Local Area Networks (LANs)

FEUP/DEEC
Redes de Computadores
MIEEC – 2010/11
José Ruela

LANs – Local Area Networks

» As LANs desenvolveram-se a partir de meados da década de 1970, com o objectivo de satisfazer as necessidades de comunicação de dados em empresas
  – As soluções então disponíveis em WANs não eram adequadas para ambiente LAN
  – Era possível explorar soluções alternativas, na altura não viáveis em WANs

» As LANs ligam uma grande diversidade de sistemas informáticos de uma mesma organização (computadores, *workstations*, computadores pessoais, servidores, periféricos, etc.), permitindo
  – Partilha de recursos (impressoras, discos, aplicações, processadores e a própria infraestrutura de comunicação)
  – Comunicação entre sistemas (correio electrónico, transferência de ficheiros)
  – Cooperação entre sistemas (processamento distribuído, aplicações cliente-servidor)
  – Acesso a informação (bases de dados)
  – Transferência de diversos tipos de informação (dados, áudio, vídeo, imagens, gráficos)
  – Interligação de subredes (*backbone* de alta velocidade para ligação de LANs de mais baixa velocidade)

LANs – requisitos

» Em LANs, devido às pequenas distâncias envolvidas e à utilização de meios de transmissão privados, é possível explorar soluções arquitectónicas e tecnológicas orientadas para a satisfação dos seguintes requisitos típicos
  – Suporte de débitos elevados (actualmente da ordem de 1 a 10 Gbit/s)
  – Suporte de grande número de sistemas
  – Elevada disponibilidade
  – Partilha eficiente de recursos de transmissão
  – Fácil instalação, reconfiguração e expansão (inserção / remoção de sistemas)
  – Fácil manutenção
  – Baixo custo por sistema instalado

» Do ponto de vista do desempenho, é ainda desejável que permitam
  – Funcionamento estável sob carga elevada
  – Acesso equilibrado (*fairness*) por parte de todos os sistemas (eventualmente com vários níveis de prioridade e acesso rotativo em cada nível)
  – Suporte de aplicações multimédia e aplicações com requisitos de tempo real

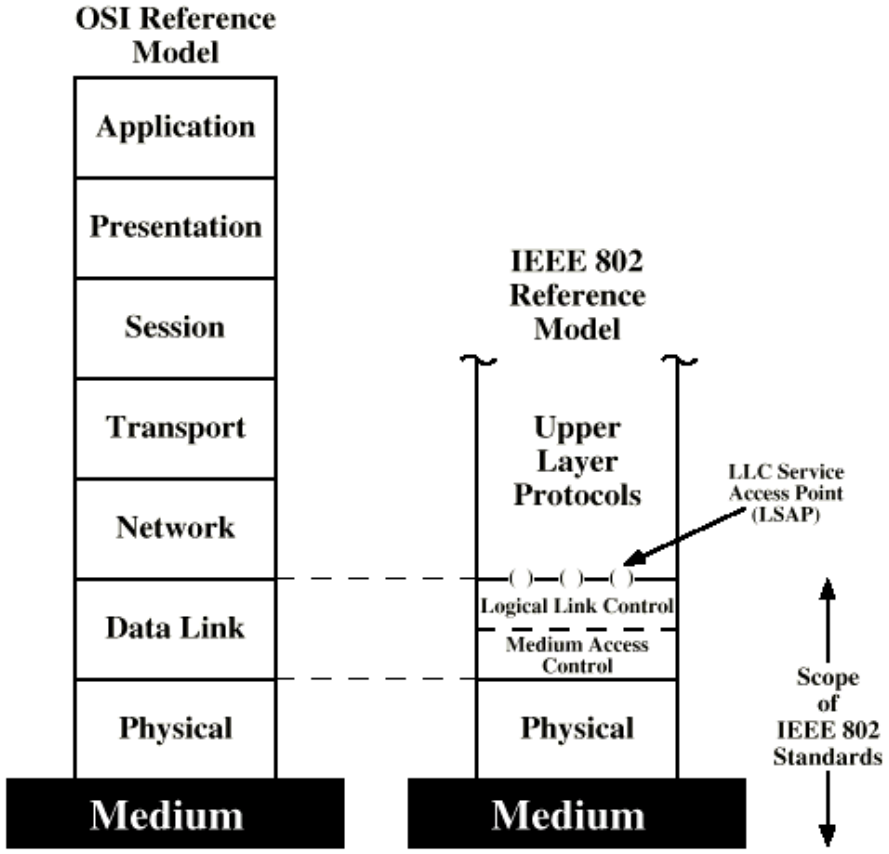
LANs – atributos

As LANs podem caracterizar-se por um conjunto de atributos típicos que as distinguem das WANs

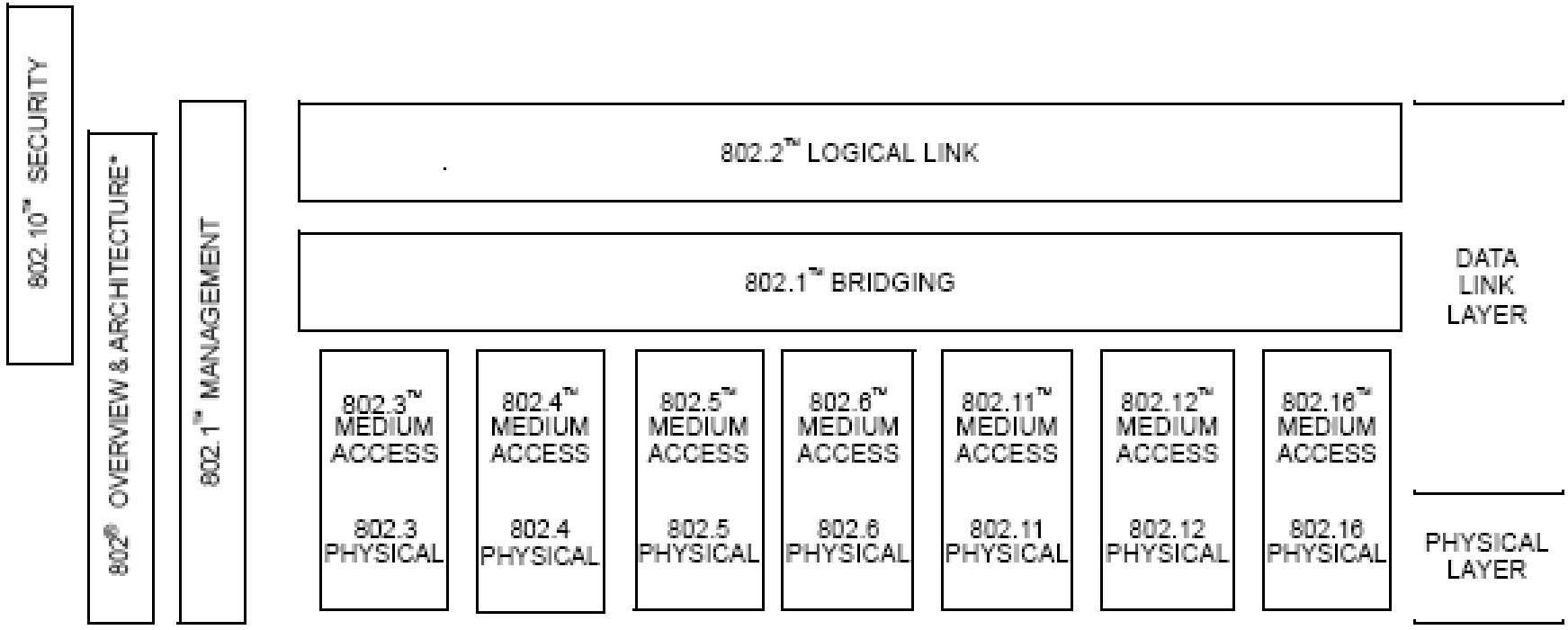
- São redes privadas
- Podem cobrir distâncias até algumas dezenas de km – algumas soluções adoptadas em LANs são igualmente viáveis em redes de área metropolitana (MANs – *Metropolitan Area Networks*)
- Oferecem ampla gama de débitos (10 / 100 Mbit/s, 1 / 10 Gbit/s)
- Utilizam topologias simples que permitem um elevado grau de conectividade entre sistemas e partilha eficiente de recursos de transmissão
- Utilizam meios de transmissão muito diversos
  - » Guiados: pares de cobre, cabo coaxial, fibra óptica
  - » Não guiados / comunicação sem fios (*wireless*): rádio frequências, infravermelhos
- Em meios partilhados são utilizados normalmente protocolos de acesso distribuídos

Arquitectura IEEE 802

» A camada de Ligação de Dados (OSI) é dividida em duas sub-camadas
  – LLC (*Logical Link Control*)
  – MAC (*Medium Access Control*)
» LLC
  – Interface comum para camadas superiores
  – Controlo de erros e de fluxo (opcional)
» MAC
  – Controlo do acesso ao meio de transmissão
  – Transmissão / recepção de tramas (*framing*)
  – Reconhecimento de endereços “físicos”
  – Detecção de erros
» Camada Física
  – Codificação / descodificação de sinais
  – Transmissão / recepção de bits
  – Interface de acesso ao meio de transmissão
  – Interligação de sistemas (topologia física)



Arquitectura IEEE 802 – modelo e protocolos



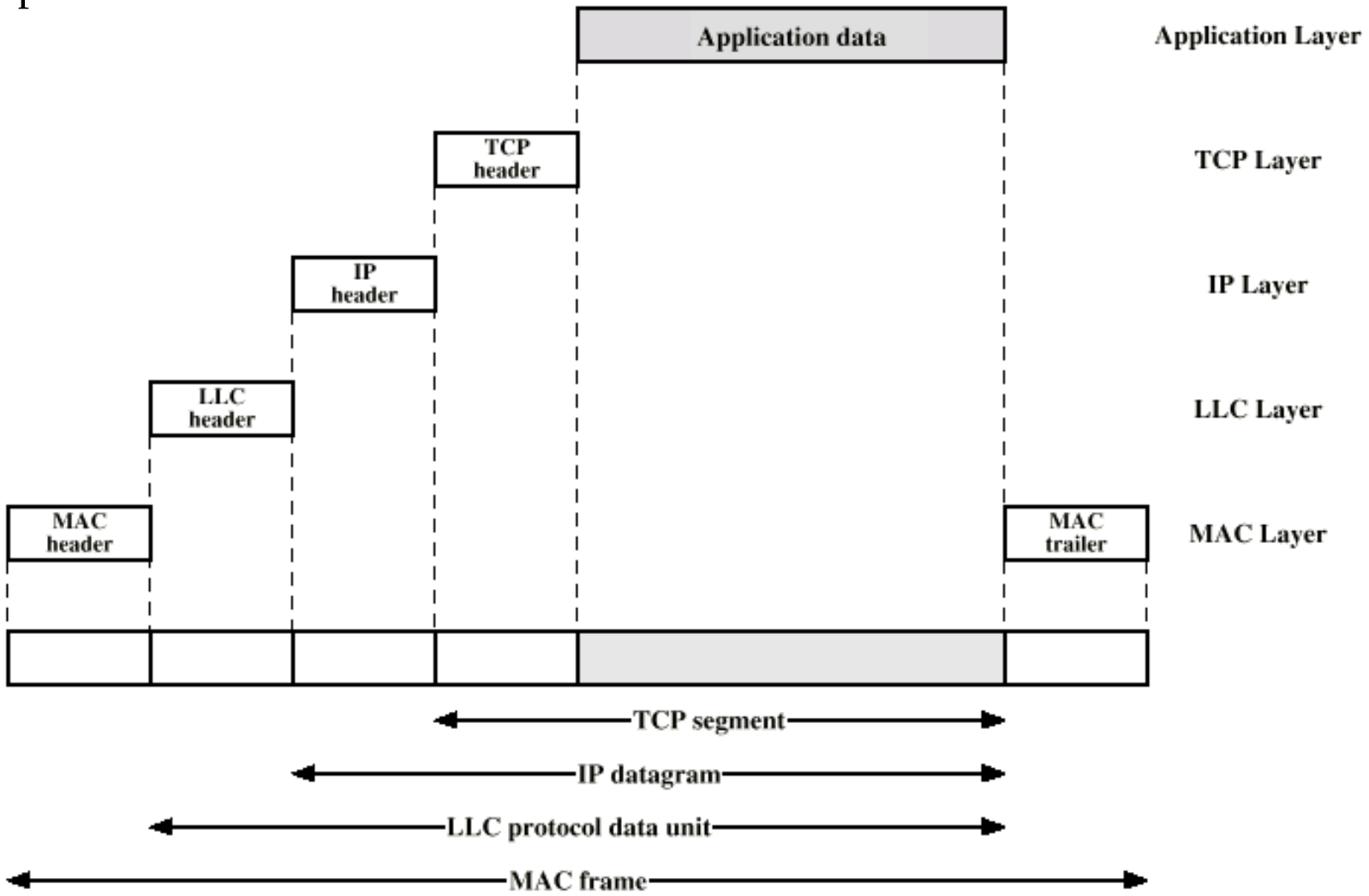
* Formerly IEEE Std 802.1A.

Arquitectura IEEE 802 – alguns protocolos

- IEEE 802.1 — *LAN/MAN architecture; internetworking among LANs, MANs and WANs; link security; network management; protocol layers above MAC / LLC*
- IEEE 802.1D — *Media Access Control (MAC) Bridges*
- IEEE 802.1Q — *Virtual Bridged Local Area Networks*
- IEEE 802.2 — *Logical Link Control*
- IEEE 802.3 — *CSMA/CD (Ethernet)*
- IEEE 802.4 — *Token Bus*
- IEEE 802.5 — *Token Ring*
- IEEE 802.6 — *Distributed Queue Dual Bus (DQDB)*
- IEEE 802.10 — *Security*
- IEEE 802.11 — *Wireless LAN*
- IEEE 802.12 — *Demand Priority*
- IEEE 802.15 — *Wireless Personal Area Network*
- IEEE 802.16 — *Broadband Wireless Access*
- IEEE 802.17 — *Resilient Packet Ring (RPR)*
- IEEE 802.20 — *Mobile Broadband Wireless Access (MBWA)*

Encapsulamento de dados

Exemplo: LAN TCP/IP



Medium Access Control (MAC)

- A lógica de controlo (protocolo) de acesso ao meio pode ser
  - Centralizada
    - Permite controlo mais completo (visão global da rede)
    - A lógica nas estações é mais simples
    - Evita problemas de coordenação entre estações
    - O elemento central é um ponto de falha único (se não existir redundância)
    - O elemento central é um ponto focal de congestionamento
  - Distribuída
    - É mais robusta
    - É mais eficiente (menor *overhead* de controlo)

- Técnica de acesso ao meio
  - Síncrona
    - Capacidade de transmissão fixa atribuída previamente a cada estação
  - Assíncrona
    - Em resposta a um pedido, explícito ou implícito (*round robin*, reserva, contenção)

Acesso assíncrono

Exemplos

» Rotativo (*round robin*)
  – Adequado para transmissões prolongadas de várias estações
  – Permite atribuir o meio a cada estação, por períodos curtos, de forma ordenada e sem conflitos (centralizado ou distribuído)

» *Polling* distribuído (*Control Token*)
  • IEEE 802.4 (*Token Bus*)
  • IEEE 802.5 (*Token Ring*), FDDI (*Fiber Distributed Data Interface*)

» *Polling* centralizado
  • IEEE 802.11 (opcional)

» Reserva
  – Adequado para tráfego contínuo (em particular tráfego isócrono)

» IEEE 802.6 – DQDB (*Distributed Queue Dual Bus*)

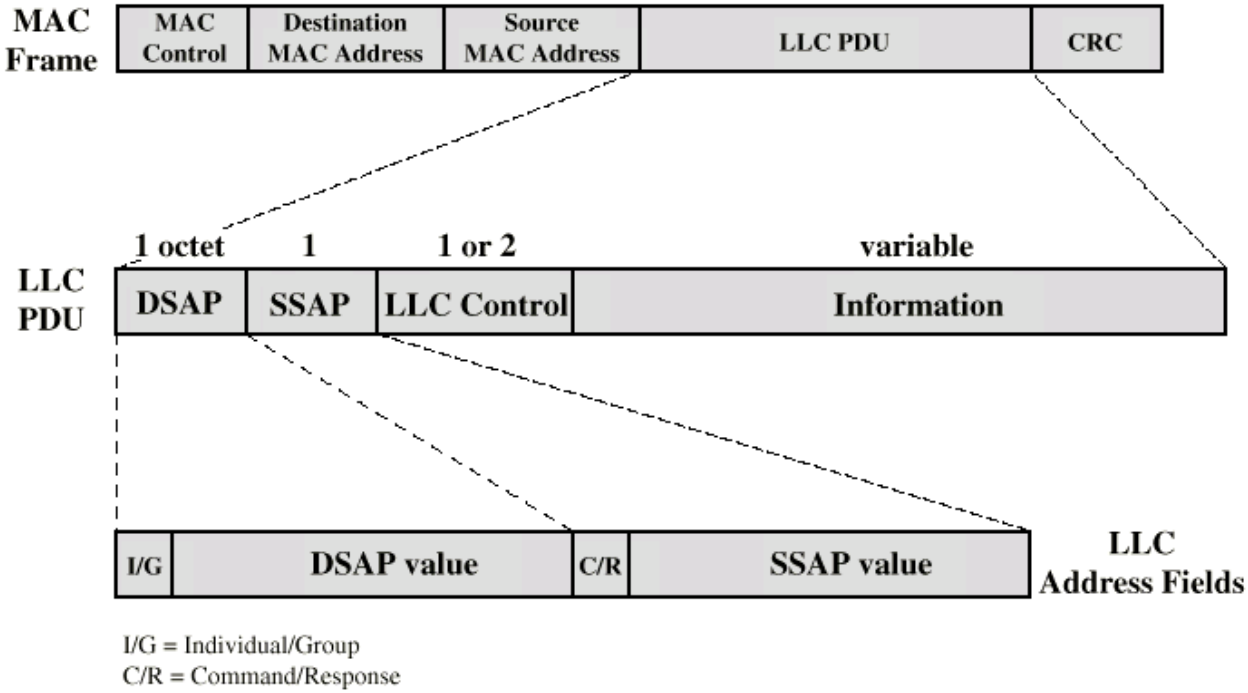
» Contenção (*contention / random access*)
  – Adequado para tráfego *bursty*
  – Baseado na competição e resolução distribuída de conflitos (colisões) entre estações
  – Eficiente para cargas moderadas, mas instável para cargas elevadas

