

Camada de Enlace

Controle de Fluxo

Controle de Fluxo

- ❑ Emissor transmitindo mais rápido que o receptor pode aceitar. O que fazer?
- ❑ Algum mecanismo de *feedback* deve ser fornecido para que o emissor fique ciente das capacidades do receptor
- ❑ Várias dessas questões se repetem em outras camadas
- ❑ A solução a ser adotada para cada questão depende da camada, protocolo e aplicação.
- ❑ Essas questões são consideradas fundamentais no projeto de qualquer protocolo.

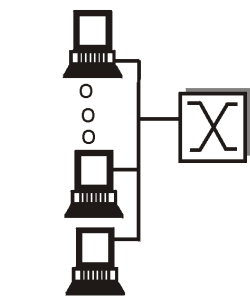
Controle de Fluxo

- ❑ Existem vários esquemas, a maioria baseada em regras sobre quando o emissor pode enviar o próximo quadro.
 - Emissor envia um quadro e espera sinal.
 - Receptor recebe o quadro.
 - Receptor envia sinal p/ emissor enviar próximos n quadros.
 - Emissor envia os quadros e espera sinal.

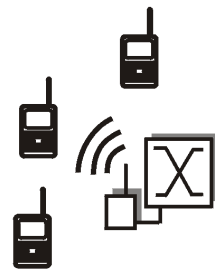
Enlaces de Acceso Múltiplo e Protocolos

Três tipos de enlaces:

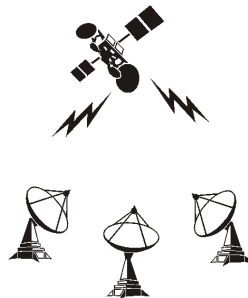
- ❑ ponto-a-ponto (fio único, ex. PPP, SLIP)
- ❑ **broadcast** (fio ou meio compartilhado; ex, Ethernet, Wavelan, etc.)



shared wire
(e.g. Ethernet)



shared wireless
(e.g. Wavelan)



satellite



cocktail party

- ❑ switched (ex., switched Ethernet, ATM etc)

Protocolos de Acesso Múltiplo

- ❑ canal de comunicação único e compartilhado
- ❑ duas ou mais transmissões pelos nós: interferência
 - apenas um nó pode transmitir com sucesso num dado instante de tempo
- ❑ *protocolo de múltiplo acesso:*
 - algoritmo distribuído que determina como as estações compartilham o canal, isto é, determinam quando cada estação pode transmitir
 - comunicação sobre o compartilhamento do canal deve utilizar o próprio canal!
 - o que procurar em protocolos de múltiplo acesso:
 - síncrono ou assíncrono
 - informação necessária sobre as outras estações
 - robustez (ex., em relação a erros do canal)
 - desempenho

Protocolos de Acesso Múltiplo

■ Características

- Quando apenas um nó tem dados para enviar, esse nó tem uma vazão de R bps
- Quando M nós têm acesso para enviar, cada um desses nós tem uma vazão de R/M bps. Isso não significa necessariamente que cada um dos M nós sempre terá uma velocidade média de transmissão de R/M durante algum intervalo de tempo adequadamente definido
- O protocolo é descentralizado, isto é, não há nós mestres que possam falhar e derrubar o sistema inteiro
- O protocolo é simples para que sua implementação seja barata

Protocolos MAC: uma taxonomia

Três grandes classes:

❑ Particionamento de canal

- dividem o canal em pedaços menores (compartimentos de tempo, frequência)
- aloca um pedaço para uso exclusivo de cada nó

❑ Acesso Aleatório

- permite colisões
- “recuperação” das colisões

❑ Passagem de Permissão

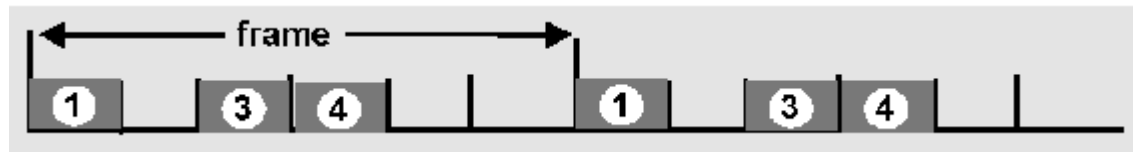
- compartilhamento estritamente coordenado para evitar colisões

Objetivo: eficiente, justo, simples,
descentralizado

Protocolos MAC com Particionamento de Canal: TDMA

TDMA: acesso múltiplo por divisão temporal

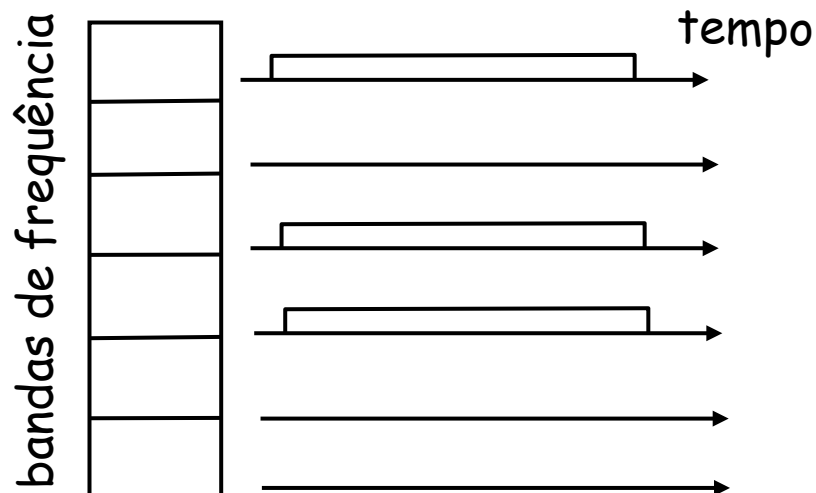
- ❑ acesso ao canal é feito por "turnos"
- ❑ cada estação controla um compartimento ("slot") de tamanho fixo (tamanho = tempo de transmissão de pacote) em cada turno
- ❑ compartimentos não usados são desperdiçados
- ❑ exemplo: rede local com 6 estações: 1,3,4 têm pacotes, compartimentos 2,5,6 ficam vazios



Protocolos MAC com Particionamento de Canal: FDMA

FDMA: acesso múltiplo por divisão de frequência

- ❑ o espectro do canal é dividido em bandas de frequência
- ❑ cada estação recebe uma banda de frequência
- ❑ tempo de transmissão não usado nas bandas de frequência é desperdiçado
- ❑ exemplo: rede local com 6 estações: 1,3,4 têm pacotes, as bandas de frequência 2,5,6 ficam vazias



