

Camada de Enlace

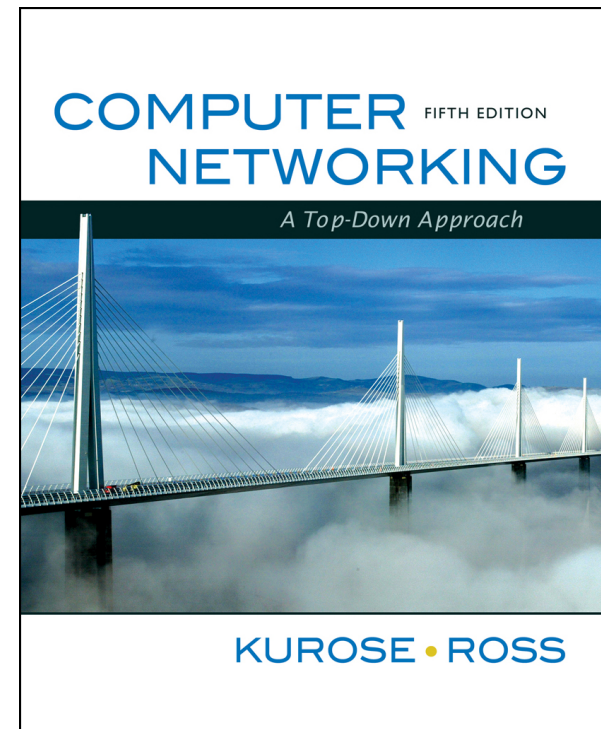
André Soares

Aviso

- Parte destes slides são inspirados ou foram retirados dos slides fornecidos com o livro:

*Computer Networking: A
Top Down Approach ,
5th edition.*

*Jim Kurose, Keith Ross
Addison-Wesley, April
2009.*



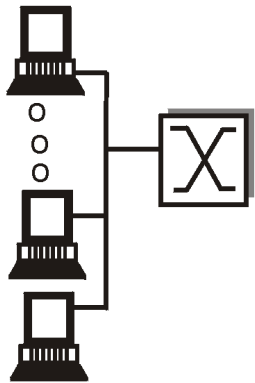
Roteiro

- Serviços da camada de Enlace
- Protocolos de acesso ao meio
- Ethernet
- ARP
- Dispositivos de interconexão

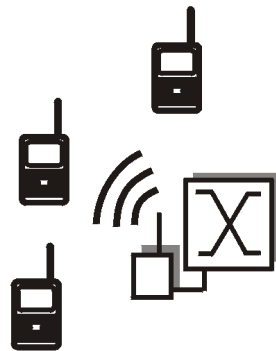
Protocolos de múltiplos acessos

Dois tipos e enlace”:

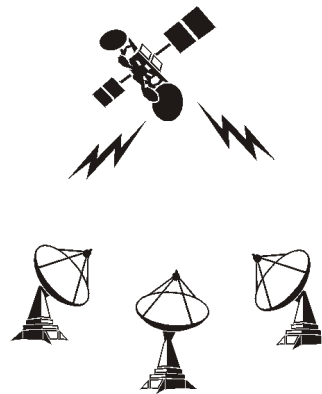
- Ponto a ponto
 - PPP para acesso de conexão discada
 - Enlace ponto a ponto entre um switch Ethernet e um host
- **broadcast** (cabo ou um meio compartilhado)
 - tradicional Ethernet
 - 802.11 wireless LAN



shared wire
(e.g. Ethernet)



shared wireless
(e.g. Wavelan)



satellite



cocktail party

Serviços da camada de enlace

- **Enquadramento de dados:**
 - Encapsular datagrama dentro do frame, adicionar cabeçalho
 - Pode ser utilizados campos de controle no fim do quadro (trailer)
- **Acesso ao enlace**
 - Acessar o canal se o meio for compartilhado
 - Endereço MAC (*Medium Access Control*) usado no cabeçalho para identificar origem e destino
 - Diferente do endereço IP
 - Ponto a Ponto ou Broadcast
- **Entrega confiável entre nós adjacentes**
 - Raramente usado em enlaces com baixa taxa de erro (fibra, alguns par trançado)
 - *wireless* : alta taxa de erro
 - Reconhecimento e retransmissões
 - Q. Por que serviço de entrega confiável tanto na camada de enlace como na camada de transporte?
 - R. No caso de erros evita a retransmissão fim a fim

Serviços da camada de enlace

- *Controle de fluxo:*
 - Os nós de cada extremidade tem capacidade limitada de armazenar quadros
 - Evitar que um nó transmissor com maior capacidade de processamento congestionue o nó receptor
- *Deteção de erro:*
 - Erros causados por atenuação do sinal, ruído
 - Receptor detecta presença de erros
 - Sinaliza o emissor para retransmitir ou descarta o frame
 - É necessária a utilização de informações de controle para a detecção de erros
- *Correção de erro:*
 - Receptor identifica e corrige o bit errado sem necessidade de retransmissão
- *Half-duplex e full-duplex*
 - Half, transmissão nos dois sentidos mas não ao mesmo tempo
 - Full, transmissão nos dois sentidos ao mesmo tempo

Protocolos de múltiplos acessos

- Único canal de broadcast (difusão) compartilhado
- 2 ou mais nós podem transmitir simultaneamente:
 - **colisão** se um nó recebe dois ou mais sinais ao mesmo tempo

Protocolo de múltiplo acesso

- Algoritmo distribuído que determina como os nós compartilham o canal, i.e., determina quando um nó pode transmitir
- Na comunicação através de um canal compartilhado, o nó deve ter o canal para si próprio
 - Não é utilizado um canal fora de banda para coordenação

Protocolo **ideal** de múltiplo acesso

Canal de broadcast com taxa de R bps

1. Quando um nó quer transmitir, ele pode enviar numa taxa de R bps
2. Quando M nós querem transmitir, cada nó envia numa taxa média de R/M bps
3. Totalmente descentralizado:
 - Nenhum nó especial para coordenar as transmissões
 - Sem sincronização de relógios, *slots*
4. Simples

Protocolos MAC : classificação

Três classes:

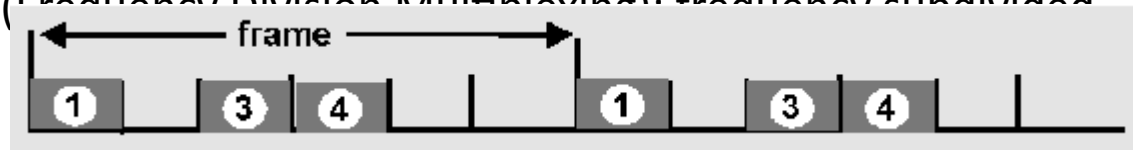
- **Divisão de canal**
 - Divide o canal em pequenos pedaços (slots de tempo, frequência, código)
 - Aloca esses pequenos pedaços para uso exclusivo dos nós
- **Acesso aleatório**
 - Canal não é dividido, permite colisões
 - “Recuperação” de colisões
- **Revezamento**

Protocolo MAC particionando o canal : TDMA

TDMA: Time Division Multiple Access

- Acesso ao canal em ciclos
- Cada estação possui um slot de tamanho fixo em cada ciclo
- Slots sem uso ficam ociosos (desperdício)
- Exemplo: 6-estações LAN, 1,3 e 4 possuem quadros para transmitir. Slots 2,5 e 6 ficam ociosos

