RECEIVE	Receber alguns dados da conexão
CLOSE	Encerrar a conexão

Primitivas de Sockets para TCP

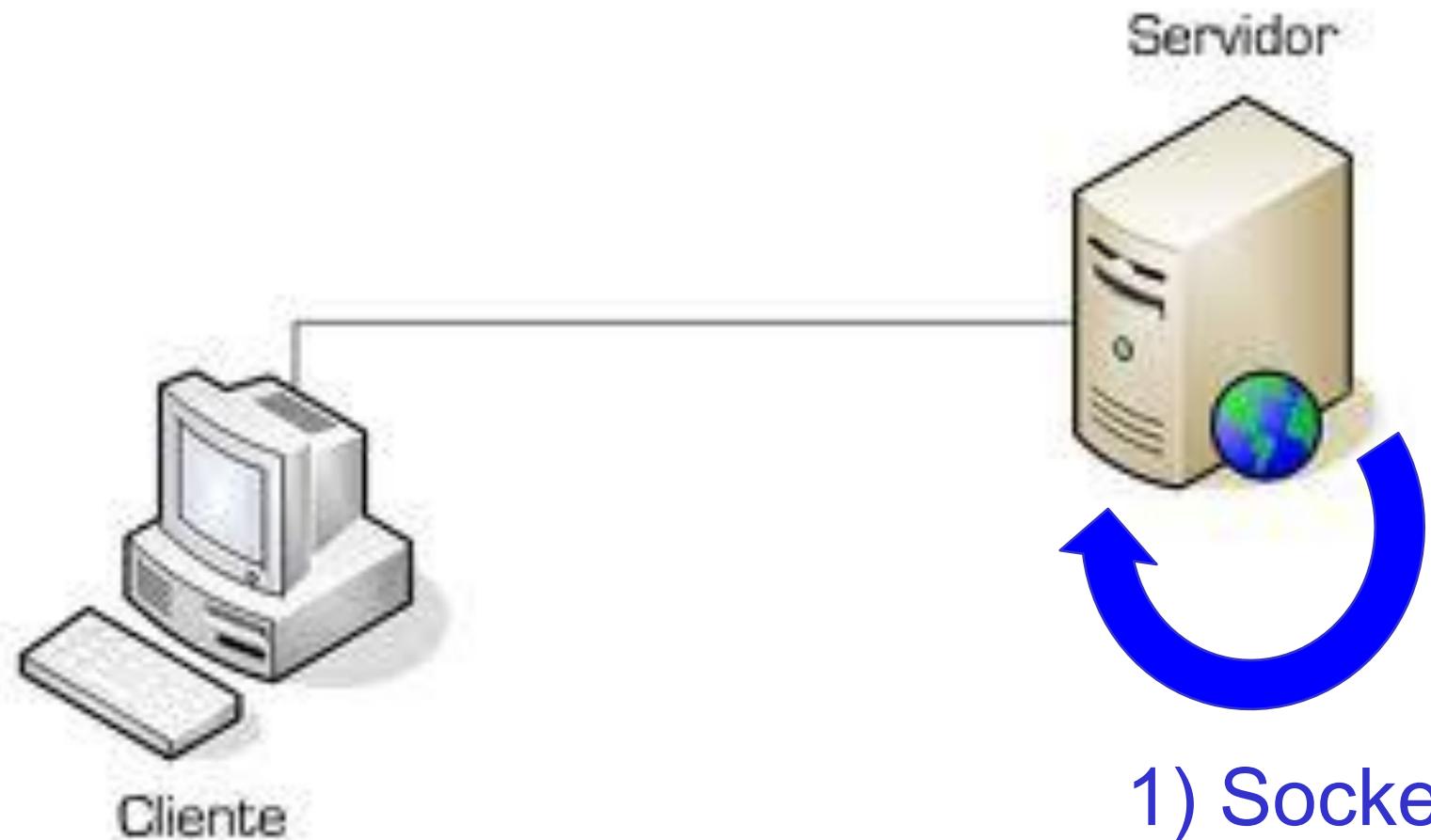
Primitiva	Significado
SOCKET	Criar um novo ponto final de comunicação
BIND	Anexar um endereço local a um soquete
LISTEN	Anunciar a disposição para aceitar conexões; mostrar o tamanho da fila
ACCEPT	Bloquear o responsável pela chamada até uma tentativa de conexão ser recebida

As quatro primeiras primitivas são executadas pelo servidor nessa mesma ordem

Primitivas de Sockets para TCP

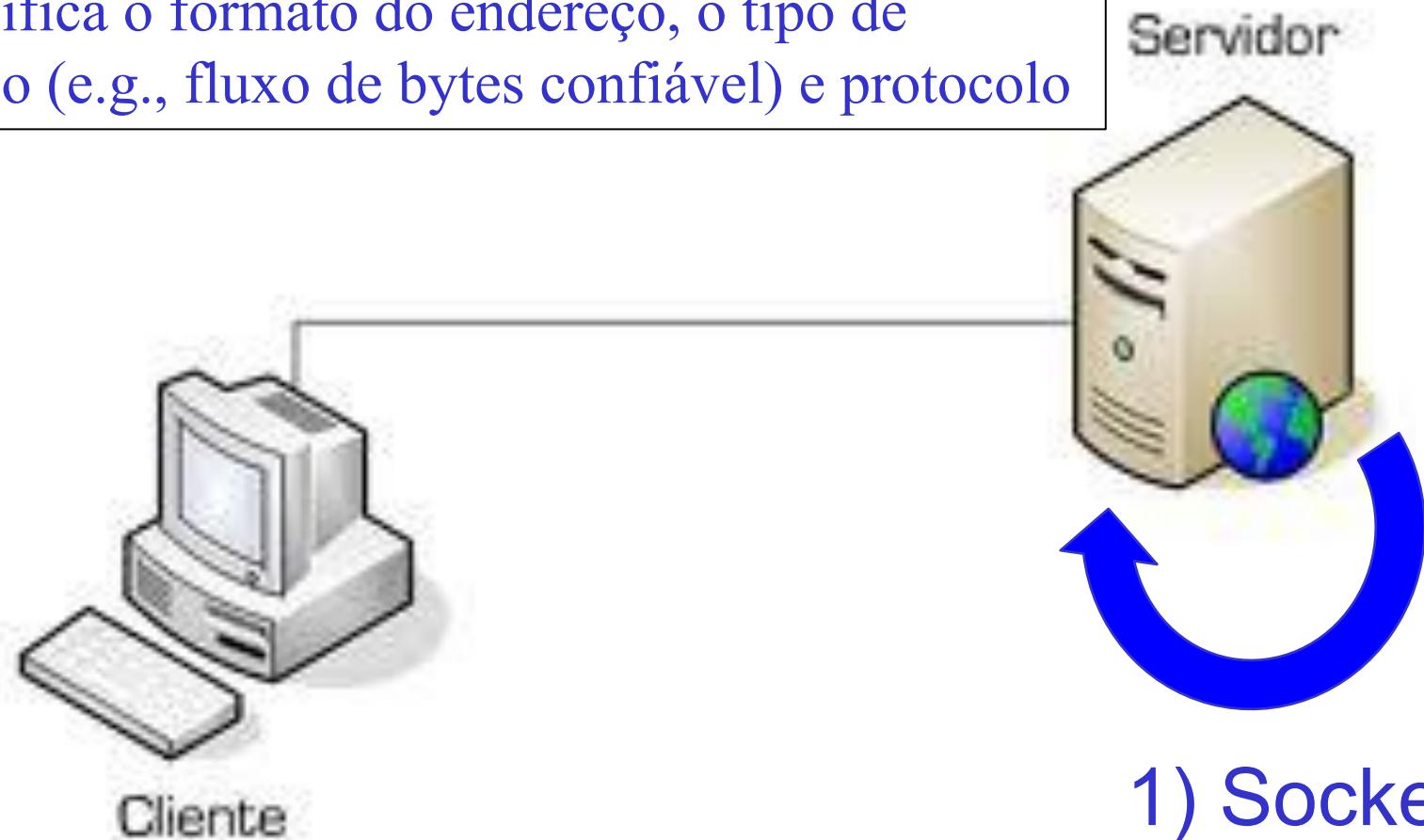


Primitivas de Sockets para TCP

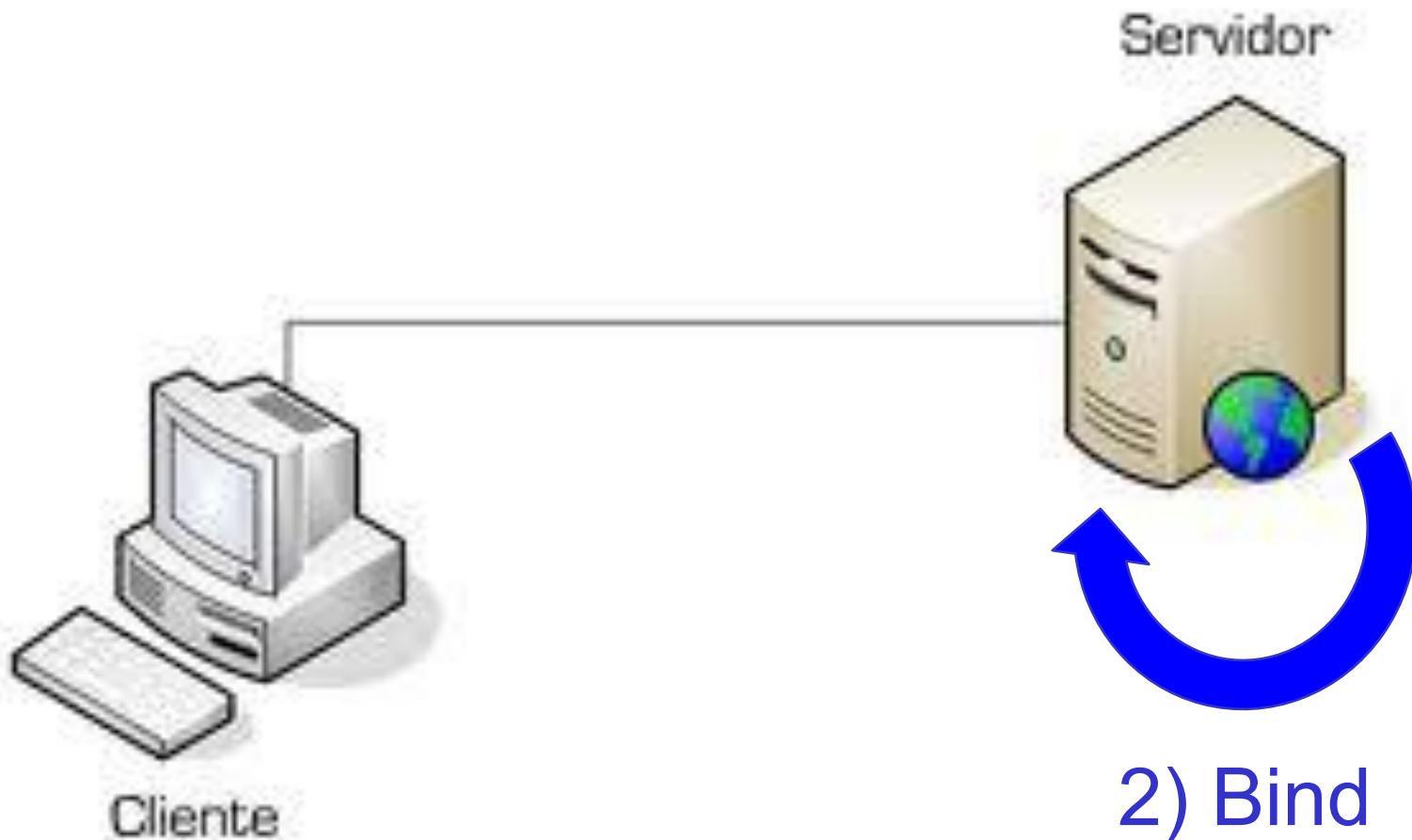


Primitivas de Sockets para TCP

Especifica o formato do endereço, o tipo de serviço (e.g., fluxo de bytes confiável) e protocolo

