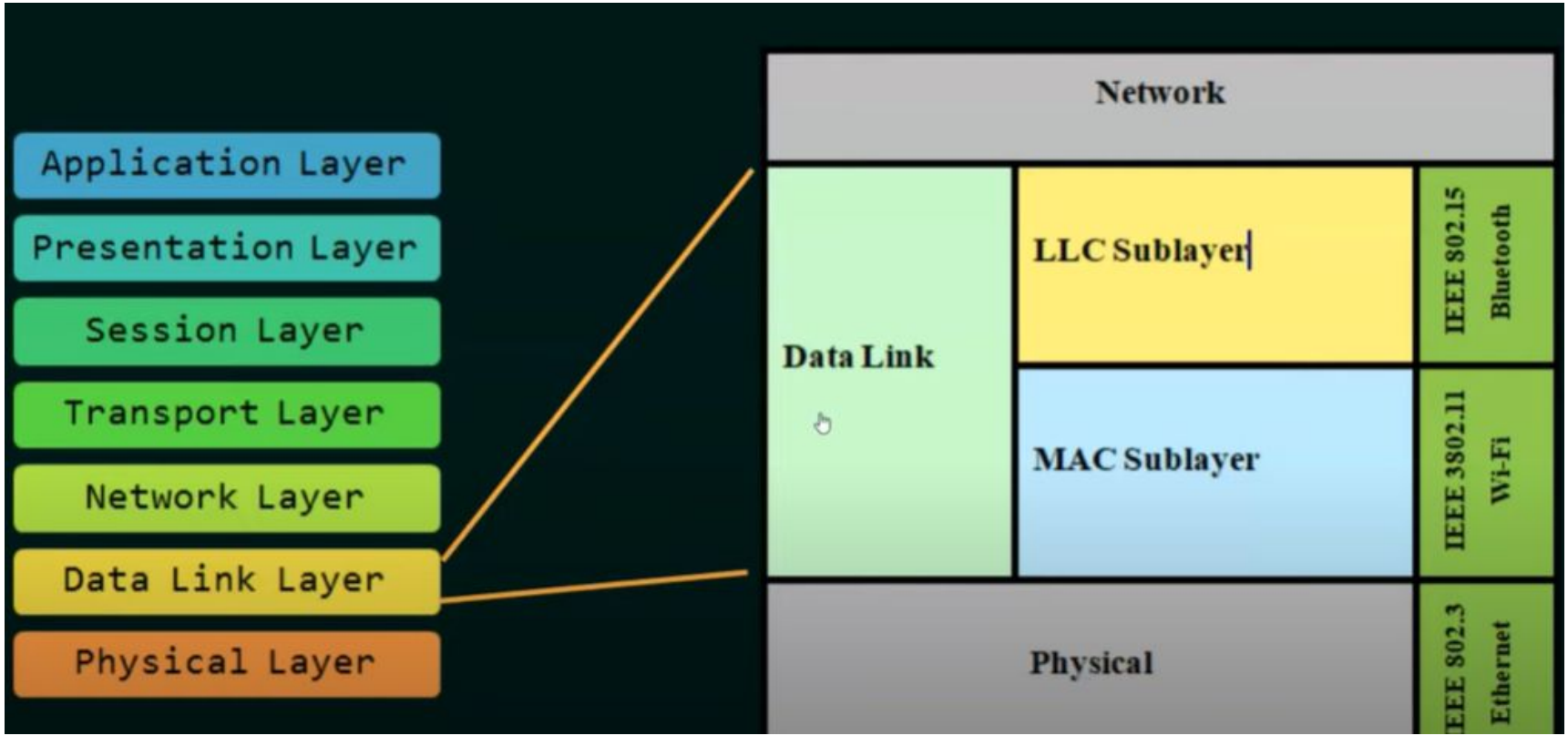
URI | UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES

30-764

Redes de Computadores I

MSc. Fernando Schubert

IMPLEMENTAÇÃO



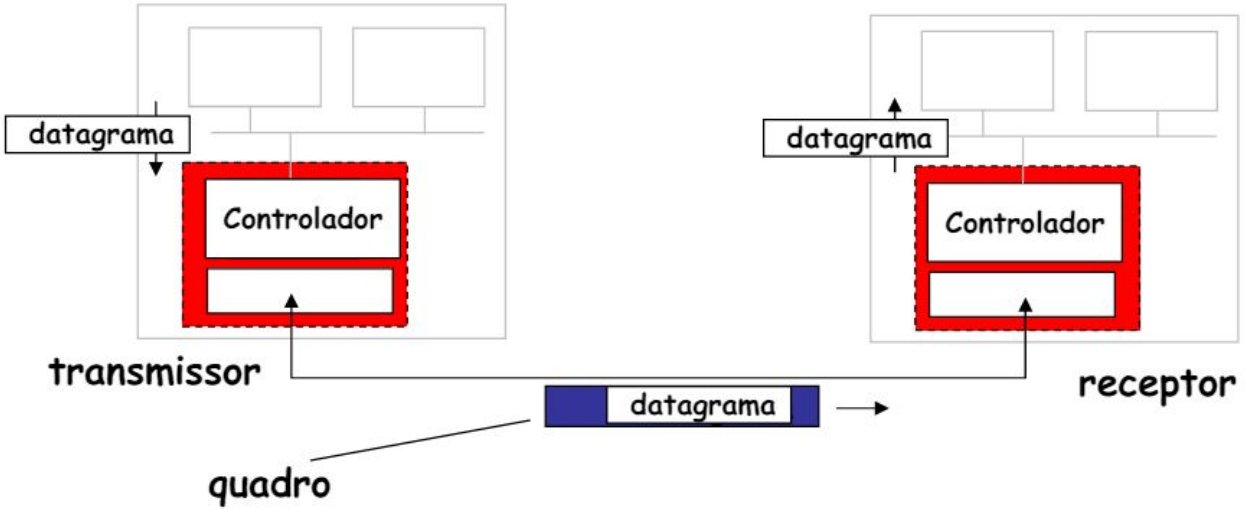
IMPLEMENTAÇÃO

- Sub-camadas da camada de enlace:
  - Logical link control (LLC) - controle lógico do enlace
    - Gerencia a comunicação entre as camadas superiores e inferiores
    - Adiciona informações de controle de fluxo aos dados recebidos da camada de rede
  - Medium access control (MAC) - controle de acesso ao meio
    - Constitui-se na sub-camada mais baixa da camada de enlace
    - Geralmente desenvolvida em hardware, junto à placa de rede
    - Responsabilidades:
      - Encapsulamento dos dados
      - Controle de acesso ao meio

IMPLEMENTAÇÃO

- A camada de enlace é implementada por cada um dos nós da rede
  - Cada um pode implementar uma tecnologia
- É implementada no “adaptador” (Network Interface Card - NIC)
  - Exs: placa Ethernet, cartão PCMCIA, cartão 802.11
  - Também implementa a camada física
  - Está conectado ao barramento de sistema do nó
  - Ou integrada na placa mãe – É uma combinação de hardware, software e firmware

COMUNICAÇÃO ENTRE ADAPTADORES



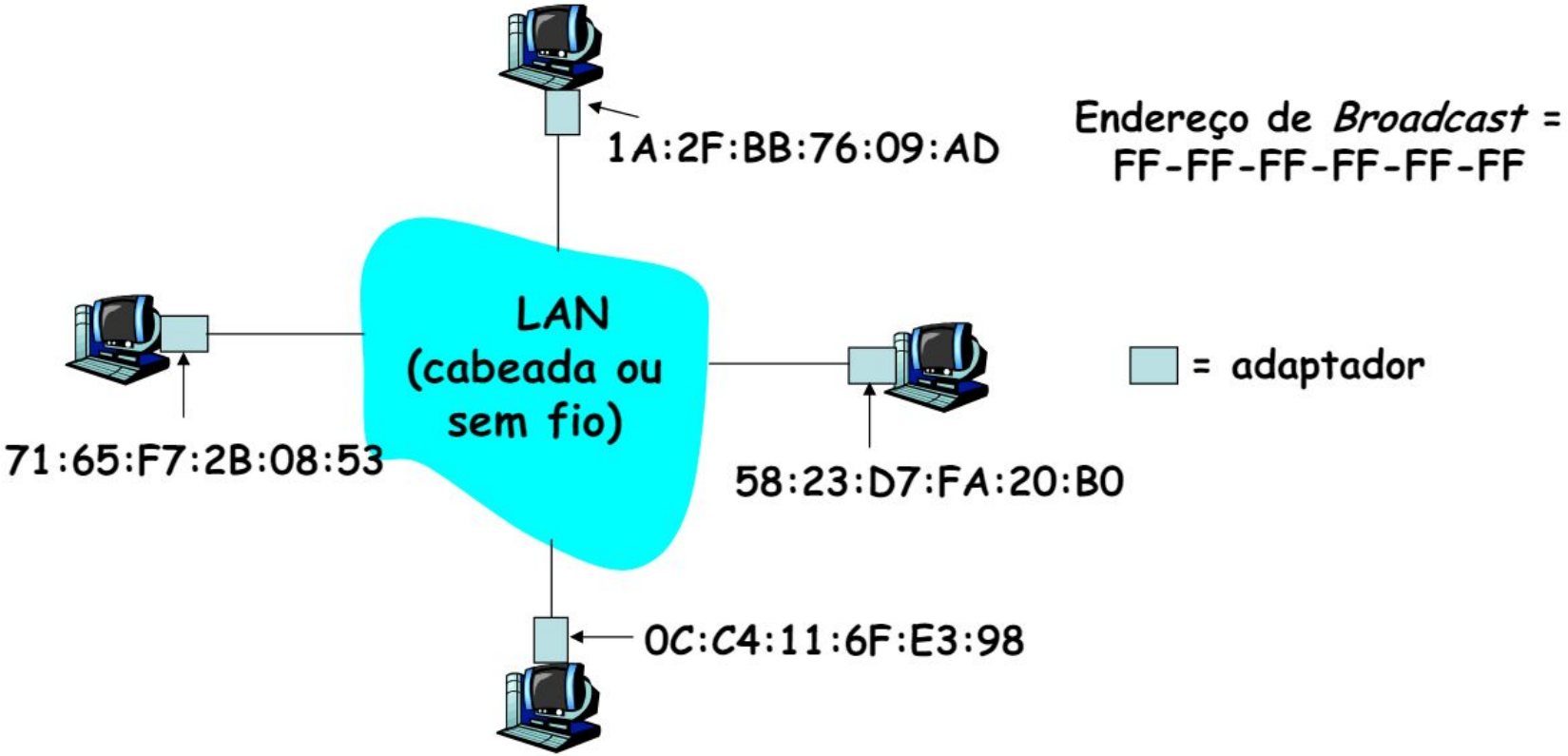
Lado transmissor
Encapsula o datagrama em um quadro
Adiciona bits de verificação de erro, transferência confiável de dados, controle de fluxo, etc.

Lado receptor
Verifica erros, transporte confiável, controle de fluxo, etc.
Extrai o datagrama, passa para o nó receptor

ENDEREÇAMENTO MAC

- MAC - Medium Access Control
- Endereço IP de 32 bits
  - Endereços da camada de rede
  - Usado para levar o datagrama à sub-rede IP destino
- Endereço MAC (ou LAN, ou físico, ou Ethernet)
  - Leva o datagrama de uma interface até outra interface conectada fisicamente (na mesma rede)
  - Possui 48 bits (para a maioria das redes)
  - Representados por 12 dígitos hexadecimais agrupados 2 a 2 (Ex.: 1A:2F:BB:76:09:AD)
  - Gravado na ROM do adaptador ou configurado por software

ENDEREÇAMENTO MAC



ENDEREÇAMENTO MAC

- Alocação de endereços MAC gerenciada pelo IEEE
- Um fabricante compra uma parte do espaço de endereços
  - Garantia de unicidade
- Analogia:
  - Endereço MAC
    - Como número do CPF
  - Endereço IP
    - Como endereço postal (CEP)

ENDEREÇAMENTO MAC

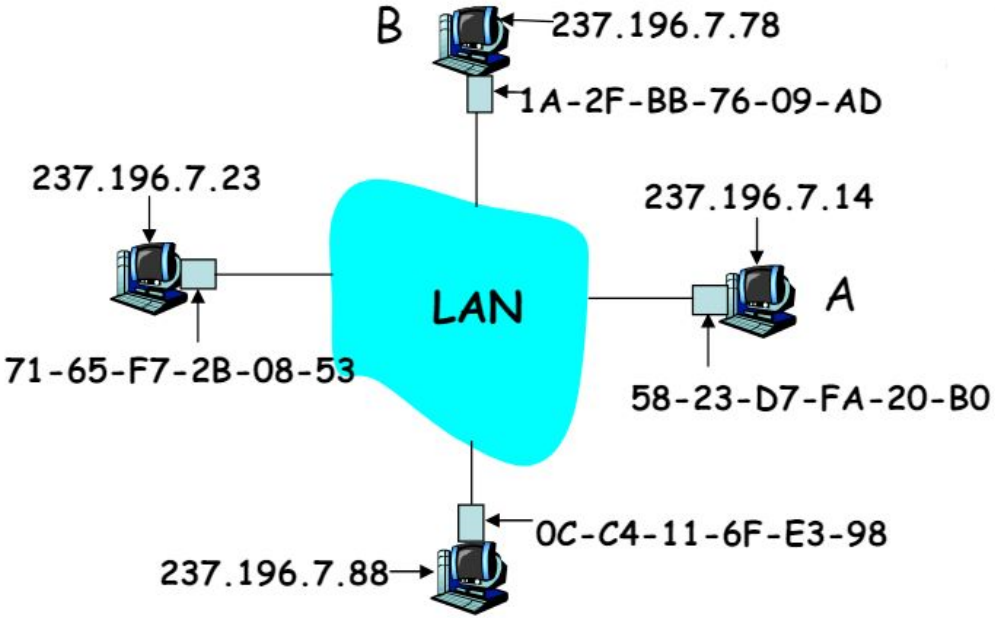
- Endereço MAC tem estrutura linear
  - Portabilidade
    - É possível mover um cartão LAN de uma LAN para outra

- Endereço IP hierárquico NÃO é portátil
  - Requer IP móvel, por exemplo
  - Depende da sub-rede IP à qual o nó está conectado

PROTOCOLO ARP

- Protocolo de resolução de endereços (Address Resolution Protocol)
  - Descrito na RFC 826
- Faz a tradução de endereços IP para endereços MAC da maioria das redes IEEE 802
- Executado dentro da sub-rede
  - Cada nó (estação ou roteador) possui uma tabela ARP
  - Contém endereço IP, endereço MAC e TTL
  - Tabela ARP construída automaticamente

PROTOCOLO ARP



- Cada nó de uma LAN possui uma tabela ARP
- Tabela ARP: mapeamento de endereços IP/MAC para alguns nós da LAN
- TTL (Time To Live): tempo a partir do qual o mapeamento de endereços será esquecido (valor típico de 20 min)

PROTOCOLO ARP

- Funcionamento na mesma rede LAN
  - A deseja enviar datagrama para B, mas o endereço MAC de B não está na tabela ARP
  - Para descobrir o endereço MAC de B, A difunde um pacote de solicitação ARP com o endereço IP de B
    - Endereço MAC destino = FF-FF-FF-FF-FF-FF
    - Todas as máquinas na LAN recebem a consulta do ARP
  - B então recebe o pacote ARP com a solicitação e responde a A com o seu endereço MAC
    - Quadro de resposta é enviado para o endereço MAC (unicast) de A

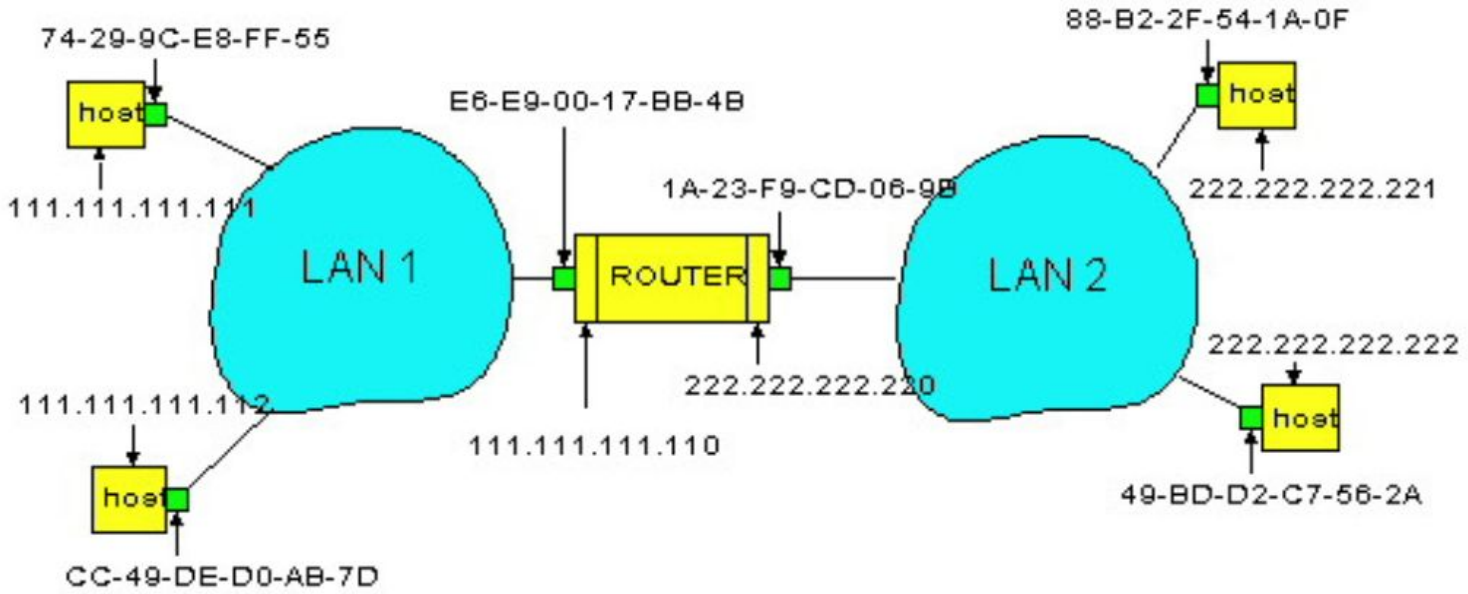
PROTOCOLO ARP

- Funcionamento na mesma rede LAN
  - Um cache (salva) o par de endereços IP-para-MAC na sua tabela ARP até que a informação expire
    - É “soft state”
      - Informação que expira a menos que seja renovada
    - Um nó pode responder a uma requisição com um endereço MAC que conheça
      - Não necessariamente o próprio nó de destino
    - ARP é “plug-and-play”
      - Os nós criam suas tabelas ARP sem a intervenção do administrador da rede

PROTOCOLO ARP

- Funcionamento entre redes diferentes:
  - Envio de datagrama de A para B através de R
  - O Roteador R possui duas tabelas ARP
  - Uma para cada rede local

PROTOCOLO ARP



PROTOCOLO ARP

- Funcionamento entre redes diferentes:
  - A cria o datagrama com endereço IP de fonte A e de destino B
  - A consulta a tabela de roteamento e obtém R como próximo salto
  - A usa o ARP para obter o endereço MAC de R
  - A cria um quadro com endereço MAC de destino R e o datagrama de A para B na carga útil
  - Adaptador de A envia o quadro para R
  - Adaptador de R recebe o quadro

PROTOCOLO ARP

- Funcionamento entre redes diferentes:
  - R remove o datagrama IP do quadro Ethernet e verifica que é destinado a B
  - R consulta a tabela de roteamento • R usa o ARP para obter o endereço MAC de B • R cria o quadro contendo o datagrama de A para B • Adaptador de R envia o quadro para B • Adaptador de B recebe o quadro

PROTOCOLO ARP

- Ferramentas arp

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

Interface: 192.168.100.149 --- 0xb
  Internet Address      Physical Address      Type
  192.168.100.1         18-3c-b7-10-19-dd     dynamic
  192.168.100.119       40-aa-56-00-6f-11     dynamic
  192.168.100.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.60            01-00-5e-00-01-3c     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  239.255.255.255       01-00-5e-7f-ff-ff     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