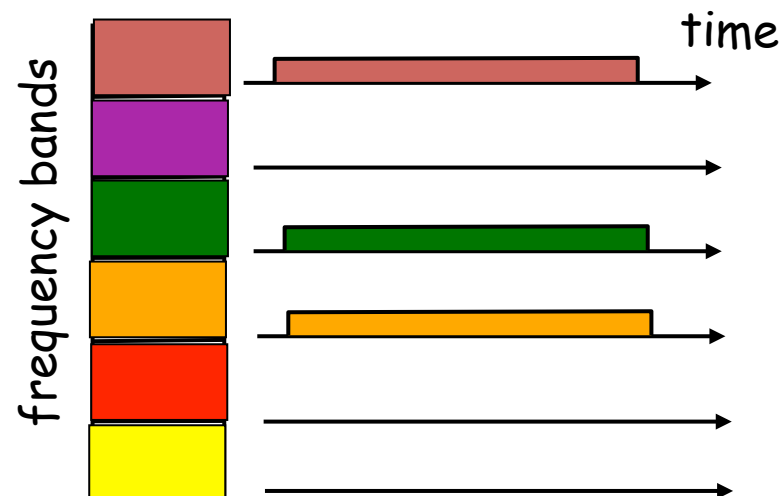
- TDM (Time Division Multiplexing): channel divided into N time slots, one per user; inefficient with low duty cycle users and at light load.
- FDM (Frequency Division Multiplexing): frequency subdivided



Protocolo MAC particionando o canal: FDMA

FDMA: frequency division multiple access

- Canal é dividido em freqüências de banda
 - Vários subcanais
- Para cada estação é atribuída um freqüência fixa (banda do subcanal)
- Subcanais ficam ociosos caso determinada estação não esteja transmitindo
- Exemplo: 6-estações LAN, 1,3 e 4 possuem quadros para transmitir.
freqüências 2,5 e 6 ficam ociosas



Protocolo de Acesso Aleatório

- Quando um nó tem quadros para transmitir
 - Transmite utilizando todo o canal, taxa R
 - Nenhuma coordenação entre a priori entre os nós
- Dois ou mais nós transmitindo = colisão
- **Protocolo MAC de acesso aleatório** especifica:
 - Como detectar colisões
 - Como recuperar após a ocorrência de colisões (e.g. aguardar um tempo antes de retransmissões)
- Exemplos:
 - slotted ALOHA
 - ALOHA
 - CSMA, CSMA/CD, CSMA/CA

CSMA (*Carrier Sense Multiple Access*)

CSMA: escuta o meio antes de transmitir:

Se o canal estiver desocupado: transmite quadro inteiro

- Se o canal estiver ocupado: adia a transmissão
- Análogo aos humanos: uns não “interropem” os outros

CSMA colisões

Colisões ainda podem ocorrer:

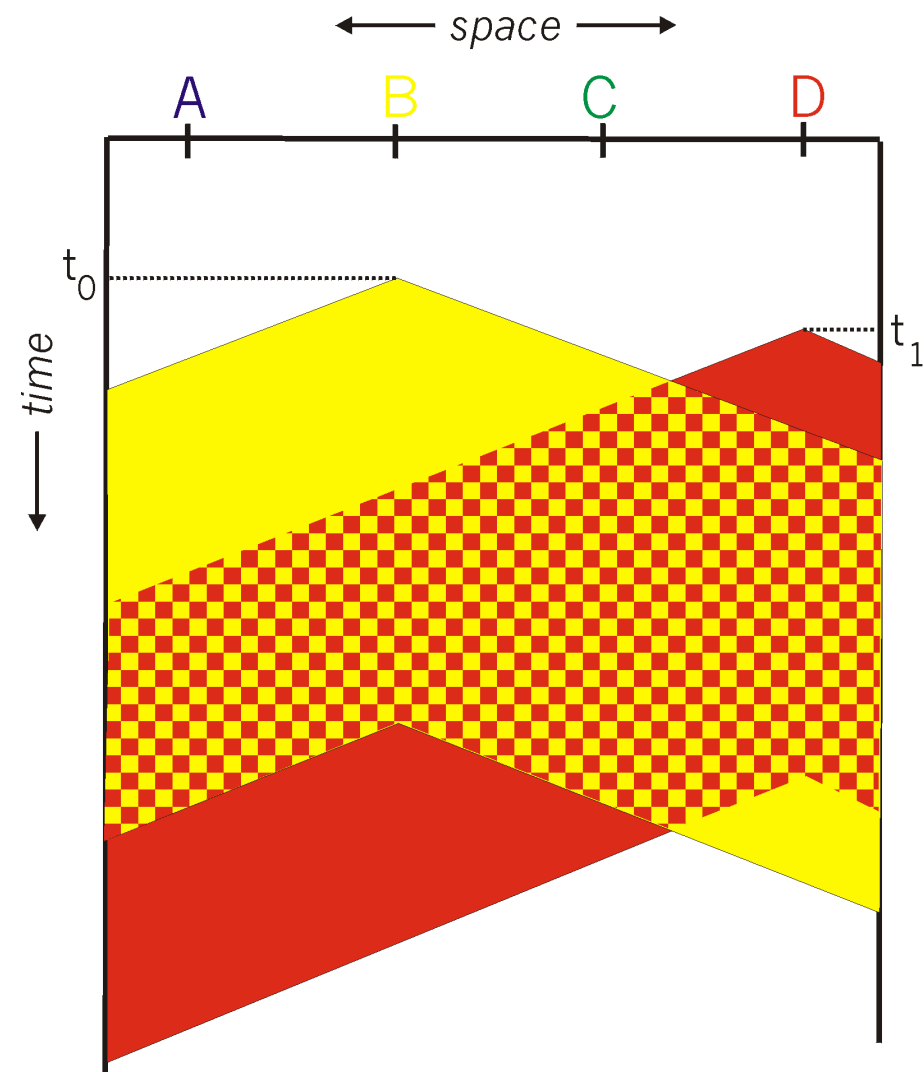
Atrasos de propagação significa que alguns nós podem não escutar a transmissão de outro nó

colisão:

Todo o tempo de transmissão do quadro é perdido

note:

Distância / propagação determina a probabilidade de colisão

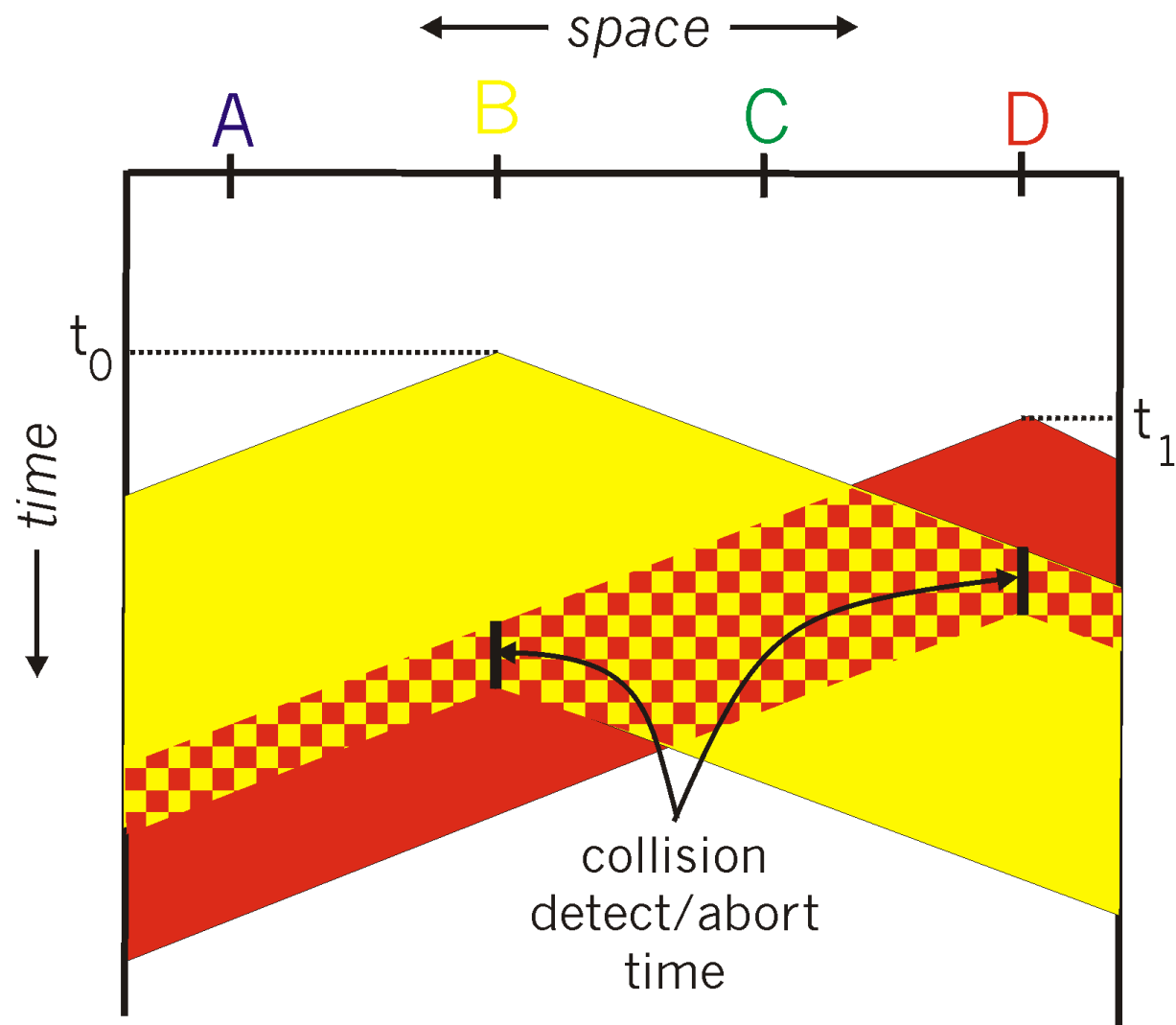


CSMA/CD (*Collision Detection*)

CSMA/CD:

- Detecção de colisão em curtos intervalos de tempo
- Havendo colisões a transmissão é abortada, reduz o tempo desperdiçado do canal
- Detecção de colisão:
 - Fácil de implementar em redes com fio
 - Difícil de implementar em redes sem fio
- É assim que os seres humanos conversam

CSMA/CD collision detection



Protocolos MAC “Revezamento”

Protocolos MAC com particionamento de canal :

- Canal compartilhado de forma eficiente e justo sob altas cargas
- Ineficiente sob baixas cargas: atraso no acesso ao canal, $1/N$ de banda alocada
 - mesmo existindo somente 1 nó ativo

Protocolos MAC de acesso aleatório

- Eficiente sob baixa carga: um único nó pode utilizar canal todo
- Alta carga: *collision overhead*

Protocolos MAC “Revezamento”

Procura ter o melhor dos dois mundos!

Protocolos MAC - Revezamento

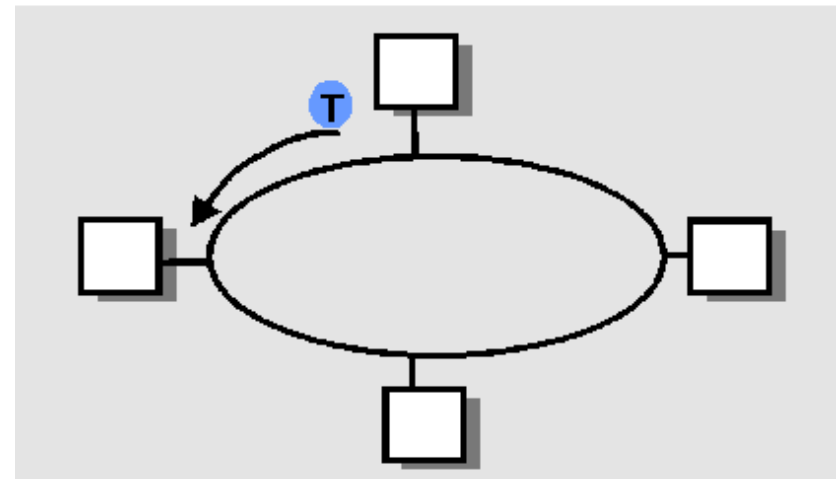
Seleção (*Polling*):

- Nó mestre convida nós escravos a transmitir em voltas (*turn*)
- problema:
 - Tempo da seleção (overhead)
 - latência
 - Simples ponto de falha (master)
- Nó mestre envia uma mensagem para o nó 1 dizendo que ele pode transmitir um n^o máx. de x quadros
- Depois do nó 1 o mestre faz o mesmo com o nó 2

Protocolos MAC - Revezamento

Passagem de permissão (Token passing):

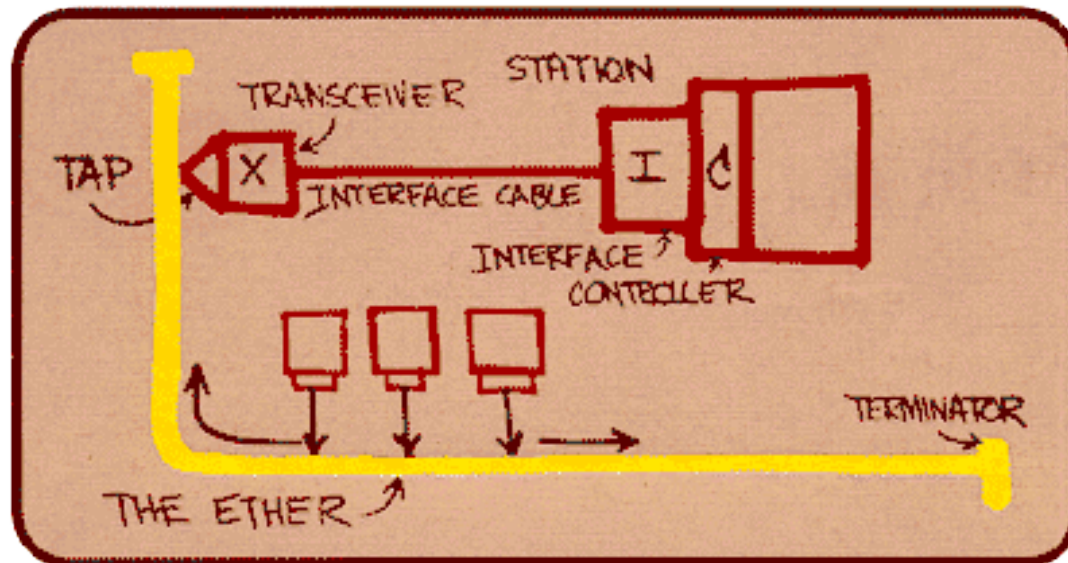
- Controle do token passado de um nó para o próximo nó
 - Ausência de nó mestre
 - Uso do token
 - problemas:
 - *token overhead*
 - latência
 - Simples ponto de falha (*token*)
- Um nó somente retém o *token* se tiver algo para transmitir.
 - Existe um número máximo de quadros que podem ser transmitidos



Ethernet

Domina tecnologia de LAN com cabo

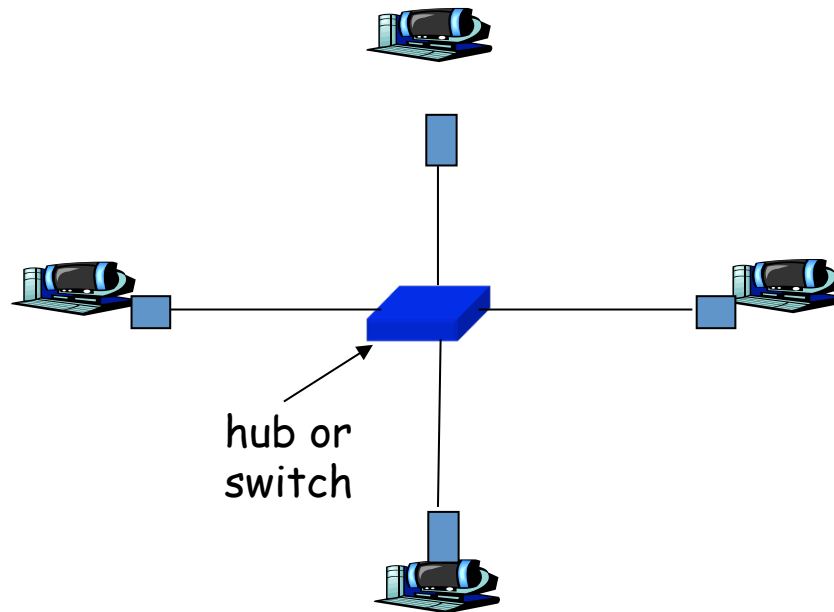
- Barato, R\$ 30,00 – 40,00 para 100Mbps!
- Primeira tecnologia LAN amplamente utilizada
- Mais simples, mais barata do que token LANs e ATM
- Trabalha com taxas de 10 Mbps – 10 Gbps