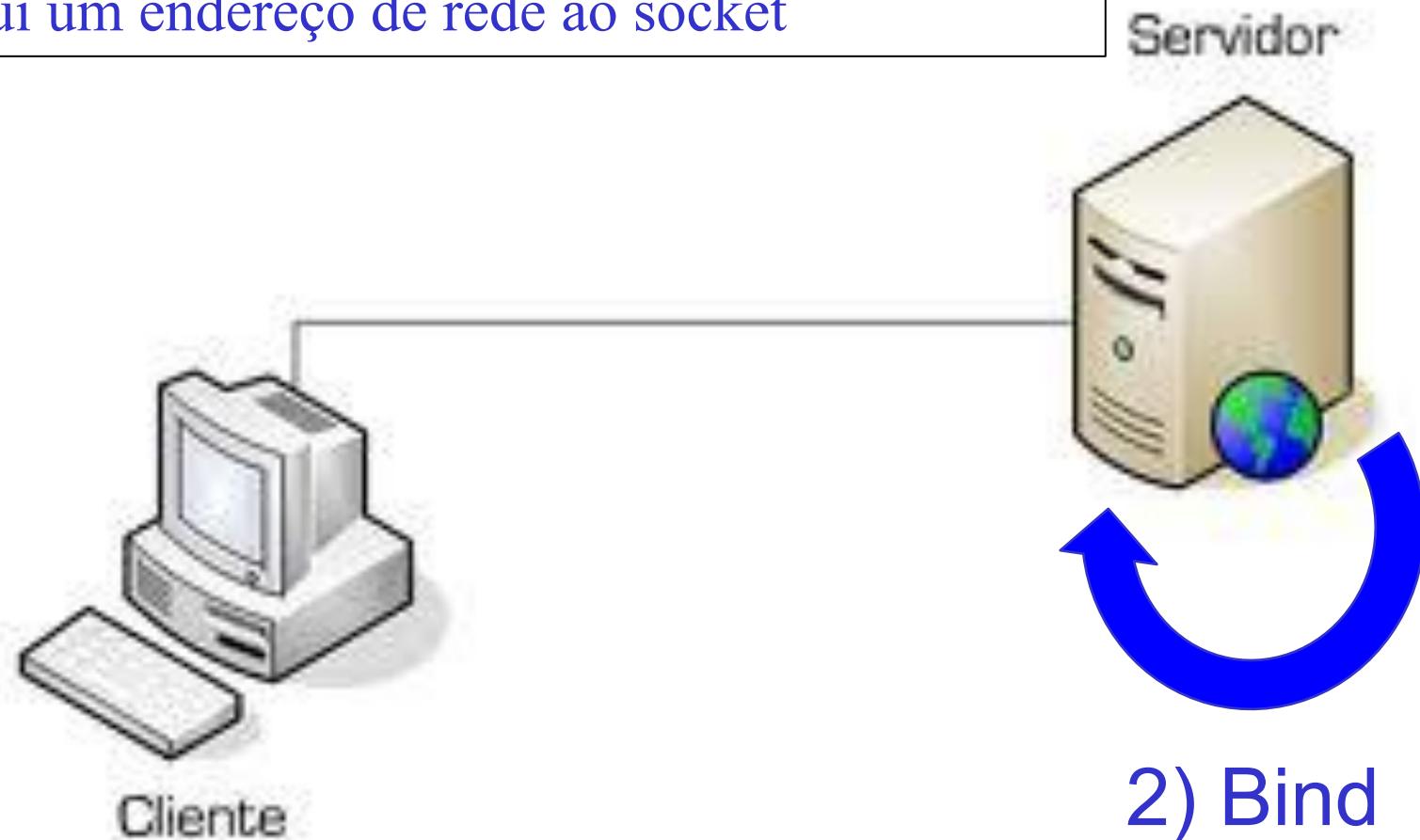


Primitivas de Sockets para TCP



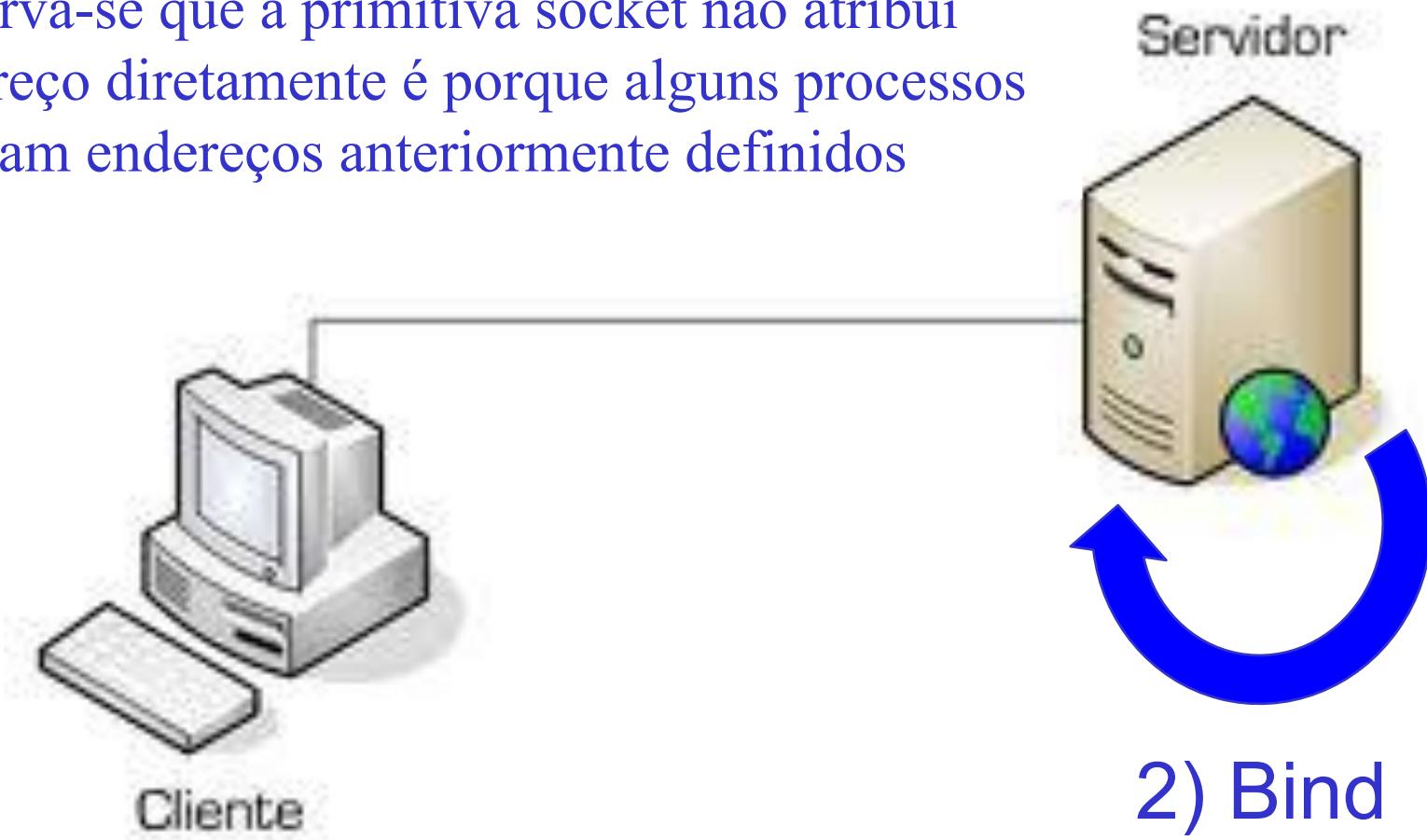
Primitivas de Sockets para TCP

Atribui um endereço de rede ao socket



Primitivas de Sockets para TCP

Observa-se que a primitiva socket não atribui endereço diretamente é porque alguns processos utilizam endereços anteriormente definidos



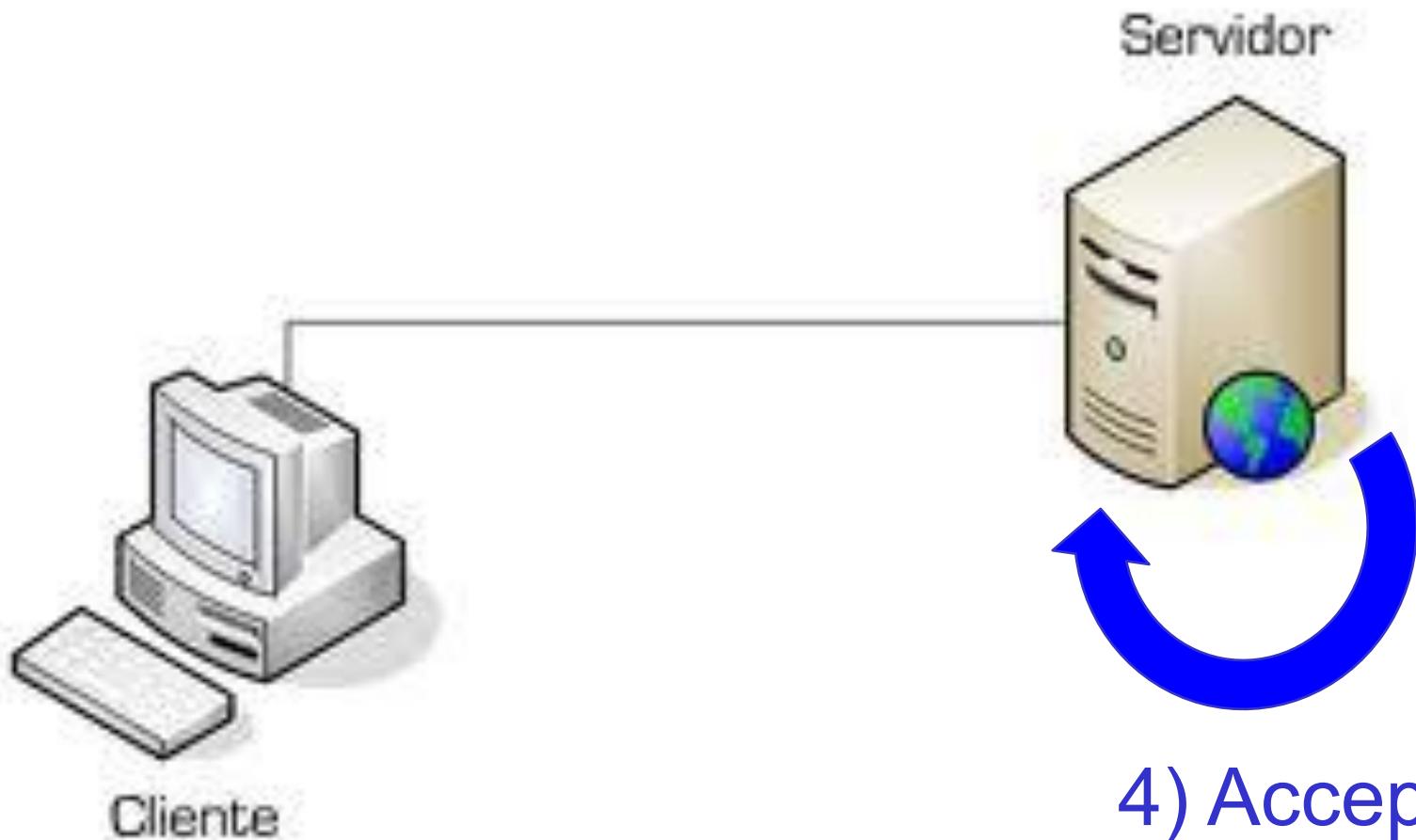
2) Bind

Primitivas de Sockets para TCP

Aloca espaço para a fila de chamadas recebidas

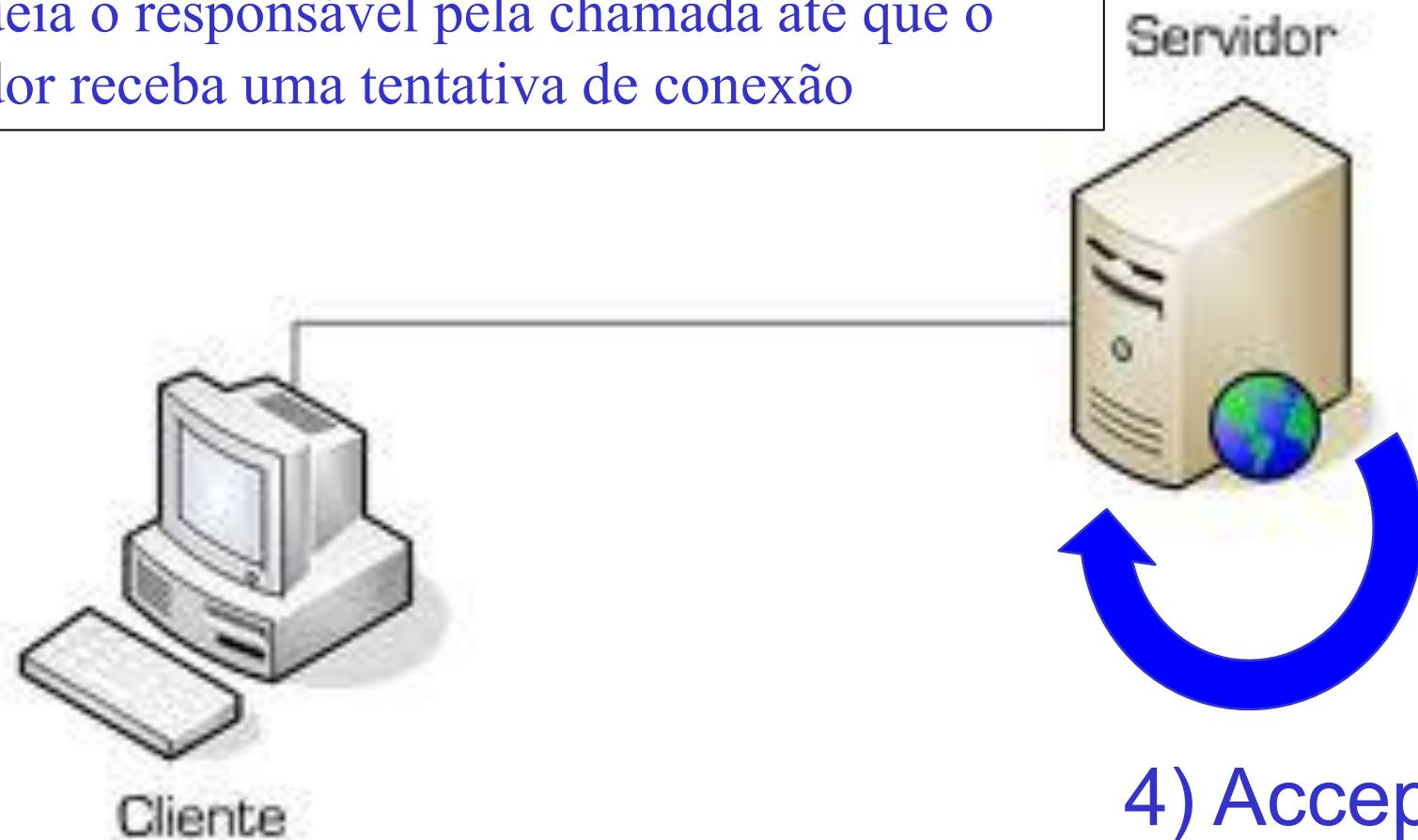


Primitivas de Sockets para TCP



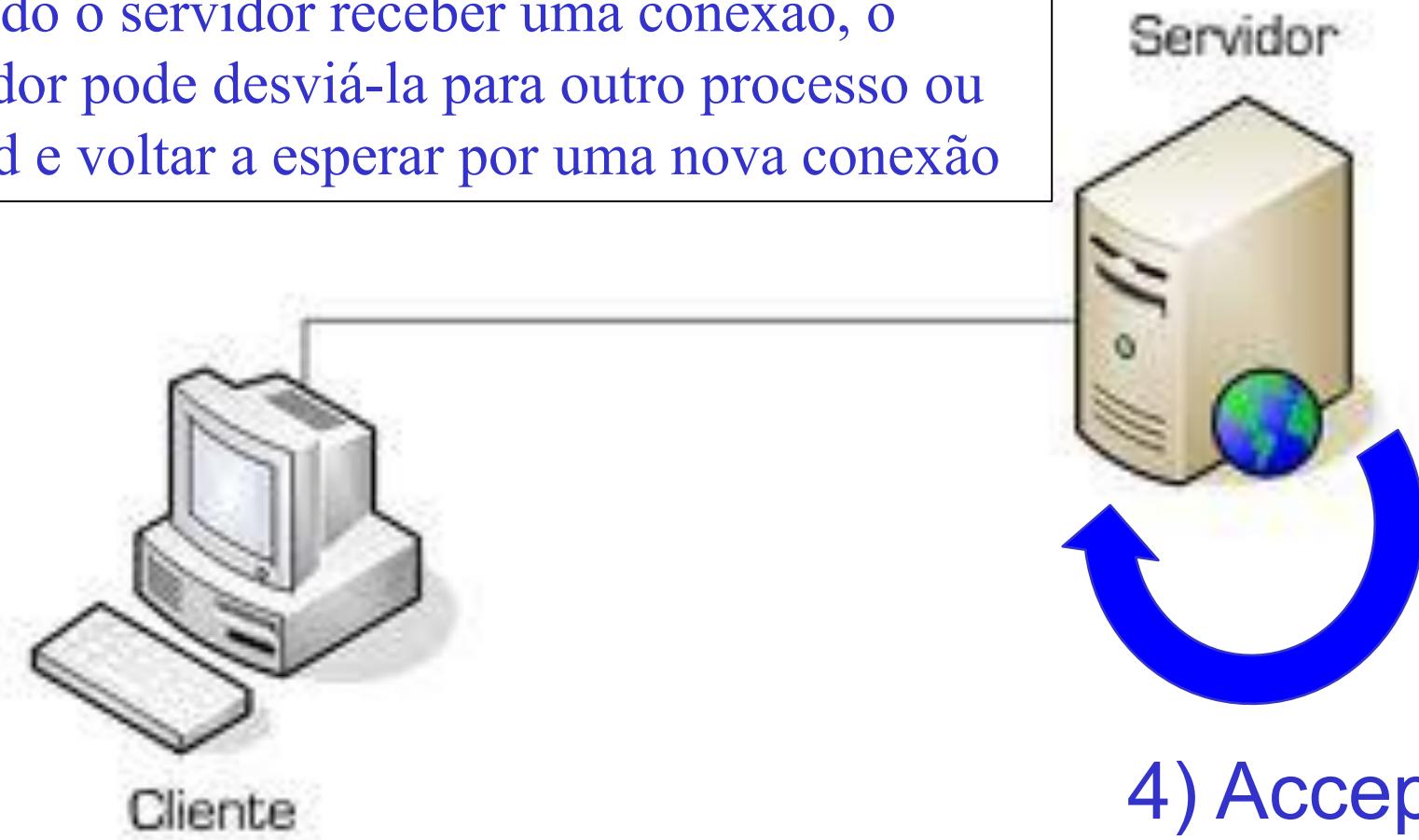
Primitivas de Sockets para TCP

Bloqueia o responsável pela chamada até que o servidor receba uma tentativa de conexão



Primitivas de Sockets para TCP

Quando o servidor receber uma conexão, o servidor pode desviá-la para outro processo ou thread e voltar a esperar por uma nova conexão