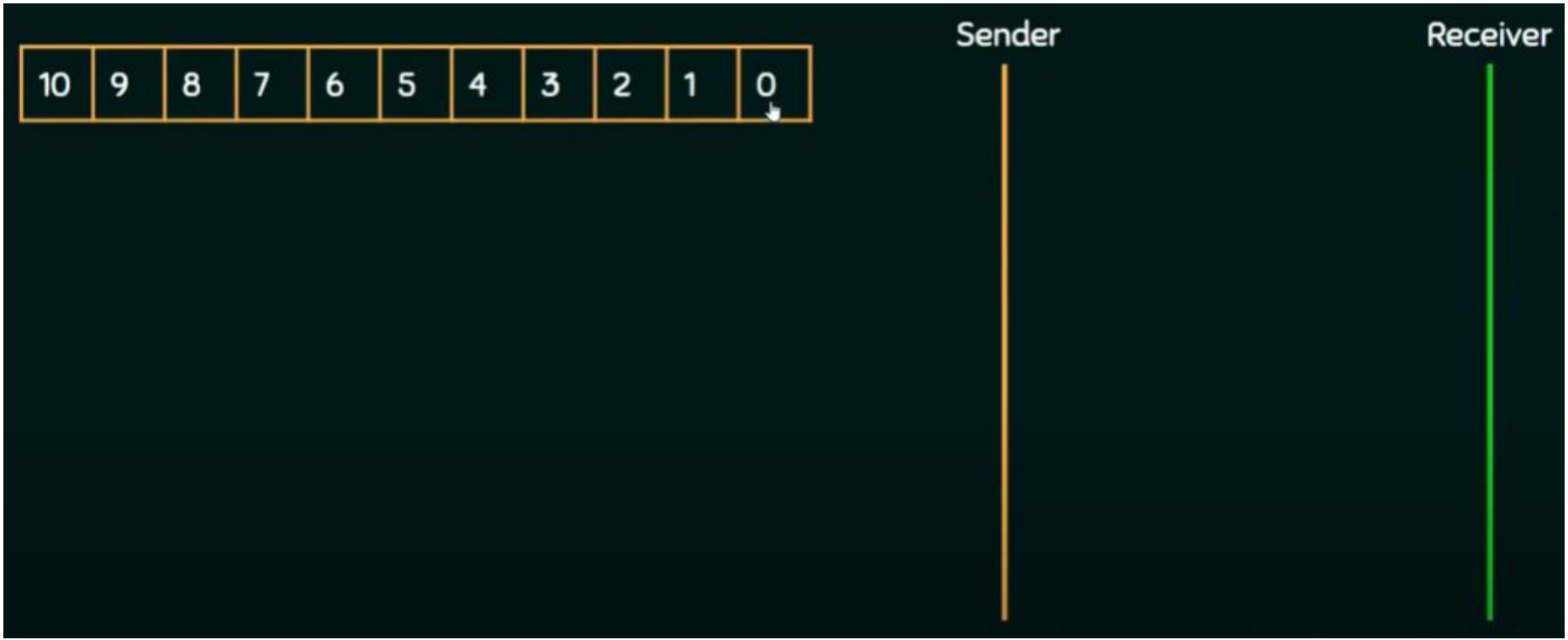
PROTOCOLOS DE ENLACE

- Tipos diferentes de canais de comunicação:
  - Canal ponto-a-ponto
    - Uma estação em cada extremidade
    - Requer controle simples de acesso
    - Exs.: redes entre roteadores
  - Canal de difusão (broadcast)
    - Várias estações conectadas ao mesmo canal
    - Requer controle de acesso ao meio para coordenar as transmissões
    - Ex. rede sem-fio

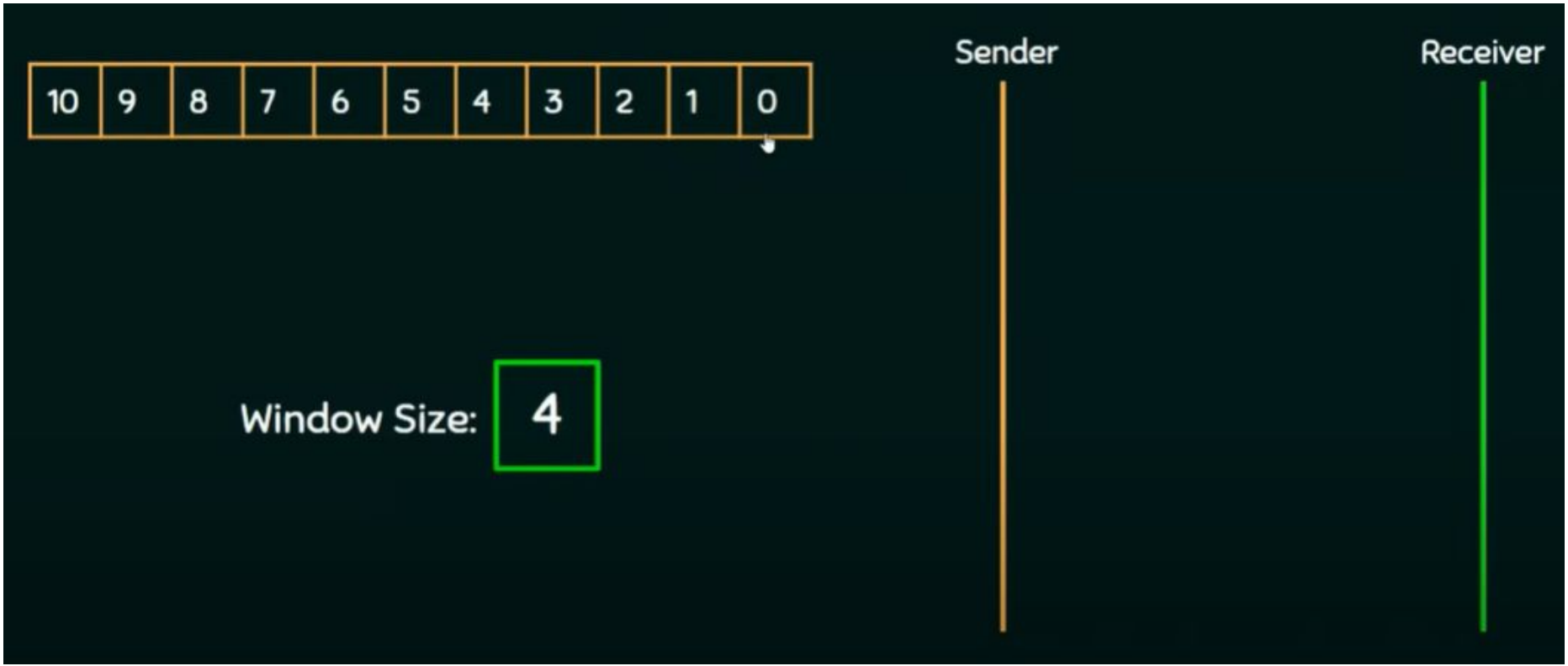
PROTOCOLOS DE JANELA DESLIZANTE

- Envia vários frames (quadros) ao mesmo tempo
- Número de quadros baseados no tamanho da janela
- Enviam quadros identificados por números de sequência
  - Pode variar de 0 até um valor máximo
    - Valor máximo = 2n – 1, onde n é o número de bits
- Transmissores mantêm um conjunto de números de sequência relacionados a quadros que ele pode enviar
  - Quadros pertencem à janela de transmissão
- Receptores também mantêm um conjunto de números de sequência relacionados a quadros que pode aceitar
  - Quadros pertencem à janela de recepção

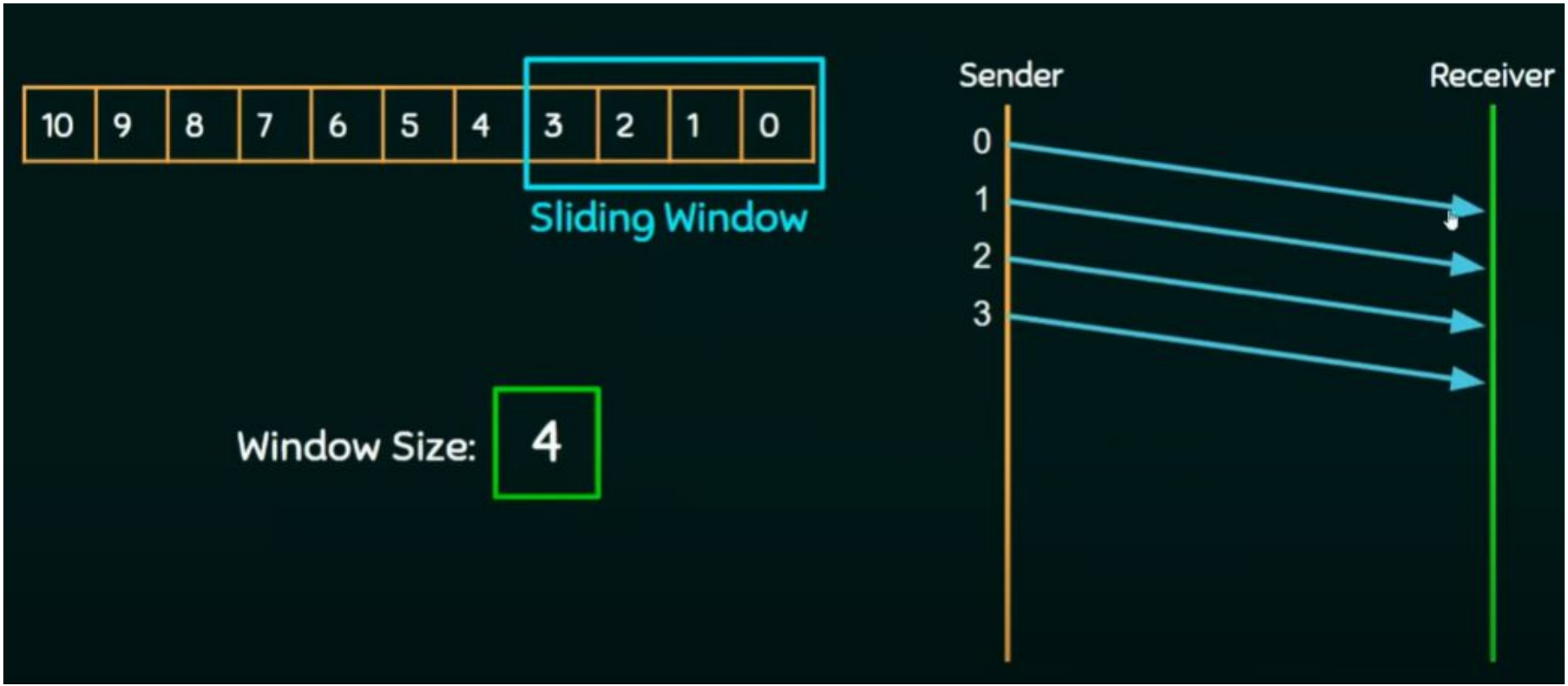
PROTOCOLOS DE JANELA DESLIZANTE



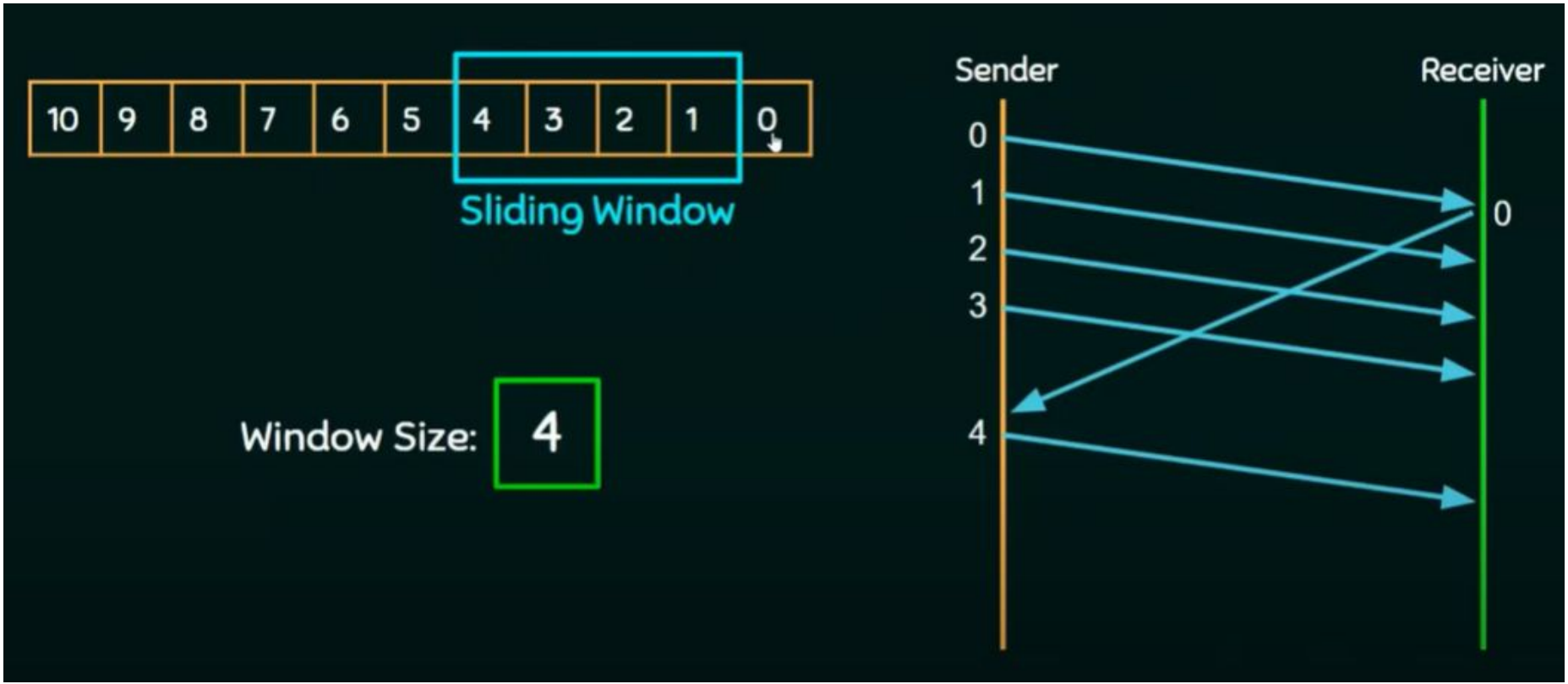
PROTOCOLOS DE JANELA DESLIZANTE



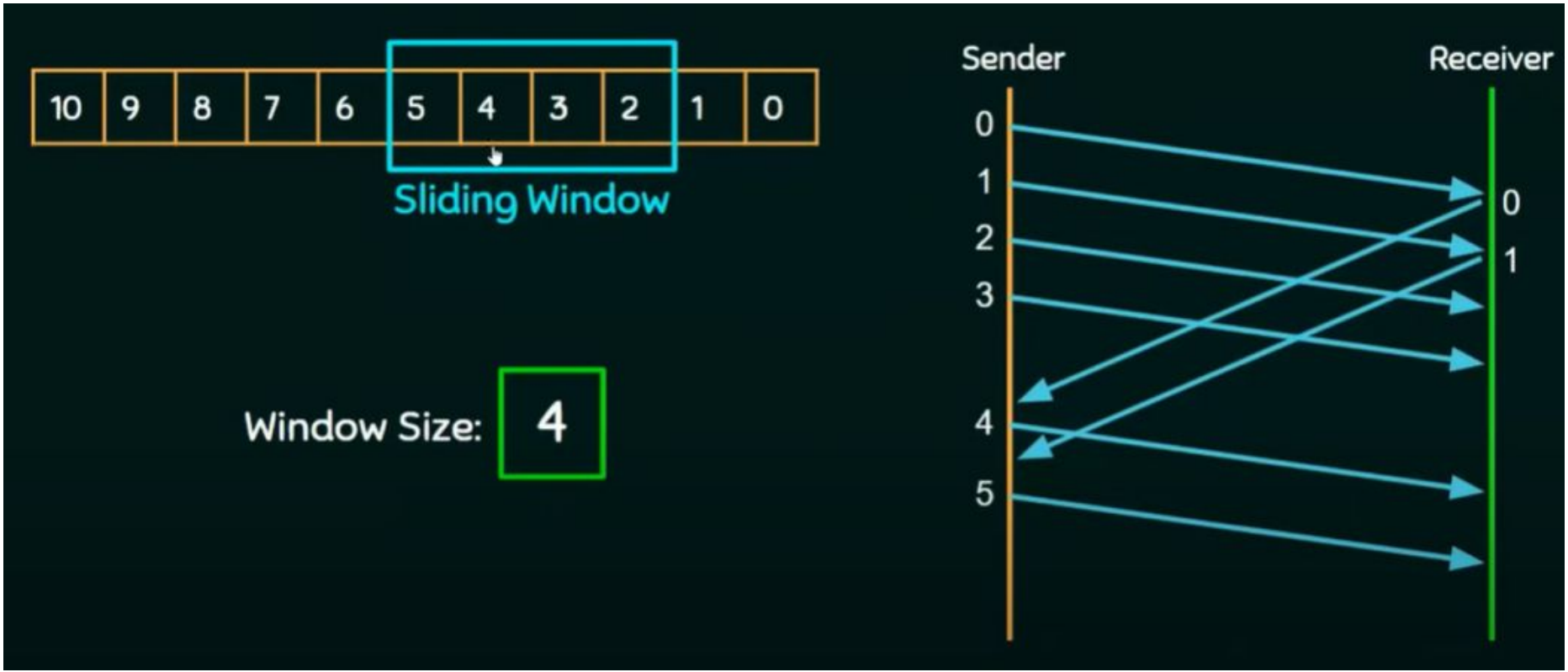
PROTOCOLOS DE JANELA DESLIZANTE



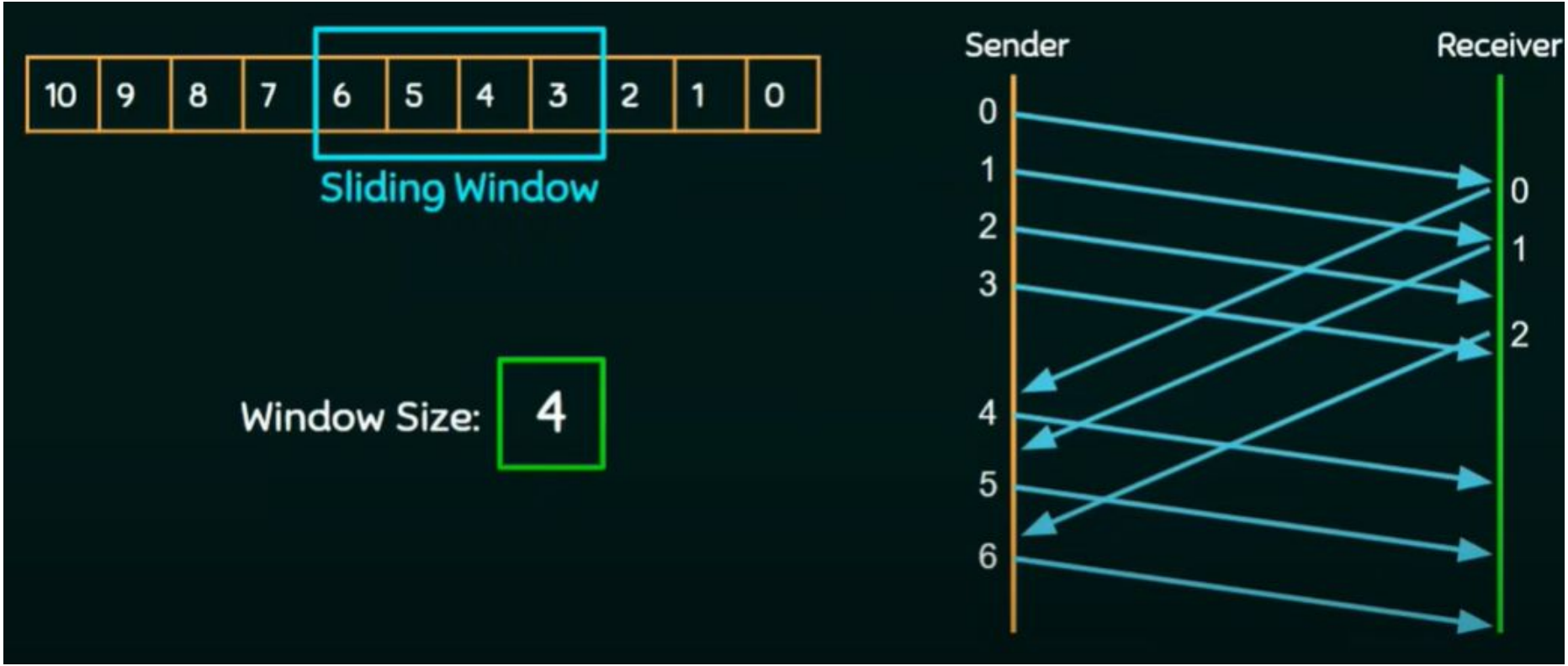
PROTOCOLOS DE JANELA DESLIZANTE



PROTOCOLOS DE JANELA DESLIZANTE

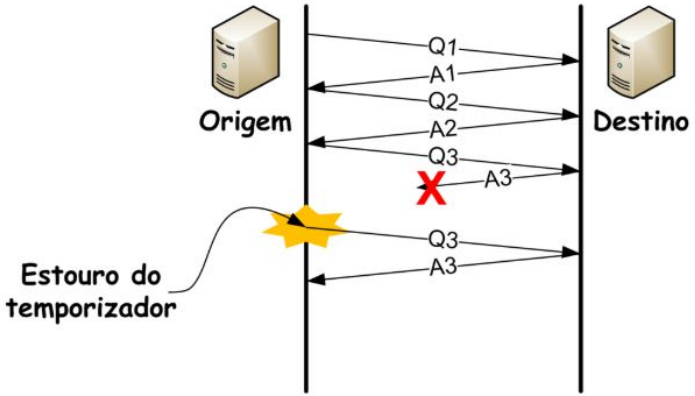


PROTOCOLOS DE JANELA DESLIZANTE



PROTOCOLO PARE E ESPERE (STOP AND WAIT)