Metcalfe's Ethernet sketch

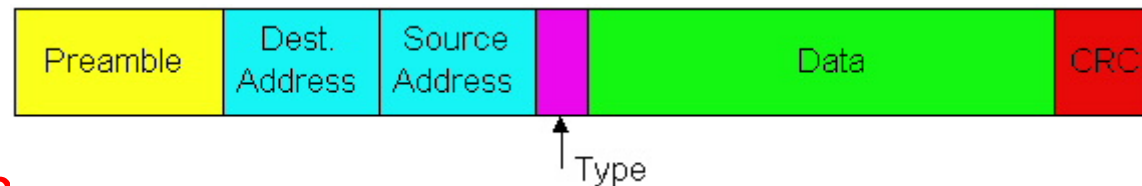
Topologia em estrela

- Topologia em barra, popular nos anos 90
- Agora prevalece topologia “estrela”
- Tipos de conexões: hub ou switch



Estrutura do quadro Ethernet

Adaptador do emissor encapsula datagrama IP (ou outro pacote da camada de rede) no **quadro Ethernet**

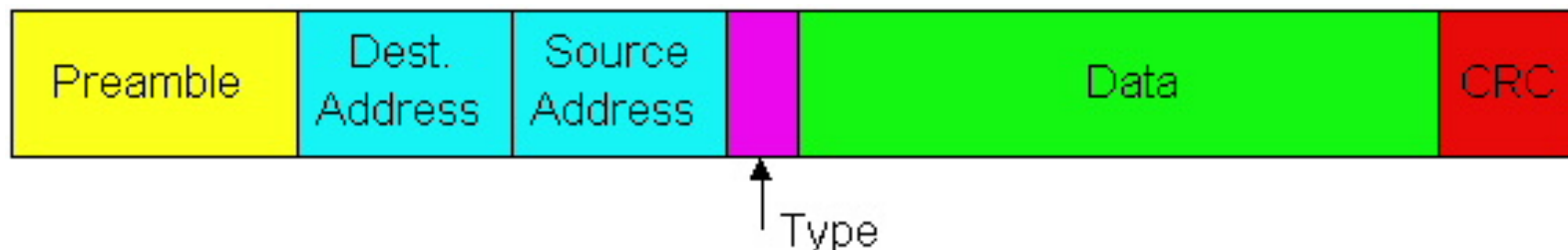


Preâmbulo: 7 bytes com padrão 10101010 seguidos de 1 byte com padrão 10101011

- 7 bytes com padrão 10101010 seguidos de 1 byte com padrão 10101011
- Usado para sincronizar receptor com o relógio do emissor

Estrutura do quadro Ethernet

- **Endereço: 6 bytes**
 - Se o adaptador recebe um quadro com endereço de destino, ou como endereço de broadcast (e.g. pacote ARP), ele passa os dados para a camada de rede
 - Caso contrário, adaptador descarta o quadro
- **Type: (2 bytes)** indica o protocolo da camada superior (na maioria é IP mas outros são suportados como Novell IPX e AppleTalk)
 - Hosts podem usar outro protocolo de rede junto com o IP
- **Dados: (46 a 1500 Bytes).**
 - Pode haver necessidade acrescentar bits para completar os 46 Bytes.
 - Esse “recheio” é removido no destino pela camada de rede analisando o tamanho do pacote IP
- **CRC: (4 Bytes)** verifica no receptor se algum erro foi detectado. Neste caso o quadro é descartado



Serviço não confiável não orientado à conexão

- **Sem conexão:** Nenhum acordo entre emissor e receptor
- **Não confiável:** receptor não envia acks ou nacks para o emissor.
 - No fluxo de datagramas passados para a camada de rede pode haver falhas
 - Falhas serão eliminadas se a aplicação usar TCP
 - Caso contrário, aplicação terá que identificar as falhas

Ethernet CSMA/CD algorithm

1. Adaptador recebe um datagrama da camada de rede e cria um quadro
2. Se o canal estiver livre ele transmite o quadro. Se o canal tiver ocupado ele espera o canal ficar livre e transmite o quadro
5. Se o adaptador transmitir o quadro inteiro sem detectar transmissão de outro adaptador então a transmissão foi feita sem colisão.
4. Se o adaptador detectar a transmissão de outro adaptador ele aborta a transmissão do quadro e manda o sinal de reforço
5. Depois entra em fase de **backoff exponential** : depois da m-ésima colisão, o adaptador escolhe K aleatoriamente de $\{0, 1, 2, \dots, 2^m-1\}$, onde $m = \min(m, 10)$.
O adaptador espera $K \cdot 512$ tempos de bits e volta para o passo 2

Para FastEthernet o tempo de bit = 0,1 microsegundo

Por que backoff exponencial?

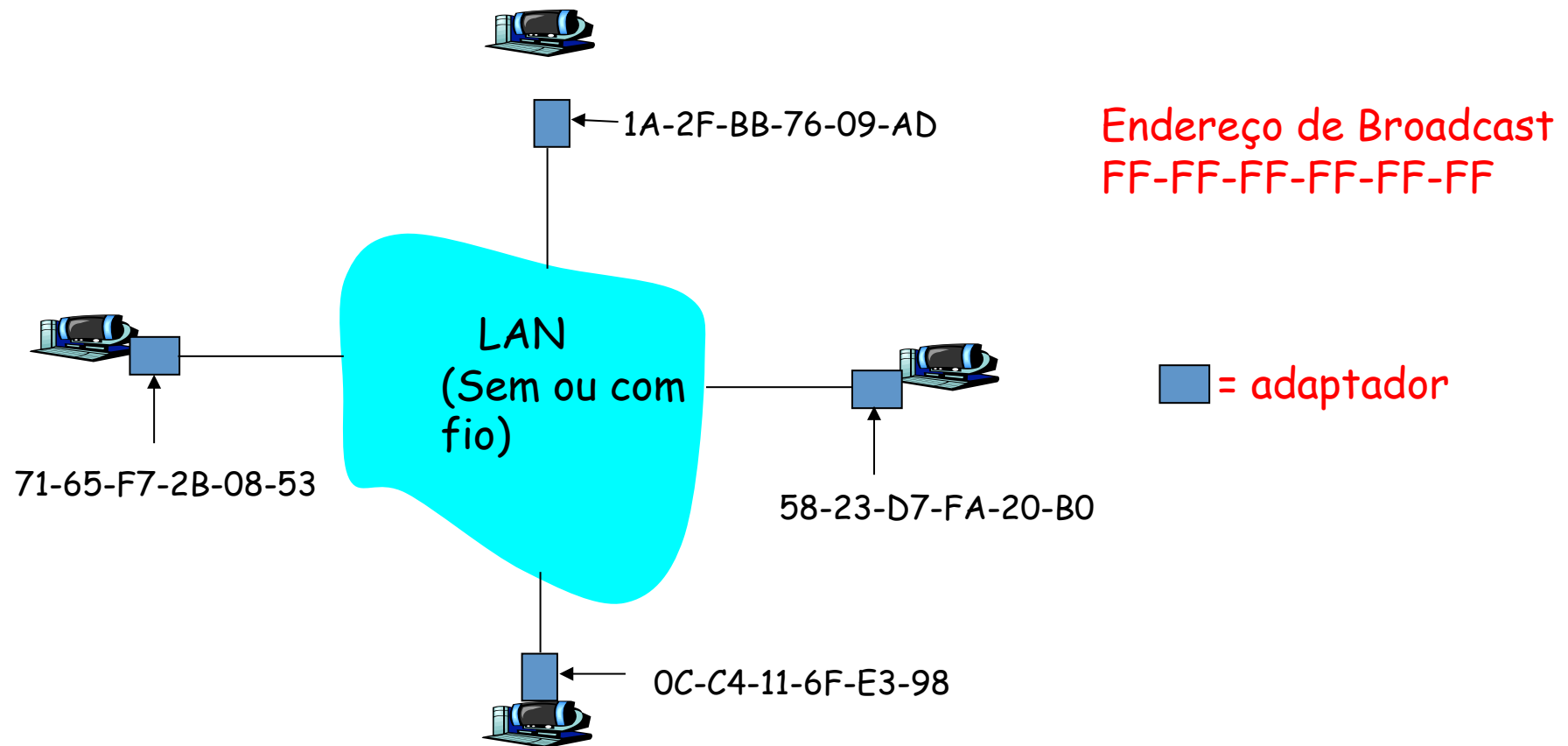
- Por que, por exemplo, não escolher um k entre $\{1,2,3,4,5,6,7\}$ após cada colisão?
- “Tentativa de reagir em função do número de adaptadores envolvidos na colisão
 - K pequeno para poucos adap. envolvidos
 - K maior quando muitos adap. envolvidos”
- Para cada novo quadro não é levado em consideração colisões anteriores