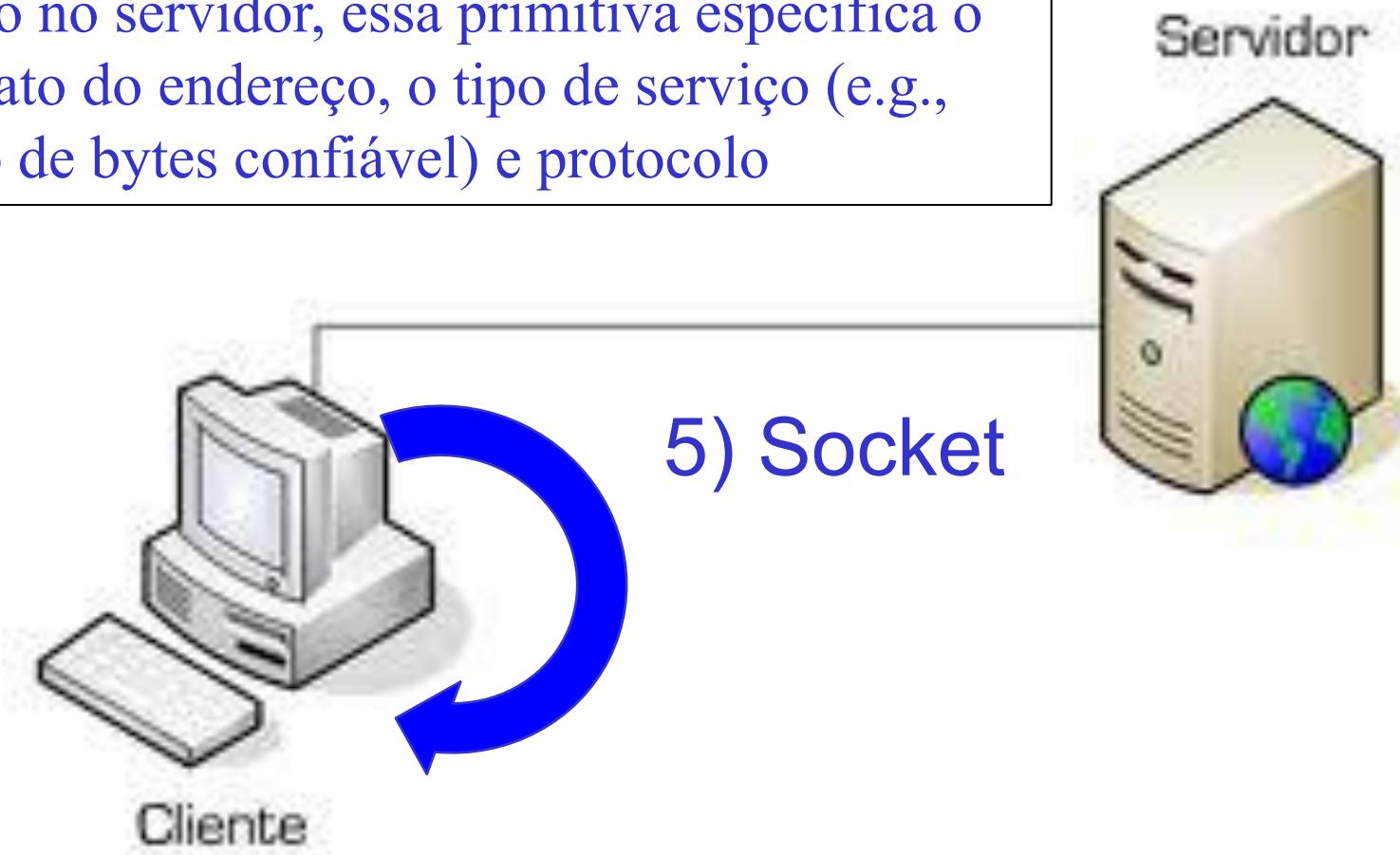


Primitivas de Sockets para TCP

Vamos para o
lado do cliente

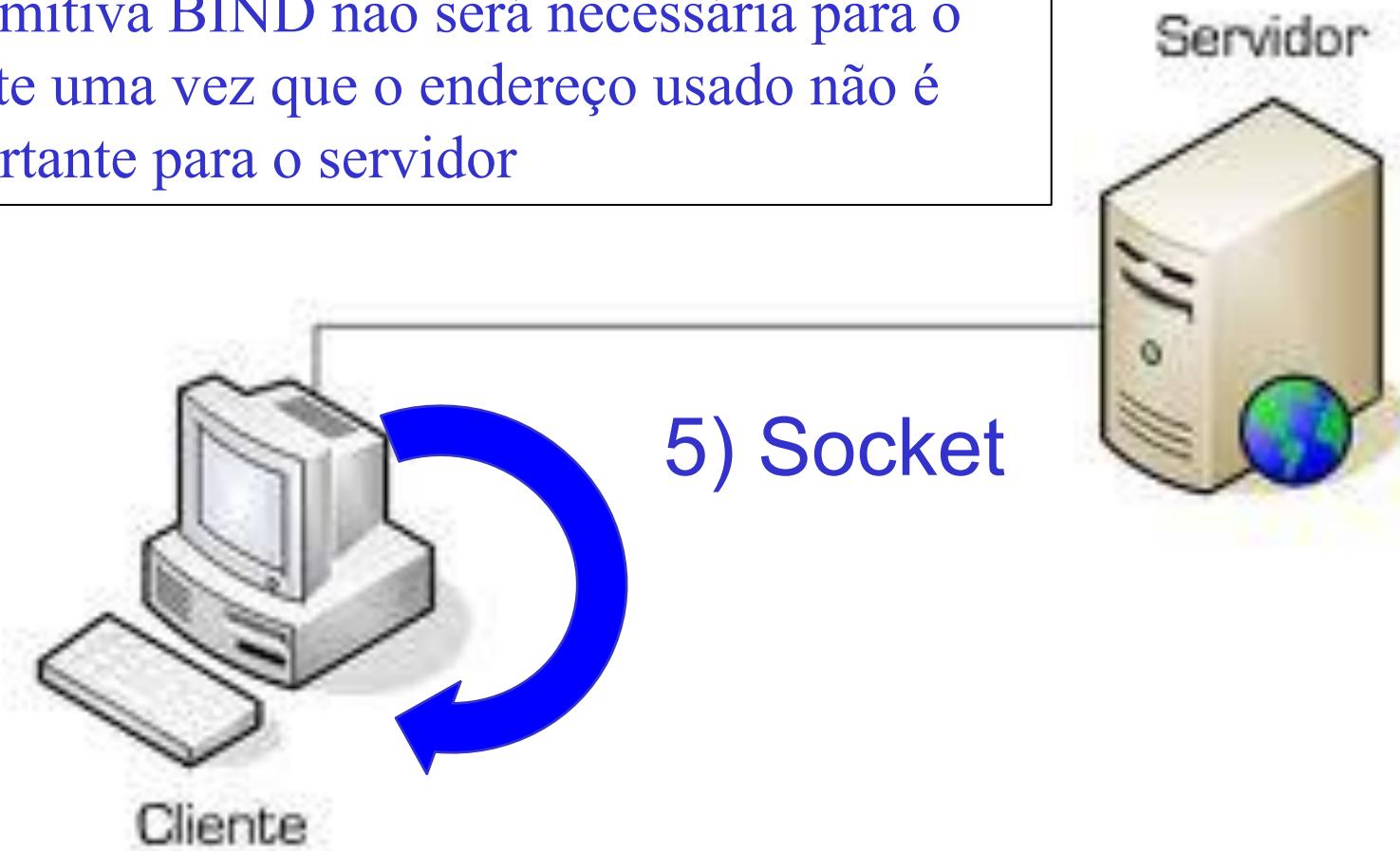
Primitivas de Sockets para TCP

Como no servidor, essa primitiva especifica o formato do endereço, o tipo de serviço (e.g., fluxo de bytes confiável) e protocolo

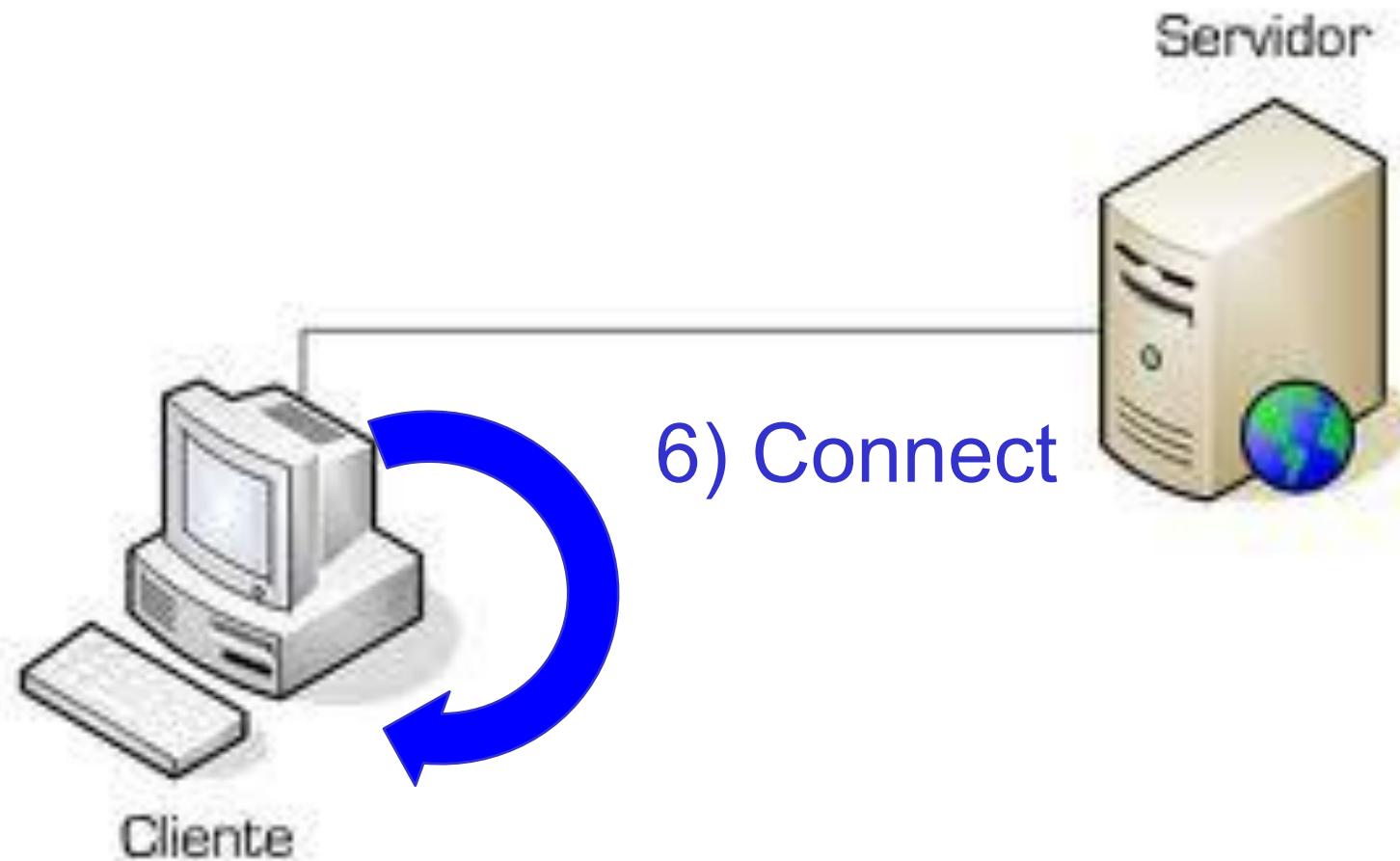


Primitivas de Sockets para TCP

A primitiva BIND não será necessária para o cliente uma vez que o endereço usado não é importante para o servidor



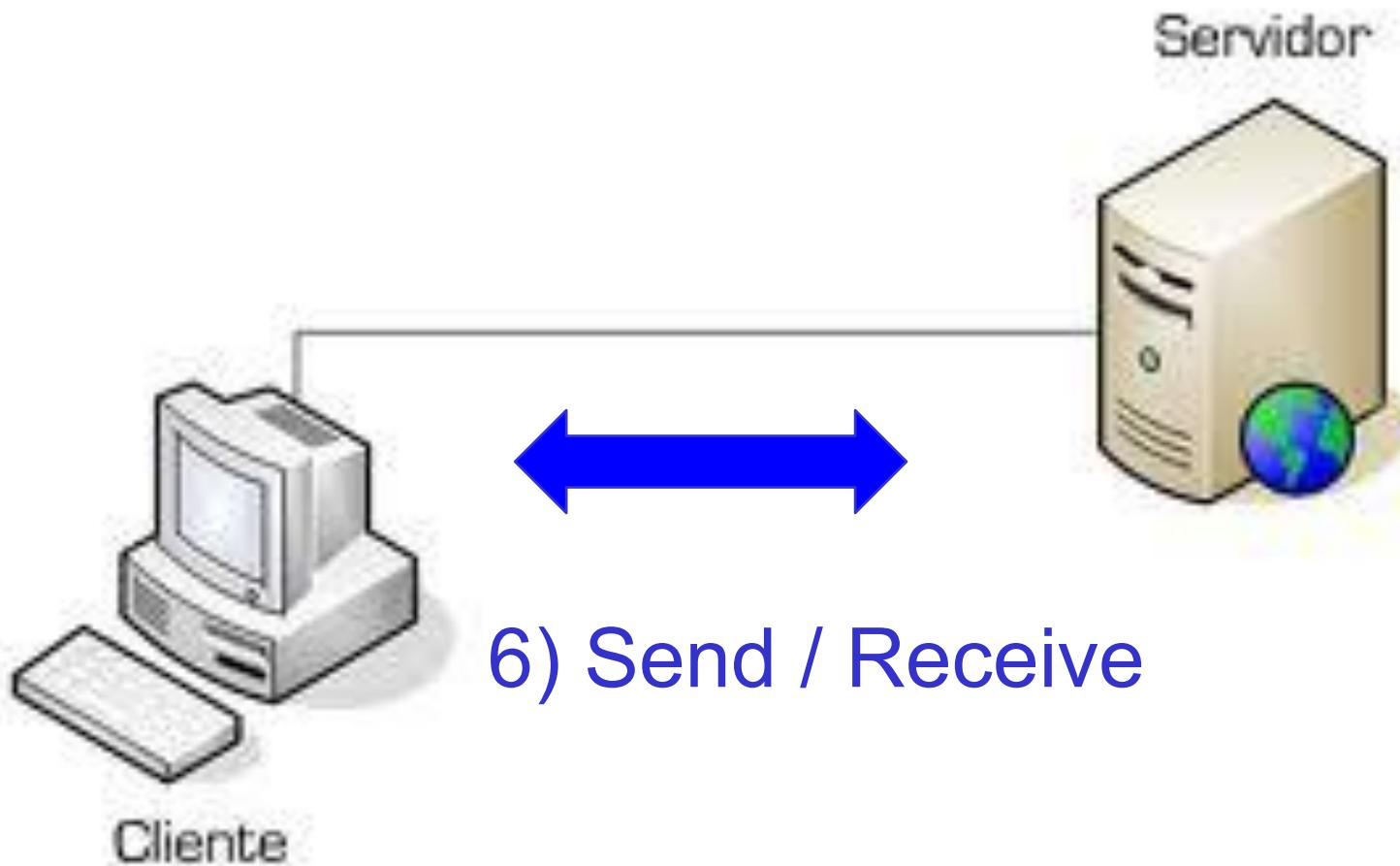
Primitivas de Sockets para TCP



Primitivas de Sockets para TCP

Primitiva	Significado
SOCKET	Criar um novo ponto final de comunicação
BIND	Anexar um endereço local a um soquete
LISTEN	Anunciar a disposição para aceitar conexões; mostrar o tamanho da fila
ACCEPT	Bloquear o responsável pela chamada até uma tentativa de conexão ser recebida
CONNECT	Tentar estabelecer uma conexão ativamente
SEND	Enviar alguns dados através da conexão
RECEIVE	Receber alguns dados da conexão
CLOSE	Encerrar a conexão