» IEEE 802.3 (CSMA/CD)
» IEEE 802.11 (CSMA/CA)

Formato genérico de tramas MAC / LLC

- *MAC Control*
  - Informação protocolar de controlo
- *Destination / Source MAC Address*
  - Endereço MAC de destino / origem
- CRC
  - Código detector de erros

- MAC
  - Encapsula os dados da camada LLC
  - Detecta e elimina tramas com erros
- LLC
  - Encapsula e identifica protocolos de alto nível
  - Controlo de erros e de fluxo (opcional)



Endereços MAC – atributos

» São endereços não estruturados (*flat* – ausência de hierarquia)

» Não têm qualquer relação com a localização física da estação na rede

» São endereços "físicos" (ou de *hardware*) uma vez que identificam a carta de interface (mas não o ponto onde a estação se liga à rede); distinguem-se de endereços "lógicos" (ou de *software*), de que são exemplo os endereços IP, que definem a pertença a uma subrede lógica

» Quando as tramas encapsulam pacotes destinados a entidades endereçáveis na camada de Rede, é necessário um mecanismo de resolução de endereços, por exemplo a determinação do endereço MAC, conhecido o endereço IP

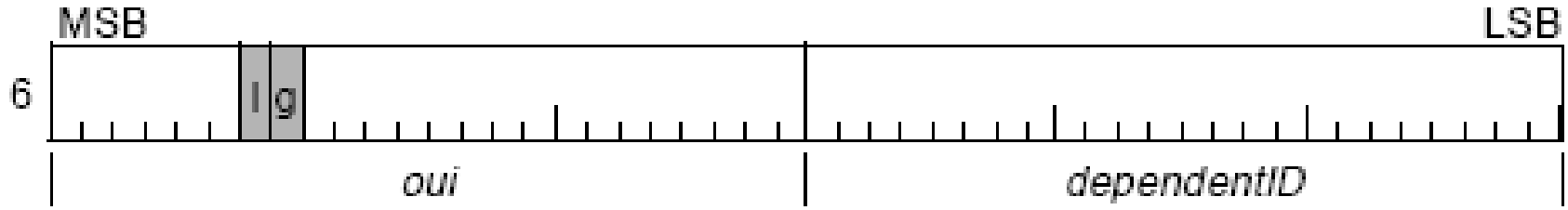
Endereços MAC – tipos e formatos

» Tipos
  – *Unicast*
  – *Multicast*
  – *Broadcast*

  Uma estação tem associado um endereço *unicast* (que deve ser único, pelo menos na sua subrede), pode pertencer a vários grupos *multicast* (ou a nenhum) e aceita todas as tramas com endereço *broadcast* (difusão) na sua subrede

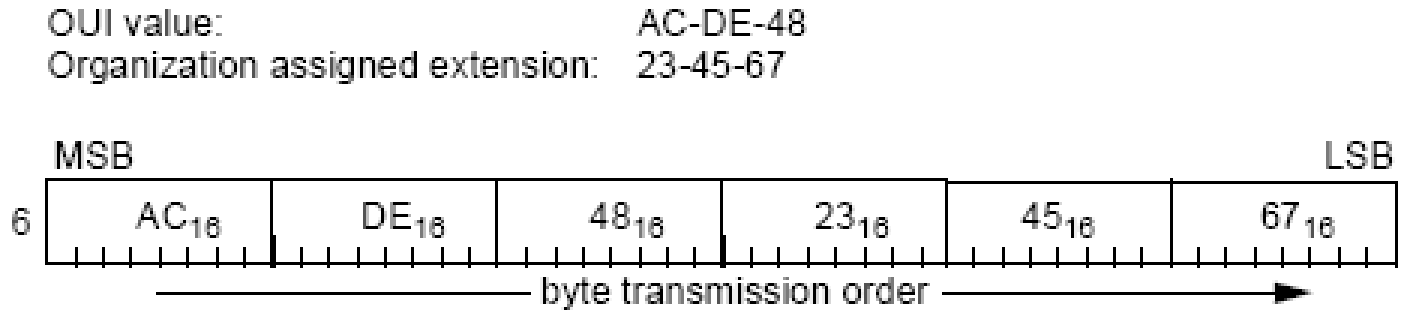
» Formatos
  – Dois octetos – administrados localmente
  – Seis octetos – administrados globalmente (IEEE) ou localmente
    » A administração global garante unicidade numa rede constituída por várias subredes
    » O IEEE atribui gamas de endereços globais aos diferentes fabricantes

Endereços MAC – atribuição



- OUI – *Organizationally Unique Identifier*
- *l* – administração local (1) / universal (0)
- *g* – endereço de grupo (1) / individual (0)

Exemplo



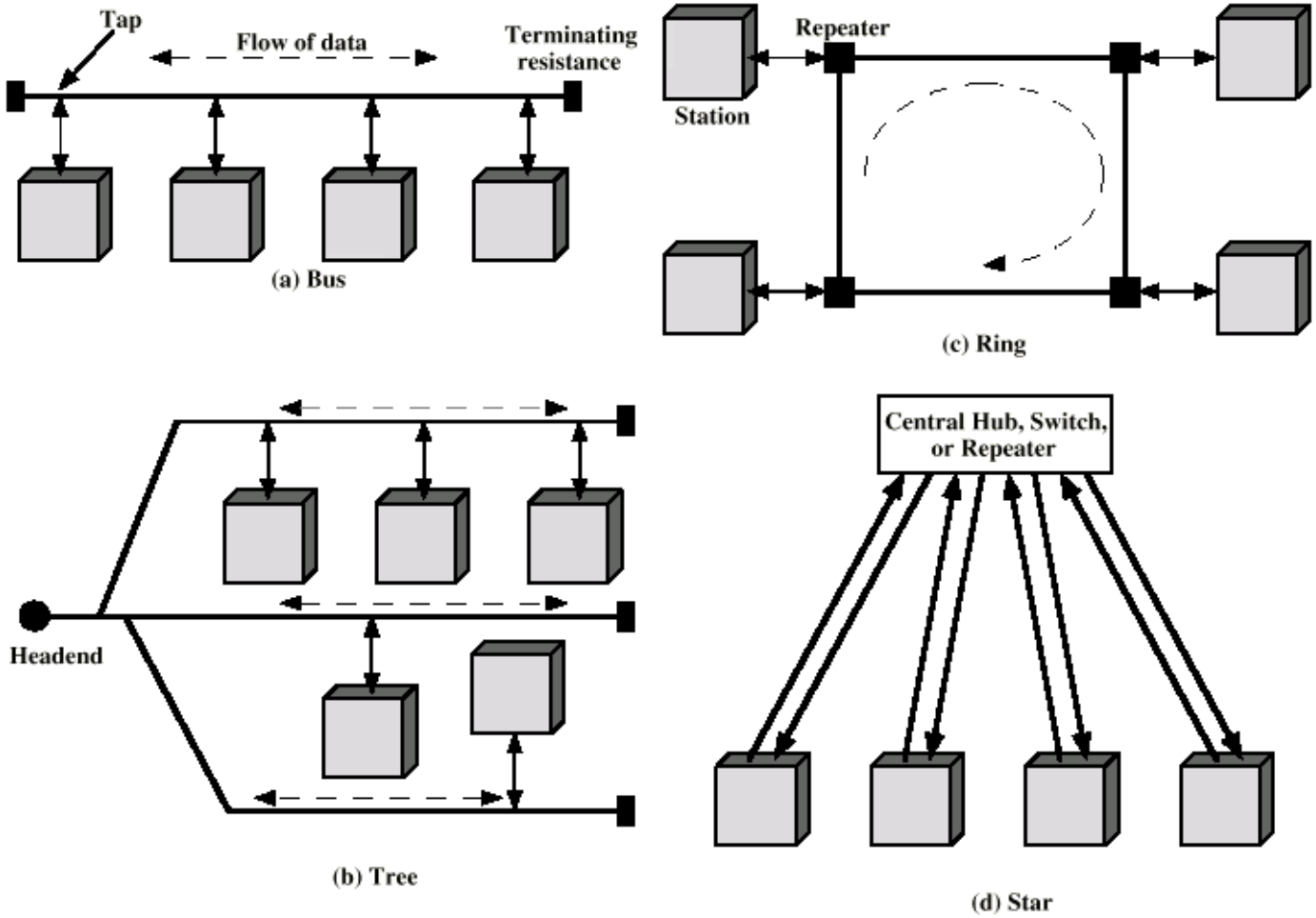
Controlo da Ligação Lógica (LLC) – IEEE 802.2

- Características
  - Fornece serviço independente da tecnologia de subrede e do serviço MAC
  - Define um único formato para encapsular dados e identificar protocolos encapsulados
  - Endereçamento
    - DSAP / SSAP (*Destination / Source Service Access Point*)

- Serviços
  - LLC1 – não confirmado, sem conexão (*unacknowledged connectionless service)*
    - É o mais comum (suportado obrigatoriamente em todas as LANs IEEE 802)
    - Usa tramas do tipo *Unnumbered Information*
  - LLC2 – com conexão (*connection-mode service*)
    - Suporta controlo de erros (serviço fiável) e controlo de fluxo
    - Baseado em HDLC
  - LLC3 – confirmado, sem conexão (*acknowledged connectionless service)*

Topologias físicas

Topologias básicas: barramento (*bus*), árvore (*tree*), anel (*ring*), estrela (*star*)



Topologias em barramento e em árvore

» Configuração física multiponto, aberta (sem percursos fechados)

» O meio (canal) é partilhado
  – É necessário um protocolo para controlo de acesso ao meio (para evitar que duas ou mais estações interfiram, provocando colisões)

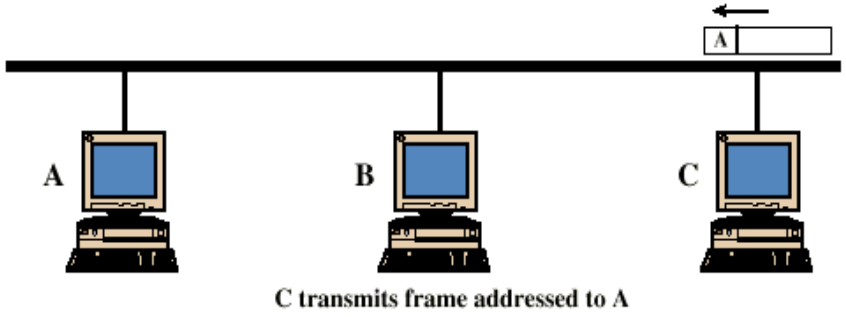
» O sinal é difundido (propaga-se) no meio – as tramas são escutadas por todas as estações
  – É necessário identificar a estação (ou estações) de destino
  – Cada estação tem de possuir um endereço único (*unicast*) para além de poder ter endereço(s) de grupo (*multicast*)

» Ligação física *full-duplex* entre a estação e o ponto de acesso (*transceiver*)

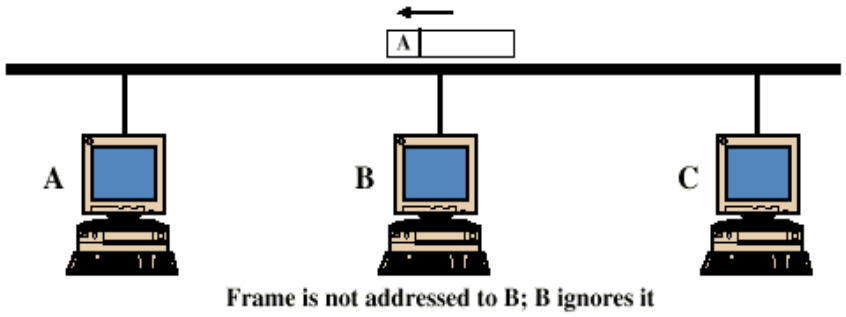
» Funcionamento lógico *half-duplex*
  – A transmissão e recepção simultânea de tramas no mesmo ponto de acesso é um indício de ocorrência de colisão (mais do que uma estação a transmitir)
  – O protocolo de acesso deve garantir um funcionamento lógico *half-duplex*

» O sinal no extremo do meio é absorvido por um terminador (evita reflexões)

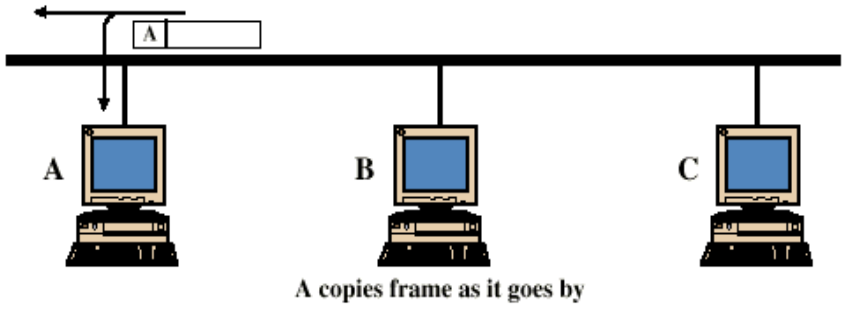
Topologia em barramento



C transmits frame addressed to A



Frame is not addressed to B; B ignores it



A copies frame as it goes by

LANs em barramento

» A potência do sinal emitido deve cumprir vários requisitos
  – Considerando a atenuação no meio, deve ser compatível com a sensibilidade e a gama dinâmica dos receptores, garantindo relação sinal / ruído adequada para detecção com taxa de erros muito baixa
  – Não deve provocar sobrecarga (*overload*) do emissor (e consequente distorção do sinal)
  – Deve permitir satisfazer as combinações possíveis de localização de estações (emissores e receptores) no meio

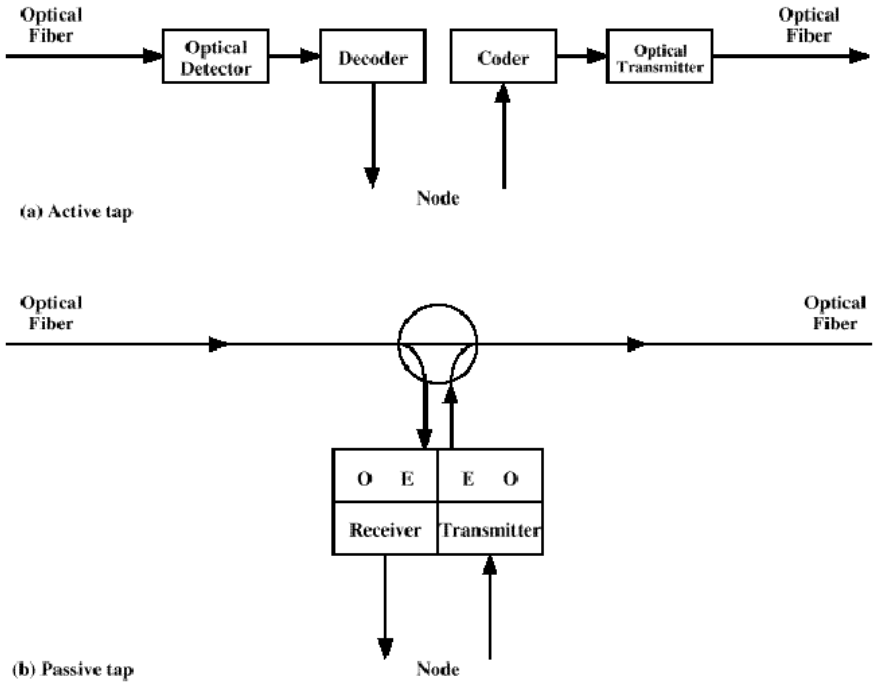
» Segmentação da rede
  – A rede pode ser constituída por vários segmentos físicos interligados, o que permite cobrir maiores distâncias
  – Os segmentos podem ser ligados com repetidores (garantem continuidade ao nível físico) ou com outros elementos activos (*bridges* / comutadores e *routers*)

» Meios de transmissão
  – Os barramentos físicos são normalmente realizados em cabo coaxial, usando tecnologia *baseband* (um único canal) ou *broadband* (vários canais)
  – É possível criar o equivalente lógico de uma LAN em barramento usando topologias físicas em estrela e repetidores (*hubs*) que realizam a difusão do sinal; a solução mais usual recorre a cablagens estruturadas realizadas com pares de cobre entrançados (*twisted pair*)
  – Podem usar-se igualmente fibras ópticas em ligações ponto a ponto entre repetidores ou em redes com topologia em barramento ou estrela (acoplamento activo ou passivo)

Barramentos de fibra óptica

» Acoplamento activo
  – O barramento é realizado com ligações ponto a ponto entre repetidores e inclui conversores óptico-eléctricos e electro-ópticos
  – As estações ligam-se ao meio através dos repetidores

» Acoplamento passivo
  – Acopladores direccionais (com 3 ou 4 portas) permitem derivar e injectar directamente sinal óptico na fibra
  – As perdas nos acopladores limitam seriamente o número de estações no barramento

