Sistemas de Comunicação

Prof. Klayton Castro
klayton.castro@ceub.edu.br

Introdução

Nossos objetivos:

- Obter contexto, terminologia, “sentimento” sobre redes
- Abordagem: Usar a Internet como exemplo

Visão geral:

- O que é a Internet
- O que é um protocolo?
- Bordas da rede
- Núcleo da rede
- Rede de acesso e meio físico
- Estrutura de Internet/ISP
- Desempenho: perda, atraso
- Camadas de protocolo, modelos de serviços
- Modelagem de redes

Conceitos Importantes em Redes

Largura de banda (ou Bandwidth) pode ser definida como a medida da quantidade de dados que pode ser transmitida durante um período de tempo fixo, cuja unidade básica é bits por segundo (bps), podendo ser descrita como milhares de bits por segundo (Kbps), milhões (Mbps) e até mesmo bilhões (Gbps) ou trilhões de bits por segundo (Tbps).

- Embora os termos largura de banda e velocidade sejam confundidos por alguns, de forma alguma eles podem ser considerados sinônimos.
- Por exemplo: uma conexão T3 a 45Mbps é capaz de operar em maior velocidade se comparada a uma conexão T1 a 1,544Mbps. No entanto, se não há dados suficientes transitando no enlace, ambas as conexões podem apresentar o mesmo desempenho para uma tarefa específica, mesmo com T3 oferecendo um potencial maior de trabalho. Assim, a velocidade está de fato mais relacionada à Vazão, ou seja, a medida de desempenho efetivamente alcançada.
- Surge então a definição de **Throughput**, que é a medida utilizada para mensurar a taxa em que os dados são transmitidos com êxito, de um lugar para outro, em um determinado período de tempo.

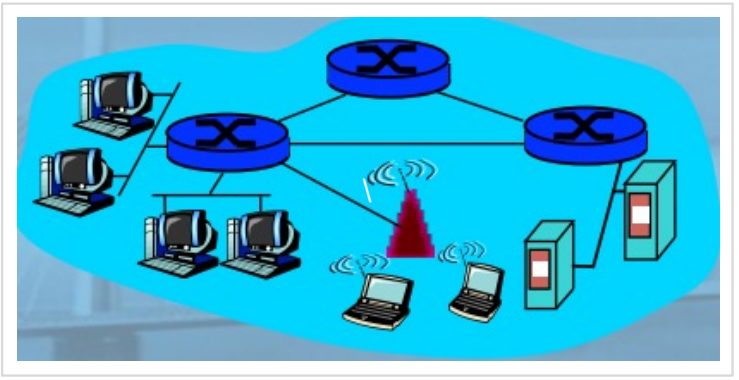
Conceitos Importantes em Redes

Os Diferentes Tipos de Comunicação de Dados

O que é a Internet: visão dos elementos básicos.

- Protocolos controle de envio e recepção de mensagens.

Ex: TCP, IP, HTTP, Skype, Ethernet



Fonte: Kurose,2010

Conceitos Importantes em Redes

Os Diferentes Tipos de Comunicação de Dados

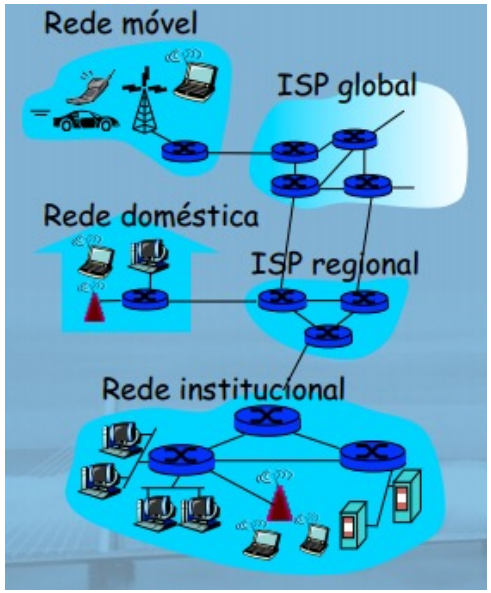
O que é a Internet: visão dos elementos básicos

- Internet: “rede de redes”

  - vagamente hierárquica;
  - Internet pública versus intranet privada.

- Padrões da Internet

  - RFC: Request For Comments
  - IETF: Internet Engineering Task Force



Fonte: Kurose, 2010

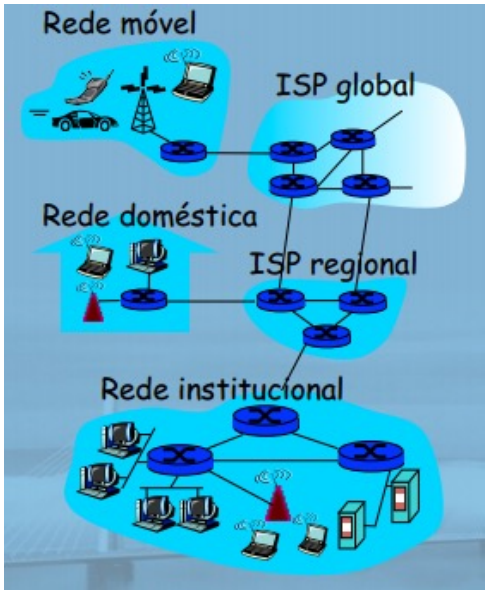
Conceitos Importantes em Redes

Os Diferentes Tipos de Comunicação de Dados

O que é a Internet: uma visão de serviço

Infraestrutura de comunicação possibilita aplicações distribuídas:

- Web;
- VoIP;
- E-mail;
- Jogos;
- E-commerce;
- Compartilhamento de arquivos;



Fonte: (Kurose, 2010)

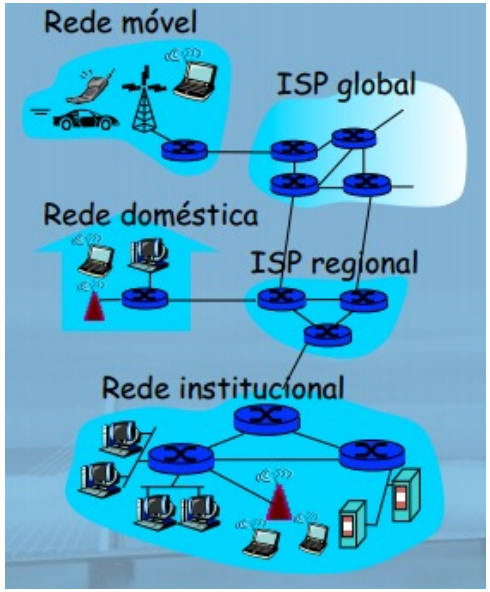
Os Diferentes Tipos de Comunicação de Dados

O que é a Internet: uma visão de serviço

Serviços de comunicação fornecidos às aplicações:

- Entrega de dados confiável da origem ao destino;

- Entrega de dados pelo “melhor esforço”
(não confiável).

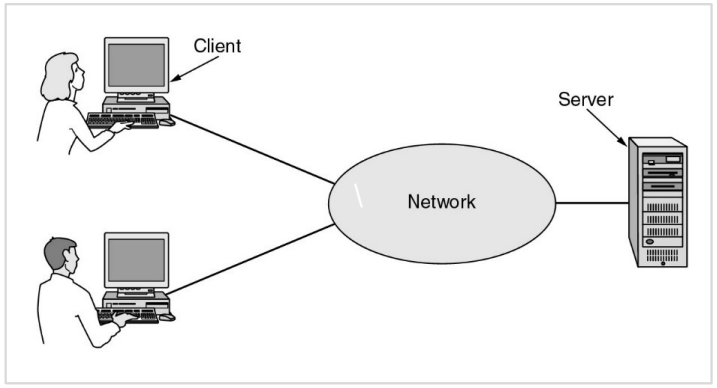


Fonte: (Kurose, 2010)

Os Principais Componentes da Comunicação de Dados

Rede de Computadores:

Conjunto de módulos processadores interligados por um *sistema de comunicação* capazes de *trocar informações* e *compartilhar recursos*.

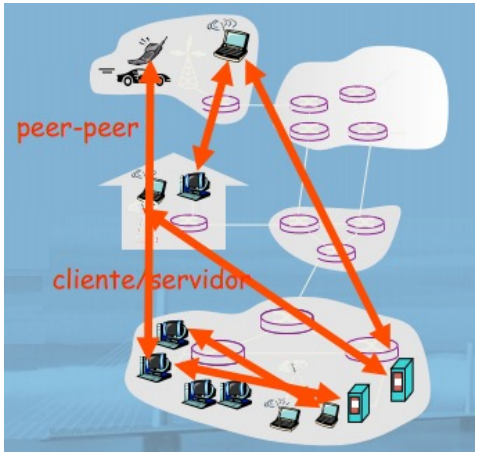


Fonte: (Tanenbaum, 2008)

Os Principais Componentes da Comunicação de Dados

Sistema de Comunicação:

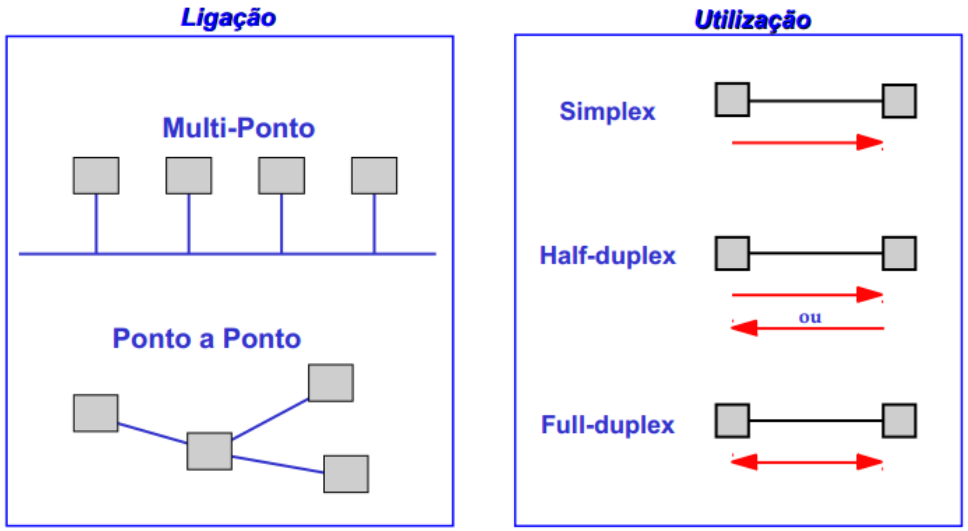
Arranjo *topológico* que interliga os módulos processadores através de *enlaces* e *regras* (protocolos) para organizar a comunicação.



Fonte: (Kurose, 2010)

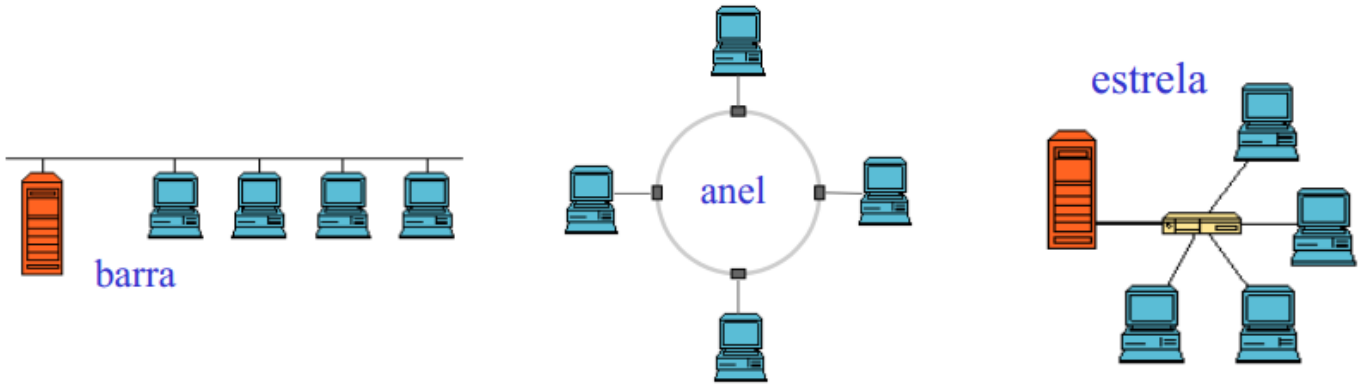
Topologias Físicas de Redes de Computadores

Topologia:
É o arranjo de interligação entre os nós de uma rede.



Fonte (Moura, 2012)

Topologias Físicas de Redes de Computadores

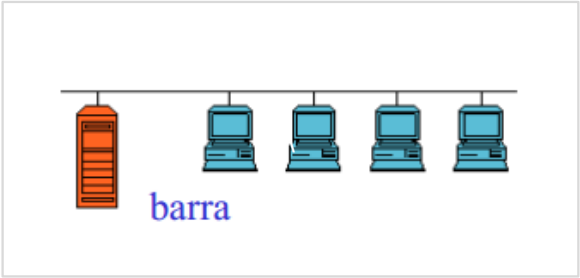


Fonte (Moura, 2012)

Topologias Físicas de Redes de Computadores

Topologia em Barra

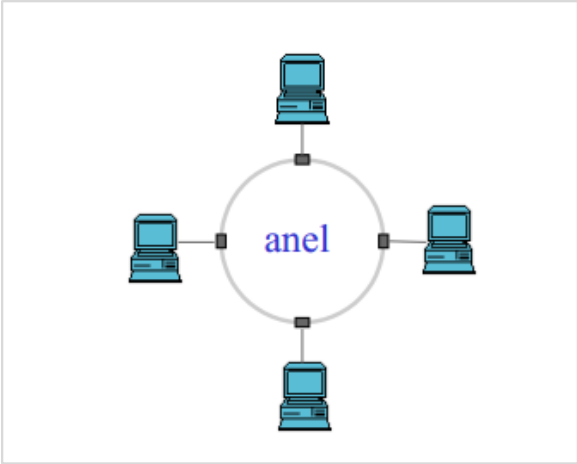
- Nós ligados a um mesmo barramento;
- Não possuem estação supervisora;
- Broadcast mais simples que no anel;
- Acesso ao meio mais complexo que na estrela (tratamento de colisões);
- Facilidade de expansão, com risco de degradar o desempenho;
- As interfaces são passivas, o funcionamento da rede não depende do funcionamento das interfaces.



Topologias Físicas de Redes de Computadores

Topologia em Anel

- Nós ligados em série formando uma malha fechada;
- Os dados podem circular em ambas as direções, mas geralmente redes em anel são unidirecionais;
- Redundância com duplo anel. Em geral NÃO dispensam um nó supervisor;
- Falha em qualquer interface impede o funcionamento da rede;



Topologias Físicas de Redes de Computadores

Topologia em Estrela

- Todos os nós ligados ao nó central;
- Desempenho da rede em função da capacidade do nó central;
- Vulnerabilidade em relação ao nó central;
- Dificuldade de expansão – limitações do nó central “Cabeamento” extenso Interface nó/rede simplificada;
- Técnicas de transmissão mais simples.

Classificação de Redes Quanto a Escala

- LANs: Local Area Networks
- MANs: Metropolitan Area Networks
- WANs: Wide Area Networks

Classificação de Redes Quanto a Escala

LANs: Local Area Networks

- Distância entre os nós: 10m (sala), 100m (prédio), 1Km (campus);
- Taxa de erros: muito baixa;
  Taxa de transferência: alta (10Mbps – 1Gbps);
  Retardos de propagação: baixos.
- Exemplos: Ethernet, Fast Ethernet, Gigabit Ethernet

Classificação de Redes Quanto a Escala

MAN (Metropolitan Area Network)

- Distância entre os nós: 10 Km (cidade);
- Taxa de erros: baixa;
- Taxa de transferência: 100Mbps;
- Retardos de propagação: médios.

Exemplos: ATM, MPLS

Classificação de Redes Quanto a Escala

WAN: (World Area Network)

- Distância entre nós: 100 Km (país), 1000 Km (continente);
- Taxa de erros: maior que LANs e MANs;
- Taxa de transferência: de alguns Kbps a centenas de Mbps;
- Retardos de propagação: grandes;

Exemplos: X.25, Frame Relay, ATM.

Classificação de Redes Quanto a Escala

	LAN	MAN	WAN
distância entre processadores	10m (sala), 100m (prédio), 1Km (campus);	10 Km (cidade)	100 Km (país), 1000 Km (continente);
taxa de erros	muito baixa	baixa	maior que LANs e MANs
taxa de transferência	10Mbps a 1Gbps	100Mbps	de Kbps a centenas de Mbps
retardo propagação	Baixos	Médios	Grandes

Fonte (Moura, 2012)

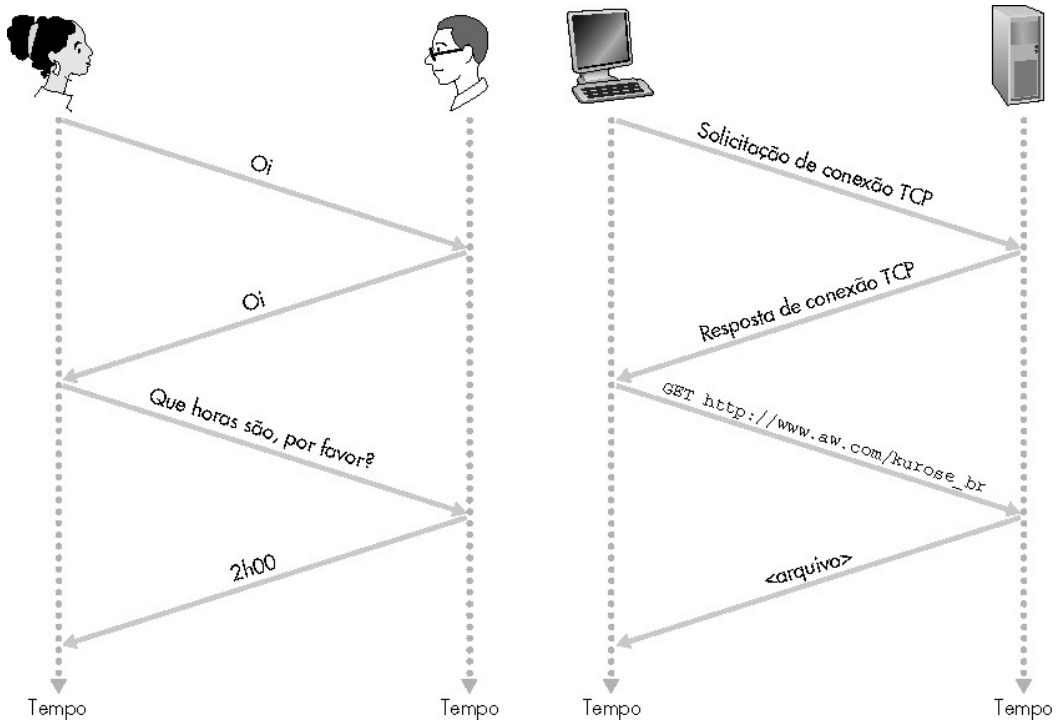
Redes são complexas! Como **organizar** a arquitetura de uma rede?

Muitos componentes:

- Hospedeiros
- Roteadores
- Enlaces de vários tipos
- Aplicações
- Protocolos
- Hardware, software

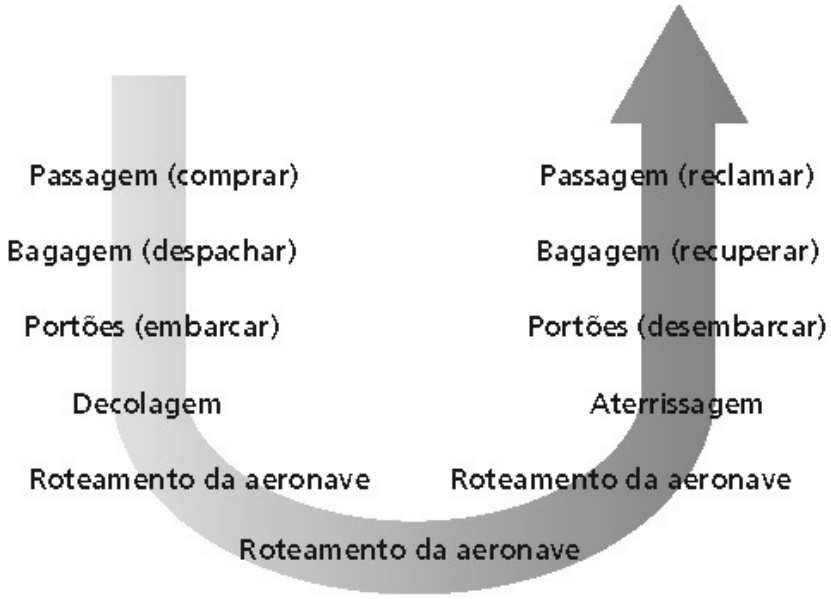
O que é um protocolo?