Primitivas de Sockets para TCP



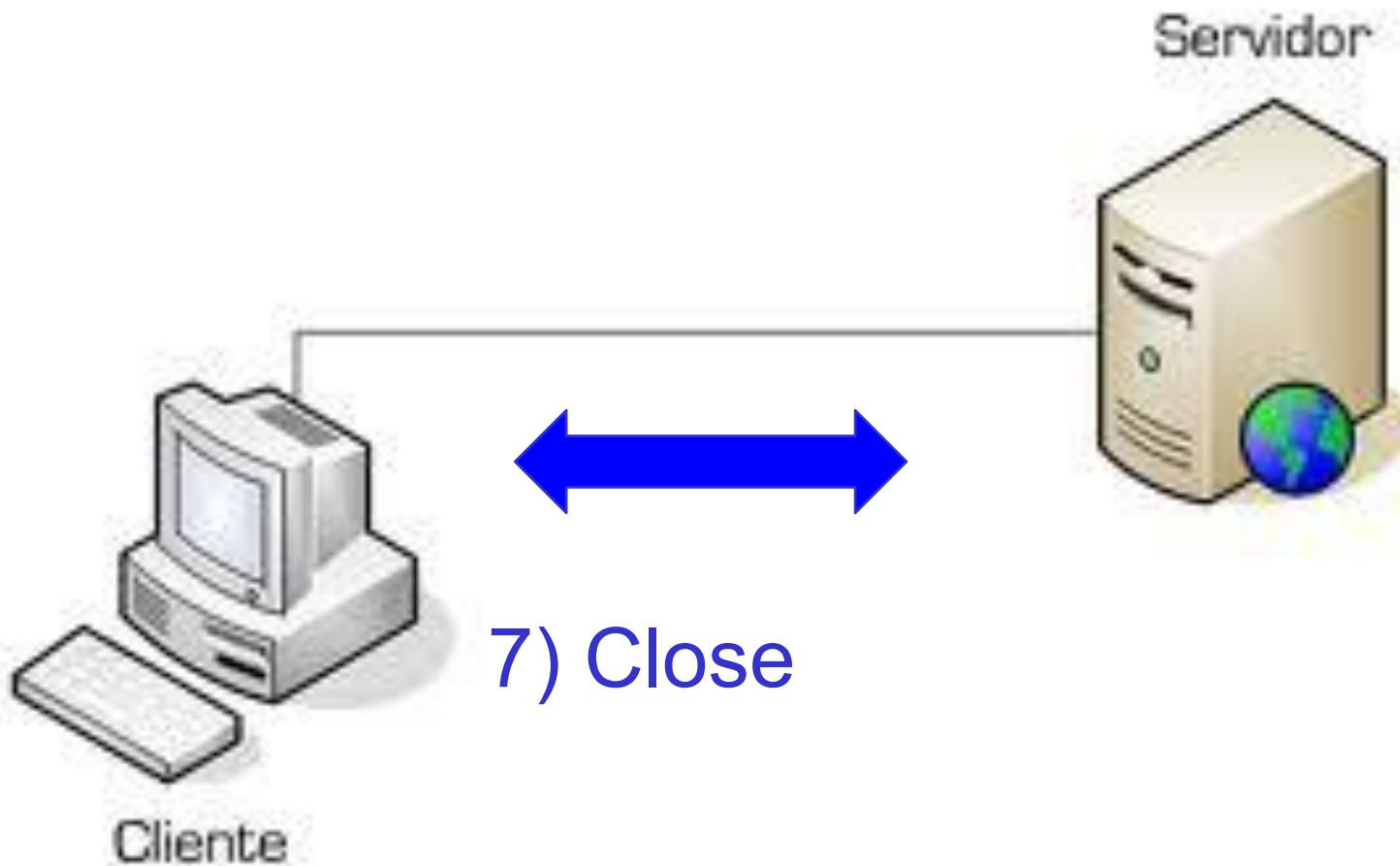
Primitivas de Sockets para TCP

As partes devem ter uma política para definir de quem é a vez de enviar dados



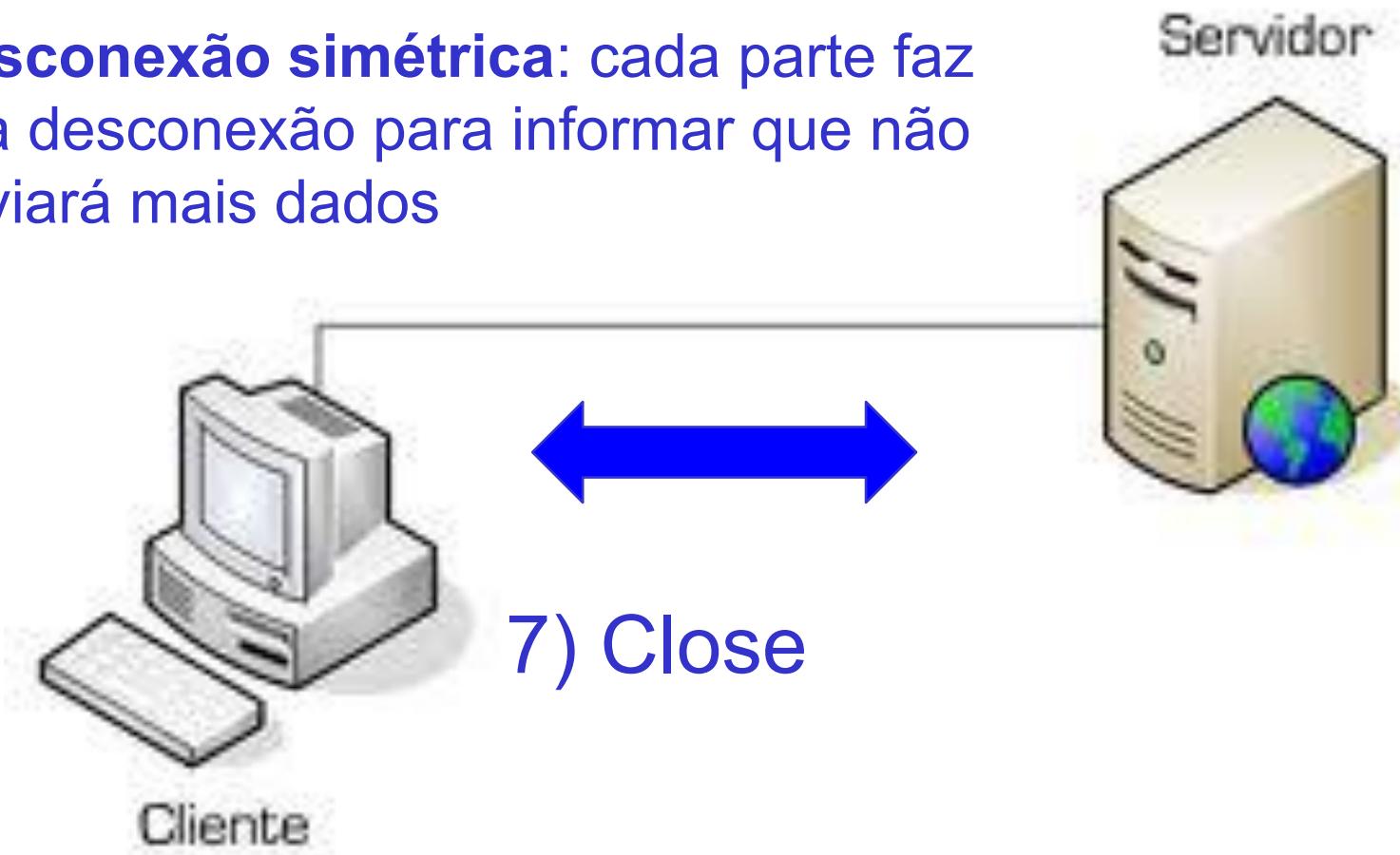
6) Send / Receive

Primitivas de Sockets para TCP

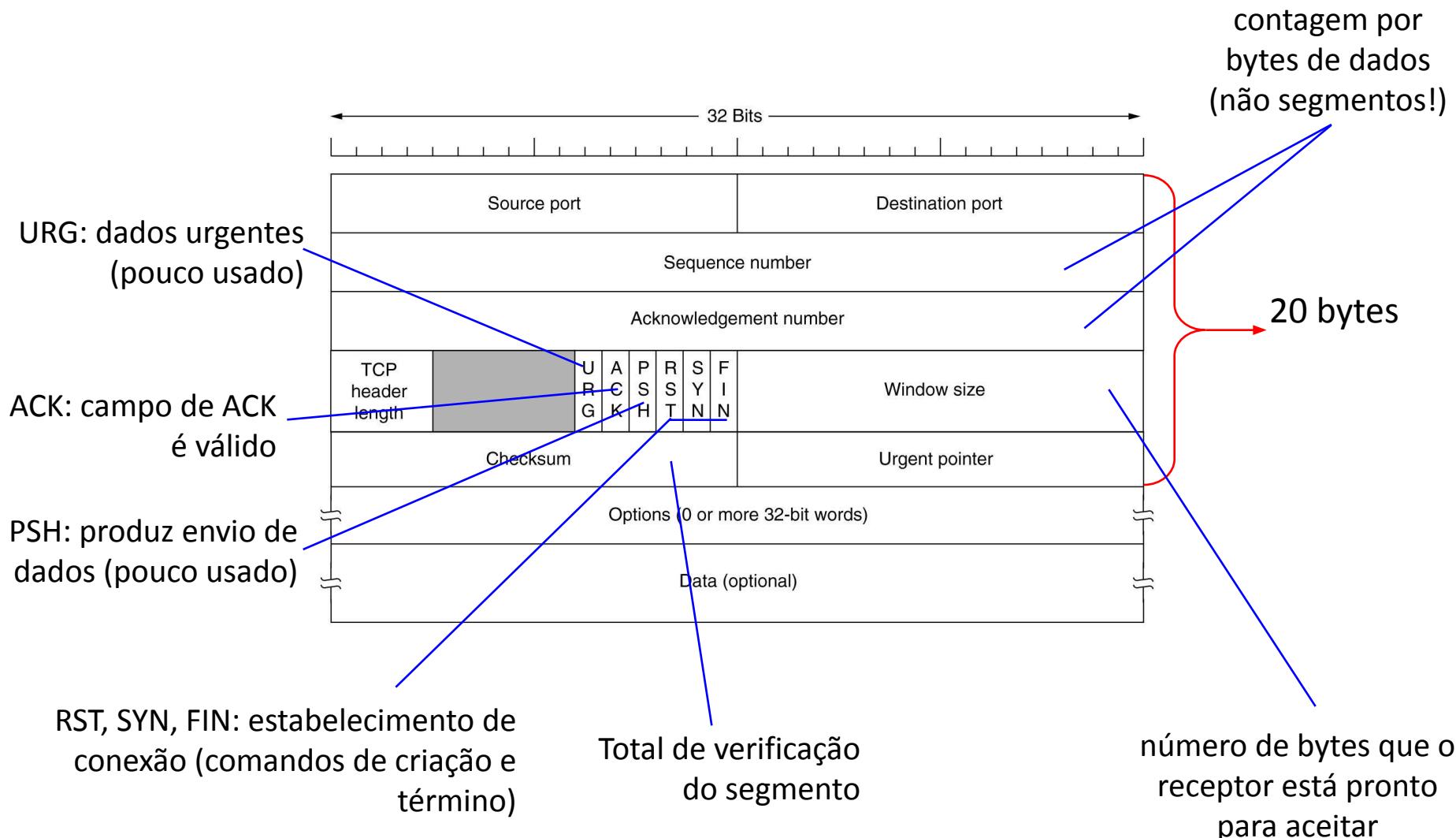


Primitivas de Sockets para TCP

Desconexão simétrica: cada parte faz sua desconexão para informar que não enviará mais dados

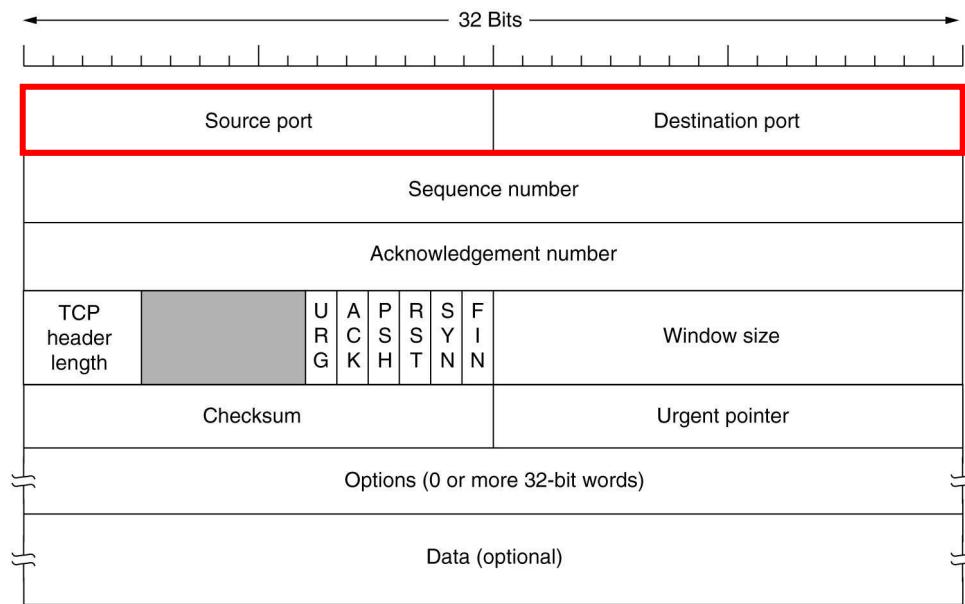


Segmento TCP



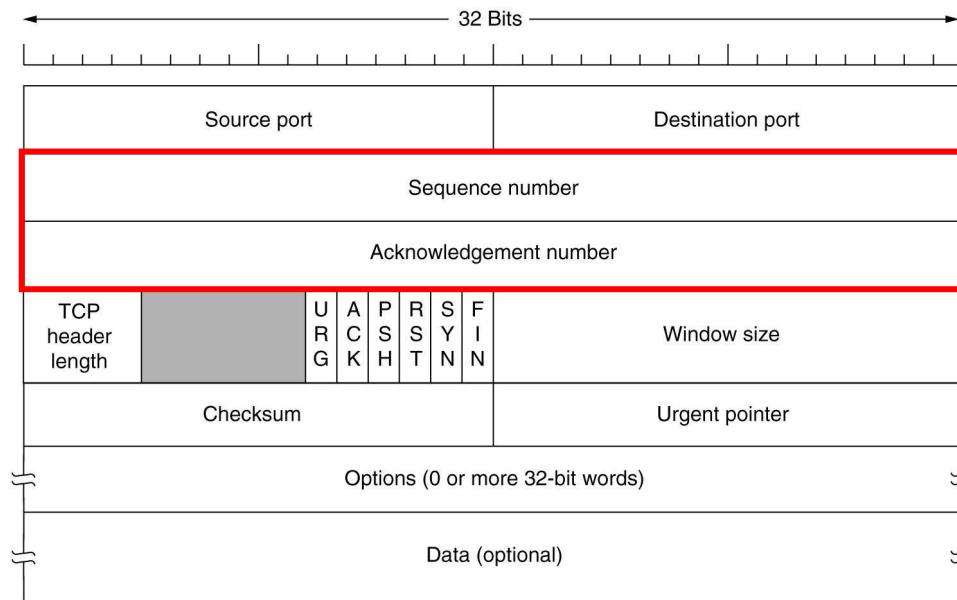
Segmento TCP

- Portas de origem (16 bits) e de destino (16 bits):



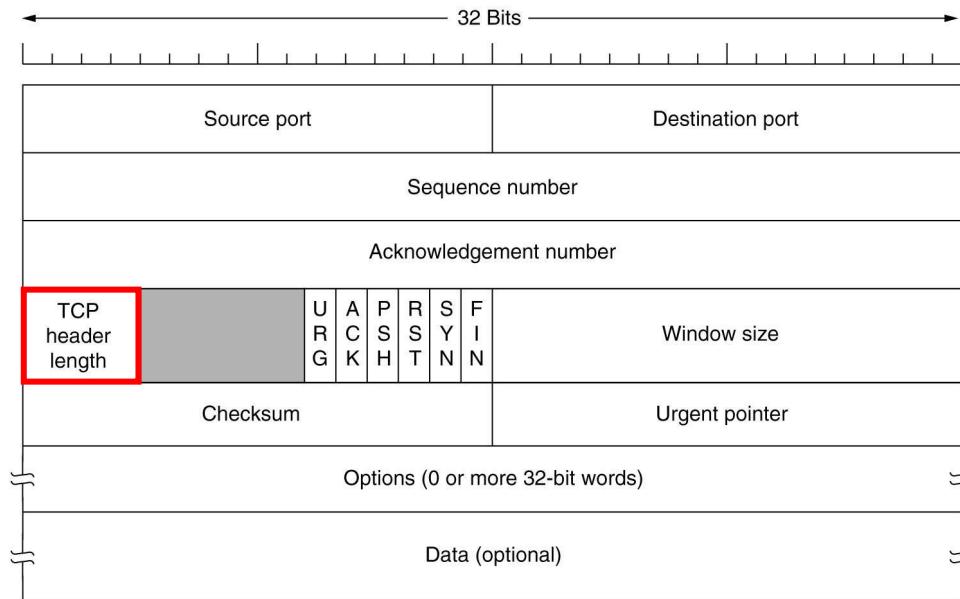
Segmento TCP

- Sequence number (32 bits) e Acknowledgement number (32 bits) □ **Transferência confiável de dados**