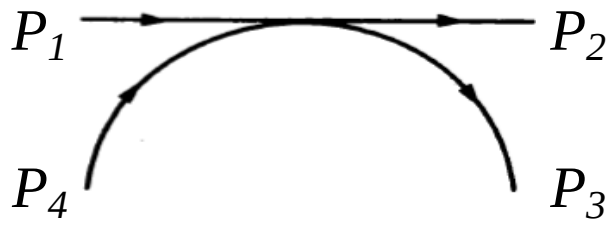


Acopladores ópticos direccionais – caracterização

» Os acopladores ópticos direccionais (*directional couplers*) são dispositivos passivos constituídos, no caso geral, por 4 portas – 2 de entrada e 2 de saída

– Podem ter apenas 3 portas externas (*T-couplers*), sendo a quarta porta terminada internamente – usam-se para separar (*splitters*) ou combinar (*combiners*) sinais ópticos

» Na figura, 1 e 2 são as portas de entrada e 3 e 4 as portas de saída – no entanto, os acopladores são simétricos (isto é, o papel das portas pode ser invertido)



» Os acopladores direccionais podem caracterizar-se pelas suas perdas intrínsecas (*Excess Loss*) e pelo coeficiente de acoplamento entre fibras (*C*)

– Uma fracção da potência injectada na(s) porta(s) de entrada é perdida na junção (*Excess Loss*)

– A menos das perdas intrínsecas, a potência aplicada em qualquer das portas de entrada é dividida pelas portas de saída, numa proporção determinada por *C*, podendo desprezar-se a potência reflectida na outra porta de entrada

Acopladores ópticos direccionais – perdas

» As perdas intrínsecas são definidas pela relação α entre a potência total nas portas de saída e nas portas de entrada (a relação em *dB* é representada por E_c)

$$\alpha = \frac{P_2 + P_3}{P_1 + P_4} = 10^{-E_c/10}$$

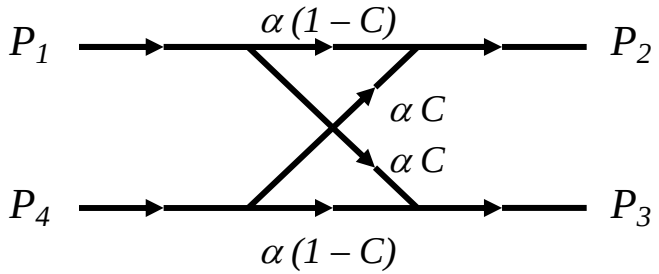
$$\alpha = 0.8, \;\; E_c = 1\,dB$$

$$E_c(dB) = -10\log_{10}\alpha$$

» Os acopladores direccionais obedecem à condição de reciprocidade

– Admitindo qua as portas 1 e 2 estão associadas à fibra principal (e portanto 3 e 4 são portas locais), a fracção da potência removida da fibra principal, através da porta 3 ($\alpha\, C$) é igual à fracção da potência injectada nessa fibra, através da porta 4

$$\begin{bmatrix} P_2 \\ P_3 \end{bmatrix} = \begin{bmatrix} \alpha(1-C) & \alpha C \\ \alpha C & \alpha(1-C) \end{bmatrix} \begin{bmatrix} P_1 \\ P_4 \end{bmatrix}$$



– A relação de potências nas portas de saída (P2 : P3) é dada por (1 – C) / C
  » Exemplos: se C = 1 / 16, a relação é 15 : 1; se C = 1 / 2, a relação é 1 : 1

» *Insertion Loss:* $-10\log_{10}\alpha(1-C)$

» *Isolation Loss:* $-10\log_{10}\alpha C$

Acopladores ópticos direccionais – análise

» A utilização de acopladores direccionais em barramentos ópticos passivos é fortemente condicionada pelas perdas intrínsecas (tipicamente 1 dB) e pela condição de reciprocidade – a utilização de um valor de *C* pequeno para limitar as perdas na fibra principal (*Insertion Loss* pequena) limita igualmente a potência injectada localmente na fibra principal (*Isolation Loss* elevada)

Exemplo: $\alpha = 0.8,\ E_c = 1\,dB$

$C = 1/16$

$$\begin{bmatrix} P_2 \\ P_3 \end{bmatrix} = \begin{bmatrix} 0.75 & 0.05 \\ 0.05 & 0.75 \end{bmatrix} \begin{bmatrix} P_1 \\ P_4 \end{bmatrix}$$

Insertion Loss = 1.25 dB

Isolation Loss = 13.0 dB

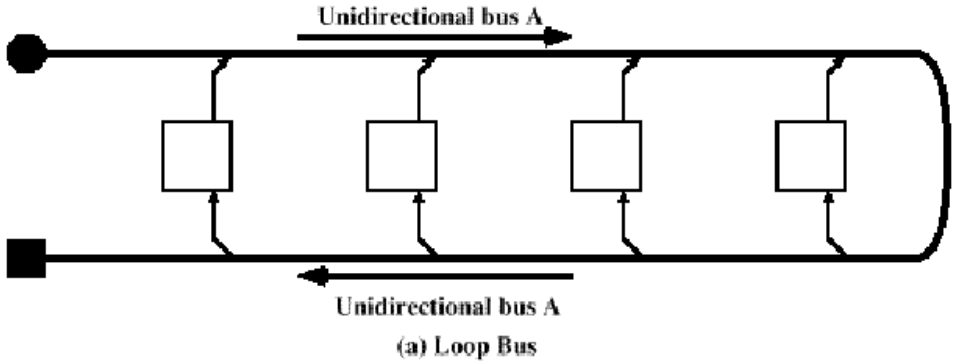
» Considerando um barramento unidireccional com *N* acopladores, a perda máxima de potência (entre o primeiro emissor e o último receptor) é dada por $2 * \textit{Isolation Loss} + (N - 2) * \textit{Insertion Loss}$ e, com os valores anteriores, é igual a $26 + (N - 2) * 1.25$

- Se considerarmos uma margem de potência típica da ordem de 40 dB, o valor máximo de *N* será da ordem de 13 (seria cerca de 14 se $\alpha = 0.8$ e C = 1 / 4)
- Na prática não existe o equivalente óptico de uma derivação de alta impedância

Barramentos unidireccionais

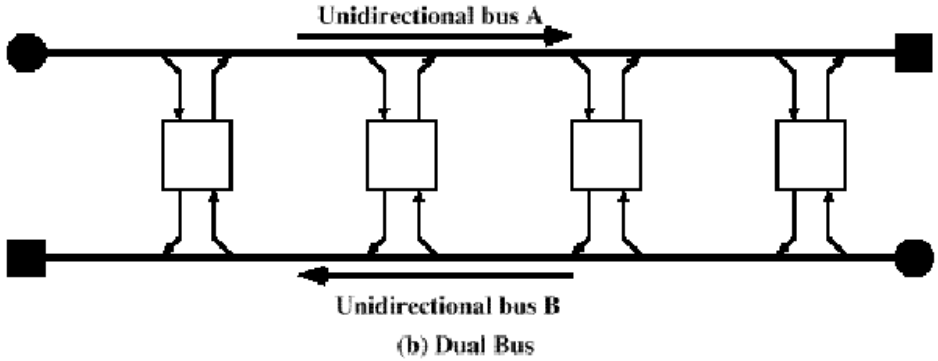
Configurações usadas com fibra óptica ou com cabo coaxial

» Barramento simples dobrado (*folded bus* ou *loop bus*)



(a) Loop Bus

» Barramento duplo (*dual bus*)



(b) Dual Bus

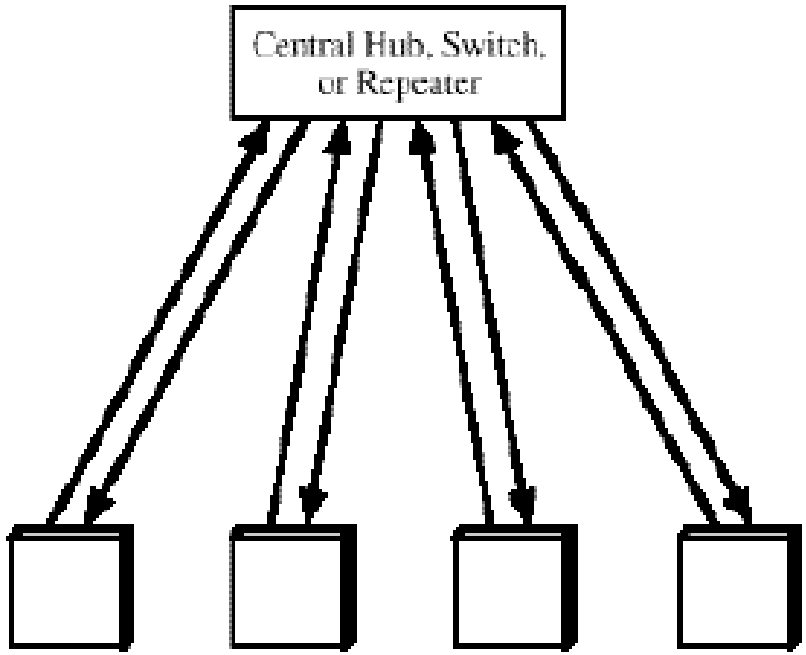
Topologia em estrela

» Cada estação liga-se a um elemento central
  – Duas ligações ponto a ponto (2 pares) para transmissão e recepção, respectivamente

» O elemento central pode ser um repetidor multiporta (*hub*) ou um comutador

» Repetidor
  – Repete (difunde) o sinal recebido numa porta em todas as outras portas
  – Logicamente equivalente a um barramento
  – É necessário controlar o acesso das estações ao meio – funcionamento *half-duplex*

» Comutador
  – Comuta simultaneamente tramas entre portas de entrada e de saída (com base no endereço MAC de destino); pode ainda copiar uma trama para várias portas de saída
  – Funcionamento *full-duplex*
  – Componente essencial na formação de LANs Virtuais (*Virtual LANs* – VLANs)



(d) Star

Estrela de fibra óptica

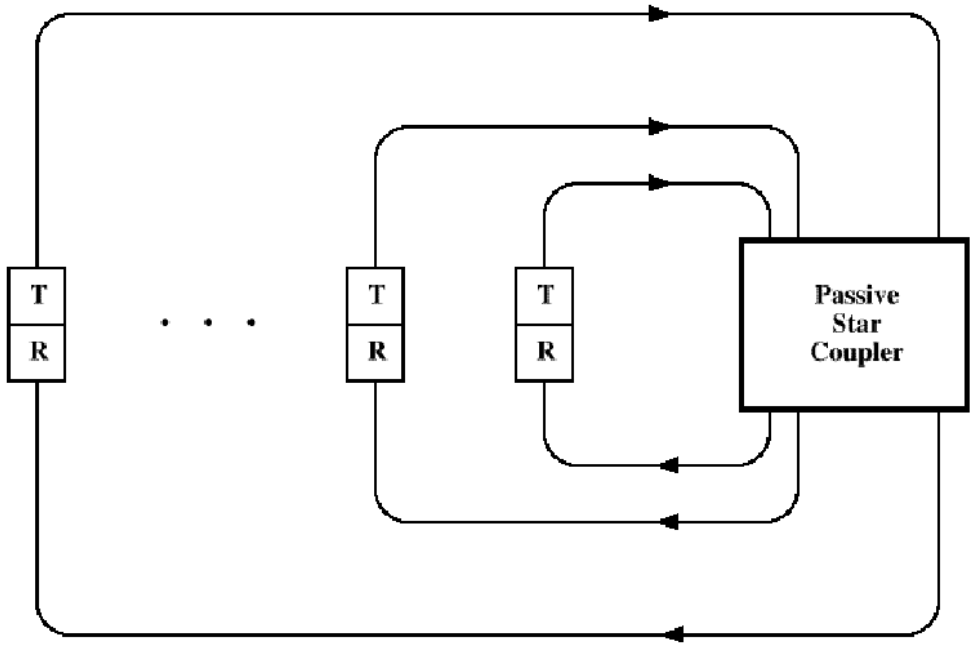
» Estrela realizada com acoplador óptico passivo (*star coupler*)

  – Dispositivo com N entradas e N saídas

» O sinal óptico aplicado numa entrada é dividido de forma aproximadamente igual pelas saídas

  – A atenução do sinal é provocada pela divisão de potência mas também pelas perdas intrínsecas devidas ao acoplamento

» A topologia física é uma estrela mas a topologia lógica é equivalente a um barramento



Acopladores ópticos em estrela – análise

» As perdas totais num acoplador em estrela (*star coupler*) resultam das perdas intrínsecas (*Excess Loss*) e da divisão de potência pelas *N* portas de saída

$$E_c + 10\log_{10} N$$

» Enquanto num barramento óptico as perdas intrínsecas crescem linearmente com o número de acopladores direccionais, num acoplador em estrela as perdas intrínsecas estão concentradas num único dispositivo – e crescem aproximadamente com o logaritmo do número de portas

$$E_c \sim E_2 * \log_2 N$$

sendo E_2 as perdas num acoplador com 2 portas de entrada e 2 de saída

» Então as perdas totais podem ser aproximadas por

$$E_2 * \log_2 N + 10\log_{10} N \sim (E_2 + 3) * \log_2 N$$

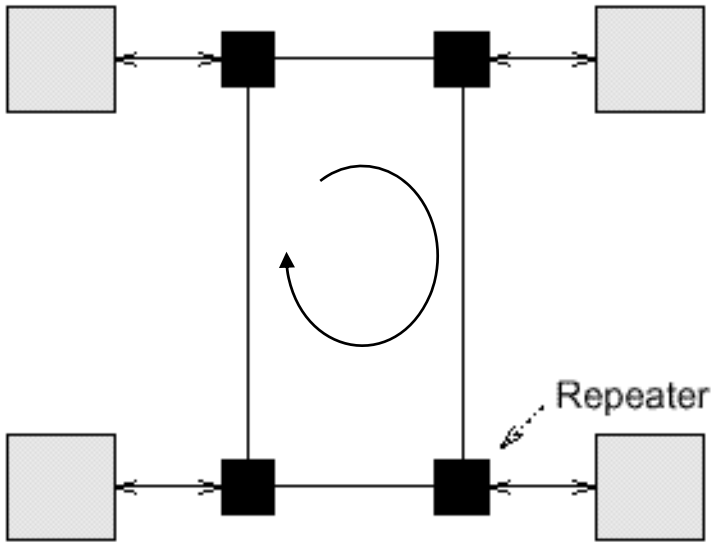
» Se considerarmos E_2 ~ 1 dB e uma margem de potência da ordem de 40 dB, o valor máximo de *N* será da ordem de 1000

Topologia em anel – caracterização

» Um anel é constituído por repetidores (elementos activos) unidos por ligações ponto a ponto unidireccionais, formando um percurso fechado para o sinal

- As estações ligam-se aos repetidores para poderem transmitir e receber tramas
- Cada repetidor liga-se a dois repetidores adjacentes (a montante e a jusante)
- O sinal é transmitido de um repetidor para o seguinte (a jusante)

» O atraso do sinal no anel (latência) resulta do atraso de propagação no meio e do atraso nos repetidores



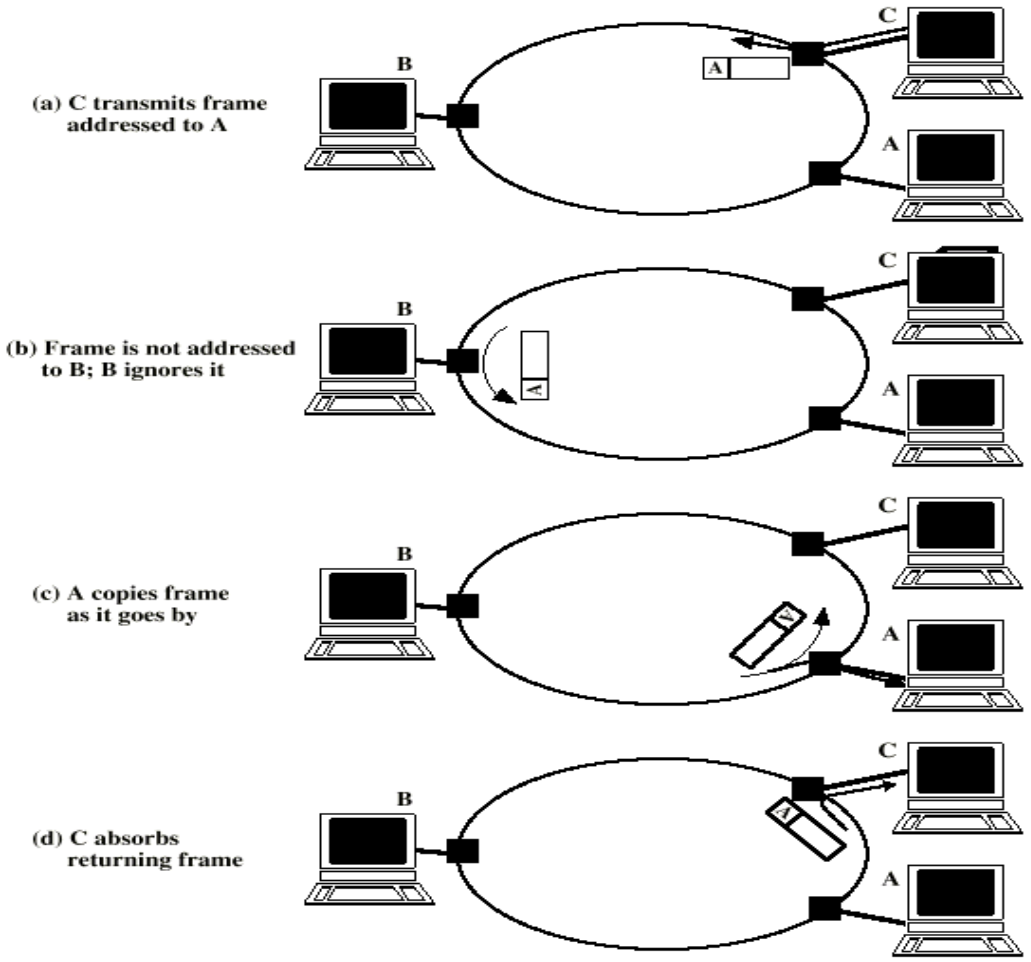
Topologia em anel – acesso ao meio

» Os dados são enviados em tramas endereçadas
  – As tramas circulam no anel
  – Se uma estação reconhecer que uma trama que lhe é destinada, copia a trama para um *buffer* interno
    » Casos possíveis – o endereço de destino da trama coincide com o endereço *unicast* da estação, é o endereço *broadcast* ou é um endereço *multicast* de um grupo a que a estação pertence
  – Conforme o protocolo, uma trama pode ser removida do anel pela estação (repetidor) de origem ou de destino – remover uma trama significa que a trama não é retransmitida pelo repetidor
    » No caso de uma trama com endereço de destino *broadcast* ou *multicast* a remoção é necessariamente feita pela estação de origem