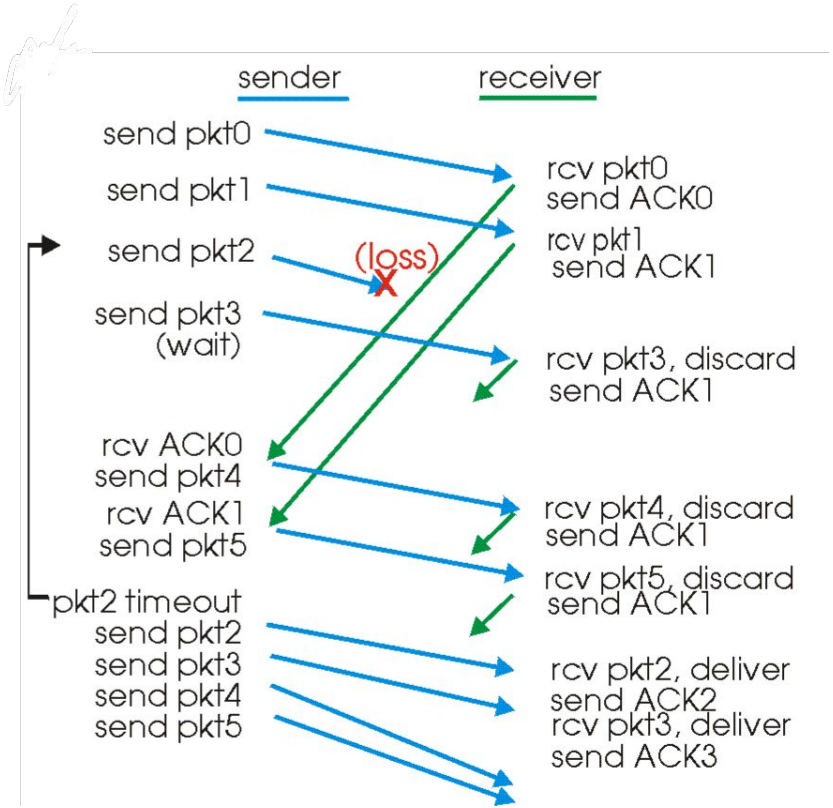
- Transmissor só pode enviar um quadro por vez
- Janela de transmissão e de recepção são iguais a 1
  - Próximo quadro só pode ser transmitido após a recepção do reconhecimento positivo (ACK) do atual



PROTOCOLO GO BACK N

- Go Back N
  - Transmissor pode enviar até N pacotes não reconhecidos (“em trânsito”)
    - Janelas de transmissão e de recepção são iguais a N
  - Receptor envia apenas ACKs cumulativos
    - Não reconhece pacote se houver falha de sequência
  - Transmissor possui um temporizador para o pacote mais antigo ainda não reconhecido
    - Se o temporizador estourar, retransmite todos os pacotes ainda não reconhecidos

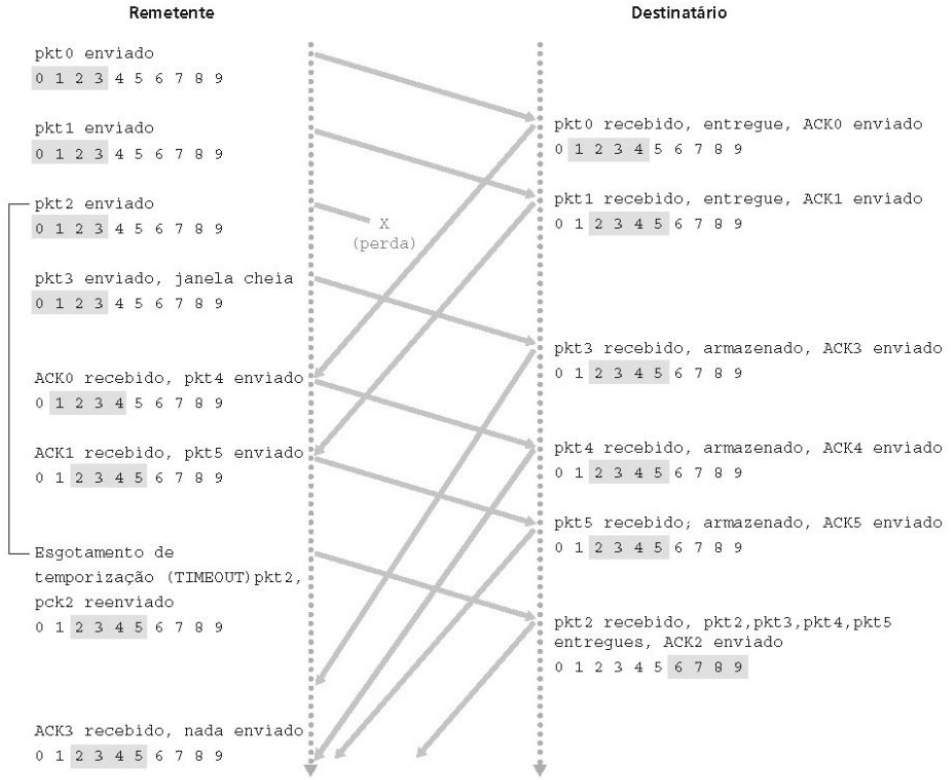
PROTOCOLO GO BACK N



PROTOCOLO DE RETRANSMISSÃO SELETIVA

- Receptor reconhece individualmente todos os pacotes recebidos corretamente
  - Armazena pacotes no buffer, conforme necessário, para posterior entrega ordenada à camada superior
- Transmissor apenas reenvia pacotes para os quais um ACK não foi recebido
  - Temporizador no remetente para cada pacote sem ACK
- Janela de transmissão
  - N números de sequência consecutivos
  - Outra vez limita números de sequência de pacotes enviados, mas ainda não reconhecidos

PROTOCOLO DE RETRANSMISSÃO SELETIVA



PIGGYBACKING

- Seja o seguinte protocolo ponto-a-ponto entre entidades A e B:
  - Usa confirmação
  - A transmissão de dados é full-duplex
  - É possível embutir numa PDU de dados enviada de B para A a confirmação de uma PDU de dados enviada de A para B já recebida (o mesmo para o caso contrário)
- Isto é conhecido como confirmação na carona ou Piggyback

PIGGYBACKING

- Melhor utilização do canal
- Utiliza apenas alguns bits ao contrário de uma PDU de controle
- Menos PDUs a processar
- Possivelmente menos buffers no RX
- Se não há uma PDU para ser enviada de B A, quanto tempo deve-se esperar para confirmar uma PDU já enviada e recebida de A B

PROTOCOLOS PONTO-A-PONTO

- Canal ponto-a-ponto
  - Um transmissor, um receptor, um canal
- Mais fácil que um canal de difusão
  - Sem controle de acesso ao meio (MAC)
  - Sem necessidade de endereçamento MAC explícito
  - Entretanto, precisa de enquadramento, controle de fluxo, detecção e correção de erro etc.
- Ex.: canal discado, canal ISDN/RDSI
- Protocolos: HDLC e PPP

PROTOCOLO HDLC

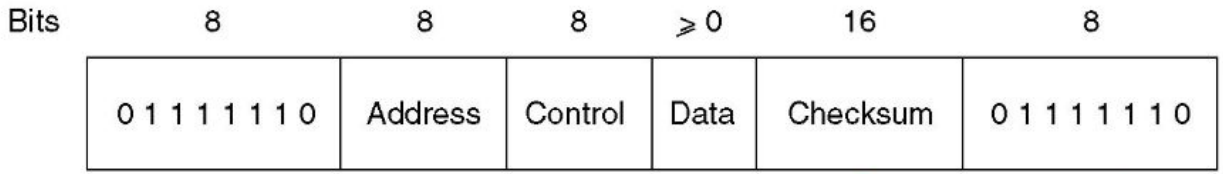
- Controle de enlace de dados de alto nível (High-level Data Link Control)
  - Enquadramento e detecção de erros
  - Usado no X.25
- Orientado a conexão
- Orientado a bits
  - Não se preocupam com o número de bytes do quadro

PROTOCOLO HDLC

- Usa a técnica de inserção de bits
  - Evita que sequências de delimitação de quadros apareçam no campo de informação
- Usa um protocolo de janela deslizante do tipo GoBack-N ou Retransmissão Seletiva
  - Semelhante aos mecanismos do TCP

PROTOCOLO HDLC - ENQUADRAMENTO

- Flags inicial e final: Sequência 01111110
- Endereço
- Controle
  - Números de sequência, confirmações, outros
- Dados
  - Sem limite de tamanho
- Verificação
  - Variação do CRC

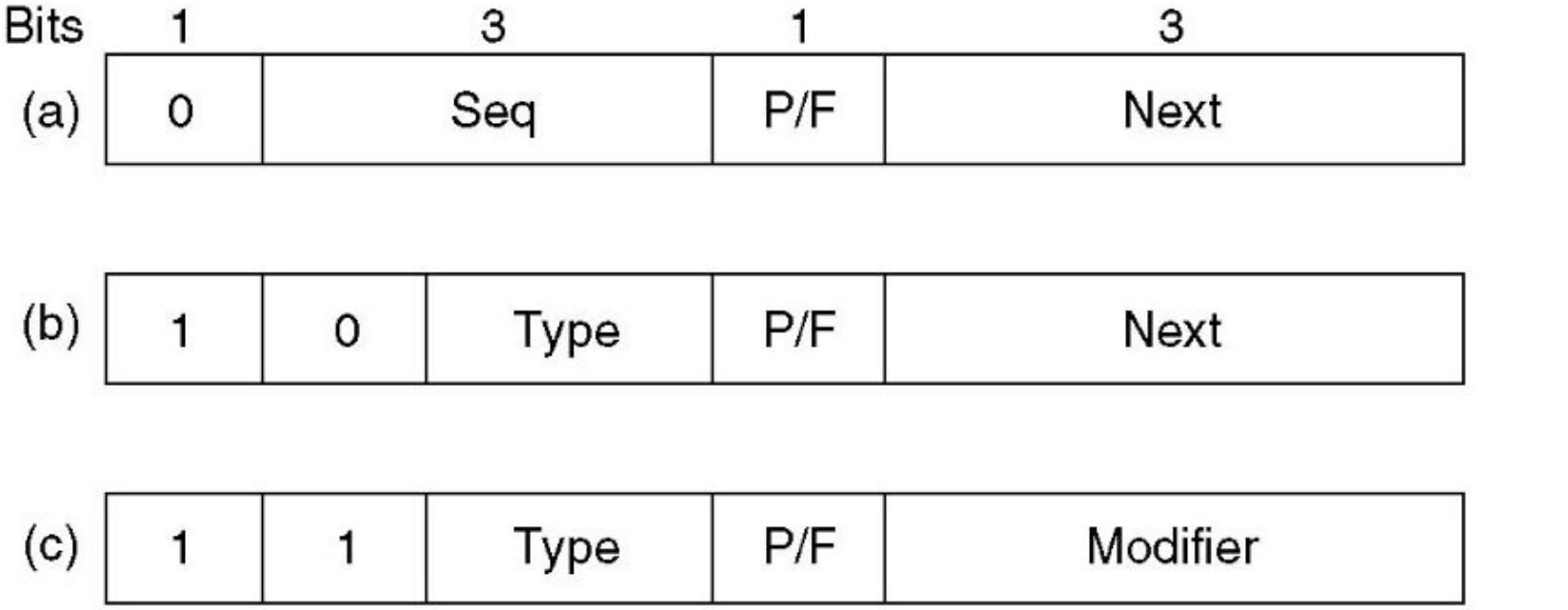


Fonte: Tanenbaum

PROTOCOLO HDLC - TIPOS DE QUADROS

- Três tipos
  - Informação
    - Dados
  - Supervisor
    - Controle de fluxo ou de erro, quando não é possível fazer piggyback no quadro de dados
  - Não-numerado
    - Vários propósitos, inclusive para envio de dados ou controle
- Tipos de quadros se diferenciam no campo controle

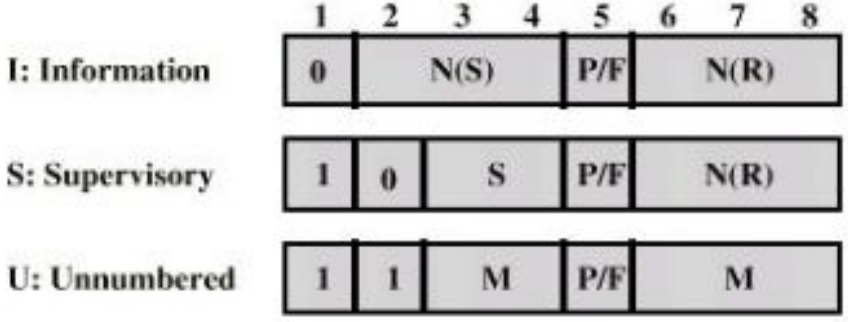
PROTOCOLO HDLC - TIPOS DE QUADROS



(a) Informação (b) Supervisor (c) Não-numerado

PROTOCOLO HDLC - TIPOS DE QUADROS

FORMATO CAMPO DE CONTROLE - 8 BITS:



N(S) - # sequência "sender"
N(R) - # sequência "receiver"
S - bits de supervisão
M - bits não-numerado
P/S- Poll/Final Bit

P/F (**Normal Response Mode**) = ***Poll bit*** para **comandos** (primário) e ***Final bit*** para **respostas** (P/F=1 indica que a S_i envia último quadro I).

P/F (**Asynchronous Balanced Mode**) = A estação transmissora solicita um RR com P/F=1, quando não recebe resposta da receptora.

Neste caso, a receptora deve enviar uma resposta, com P/F=1 também

Evita a retransmissão de vários quadros, quando o ACK foi perdido.

PROTOCOLO PPP

- Protocolo Ponto-a-Ponto (Point-to-Point Protocol)
- Protocolo de enlace usado em linhas ponto-a-ponto na Internet
  - Mais simples que o HDLC
    - Orientado a caracteres e não a bits como o HDLC
    - Usado frequentemente em:
      - Conexões de linhas privadas entre roteadores
      - Conexões de acesso entre estações de usuários domiciliares e roteadores
- Definido nas RFCs 1661 a 1663 e em outros

PROTOCOLO PPP

- Usa a técnica de inserção de bytes de flags em linhas de discagem por modem
- PPP pode usar linhas SONET, linhas HDLC orientadas a bits, circuitos RDSI e outros
- Possui dois modos de transmissão
  - Não confiável
    - Sem números de sequência e confirmações
    - Confiável
      - Raramente usado

PROTOCOLO PPP

- Possui três funções principais
  - 1. Enquadramento e detecção de erros
  - 2. Ativação, teste, negociação e desativação de linhas
    - Através do protocolo de controle de enlace (Link Control Protocol - LCP)
      - Ex.: negociação da taxa de transmissão, tamanho máximo da carga útil
  - 3. Negociação de opções da camada rede independente do protocolo de rede utilizado
    - Através do protocolo de controle de rede (Network Control Protocol - NCP)
      - Ex.: definição de endereços IP

PROTOCOLO PPP

- Possui três funções principais
  - 1. Enquadramento e detecção de erros
  - 2. Ativação, teste, negociação e desativação de linhas
    - Através do protocolo de controle de enlace (Link Control Protocol - LCP)
      - Ex.: negociação da taxa de transmissão, tamanho máximo da carga útil
  - 3. Negociação de opções da camada rede independente do protocolo de rede utilizado
    - Através do protocolo de controle de rede (Network Control Protocol - NCP)
      - Ex.: definição de endereços IP

PPP - REQUISITOS DO PROJETO

- Detecção de erro
- Vida da conexão
  - Detecta, indica falhas do enlace para a camada de rede
- Negociação do endereço da camada de rede
  - Pontos terminais podem aprender/configurar o endereço de rede do outro

PPP - REQUISITOS DO PROJETO

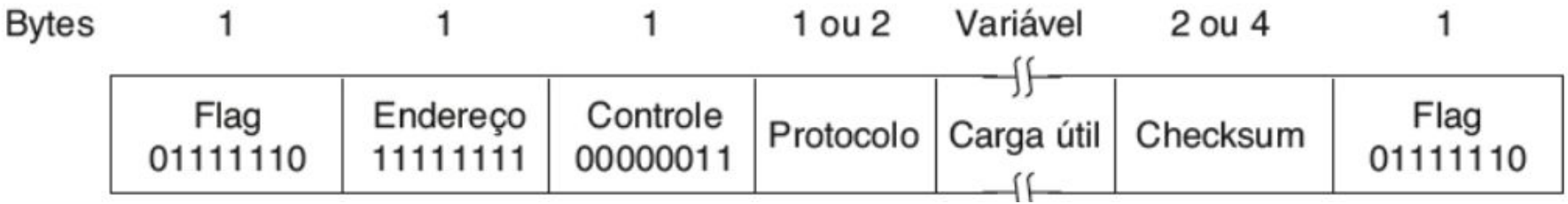
- Enquadramento do pacote
  - Encapsula datagramas da camada de rede em quadro da camada de enlace
  - Transporta dados da camada de rede de qualquer protocolo de camada de rede (não apenas do IP), simultaneamente
- Transparência
  - Transporta qualquer padrão de bits no campo de dados
- Múltiplos protocolos de rede e tipos de enlace

PPP - REQUISITOS DO PROJETO

- Ser o mais simples possível
  - Não faz correção/recuperação de erros
  - Sem controle de fluxo
  - Sem controle de sequenciamento
  - Sem necessidade de dar suporte a canais de difusão
- Recuperação de erros, controle de fluxo e reordenamento dos dados foram deixados para camadas superiores...