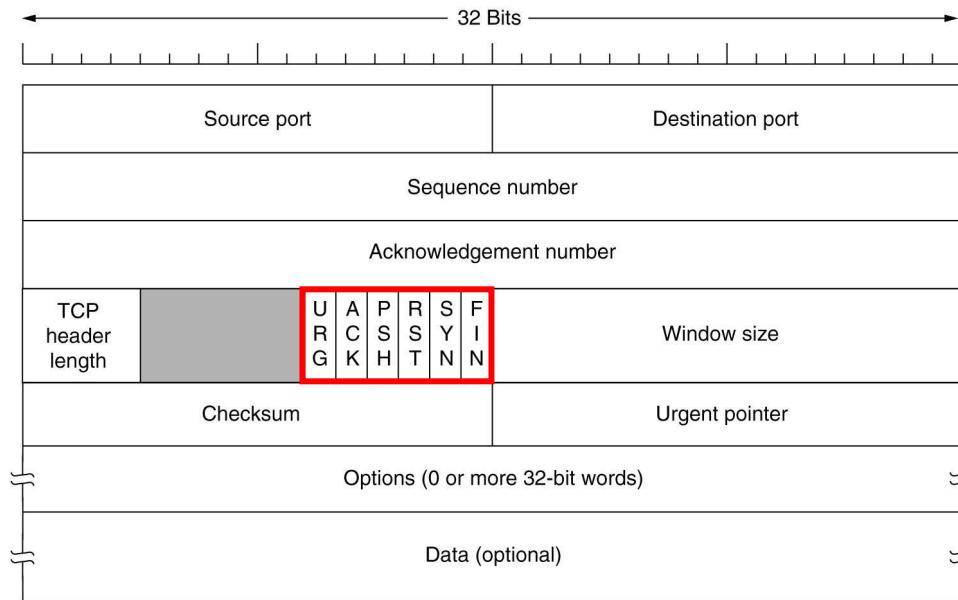
Segmento TCP

- TCP header length (4 bits): informa quantas palavras de 32 bits existem no cabeçalho TCP



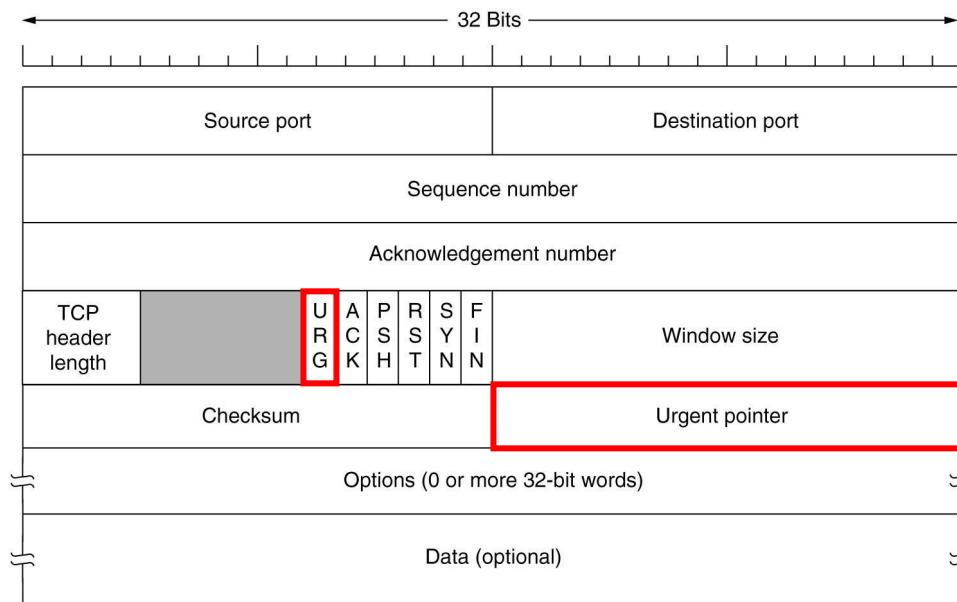
Segmento TCP

- Seis Flags (URG, ACK, PSH, PST, SYN e FIN):



Segmento TCP

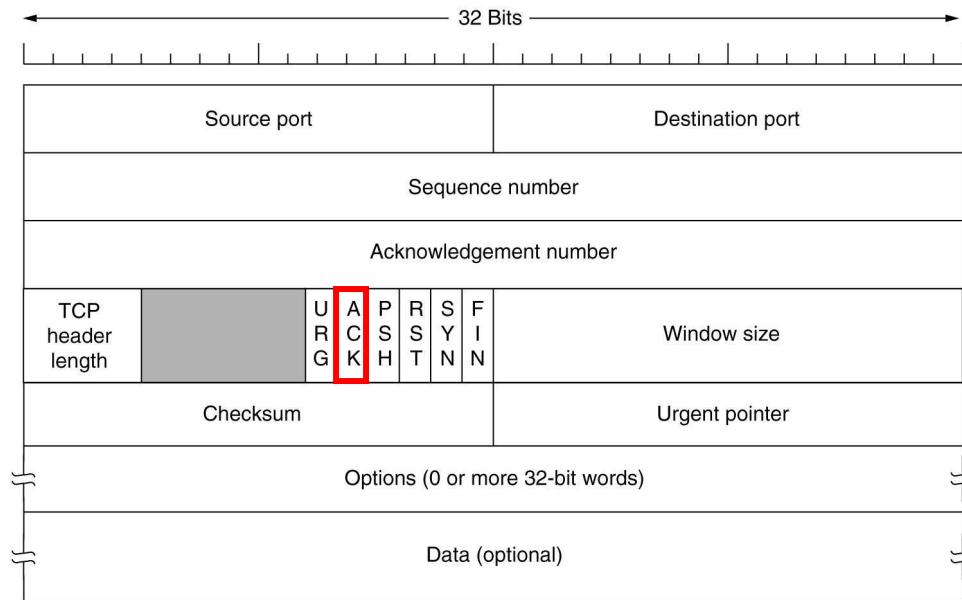
- Bit URG e Urgent pointer (16 bits):
 - ◆ URG = 1, se Urgent pointer estiver sendo usado
 - ◆ Urgent pointer indica o deslocamento de bytes para os dados urgentes (mensagens de interrupção)



Segmento TCP

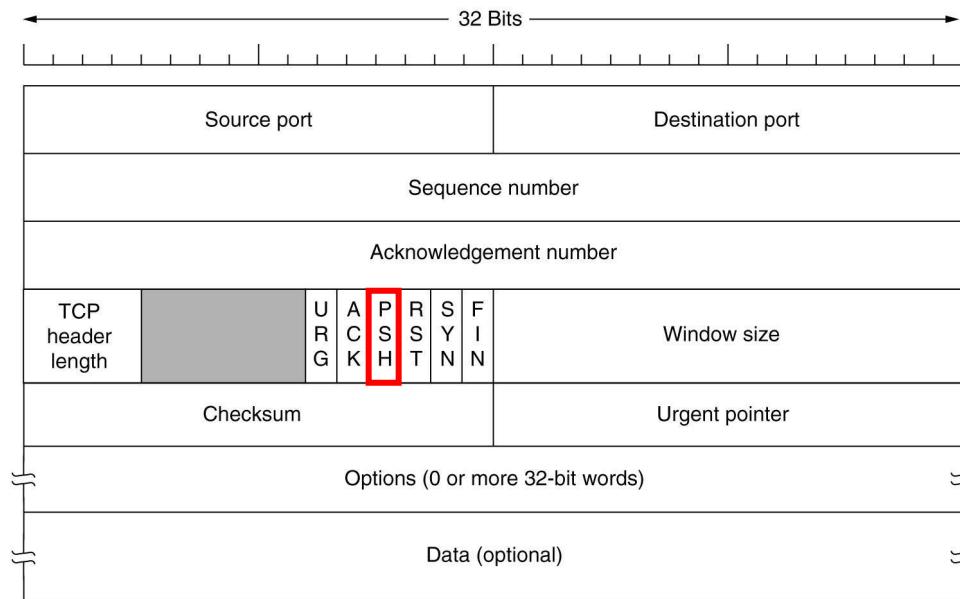
■ Bit ACK:

- ◆ ACK = 1, se o campo *Acknowledgement number* é válido
- ◆ Se ACK = 0, o segmento não contém uma confirmação



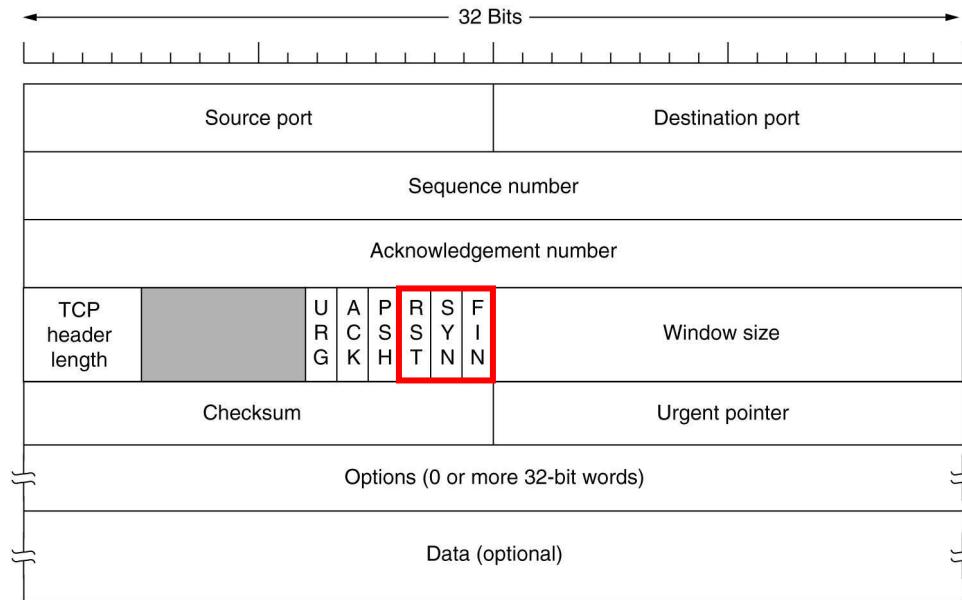
Segmento TCP

- Bit PSH (pouco utilizado):
 - ◆ Informa ao TCP para não retardar a transmissão
 - ◆ O receptor é solicitado a entregar os dados à aplicação imediatamente



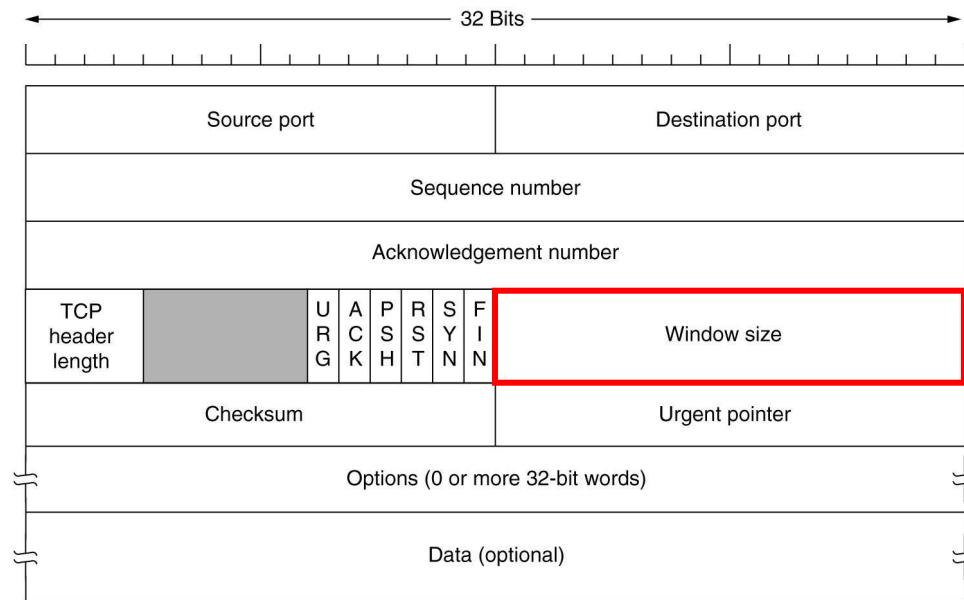
Segmento TCP

- Bits RST, SYN e FIN □ Gerenciamento de conexões



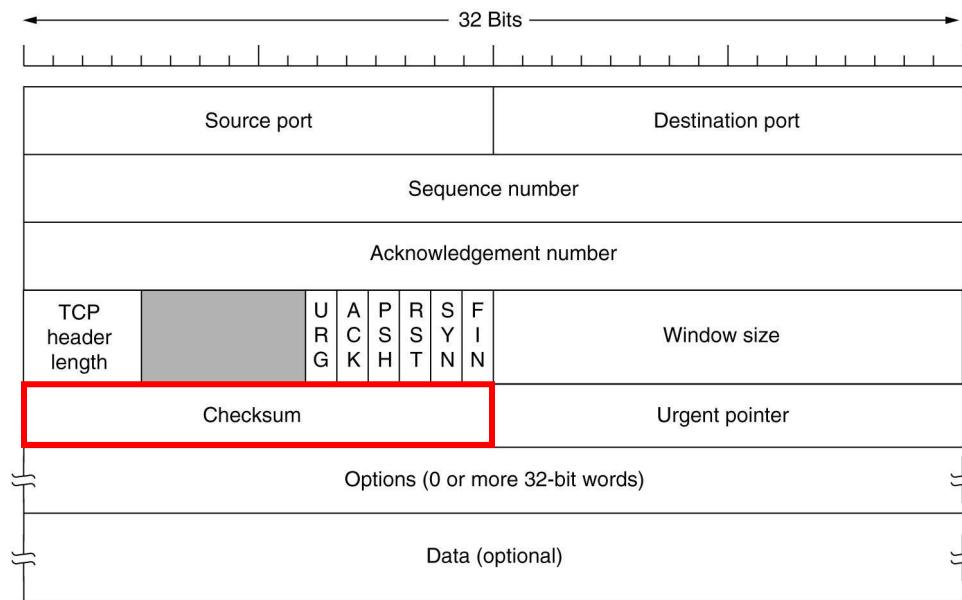
Segmento TCP

- Window size (16 bits) □ Controle de fluxo



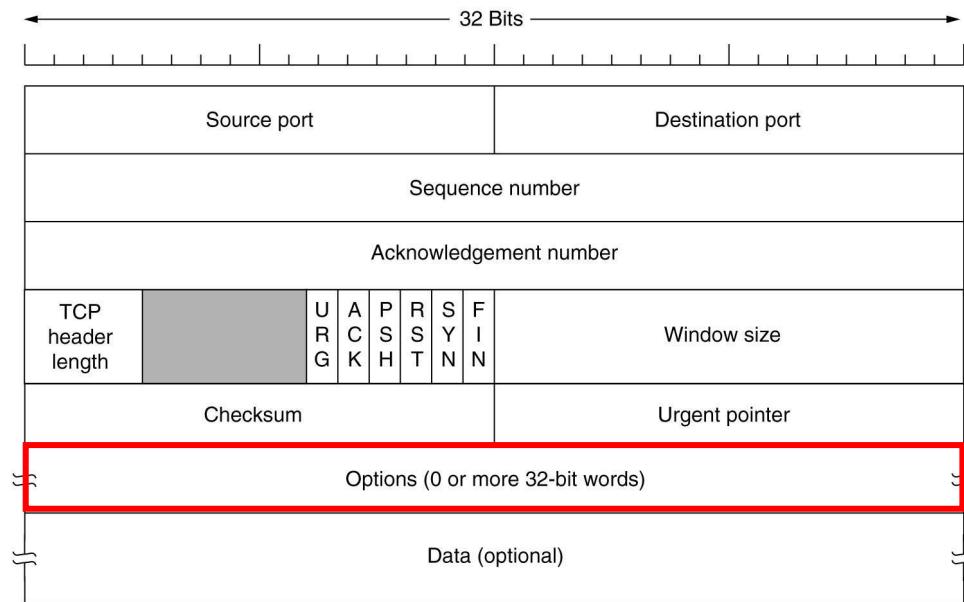
Segmento TCP

- Checksum (16 bits) □ Verificação do segmento



Segmento TCP

- Options (máximo 40 bytes): Forma de oferecer recursos que não foram previstos pelo cabeçalho comum
 - ◆ Ex.: negociação entre os hosts para estipular o máximo de carga útil do TCP



Serviços do TCP

- Transferência Confiável de Dados
- Gerenciamento da Conexão TCP
- Controle de Fluxo
- Controle de Congestionamento
- Gerenciamento de Temporizadores

Transferência Confiável de Dados

- O TCP garante que quando um processo destino lê de seu buffer uma stream, essa:
 - ◆ Não está corrompida
 - ◆ Não tem lacunas
 - ◆ Não possui duplicações
 - ◆ Está em sequência
 - ◆ A cadeia de bytes é exatamente a mesma enviada pelo processo origem