» É necessário um protocolo para controlo de acesso ao meio
  – Define as condições em que uma estação pode transmitir (inserir uma trama no anel)
  – Dependendo do protocolo de acesso pode haver ou não acessos simultâneos por parte de várias estações e pode haver uma ou mais tramas (completas ou não) em circulação no anel

Topologia em anel – remoção de uma trama

Exemplo com remoção da trama pela estação (repetidor) de origem



Topologia em anel – características

» Meio de transmissão partilhado
  – As tramas enviadas pelas várias estações circulam no anel, que oferece um único percurso para os dados
» Possibilidade de endereçamento múltiplo (*multicast*, *broadcast*)
  – Obriga a que uma trama percorra todo o anel, para permitir cópia pelas estações endereçadas
» Ligações ponto a ponto entre repetidores
  – A regeneração do sinal garante maior imunidade a erros e permite cobrir maiores distâncias
  – É possível usar cabo coaxial, par entrançado ou fibra óptica
» Vulnerabilidade
  – A rede torna-se inoperacional por falha duma ligação ou dum repetidor (deixa de haver continuidade física para o sinal)
» Latência
  – Aumenta com o número de estações ligadas à rede, com possível impacto no desempenho
» Inserção / remoção de repetidores
  – Cria dificuldades de instalação, reconfiguração e manutenção (cablagem, detecção de falhas)
  – Provoca alterações não controladas do comprimento do anel (e portanto da latência)
» Necessário mecanismo de remoção de tramas

Funções dos repetidores

Os repetidores desempenham duas funções importantes numa rede em anel

» Regeneração e retransmissão do sinal, permitindo a sua circulação no meio

» Acesso ao meio por parte da estação ligada a cada repetidor

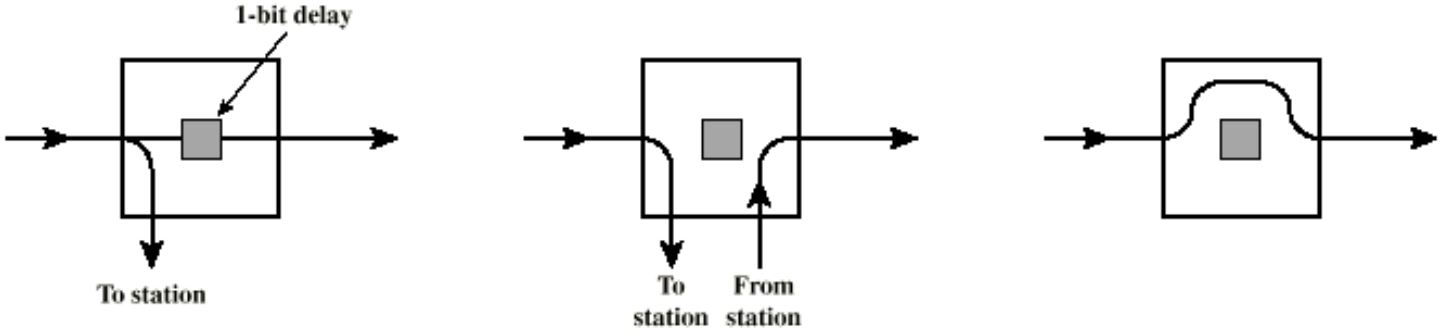
- Recepção de tramas (cópia de tramas para *buffers* internos da estação)
- Transmissão de tramas (inserção de tramas no meio)
- Remoção de tramas (isto é, não repetição de tramas, para evitar a sua circulação indefinida e assim permitir acesso ao meio por parte de outras estações)
- A remoção pela estação de origem tem algumas vantagens
  - » Permite enviar confirmação por parte da estação de destino (*piggyback*)
  - » Permite ordenar os acessos ao meio (*round robin*) e facilita o suporte de prioridades
  - » É obrigatória no caso de transmissão *multicast* ou *broadcast*
- A remoção pela estação de destino permite uma melhor utilização do meio
  - » Só possível no caso de transmissão *unicast*

Estados de um repetidor

» Escuta
  – Procura padrões de bits (endereços e bits associados ao protocolo de acesso)
  – Copia uma trama para a estação quando reconhece que a trama lhe é endereçada
  – Retransmite os bits com pequeno atraso, podendo ainda modificar bits do cabeçalho

» Transmissão
  – Quando a estação tiver dados e permissão para transmitir
  – Recebe bits em circulação – não os retransmite e copia-os para processamento por parte da estação (de acordo com o protocolo)

» *Bypass*
  – Permite isolar uma estação inactiva, que assim não contribui com atraso (latência) adicional
  – Em caso de falha permite isolar um repetidor e a estação correspondente

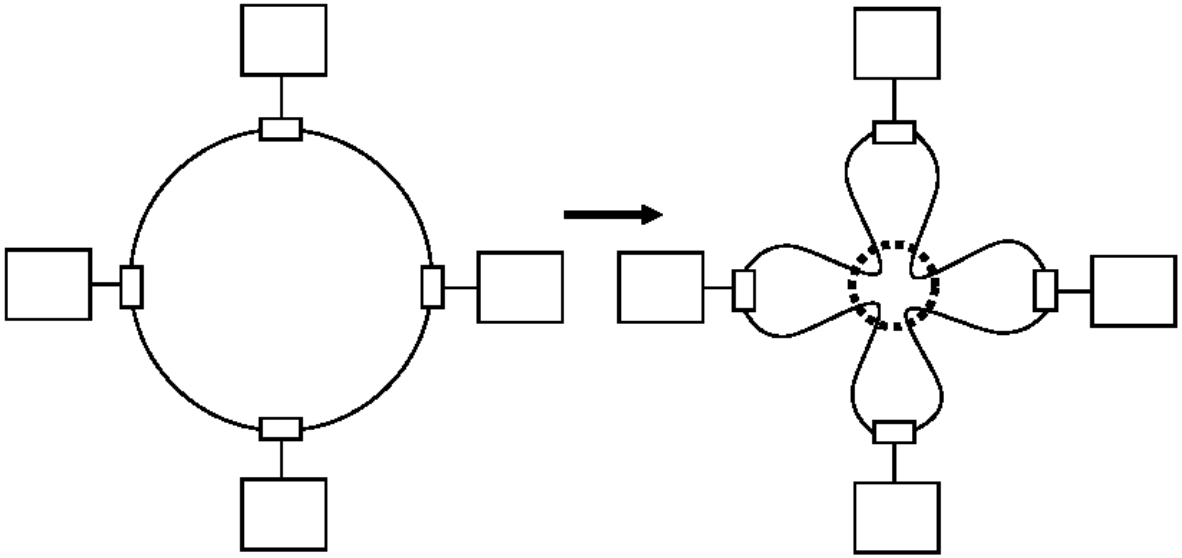


(a) Listen state (b) Transmit state (c) Bypass state

Star Ring – anel-em-estrela

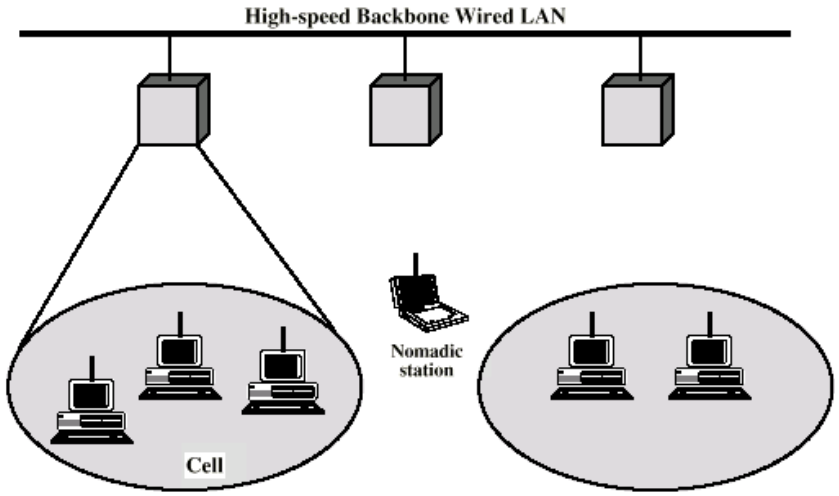
» A utilização de *Wiring Concentrators* (concentradores de cabos, constituídos por relés activados remotamente pelas estações) numa configuração física em estrela (*Star Ring*) permite solucionar alguns dos problemas referidos

– Facilita a manutenção (acesso centralizado) e a localização de falhas
– Permite isolamento (*bypass*) de elementos defeituosos (fiabilidade)
– Permite inserção / remoção automática de estações (reconfiguração)

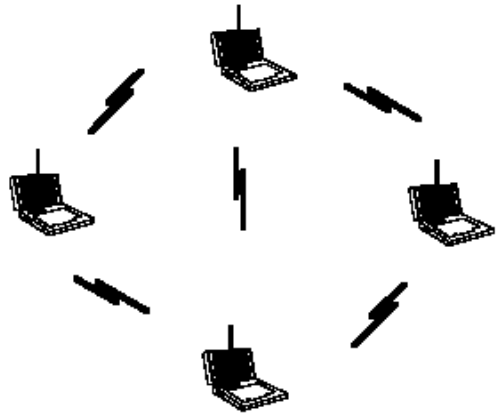


LANs sem fios

- Transmissão por propagação no espaço livre
- Aplicações
  - Extensão de LANs
  - Interligação de edifícios
  - Acesso de terminais móveis
  - Redes *ad-hoc*
- Requisitos específicos
  - Reduzido consumo de energia
  - Robustez e segurança de transmissão
  - Espectro não licenciado
  - Configuração dinâmica
- Tecnologias
  - Infravermelhos, *spread spectrum*, rádio frequências



(a) Infrastructure Wireless LAN



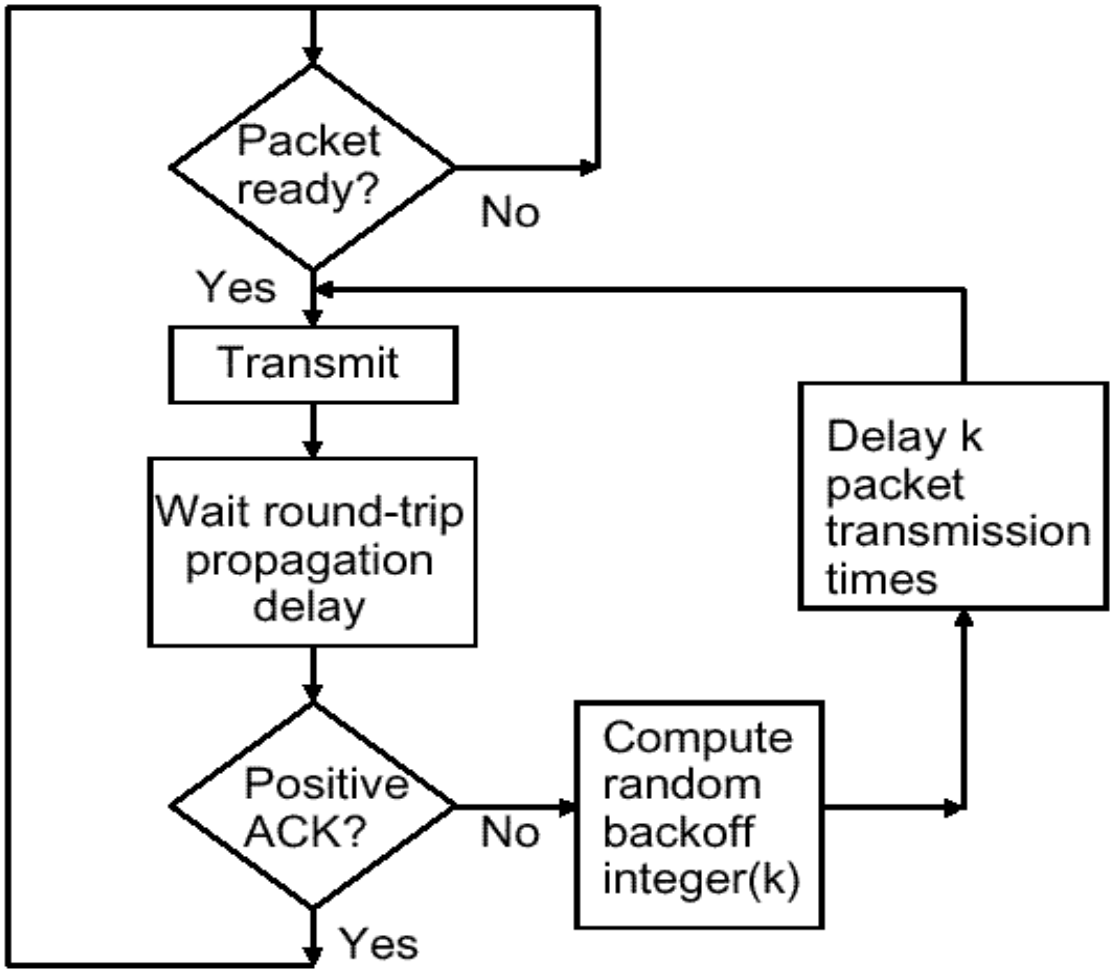
(b) Ad hoc LAN

Protocolos e Sistemas

ALOHA

- A rede Aloha (*packet radio*) foi desenvolvida na Universidade do Hawaii com o objectivo de ligar terminais remotos a um computador central
- Estação emissora – quando tem uma trama pronta para transmitir, transmite incondicionalmente (*talk when you please*)
  - Transmissões simultâneas provocam colisões, mas com a rede pouco carregada o atraso no acesso ao meio é pequeno visto a probabilidade de colisões ser baixa
- Estação receptora – confirma tramas correctamente recebidas (ACK positivo)
- Detecção de colisões
  - A estação emissora espera confirmação positiva (ACK) durante *round trip time*
    - Se receber ACK, pode transmitir nova trama
    - Se não receber ACK, ocorreu colisão ou a trama foi corrompida por outra razão – a estação deve retransmitir, podendo tentar um número máximo de vezes predefinido, após o que desiste
  - Nalguns casos (satélite) uma colisão pode ser detectada comparando a trama transmitida com a trama recebida após o tempo de propagação
- Retransmissão
  - Para minimizar a probabilidade de novas colisões, a estação emissora espera intervalo de tempo aleatório antes de retransmitir uma trama não confirmada

ALOHA – protocolo de acesso



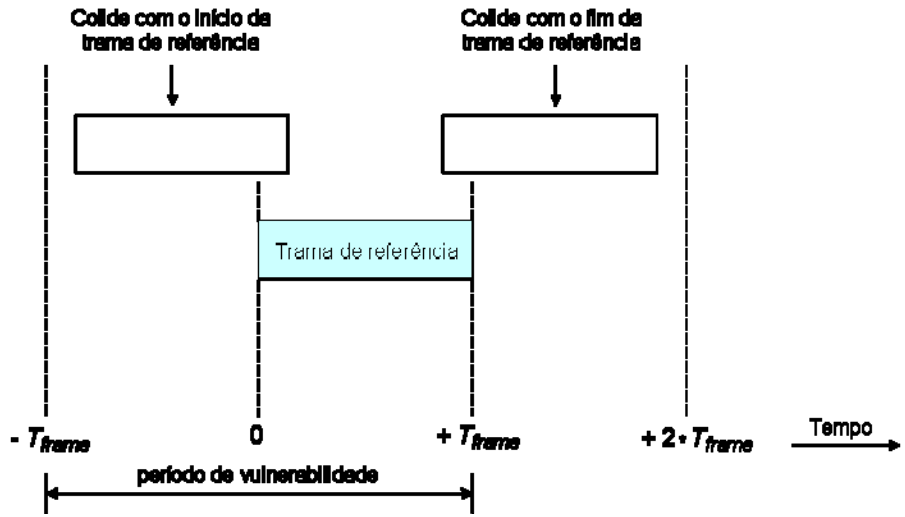
ALOHA – eficiência

- Período de vulnerabilidade de uma trama
  - Assumindo tramas com o mesmo comprimento, o período de vulnerabilidade de uma trama é o dobro do tempo de transmissão da trama (T_{frame})
  - Uma colisão ocorre se outra transmissão se iniciar no intervalo] - T_{frame}, +T_{frame} [relativamente ao início de transmissão da trama
- Eficiência
  - S – tráfego útil (relativo) transmitido, ou seja, representa a eficiência do protocolo
    - S é sempre inferior a 1
  - G – tráfego total (relativo) oferecido
    - G pode ser superior a 1 (pois inclui as transmissões que resultam em colisão e as respectivas retransmissões)