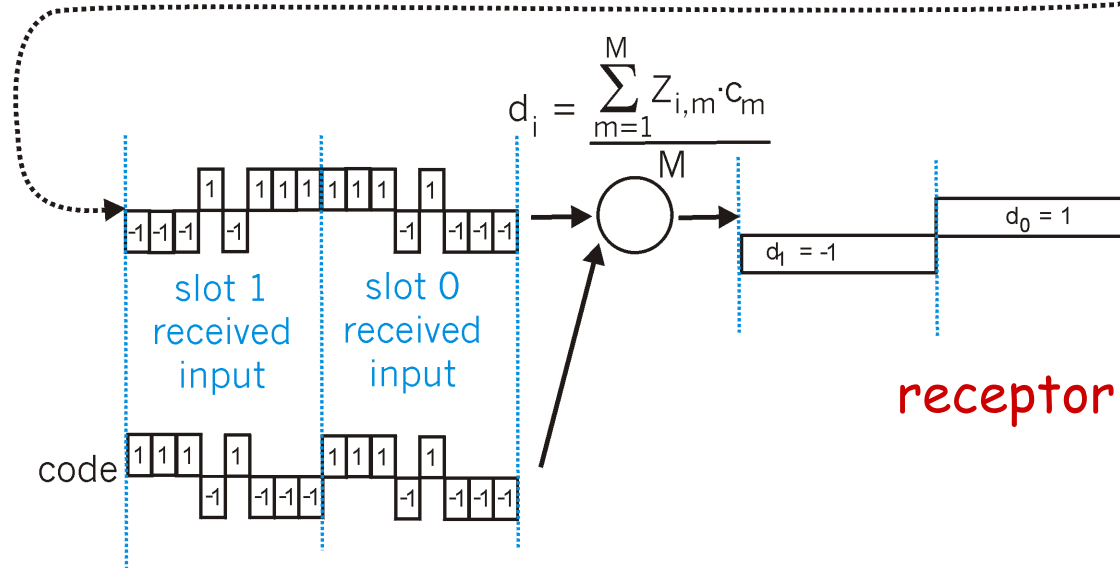
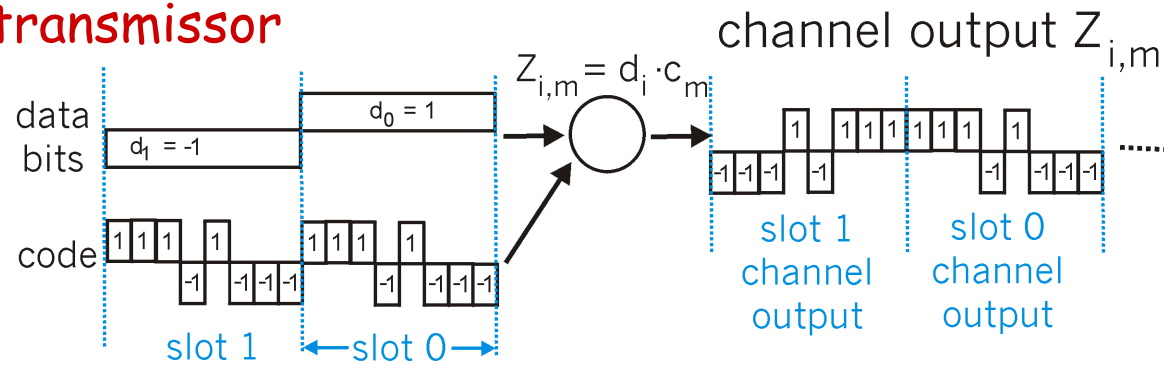
Particionamento de Canal (CDMA)

CDMA (Acesso Múltiplo por Divisão de Códigos)

- ❑ um código único é atribuído a cada usuário, isto é, o código define o particionamento
- ❑ muito usado em canais broadcast, sem-fio (celular, satellite, etc)
- ❑ todos os usuários usam a mesma frequência, mas cada usuário tem a sua própria maneira de codificar os dados. Esta codificação é definida pelo código que o usuário recebe (“*chipping sequence*”)
- ❑ *sinale codificado* = (dados originais) X (*chipping sequence*)
- ❑ *decodificação*: produto interno do sinal codificado e da sequência de codificação (“*chipping sequence*”)
- ❑ permite que múltiplos usuários “coexistam” e transmitam simultaneamente com mínima interferência (os códigos que minimizam a interferência são chamados “ortogonais”)