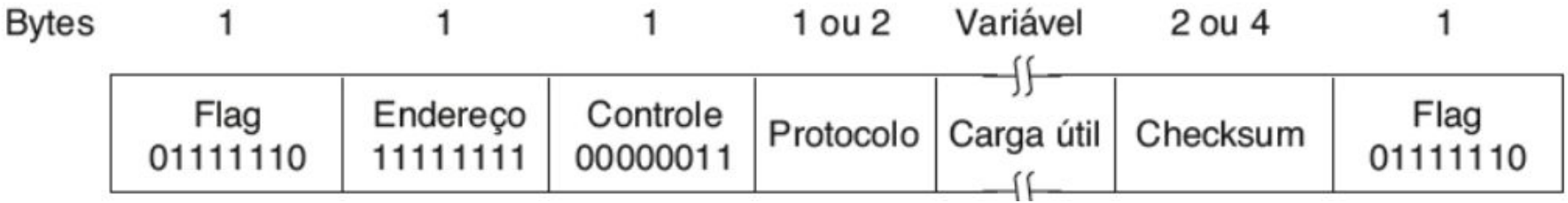
PPP - FORMATO DO QUADRO

- Flags inicial e final: Sequência 01111110
- Endereço
  - O único valor é o 11111111
    - Todas as estações aceitam esse endereço
- Controle
  - Para quadros não numerados é 00000011



PPP - FORMATO DO QUADRO

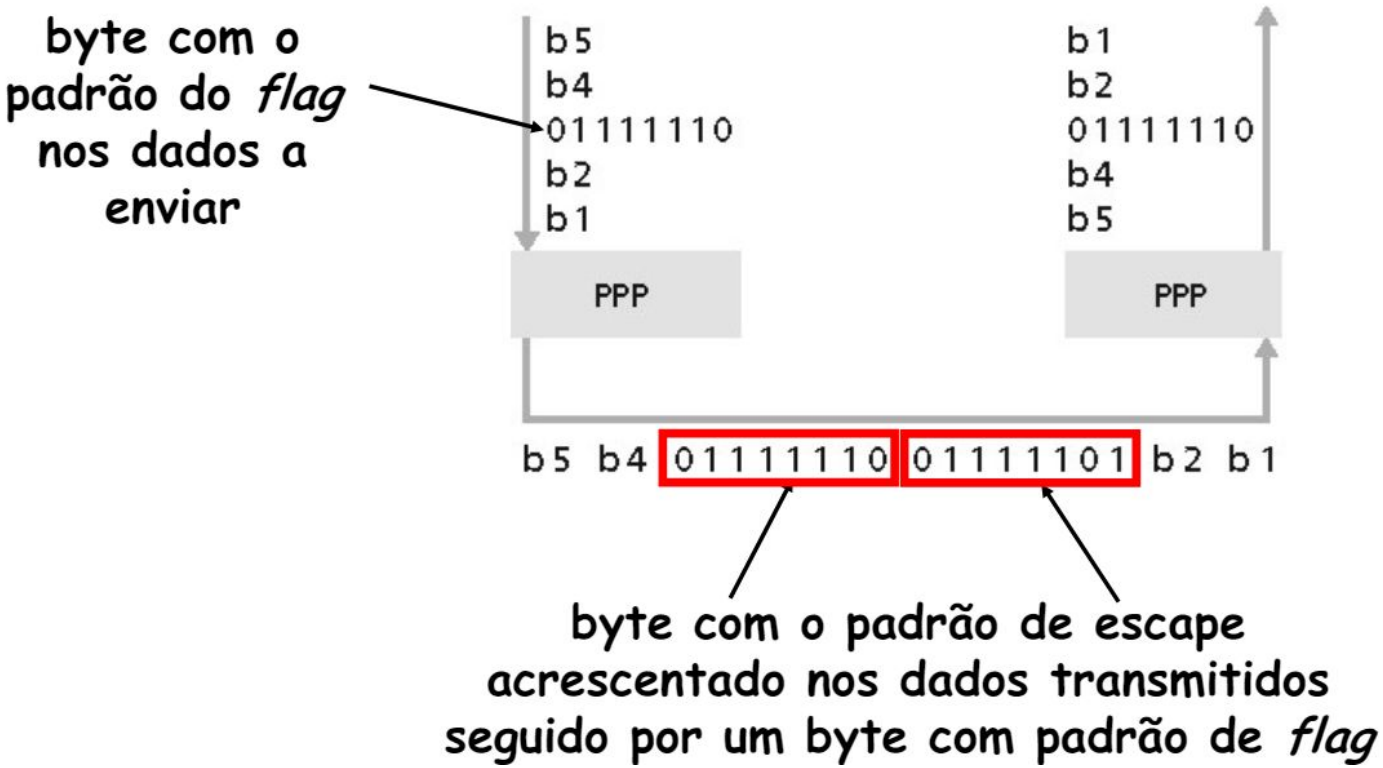
- Protocolo
  - Tipo de pacote da carga útil (ex., o protocolo IP)
- Carga útil
  - Possui um tamanho máximo negociado (LCP)
  - Padrão é 1500 octetos
  - Byte de escape é 01111101 (problema da sequência do flag no meio do quadro)
- Verificação: CRC



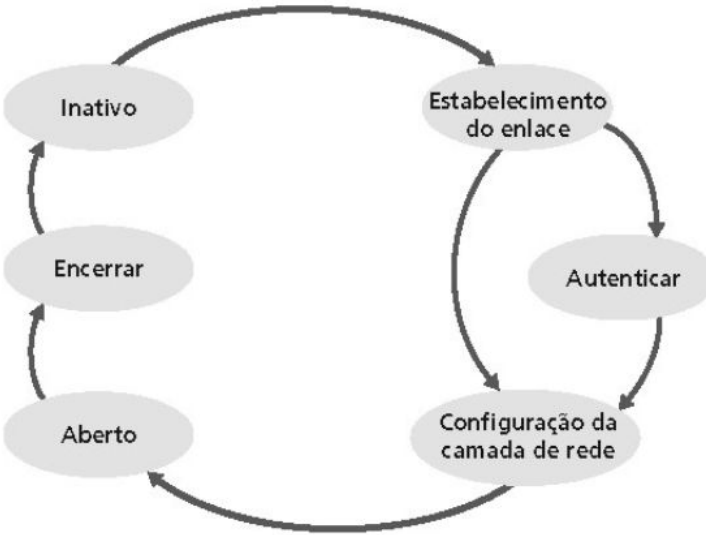
PPP - ENCHIMENTO (BYTE STUFFING)

- Requisito de “transparência dos dados”
  - Carga útil pode conter o padrão do flag 01111110
  - Se um 01111110 for recebido, ele é dados ou flag
- Transmissor
  - Adiciona (“enche”) um byte de controle de escape 01111101 antes de cada byte 01111110 de dados
  - Receptor
    - Se encontrar um 01111110 precedido de um 01111101
  - Descarta o primeiro byte e continua a recepção dos dados
- Se houver apenas um único 01111110 byte de flag

PPP - ENCHIMENTO (BYTE STUFFING)

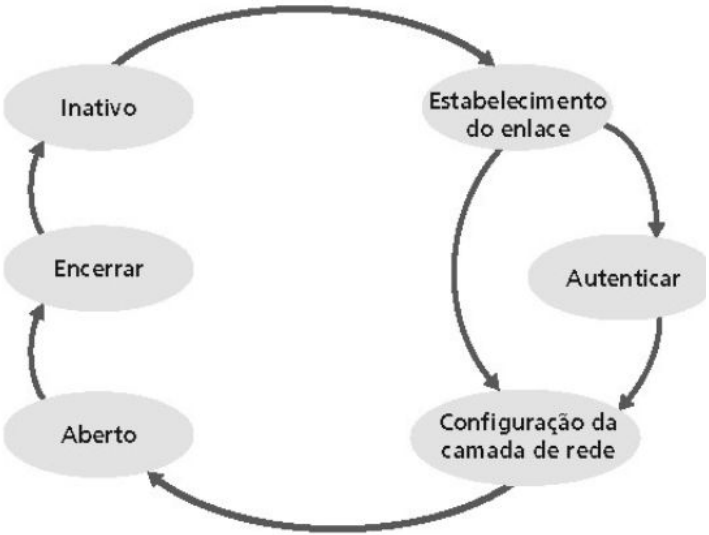


PPP - FUNCIONAMENTO



- Antes de trocar dados da camada de rede, os parceiros do enlace de dados devem…
    1. Configurar o enlace PPP
        Compr. máx. quadro, etc.
        Autenticação
    2. Obter/configurar informações da camada de rede
        Para IP: transporta mensagens do Protocolo de Controle IP (IPCP) para configurar/obter o endereço IP
    3. Aberto
        Transporta dados

PPP - FUNCIONAMENTO

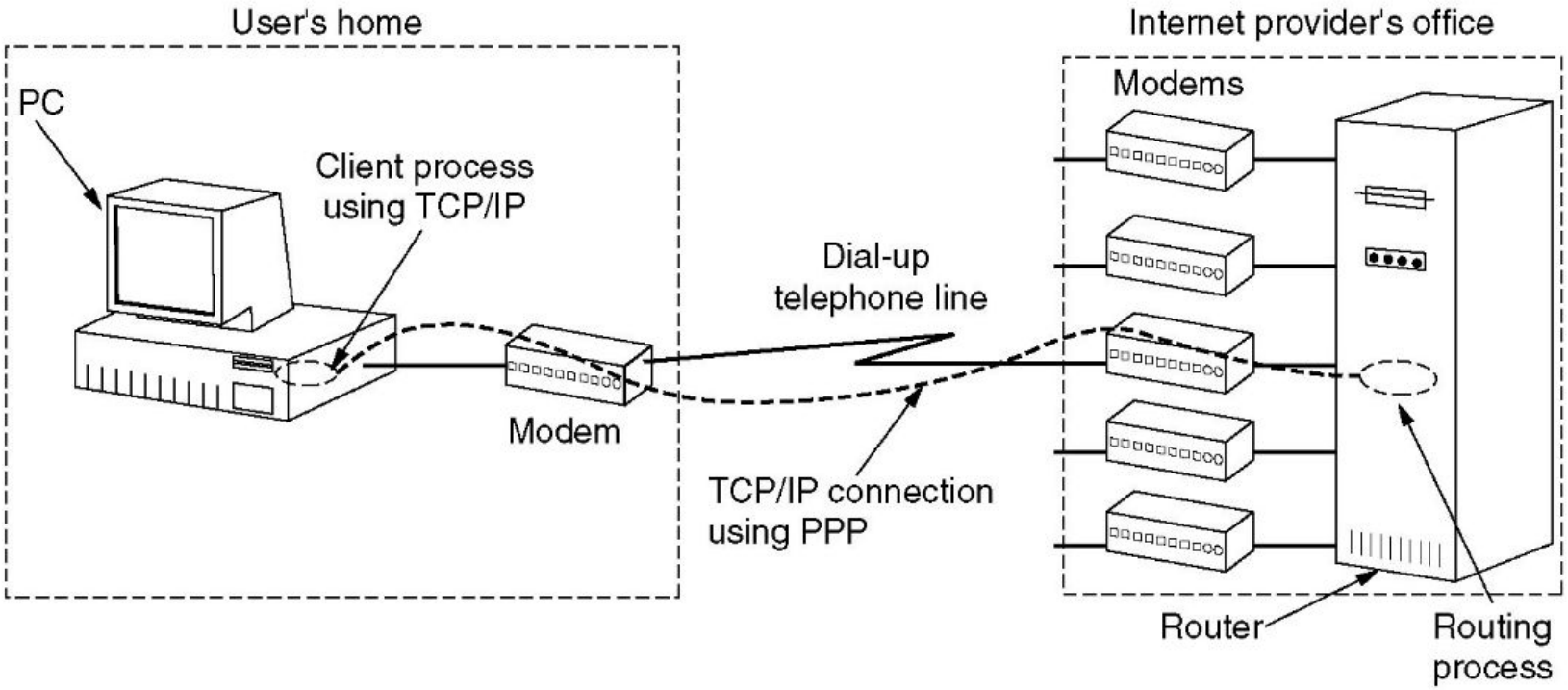


- Antes de trocar dados da camada de rede, os parceiros do enlace de dados devem…
    1. Configurar o enlace PPP
        Compr. máx. quadro, etc.
        Autenticação
    2. Obter/configurar informações da camada de rede
        Para IP: transporta mensagens do Protocolo de Controle IP (IPCP) para configurar/obter o endereço IP
    3. Aberto
        Transporta dados

PPP - FUNCIONAMENTO

- Exemplo de uso domiciliar:
  - Estação “chama” o roteador do ISP através de um modem
  - Após o estabelecimento de uma conexão física, a estação envia quadros LCP em um ou mais quadros PPP
- Selecionam os parâmetros PPP a serem usados
  - Envia pacotes NCP
- Em geral obtém endereço IP
  - Desconexões ocorrem na “ordem inversa”
- Rede (NCP), enlace (LCP) e física (modem desliga o telefone)

PPP - FUNCIONAMENTO



PPPoE

- Conexões PPP tradicionais:
  - Estabelecidas entre duas estações conectadas através de um enlace ponto-a-ponto
    - Não há dúvidas que um quadro enviado por uma estação vá alcançar a outra
- Conexões PPP em redes Ethernet:
  - Uma estação pode alcançar todas as estações na rede
    - Nesse caso, quem seria o provedor de acesso?
- PPPoE adiciona um estágio de descobrimento da estação do provedor de acesso, antes da sessão PPP. Dessa forma, as duas estações passam a conhecer o endereço MAC uma da outra

PROTOCOLOS DE ENLACE POR CANAL DE DIFUSÃO - CONTROLE DE ACESSO AO MEIO

- Protocolos de múltiplo acesso usados em canais de difusão
  - Coordenação de transmissores e de receptores em um canal de difusão compartilhado
  - São algoritmos distribuídos que determinam como os nós compartilham o canal
    - Determinam quando um nó pode transmitir
  - Comunicação sobre o compartilhamento do canal deve usar o próprio canal!
    - Não há canal fora da faixa para coordenar a transmissão

CONTROLE DE ACESSO AO MEIO - COLISÕES

- Por que o Acesso ao Meio Precisa Ser Controlado?
  - Para evitar interferência entre transmissões simultâneas
    - Quando dois ou mais nós transmitem ao mesmo tempo, uma colisão pode ocorrer no nó receptor caso dois ou mais sinais cheguem ao mesmo tempo...

CONTROLE DE ACESSO AO MEIO - COLISÕES

- Colisão em protocolos:
  - Duas entidades enviam dados “simultaneamente”, cada uma para a outra
  - Não é um erro do protocolo mas afeta o seu desempenho

CONTROLE DE ACESSO AO MEIO - COLISÕES

- Tipos de colisão
  - Domínio de colisão único. Este é o tipo mais simples de colisão, ocorrendo quando vários dispositivos tentam enviar dados no mesmo segmento de rede ao mesmo tempo.
  - Múltiplos domínios de colisão. Esse tipo de colisão ocorre em redes maiores com vários segmentos (domínios de colisão). Se dispositivos em segmentos diferentes tentarem enviar dados ao mesmo tempo, isso poderá resultar em uma colisão na espinha dorsal da rede (a linha de transmissão de dados principal que conecta esses segmentos).

CONTROLE DE ACESSO AO MEIO - COLISÕES

- Problemas de rede causados por colisões
  - Degradação do desempenho da rede. Colisões frequentes podem diminuir o desempenho da rede, já que os dispositivos frequentemente precisam parar, esperar e tentar reenviar pacotes.
  - Perda de dados. Colisões podem levar à perda ou danos de pacotes, exigindo a retransmissão e utilizando recursos de rede adicionais.
  - Instabilidade de rede. Em casos extremos, uma taxa alta de colisões pode tornar uma rede instável ou inutilizável, resultando em impactos significativos nos negócios.

PROTOCOLO IDEAL DE ACESSO MÚLTIPLO

- Para um canal de difusão com taxa de R b/s:
  - 1. Quando apenas um nó tem dados para enviar, esse nó obtém uma vazão de R b/s
  - 2. Quando M nós têm dados para enviar, cada um desses nós poderá transmitir em média a uma taxa de R/M b/s
  - 3. O protocolo é completamente descentralizado
    - Nenhum nó especial (mestre) para coordenar as transmissões e se tornar um ponto de falha
  - 4. O protocolo é simples para que sua implementação seja barata

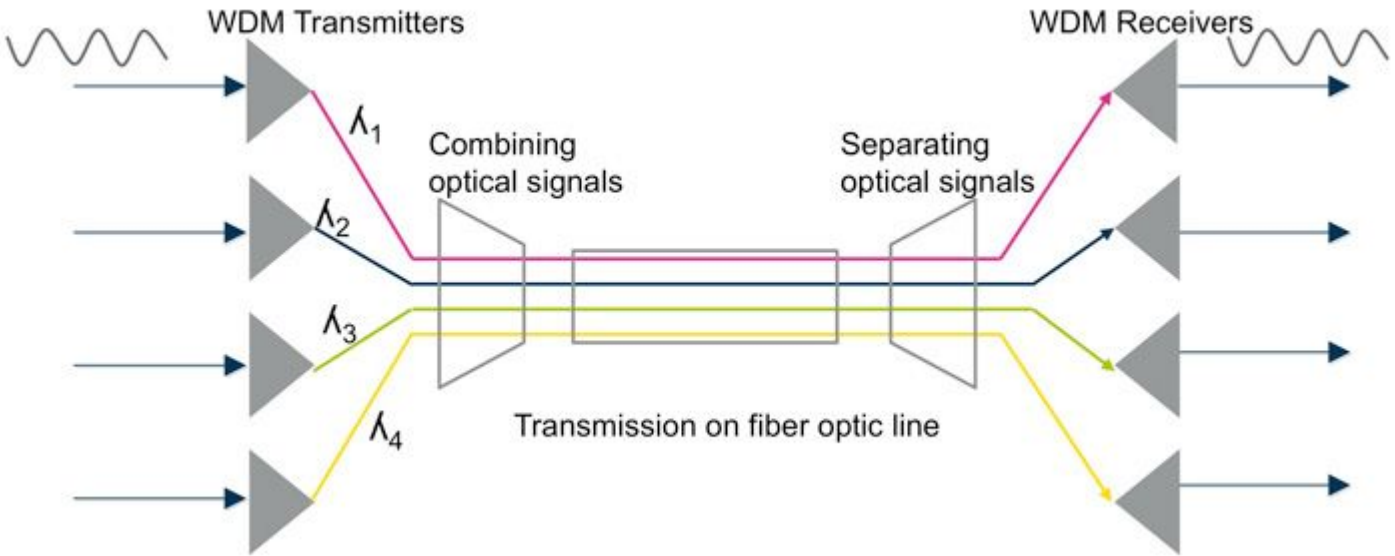
CLASSES DE PROTOCOLOS DE ACESSO MÚLTIPLO

- Protocolos de Divisão de Canal
  - Divide o canal em pequenos “pedaços” (slots de tempo, frequências, códigos)
    - Aloca pedaços a um nó para seu uso exclusivo
- Protocolos de Acesso Aleatório
  - Canal não é dividido, podem ocorrer colisões
    - “Recupera” as colisões
- Protocolos de Revezamento
  - Nós se revezam no acesso ao meio
    - Alterna oportunidades de acesso ao meio sem que ninguém tente acessar ao mesmo tempo

MULTIPLEXAÇÃO

- Tem por objetivo compartilhar o meio físico
  - Divisão do meio ocorre na camada física
- Geralmente centralizada em um dispositivo denominado multiplexador
- Pode ser classificada em função da variável usada para separar as fontes
  - Divisão de tempo (Time Division Multiplexing - TDM)
  - Divisão de frequência (Frequency Division Multiplexing - FDM)
  - Divisão de comprimentos de onda (Wavelenght Division Multiplexing – WDM)