Um protocolo humano e um protocolo de rede de computadores:



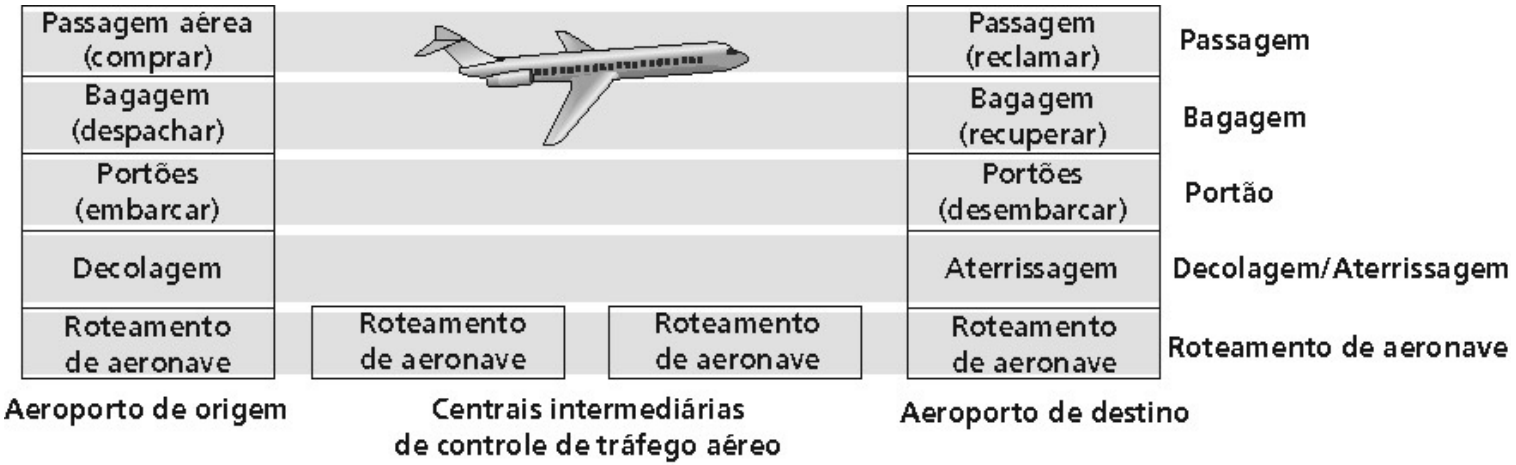
O que é um protocolo?

Uma série de passos



Camadas de atuação do protocolo

Camadas: cada camada implementa um serviço, com suas próprias ações internas, confiando em serviços fornecidos pela camada inferior.



Camadas de atuação do protocolo

Convivendo com sistemas complexos:

A estrutura explícita permite identificação, o relacionamento das partes de um sistema complexo

Um modelo de referência em camadas permite a discussão da arquitetura

Modularização facilita a manutenção, atualização do sistema

As mudanças na implementação de uma camada são transparentes para o resto do sistema

Ex.: novas regras para embarque de passageiros não afetam os procedimentos de decolagem

A divisão em camadas é considerada perigosa?

PDU (Protocol Data Unit)

Bloco de dados transmitido entre duas instâncias da mesma camada. Cada camada recebe a PDU da camada superior como um bloco de dados, adiciona seus cabeçalhos (e em alguns casos, rodapés) de controle, criando a sua própria PDU, num processo chamado de encapsulamento.

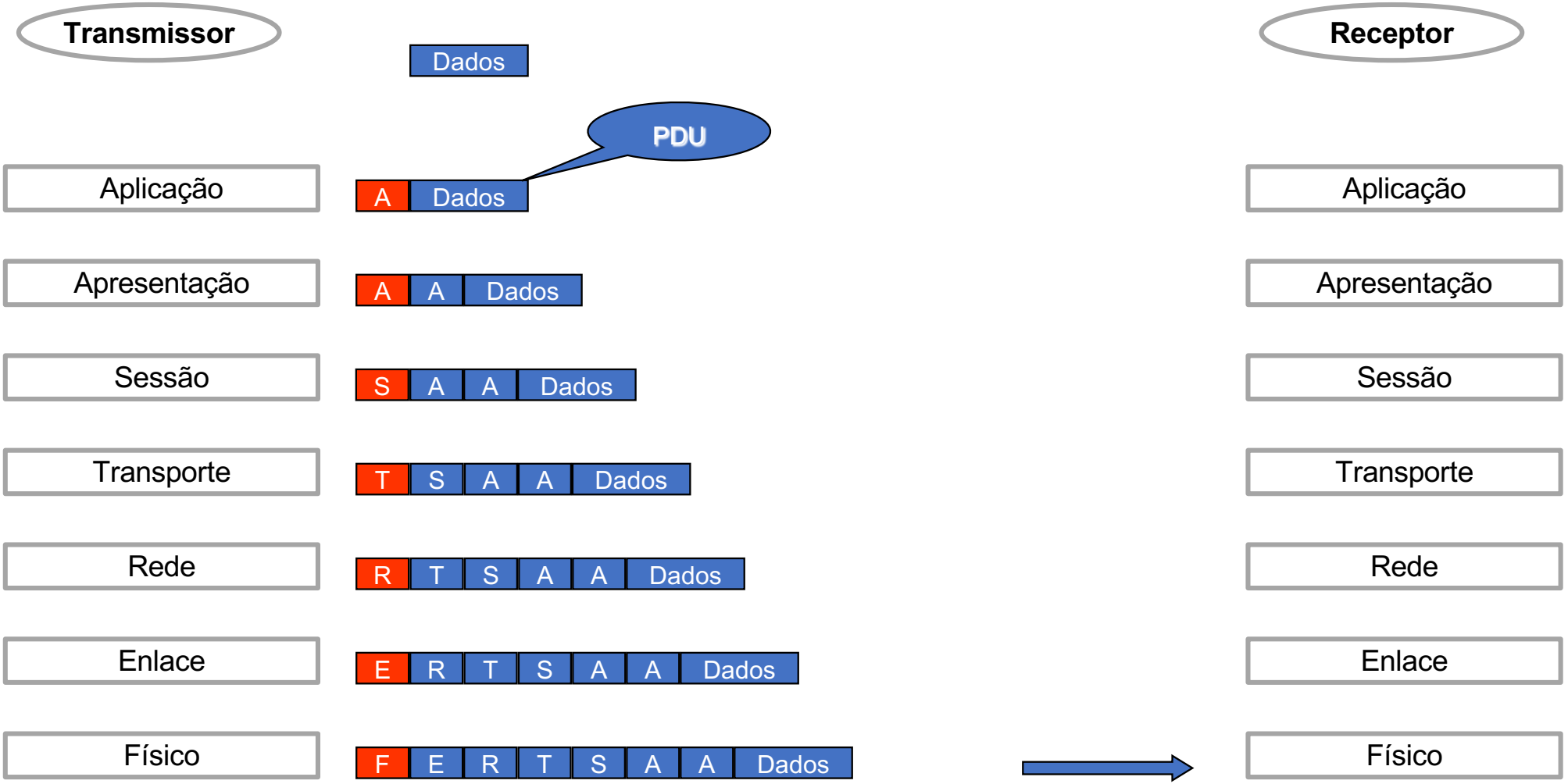
PDU (Protocol Data Unit)

Embora seja comum o uso do termo "Pacote" para todas as informações trocadas numa rede, este termo só é adequado às PDUs de camada 3 (Rede). Em algumas camadas, as PDUs recebem nomes distintos:

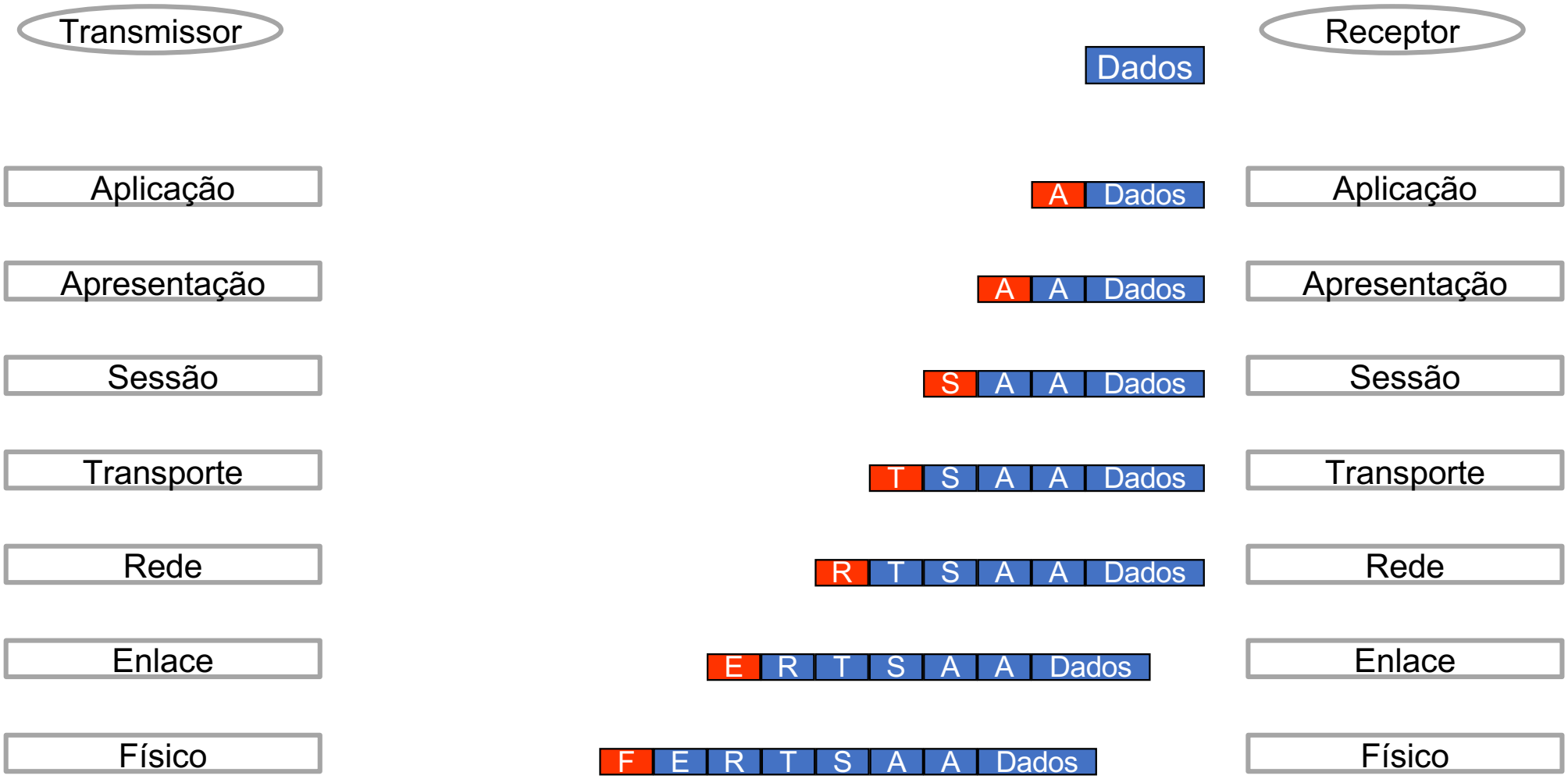
- Camada de Física: Bit
- Camada de Enlace: Quadro ou Frame
- Camada de Rede: Pacote ou Datagrama
- Camada de Transporte: Segmento

Nas camadas de Sessão, Apresentação e Aplicação as PDUs são chamadas genericamente de "dados" ou "mensagens".

Modelo OSI (Open Systems Interconnection)



Modelo OSI (Open Systems Interconnection)



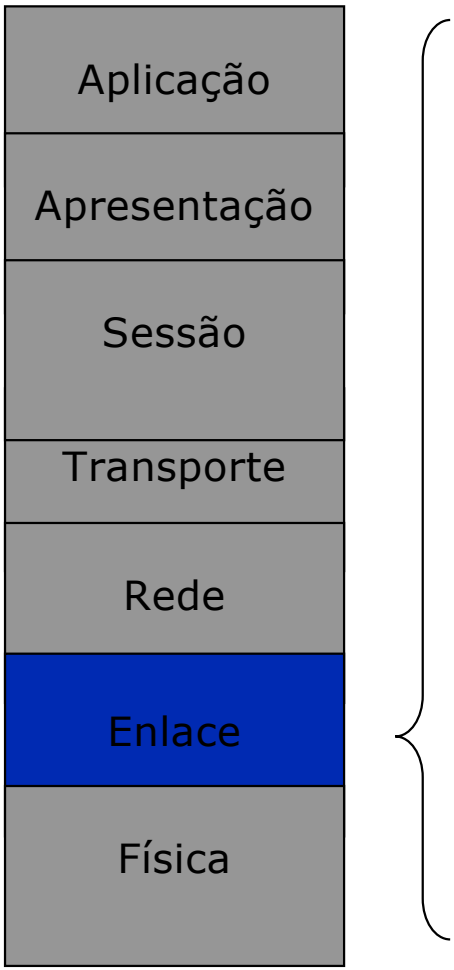
Revisão dos Modelos de Referência em Redes de Computadores

- Princípios da Abordagem por Camadas:
  - Um nível de abstração por camada
  - Camadas com funções bem definidas
  - Em cada camada devem ser usados protocolos padronizados internacionalmente
  - Número de camadas nem grande, nem pequeno

Camada Física

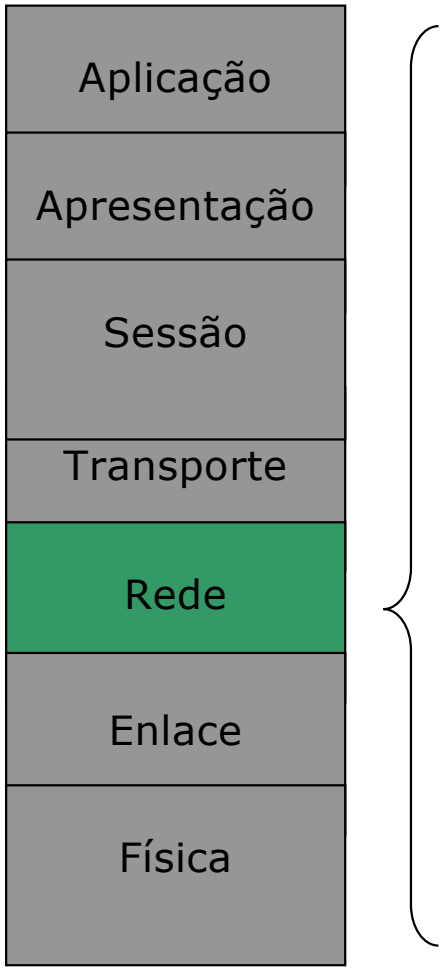
- Trata das características
  - mecânicas, elétricas, funcionais e de procedimentos para conexão física entre entidades da camada de enlace
- Transmite uma sequência de bits
- Não se preocupa com o significado dos bits

Camada de Enlace



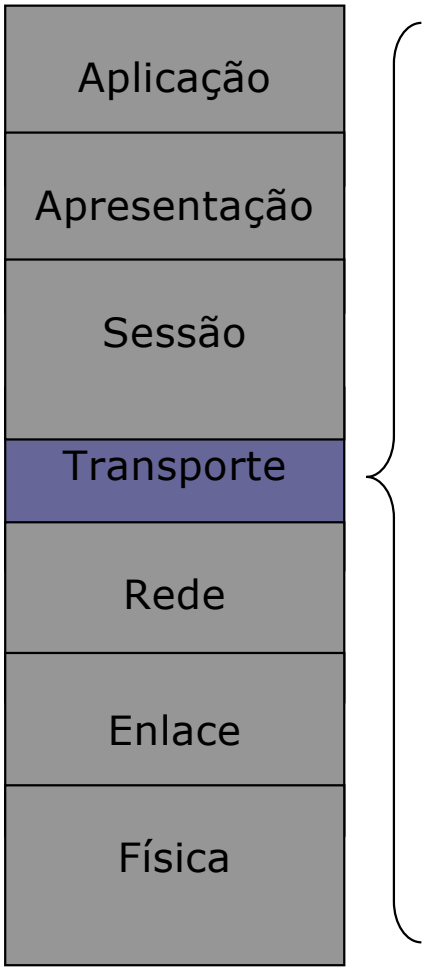
- Trata o fluxo de dados no enlace entre transmissor e receptor:
  - Controle de fluxo
  - Detecção e correção de erros
  - Acesso ao meio compartilhado
- Não permite ligação entre redes distintas

Camada de Rede



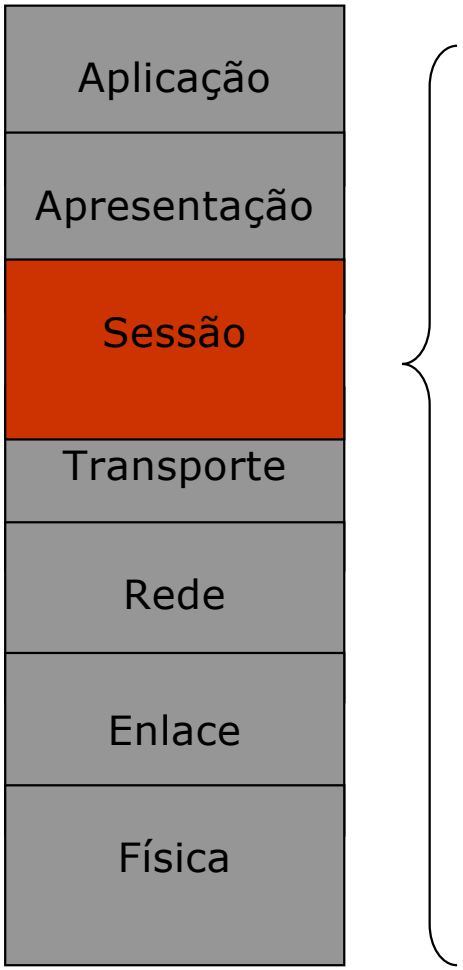
- Controla as operações na sub-rede:
  - Roteamento: estático ou dinâmico
  - Controle de congestionamento
  - Interconexão de redes
- Não garante que o pacote chegue ao destino

Camada de Transporte



- Divide as mensagens em pacotes
- É a primeira camada fim-a-fim
- Deve garantir:
  - Comunicação fim-a-fim confiável
  - Multiplexação/*splitting* de conexões
  - Controle de fluxo fim-a-fim

Camada de Sessão



- Permite que aplicações em *hosts* diferentes partilhem uma sessão
- Provê:
  - Controle de diálogo
  - Controle de *token*
  - Sincronização

Camada de Apresentação

- Realiza transformações adequadas nos dados:
  - Tradução dos dados
  - Compressão de textos
  - Criptografia
  - Conversão de padrões

Camada de Aplicação

- Provê serviços que suportam diretamente as aplicações do usuário, como:
  - Correio eletrônico
  - Transferência de arquivos
  - Acesso a banco de dados
- Não define as aplicações em si!

Comutação de Pacotes x Comutação de Circuitos

Malha de roteadores interconectados

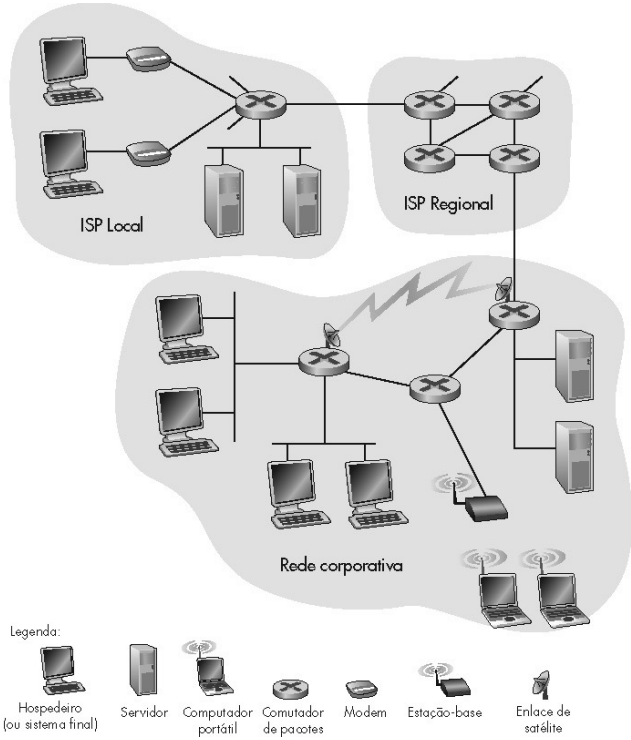
A questão fundamental:

como os dados são transferidos através da rede?