MAC Addresses and ARP

- Endereço IP de 32-bit:
 - *Endereço da camada de rede*
 - Usado para entregar um datagrama para a sub-rede IP de destino
- MAC (or LAN or physical or Ethernet) address:
 - Usado para entregar um datagrama de uma interface para outra fisicamente conectada (mesma rede)
 - Endereço MAC (48 bits) é gravado na memória da placa de rede

LAN Addresses and ARP

Cada adaptador na rede tem um endereço MAC único

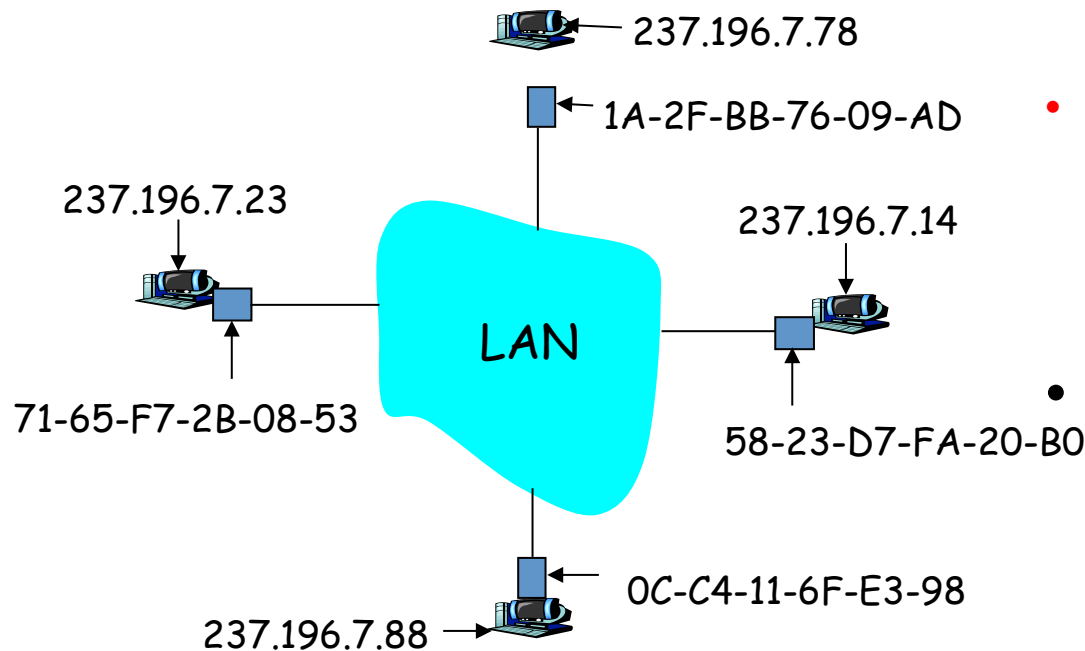


Endereço de rede

- Endereço MAC é administrado pelo IEEE
- Fabricante compra um espaço de endereços (garantir que todos os end. são únicos)
- Analogia:
 - (a) End. MAC: número do CPF
 - (b) End. IP: end. de correspondência
- End. MAC
 - portabilidade
 - Pode mover uma placa de rede para uma outra rede
 - *notebook*
- End. IP (hierárquico)
 - Não é portátil
 - Depende do end. IP da sub-rede

ARP: Address Resolution Protocol

Questão: como saber o end. MAC de B sabendo o End. IP ?



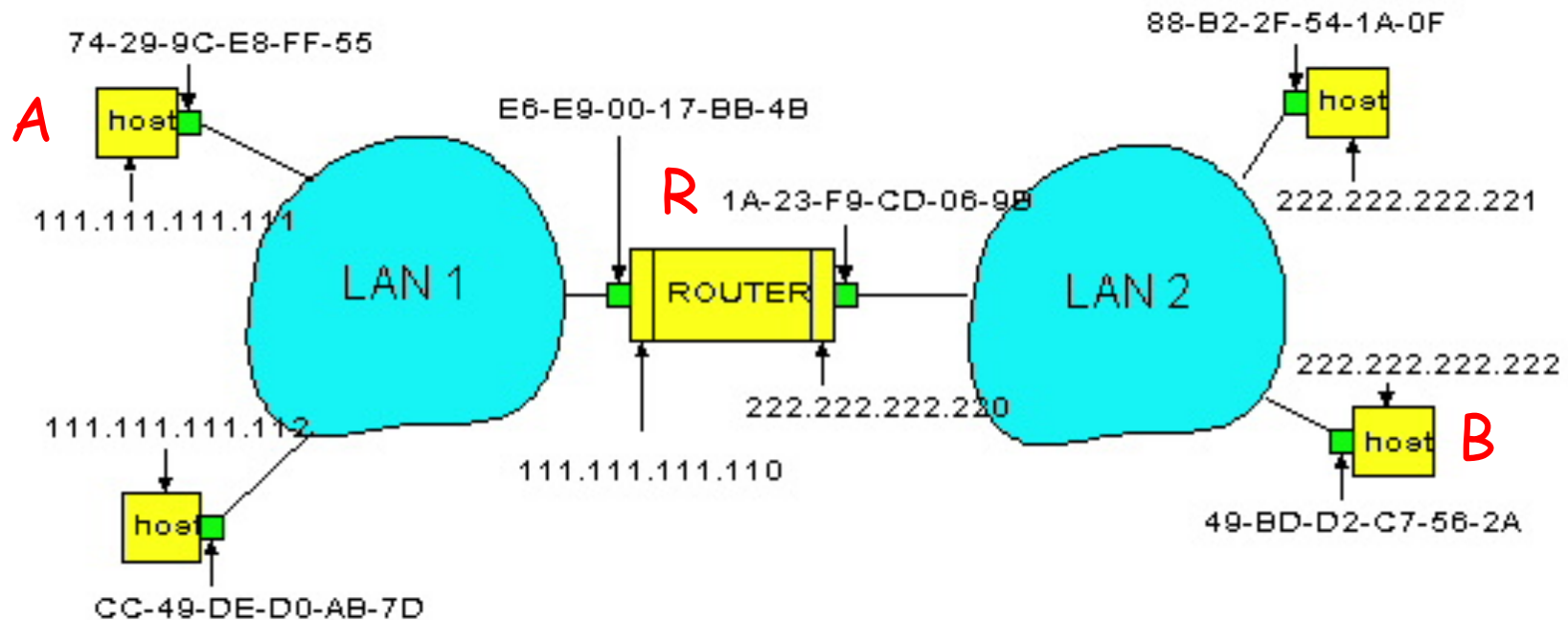
- Cada nó IP (Host, Roteador) na rede tem uma tabela **ARP**
- Tabela ARP: IP/MAC end. mapeamento somente para nós da rede
- **< IP address; MAC address; TTL >**
 - TTL (Time To Live): tempo que após o mapeamento a informação expira (tipicamente 20 min)
- Tabela ARP é armazenada na memória RAM no Nó