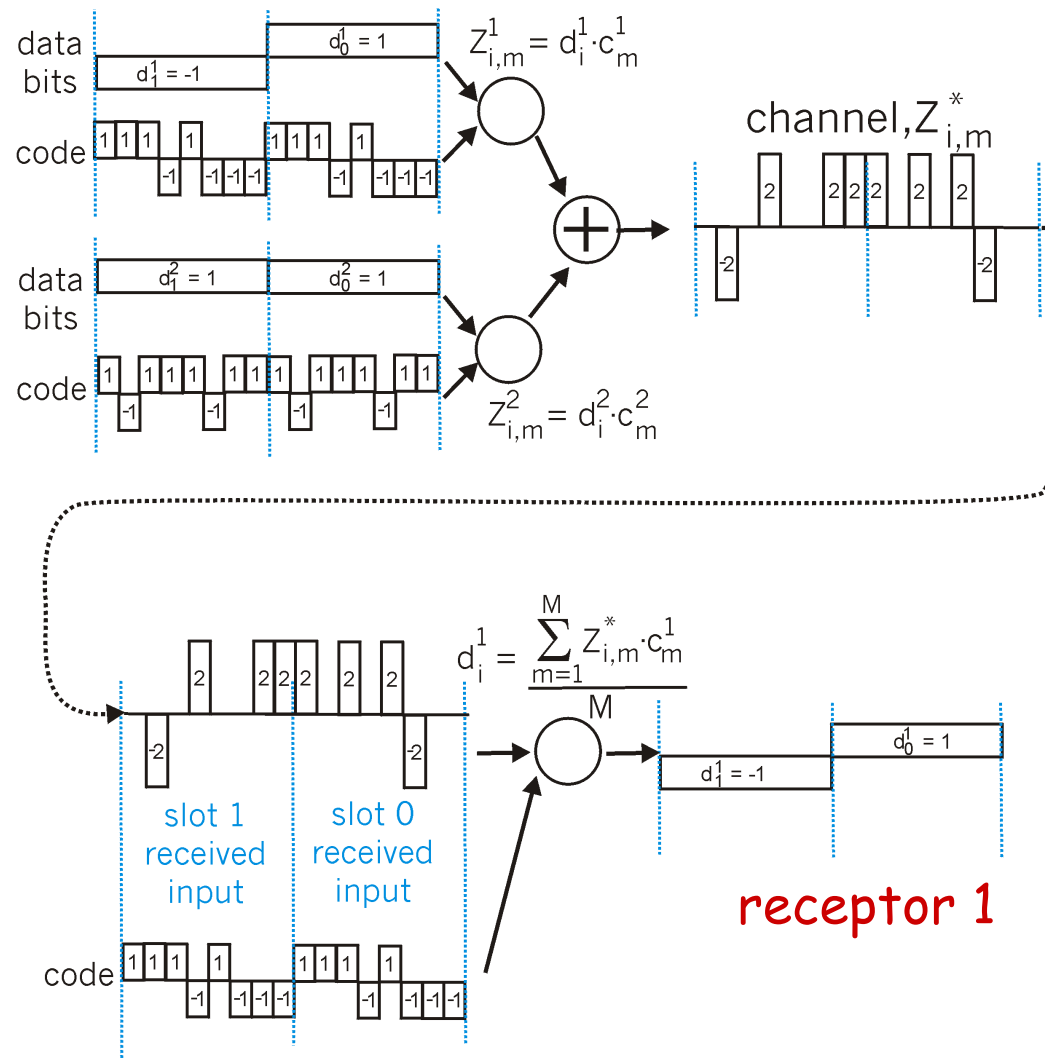
CDMA Codificação e Decodificação

transmissor



CDMA: interferência de dois transmissores

transmissores

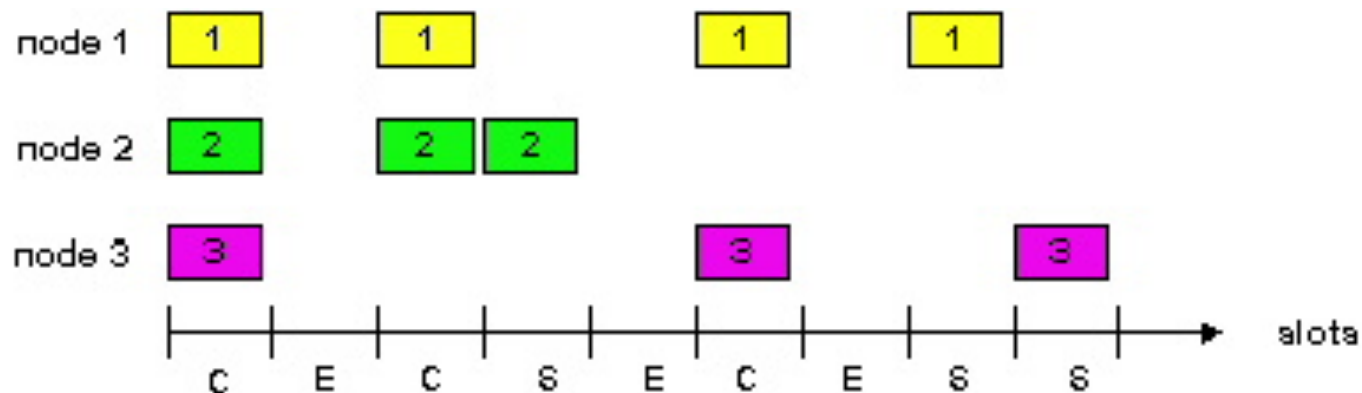


Protocolos de Acesso Aleatório

- ❑ Quando o nó tem um pacote a enviar:
 - transmite com toda a taxa do canal R.
 - não há uma regra de coordenação *a priori* entre os nós
- ❑ dois ou mais nós transmitindo -> “colisão”,
- ❑ **Protocolo MAC de acesso aleatório** especifica:
 - como detectar colisões
 - como as estações se recuperam das colisões (ex., via retransmissões atrasadas)
- ❑ Exemplos de protocolos MAC de acesso aleatório:
 - slotted ALOHA
 - ALOHA
 - CSMA e CSMA/CD

Slotted Aloha

- tempo é dividido em compartimentos de tamanho igual (= tempo de transmissão de um pacote)
- nó com pacote pronto: transmite no início do próximo compartimento
- se houver colisão: retransmite o pacote nos futuros compartimentos com probabilidade p , até que consiga enviar.



Compartimentos: Sucesso (S), Colisão (C), Vazio (E)

Eficiência do Slotted Aloha

P: qual a máxima fração de compartimentos com sucesso?

R: Suponha que N estações têm pacotes para enviar

- cada uma transmite num compartimento com probabilidade p
- prob. sucesso de transmissão, S , é:

por um único nó: $S = p (1-p)^{N-1}$

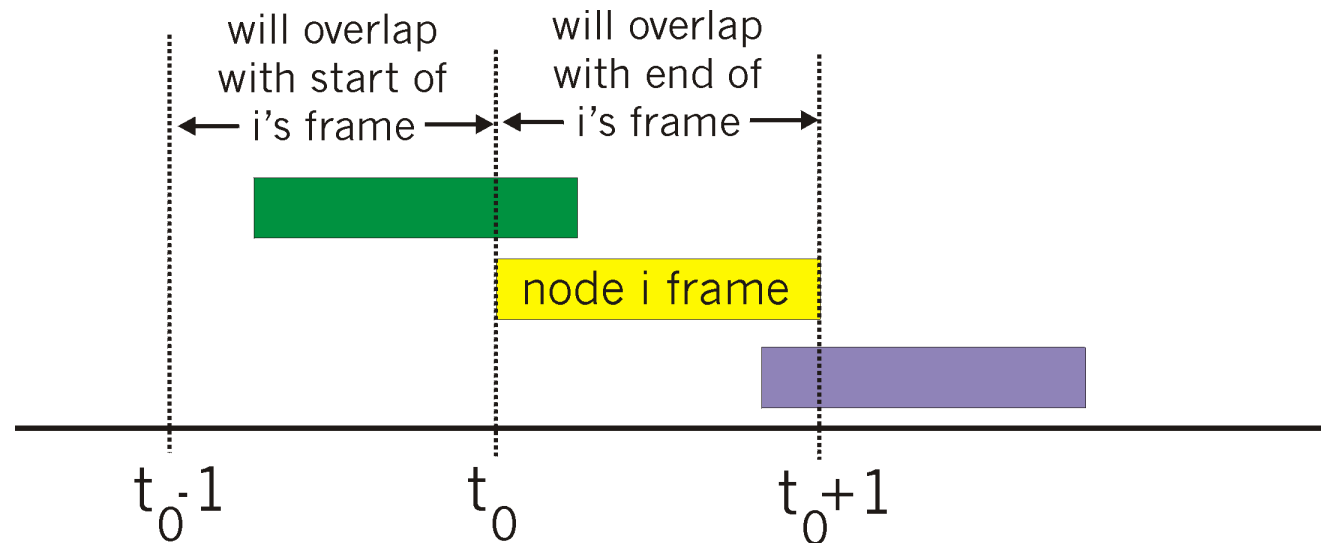
por qualquer um dos N nós

$$\begin{aligned} S &= \text{Prob (apenas um transmite)} \\ &= N p (1-p)^{N-1} \\ &\dots \text{escolhendo } p \text{ ótimo quando } N \rightarrow \text{infinito} \dots \\ &= 1/e = .37 \text{ quando } N \rightarrow \text{infinito} \end{aligned}$$

No máximo: uso do canal para envio de dados úteis: 37% do tempo!

ALOHA Puro (unslotted)

- ❑ unslotted Aloha: operação mais simples, não há sincronização
- ❑ pacote necessita transmissão:
 - enviar sem esperar pelo início de um compartimento
- ❑ a probabilidade de colisão aumenta:
 - pacote enviado em t_0 colide com outros pacotes enviados em $[t_0-1, t_0+1]$



Aloha Puro (cont.)