Comutação de circuitos: usa um canal dedicado para cada conexão

Ex.: rede telefônica

Comutação de pacotes: dados são enviados em "blocos"



Comutação de Circuitos

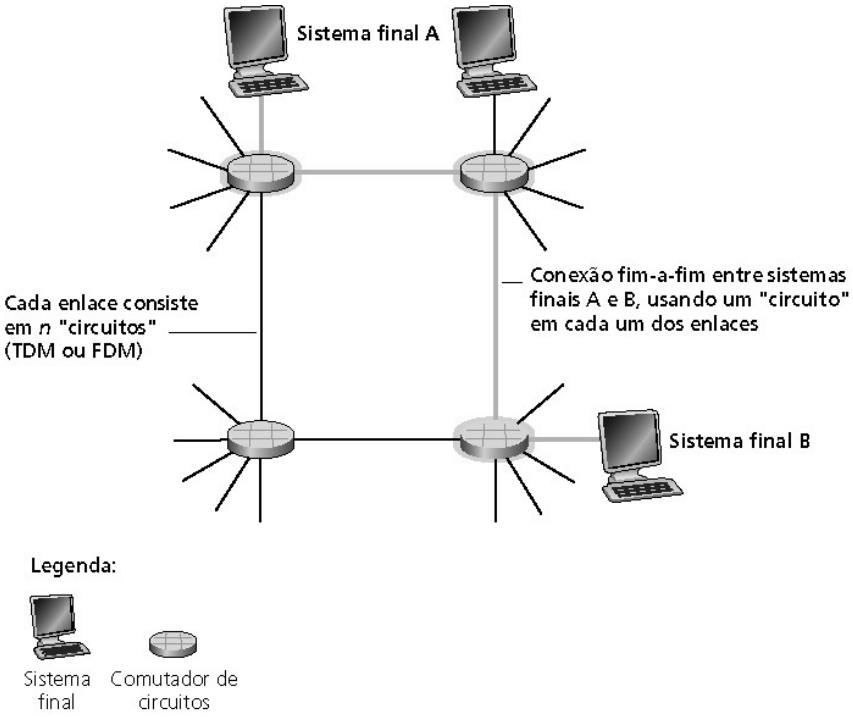
Recursos fim-a-fim são reservados por "chamada"

Taxa de transmissão, capacidade dos comutadores

Recursos dedicados: não há compartilhamento

Desempenho análogo aos circuitos físicos (QoS garantido)

Exige estabelecimento de conexão



Comutação de Circuitos

Recursos da rede (ex.: capacidade de transmissão) dividida em “pedaços”

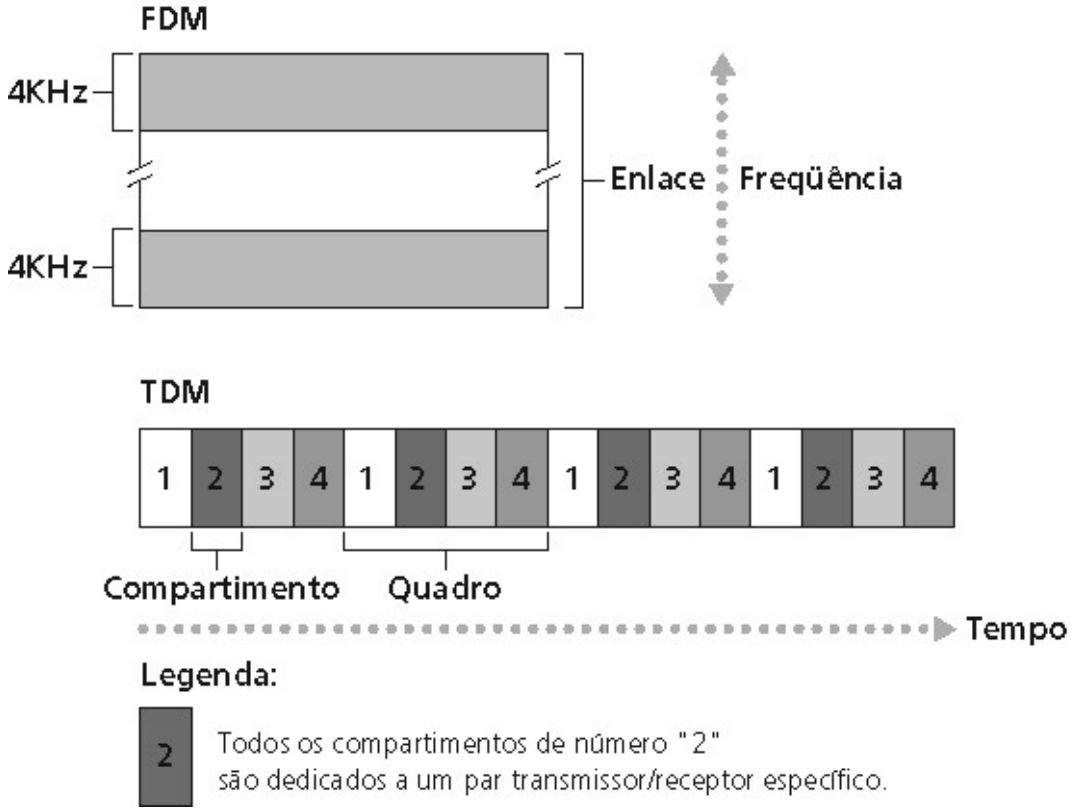
“Pedaços” alocados às chamadas

“Pedaço” do recurso desperdiçado se não for usado pelo dono da chamada **(sem divisão)**

Formas de divisão da capacidade de transmissão em “pedaços”

- Divisão em freqüência
- Divisão temporal

Comutação de Circuitos

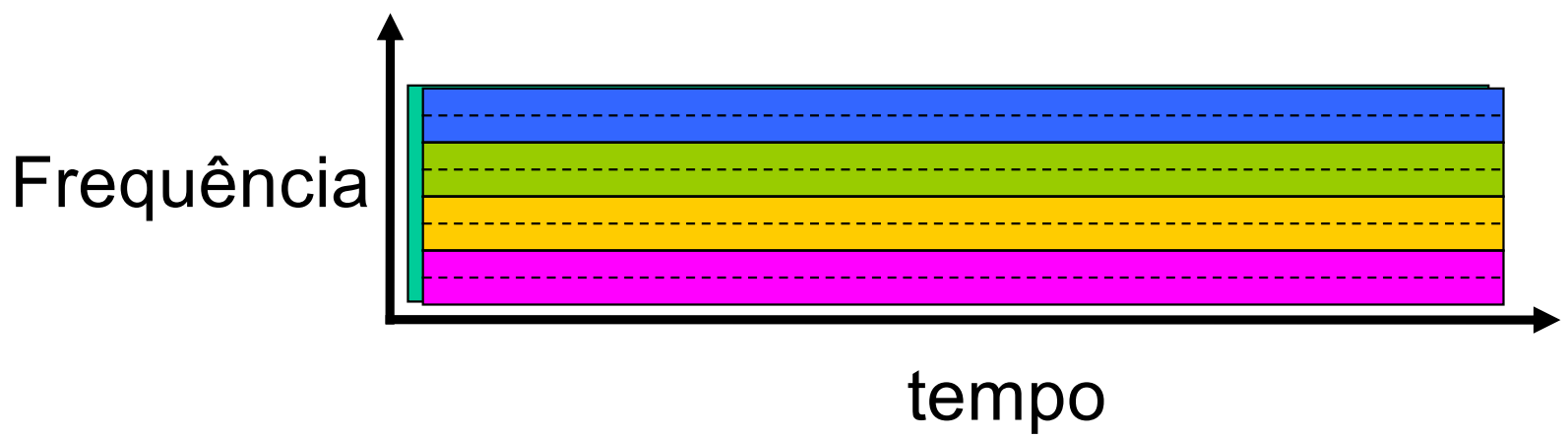


Comutação de Circuitos

FDM

Exemplo:

4 usuários

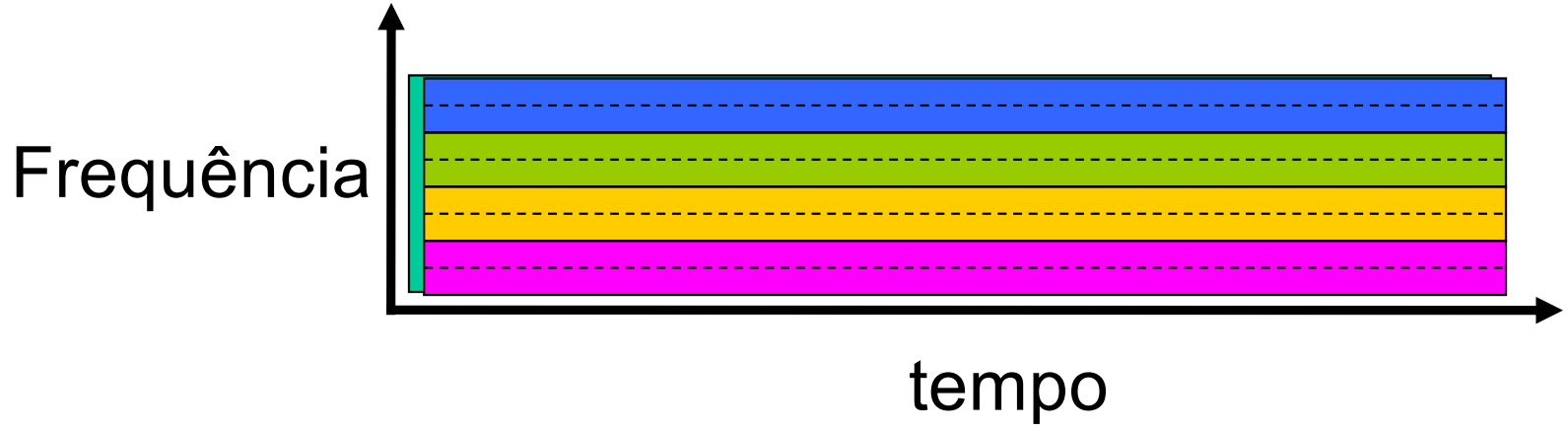


Comutação de Circuitos

FDM

Exemplo:

4 usuários



Comutação de Pacotes

Cada fluxo de dados fim-a-fim é dividido em pacotes

Os recursos da rede são compartilhados em bases estatísticas

Cada pacote usa toda a banda disponível ao ser transmitido

Recursos são usados na medida do necessário

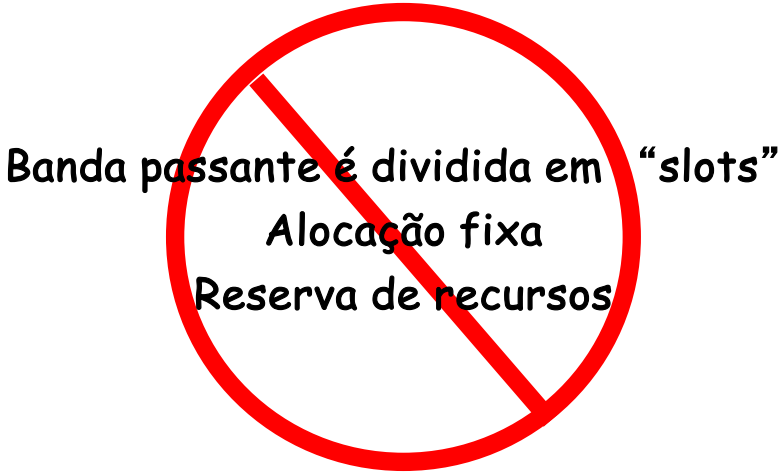
Contenção de recursos:

A demanda agregada por recursos pode exceder a capacidade disponível

Congestão: filas de pacotes, espera para uso do link

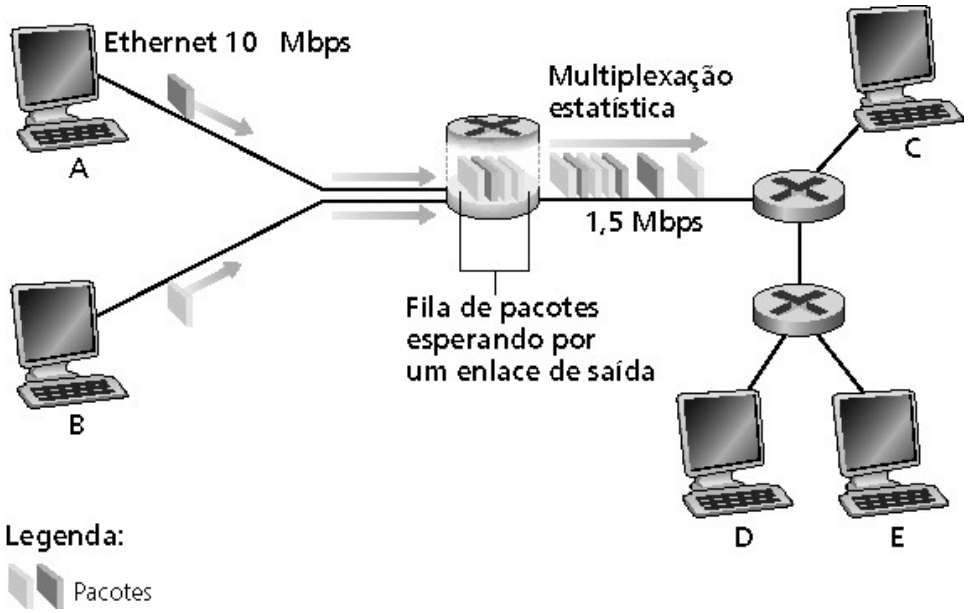
Armazena e reenvia: pacotes se movem um “salto” por vez

O nó recebe o pacote completo antes de encaminhá-lo



Comutação de Pacotes

Comutação de pacotes permite que mais usuários usem a mesma rede simultaneamente!



Modelo TCP/IP

- O TCP é o protocolo da camada de transporte orientado à conexão, que oferece um serviço confiável. Frequentemente aparece como parte da pilha TCP/IP da arquitetura Internet, mas é um protocolo de propósito geral que pode ser adaptado para uso em uma grande variedade de sistemas.
- O IP é um protocolo para comunicação em nível 3, na camada de rede. Ele é o responsável pela transmissão de nível inferior (host-to-host), e geralmente é utilizado em dois tipos de estações: hosts e gateways.

Modelo TCP/IP

- Serviço baseado na comutação de pacotes, não orientado a conexões: habilidade de sobreviver a falhas nas subredes.
- Permanece o conceito de **encapsulamento**: quando uma aplicação envia dados usando TCP/IP, ela os envia através de cada nível da pilha de protocolos.
- Cada nível adiciona sua informação aos dados da camada superior. No final, os dados são enviados como uma sequência de bits, pela rede.

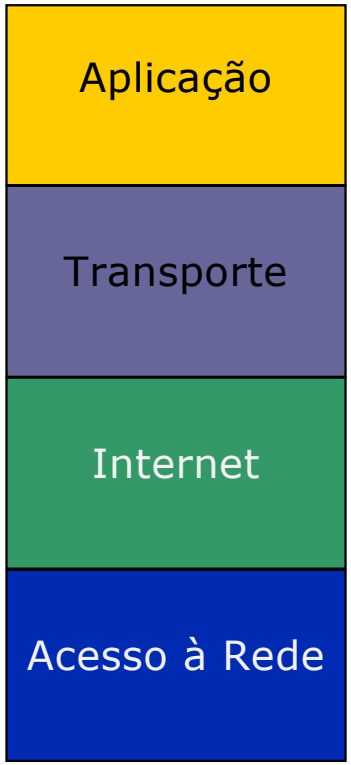
Modelo de Referência TCP/IP

- 1969 - **A**dvanced **R**esearch **P**roject **A**gency (ARPA) financia a pesquisa e o desenvolvimento de uma rede experimental de comutação de pacotes (ARPANET)
- O objetivo era estudar técnicas para implementar sistemas de comunicação de dados robustos e independentes de fornecedores
- ARPANET foi tão bem sucedida que várias organizações ligadas à rede passaram a usá-la cotidianamente
- 1975 - ARPANET deixa o caráter experimental, transformando-se em uma rede operacional, quando a **D**efense **C**ommunications **A**gency (DCA) assume o seu controle

Modelo de Referência TCP/IP

- Os protocolos TCP/IP foram desenvolvidos como padrões militares. Todos os hosts na rede tiveram que se converter para os novos protocolos
- DARPA financiou a implementação do TCP/IP na versão Berkley (BSD) Unix
- O termo “Internet” se popularizou
- 1983 - ARPANET divide-se em MILNET e uma nova (e menor) ARPANET
- 1985 - A **N**ational **S**cience **F**oundation (NSF) cria a NSFNet e a conecta a internet
- 1987 - NSF cria um novo e mais rápido backbone e uma topologia em três camadas que incluem o backbone, redes regionais e redes locais
- 1990 - ARPANET encerra suas atividades
- 1995 - NSFNet deixa de ser o principal backbone da Internet

Modelo de Referência TCP/IP



HTTP, FTP, E-mail (IMAP, POP3...),

Acesso Remoto (SSH, Telnet...)