$S = G\, e^{-2G}$

- Eficiência máxima

$S_{max} = 18.4\ \%\ (G = 0.5)$

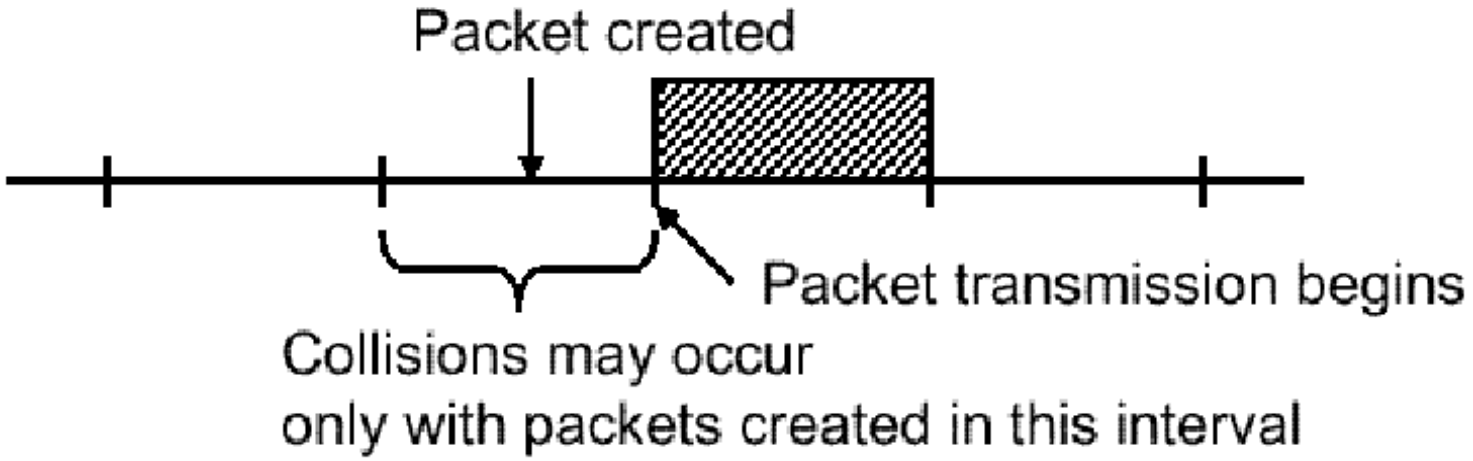


Slotted ALOHA

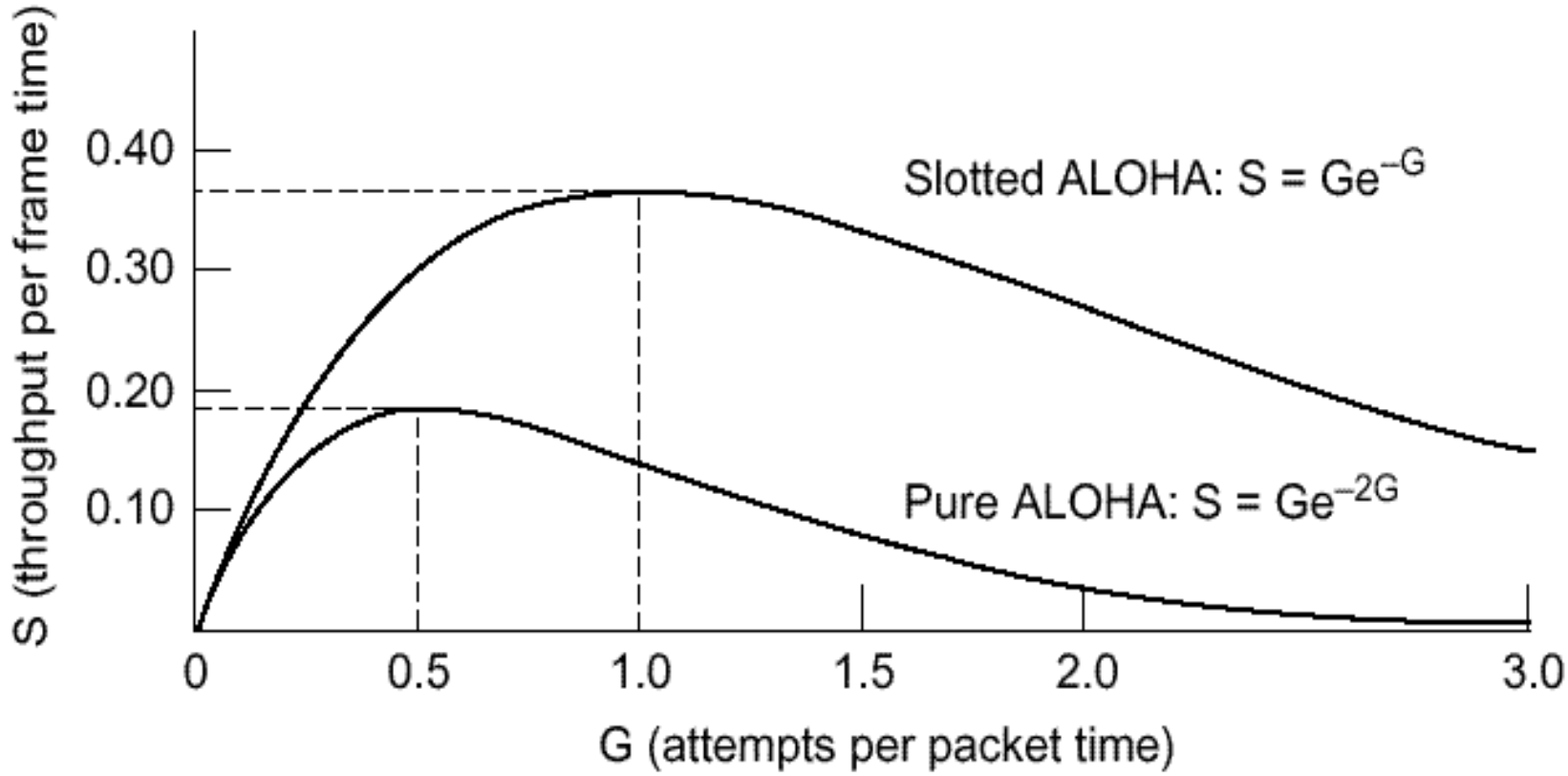
- Estações sincronizam transmissões pelo início de *time slots*
  - Necessário mecanismo para distribuir às estações um sinal de sincronização de início dos *time slots*
  - Quando uma estação tem uma trama pronta a transmitir, espera pelo início do próximo *time slot* e transmite incondicionalmente
  - Não ocorrem colisões parciais – ou não há colisão ou a colisão é total, pelo que o período de vulnerabilidade é igual a T_{frame} (ou seja a duração do *time slot*, desprezando atrasos de propagação)
- Eficiência

  $S = G\, e^{-G}$
- Eficiência máxima

  $S_{max} = 36.8\ \%\ (G = 1)$



Aloha e Slotted ALOHA – eficiência



Carrier Sense Multiple Access (CSMA)

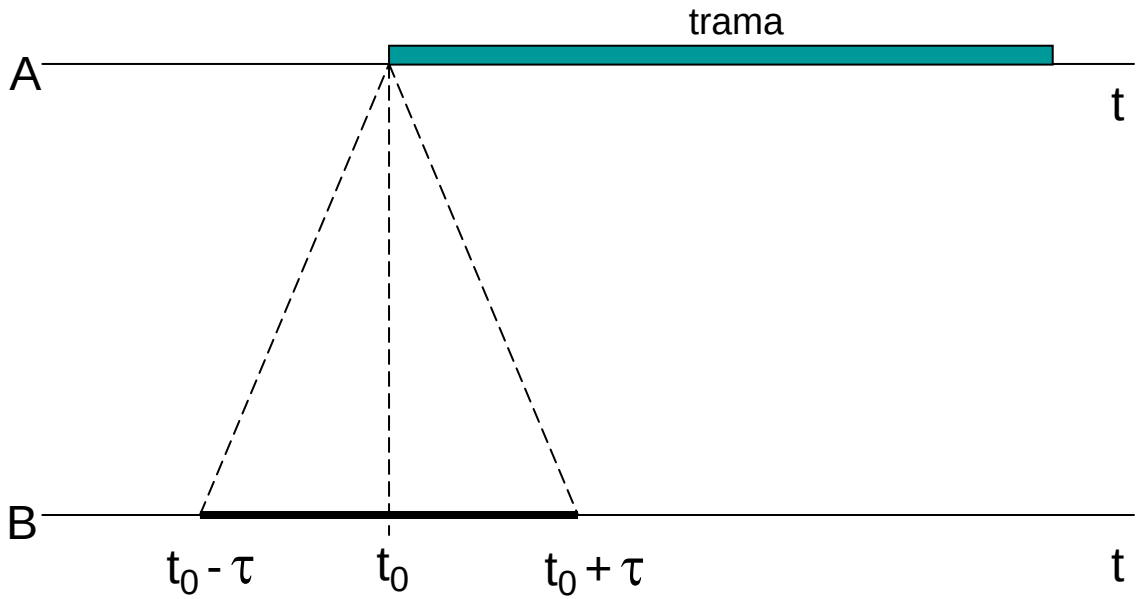
- Nos protocolos do tipo CSMA uma estação escuta o meio (*carrier sense*) antes de transmitir (*listen before talk*) – não inicia uma transmissão (defere) se tiver detectado que outra transmissão está em curso (meio ocupado), evitando assim uma colisão certa
  - Após iniciar uma transmissão, uma estação não continua a escutar o meio (ao contrário de CSMA/CD), pelo que não detecta directamente eventuais colisões
- A escuta do meio não evita o risco de colisões, pois é possível que diferentes estações iniciem transmissões presumindo que o meio está livre
- As colisões não são detectadas durante a transmissão, isto é, uma estação completa sempre uma transmissão que tenha iniciado (mesmo que venha a ocorrer uma colisão)
- As colisões são detectadas indirectamente – após concluir uma transmissão, uma estação fica à espera de uma confirmação (ACK) durante um intervalo de tempo que não deve ser inferior a 2τ
  - Se não receber qualquer confirmação (o que pode dever-se à ocorrência de uma colisão ou outra causa), retransmite a trama após um intervalo de tempo aleatório (até um número máximo de vezes predefinido)

CSMA – período de vulnerabilidade

- Nas condições mais desfavoráveis, o período de vulnerabilidade de uma estação (ou seja, susceptibilidade a colisões resultantes de outras transmissões iniciadas durante esse período), é igual ao *round trip time* (2τ) no meio
- Se não se iniciar outra transmissão durante o período de vulnerabilidade, a estação adquire o meio em exclusividade e a transmissão é concluída com sucesso, o que constitui uma melhoria significativa em relação a Aloha
  - Uma trama pode sofrer uma colisão durante o tempo em que se propaga no meio, isto é, durante um intervalo de tempo igual a τ, após início da respectiva transmissão
- O uso de CSMA é recomendado quando o período de vulnerabilidade é muito menor que o tempo de transmissão de uma trama ($2\tau << T_{frame}$), ou seja, quando $a = \tau / T_{frame} << 1$, situação comum em LANs de baixa velocidade e com pequeno diâmetro, mas o desempenho degrada-se quando a aumenta

CSMA – período de vulnerabilidade (análise)

- Se A iniciar uma transmissão em t_0, tal será reconhecido por B em $t_0 + \tau$, e B não inicia qualquer transmissão após $t_0 + \tau$
- Se B iniciar uma transmissão antes de $t_0 - \tau$, tal será reconhecido por A antes de t_0 e A não inicia a transmissão em t_0
- A transmissão de A pode colidir com uma transmissão de B iniciada durante o intervalo $] t_0 - \tau, t_0 + \tau [$ de duração 2τ (período de vulnerabilidade) – uma eventual colisão ocorre algures no meio num instante no intervalo $] t_0 , t_0 + \tau [$



CSMA – variantes

» Persistente
  – Se meio livre: transmite
  – Se meio ocupado: espera até ficar livre e transmite

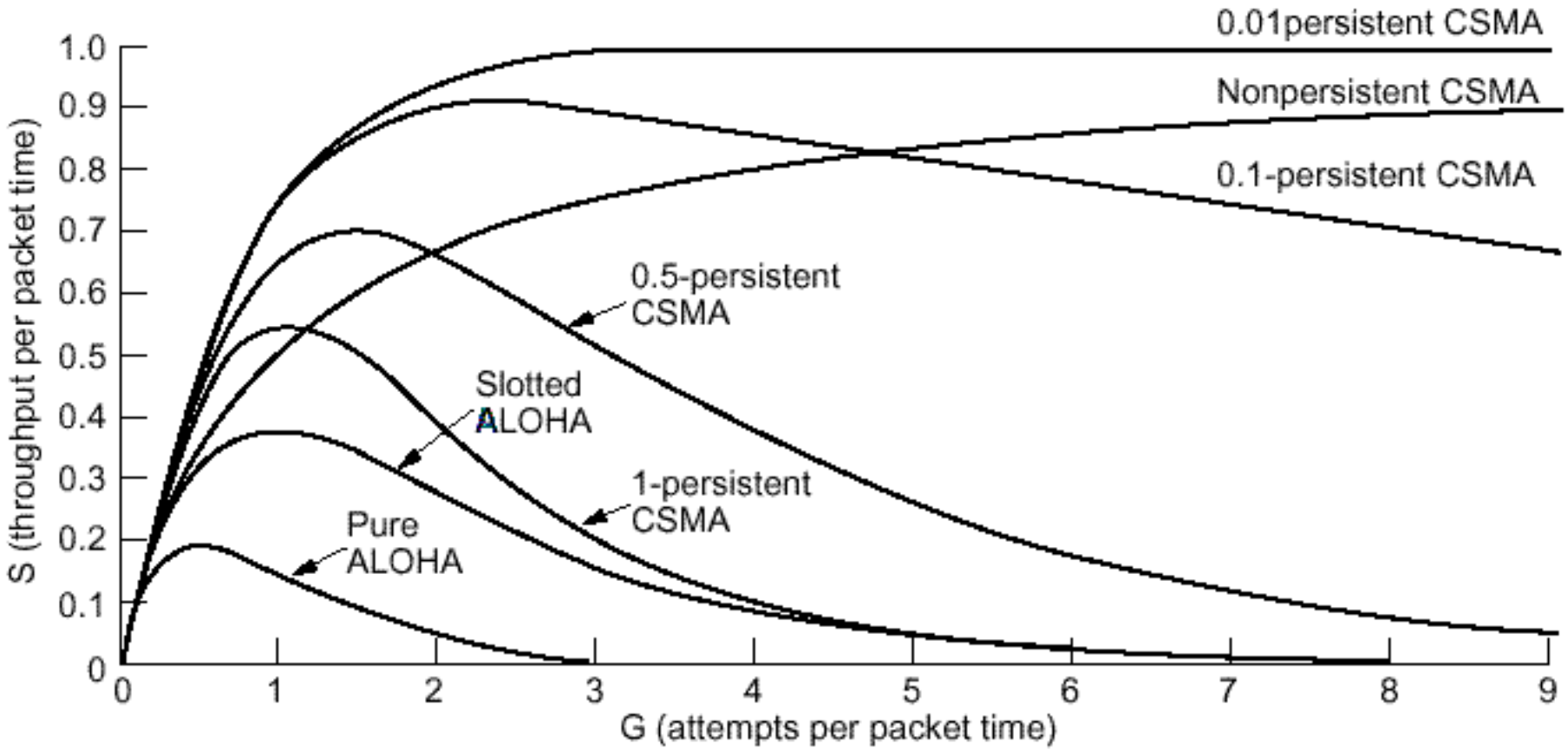
  Quando a rede está moderadamente carregada e a << 1, a probabilidade de duas estações iniciarem transmissões durante o período de vulnerabilidade é pequena, excepto se estiverem à espera que termine uma transmissão em curso (este problema é minimizado com variantes não persistentes)

» Não persistente
  – Se meio livre: transmite
  – Se meio ocupado: espera intervalo de tempo aleatório e repete o algoritmo

» p-persistente
  – *Slot time = round trip time* máximo na rede (usado para atrasar tentativas de acesso)
  – Se meio livre: transmite com probabilidade *p* e atrasa a tentativa de acesso de um *slot time* com probabilidade *1-p*, repetindo então o algoritmo; se encontrar o meio ocupado depois de antes ter encontrado o meio livre e ter deferido, espera intervalo de tempo aleatório e repete o algoritmo desde o início
  – Se meio ocupado: espera até ficar livre e aplica o algoritmo