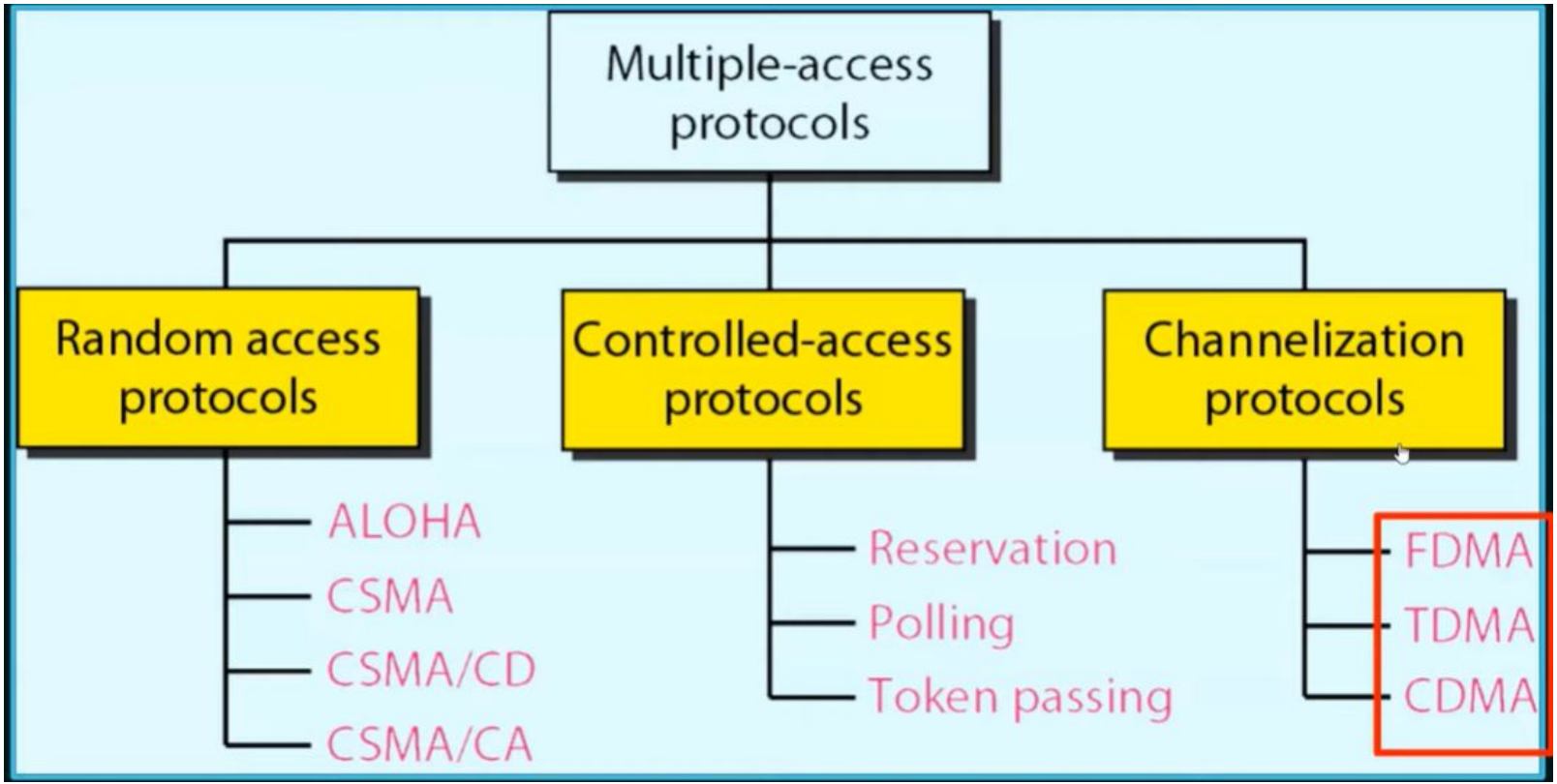
MULTIPLEXAÇÃO



DUPLEXAÇÃO

- Tipo especial de multiplexação
  - Comunicação entre duas estações pode ser classificada em:
    - Simplex único sentido
    - Half-duplex dois sentidos, porém não simultaneamente
    - Full-duplex dois sentidos, simultaneamente
- Também pode ser classificada em função da variável usada para separar as fontes
  - Divisão de tempo (Time Division Duplexing - TDD)
  - Divisão de frequência (Frequency Division Duplexing - FDD)

CLASSES DE PROTOCOLOS DE ACESSO MÚLTIPLO



PROTOCOLOS DE DIVISÃO DE CANAL

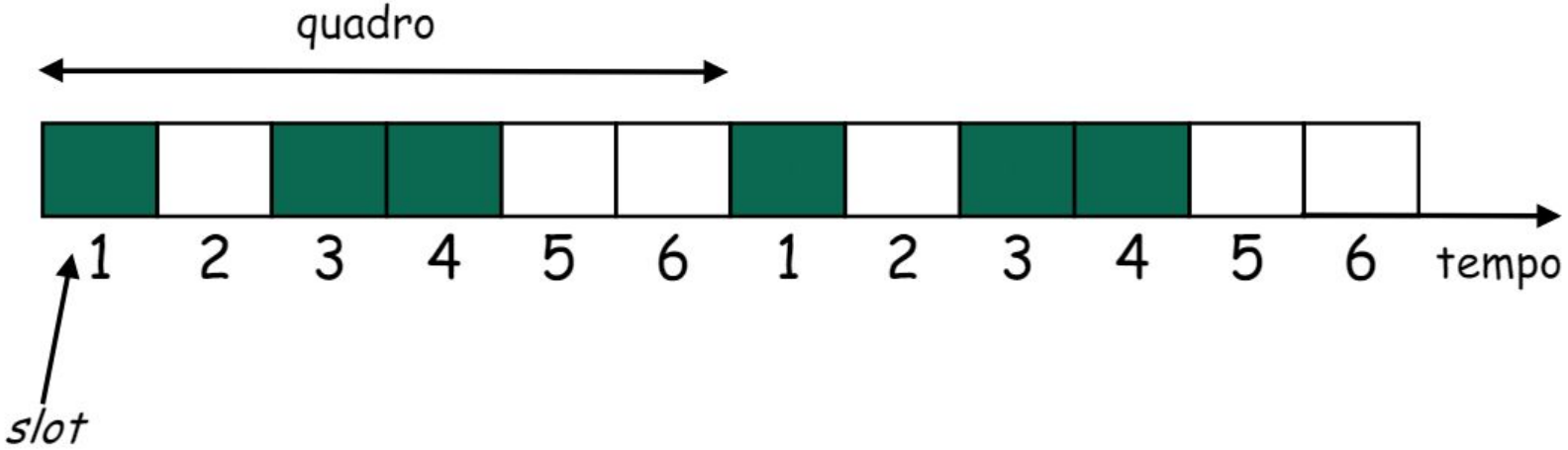
- Acesso ao meio é dividido entre as estações
  - Não podem ocorrer colisões
- Estação compartilha a taxa do canal com outras estações
- Exemplos:
  - TDMA
  - FDMA
  - CDMA

PROTOCOLOS DE DIVISÃO DE CANAL - TDMA

- Acesso múltiplo por divisão de tempo (Time Division Multiple Access)
- Acesso múltiplo feito em função do tempo
- Tempo é dividido em slots
  - Geralmente de tamanho fixo e igual ao tempo para transmitir um pacote
- Em cada slot somente uma estação pode transmitir
  - Acesso ao canal em “turnos“

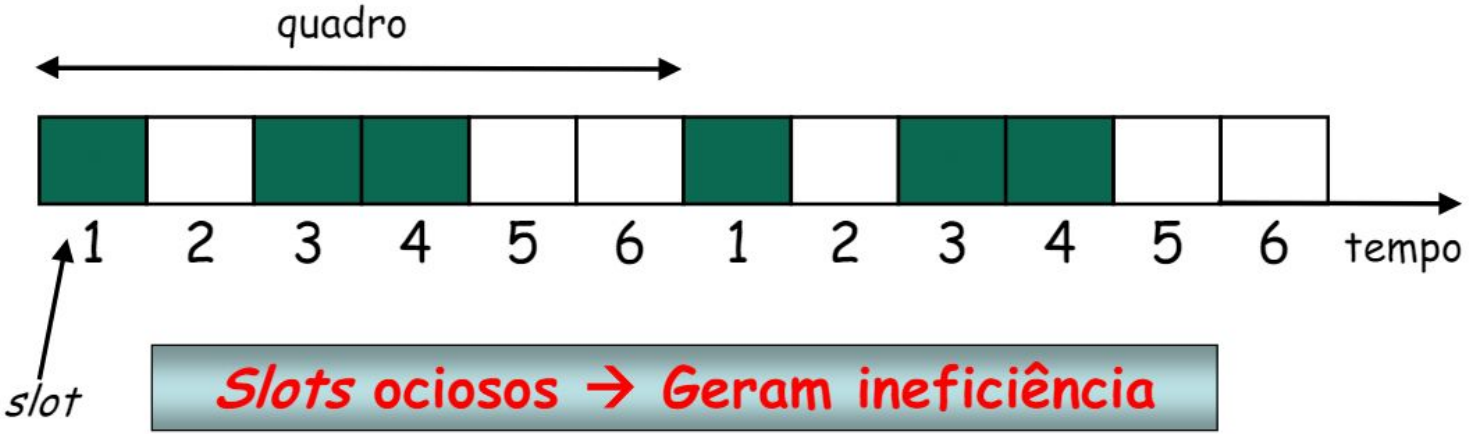
PROTOCOLOS DE DIVISÃO DE CANAL - TDMA

- Exemplo
  - Rede local com 6 estações
  - Slots 1, 3 e 4 com pacotes
  - Slots 2, 5 e 6 ociosos

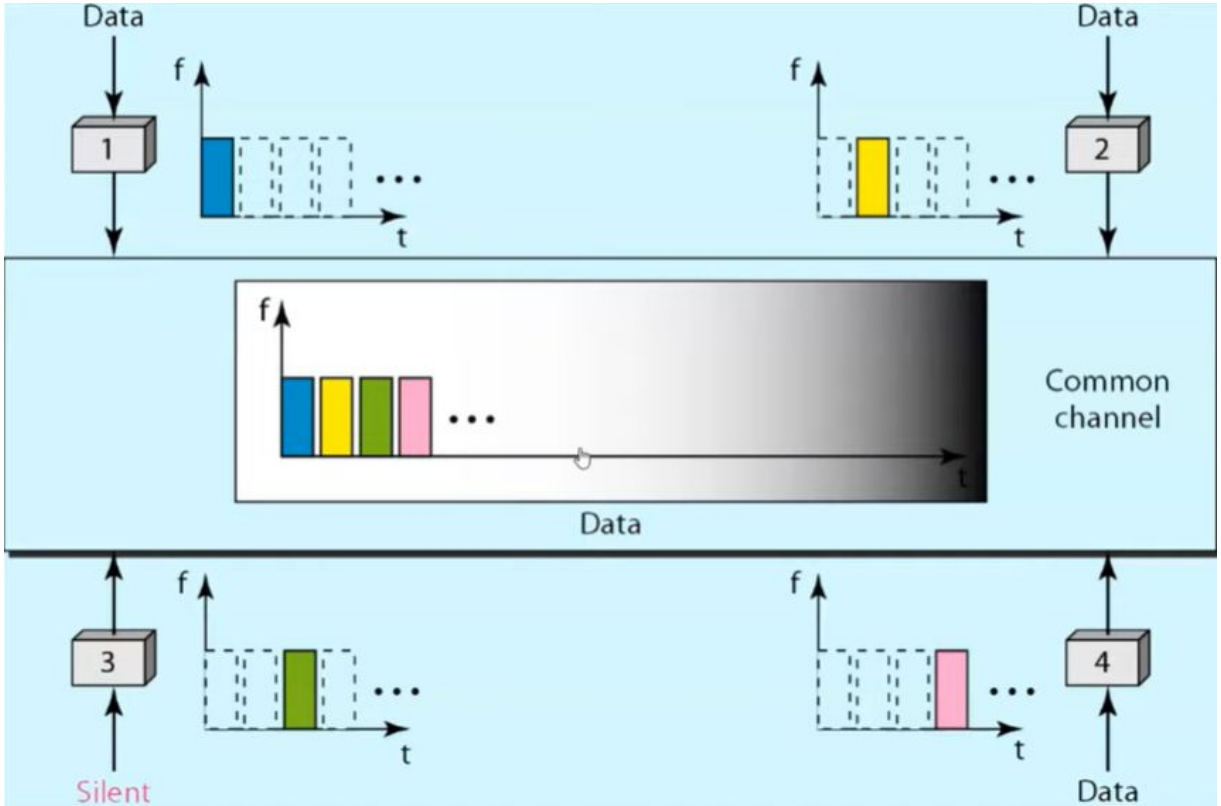


PROTOCOLOS DE DIVISÃO DE CANAL - TDMA

- Exemplo
  - Rede local com 6 estações
  - Slots 1, 3 e 4 com pacotes
  - Slots 2, 5 e 6 ociosos



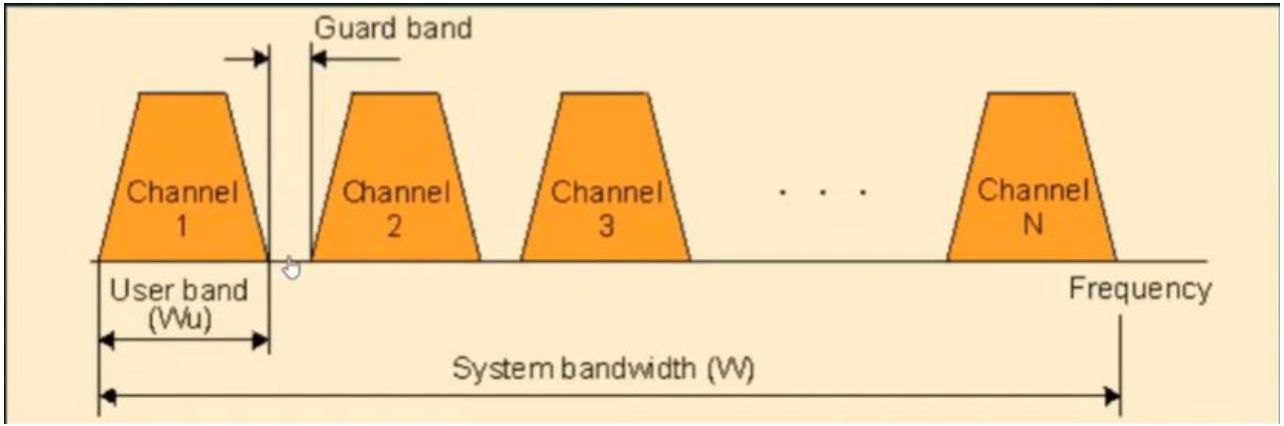
PROTOCOLOS DE DIVISÃO DE CANAL - TDMA



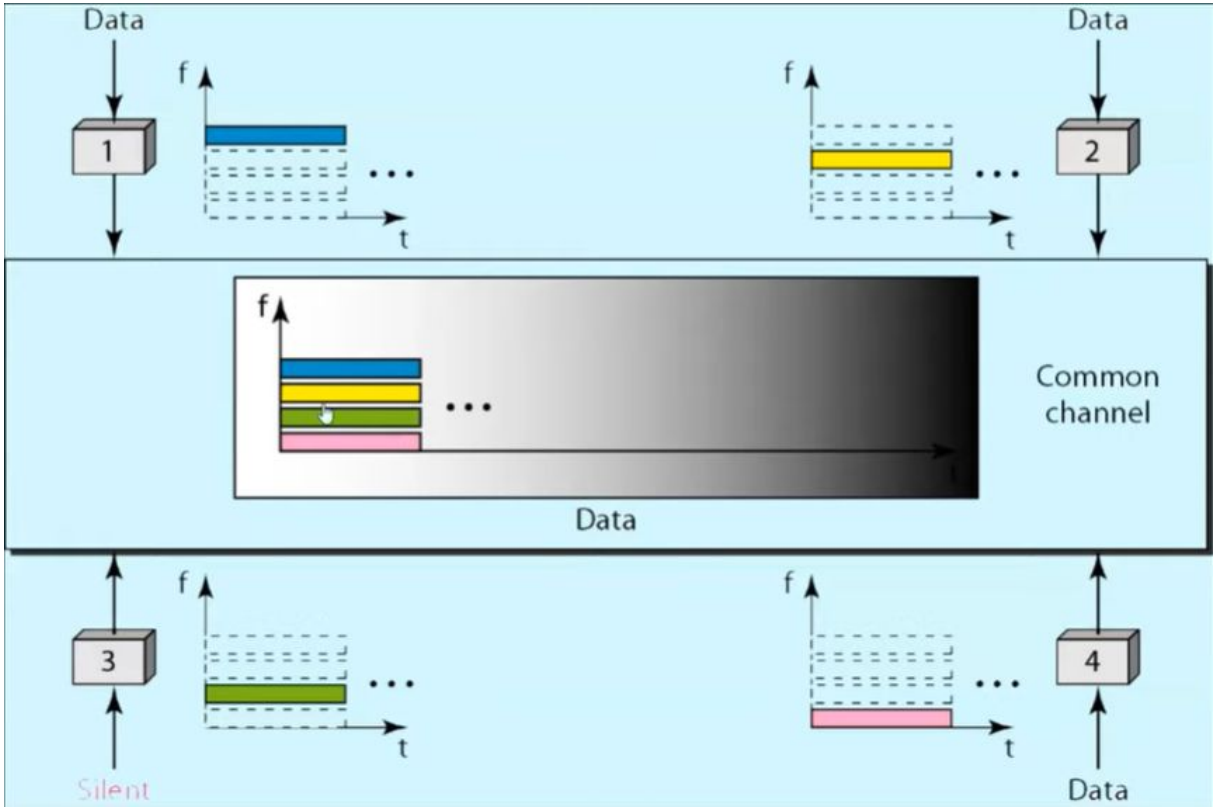
PROTOCOLOS DE DIVISÃO DE CANAL - FDMA

- Acesso múltiplo por divisão de frequência (Frequency Division Multiple Access)
- Acesso múltiplo feito em função da frequência
- Espectro do canal dividido em bandas de frequência
  - Cada estação está associada a uma banda de frequência diferente
  - Bandas isoladas por pequenas bandas de guarda
- Problema semelhante ao TDMA
  - Tempo de transmissão não usado nas bandas permanecem ociosos
  - Em sistemas de computação, o tráfego é tipicamente em rajadas

PROTOCOLOS DE DIVISÃO DE CANAL - FDMA



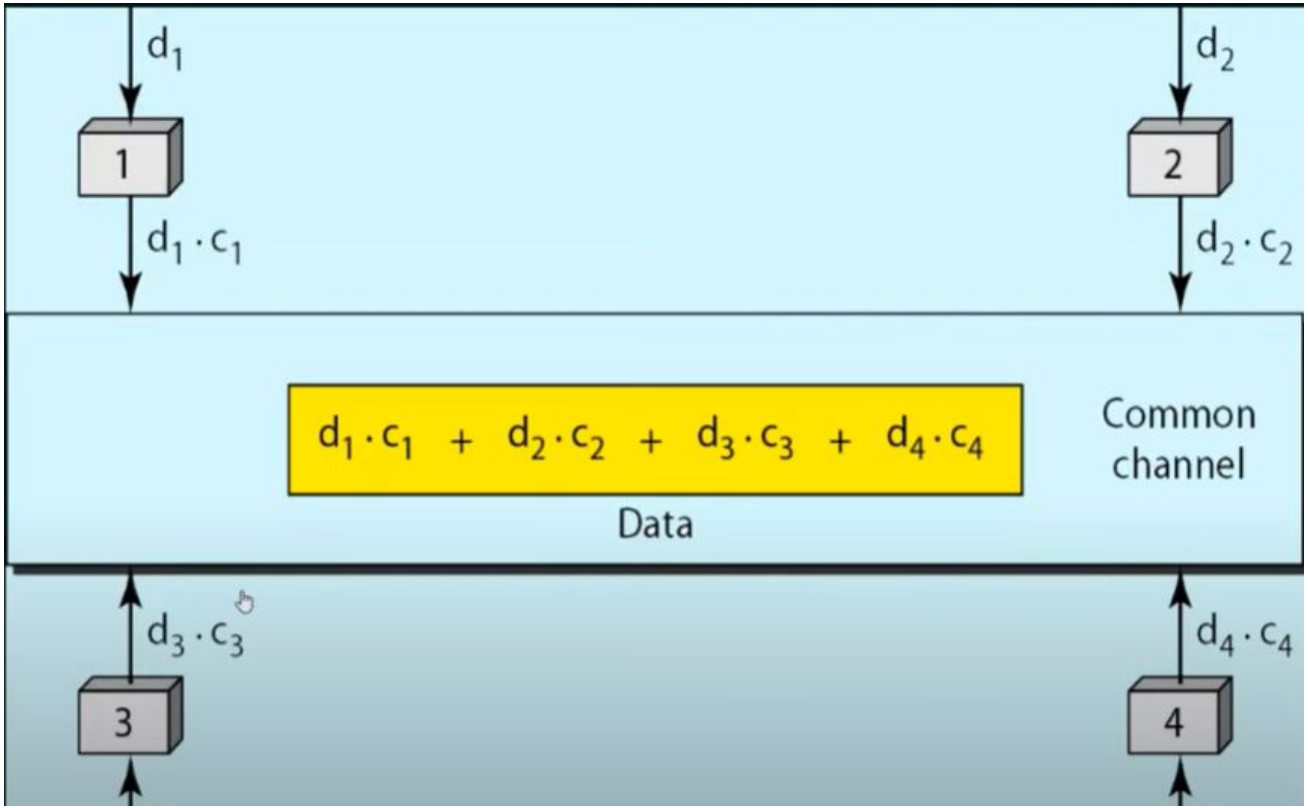
PROTOCOLOS DE DIVISÃO DE CANAL - FDMA



PROTOCOLOS DE DIVISÃO DE CANAL - CDMA

- Acesso múltiplo por divisão de código (Code Division Multiple Access)
- Acesso múltiplo feito em função do código
- Cada estação está associada a um código diferente
  - Destino deve conhecer o código da fonte
- Muito usado em redes sem fio
- Vantagem
  - Estações podem transmitir simultaneamente usando códigos diferentes