TCP: orientado a conexão => confiável
UDP: não orientado a conexão => não confiável

IP, ICMP, IGMP

Device Driver e NIC

Serviço Orientado a Conexão

Meta: transferência de dados entre sistemas finais.
Handshaking: estabelece as condições para o envio de dados antes de enviá-los
Alô: protocolo humano
Estados de "conexão" controlam a troca de mensagens entre dois hospedeiros

TCP - Transmission Control Protocol
Realiza o serviço orientado à conexão da Internet

Serviço TCP [RFC 793]
Transferência de dados confiável e seqüencial, orientada à cadeia de bytes
Perdas: reconhecimentos e retransmissões
Controle de fluxo:
Evita que o transmissor afogue o receptor
Controle de congestão:
Transmissor reduz sua taxa quando a rede fica congestionada

Serviço Não Orientado a Conexão

Meta: transferência de dados entre sistemas finais

UDP - User Datagram Protocol [RFC 768]: oferece o serviço sem conexão da Internet

- Transferência de dados não confiável
- Sem controle de fluxo
- Sem controle de congestão

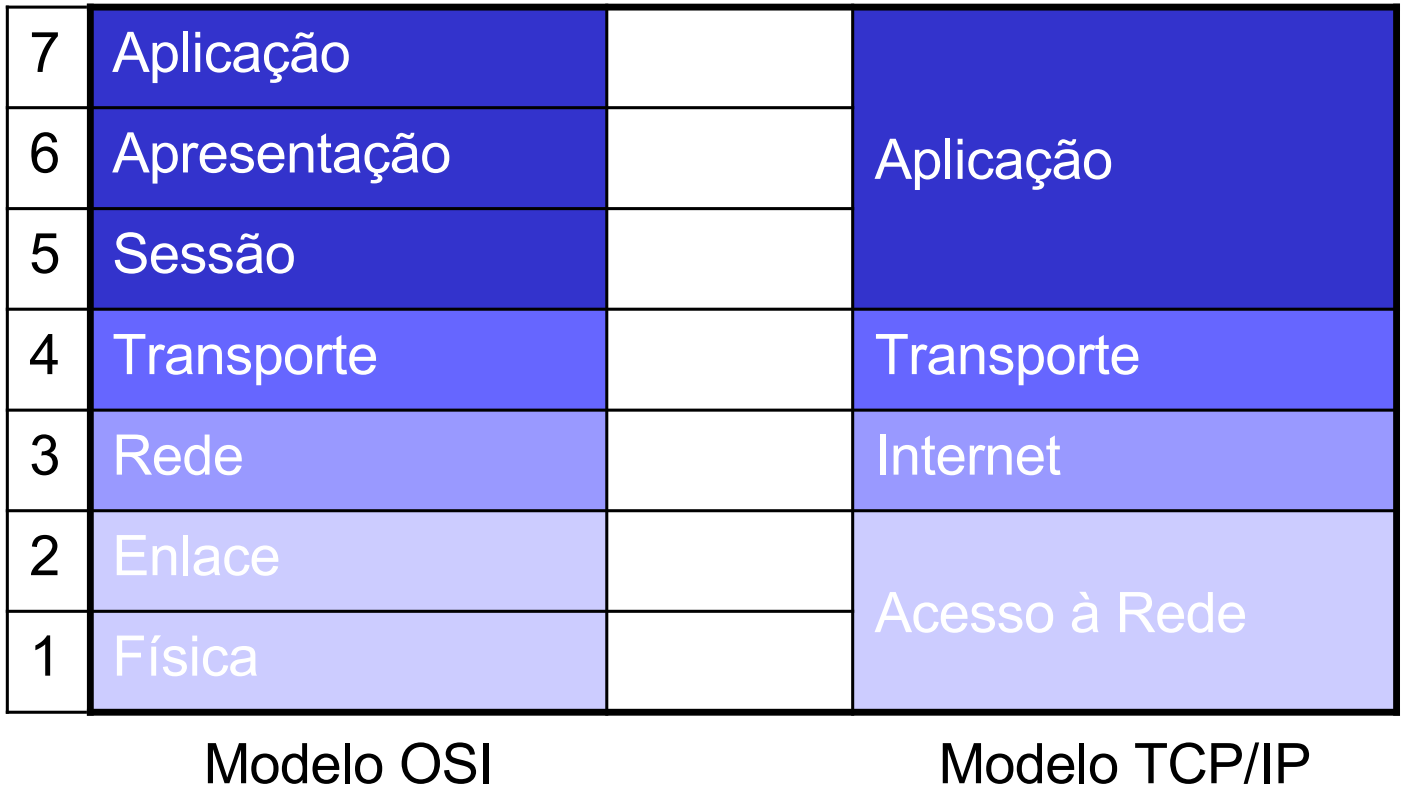
Aplicativos que usam TCP:

HTTP (Web), FTP (transferência de arquivo), Telnet (login remoto), SMTP (e-mail)

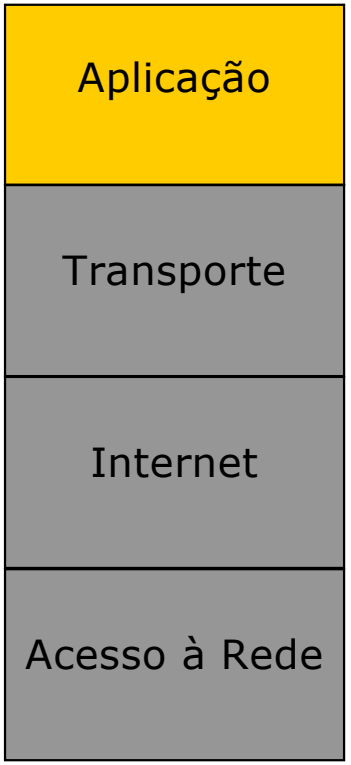
Aplicativos que usam UDP:

Streaming de mídia, vídeoconferência, DNS, telefonia VoIP

Camadas do Modelo OSI x Camadas do Modelo TCP/IP

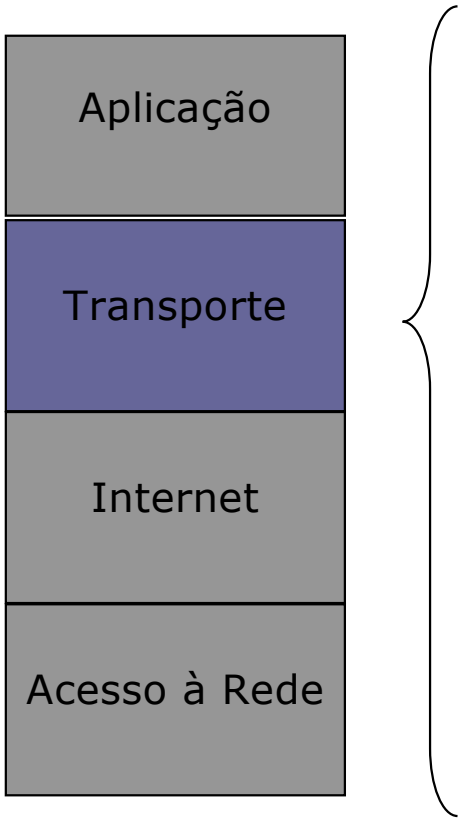


Modelo de Referência TCP/IP



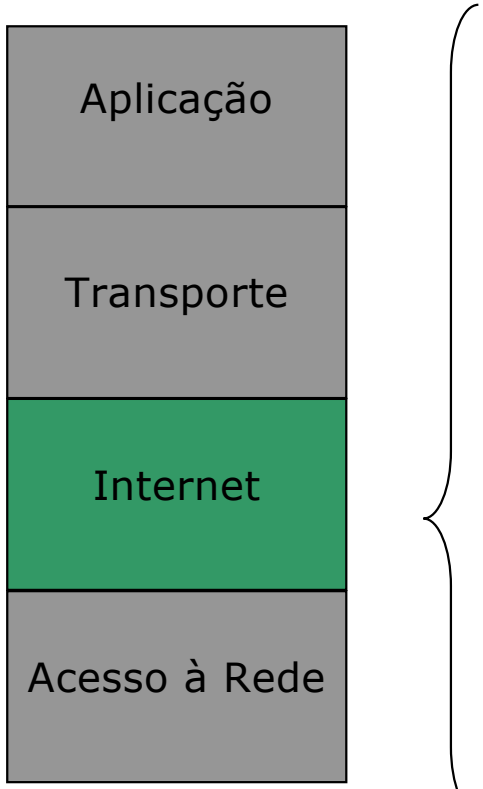
- Este nível trata dos detalhes específicos de cada aplicação
  - Representação, codificação e controle de diálogo
- Exemplos
  - Telnet, FTP, SMTP, SNMP

Modelo de Referência TCP/IP



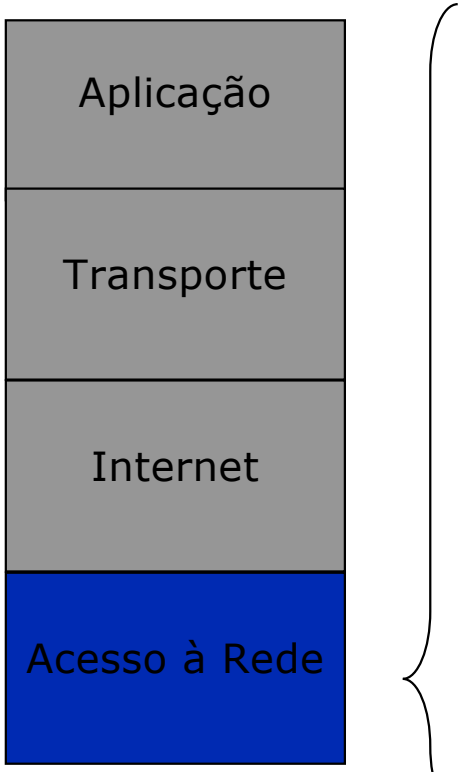
- Proporciona um fluxo de dados entre dois hosts (fim-a-fim)
  - TCP: Confiável. Sequencia os dados recebidos do nível de aplicação, agrupando-os em segmentos. Estabelece conexões (three way handshake). Confirma recepção dos segmentos enviados.
  - UDP: Não-confiável. Envia pacotes de dados (datagramas) de um host para outro, sem garantia de entrega. A sobrecarga desse protocolo é menor que a do TCP

Modelo de Referência TCP/IP



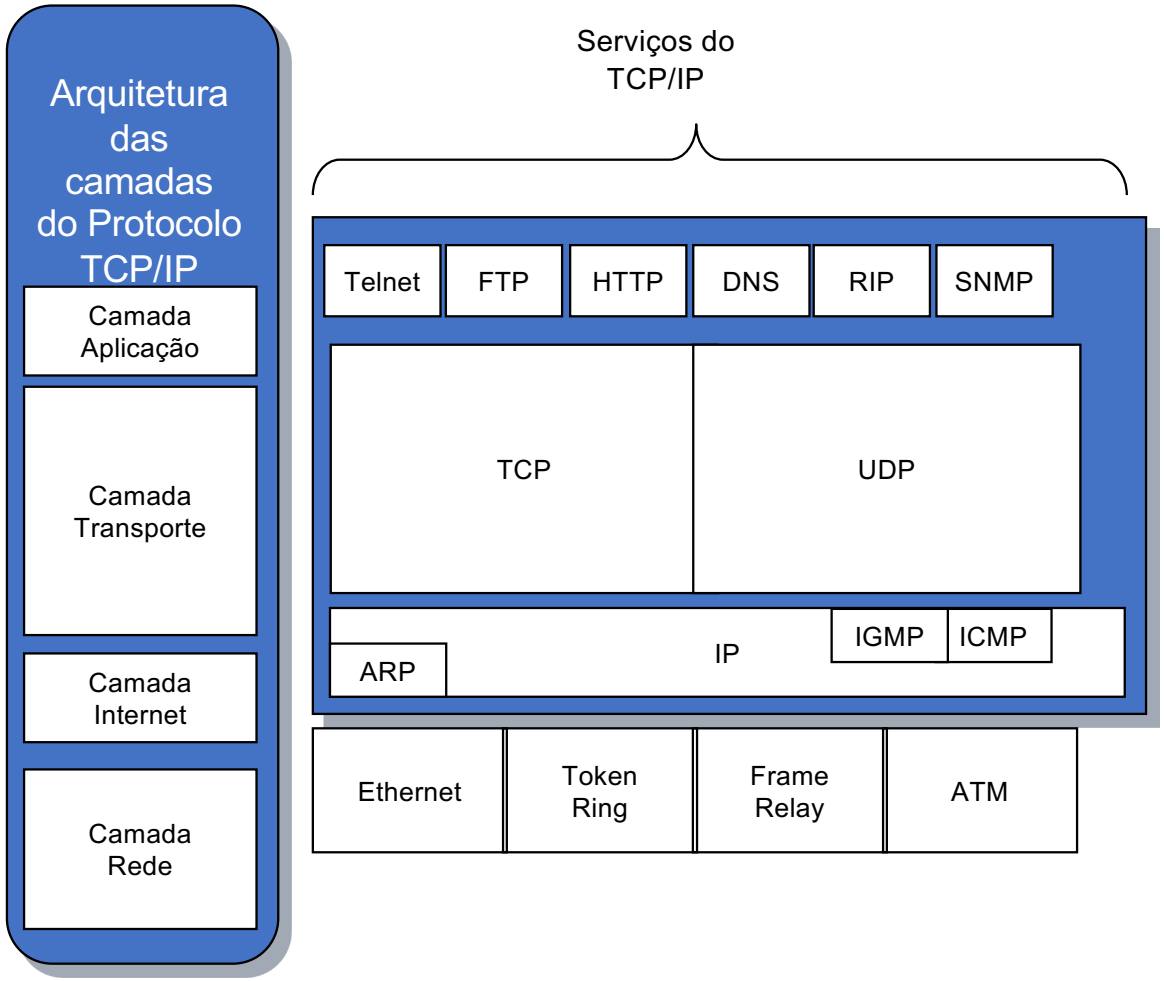
- Garantir a transmissão de pacotes independente da localização dos hosts
  - Endereçamento dos hosts
  - Roteamento
  - Controlar Congestionamento

Modelo de Referência TCP/IP



- O modelo não especifica muitos detalhes
- Abrange o driver de dispositivo no SO e a correspondente placa de rede.
- Trata dos detalhes de hardware necessários para o interfaceamento físico com a rede

Revisão Modelo TCP/IP



Comparação Modelos OSI x TCP/IP

- OSI Surgiu o primeiro modelo
  - Bem genérico
  - Houve a necessidade de criar subcamadas
- Camada de rede
  - Orientada e não orientada a conexões
- Camada de transporte
  - Orientada a conexões

- No TCP/IP surgiram os primeiros protocolos
  - Bem específico
  - Não descreve bem redes diferentes
- Camada de rede
  - Não orientada a conexões
- Camada de transporte
  - Orientada e não orientada a conexões

Por que a “rede” deve detectar e corrigir erros de transmissão?

- A detecção e correção de erros de transmissão é essencial em redes de comunicação para garantir que os dados enviados de um dispositivo para outro sejam recebidos corretamente, sem corrupção ou perda de informações.
- Isso é particularmente importante em redes TCP/IP, amplamente utilizadas na Internet e em redes locais.

Como a “rede” deve detectar e corrigir erros de transmissão?

- As técnicas utilizadas para detectar e corrigir erros de transmissão em redes TCP/IP incluem:
  - **Acknowledgement**: quando um dispositivo recebe dados, ele envia um sinal de confirmação de recebimento (ACK) de volta ao transmissor. Se o transmissor não receber um ACK, ele retransmite os dados.
  - **Checksum**: essa técnica envolve a adição de um valor de verificação de redundância cíclica (CRC) aos dados a serem transmitidos. O receptor verifica o CRC recebido e, se houver um erro, solicita que os dados sejam retransmitidos.

Como a “rede” deve detectar e corrigir erros de transmissão?

- As técnicas utilizadas para detectar e corrigir erros de transmissão em redes TCP/IP incluem:
  - **Controle de fluxo**: o controle de fluxo ajuda a garantir que os dados sejam transmitidos em uma taxa que o receptor possa lidar. Se o receptor não puder acompanhar a taxa de transmissão, ele pode enviar uma mensagem de "janela de recepção" de volta ao transmissor para informá-lo de que ele precisa diminuir a taxa de transmissão.
  - **Retransmissão seletiva**: essa técnica permite que apenas os pacotes perdidos sejam retransmitidos em vez de toda a mensagem, o que pode economizar tempo e recursos de rede.

Técnicas Utilizadas na Detecção de Erros

- Verificação de Paridade: avalia a integridade dos dados transmitidos em redes de comunicação adicionando um bit chamado de "bit de paridade" a um conjunto de bits de dados;

- O bit de paridade é definido de tal forma que a soma dos bits de dados mais o bit de paridade é sempre um número par ou ímpar, dependendo do tipo de verificação de paridade usada (par ou ímpar). Por exemplo: se um conjunto de dados contiver 5 bits "1", o bit de paridade deve ser definido como "1" para que a soma total seja um número ímpar.

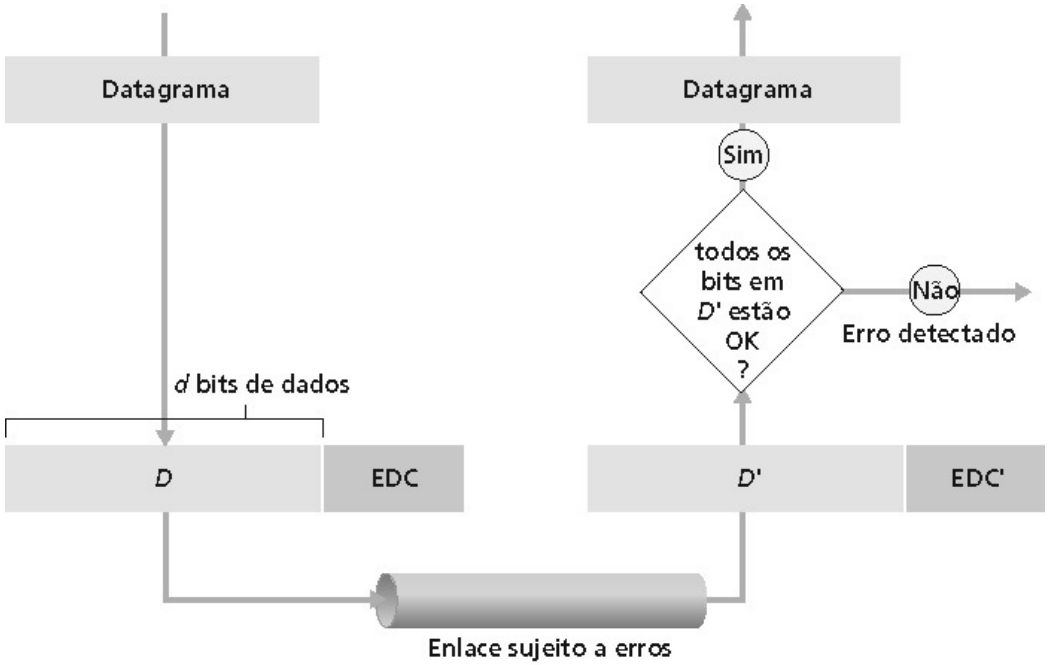
- O receptor verifica o bit de paridade para garantir que a soma total dos bits seja um número par ou ímpar, dependendo do tipo de verificação de paridade usada. Se a soma total não corresponder ao valor esperado, isso indica que um ou mais bits foram alterados durante a transmissão e que houve um erro na transmissão.

Técnicas Utilizadas na Detecção de Erros

EDC (Error Detection and Correction)= Bits de detecção e correção de erros (redundância)

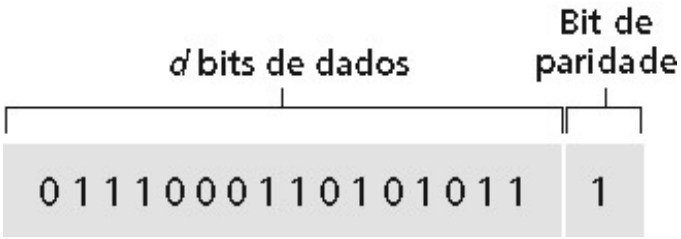
D = Dados protegidos pela verificação de erros; podem incluir os campos de cabeçalho

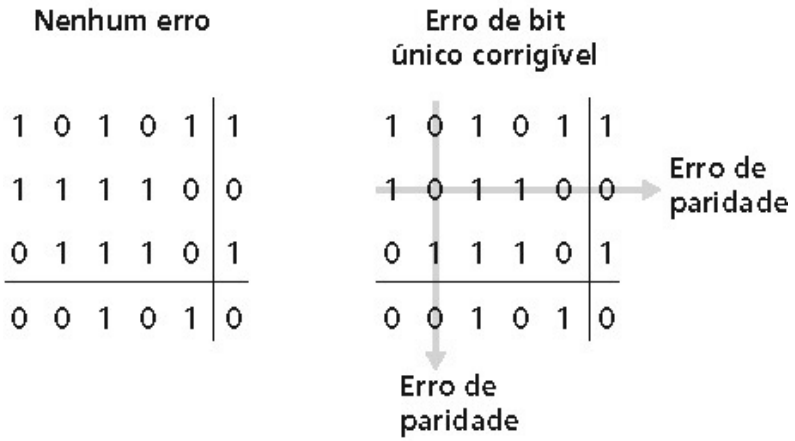
- A detecção de erros não é 100% confiável!
- Protocolos podem deixar passar alguns erros
- Quanto maior o campo EDC, melhor é a capacidade de detecção e correção de erros



Verificação de Paridade

Paridade com bit único:
Detecta erro de um único bit





Checksum

Objetivo: detectar “erros” (ex.: bits trocados) num segmento transmitido (nota: TCP e UDP computa sobre o datagrama (dados+cabeçalhos) no IP, apenas sobre o cabeçalho)

Transmissor:

- Trata o conteúdo de segmentos como seqüências de números inteiros de 16 bits
- Checksum: adição (soma em complemento de um) do conteúdo do segmento
- Transmissor coloca o valor do checksum no campo checksum do UDP/TCP

Receptor:

- Computa o checksum do segmento recebido
- Verifica se o checksum calculado é igual ao valor do campo checksum:
- NÃO — erro detectado
- SIM — não detectou erro. **Mas talvez haja erros apesar disso?**