CSMA – eficiência

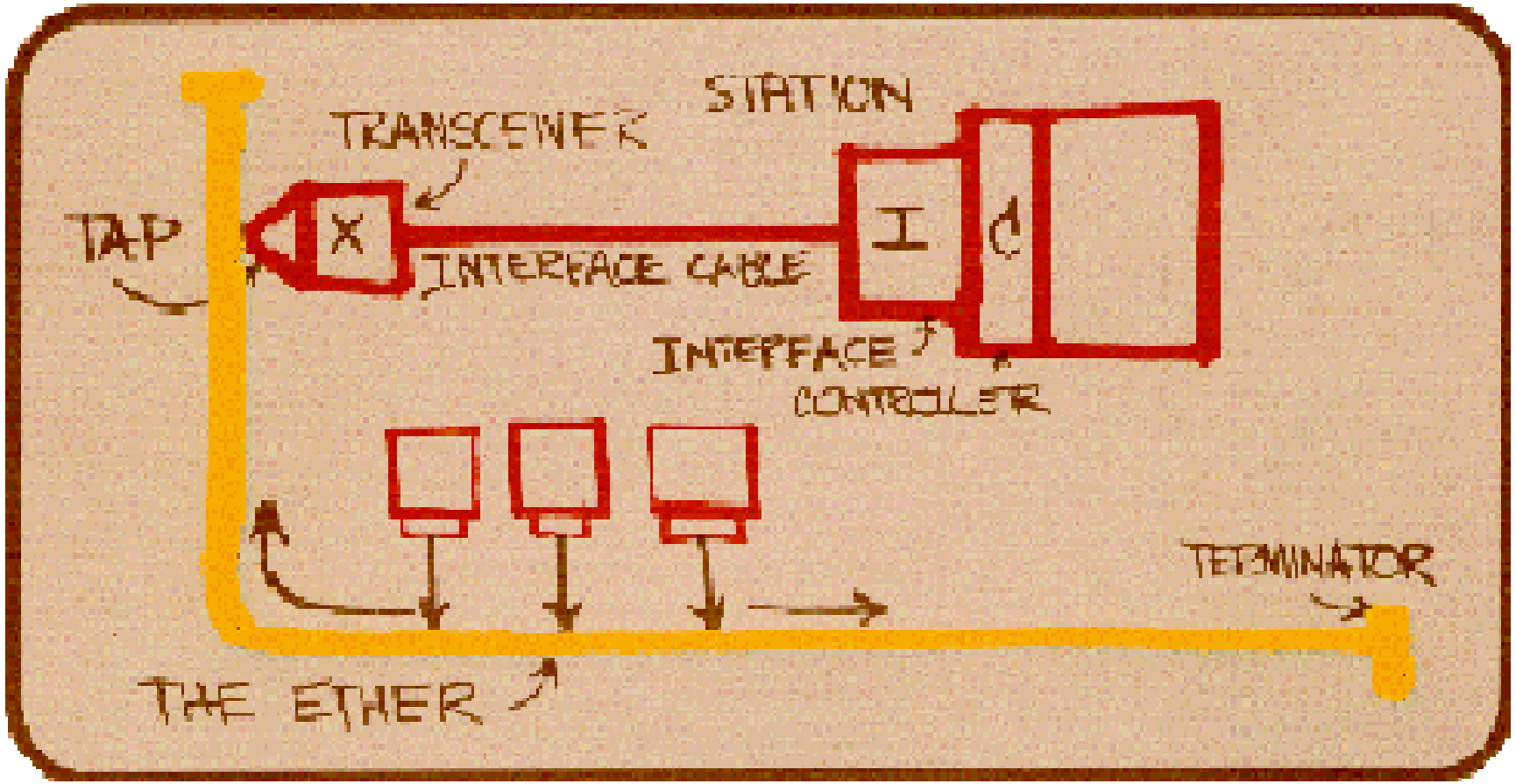
CSMA não persistente – S = G / (1 + G) (se a = 0)



Ethernet – origem e evolução

- A rede Ethernet foi desenvolvida no Centro de Investigação da Xerox em Palo Alto (PARC)
- A Ethernet experimental (1976) caracterizava-se por
  - Funcionar a 3 Mbit/s num segmento de cabo coaxial com comprimento máximo de 1 km
  - Adoptar um protocolo de acesso ao meio inovador – CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) – que constituía uma evolução de protocolos de acesso múltiplo do tipo contenção, como o Aloha e o CSMA
- A especificação produzida em 1980 pela DEC, Intel e Xerox (DIX) definiu uma velocidade de transmissão de 10 Mbit/s, em segmentos de cabo coaxial com comprimento máximo igual a 500 m, podendo ser coberta uma distância máxima (com repetidores) de 2.5 km
- A norma IEEE 802.3 adoptou os principais aspectos desta especificação
- A evolução das redes IEEE 802.3 processou-se em várias direcções
  - Utilização de pares de cobre em alternativa a cabo coaxial, em topologias físicas em estrela, sendo a difusão do sinal realizada por repetidores multiporta (*hubs*)
  - Utilização de comutadores (*switches*) substituindo total ou parcialmente os *hubs*, sem necessidade de substituir a infraestrutura de cabos instalada
  - Aumento da velocidade de operação para 100 Mbit/s (*Fast Ethernet*), 1 Gbit/s (*Gigabit Ethernet*) e 10 Gbit/s (*10G Ethernet*)

Ethernet – componentes



Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

» O protocolo CSMA/CD (usado pela primeira vez na Ethernet e adoptado pelo IEEE 802.3) baseia-se na detecção de colisões durante a transmissão – caso ocorra, uma colisão é detectada no máximo ao fim de um intervalo de tempo igual a 2τ (período de vulnerabilidade) após o início da transmissão

  – O período de vulnerabilidade é usado como unidade de tempo (*slot time*) para sincronizar as tentativas de retransmissão de tramas pelas estações após a ocorrência de uma colisão

» Uma estação escuta o meio antes de transmitir (*carrier sense*)

  – Se o meio estiver livre, a estação inicia a transmissão

  – Se o meio estiver ocupado, a estação espera até que fique livre e inicia a transmissão (adopta-se a variante persistente)

    » O mecanismo de detecção de colisões evita os problemas do CSMA persistente

» Uma estação continua a escutar o meio durante um intervalo de tempo igual ao *slot time* de contenção, após o início de uma transmissão (*listen while talk*), de forma a detectar uma eventual colisão e, caso isso aconteça, activar um mecanismo de recuperação

CSMA/CD – binary exponential back-off

Em condições normais, uma eventual colisão é detectada, no máximo, ao fim de um intervalo de tempo igual ao *slot time* de contenção, após o início de uma transmissão, pelo que apenas é necessário continuar a escutar o meio durante esse intervalo

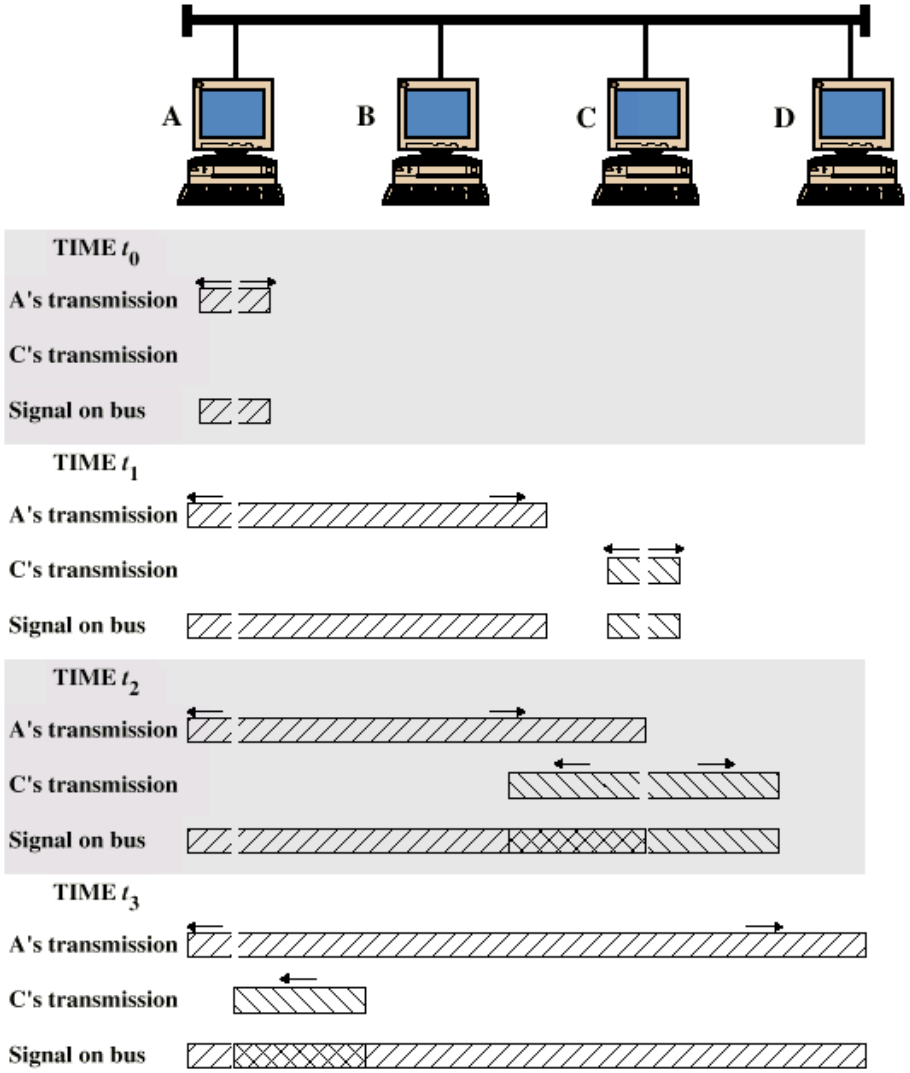
- Se não for detectada qualquer colisão, a estação completa a transmissão sem qualquer risco de colisão
- Se for detectada uma colisão, esta é reforçada (*jamming*), a estação aborta a transmissão e escalona (atrasa) a retransmissão da trama de acordo com um algoritmo designado *binary exponential back-off*
  - Na primeira tentativa de transmissão, o algoritmo é persistente ($p = 1$)
  - Após a ocorrência de uma colisão (a mesma trama pode sofrer várias colisões até eventualmente ser transmitida), a probabilidade de acesso p é reduzida a metade do valor anterior ($p = 1 / 2^n$) e a estação selecciona com probabilidade p um dos 2^n slots de contenção seguintes para iniciar a transmissão, caso o meio não tenha sido entretanto ocupado (n é o número de colisões sofridas por uma trama, pelo que $n = 0$ corresponde à primeira tentativa de acesso)

CSMA/CD – detecção de colisão

- Detecção de colisão num barramento
  - Tensão no barramento >> tensão do sinal devido a uma transmissão
- O efeito da atenuação deve ser considerado, o que limita a distância máxima em segmentos de cabo coaxial
  - 10Base5 – 500 m
  - 10Base2 – 185 m
- Para garantir detecção de colisão durante a transmissão é necessário impor a condição

$$T_{frame} \geq 2 \times \tau \Leftrightarrow a \leq 0.5$$

- Detecção de colisão num *hub*
  - Actividade em mais do que uma porta
  - O *hub* gera sinal de presença de colisão



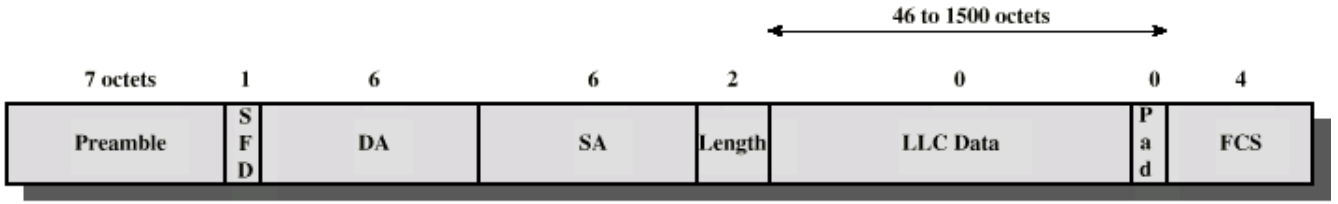
CSMA/CD – eficiência

- τ – tempo de propagação no cabo (extremo a extremo)
- 2τ – *round-trip time* = *slot time* de contenção
- T_f – tempo de transmissão de uma trama
- s – número médio de s*lots* de contenção necessários para aquisição do meio
- Eficiência

  $S = T_f / (T_f + s.2\tau) = 1 / (1 + 2sa)$
- **S** diminui com
  - Aumento da velocidade de transmissão (T_f diminui)
  - Aumento do comprimento do cabo (τ aumenta)
  - Aumento do número de estações activas (*s* aumenta, devido a aumentar a probabilidade de colisões)
  - Diminuição do comprimento dos pacotes (T_f diminui)
- Para uma rede CSMA/CD carregada, em condições óptimas (ideais)

  $S_{max} = 1 / (1 + 3.44\ a)$ (se a = 0.5, S_{max} = 36.8 %, como em *Slotted Aloha*)
- A norma IEEE 802.3 especifica uma distância máxima entre estações de cerca de 2.5 km a 10 Mbit/s – a 100 Mbit/s a distância máxima é cerca de 10 vezes menor (200 m), tendo sido necessário introduzir algumas alterações no protocolo para permitir distâncias da mesma ordem de grandeza a 1 Gbit/s

IEEE 802.3 – formato da trama MAC



SFD = Start of frame delimiter
DA = Destination address
SA = Source address
FCS = Frame check sequence

» *Preamble*
  – 7 octetos de 0s e 1s alternados (10101010)
  – Usado pelo receptor para sincronização de bit
» *Start of Frame Delimiter* – campo 10101011 que indica o início da trama
» *Destination Address* (DA), *Source Address* (SA) – endereços MAC de destino e origem
» *Length* – Comprimento do campo de dados (substitui o campo *Type* da Ethernet)
» *LLC Data* – Campo de dados (LLC PDU)
» *Pad* (*padding*) – octetos adicionados para garantir um comprimento mínimo da trama, que permita detecção de colisão durante a transmissão (*a* não pode exceder 0.5)
  – Comprimento mínimo da trama (excluindo Preâmbulo e SFD) – 512 bits (64 octetos)
  – Comprimento máximo do campo de dados – 1500 octetos (trama – 1518 octetos)
» *FCS* – CRC de 32 bits

IEEE 802.3 / Ethernet a 10 Mbit/s

As especificações IEEE 802.3 a 10 Mbit/s incluem as seguintes (principais) alternativas ao nível físico

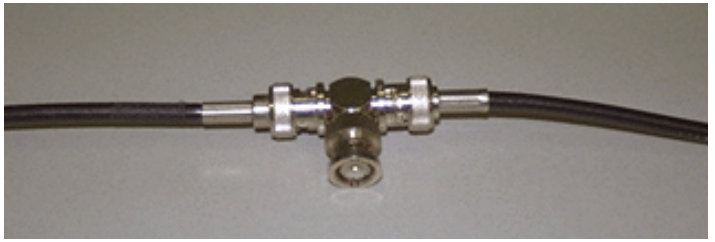
- Cabo coaxial em banda base
  - Topologia física: barramento
  - Especificações: 10Base5 e 10Base2
  - A utilização de repetidores interligando segmentos de cabo coaxial permite estender a cobertura física da rede
- Par de cobre entrançado (UTP – *Unshielded Twisted Pair*)
  - Topologia física: estrela
  - Especificação: 10Base-T
  - O elemento central da topologia é um *hub* (repetidor multiporta)
  - Esta configuração pode evoluir para uma rede comutada, substituindo *hubs* por comutadores, sem necessidade de reconfigurar a infraestrutura física

Cabo coaxial – 10Base5 e 10Base2

» Caracterização
  – Sinal digital → codificação Manchester ou Manchester Diferencial
  – Usado todo o espectro de frequências do cabo
  – Canal único, transmissão bidireccional
  – Usado na Ethernet a 10 Mbit/s; cabo com impedância 50 Ω

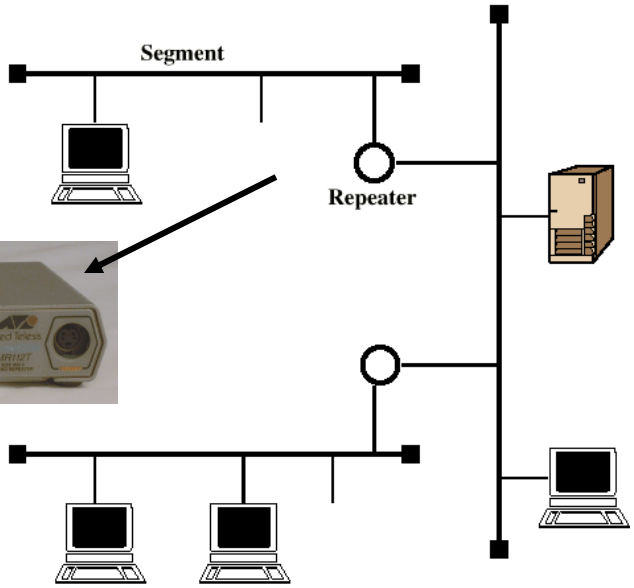
» 10Base5 (10 Mbit/s, *Baseband*, 500 m de comprimento)
  – Diâmetro do cabo – 1 cm (0.4 polegadas)
  – Comprimento máximo do cabo – 500 m
  – Distância entre estações adjacentes – múltipla de 2.5 m
  – 100 estações por segmento, no máximo

» 10Base2 (10 Mbit/s, *Baseband*, 200 m de comprimento)
  – Diâmetro do cabo – 0.6 cm (0.25 polegadas)
  – Mais flexível, mais barato (inicialmente designado *Cheapernet*)
  – Maior atenuação, menor imunidade ao ruído
  – Menor número de estações por segmento (30), menor comprimento do cabo (185 m)



Ligação de segmentos com repetidores e bridges

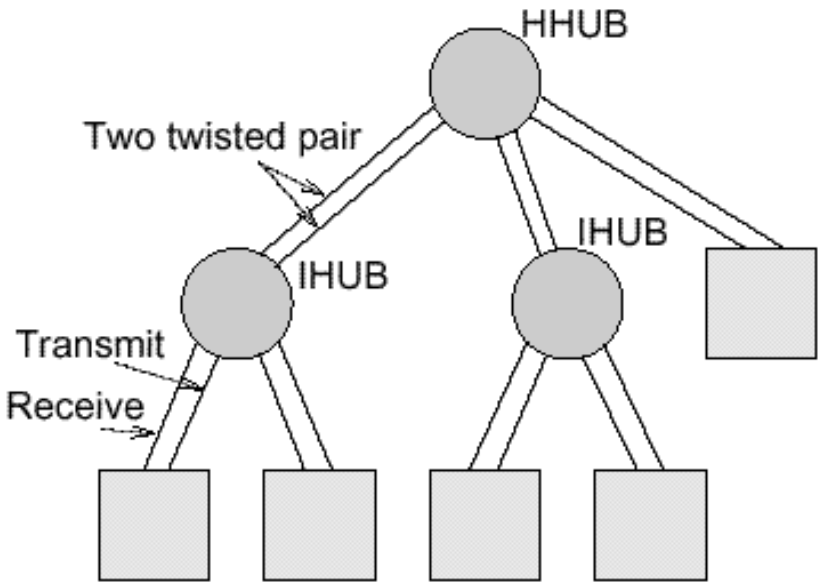
» Repetidores
  – Unem dois segmentos de cabo coaxial; retransmitem num segmento o sinal recebido no outro segmento
  – Transmissões simultâneas nos dois segmentos provocam colisões
  – Existe um único trajecto possível entre duas quaisquer estações
  – Distância máxima entre estações: 2.5 km em 10Base5 e 1 km em 10Base2