$P(\text{sucesso por um dado nó}) = P(\text{nó transmite}) \cdot$

$P(\text{outro nó não transmite em } [t_0-1, t_0]) \cdot$

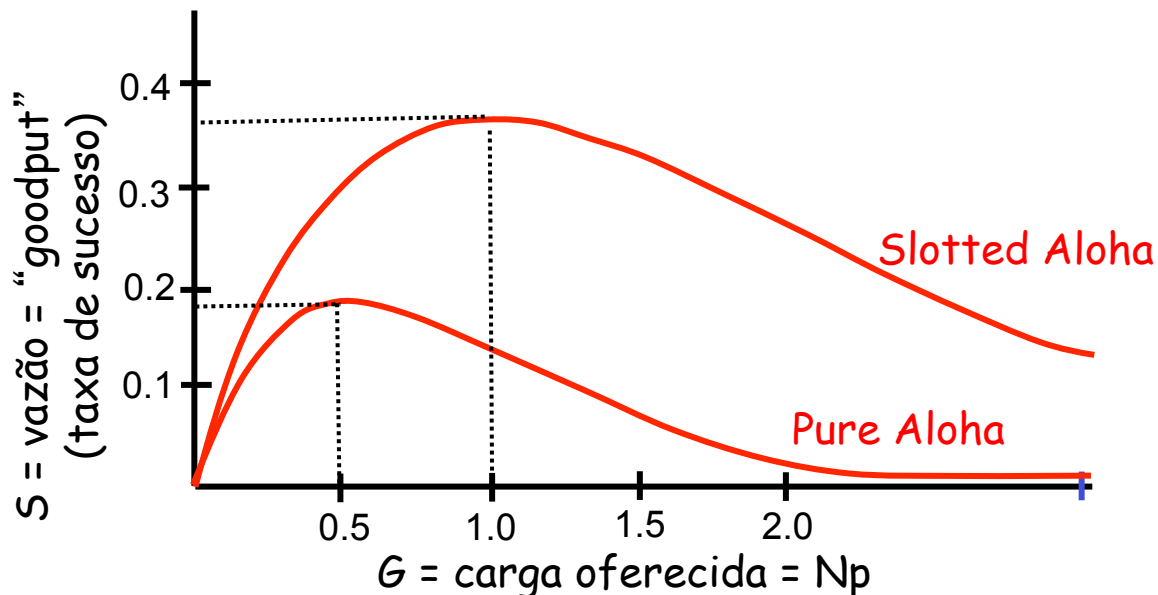
$P(\text{outro nó não transmite em } [t_0, t_0+1])$

$$= p \cdot (1-p) \cdot (1-p)$$

$P(\text{sucesso por um qualquer dos } N \text{ nós}) = N p \cdot (1-p) \cdot (1-p)$

... escolhendo p ótimo quando $n \rightarrow \text{infinito}$...

$$= 1/(2e) = .18$$



protocolo limita a vazão efetiva do canal!

CSMA: Carrier Sense Multiple Access

CSMA: escuta antes de transmitir:

- ❑ Se o canal parece vazio: transmite o pacote
- ❑ Se o canal está ocupado, adia a transmissão
 - **CSMA Persistente**: tenta outra vez imediatamente com probabilidade p quando o canal se torna livre (pode provocar instabilidade)
 - **CSMA Não-persistente**: tenta novamente após um intervalo aleatório
- ❑ analogia humana: não interrompa os outros!

Colisões no CSMA

colisões podem ocorrer:

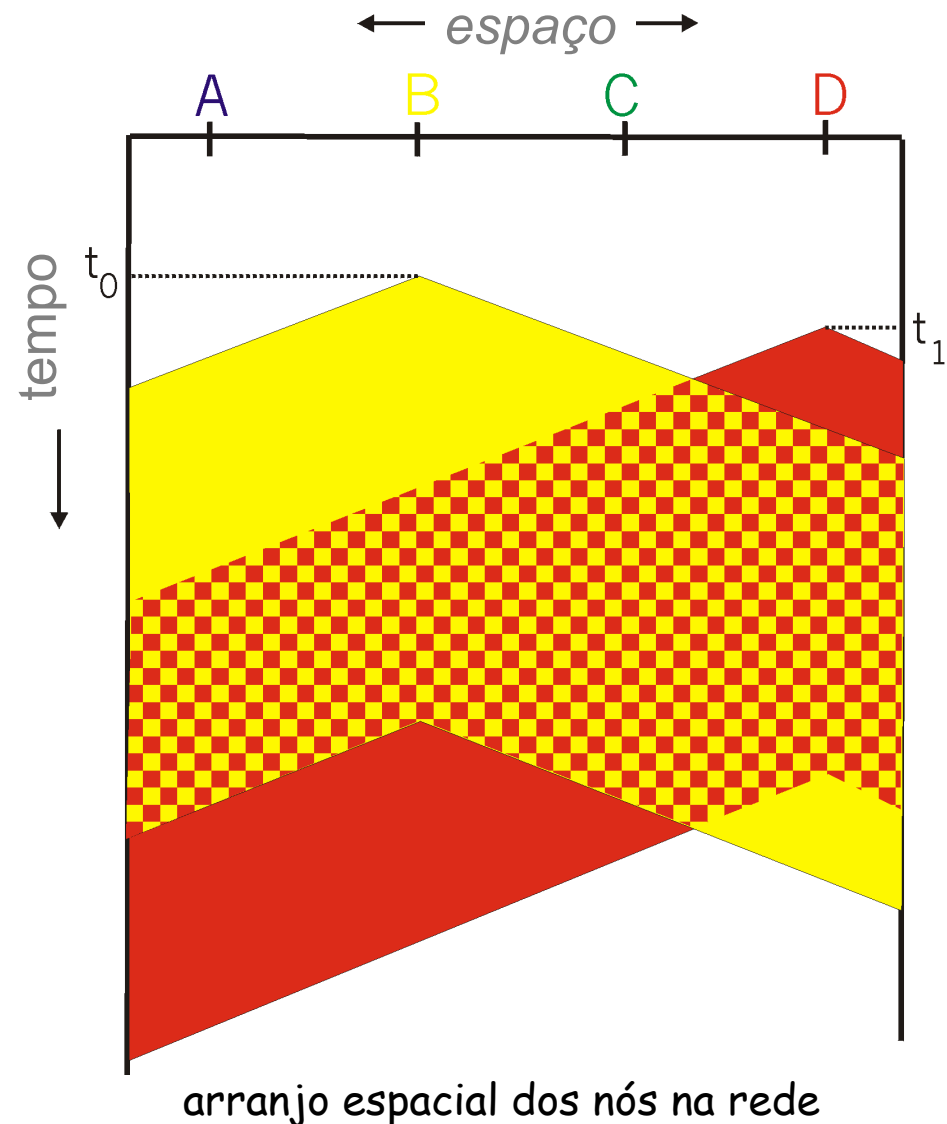
o atraso de propagação implica que dois nós podem não ouvir as transmissões de cada outro

colisão:

todo o tempo de transmissão do pacote é desperdiçado

nota:

papel da distância e do atraso de propagação na determinação da probabilidade de colisão.