Verificação de redundância cíclica

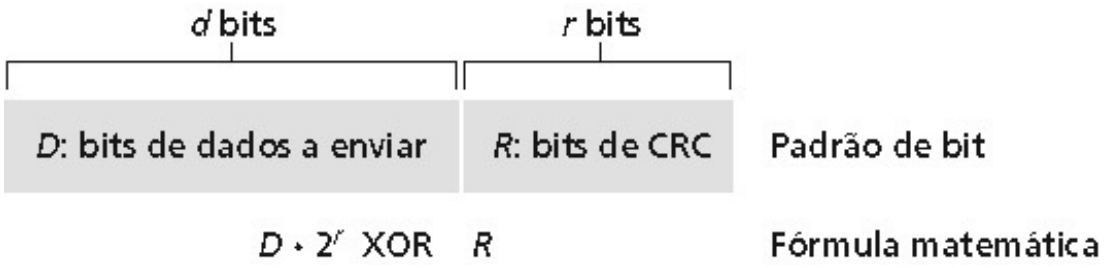
A idéia básica dos algoritmos CRC (*cyclic redudance check*) é dividir a cadeia de bits por uma outra cadeia de bits e utilizar o resto dessa divisão como checksum

- Exemplo:
  - Transmissor: Divide 327 por 9, o resto será 3.
    - Envia 327 e 3
  - Receptor: Recebe 327 e 3
    - Repete o processo do transmissor e verifica o resultado
      - 327%9= 3
      - Ou 327+(9-3)=333%9=0
      - Ou 327-3 = 324%9=0

Verificação de redundância cíclica

- Encara os bits de dados, D, como um número binário
- Escolhe um padrão gerador de r + 1 bit, G
- Objetivo: escolhe r CRC bits, R, tal que

  <D,R> é divisível de forma exata por G (módulo 2)
- Receptor conhece G, divide <D,R> por G. Se o resto é diferente de zero, erro detectado! Largamente usado na prática (ATM, HDCL)



Exemplo de CRC

desejado:

$D \cdot 2^r$ XOR R = nG

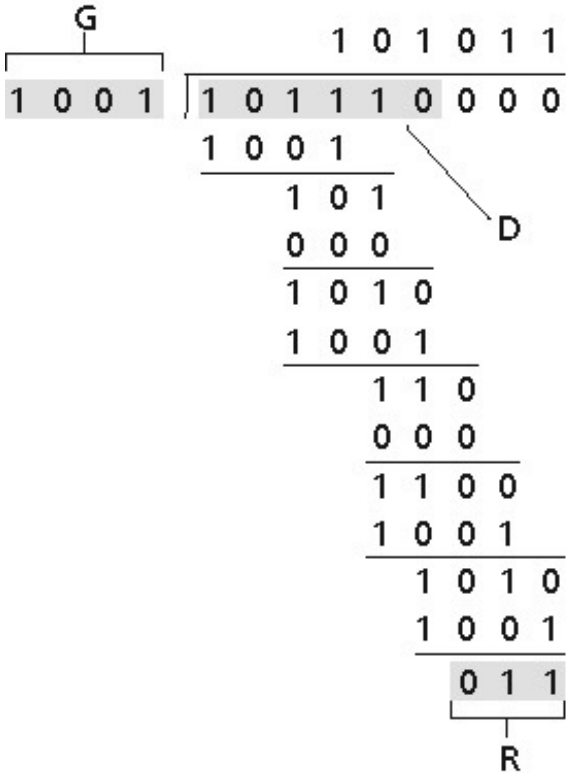
equivalente a:

$D \cdot 2^r$ = nG XOR R

equivalente a:

se nós dividimos $D \cdot 2^r$ por G, buscamos resto R

$$R = \text{resto}\left[\frac{D \cdot 2^r}{G}\right]$$



CRC - Desempenho

- O CRC pode detectar:
  - Pode detectar todos os erros em rajada (sequência de erros) com comprimento menor que r + 1 bit
  - CRC pode detectar, com alta probabilidade, os erros de comprimento maior do que o grau do polinomial.

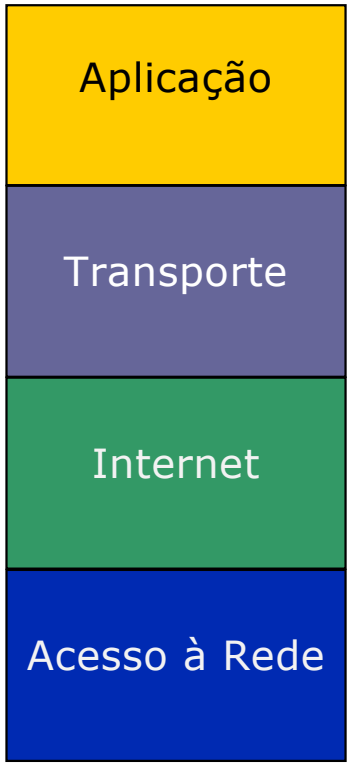
Modelo TCP/IP

- Característsticas do TCP:
  - Adota o "**Handshaking**": estabelece as condições para o envio de dados antes de efetivamente encaminhá-los (SYN, SYN-ACK, ACK, negociação);
  - **Reconhece perdas e realiza retransmissões**: transferência de dados confiável e sequencial, orientada à cadeia de bytes;
  - Realiza **controle de fluxo**: Evita que o transmissor sobrecarregue o receptor;
  - Realiza **controle de congestão**: o transmissor reduz sua taxa de transmissão ao detector que a rede está congestionada.

Modelo TCP/IP

- Característsticas do UDP:
  - Não adota o processo de handshaking;
  - Transferência de dados não confiável;
  - Sem controle de fluxo;
  - Sem controle de congestão;
  - Adotado nas comunicações onde a “velocidade” é mais importante que a “confiabilidade”.

Modelo TCP/IP



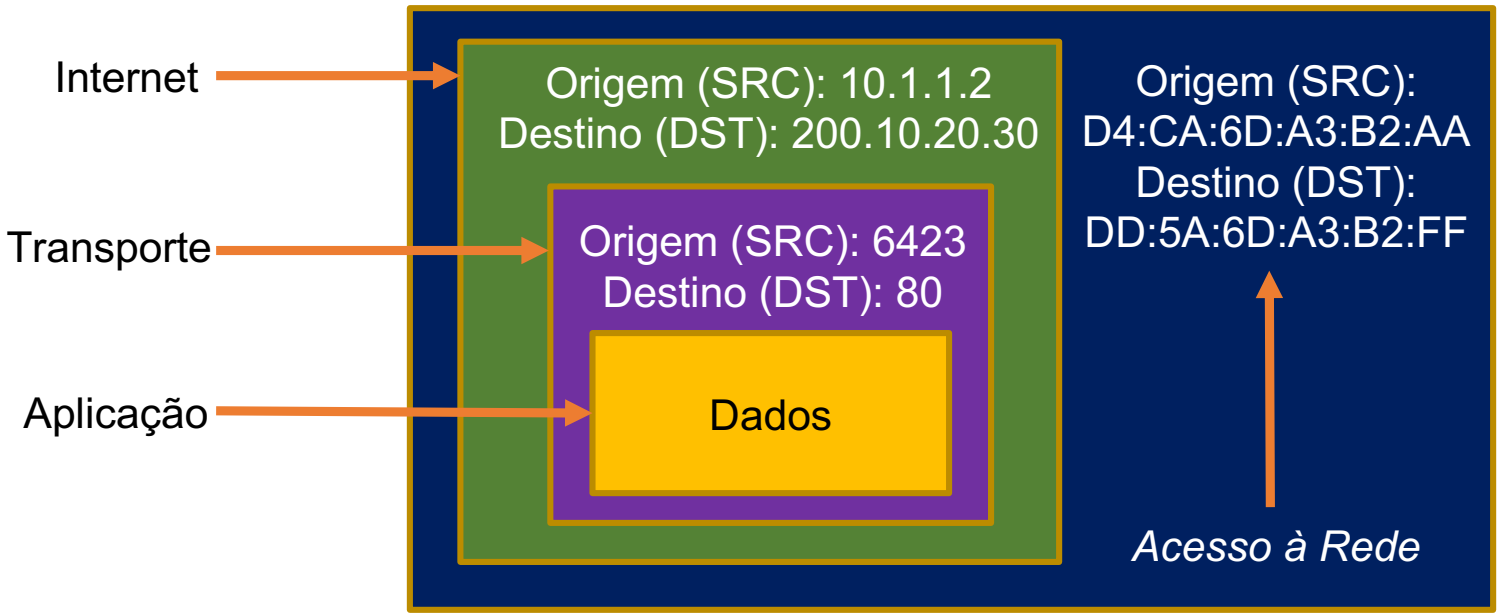
OSI L7: Os dados são gerados na camada de aplicação (Layer-7) e encapsulados camada por camada até a transformação em sinais (elétricos, luminosos, etc)

OSI L4: Cabeçalho possui porta (TCP/UDP) de origem e destino

OSI L3: Cabeçalho possui IP de origem e destino

OSI L2: Cabeçalho possui MAC de origem e destino

Modelo TCP/IP



TCP é confiável?

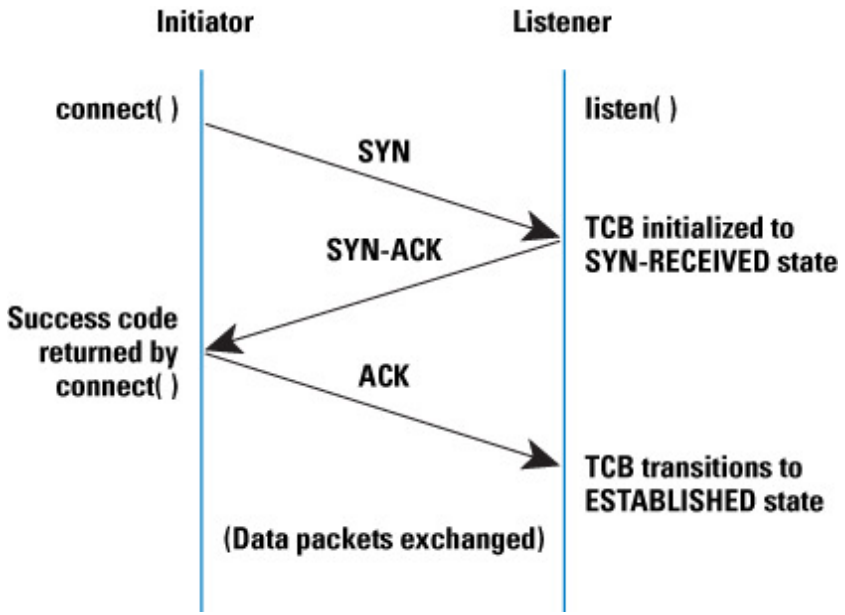
- O que queremos dizer com "confiável"?
  - Sabemos quando a outra parte recebe ou não determinados dados;
  - Os dados chegam íntegros;
  - Os dados chegam na ordem correta (ao menos para a camada de aplicação);

Como se atinge a confiabilidade?

- Qual é o principal mecanismo para assegurar a confiabilidade?
  - Números de sequência!
  - Eles permitem que os pacotes sejam identificados, reconhecidos e, implicitamente, re-solicitados
  - Para que o TCP funcione, os clientes devem conhecer os esquemas de números de sequência uns dos outros

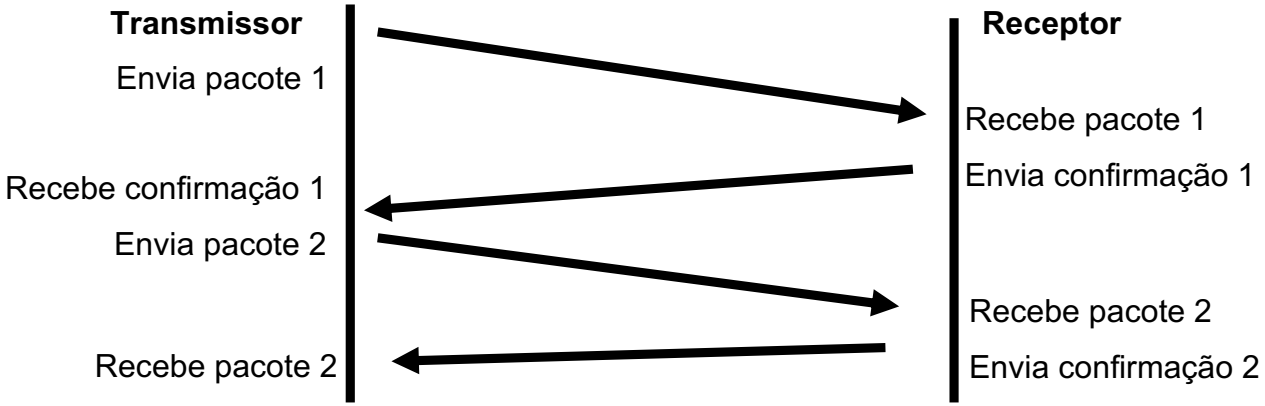
Iniciando a Comunicação: O Aperto de Mão de Três Vias (3-Way Handshaking)

- Necessidade de sincronizar a comunicação e números sequenciais;
  - Como podemos fazer isso?
- Mecanismo: Aberto Ativo x Aberto Passivo
  - Métodos: Conect() x Listen()
- Pacote SYN: Envia o próprio número de sequência A
- Pacote SYN/ACK: Reconhece com A+1, envia o próprio número de sequência B
- Pacote ACK: Reconhece com B+1

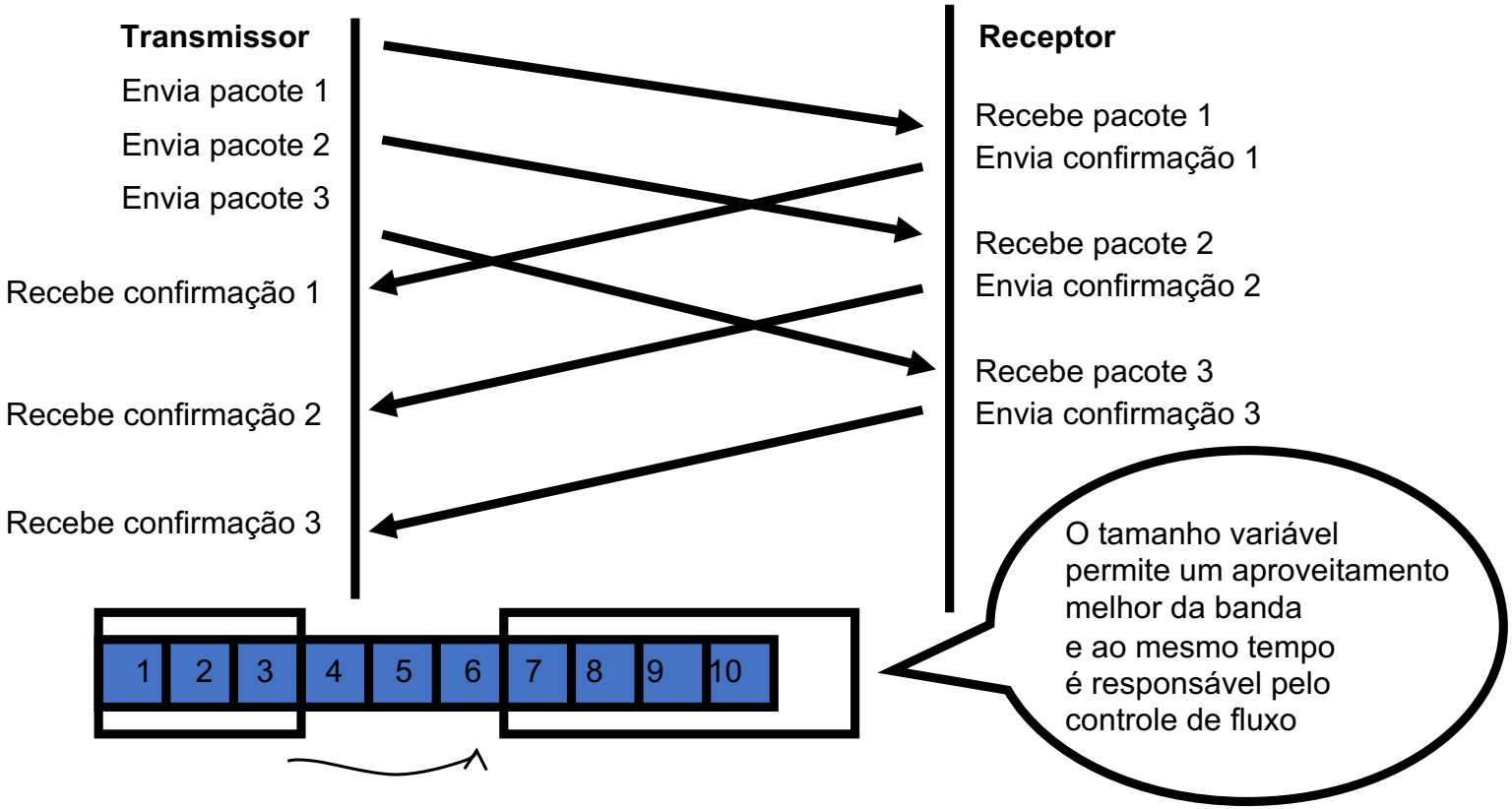


Iniciando a Comunicação: O Aperto de Mão de Três Vias (3-Way Handshaking)

- Confirmação positiva
- Retransmissão de pacotes com erro
- Ordenação dos pacotes



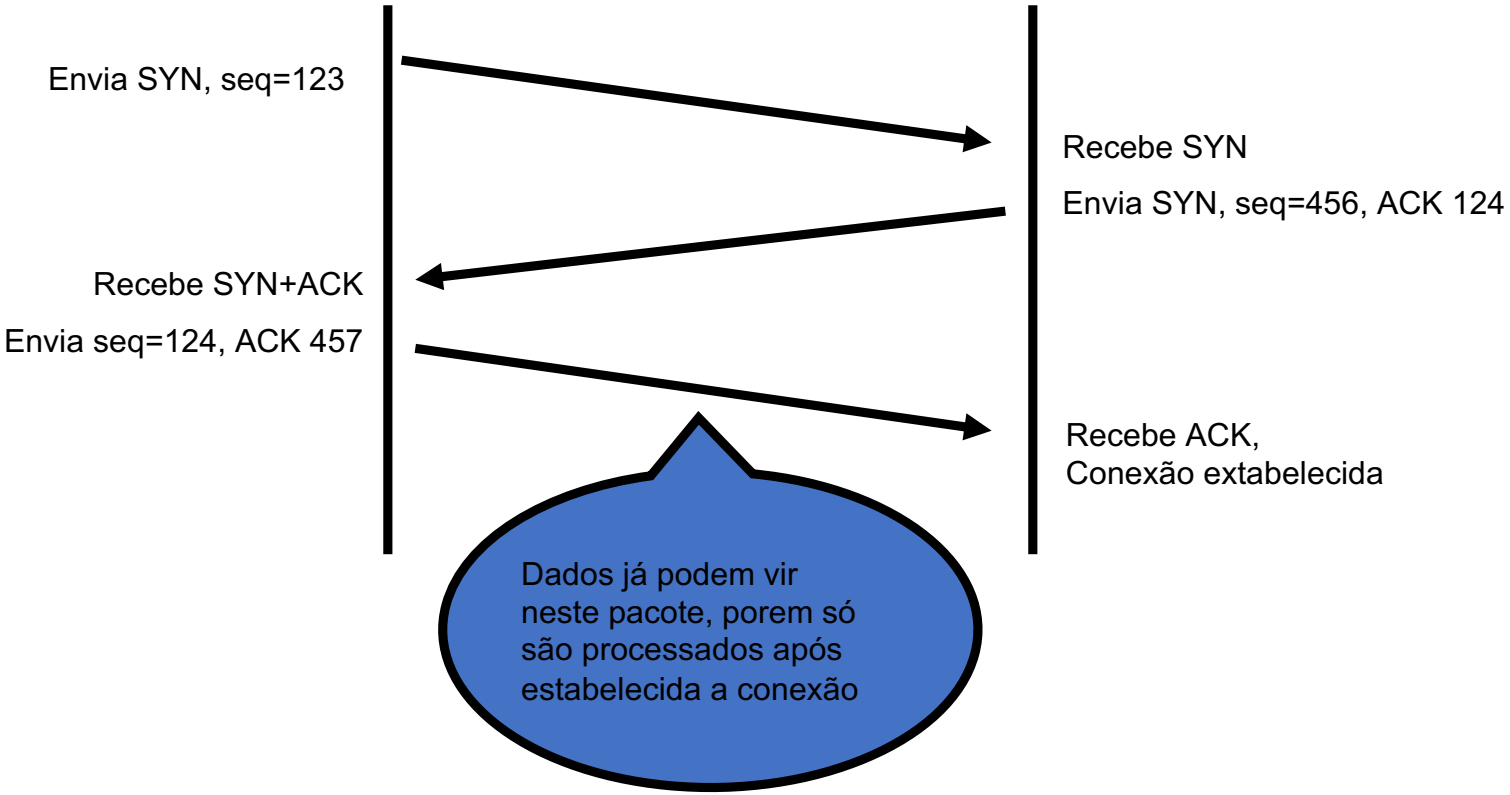
Janela Deslizante



Início da conexão

- Sincronização entre as duas pontas para o início da troca de dados
- Acordo em 3 etapas (3-way hand-shake)
- Evita que pacotes duplicados antigos provoquem uma falsa conexão.