Transferência Confiável de Dados

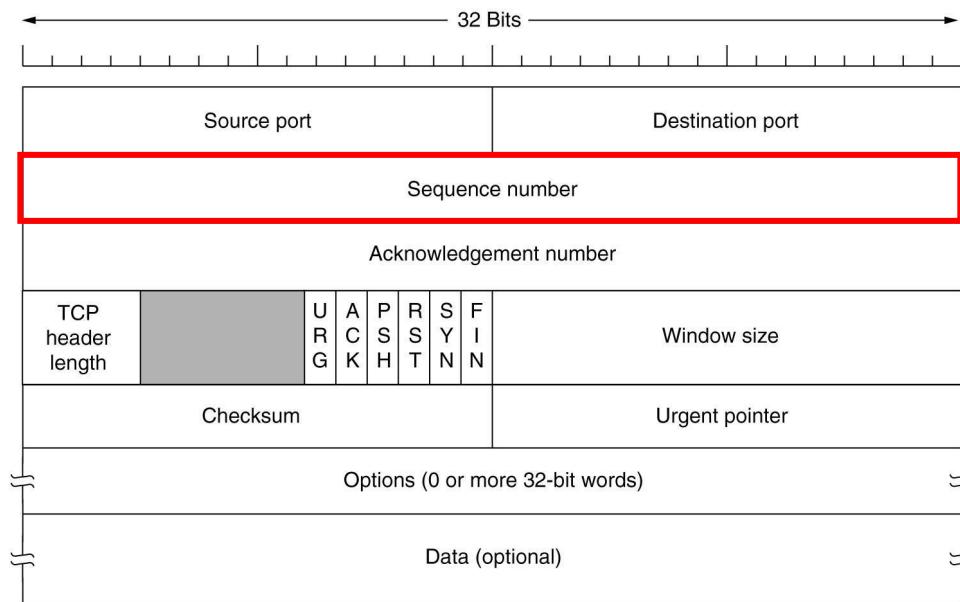
■ Considerações:

- ◆ O TCP vê os dados como uma cadeia de bytes desestruturada, mas ordenada
- ◆ Cada byte em uma conexão TCP tem seu próprio número de sequência de 32 bits

Transferência Confiável de Dados

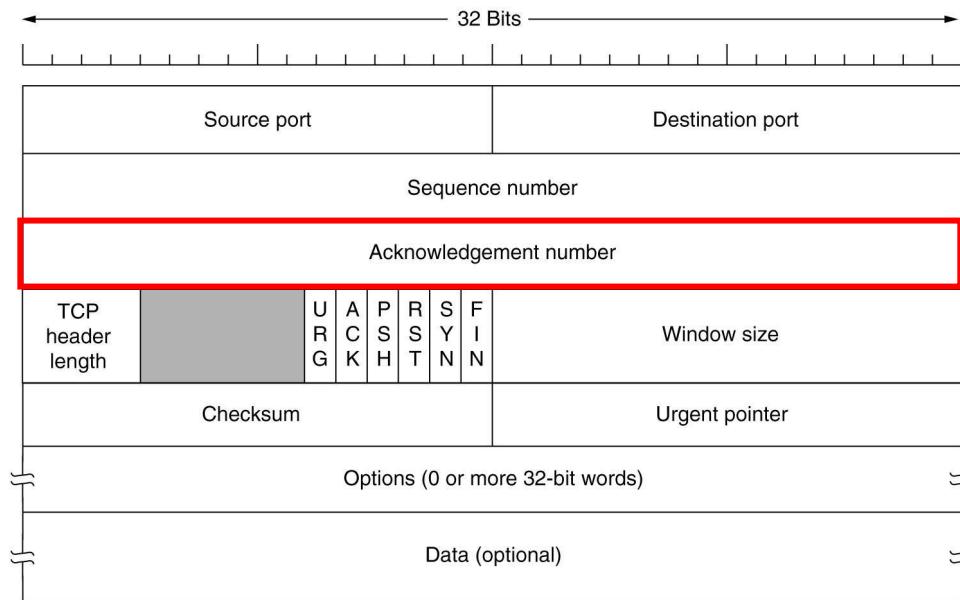
■ Sequence number:

- ◆ Número do primeiro byte no segmento de dados
- ◆ Aplicados sobre a cadeia de bytes transmitidos e não sobre a série de segmentos transmitidos

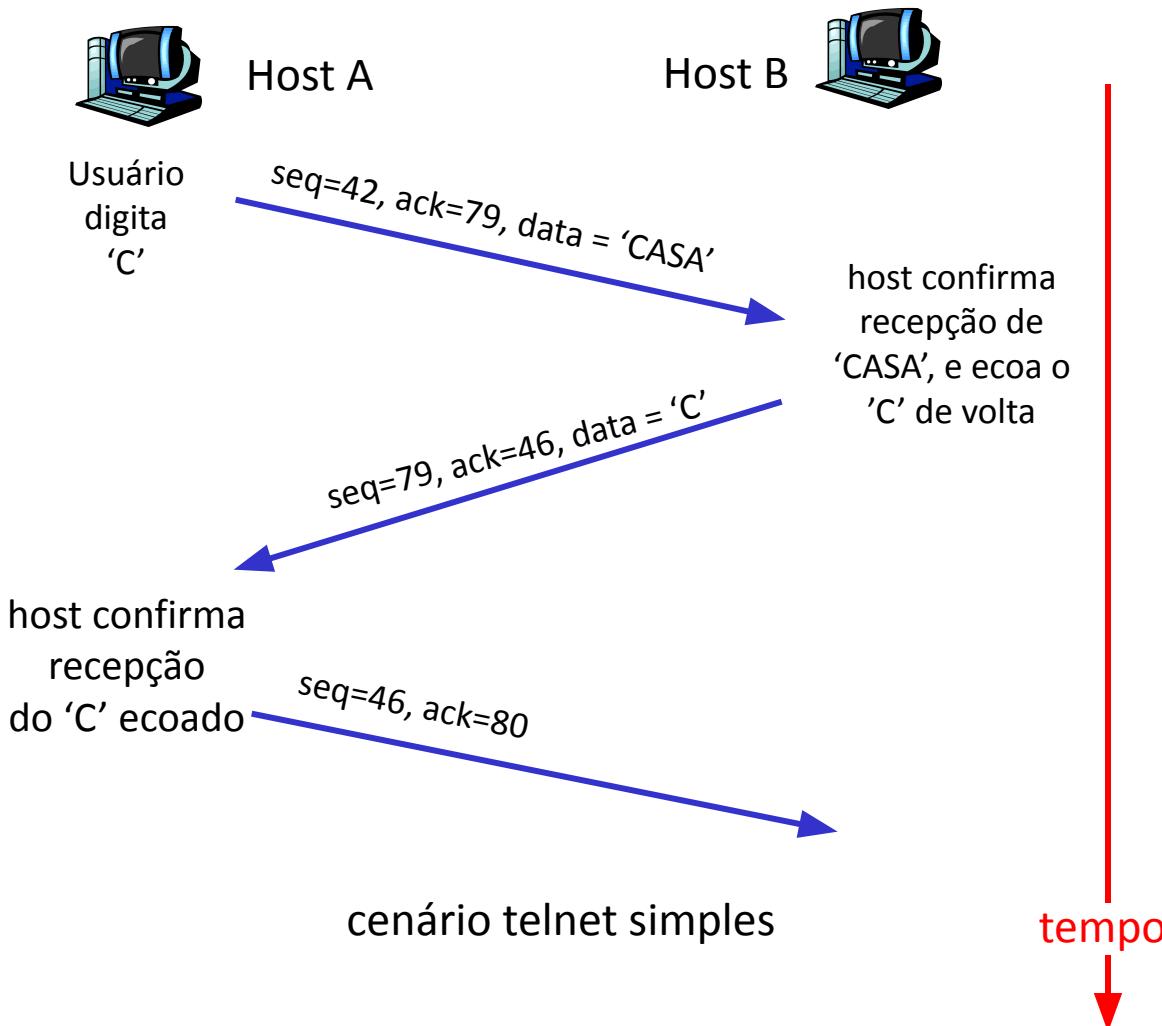


Transferência Confiável de Dados

- Acknowledgement number : Especifica o número do próximo byte esperado e não o último byte recebido corretamente



Transferência Confiável de Dados



Gerenciamento da Conexão TCP

- Utilizam os bits RST, SYN e FIN do cabeçalho TCP
 - ◆ Bit RST: Recusa uma tentativa de conexão
 - ◆ Bit SYN: Estabelece conexões
 - ◆ Bit FIN: Finaliza uma conexão

Gerenciamento da Conexão TCP

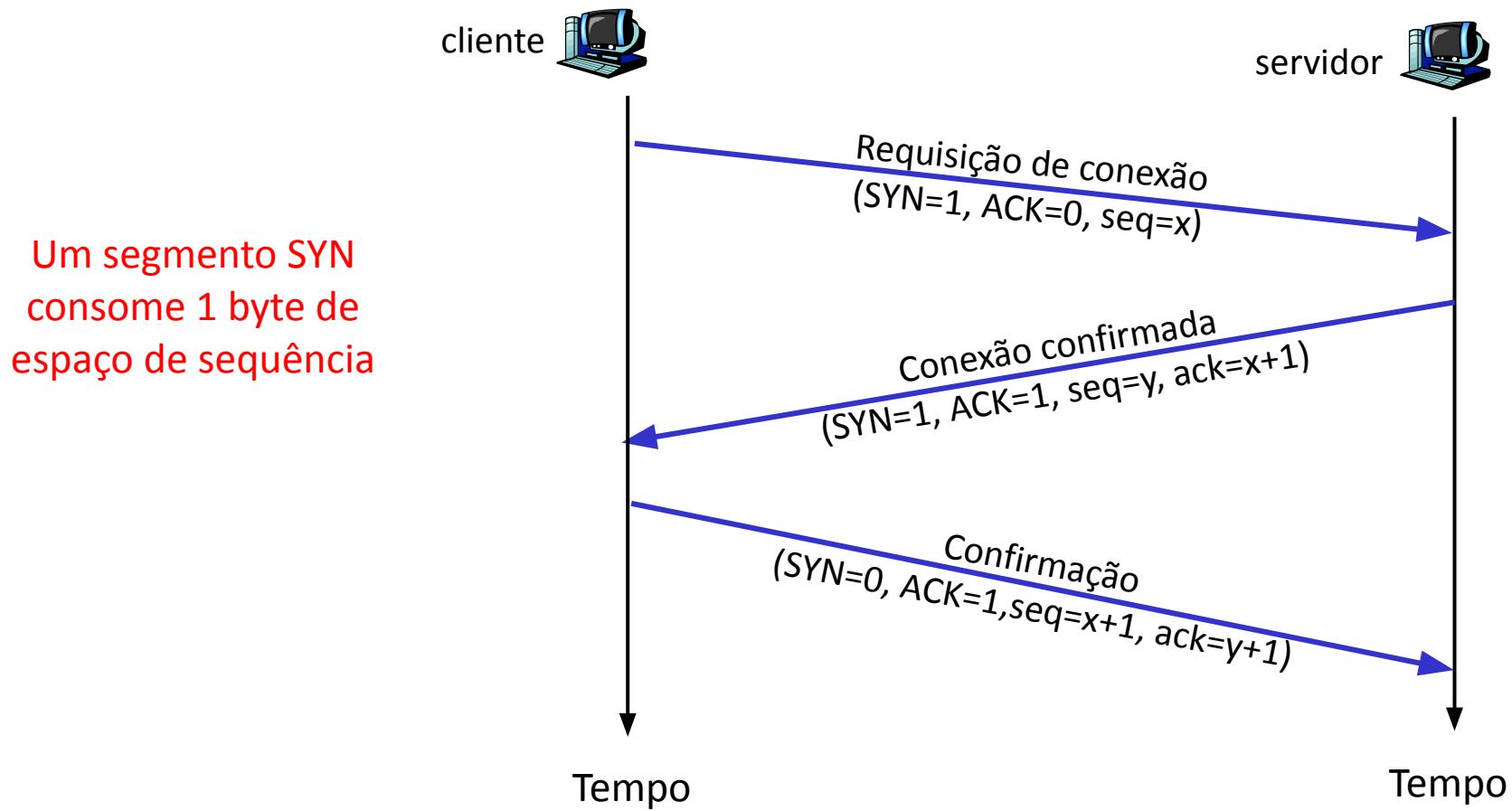
- O TCP emissor estabelece uma conexão com o receptor antes de trocar segmentos de dados
- As conexões são estabelecidas no TCP por meio do handshake de três vias (3-way handshake)
- Inicialização de variáveis:
 - ◆ Números de sequência
 - ◆ Buffers, controle de fluxo

Gerenciamento da Conexão TCP

- Estabelecimento da conexão TCP:
 - ◆ **Passo 1)** O cliente envia um segmento com SYN=1 e ACK=0 ao servidor para especificar o número inicial da sequência
 - ◆ **Passo 2)** O servidor responde com o segmento SYNACK (SYN=1, ACK=1), reconhecendo o SYN recebido, alocando buffers e especificando o número de inicial de sua sequência
 - ◆ **Passo 3)** O cliente recebe o SYNACK

Gerenciamento da Conexão TCP

■ Estabelecimento da conexão TCP:



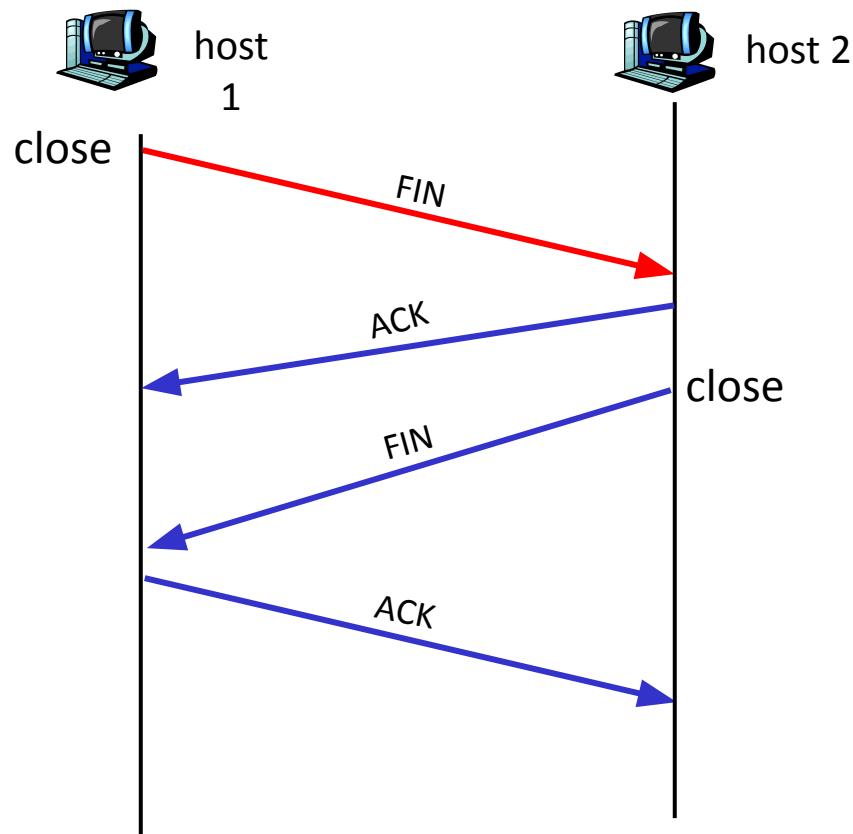
Gerenciamento da Conexão TCP

■ Término da conexão TCP:

- ◆ Apesar das conexões TCP serem *full-duplex*, fica mais fácil compreender como as conexões são encerradas se as considerarmos um par de conexões simplex
- ◆ Cada conexão simplex é encerrada de modo independente de sua parceira