CSMA/CD (Detecção de Colisão)

CSMA/CD: detecção de portadora

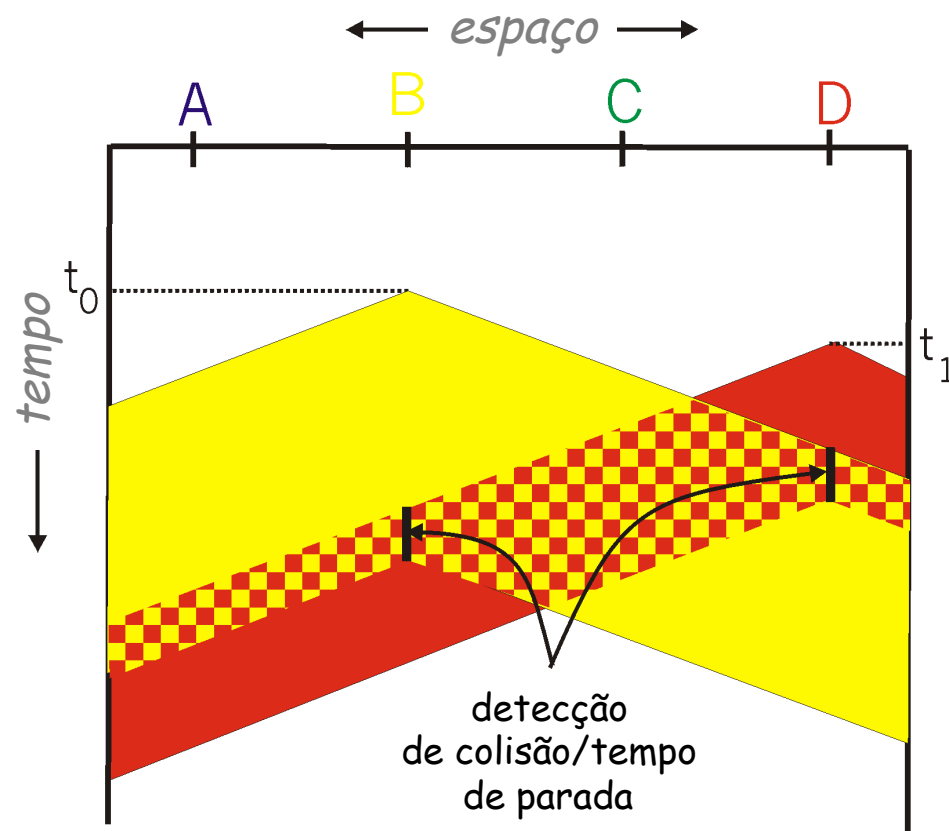
- colisões *detectadas* num tempo mais curto
- transmissões com colisões são interrompidas, reduzindo o desperdício do canal
- retransmissões persistentes ou não-persistentes

□ detecção de colisão:

- fácil em LANs cabeadas: medição da intensidade do sinal, comparação dos sinais transmitidos e recebidos
- difícil em LANs sem fio: receptor desligado enquanto transmitindo

□ analogia humana: o “bom-de-papo” educado

CSMA/CD detecção de colisão



Protocolos MAC com Passagem de Permissão

Protocolos MAC com particionamento de canais:

- compartilham o canal eficientemente quando a carga é alta e bem distribuída
- ineficiente nas cargas baixas: atraso no acesso ao canal. A estação consegue uma banda de $1/N$ da capacidade do canal, mesmo que haja apenas 1 nó ativo!

Protocolos MAC de acesso aleatório

- eficiente nas cargas baixas: um único nó pode usar todo o canal
- cargas altas: excesso de colisões

Protocolos de passagem de permissão

buscam o melhor dos dois mundos!

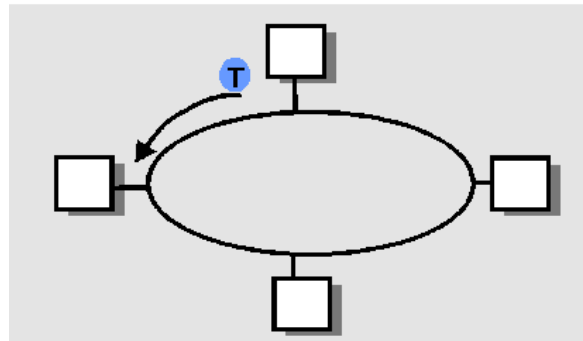
Protocolos MAC com Passagem de Permissão

Polling:

- ❑ nó mestre “convida” os escravos a transmitirem um de cada vez
- ❑ Mensagens Request to Send e Clear to Send
- ❑ problemas:
 - polling overhead
 - latência
 - ponto único de falha (mestre)

Token passing:

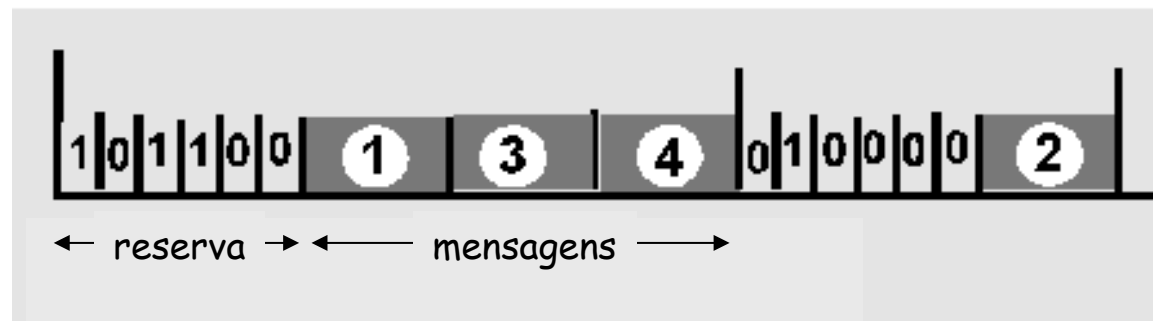
- ❑ controla um **token** passado de um nó a outro sequencialmente.
- ❑ mensagem token
- ❑ problemas:
 - token overhead
 - latência
 - ponto único de falha (token)



Protocolos de Reserva

Polling distribuído:

- ❑ O tempo é dividido em compartimentos (“slots”)
- ❑ começa com N **compartimentos de reserva**, mais curtos
 - tempo do compartimento de reserva é igual ao atraso de propagação fim-a-fim do canal
 - estação com mensagem a enviar faz uma reserva
 - reserva é vista por todas as estações
- ❑ depois dos compartimentos de reserva ocorre a transmissão das mensagens ordenadas pelas reservas e pelas prioridades de transmissão



Sumário dos protocolos MAC

- ❑ Como se faz com um canal compartilhado?
 - Particionamento de canal, no tempo, por frequência ou por código
 - Divisão temporal, divisão por código, divisão por frequência
 - Particionamento aleatório (dinâmico),
 - ALOHA, S-ALOHA, CSMA, CSMA/CD
 - detecção de portadora: fácil em alguns meios físicos (cabos) e difícil em outros (wireless)
 - CSMA/CD usado na rede Ethernet
 - Passagem de permissão
 - polling a partir de um site central, passagem de token

Adicionando os cabeçalhos e trailers

- ❑ Na camada de enlace de dados, cabeçalhos e trailers são adicionados aos dados da camada superior. O cabeçalho e o trailer contêm informações de controle destinadas à camada de enlace de dados no sistema de destino. O conjunto Cabeçalho + Dados + Trailer da camada de enlace chamamos de Quadro. Um quadro é uma unidade de dados de protocolo (PDU – Protocol data unit) da camada interface de rede.