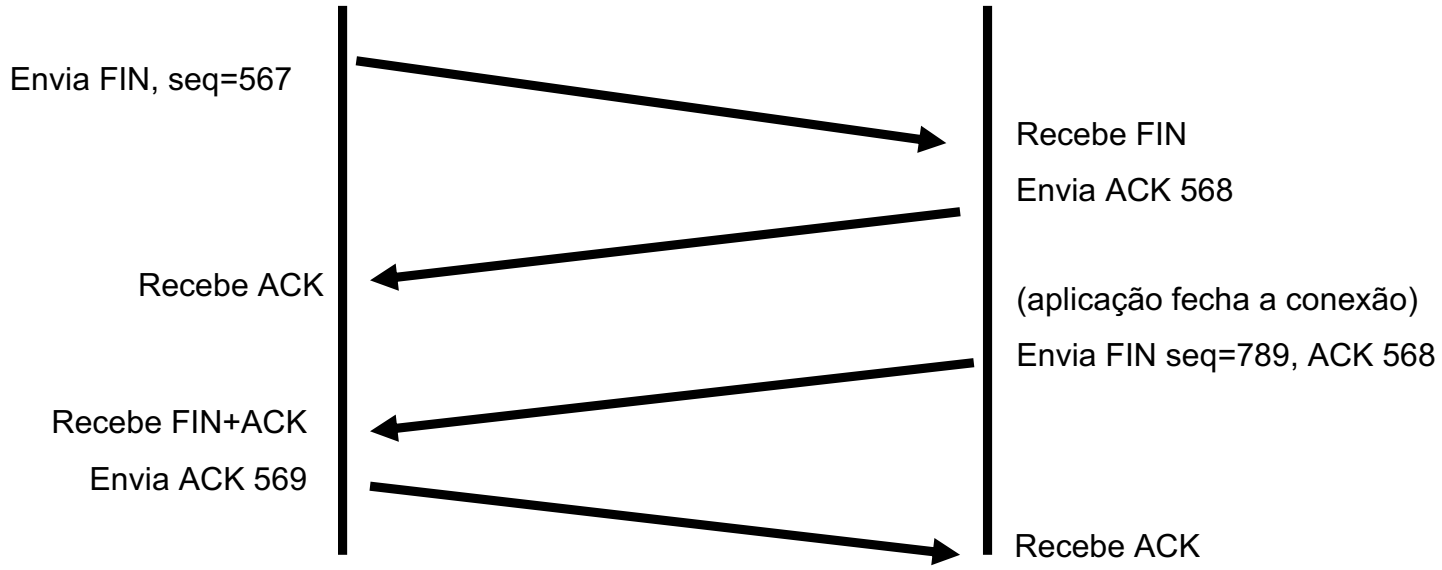
Acordo em 3 etapas

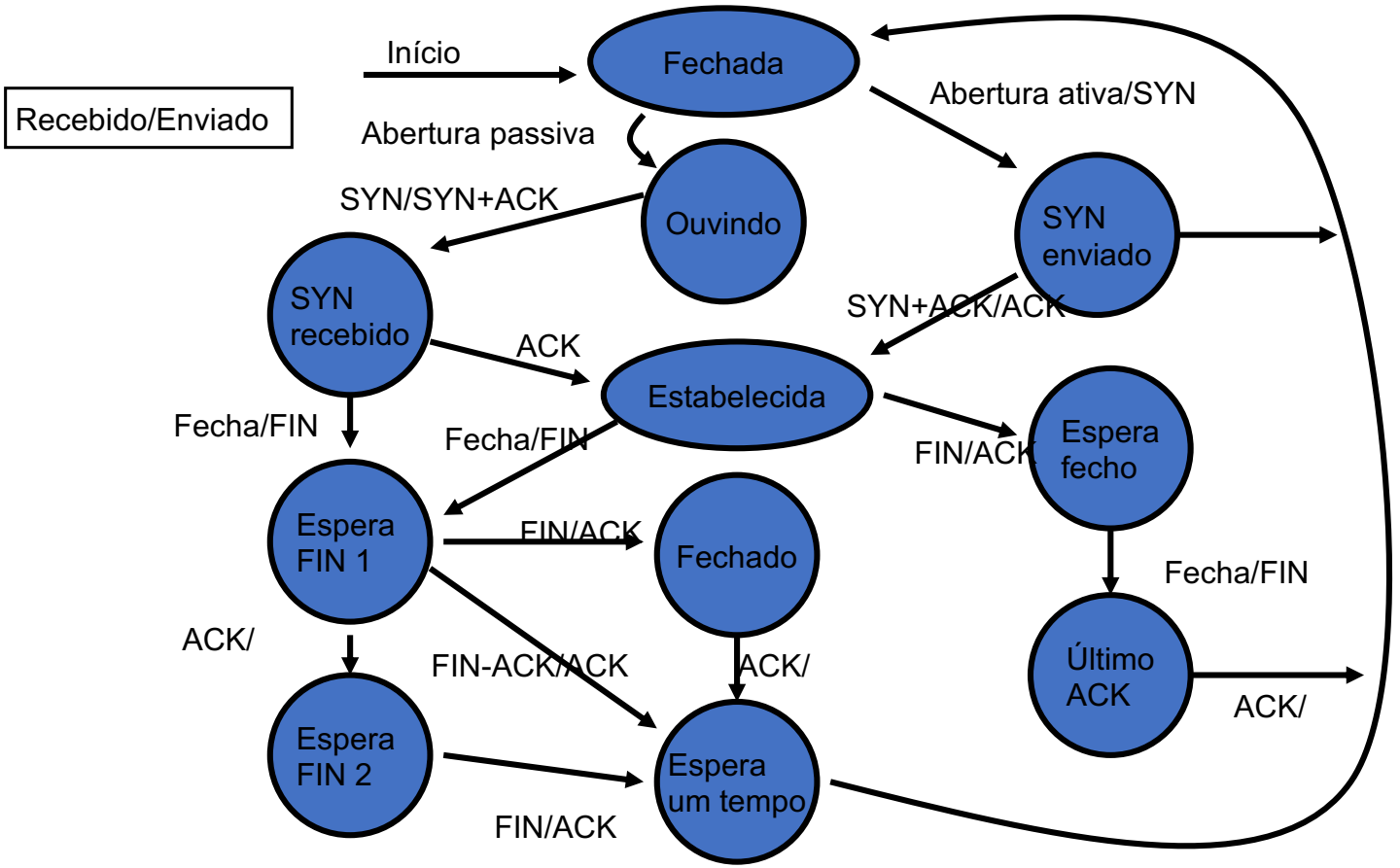


Fechamento da conexão

- 3 etapas modificado
- Fechamento da comunicação bidirecional

Fechamento TCP

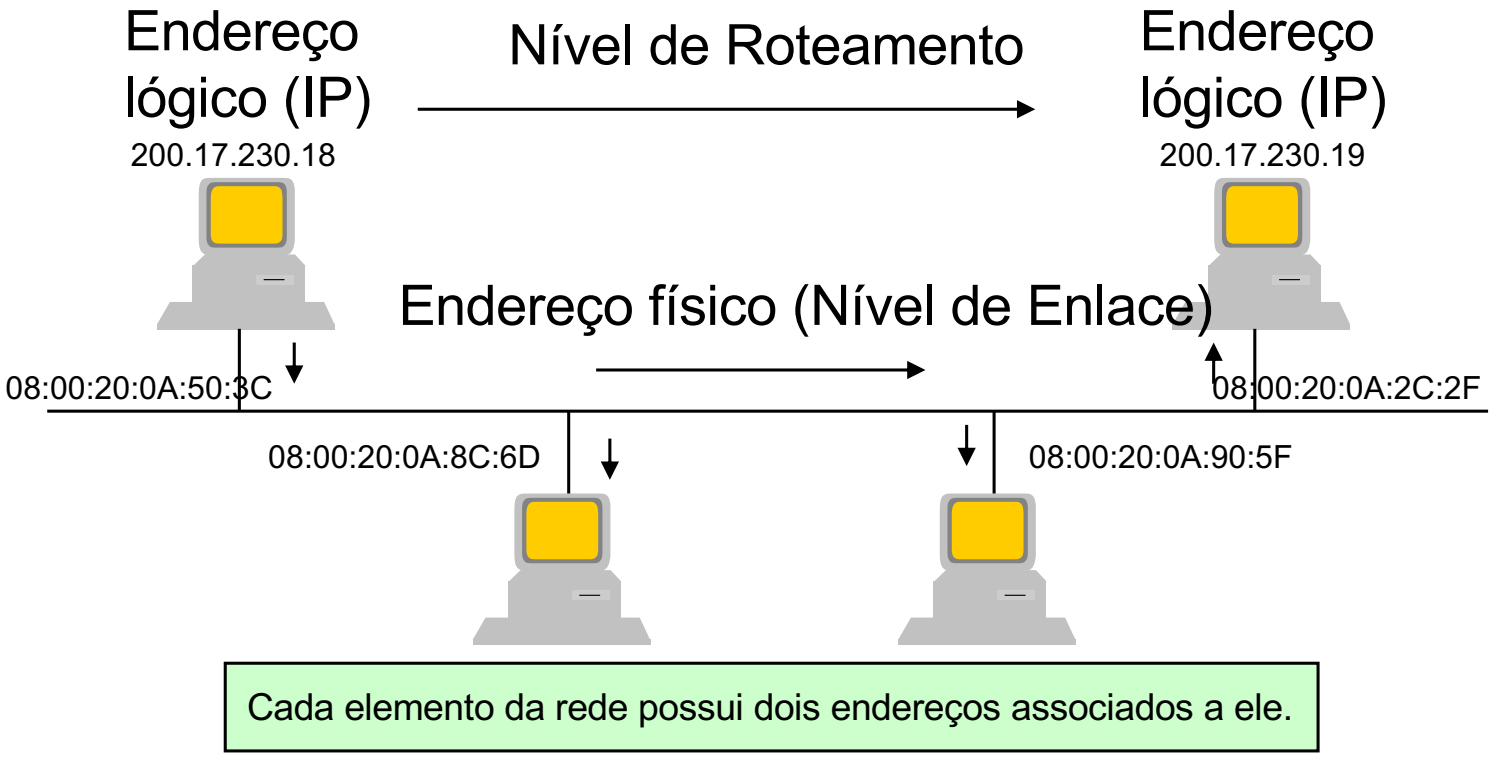



Recebido/Enviado
Início
Fechada
Abertura ativa/SYN
Abertura passiva
Ouvindo
SYN/SYN+ACK
SYN enviado
SYN recebido
SYN+ACK/ACK
ACK
Estabelecida
Fecha/FIN
Fecha/FIN
FIN/ACK
Espera fecho
Espera FIN 1
FIN/ACK
Fechado
Fecha/FIN
ACK/
FIN-ACK/ACK
ACK/
Último ACK
ACK/
Espera FIN 2
Espera um tempo
FIN/ACK

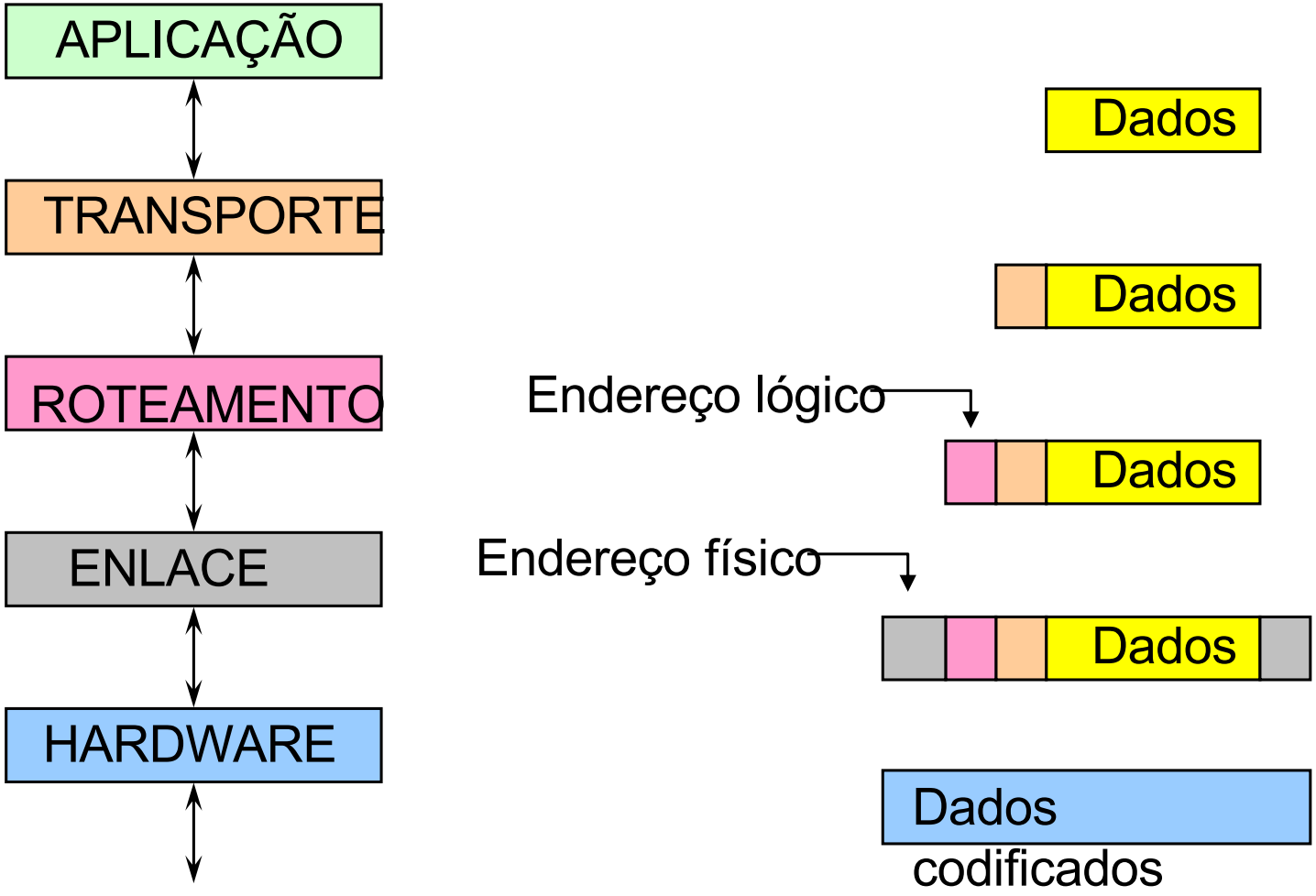
Modelo TCP/IP

```
MacBook-Air-de-Klayton:~ klayton$ netstat -nb
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)        rxbytes    txbytes
tcp4       0    239  192.168.0.136.53877    34.95.229.88.443       ESTABLISHED          0        407
tcp4       0      0  192.168.0.136.53875    34.102.185.99.443      ESTABLISHED       7638       1956
tcp4       0      0  192.168.0.136.53874    35.198.44.170.443      ESTABLISHED       4317       2305
tcp4       0      0  192.168.0.136.53873    54.85.136.197.443      ESTABLISHED       5584       1793
tcp6       0      0  2804:3a8:3ab5:27.53872 2606:4700::6810:.443   ESTABLISHED       3788       2007
tcp4       0      0  192.168.0.136.53871    35.198.52.213.443      ESTABLISHED      13704       5292
tcp4       0      0  192.168.0.136.53870    34.95.229.88.443       ESTABLISHED       7234       2902
tcp6       0      0  2804:3a8:3ab5:27.53869 2606:4700::6812:.443   ESTABLISHED       4359       2046
tcp4       0      0  192.168.0.136.53868    35.198.42.85.443       ESTABLISHED      18259       3615
tcp6       0      0  2804:3a8:3ab5:27.53867 2800:3f0:4004:80.443   ESTABLISHED       5995       2250
tcp6       0      0  2804:3a8:3ab5:27.53865 2800:3f0:4004:81.443   ESTABLISHED       8616       2317
```

Resolução de Endereços



Endereço em cada camada



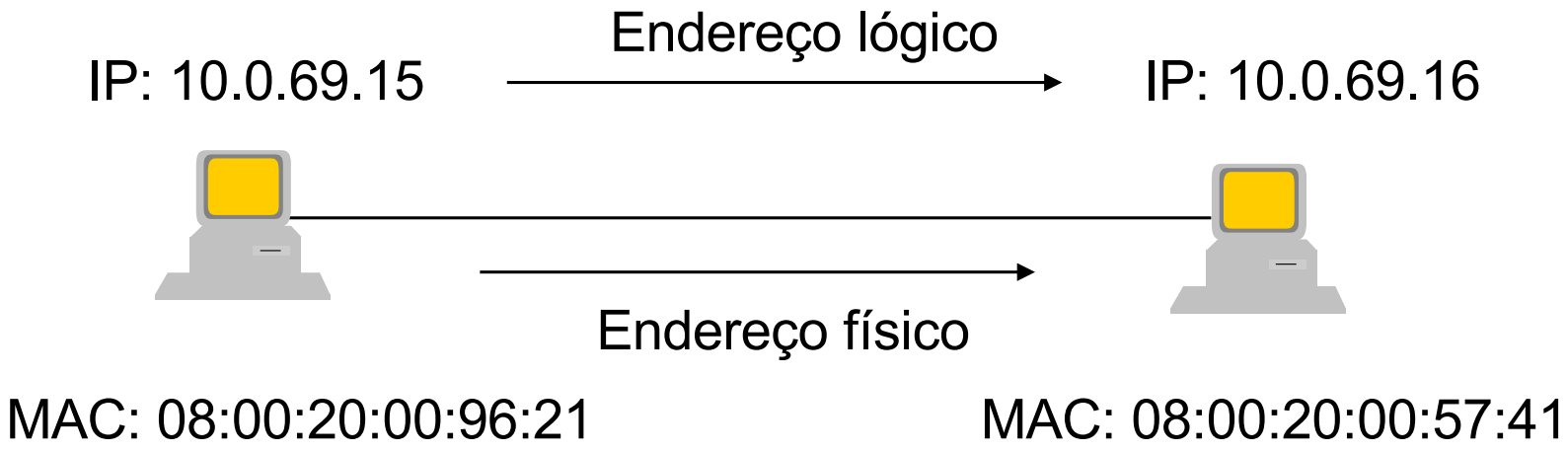
O endereço Físico

- Numa rede Ethernet o endereço usado pela camada de enlace (endereço físico) chama-se Endereço MAC (Media Access Control) e vem gravado no Hardware do dispositivo de rede
- é um endereço de 48 bits representado em notação hexadecimal pontuada.
- Exemplo: 08:00:20:0A:8C:6D
- são atribuídos pelo IEEE e não se repetem nunca
- os três primeiros bytes correspondem ao código do fabricante