PROTOCOLOS DE DIVISÃO DE CANAL - CDMA



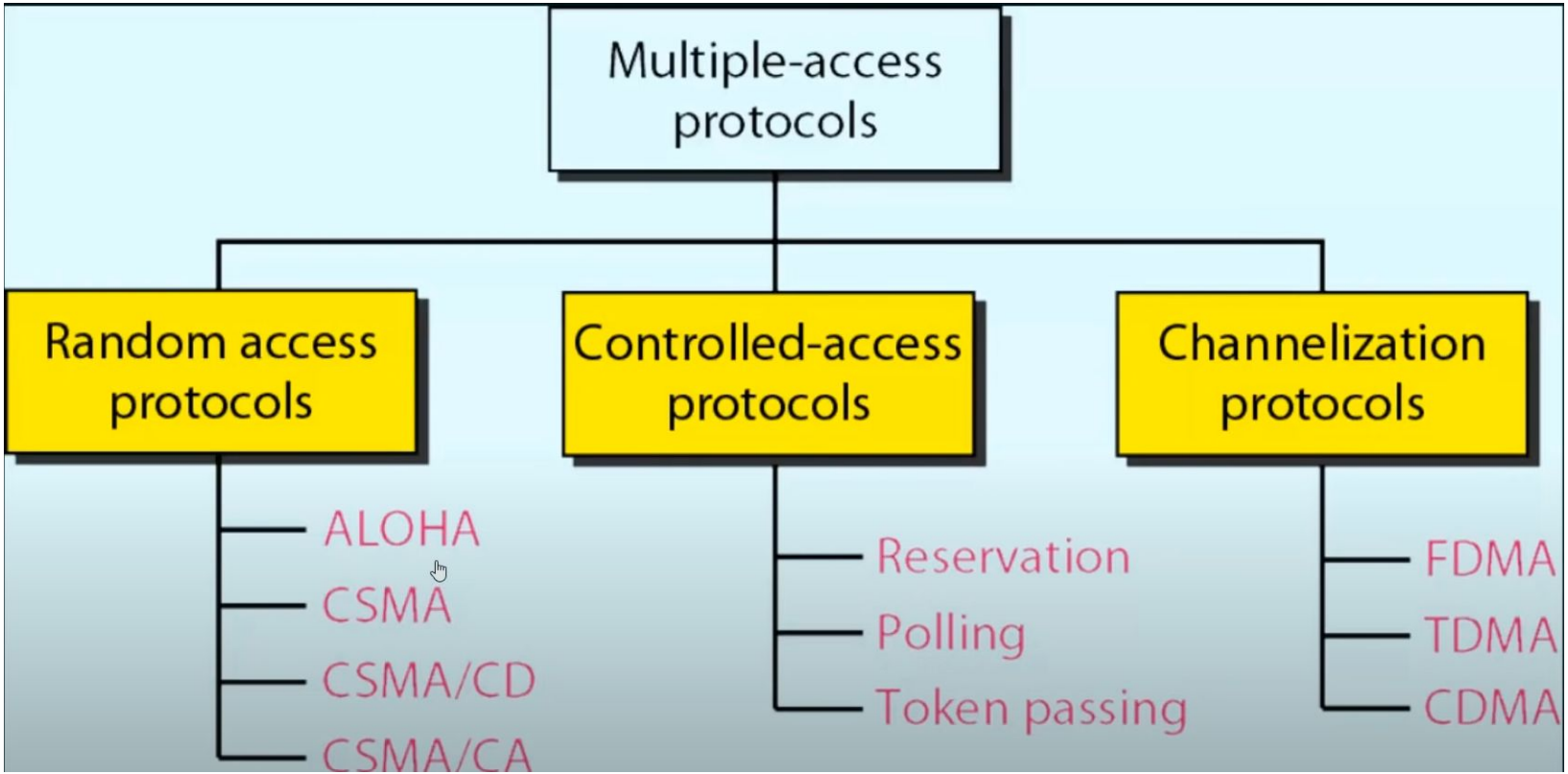
PROTOCOLOS DE ACESSO ALEATÓRIO

- Quando um nó tiver um quadro a transmitir
  - Tenta transmitir à taxa máxima do canal sem nenhuma coordenação a priori entre os nós
- Entretanto, se dois ou mais nós transmitirem ao mesmo tempo:
  - Há uma colisão!
    - Acesso ao meio é realizado de forma não determinística
- Nesse cenário, o protocolo de acesso aleatório específica:
  - Como detectar colisões e como se recuperar delas
    - Através de retransmissões retardadas, por exemplo

PROTOCOLOS DE ACESSO ALEATÓRIO

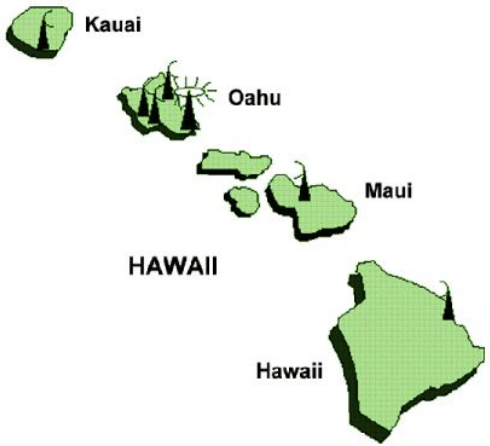
- Aloha
- Slotted Aloha
- CSMA persistente
- CSMA não persistente
- CSMA p-persistente
- CSMA/CD
- Outros

PROTOCOLOS DE ACESSO ALEATÓRIO



PROTOCOLOS DE ACESSO ALEATÓRIO - ALOHA

- Rede ALOHA
- Criada por Norman Abranson em 1960
- Primeira rede baseada em pacotes
- Interligação de computadores em várias ilhas do Havaí compartilhando um meio (RF)
- Comunicação com um computador central
- Disputa do meio



PROTOCOLOS DE ACESSO ALEATÓRIO - ALOHA PURO

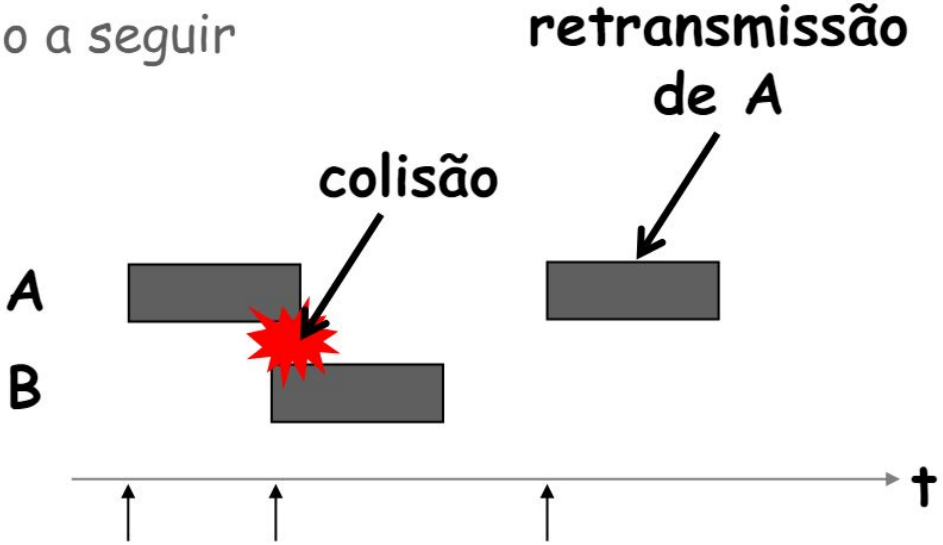
- Projetada para redes sem fio
- Protocolo de acesso aleatório
- Estação transmite quando desejar
  - Não há escuta do meio…
  - Se o quadro for recebido sem erros
    - Um reconhecimento positivo é enviado ao remetente
  - Se duas ou mais estações transmitirem ao mesmo tempo
    - Colisão!
      - Colisão inferida através do não recebimento do reconhecimento positivo em um tempo
  - Se o quadro for recebido com erro
    - Remetente também não recebe reconhecimento positivo

PROTOCOLOS DE ACESSO ALEATÓRIO - ALOHA PURO

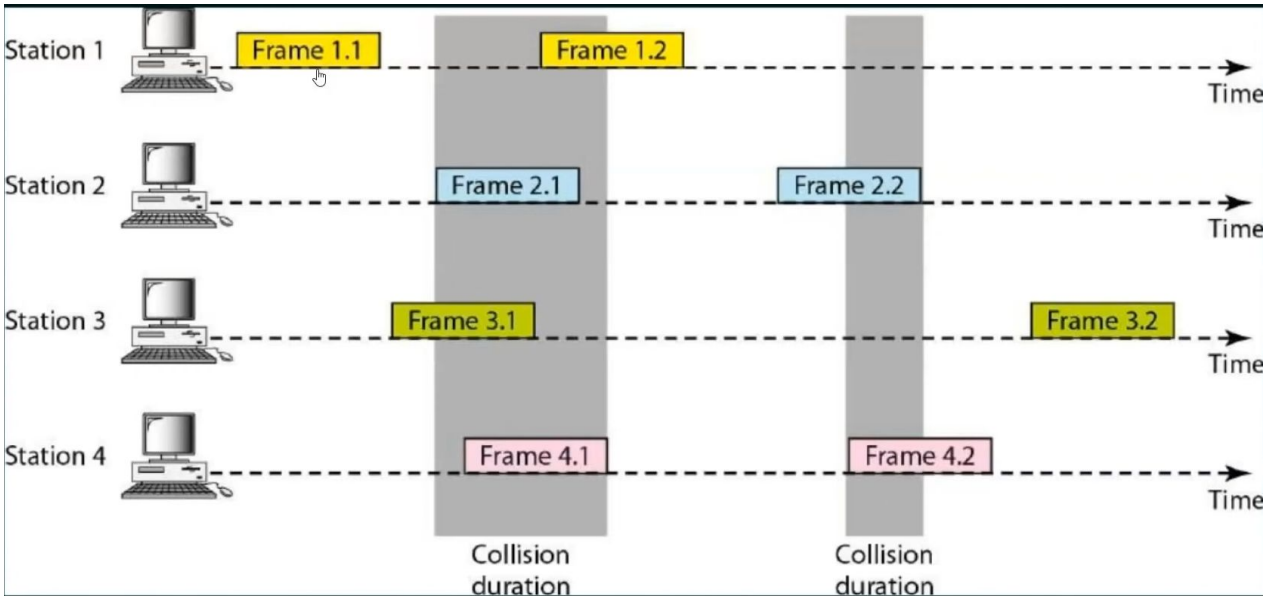
- Se o reconhecimento positivo não for recebido...
  - Quadro é retransmitido…
    - Retransmissão após a tempo aleatório para redução da probabilidade de nova colisão
  - Processo é repetido continuamente até que o reconhecimento seja recebido pelo remetente

PROTOCOLOS DE ACESSO ALEATÓRIO - ALOHA PURO

- Baixa eficiência
  - Cálculo a seguir



PROTOCOLOS DE ACESSO ALEATÓRIO - ALOHA PURO



PROTOCOLOS DE ACESSO ALEATÓRIO - ALOHA PURO

- Permite que as estações enviem PDUs quando tiver dados a enviar
- A estação que envia espera por uma confirmação
- Se a combinação não é recebida a estação aguarda uma quantia randômica de tempo chamada back-off time e então reenvia o dado
- Como todas as estações esperam uma quantidade aleatória de tempo a probabilidade de colisão é diminuída
- A eficiência máxima do ALOHA puro é de 18,39% porém na prática é menor.

PROTOCOLOS DE ACESSO ALEATÓRIO - SLOTTED ALOHA

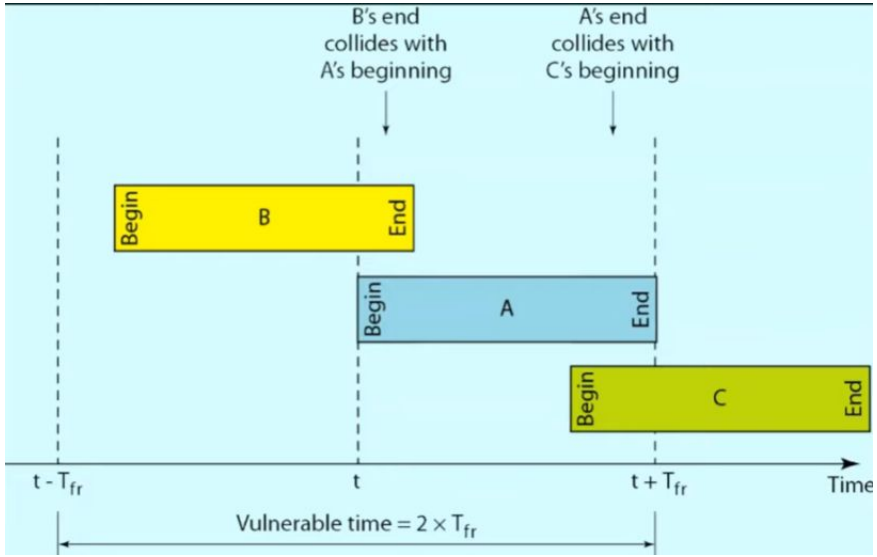
- Hipóteses:
  - Todos os quadros têm o mesmo tamanho (L bits)
  - Tempo é dividido em slots de tamanho igual
    - Tempo para transmitir 1 quadro (L/R seg)
  - Nós começam a transmitir quadros apenas no início dos intervalos (slots)
  - Nós são sincronizados para que saibam onde os intervalos começam
  - Se dois ou mais nós transmitirem em um slot, todos os nós envolvidos deixam de receber um reconhecimento

PROTOCOLOS DE ACESSO ALEATÓRIO - SLOTTED ALOHA

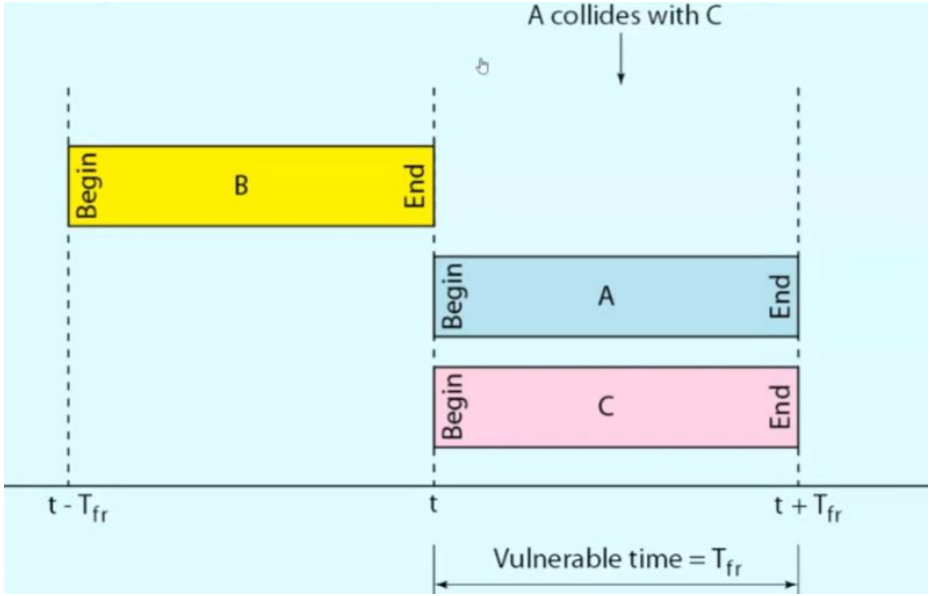
- Operação
  - Quando o nó obtém um novo quadro, ele espera até o início do próximo slot e transmite o quadro inteiro
    - Se não houver colisão, o nó poderá enviar um novo quadro no próximo slot
    - Caso haja uma colisão (percebida antes do final do intervalo), o nó retransmite o quadro em intervalo subsequente com probabilidade p até obter sucesso

PROTOCOLOS DE ACESSO ALEATÓRIO - SLOTTED ALOHA

ALOHA PURO

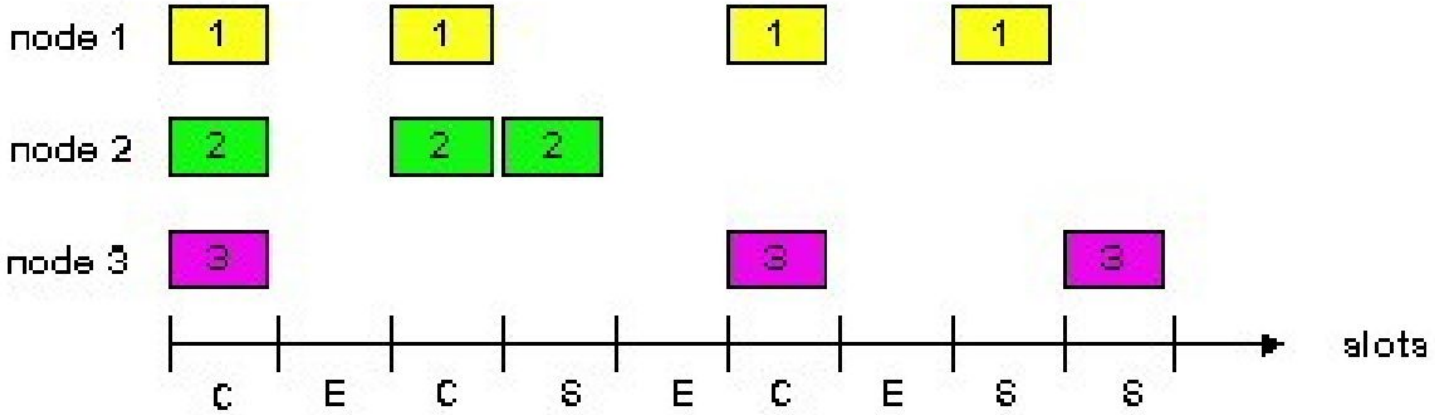


SLOTTED ALOHA



PROTOCOLOS DE ACESSO ALEATÓRIO - SLOTTED ALOHA

- Operação



PROTOCOLOS DE ACESSO ALEATÓRIO - SLOTTED ALOHA

- Vantagens
  - Único nó ativo pode transmitir continuamente na taxa máxima do canal
  - Altamente descentralizado
    - Apenas os slots nos nós precisam estar sincronizados
  - Simples
  - Aumenta a eficiência do protocolo para 36.8%
- Desvantagens
  - Quando há colisões slots desperdiçados
  - Slots ociosos desperdício
    - Retransmissões em slots aleatórios podem gerar slots ociosos
  - Requer a sincronização dos relógios

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- CSMA (Carrier Sense Multiple Acess)
- Uso de detecção de portadora (sinal no meio)
  - Escuta o meio antes de transmitir
    - Se o canal estiver livre, transmite o quadro
    - Se o canal estiver ocupado, adia a transmissão
  - Objetivo evitar colisões!
- Analogia humana: não interrompa os outros!
  - Escute antes de falar detecção de portadora
  - Se alguém começa a falar junto de você, pare de falar → detecção de colisão

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- Diferenças em relação ao ALOHA:
  - Aloha não escuta o meio
  - Aloha não pára a transmissão caso detecte uma colisão