ARP protocol: Same LAN (network)

- **A** deseja enviar um datagrama para **B** (end. IP = 10.0.0.5), e end. MAC de B não está na Tab. ARP de **A**
- **A** envia um pacote ARP (Query) por **broadcasts** perguntando qual o end. MAC da máq. cujo o end. IP é 10.0.0.5 (maq. **B**)
 - Dest MAC address = FF-FF-FF-FF-FF-FF
 - Pergunta chega para todas as máquinas da rede
- **B** recebe o pacote ARP e responde para **A** com o seu end. MAC
 - Quadro de resposta para **A** é enviado com end. Unicast
- **A** grava end. IP/MAC na sua tabela ARP até a informação expirar.
- ARP é “*plug-and-play*”:
 - Cada nó cria suas tabelas ARP sem intervenção do administrador de rede

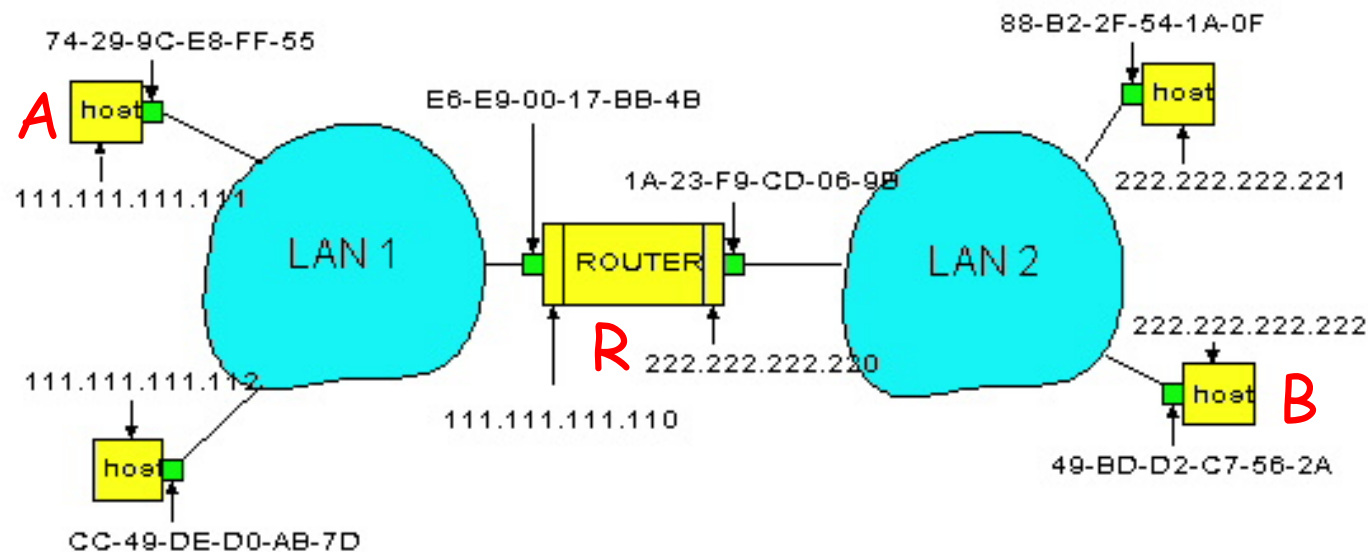
Roteamento para uma outra LAN

Travessia: envio de datagrama A para B via R. Assume-se que A sabe o end. IP de B

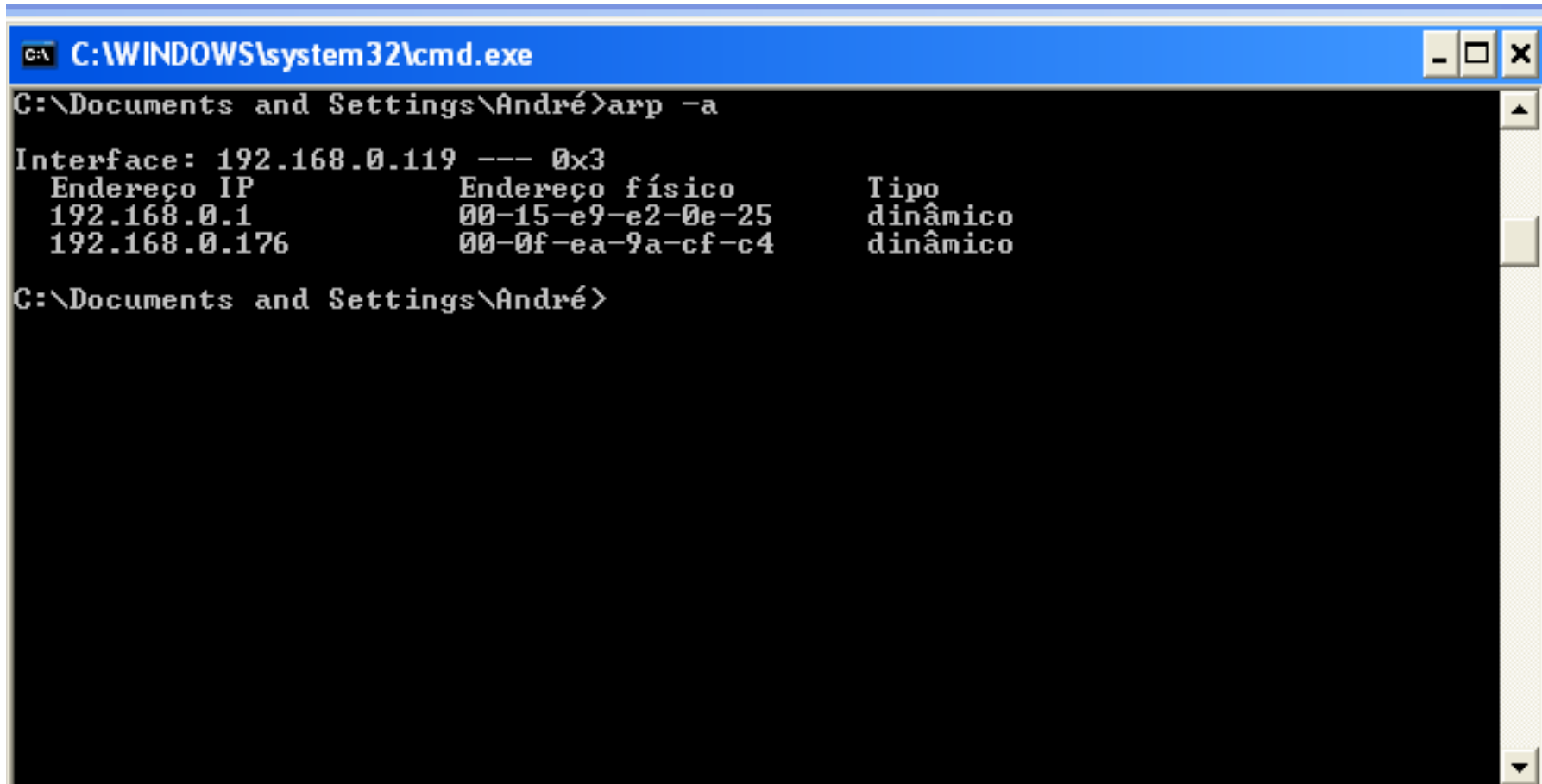


- Duas tabelas ARP no roteador R, uma para cada placa
- Na tabela de roteamento do nó origem, procura roteador 111.111.111.110
- Na tabela ARP da origem, procura end. MAC E6-E9-00-17-BB-4B, etc