O quadro Ethernet é definido da seguinte forma:

	Preâmbulo	SFD	Endereço de Destino	Endereço de Origem	Comprimento/Tipo	Dados Enchimento	FCS
Nº Bytes	7	1	6	6	2	46 a 1500	4

O Quadro Ethernet

- ❑ O Preâmbulo é um padrão de uns e zeros alternados usado para a sincronização da temporização em Ethernet assíncrona de 10 Mbps e em implementações mais lentas. As versões mais rápidas da Ethernet são síncronas, e essa informação de temporização é redundante mas mantida para fins de compatibilidade.
- ❑ Um Delimitador de Início de Quadro (SDF - Start Frame Delimeter) consiste em um campo de um octeto que marca o final das informações de temporização e contém a sequência de bits 10101011.

O Quadro Ethernet

- ❑ O campo Endereço de Destino contém um endereço de destino MAC. O endereço de destino pode ser *unicast*, *multicast* ou *broadcast*.
- ❑ O campo Endereço de Origem contém um endereço de origem MAC. O endereço de origem é geralmente o endereço *unicast* do nó Ethernet que está transmitindo. Existe, contudo, um crescente número de protocolos virtuais em uso que utiliza, e às vezes, compartilha um endereço MAC de origem específico para identificar a entidade virtual.

O Quadro Ethernet

- ❑ O campo Comprimento/Tipo suporta dois usos diferentes. Se o valor for inferior a 1536 decimal, 0x600 (hexadecimal), então o valor indica o comprimento. O valor do tipo especifica o protocolo da camada superior que recebe os dados depois que o processamento da Ethernet estiver concluído. O tamanho indica o número de bytes de dados que vêm depois desse campo.

O Quadro Ethernet

- ❑ O campo Dados e o Enchimento, se necessário, pode ser de qualquer tamanho que não faça com que o quadro exceda o tamanho máximo permitido para o quadro. A MTU (Unidade de Transmissão Máxima) para Ethernet é de 1500 octetos. Portanto, os dados não devem exceder esse tamanho. O conteúdo desse campo não é especificado. Um enchimento não especificado será inserido imediatamente após os dados do usuário quando não houver dados de usuário suficientes para que o quadro satisfaça o comprimento mínimo para o quadro. A Ethernet exige que o quadro tenha entre 64 e 1518 octetos. Esse processo de inserção de dados para complementar um quadro muito pequeno é chamado de padding (enchimento).

O Quadro Ethernet

- ❑ Uma FCS, *Frame Check Sequence* (CRC Checksum) contém um valor CRC de 4 bytes que é criado pelo dispositivo emissor e recalculado pelo dispositivo receptor para verificar se há quadros danificados. Já que a corrupção de um único bit em qualquer lugar desde o início do Endereço de Destino até o final do campo FCS fará com que o checksum seja diferente, o cálculo do FCS inclui o próprio campo FCS. Não é possível distinguir entre a corrupção do próprio FCS e a corrupção de qualquer outro campo usado no cálculo.

Juntando os Pedacos

- No processo de **envio** de algum dado, a camada de enlace pega os dados, encapsula-os com um cabeçalho e trailer, preenchendo os campos Mac de origem e destino (função de endereçamento), o campo comprimento/tipo (identificação de conteúdos) e o campo FCS (detecção de erros). Antes de transmitir ele verifica se tem alguém transmitindo e ao transmitir verifica se houve colisão (arbitragem).

Na **recepção**, é verificada se o endereço de destino do quadro é igual ao endereço da placa de rede (endereçamento), é realizado novamente o cálculo do FCS e comparado com o original (verificação de erros) os cabeçalhos e trailers são removidos e os dados são passados para a camada superior competente (identificação de conteúdos).

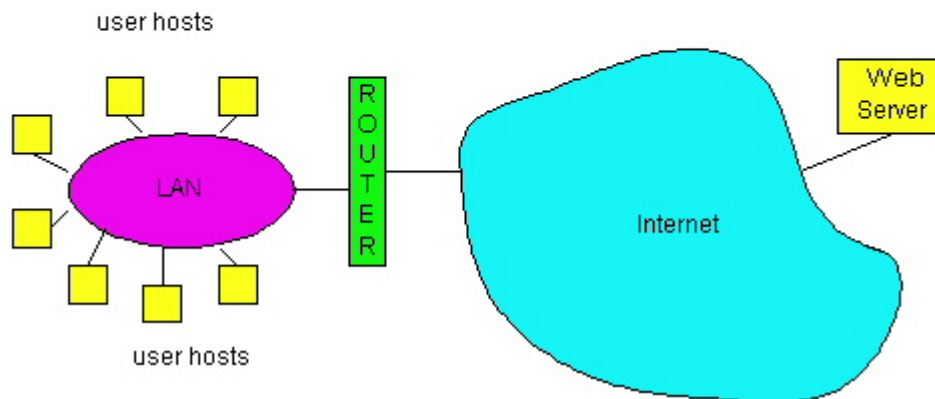
Tecnologias de LAN

Camada de enlace até agora:

- serviços, detecção de erros/correção, acesso múltiplo

A seguir: tecnologias de redes locais (LAN)

- endereçamento
- Ethernet
- pontes, switches
- 802.11
- PPP
- ATM



Endereços de LAN e ARP

Endereços IP de 32-bit:

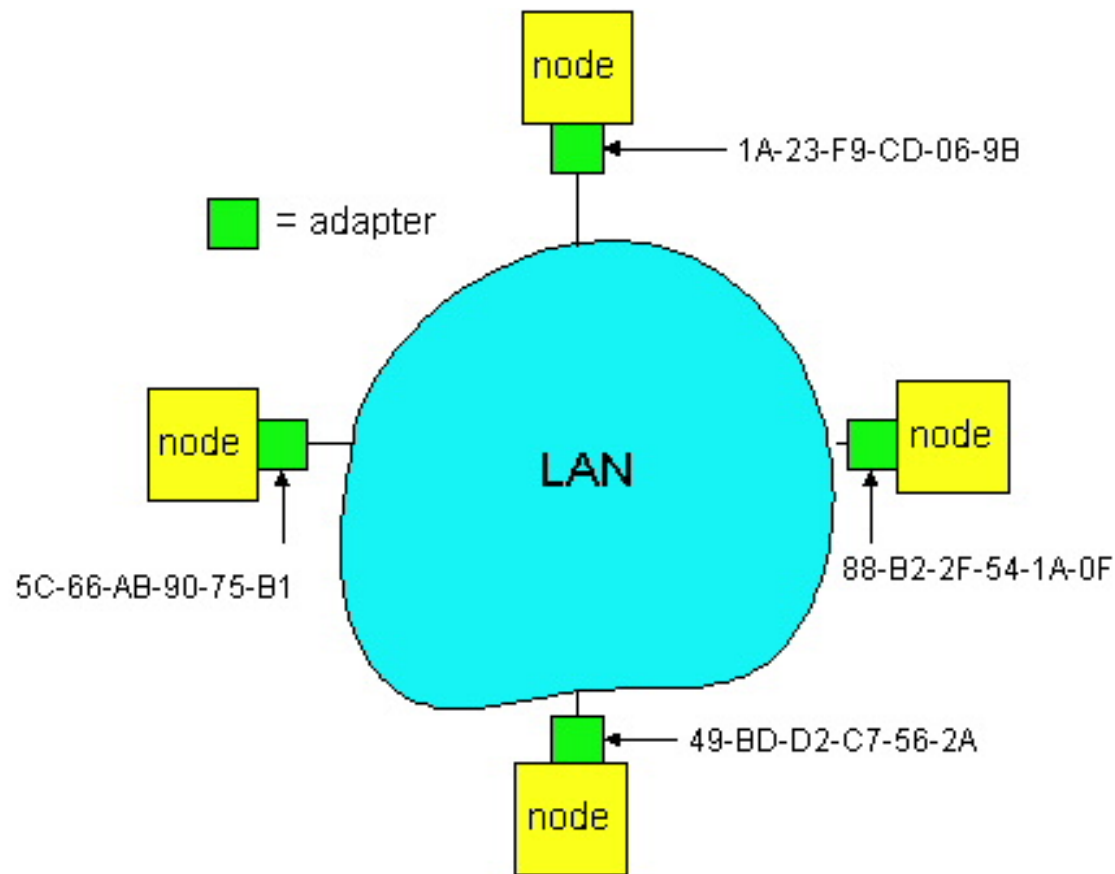
- ❑ endereços da *camada de rede*
- ❑ usados para levar o datagrama até a rede de destino

Endereço de LAN (ou MAC ou físico):

- ❑ usado para levar o datagrama de uma interface física a outra fisicamente conectada com a primeira (isto é, na mesma rede)
- ❑ Endereços MAC com 48 bits (na maioria das LANs) gravado na memória fixa (ROM) do adaptador de rede

Endereços de LAN e ARP

Cada adaptador numa LAN tem um único endereço de LAN



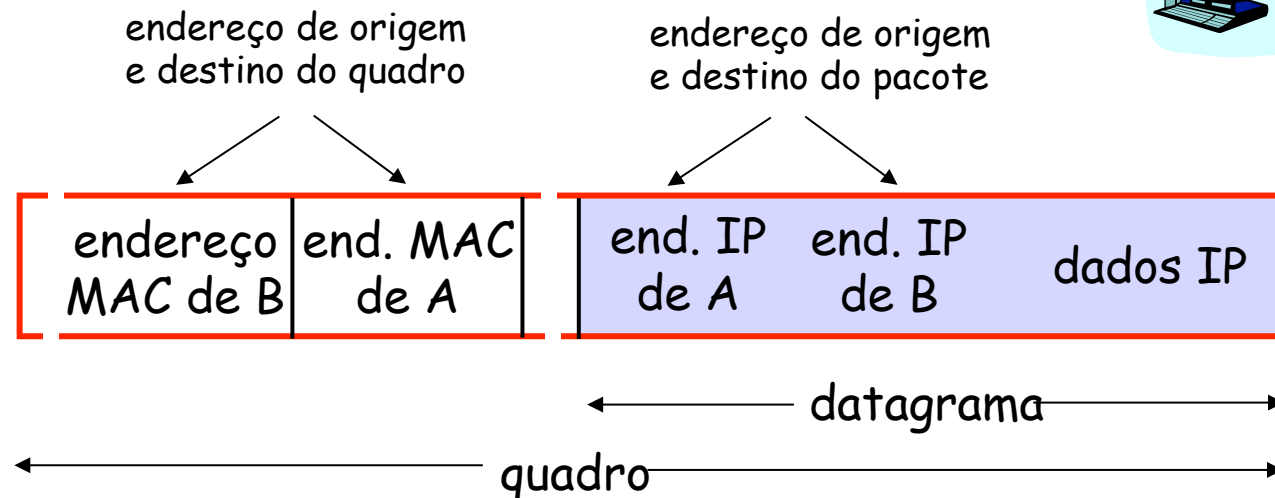
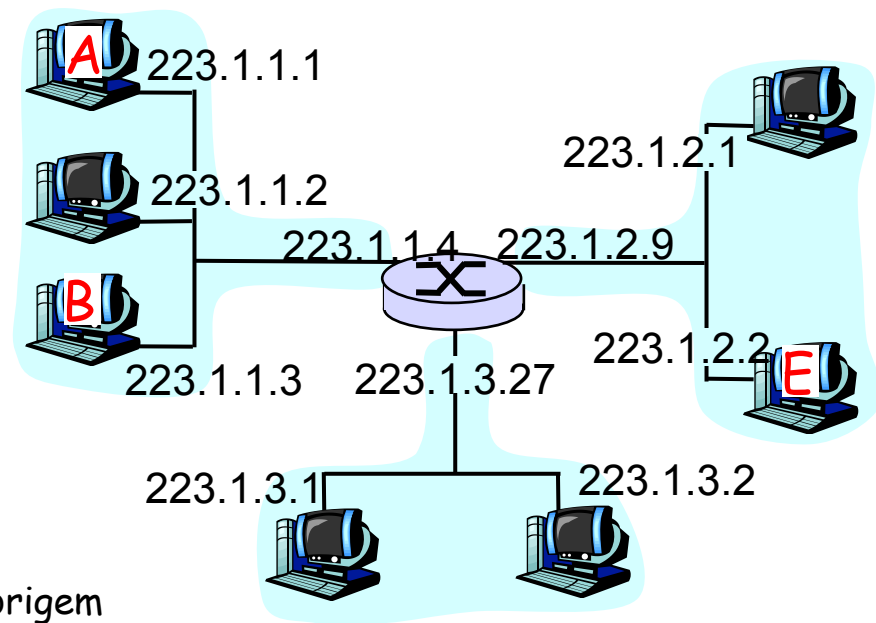
Endereços de LAN (mais)

- ❑ A alocação de endereços MAC é administrada pelo IEEE
- ❑ O fabricante compra porções do espaço de endereço MAC (para assegurar a unicidade)
- ❑ Analogia:
 - (a) endereço MAC: semelhante ao número do RG
 - (b) endereço IP: semelhante a um endereço postal
- ❑ endereçamento MAC é “flat” => portabilidade
 - é possível mover uma placa de LAN de uma rede para outra sem reconfiguração de endereço MAC
- ❑ endereçamento IP “hierárquico” => NÃO portátil
 - depende da rede na qual se está ligado

Lembre a discussão anterior sobre roteamento

Começando em A, dado que o datagrama está endereçado para B (endereço IP):