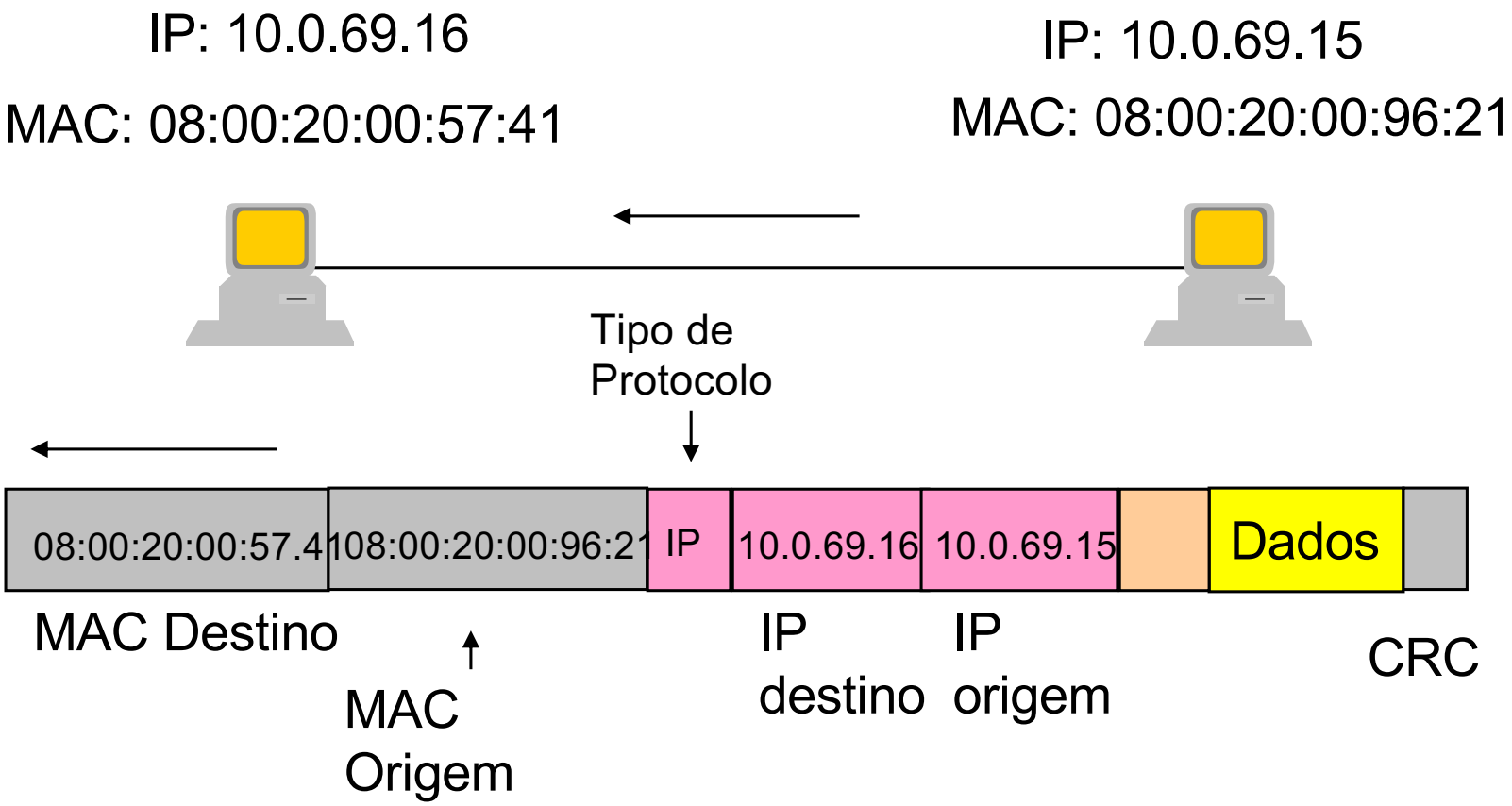
O Endereço Lógico

- O endereço IP é o endereço lógico de uma rede TCP/IP
- ele é programado na máquina, quando esta é ligada em rede.
- O endereço IP depende do local dentro da rede onde a máquina está instalada (segmento da rede ao qual ele pertence)
- Existe uma tabela que relaciona o endereço IP com o endereço MAC

O endereçamento na rede



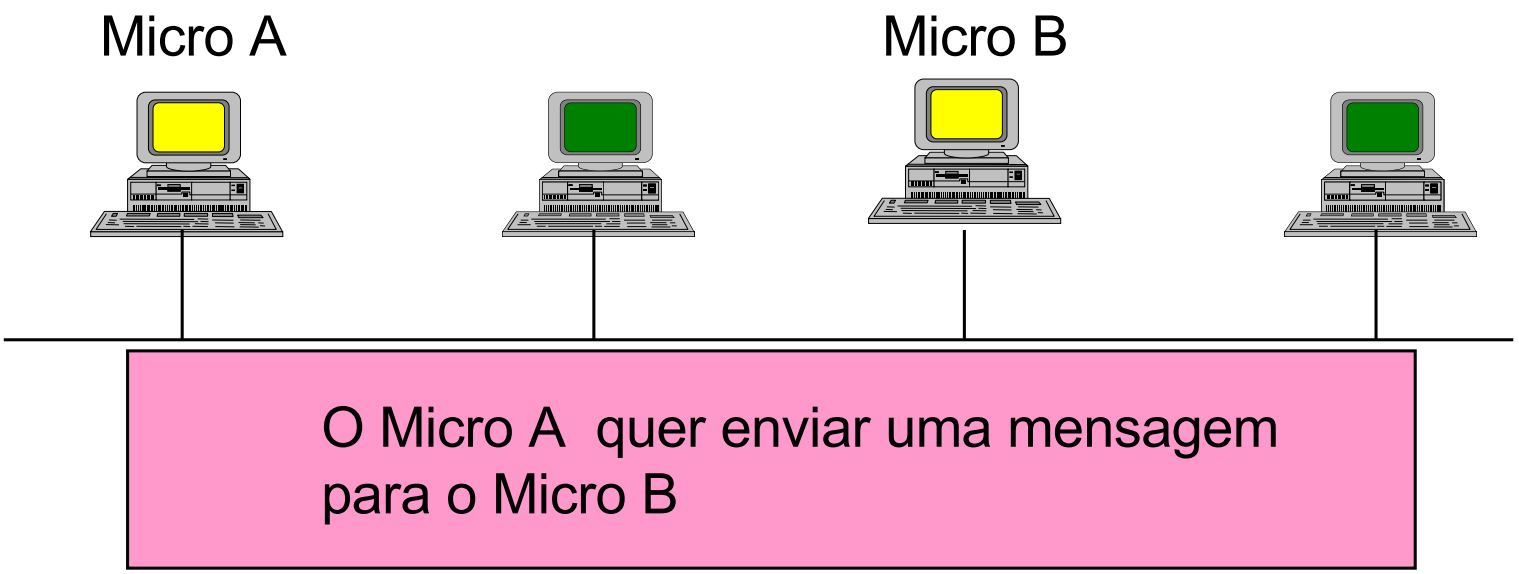
Mensagem TCP/IP no Nível de Enlace em uma Rede Ethernet



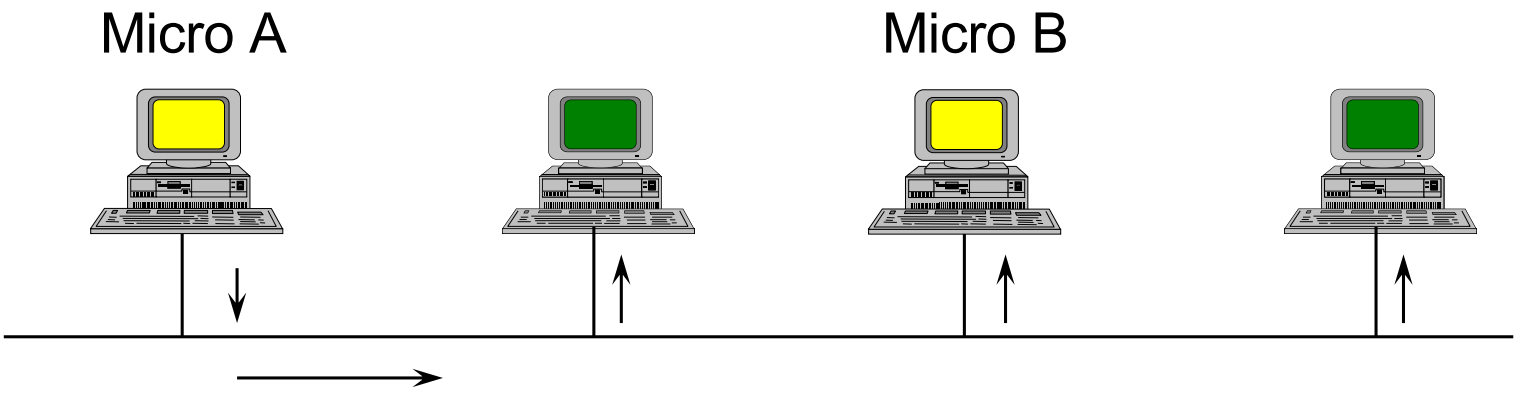
ARP - Address Resolution Protocol

- em cada máquina existe uma tabela que possui a relação entre o endereço MAC e o Endereço IP correspondente (Tabela ARP)
- Quando um endereço IP não se encontra na tabela, a máquina manda um broadcast para saber quem tem aquele endereço IP
- Comando para listar a tabela: `arp -a`

Exemplo de Resolução de Endereços

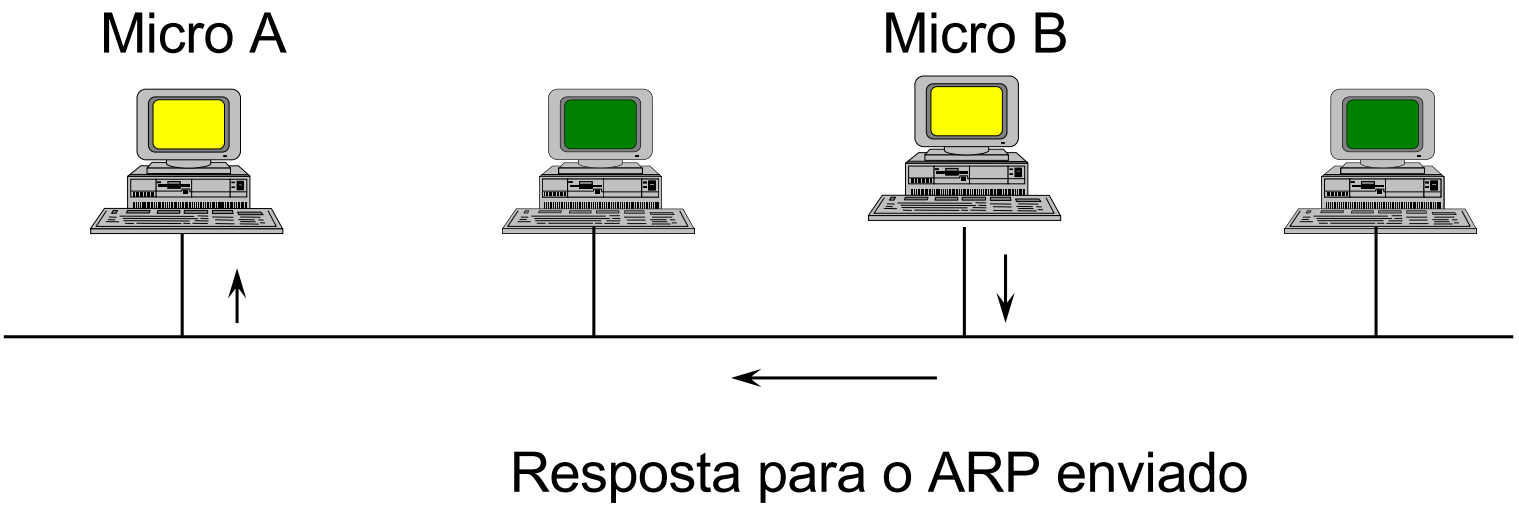


Exemplo de Resolução de Endereços



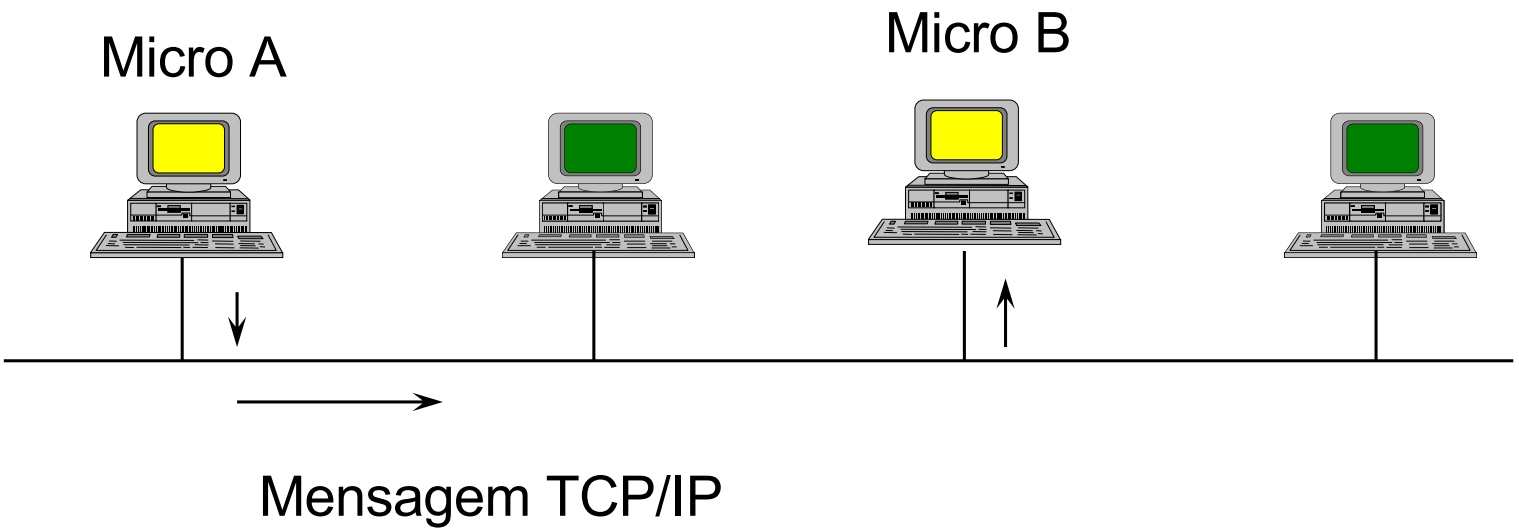
O Micro A envia uma mensagem ARP para a
rede solicitando que o Micro B informe o seu endereço MAC

Exemplo de Resolução de Endereços



O Micro B responde ao micro A, informando seu endereço MAC

Exemplo de Resolução de Endereços

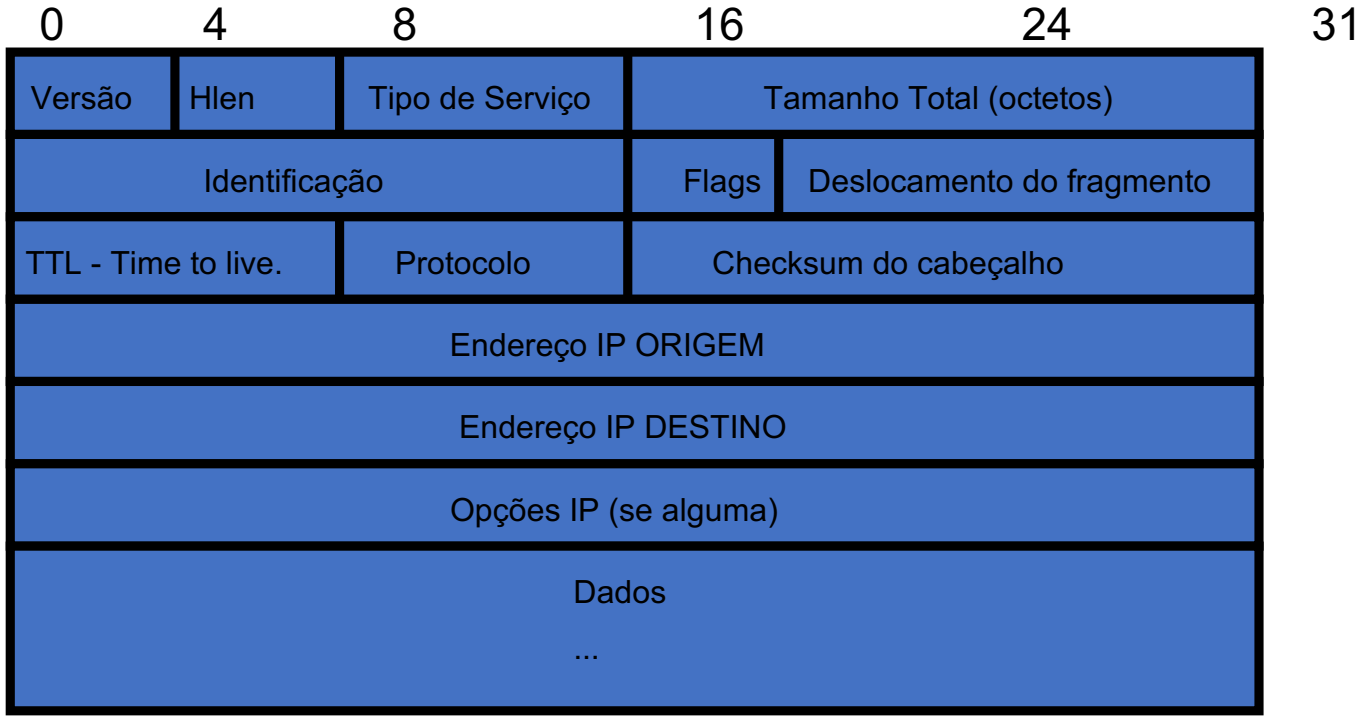


O micro A envia a mensagem, colocando no campo de destino, o endereço MAC do Micro B

Outros Protocolos de Resolução de Endereço

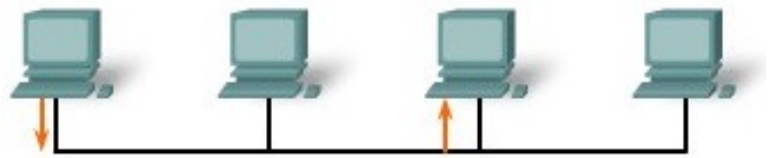
- RARP - *Reverse* ARP - Utilizado por uma estação sem disco para descobrir seu próprio endereço IP
- BOOTP - *Boot Protocol* - fornece outras informações como o *default gateway*
- DHCP - *Dynamic Host Configuration Protocol* - permite uma faixa de seja endereços alocada dinamicamente

O Datagrama IP

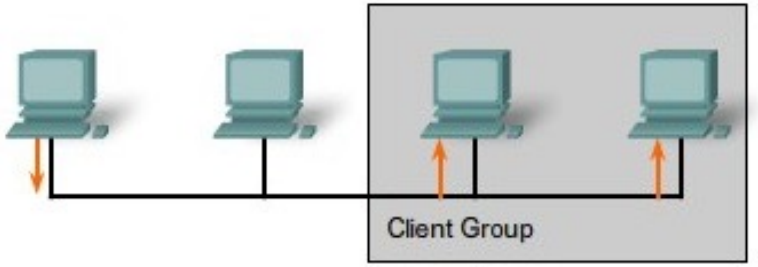


Tipo de Conexão

Unicast: Comunicação na qual um quadro é enviado de um host e endereçado a um destino específico.