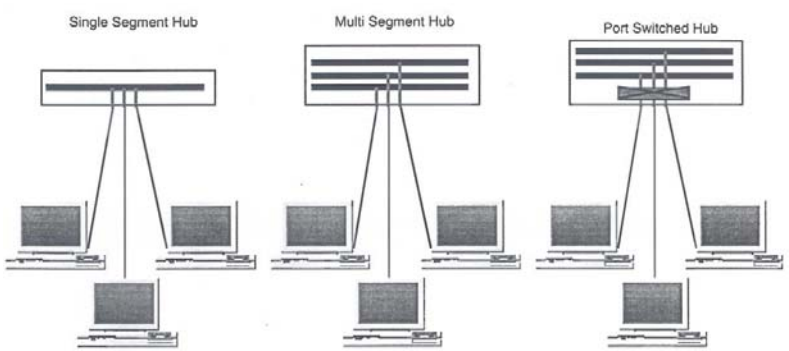
» *Bridges*
  – Ligam dois ou mais segmentos de cabo coaxial
  – As *bridges* operam na camada MAC e filtram ou retransmitem tramas (*forwarding*) com base em endereços MAC
  – Nas redes IEEE 802.3 foi definido um mecanismo de *bridging* transparente que requer que a topologia lógica seja aberta, mesmo que a topologia física contenha ciclos (*loops*)

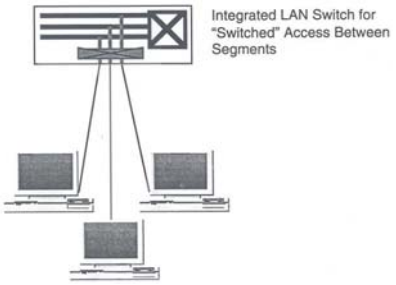
Twisted pair – 10Base-T

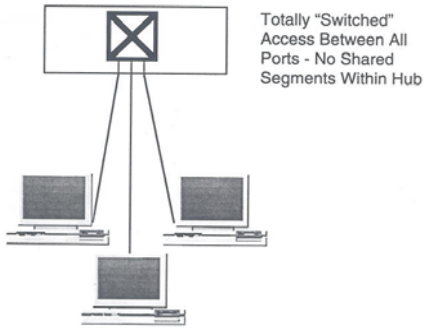
- A utilização de pares de cobre entrançados (UTP5) em redes em estrela começou por ser uma alternativa à utilização de cabo coaxial a 10 Mbit/s, devido ao seu menor custo e à possibilidade de exploração de cablagens estruturadas
- O elemento central desta configuração, designada 10Base-T, é um repetidor multiporta (*hub*)
- A ligação a um *hub* é realizada com dois pares de cobre (emissão e recepção), sendo possível mais do que um nível de *hubs*
- Esta configuração é igualmente usada nas redes IEEE 802.3 a 100 Mbit/s e 1 Gbit/s
- O comprimento máximo das ligações UTP5 é cerca de 100 m, a 10 e 100 Mbit/s
- A interligação de estações, directamente ou através de *hubs*, pode fazer-se actualmente com recurso a dispositivos que, tal como as *bridges*, processam tramas – comutadores de LAN (*LAN switches*)



Evolução – de hubs a comutadores







- Os *hubs* podem internamente suportar um ou mais segmentos independentes
- *Port-switched hubs* permitem associar (por configuração, mas de forma estática) cada porta a um dos segmentos internos
- Em ambos os casos, os segmentos internos são interligados por meio de dispositivos externos (e.g., *bridges* ou *routers*)
- Alguns fabricantes suportaram a interligação dos segmentos internos por meio de módulos adicionais (e.g., *bridges* ou *routers*), ligados ao *backplane* do *hub*
- Os comutadores (*LAN switches*) constituem o passo seguinte e final nesta evolução – o tráfego é comutado directamente entre portas, por meio de um núcleo de comutação (que pode basear-se em arquitecturas diferentes)

Hubs e comutadores

Hub

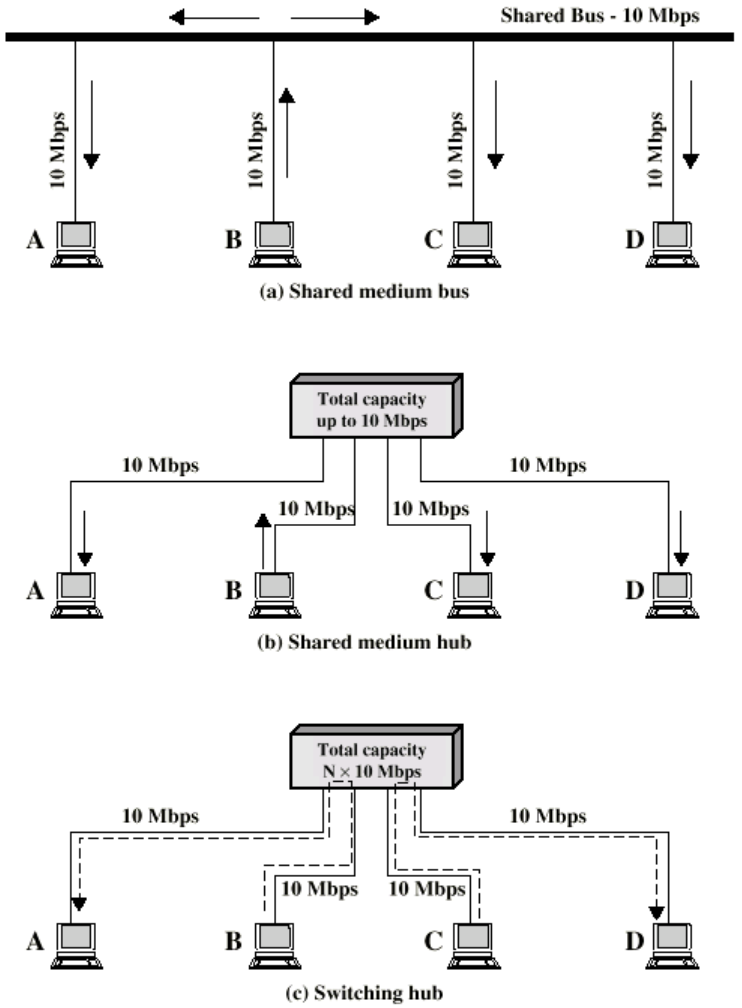
Comutador *(LAN switch)*

Cisco Catalyst 2960

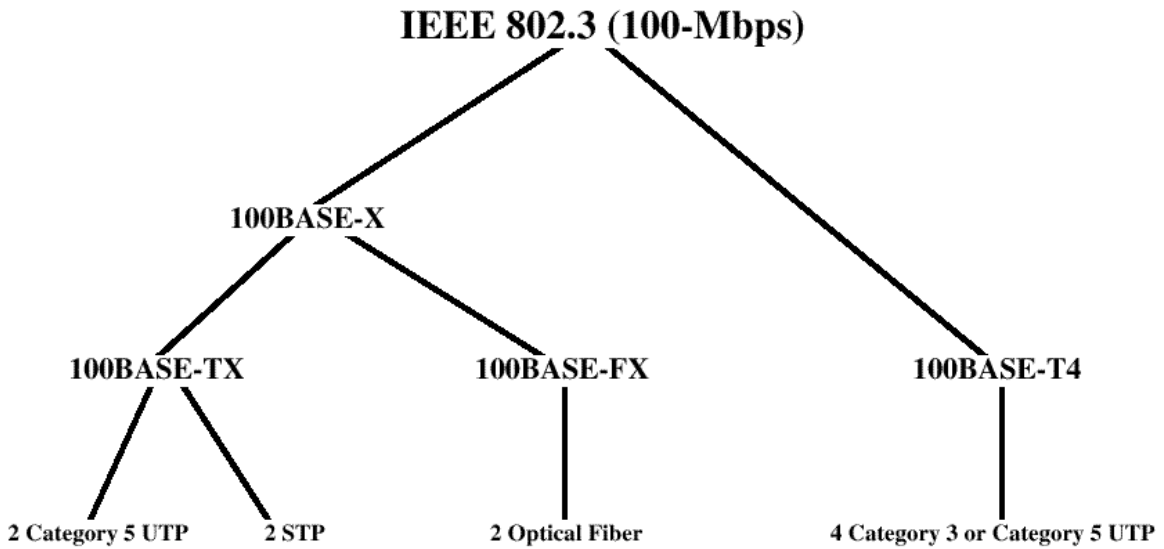
Hubs e comutadores – comparação

» *Hub*
  – Repetidor multiporta
  – Recebe o sinal numa porta de entrada e retransmite-o nas outras portas de saída
  – São impossíveis transmissões simultâneas com sucesso (podem ocorrer colisões)
  – A capacidade do meio é partilhada por todas as estações (como num barramento)

» LAN comutada
  – Os comutadores de tramas (LAN *switches*) são funcionalmente idênticos a *bridges*
    » As tramas são comutadas com base no endereço MAC de destino das tramas
  – É possível comutação simultânea entre diferentes pares de portas
  – A capacidade de uma porta é partilhada apenas pelas estações a ela ligadas (no limite, uma estação – LAN privada)

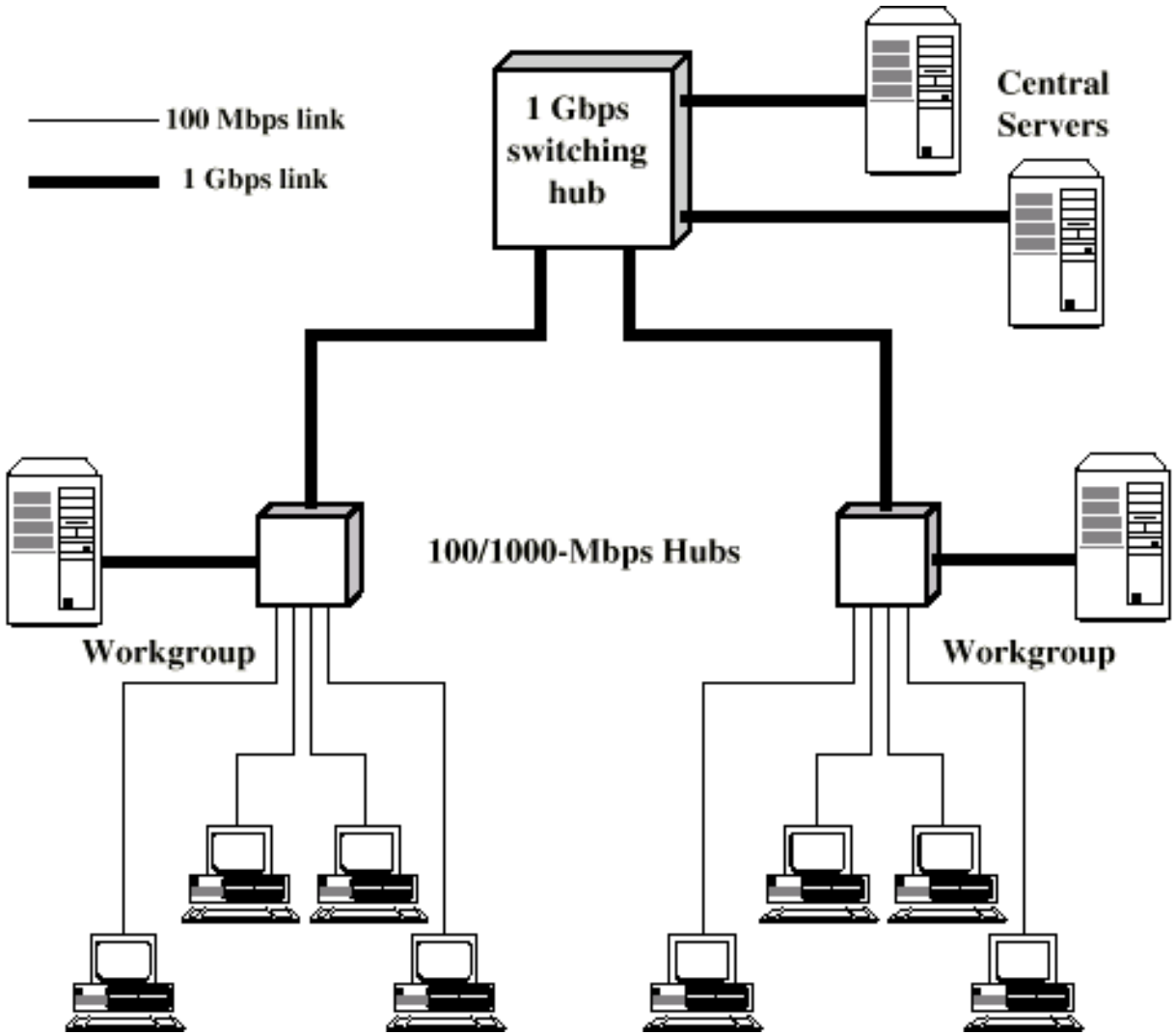


Ethernet a 100Mbit/s (Fast Ethernet)



- 100BASE-TX
  - 2 pares, STP / UTP5, código 4B5B
- 100BASE-FX
  - 2 fibras ópticas, código 4B5B
- 100BASE-T4
  - 4 pares, UTP3/4/5, código 8B6T

Gigabit Ethernet



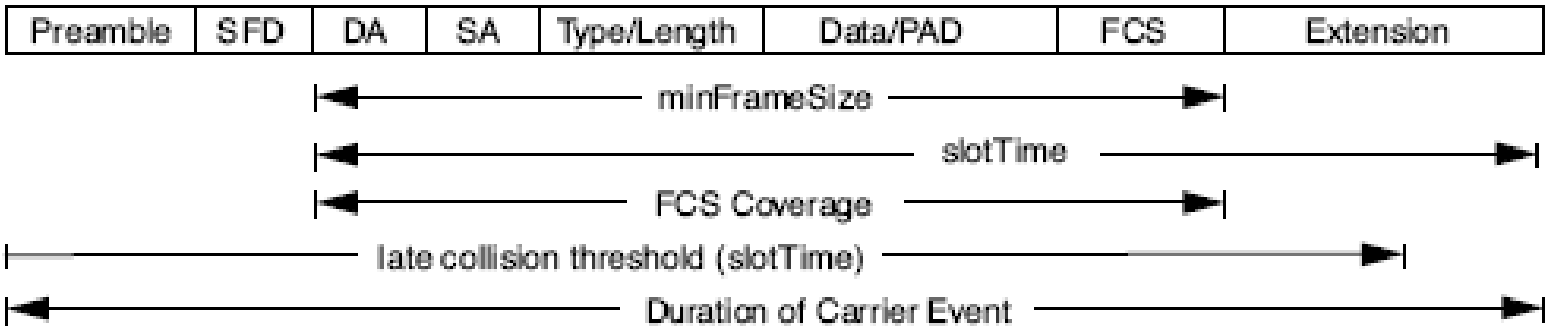
Gigabit Ethernet – extensões

» Dois modos de funcionamento possíveis
  – *Full-duplex* (ponto a ponto, CSMA/CD inibido)
  – *Half-duplex* (CSMA/CD)

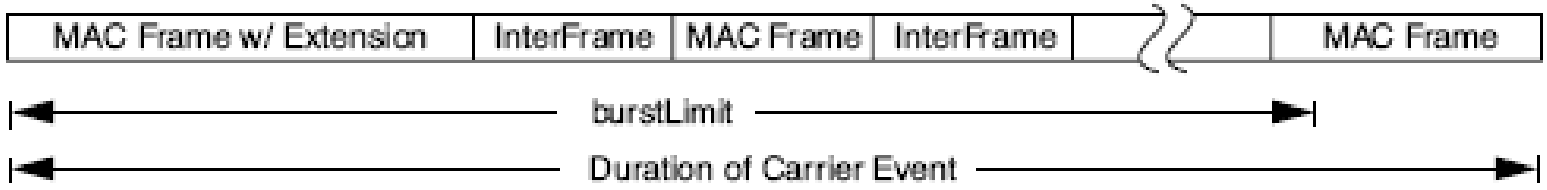
» Alteração do protocolo básico para funcionamento *half-duplex*
  – O protocolo CSMA/CD baseia-se no conceito de *slot* de contenção, que em Ethernet e Fast Ethernet corresponde à transmissão de 512 bits (sendo a duração do *slot* 51.2 μs e 5.12 μs, respectivamente)
  – Em Gigabit Ethernet, para garantir distâncias idênticas às possíveis em Fast Ethernet, foi definido um tamanho de *slot* de 4096 bits (com duração 4.096 μs) e imposto no máximo um repetidor no percurso
  – Foi definido um mecanismo de *carrier extension* para garantir ocupação do meio durante o tempo de um *slot* (permite detecção de colisão durante a transmissão), aumentando artificialmente o tamanho da trama (se inferior a 4096 bits)
  – Foi definido um mecanismo de *frame bursting* que permite transmitir várias tramas durante o mesmo acesso (após aquisição do meio), estando a primeira trama do *burst* sujeita ao mecanismo de *carrier extension* (visto poder ocorrer colisão enquanto não se esgotar o tempo correspondente ao *slot* de contenção)