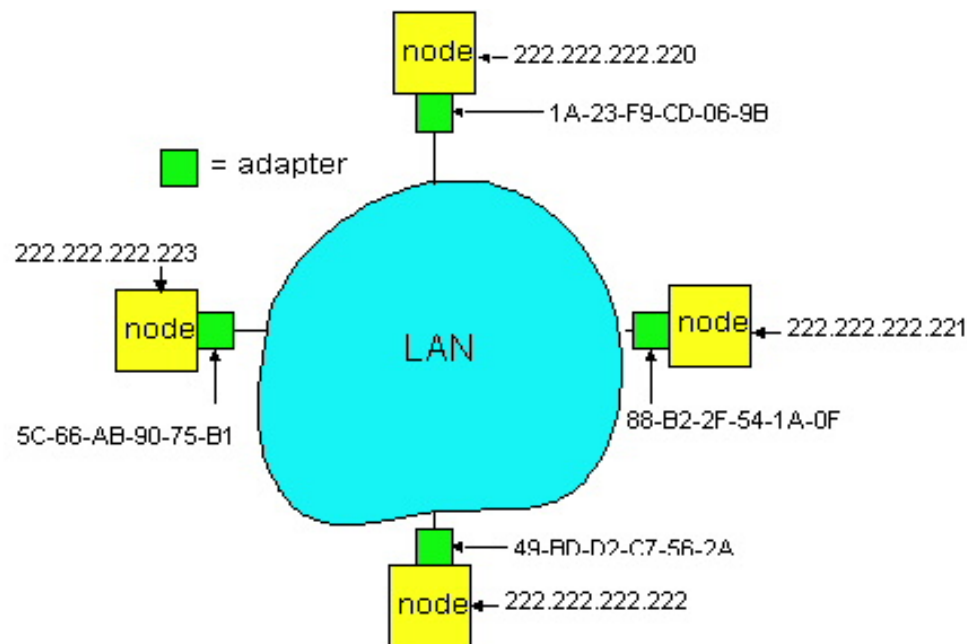
- procure rede.endereço de B, encontre B em alguma rede, no caso igual à rede de A
- **camada de enlace envia datagrama para B dentro de um quadro da camada de enlace**



ARP: Address Resolution Protocol

(Protocolo de Resolução de Endereços)

Questão: como determinar o endereço MAC de B dado o endereço IP de B?



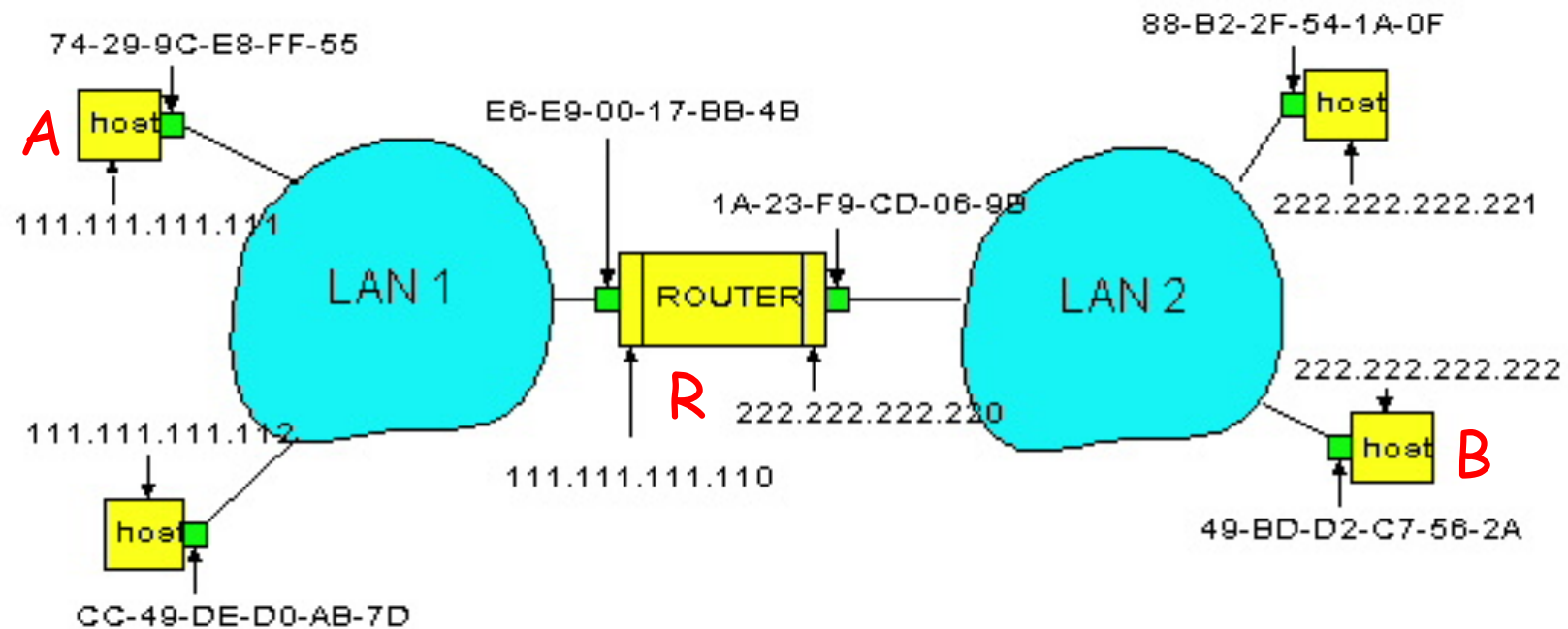
- ❑ Cada nó IP (Host, Roteador) numa LAN tem um módulo e uma tabela **ARP**
- ❑ Tabela ARP: mapeamento de endereços IP/MAC para alguns nós da LAN
< endereço IP; endereço MAC; TTL >
< >
- TTL (Time To Live): tempo depois do qual o mapeamento de endereços será esquecido (tipicamente 20 min)

Protocolo ARP

- ❑ A conhece o endereço IP de B, quer aprender o endereço físico de B
- ❑ A envia em **broadcast** um pacote ARP de consulta contendo o endereço IP de B
 - todas as máquinas na LAN recebem a consulta ARP
- ❑ B recebe o pacote ARP, responde a A com o seu (de B) endereço de camada física
- ❑ A armazena os pares de endereço IP-físico até que a informação se torne obsoleta (esgota a temporização)
 - soft state: informação que desaparece com o tempo se não for re-atualizada

Roteamento para outra LAN

caminho: roteamento de A para B via R



- ❑ Na tabela de roteamento no Host origem, encontra o roteador 111.111.111.110
- ❑ Na tabela de ARP na origem, encontra o endereço MAC E6-E9-00-17-BB-4B, etc

- ❑ A cria o pacote IP com origem A, destino B
- ❑ A usa ARP para obter o endereço de camada física de R correspondente ao endereço IP 111.111.111.110
- ❑ A cria um quadro Ethernet com o endereço físico de R como destino, o quadro Ethernet contém o datagrama IP de A para B
- ❑ A camada de enlace de A envia o quadro Ethernet
- ❑ A camada de enlace de R recebe o quadro Ethernet
- ❑ R remove o datagrama IP do quadro Ethernet, verifica que ele se destina a B
- ❑ R usa ARP para obter o endereço físico de B
- ❑ R cria quadro contendo um datagrama de A para B e envia para B