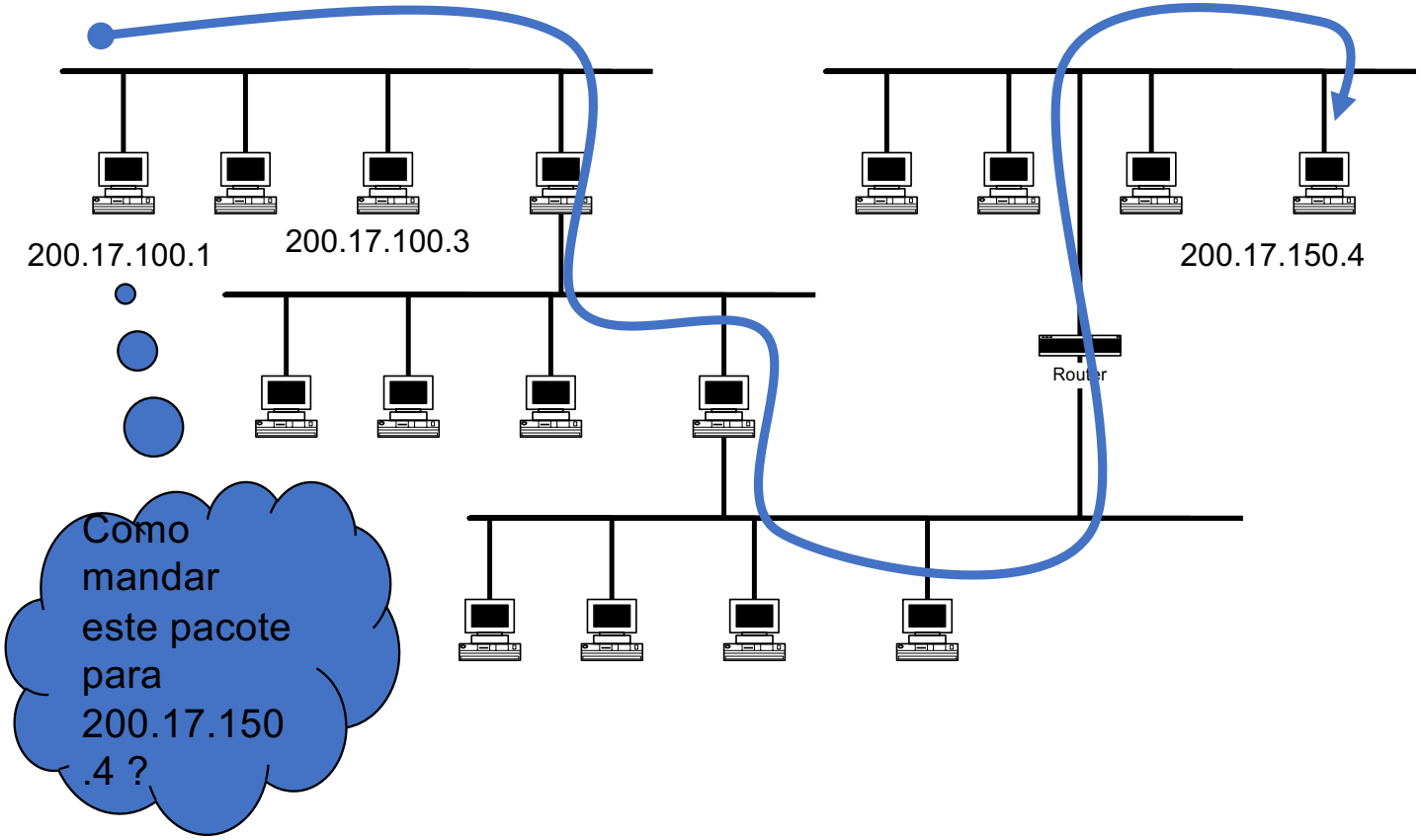


Multicast: Comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes.
Os clientes da transmissão *multicast* devem ser membros de um grupo *multicast* lógico para receber as informações.

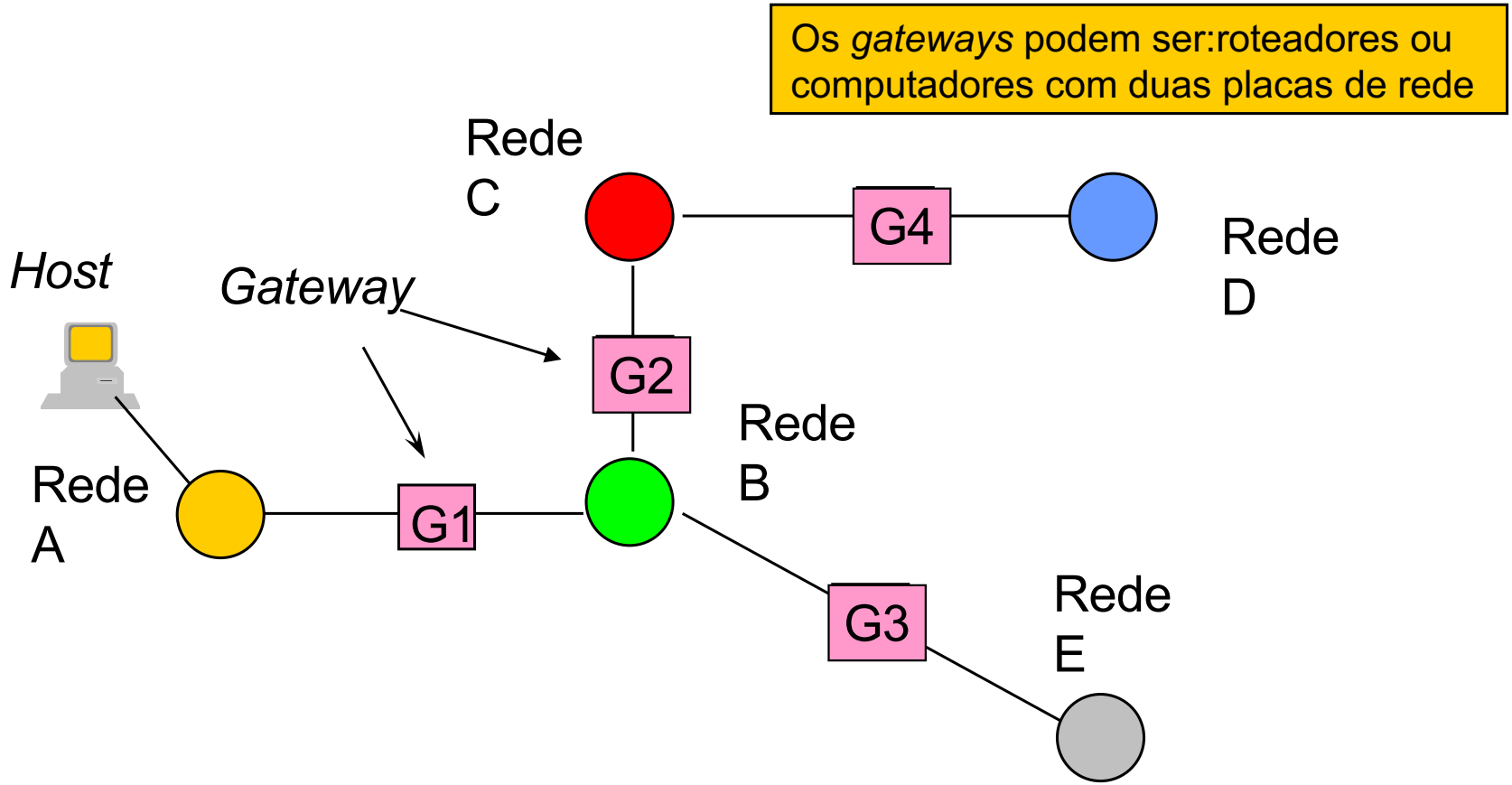


Broadcast: Comunicação na qual um quadro é enviado de um endereço para todos os outros endereços. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados.

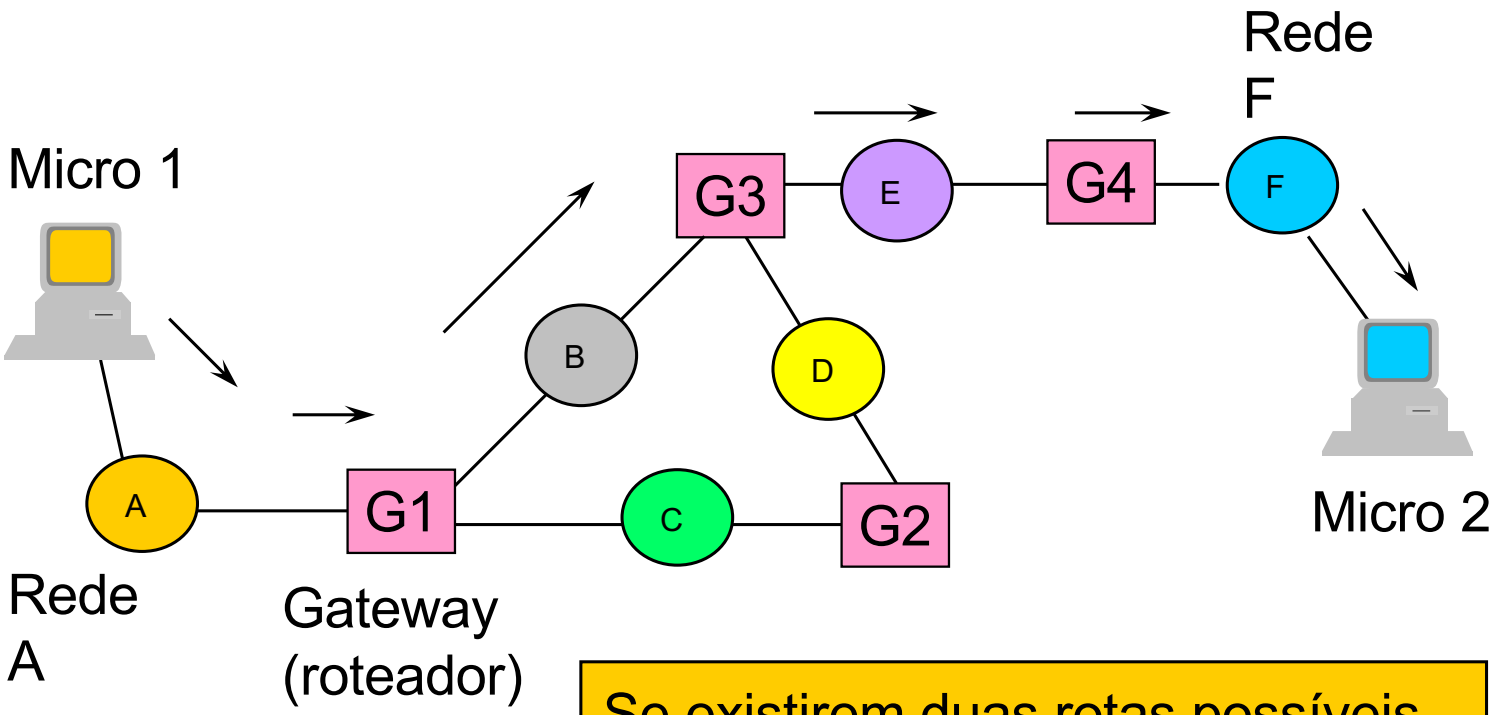
Roteamento dos Pacotes



Gateway


Os *gateways* podem ser:roteadores ou computadores com duas placas de rede
Rede C
G4
Rede D
Host
Gateway
G2
Rede B
Rede A
G1
G3
Rede E

Como a mensagem trafega numa WAN?

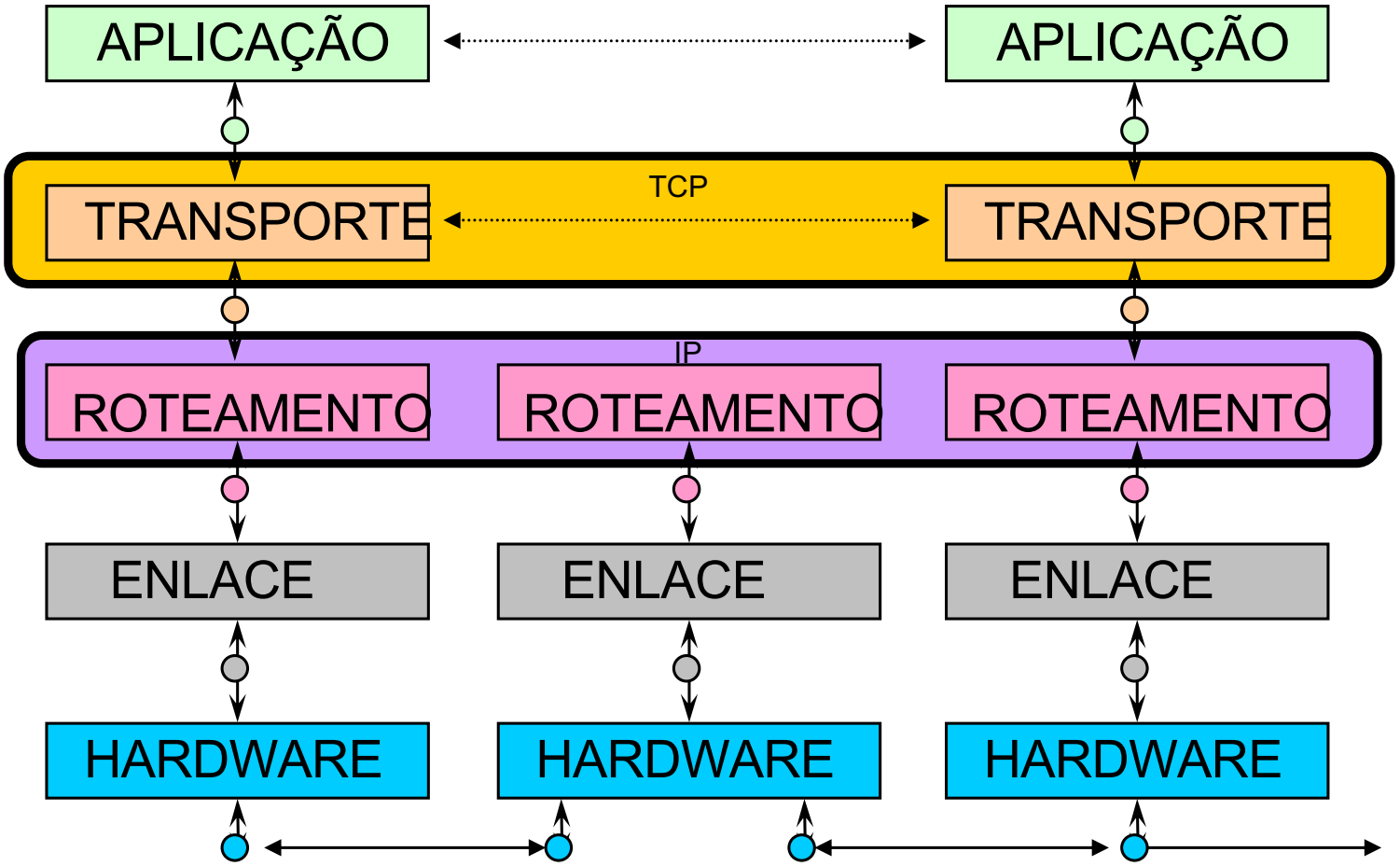


Se existirem duas rotas possíveis, apenas uma deverá estar na Tabela de Roteamento

Tabela de Roteamento do *Gateway* G1

Rede	Distância ou custo (métrica)	Próximo *Gateway* *(next hop)*
A	0	-
B	0	-
C	0	-
D	1	G2
E	1	G3
F	2	G3

Roteamento na camada IP



Tipos de Roteamento

- Estático - A tabela de roteamento é configurada de forma manual pelo operador
- Dinâmico - A tabela é dinâmicamente configurada, com informações trocadas entre os Roteadores

Comparação

- Estático - mais simples, suficiente para a maioria dos casos, porm se a tabela de rotas é muito complexa torna-se de dificil manutenção

- Dinâmico - mais complexo, indicado para roteadores fazendo a interconexão de diversas redes

Tabela de rotas estática

O roteador irá comparar o endereço IP desejado com as informações contida na tabela e enviará o pacote para o destino apropriado.

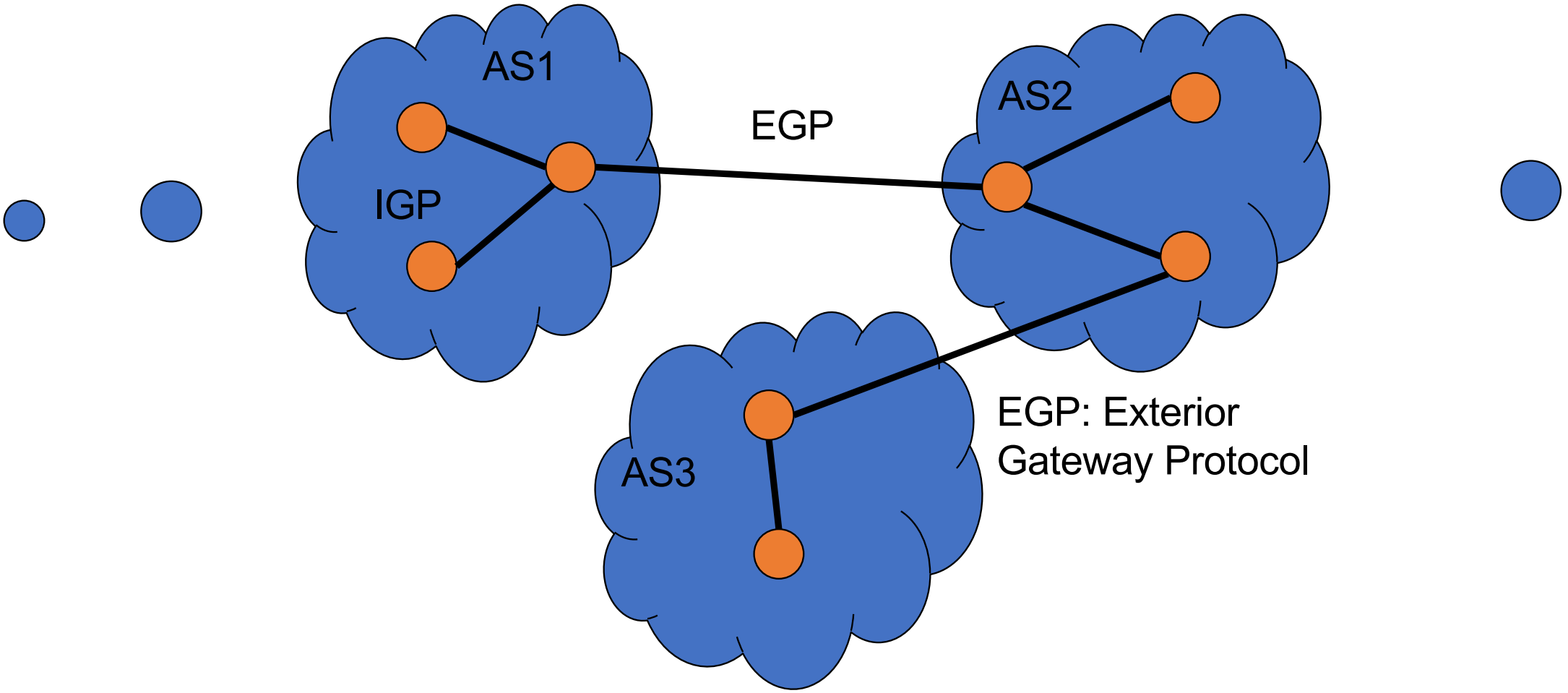
- Rede local : saída pela interface apropriada
- Rede Específica : envio para o *gateway* especificado
- Máquina específica : envio para o *gateway* especificado
- Rota padra : envio para o *gateway* padrão

O roteador só se preocupa com o próximo salto (*next hop*)

Roteamento Dinâmico

- o protocolo mais usado é o RIP (*Routing Information Protocol* - implementado pelo programa routed): os roteadores trocam informações entre si sobre as redes, as distâncias entre elas (métrica) e o próximo roteador para onde deve ser encaminhada a mensagem
- o RIP consome largura de banda, pois a cada 30 segundos os roteadores de cada rede fazem a difusão (*broadcast*) das atualizações do RIP
- o protocolo HELLO é semelhante porém utiliza o tempo como métrica ou invés do número de nós.
- o protocolo OSPF (*Open Shortest Path First*) é mais moderno e mais eficiente que o RIP porém exige um roteador com processador mais evoluído e com mais memória

Sistemas Autônomos (AS)



Protocolos Interiores e Exteriores

- IGP: *Interior Gateway Protocol* (RIP, Hello, OSPF)
- EGP: *Exterior Gateway Protocol* (GGP, BGP-Border Gateway Protocol)

Pacotes que não podem ser roteados

- isto acontece se a rede de destino não consta da tabela de roteamento de um dos roteadores
- o nó emissor se enganou e está tentando enviar uma mensagem para um endereço que não existe
- o roteador foi configurado de maneira errada e não possui informações sobre a rede destino
- todas as rotas para esta rede estão fora de funcionamento (um roteador distante do caminho apresentou defeito)
- a mensagem é interrompida e o usuário é avisado com uma mensagem: *Destination Unreachable*

ICMP - Internet Control Message Protocol

- Mensagens de Erro e Controle
- É encapsulada dentro de um datagrama IP, mas não é considerada um camada superior
- Pedido de echo: `ping`

ICMP -Tipo e Código

Tipo	
0	resposta de eco
3	destino inatingível
4	reduzir envio
5	redireciona (muda rota)
8	pedido de eco
11	tempo excedido (datagrama)
12	problema no parametrto (datagrama)
13	pedido de marca de tempo
14	resposta de marca de tempo
17	pedido de máscara de endereço
18	resposta de máscara de endereço

Código (Destino inatingível)	
0	rede inatingível
1	máquina inatingível
2	protocolo inatingível
3	porta inatingível
4	fragmentação necessária
5	falha na rota fornecida
6	rede destino desconhecida
7	máquina destino desconhecida
8	máquina fonte isolada
9	comunicação com rede destino proibidada administrativamente
11	comunicação com máquina destino proibidada administrativamente
12	máquina inatingível para tipo de serviço

Formato da mensagem ICMP