- A cria um datagrama com origem A, destino B
- A usa o ARP para obter end. MAC de R para 111.111.111.110
- A cria quadro com end. MAC de R como dest., quadro contém pacote de A para B
- Placa de A envia o quadro
- Placa de R recebe o quadro
- R remove end. IP do datagrama que viaja dentro do quadro Ethernet, verifica que o datagrama é destinado a B
- R usa sua tabela ARP para obter o end. MAC de B
- R cria um quadro contendo o pacote IP de A para B e envia para B



Verificando tabela ARP



A screenshot of a Windows command prompt window. The title bar is blue and contains the text 'C:\WINDOWS\system32\cmd.exe' and standard window control buttons. The command prompt shows the user's current directory as 'C:\Documents and Settings\André' and the command 'arp -a' has been executed. The output displays information for the network interface 192.168.0.119 (0x3), listing two dynamic ARP entries: 192.168.0.1 with MAC address 00-15-e9-e2-0e-25, and 192.168.0.176 with MAC address 00-0f-ea-9a-cf-c4.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\André>arp -a

Interface: 192.168.0.119 --- 0x3
    Endereço IP      Endereço físico      Tipo
    192.168.0.1      00-15-e9-e2-0e-25    dinâmico
    192.168.0.176    00-0f-ea-9a-cf-c4    dinâmico