Gerenciamento da Conexão TCP

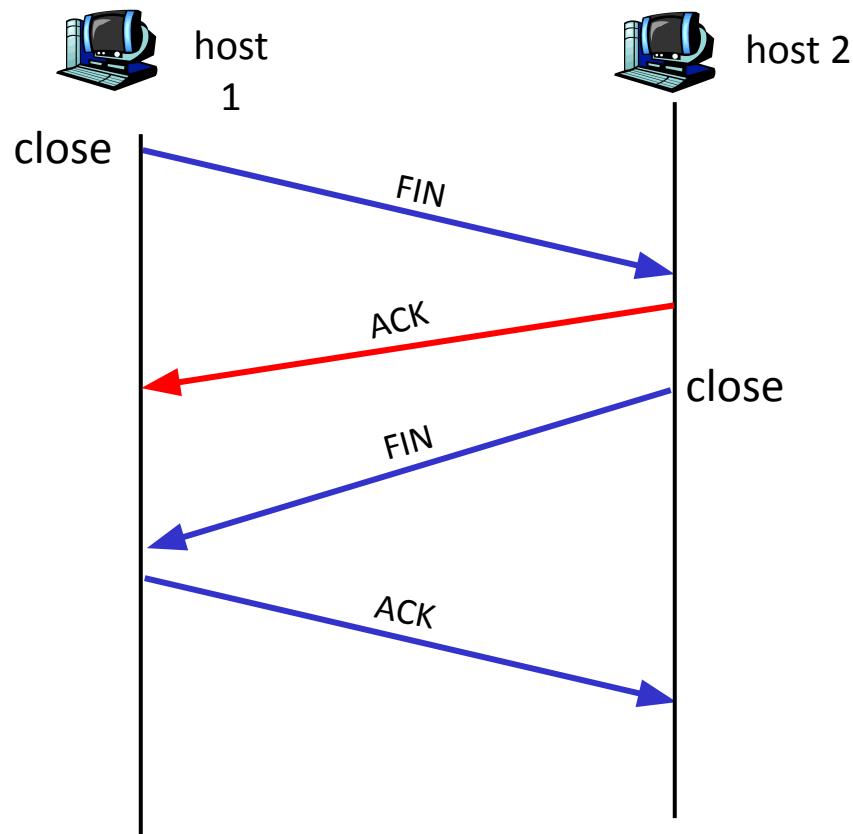
- Término da conexão TCP:



Passo 1) O host 1 envia um segmento TCP FIN para o host 2

Gerenciamento da Conexão TCP

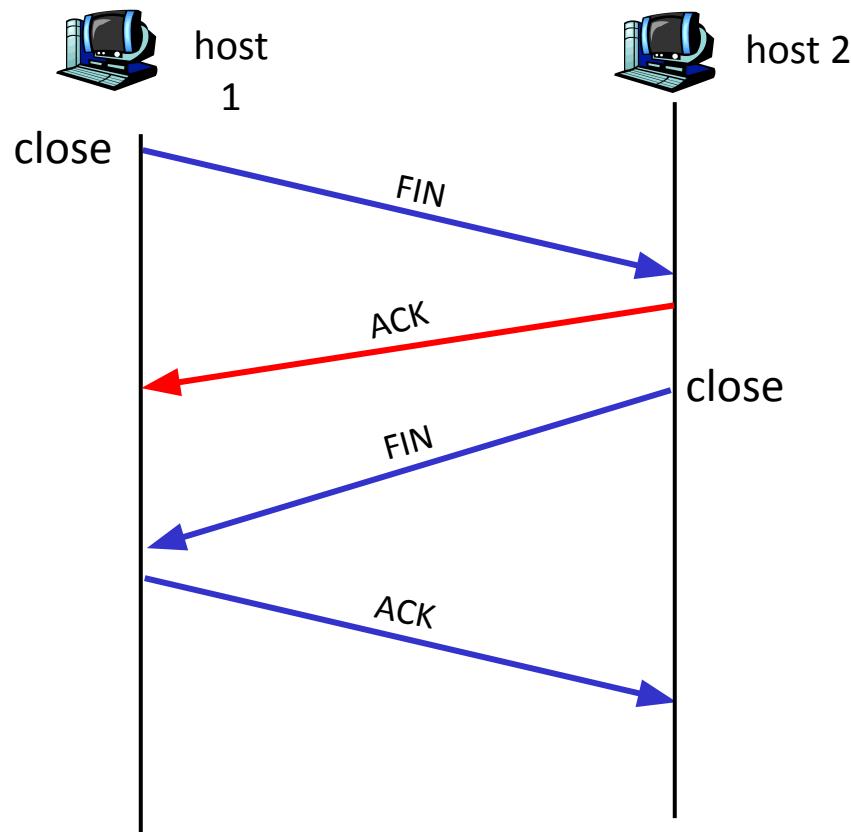
■ Término da conexão TCP:



Passo 2) O host 2 recebe o FIN e o responde com um ACK

Gerenciamento da Conexão TCP

■ Término da conexão TCP:



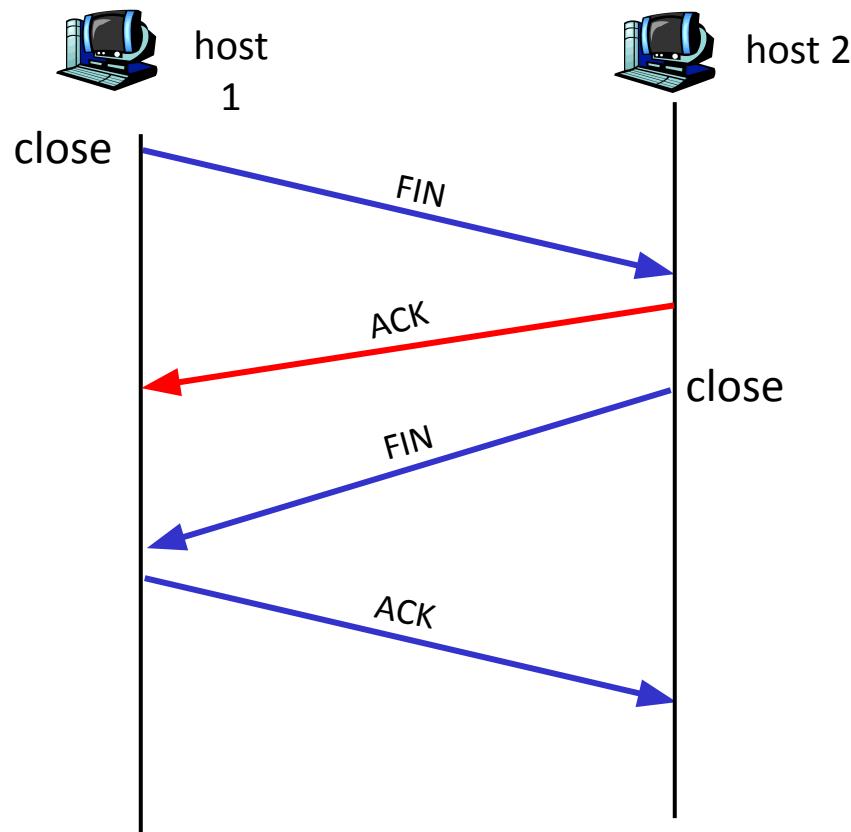
Passo 2) O host 2 recebe o FIN e o responde com um ACK

Em seguida, ele fecha a conexão no sentido host 1 ↔ host 2

Contudo, o fluxo de dados pode continuar no sentido oposto

Gerenciamento da Conexão TCP

■ Término da conexão TCP:



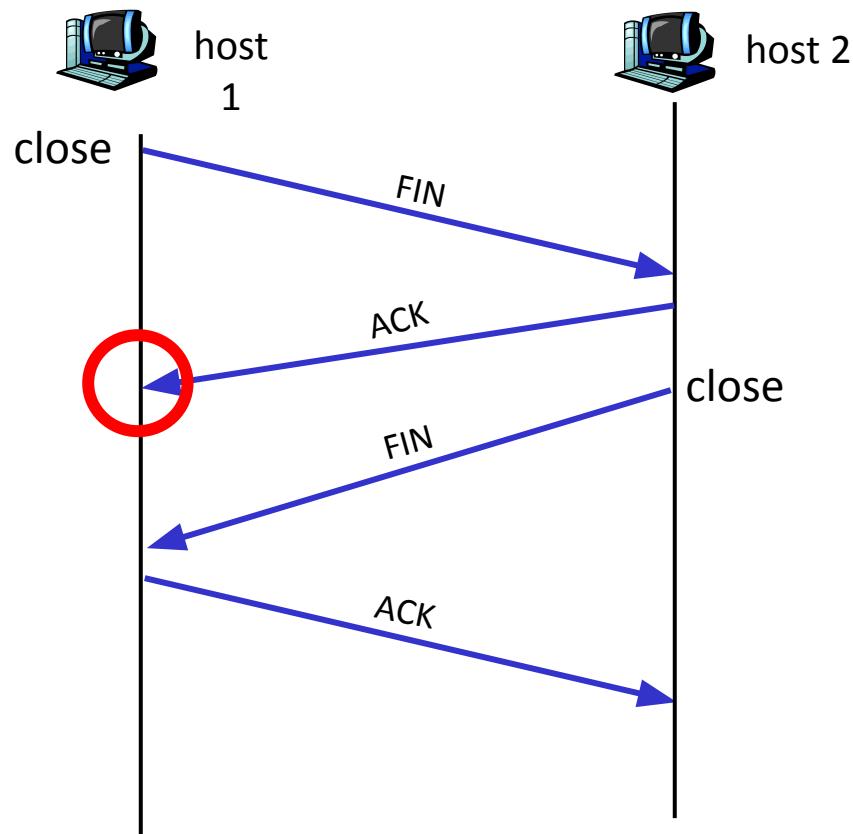
Passo 2) O host 2 recebe o FIN e o responde com um ACK

Em seguida, ele fecha a conexão no sentido host 1 → host 2

Contudo, o fluxo de dados pode continuar no sentido oposto

Gerenciamento da Conexão TCP

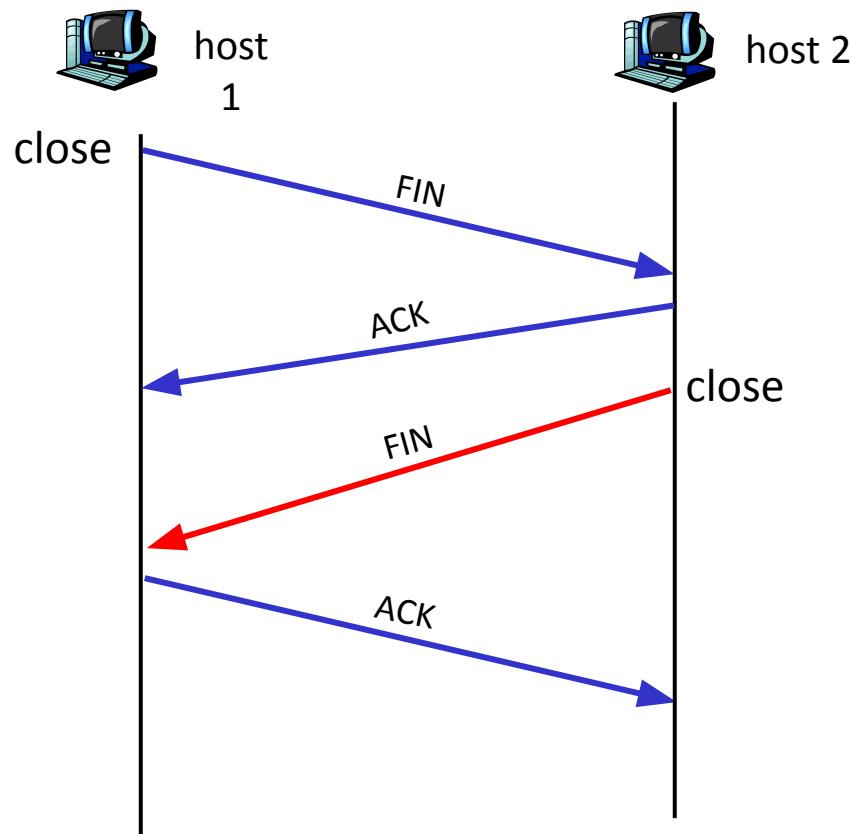
■ Término da conexão TCP:



Passo 3) O host 1 recebe o ACK e fecha a conexão no sentido host 1
□ host 2

Gerenciamento da Conexão TCP

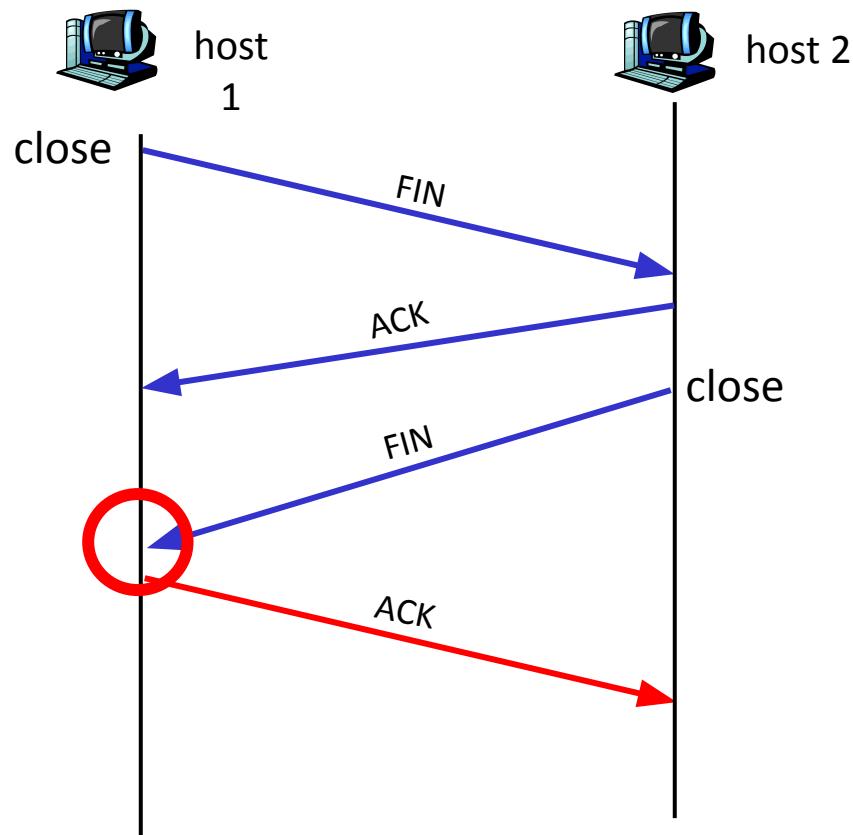
■ Término da conexão TCP:



Passo 4) O host 2 envia o segmento TCP FIN para o host 1

Gerenciamento da Conexão TCP

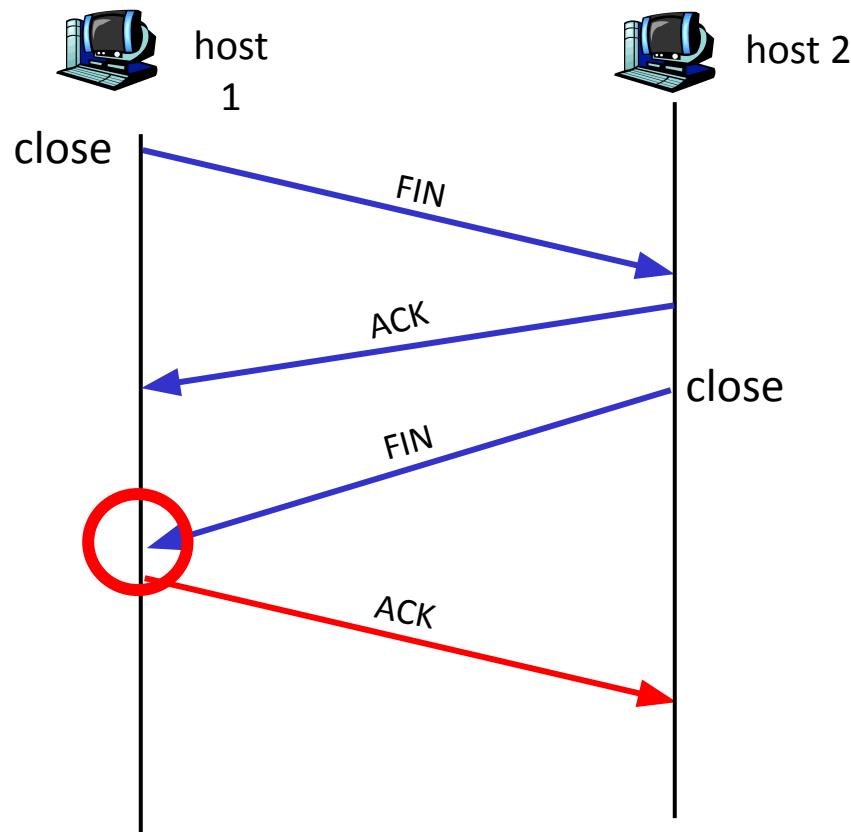
■ Término da conexão TCP:



Passo 5) O host 1 recebe o FIN e o responde com um ACK

Gerenciamento da Conexão TCP

■ Término da conexão TCP:

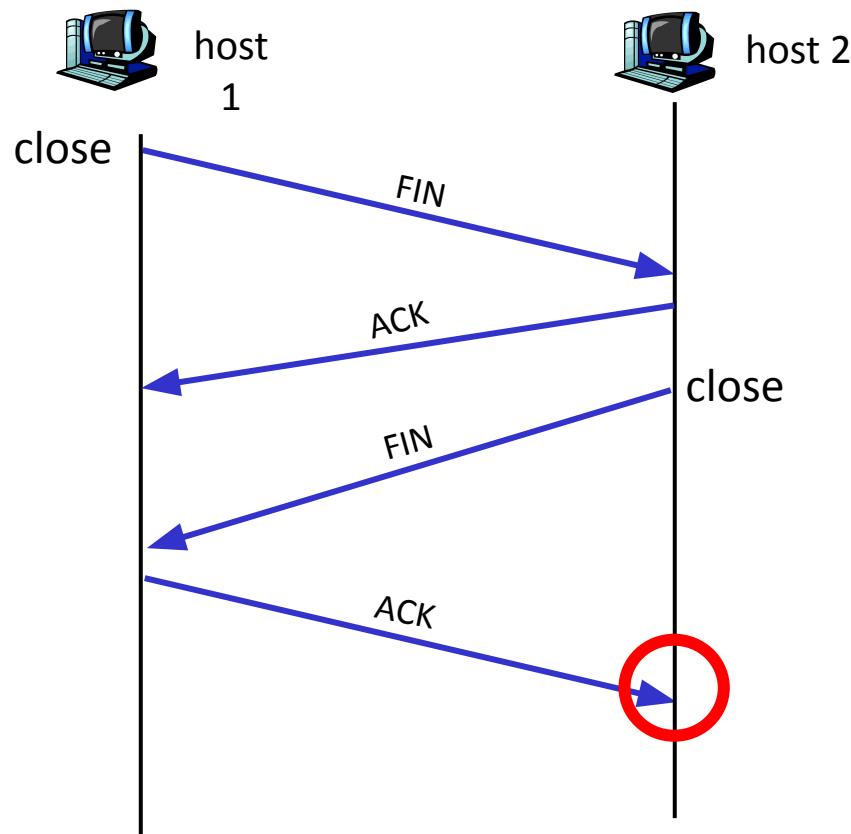


Passo 5) O host 1 recebe o FIN e o responde com um ACK

Em seguida, ele fecha a conexão no sentido host 2 → host 1

Gerenciamento da Conexão TCP

■ Término da conexão TCP:



Passo 6) O host 2 recebe o ACK e fecha a conexão no sentido host 2
□ host 1

Controle de Fluxo

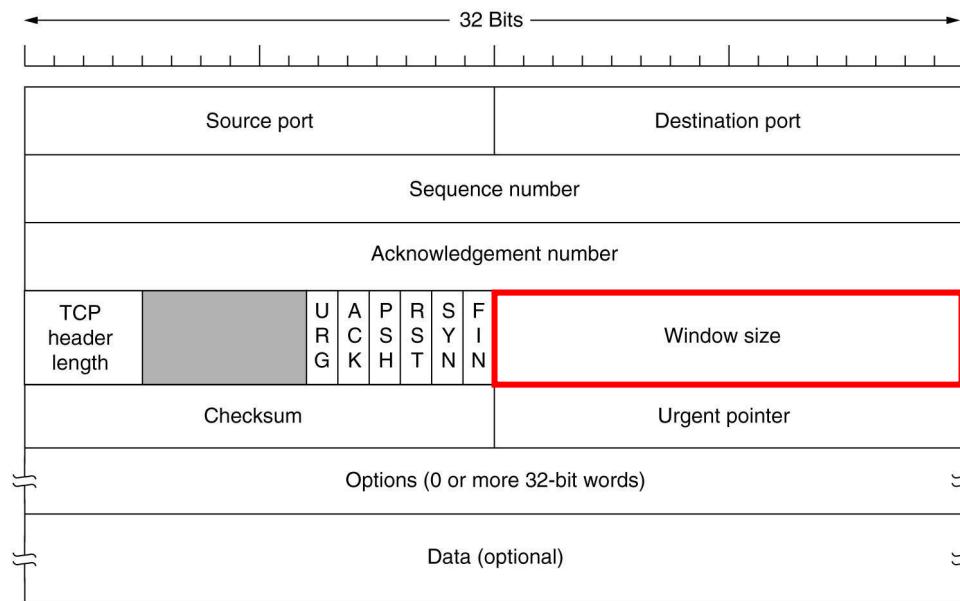
- Evitar que o emissor esgote a capacidade do receptor
- No momento do estabelecimento da conexão, um *buffer* de recepção é alocado e seu tamanho é informado para a entidade par no campo Window size
- Em toda confirmação envia-se o espaço disponível nesse *buffer* e esse espaço é chamado de janela

Controle de Fluxo

- O Emissor não deve esgotar os *buffers* de recepção enviando dados rápido demais
 - ◆ Receptor: Informa explicitamente ao emissor qual é a área livre em seu buffer através do campo *Windows size*
 - ◆ Emissor: Mantém a quantidade de dados transmitidos mas não reconhecidos menor que o último *Windows size* recebido

Controle de Fluxo

- *Window size*: Indica quantos bytes podem ser enviados a partir do byte confirmado



Controle de Congestionamento

- Quando a carga oferecida a qualquer rede é maior que sua capacidade, acontece um congestionamento
- Diferente de controle de fluxo!
- Sintomas:
 - ◆ Perda de pacotes (saturação de buffer nos roteadores)
 - ◆ Atrasos grandes (filas nos buffers dos roteadores)
- Um dos 10 problemas mais importantes na Internet!

Controle de Congestionamento

■ Considerações:

- ◆ O congestionamento da rede pode ser piorado se a camada de transporte retransmite pacotes que não foram perdidos
- ◆ Esse problema pode causar até um colapso da rede

Controle de Congestionamento

- Como detectar o congestionamento?
 - ◆ O TCP usa a quantidade de pacotes perdidos (pacotes com *timeout*) como uma medida de congestionamento
 - ◆ O TCP reduz a taxa de retransmissão a medida que esse valor aumenta

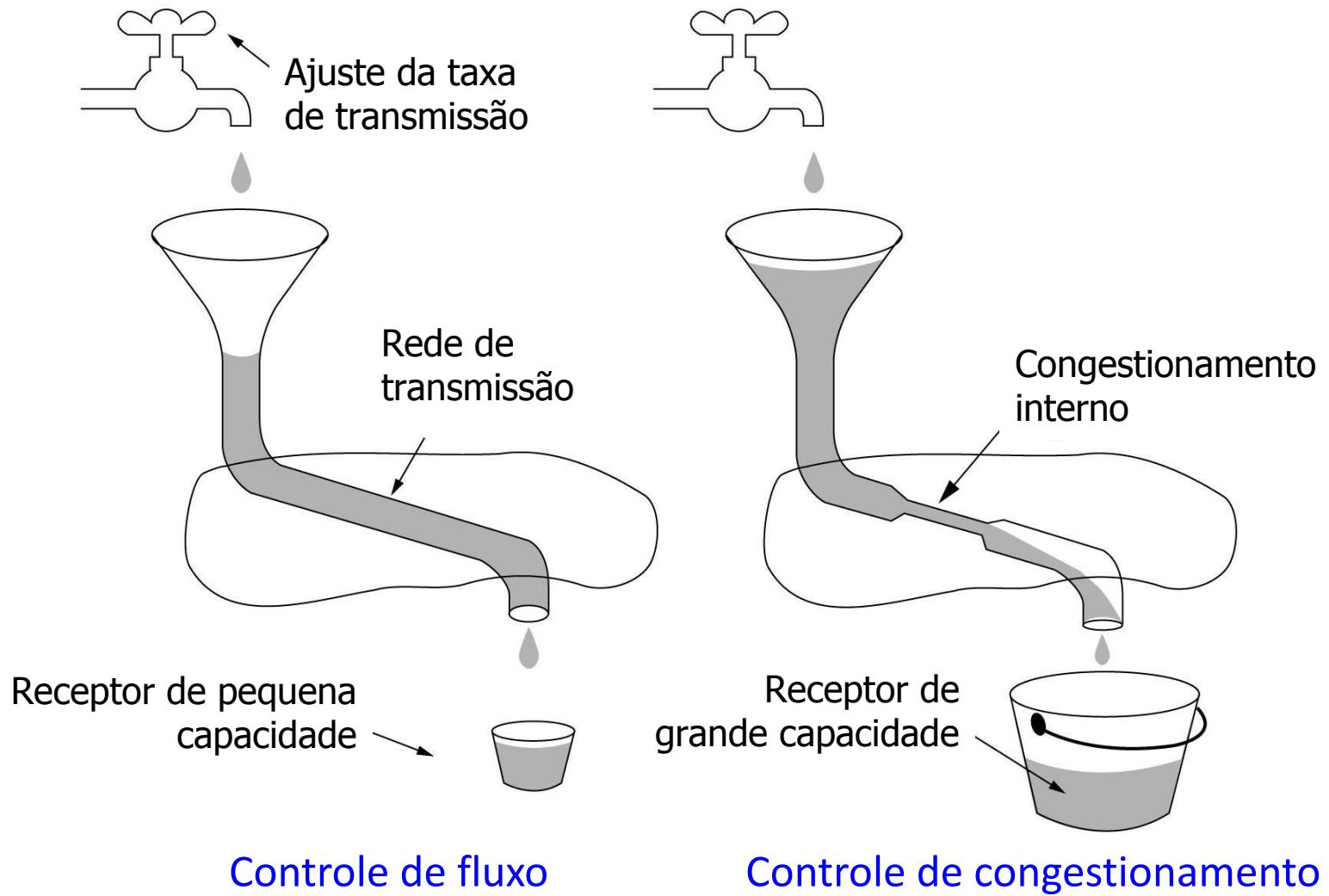
Controle de Congestionamento

- Antigamente, um timeout causado por um pacote perdido podia ter sido provocado por
 - ◆ Ruído em uma linha de transmissão, ou
 - ◆ O pacote foi descartado em um roteador congestionado
- Hoje em dia, a perda de pacotes devido a erros de transmissão é relativamente rara
- A maioria dos timeouts de transmissão na Internet se deve a congestionamentos

Controle de Congestionamento

- Na Internet, existem dois problemas potenciais:
 - ◆ A capacidade da rede □ Controle de Congestionamento
 - ◆ A capacidade do receptor □ Controle de Fluxo

Controle de Congestionamento



Controle de Congestionamento

- Cada emissor mantém duas janelas:
 - ◆ A janela fornecida pelo receptor (controle de fluxo)
 - ◆ A janela de congestionamento (controle de congestionamento)
- O número de bytes que podem ser transmitidos é o valor mínimo entre as duas janelas

Controle de Congestionamento

- Algoritmo de inicialização lenta:
 - ◆ Quando uma conexão é estabelecida, a janela de congestionamento é igual ao tamanho do segmento máximo em uso na conexão
 - ◆ Cada rajada confirmada duplica a janela de congestionamento

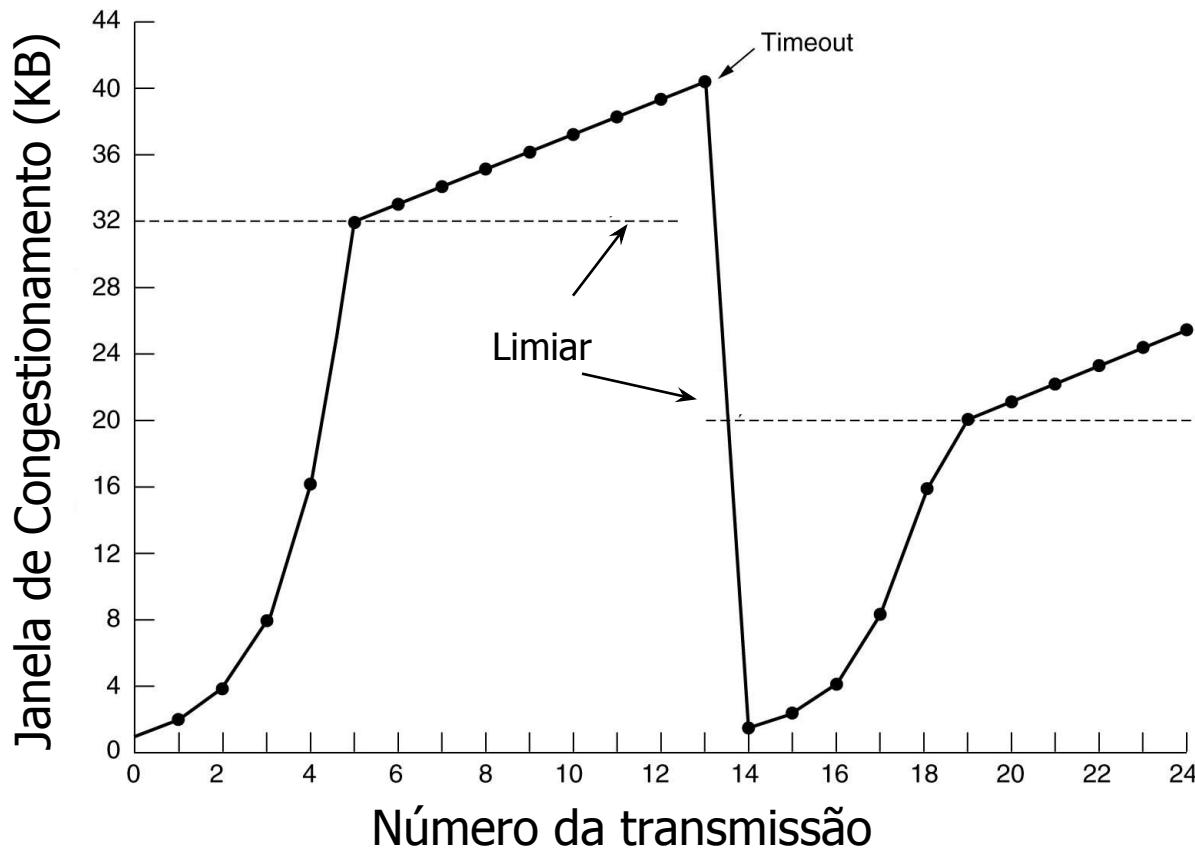
Controle de Congestionamento

- A janela de congestionamento mantém seu crescimento exponencial até que:
 - ◆ Um limiar seja atingido,
 - ◆ Aconteça um timeout, ou
 - ◆ A janela do receptor seja alcançada

Controle de Congestionamento

- Um limiar é atingido:
 - ◆ As transmissões bem-sucedidas proporcionam um crescimento linear à janela de congestionamento
- Acontece um timeout:
 - ◆ O limiar é definido como a metade da janela de congestionamento atual
 - ◆ Janela de congestionamento \leftarrow segmento máximo
 - ◆ Inicialização lenta é usada
- A janela de recepção é alcançada:
 - ◆ Janela de congestionamento pára de crescer e permanece constante

Controle de Congestionamento



A transmissão de mensagens é feita de forma exponencial até atingir um dado valor, quando passa a aumentar mais lentamente

Gerenciamento de Temporizadores

- O TCP utiliza um *timer* de retransmissão:
 - ◆ Quando um segmento é enviado, um *timer* é ativado
 - ◆ Se o segmento for confirmado antes do *timer* expirar, ele será interrompido
 - ◆ Se o *timer* expirar antes da confirmação chegar, o segmento será retransmitido e o *timer* será disparado novamente

Gerenciamento de Temporizadores

- Tempo de viagem de ida e volta (RTT): tempo transcorrido desde o instante em que um segmento é enviado até o instante em que ele é reconhecido
- Para cada conexão, o TCP mantém uma variável, RTT, que é a melhor estimativa no momento para o tempo de percurso de ida e volta até o destino em questão

Gerenciamento de Temporizadores

- Como escolher o valor do *timer* do TCP?
 - ◆ Maior que o RTT (RTT varia)
 - ◆ Muito curto: Retransmissões desnecessárias, sobrecarregando a Internet com pacotes inúteis
 - ◆ Muito longo: O desempenho será prejudicado devido ao longo retardo de retransmissão sempre que um pacote se perder

Gerenciamento de Temporizadores

- O TCP atualiza a variável RTT de acordo com a fórmula:

$$RTT = \alpha RTT + (1 - \alpha)M$$

onde:

- 4 M último RTT medido
- 4 α é um fator de suavização que determina o peso dado ao antigo valor

Gerenciamento de Temporizadores

- O TCP estima o *timer* de retransmissão como sendo β RTT, onde β é proporcional ao desvio-padrão da função de densidade de probabilidades de tempos de chegada de confirmações
 - ◆ Grande variância \square alto valor de β
 - ◆ Pequena variância \square pequeno valor de β