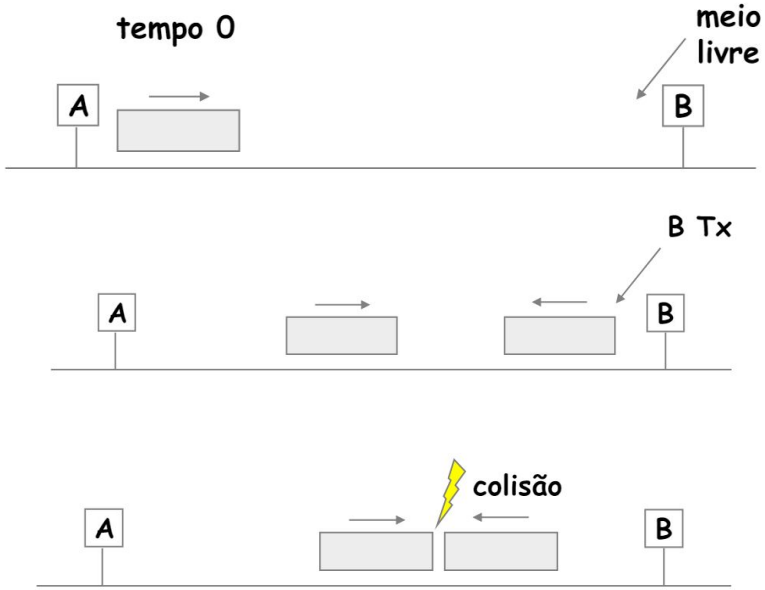
PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- Tipos de CSMA
  - Motivação: aumentar a eficiência
  - Vários tipos
    - CSMA persistente
    - CSMA não-persistente
    - CSMA p-persistente
    - CSMA/CD
    - CSMA/CA

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

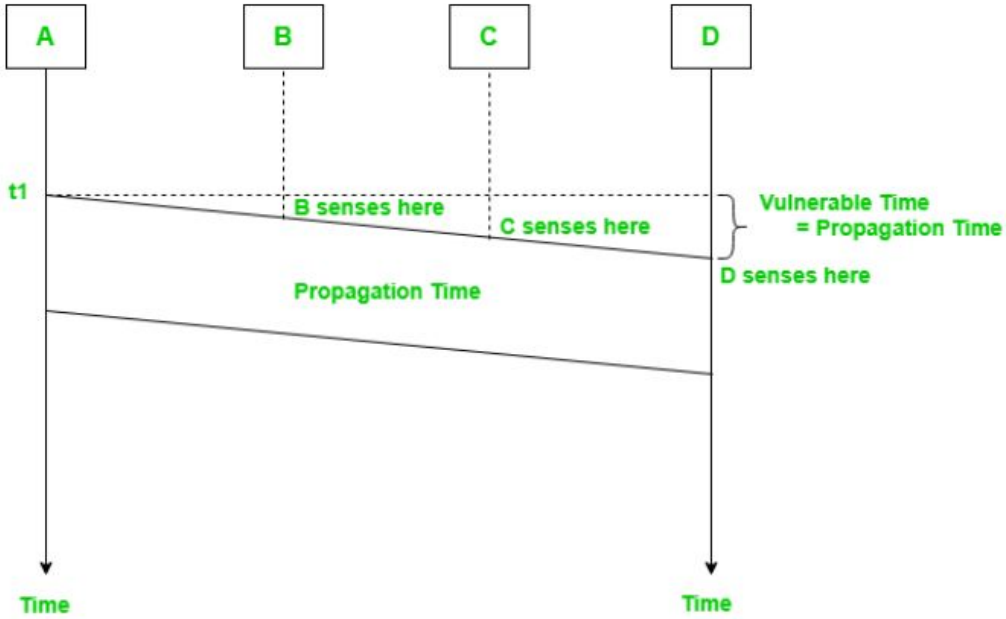
- Colisão de Quadros
  - Se todos os nós escutam o meio antes de transmitir, ainda existem colisões? SIM!
- Estação que quer transmitir um quadro ouve o meio
  - Mesmo com a escuta da portadora, ainda podem ocorrer colisões
  - Duas ou mais estações escutam o meio
    - Não escutam a transmissão da outra devido ao atraso de propagação do sinal

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA



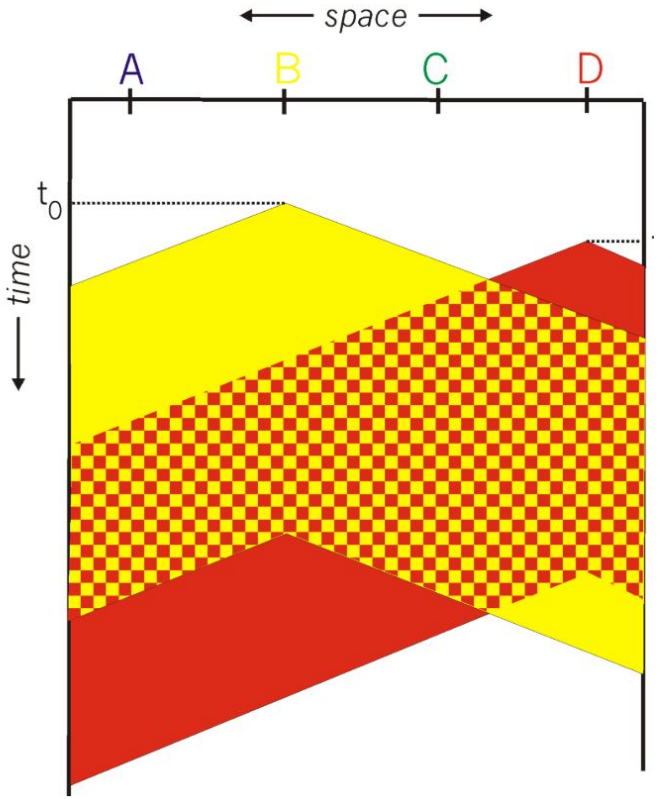
PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- Tempo vulnerável = tempo de propagação



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- Exemplo:
  - 4 estações: A, B, C e D
    - Em t0 , B escuta o meio
      - Para B, o meio está livre
    - Em t1 , D escuta o meio
      - Para D, o meio também está livre
  - Os bits enviados por B não chegaram a D



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- Mesmo com a escuta da portadora, ainda podem ocorrer colisões
  - Devido à “memória”do meio físico
  - Quanto maior o tamanho da rede
    - Maior o atraso de propagação de uma extremidade à outra
    - Maior a probabilidade de ocorrerem colisões
  - Quanto menor o tamanho da rede
    - Mais efetiva é a escuta de portadora
      - Explica o sucesso do CSMA para redes locais

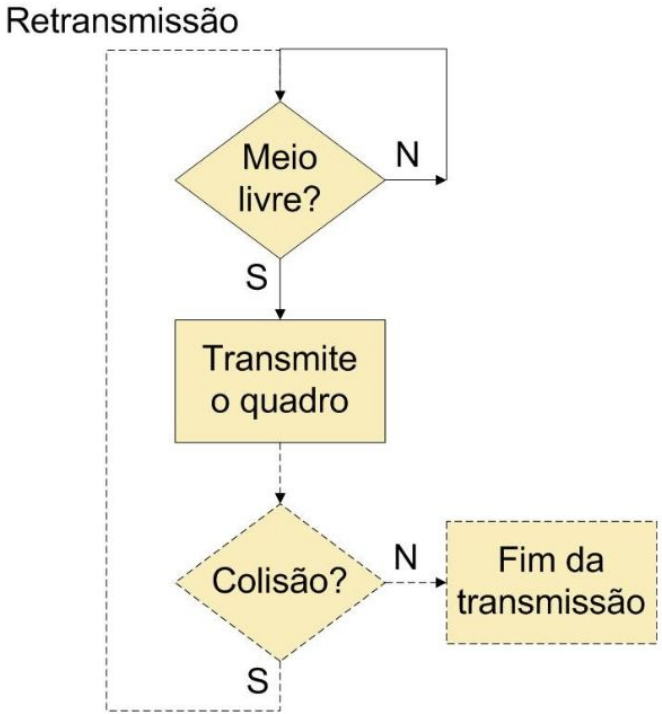
PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- Colisão de Quadros
  - Inferida
    - Através do não recebimento de um reconhecimento positivo em um tempo T
    - CSMA persistente
    - CSMA não-persistente
    - CSMA p-persistente
    - CSMA/CA (Collision Avoidance)
  - Detectada
    - CSMA/CD (Collision Detection)

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA PERSISTENTE

- Quando a estação tem um quadro para transmitir
  - Primeiro escuta o meio:
    - Se o meio estiver livre → Transmite
    - Se o meio estiver ocupado → Continua escutando o meio até que ele fique livre
    - Se houver uma colisão
      - Espera um tempo aleatório para recomeçar o processo

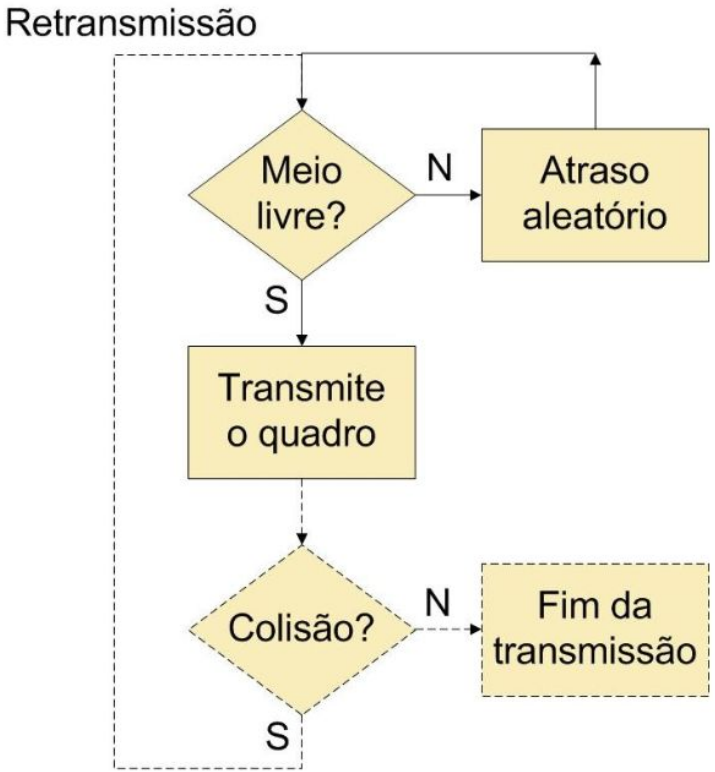
PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA PERSISTENTE



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA NÃO PERSISTENTE

- Quando a estação tem um quadro para transmitir
  - Primeiro escuta o meio:
    - Se o meio estiver livre → Transmite
    - Se o meio estiver ocupado → Estação espera um tempo aleatório e só depois volta a escutar o meio
      - Diferente do modo persistente, no qual a estação permanece escutando o meio até que ele fique livre
- Se houver uma colisão
  - Espera um tempo aleatório para recomeçar o processo

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA NÃO PERSISTENTE



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA P-PERSISTENTE

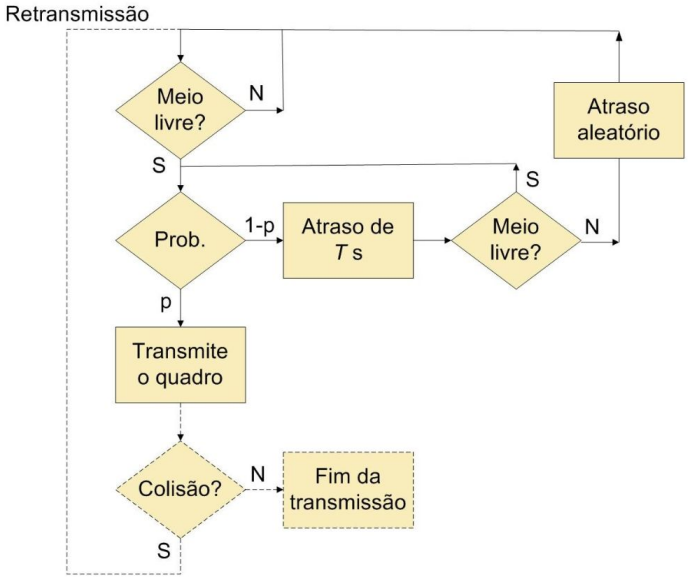
- Tempo dividido em slots
  - Definição de slot diferente da usada no Slotted Aloha
    - Quadro em geral ocupa vários slots
  - Slot de *Ts* → *tempo máximo de propagação*
- Ideia
  - Probabilidade *p* de transmitir o quadro no início de um slot

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA P-PERSISTENTE

- Quando a estação tem um quadro para transmitir
  - Primeiro escuta o meio:
    - Se o meio estiver livre
      - Estação transmite o quadro com probabilidade *p*
      - Espera pelo próximo slot com probabilidade *q = 1-p*
        - Se o meio estiver livre, novo sorteio com probabilidade *p*
        - Se o meio estiver ocupado, espera um tempo aleatório e reinicia o processo (trata como se uma colisão tivesse acontecido)
      - Se o meio estiver ocupado → Espera pelo próximo slot e repete o algoritmo

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA P-PERSISTENTE

- Em caso de colisão após a transmissão
  - Espera um tempo aleatório e o processo recomeça



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD

- Escuta de portadora
  - Como o CSMA persistente
- Detecção de colisão
  - Realizada pelo transmissor durante a transmissão do quadro
    - Transmissor escuta o meio enquanto transmite
  - Estação cancela a transmissão assim que detecta a colisão
    - Reduz o desperdício!

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD

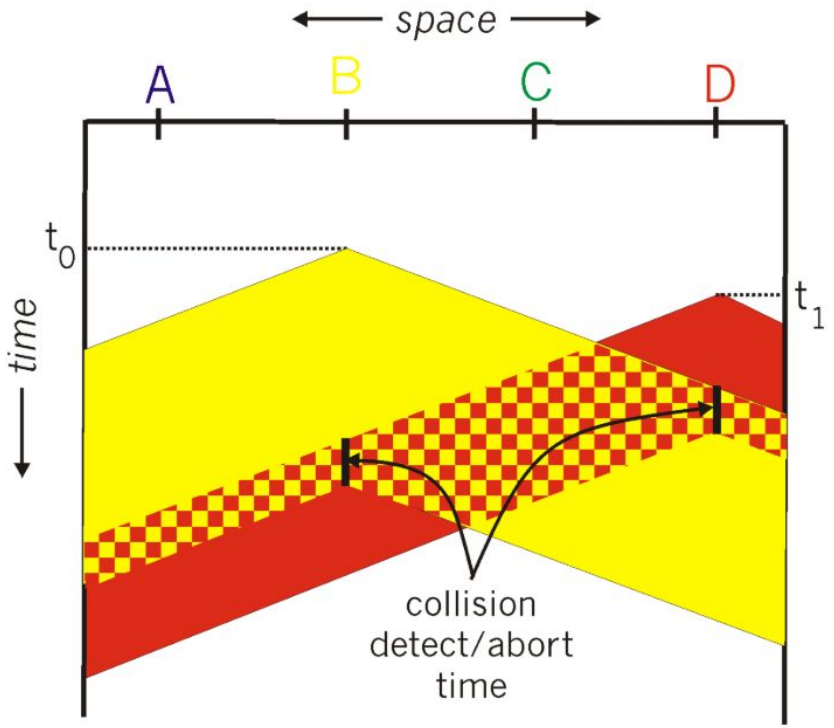
- Escuta de portadora
  - Como o CSMA persistente
- Detecção de colisão
  - Informação da colisão enviada para todas as estações tomarem conhecimento •
    - Reforço de colisão (jam)
  - Diminui-se a duração dos efeitos das colisões

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD

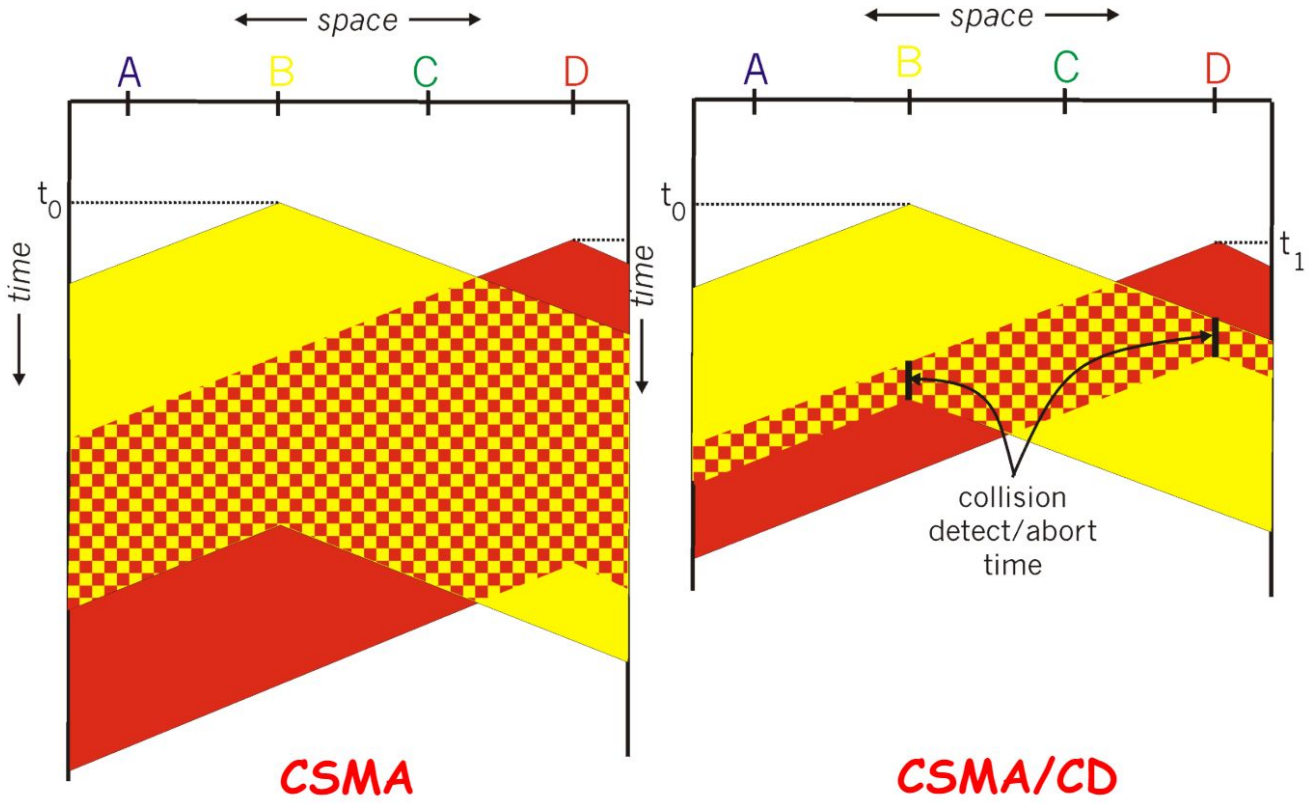
- Caso haja colisão
  - Nova tentativa de transmissão após um tempo aleatório
    - Semelhante ao CSMA persistente
- Analogia humana: bate papo educado!
- Detecção de colisões
  - Fácil em redes locais cabeadas
    - Mede a potência do sinal, comparando o sinal recebido com o transmitido
  - Difícil em redes locais sem fio
    - O receptor é desligado durante a transmissão

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD

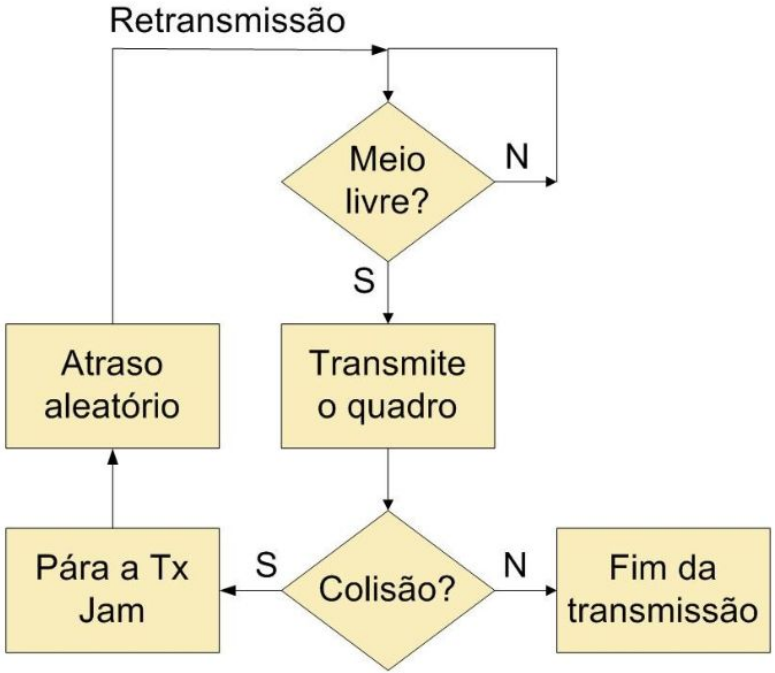
- Exemplo
  - 4 estações: A, B, C e D
    - Em t0 , B escuta o meio
      - Para B, o meio está livre
    - Em t1 , D escuta o meio
      - Para D, o meio também está livre
  - Os bits enviados por B não chegaram a D