C:\Documents and Settings\André>
```

É possível adicionar uma entrada estática

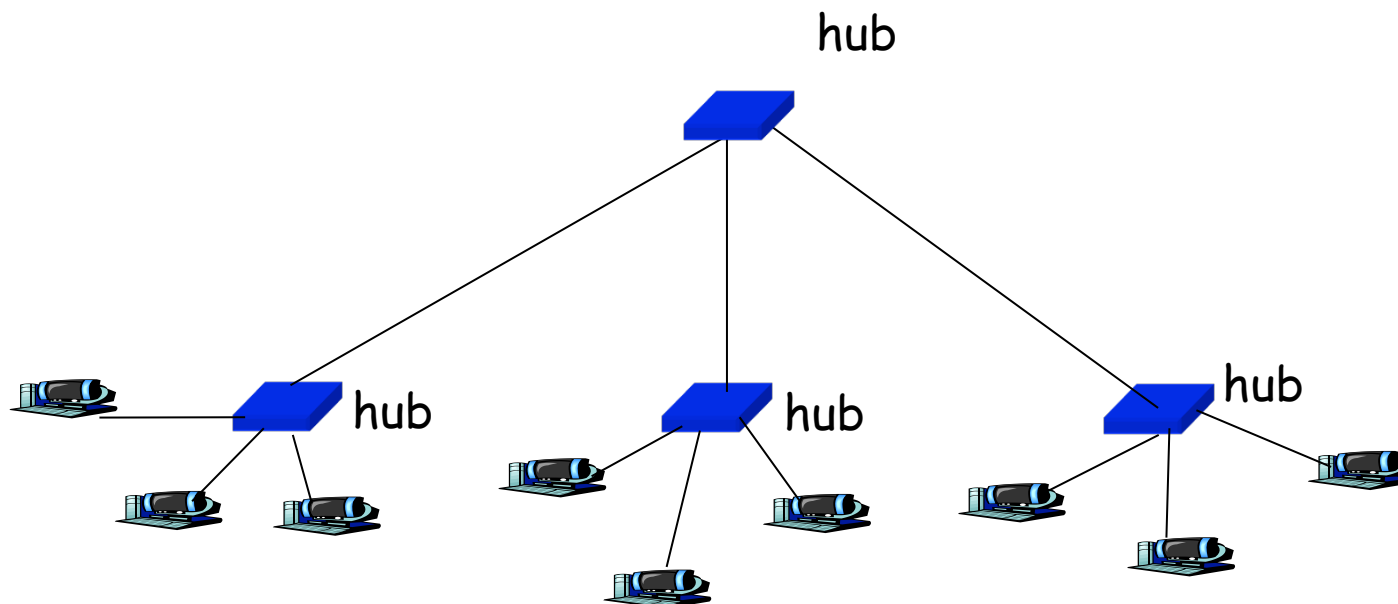
arp -s 157.55.85.212 00-aa-00-62-c6-09 Adiciona uma entrada estática

Tabela ARP

- Execute o comando `arp -a` para visualizar o atual estado a tabela arp de sua máq.
- Execute o comando `ping` especificando um endereço IP de uma máq. (da sua mesma sub-rede) que não está na tabela ARP da sua máq.
- Execute novamente o comando `arp -a` e verifique que uma nova entrada na tabela ARP foi adicionada

Interconexão com hubs

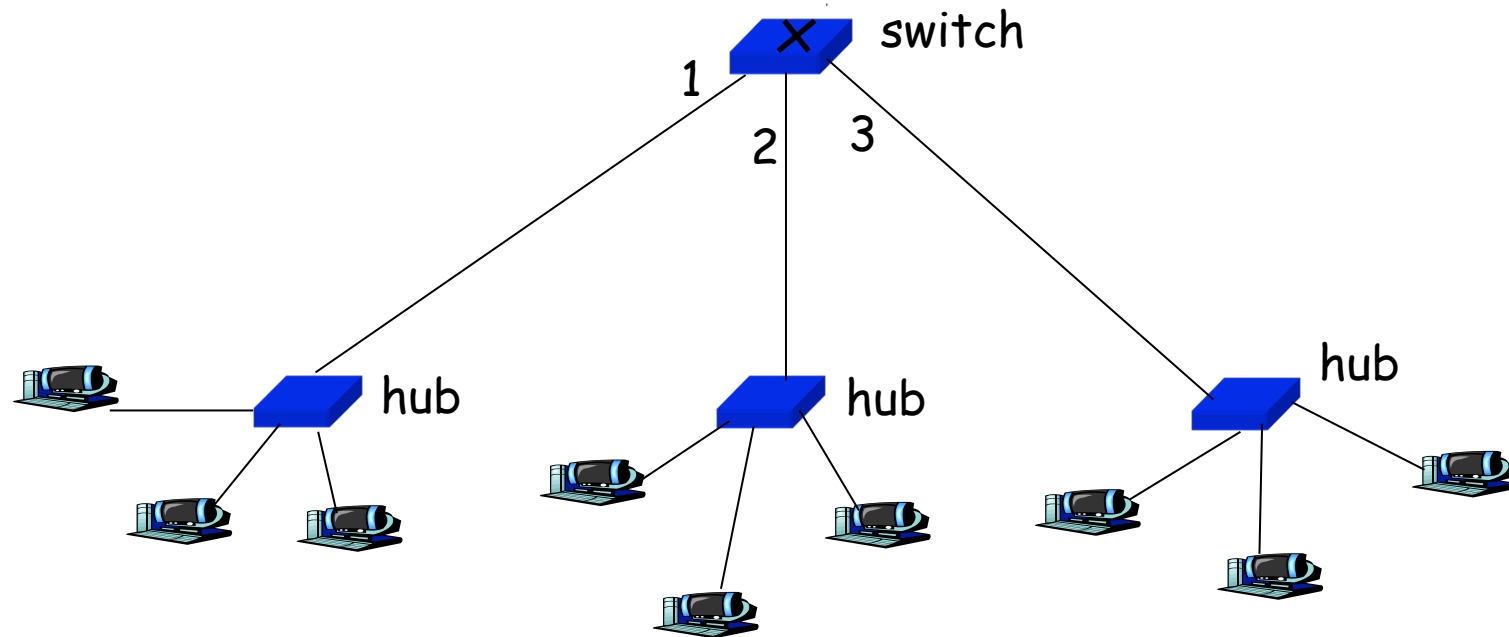
- Backbone de hubs interconectam segmentos de LAN
- Aumenta a distância máxima entre os nós
 - Desde que a distância entre um host e o hub seja de 100m
- Podem identificar máq. defeituosas
- Mas segmentos de colisão individuais tornam-se um único domínio de colisão
- Não podem interconectar diferentes tecnologias.



Switch

- Dispositivo de camada de enlace
 - Armazena e encaminha quadros Ethernet
 - Examina *header* dos quadros e os encaminha seletivamente com base no endereço MAC de destino
 - Quando o frame for encaminhado ao segmento, utiliza CSMA/CD para acessar o segmento (porta)
 - **Não possui end. MAC !!!**
- Transparente
 - Hosts não notam a presença dos switches
- *plug-and-play, self-learning*
 - switches não precisam ser configurados

Encaminhamento



- Como determinar em qual segmento um determinado quadro deve ser encaminhado?
- Parecido com o problema de roteamento

Auto aprendizado

- O switch possui uma tabela de comutação
- Entrada da tabela do switch:
 - (End. MAC, Interface, Time Stamp)
 - Entradas antigas são descartadas (TTL pode ser de 60 min)
- Switch aprende quais hosts podem ser alcançados através de cada interface
 - Quando um quadro é recebido, switch “aprende” a localização do emissor: entrada do segmento LAN (porta do switch)
 - É gravado o par (emissor, localização) na tabela do switch

Filtragem/Encaminhamento

Quando um switch recebe um frame

No Índice da tabela do switch é usado endereço MAC

if entrada encontrada para destino **then**

{

if dest está no mesmo seg. do frame que chegou **then**
descarte o frame

else

encaminhe o frame para a interface indicada

}

else

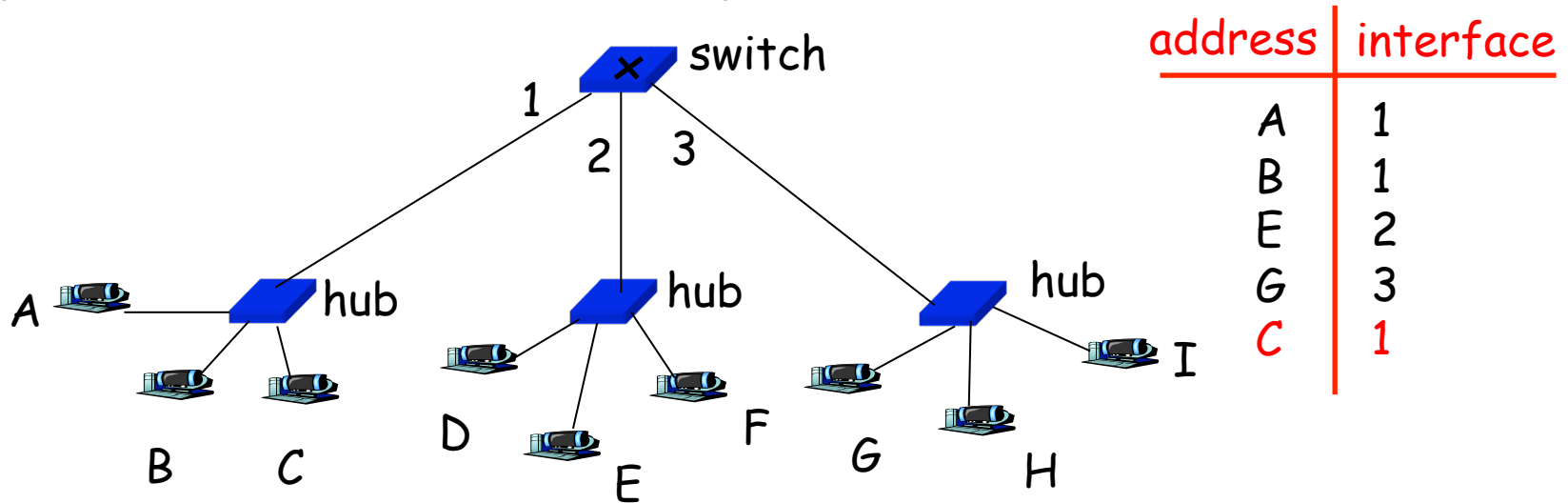
broadcast



Encaminha para todas as interface

Exemplo de Switch

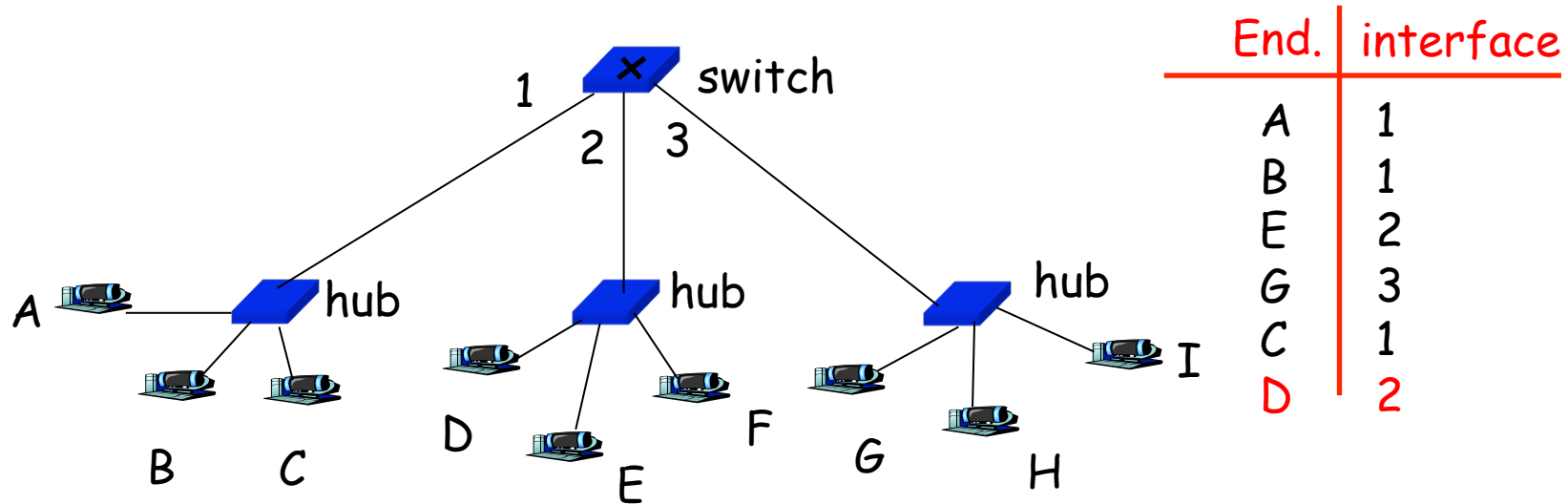
Suponha C envia um frame para D



- Switch recebe o frame de C
 - Cria na tabela uma entrada(C está na interface 1)
 - Como D não está na tabela, switch encaminha o frame para as interfaces 2 e 3
- frame recebido por D

Exemplo de Switch

Suponha que D responde de volta para C.



- Switch recebe um frame de D
 - Cria na tabela uma entrada(D está na interface 2)
 - Como C já está na tabela, switch encaminha o frame somente para interface 1
- frame recebido por C

Switch: isolamento do tráfego

- Instalação de switchs divide sub-redes no segmento LAN
- switch **filtrando** pacotes:
 - Quadros do mesmo segmento (origem=destino) não são encaminhados para outros segmentos
 - Segmentos tornam-se diferentes domínios de colisão