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD



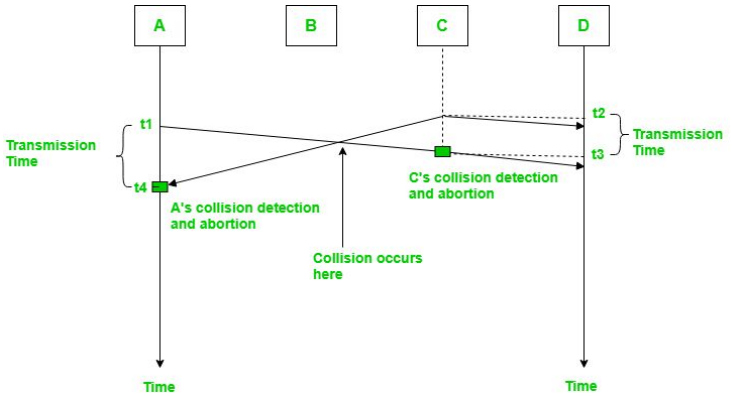
PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD

- Problema:
  - Como garantir que todas as estações detectem colisões?
- Solução:
  - Meio tem que ficar ocupado durante o dobro (ida e volta) do atraso máximo de propagação no meio (t)
    - Quadro possui um tamanho mínimo
      - Porque a colisão é detectada pelos transmissores durante o envio dos quadros
- CSMA/CD será detalhado quando trabalharmos o protocolo ETHERNET

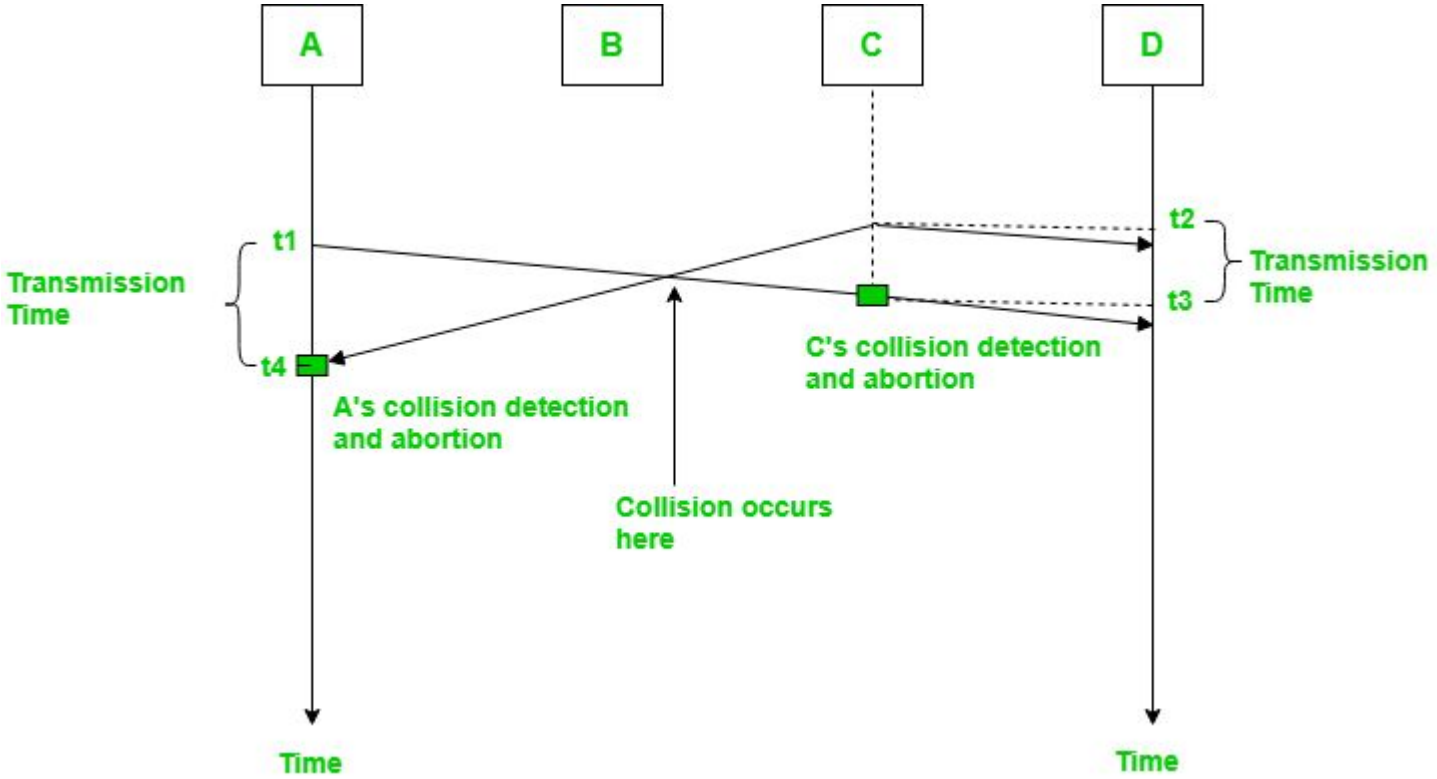
PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD

- No diagrama, A começa a enviar o primeiro bit de seu quadro em t1 e, como C vê o canal livre em t2, começa a enviar seu quadro em t2. C detecta o quadro de A em t3 e aborta a transmissão. A detecta o quadro de C em t4 e aborta sua transmissão. Portanto, o tempo de transmissão do quadro de C é t3 - t2 e o tempo de transmissão do quadro de A é t4 - t1.

- Assim, o tempo de transmissão do quadro (Tfr) deve ser, no mínimo, duas vezes o tempo máximo de propagação (Tp). Isso pode ser deduzido quando as duas estações envolvidas em uma colisão estão a uma distância máxima entre si.



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA/CD



PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- **Vantagens do CSMA:**
  - ***Aumento da eficiência***: O CSMA garante que apenas um dispositivo comunique na rede de cada vez, reduzindo colisões e melhorando a eficiência da rede.
  - ***Simplicidade***: O CSMA é um protocolo simples, fácil de implementar e não requer hardware ou software complexos.
  - ***Flexibilidade***: O CSMA é um protocolo flexível que pode ser usado em uma ampla gama de ambientes de rede, incluindo redes com fio e sem fio.
  - ***Baixo custo***: O CSMA não requer hardware ou software caros, tornando-o uma solução de comunicação de rede econômica.

PROTOCOLOS DE ACESSO ALEATÓRIO - CSMA

- **Desvantagens do CSMA:**
  - ***Escalabilidade limitada*:** O CSMA não é um protocolo escalável e pode se tornar ineficiente à medida que o número de dispositivos na rede aumenta.
  - ***Atraso:*** Em redes ocupadas, a necessidade de monitorar o meio e esperar por um canal disponível pode resultar em atrasos e maior latência.
  - ***Confiabilidade limitada*:** O CSMA pode ser afetado por interferência, ruído e outros fatores, resultando em comunicação não confiável.
  - ***Vulnerabilidade a ataques:*** O CSMA pode ser vulnerável a certos tipos de ataques, como interferência e ataques de negação de serviço, que podem interromper a comunicação na rede.

PROTOCOLOS DE ACESSO ALEATÓRIO - REVISÃO

Protocolo	Comportamento de transmissão	Método de detecção de colisão	Eficiência	Casos de uso
ALOHA Puro	Envia quadros imediatamente	Sem detecção de colisão	Baixa	Redes de baixo tráfego
ALOHA Escalonado	Envia quadros em intervalos de tempo específicos	Sem detecção de colisão	Melhor que ALOHA Puro	Redes de baixo tráfego
CSMA/CD	Monitora o meio após enviar um quadro, retransmite se necessário	Detecção de colisão monitorando transmissões	Alta	Redes com fio de tráfego moderado a alto
CSMA/CA	Monitora o meio durante a transmissão, ajusta o comportamento para evitar colisões	Evita colisões através de intervalos de tempo de recuo aleatórios	Alta	Redes sem fio com tráfego moderado a alto e altas taxas de erro

PROTOCOLOS DE REVEZAMENTO

- Divisão de canal
  - Eficiente para carga alta
    - Compartilhamento justo do canal
  - Ineficiente para carga baixa
    - Atraso no canal de acesso
    - Divisão da largura de banda mesmo com apenas 1 nó ativo
- Acesso aleatório
  - Ineficiente para carga alta
    - Sobrecarga causada por colisões
  - Eficiente para carga baixa
    - Um único nó pode utilizar completamente o canal

PROTOCOLOS DE REVEZAMENTO

- Busca unir o melhor dos dois mundos
- Geralmente o acesso ao meio é realizado em função de uma estação centralizadora
  - Determina quando uma dada estação pode transmitir
  - Garante a ausência de colisões
- Estação compartilha a taxa do canal com outras estações

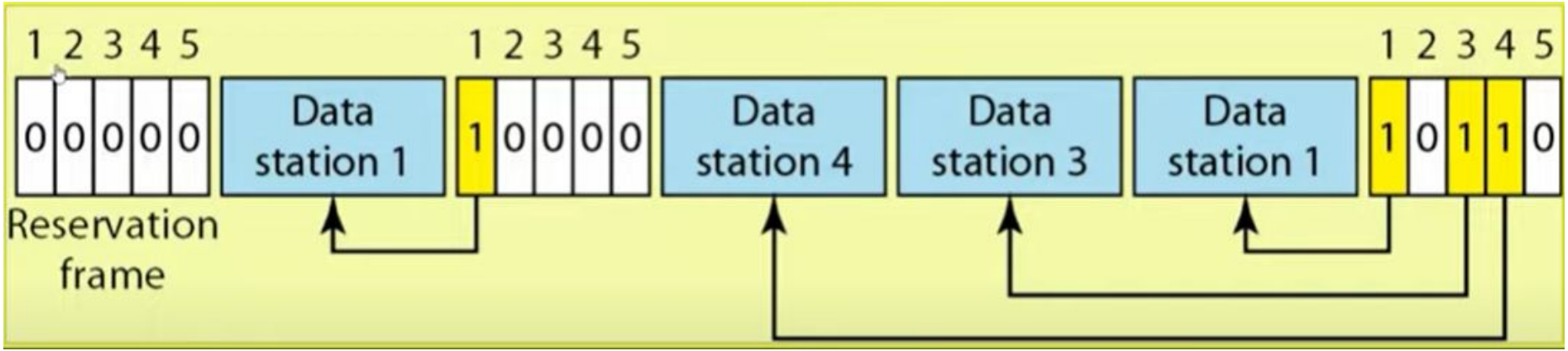
PROTOCOLOS DE REVEZAMENTO

- Varredura (polling)
- Reserva
- Passagem de ficha de permissão (token)
- Outros

PROTOCOLOS DE REVEZAMENTO - RESERVA

- Analogia da reserva do ônibus - assento é reservado antes da viagem
- Estações reservam o direito de acessar o meio compartilhado
- Pedidos de reserva são enviados pelas estações
  - Processados pela estação centralizadora que escalona o posterior acesso ao meio
    - Dependendo do protocolo, pode haver colisões de pedidos
- Um quadro de reserva precede o envio dos dados
- Se existem N nós no sistema teremos N minislots de reserva disponíveis

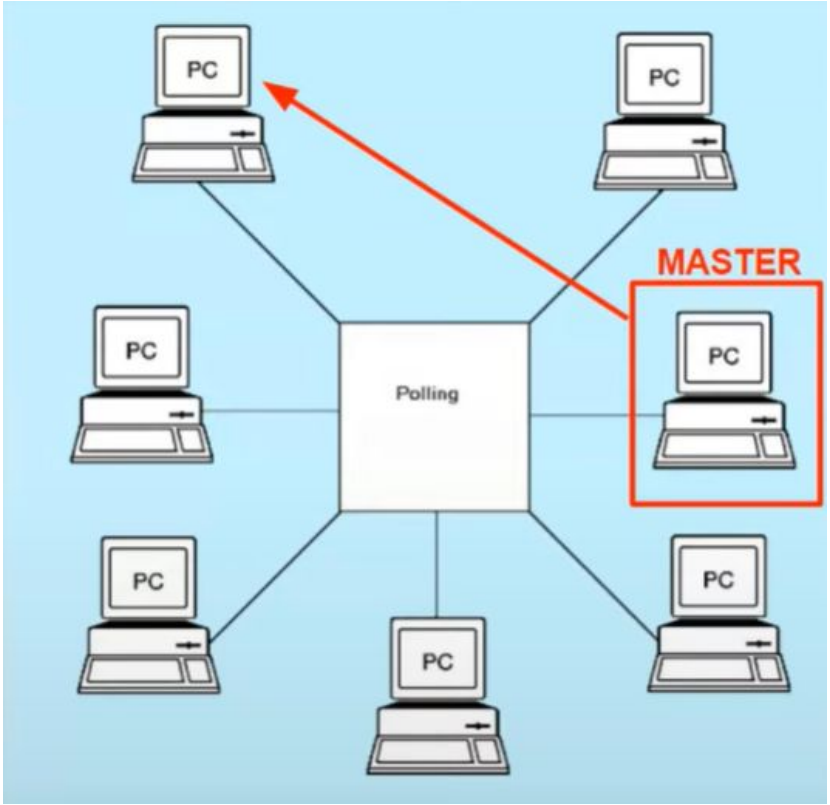
PROTOCOLOS DE REVEZAMENTO - RESERVA



PROTOCOLOS DE REVEZAMENTO - VARREDURA (*POLLING*)

- Estação controladora envia mensagens a outras
  - Convidando-as a transmitir dados
- Estações ao serem consultadas podem transmitir dados
  - Ordem das consultas-convites
- Utiliza round-robin para permitir que todas as estações enviem pacotes
- Lista armazenada na estação controladora
- Vantagens:
  - Evita colisões
  - Eficiência maior que a reserva
- Desvantagens
  - Introduz um atraso de seleção
  - Sobrecarga de controle
  - Ponto único de falha

PROTOCOLOS DE REVEZAMENTO - VARREDURA (*POLLING*)



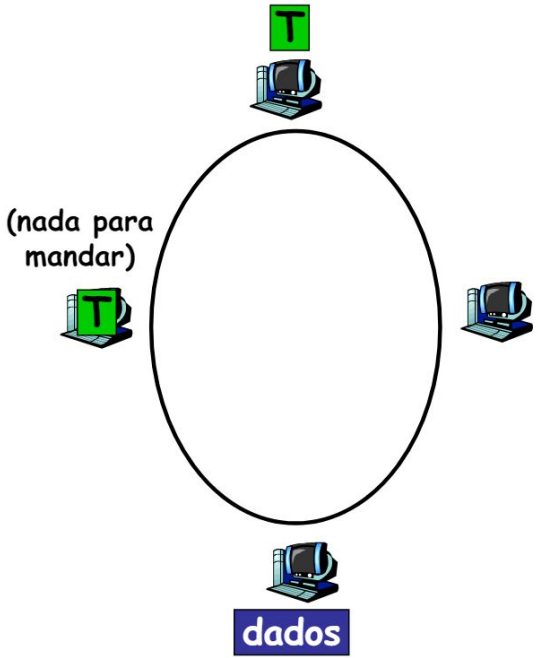
PROTOCOLOS DE REVEZAMENTO - PASSAGEM DE FICHA DE PERMISSÃO (*TOKEN*)

- Não existe estação centralizadora
- Ficha é a permissão para a transmissão de dados
  - A ficha nada mais é que um quadro de dados que é trocado entre os nós de forma circular
- Ficha é passada de estação a estação obedecendo uma ordem
  - Ao obter a ficha, a estação pode transmitir dados
  - Se a estação não possui dados a transmitir o token é repassado para o próximo nó
- Usada no Token Ring e no FDDI

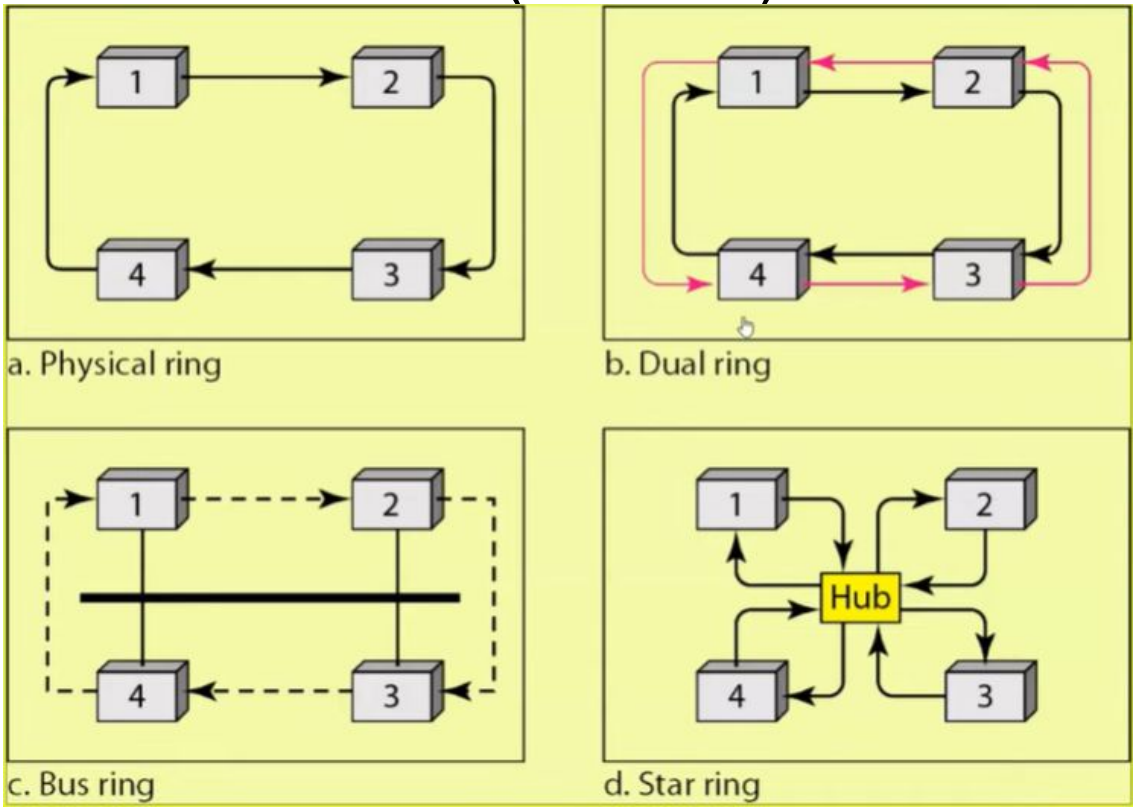
PROTOCOLOS DE REVEZAMENTO - PASSAGEM DE FICHA DE PERMISSÃO (*TOKEN*)

- Desvantagens:
  - A falha de um nó gera uma falha em toda a transmissão
  - Perda do token (estação com o token é desconectada)
  - Estação não libera o token

PROTOCOLOS DE REVEZAMENTO - PASSAGEM DE FICHA DE PERMISSÃO (*TOKEN*)



PROTOCOLOS DE REVEZAMENTO - PASSAGEM DE FICHA DE PERMISSÃO (*TOKEN*)



RESUMO DOS PROTOCOLOS MAC

- Divisão do canal por tempo, frequência ou código
  - Divisão de Tempo, Divisão de Frequência
- Acesso Aleatório
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - Escuta da portadora:
    - Fácil em algumas tecnologias (cabeadas), mas difícil em outras (sem fio)
    - CSMA/CD usado no Ethernet
    - CSMA/CA usado no IEEE 802.11 (WiFi)
- Revezamento
- Varredura (polling) a partir de um ponto central, reserva, passagem de permissões

REFERÊNCIAS

https://homepages.dcc.ufmg.br/~loureiro/rc/072/rc3_enlace_4pp

https://homepages.dcc.ufmg.br/~loureiro/rc/072/rc4_mac_4pp.pdf

https://www.gta.ufrj.br/~miguel/docs/redes/aula4.pdf

https://www.youtube.com/watch?v=KviHyRss-dE

https://www.geeksforgeeks.org/carrier-sense-multiple-access-csma/