Carrier extension e frame bursting

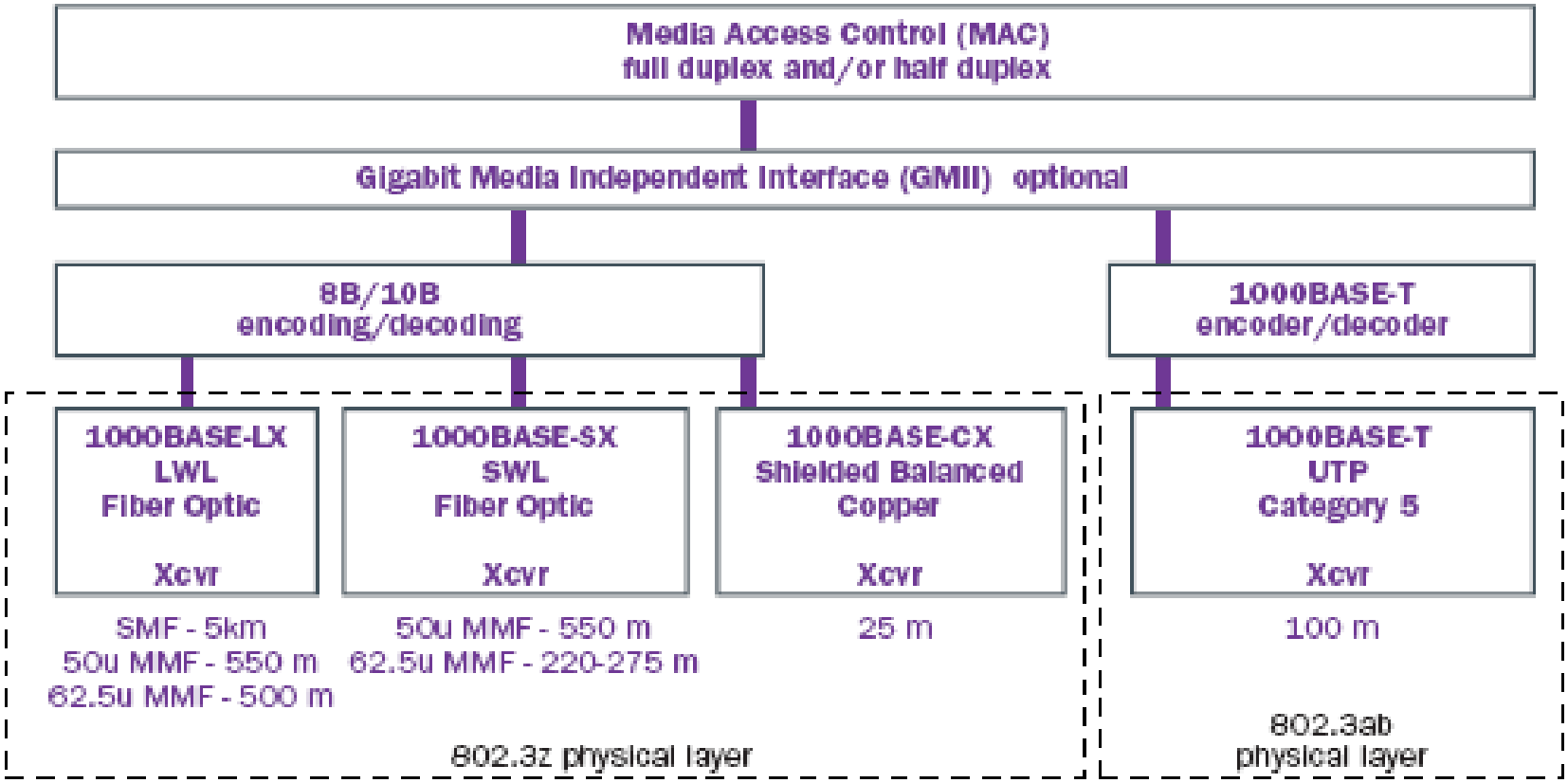
» *Carrier extension*



» *Frame bursting*



Gigabit Ethernet – arquitectura



Gigabit Ethernet – nível físico

- 1000BASE-SX
  - Comprimento de onda: 770 – 860 nm
  - Fibra multimodo, alcance: 550 m
- 1000BASE-LX
  - Comprimento de onda: 1270 – 1355 nm
  - Fibra multimodo / monomodo, alcance: 550 m / 5 km
- 1000BASE-CX
  - *Shielded twisted pair*, alcance: 25 m
- 1000BASE-T
  - 4 pares UTP5, alcance: 100 m

- Código – 8B10B (em 1000BASE-X)

Token Ring – princípio de operação

» Um protocolo de acesso do tipo *Control Token* baseia-se na circulação na rede de uma trama de controlo (*token*) que concede à estação que a recebe autorização para acesso exclusivo ao meio – o *token* funciona como um testemunho que é passado de estação em estação

» Em redes em anel (*Token Ring*), o *token* não precisa de ser endereçado – na ausência de qualquer transmissão, deve circular no anel um *token* no estado livre, isto é, uma trama constituída apenas por um campo de controlo com os respectivos delimitadores de início e fim

» Uma estação pronta a transmitir espera a passagem do *token* livre, captura-o (isto é, muda o seu estado para ocupado), passando a deter acesso exclusivo ao meio, o que lhe permite iniciar a transmissão de uma ou mais tramas

» Em geral uma trama é apenas copiada pela estação (ou estações) de destino, sendo removida pela estação de origem, a quem compete a libertação de um novo *token* no estado livre, o que permitirá o acesso ao meio por parte da estação a jusante mais próxima que tenha uma trama pronta a transmitir

Token Ring – variantes de libertação do token

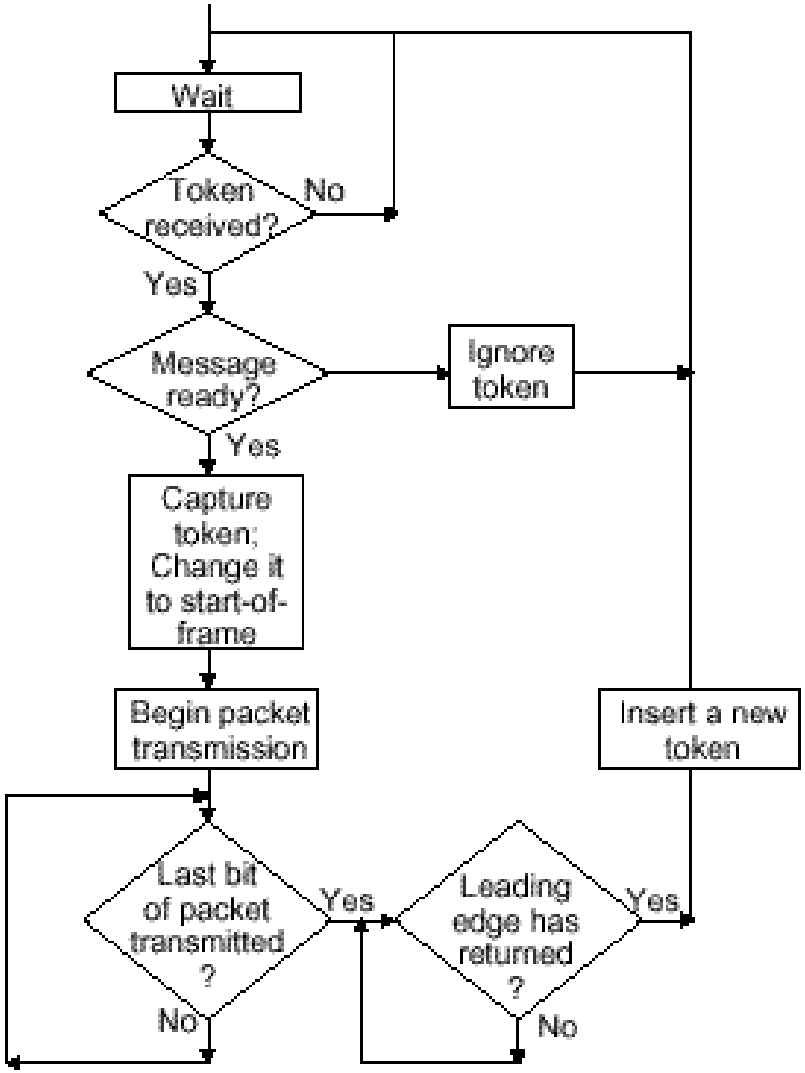
Critérios para libertação do *token* e respectivas condições a observar

- *Single Token* (IEEE 802.5 a 4 Mbit/s)
  - Condições: fim de transmissão de uma trama e início da sua remoção
    - Se $a < 1$, a primeira condição implica a segunda
    - A designação *Single Token* traduz o facto de não ser possível existir mais do que um *token* (livre ou ocupado) no anel – só pode circular um *token* livre depois de o *token* ocupado por uma trama ser removido; pode estar em circulação um fragmento de uma trama em remoção e uma nova trama (completa ou o seu início) ou um *token* livre
- *Multiple Token* (FDDI) / *Early Token Release* (IEEE 802.5 a 16 Mbit/s)
  - Condição: fim da transmissão de uma trama
    - A designação *Multiple Token* traduz o facto de ser possível existirem múltiplos *tokens* na rede, mas no máximo um no estado livre, estando os restantes ocupados, isto é, podem estar várias tramas em circulação, se a latência da rede o permitir ($a > 1$)
- *Single Packet*
  - Condição: fim da remoção de uma trama
    - A designação *Single Packet* traduz o facto de que só é possível libertar o *token* e iniciar uma nova transmissão depois de remover completamente a trama anterior
- *Single Token* e *Multiple Token* são equivalentes quando $a \leq 1$

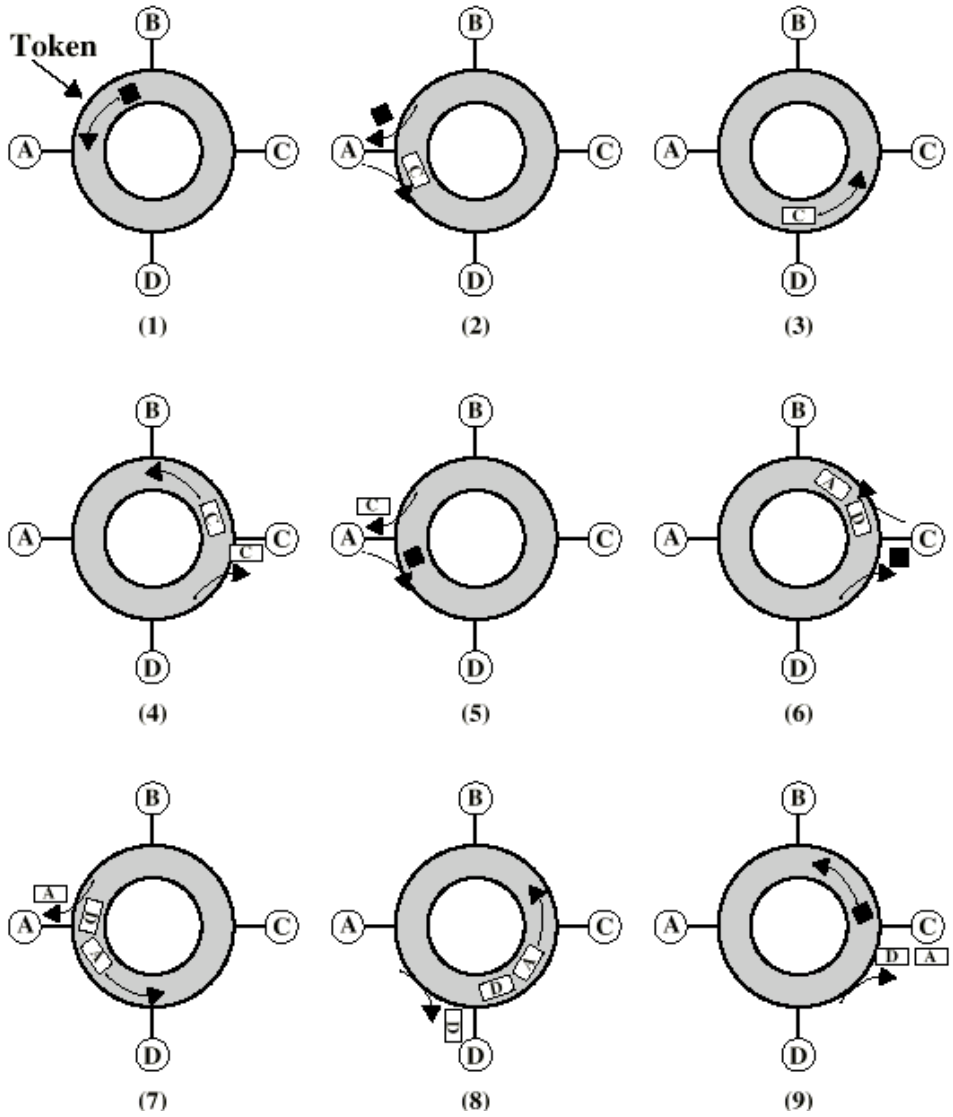
Token Ring IEEE 802.5

- Na ausência de transmissão circula no anel um *token* livre
- Estação pronta a transmitir
  - Espera o *token* livre
  - Muda o estado do *token* para ocupado
  - Anexa o resto da trama de dados
  - Quando a trama completa uma volta ao anel a estação inicia a sua remoção
  - A especificação inicial (4 Mbit/s) adopta a variante *Single Token*, isto é, a estação insere um novo *token* livre quando, após completar a transmissão da trama, tiver igualmente removido o respectivo cabeçalho (que transporta um *token* ocupado)
    - A segunda condição permite suportar o mecanismo de reserva de prioridade (nível desejado inserido no próximo *token* livre)
- O funcionamento é do tipo *round robin*, se várias estações transmitirem no mesmo ciclo de acessos

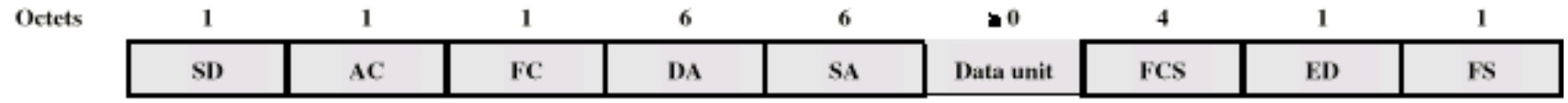
Token Ring IEEE 802.5 (Single Token)



Token Ring IEEE 802.5 – operação



Token Ring IEEE 802.5 – formato das tramas



SD = starting delimiter
AC = access control
FC = frame control
DA = destination address
SA = source address
FCS = frame check sequence
ED = ending delimiter
FS = frame status

(a) General Frame Format

(b) Token Frame Format

PPP = priority bits
T = token bit
M = monitor bit
RRR = reservation bits

(c) Access Control Field

FF = frame-type bits
ZZZZZZ = control bits

(d) Frame Control Field

J, K = non-data bits
I = intermediate frame bit
E = error-detected bit

(e) Ending Delimiter Field

A = Address recognized bit
C = Frame copied bit
rr = reserved

(e) Frame Status Field

Token Ring IEEE 802.5 – campos das tramas

- *Starting Delimiter* (SD) – JK0JK000
  - Início de trama
  - J, K – símbolos não usados para dados
- *Access Control* (AC) – PPPTMRRR
  - PPP e RRR são usados para indicar prioridade e reserva de prioridade
  - M é usado pela estação que desempenha o papel de monitor activo
  - T = 0 indica *token* livre, T = 1 indica *token* ocupado
- *Frame Control* (FC) – FFZZZZZZ
  - F – tipo de trama, Z – controlo
- *Ending Delimiter* (ED) – JK1JK1IE
  - J, K – símbolos não usados para dados
  - I = 1 – trama intermédia, I = 0 – trama final
  - E = 1 – detecção de erro
- *Frame Status* (FS) – ACXXACXX
  - A – endereço reconhecido, C – trama copiada, X – não usado

Token Ring IEEE 802.5 – opções

» Confirmação
  – Os bits A e C são usados para confirmação pelo receptor

» Prioridades
  – Os bits P e R são usados para indicar / reservar níveis de prioridade
  – São suportados 8 níveis de prioridade
  – A estação que reservou o nível mais alto de prioridade é a primeira a obter um *token* livre

» Libertação antecipada do *token* (*early token release*)
  – Se $a > 1$ para uma percentagem elevada de tramas, o protocolo de acesso torna-se muito ineficiente, o que justifica esta variante (usada a 16 Mbit/s)
    » O *token* é libertado imediatamente a seguir ao envio da trama
    » O mecanismo de prioridade é parcialmente destruído

Single Token e Multiple Token – eficiência

» Considere-se um anel com N estações ligadas, com uma latência τ (atraso de propagação e nas estações) e um tempo de transmissão de tramas T_f ($a = \tau / T_f$)

» Assume-se que durante um ciclo de acessos $N_a \leq N$ estações transmitem uma trama cada

» Em *Single Token* com a ≤ 1 ou em *Multiple Token* / *Early Token Release* a duração de um ciclo (tempo de rotação do *token*) é dada por $N_a * T_f + \tau$ e portanto a eficiência é

$$S = \frac{N_a * T_f}{N_a * T_f + \tau} = \frac{T_f}{T_f + \frac{\tau}{N_a}} = \frac{1}{1 + \frac{a}{N_a}}$$

» Em *Single Token* com a ≥ 1, o tempo de rotação do *token* é $N_a * \tau + \tau$, donde

$$S = \frac{N_a * T_f}{N_a * \tau + \tau} = \frac{T_f}{\tau + \frac{\tau}{N_a}} = \frac{1}{a + \frac{a}{N_a}}$$

» Em todos os casos, a eficiência máxima ocorre quando $N_a = N$

Token ring – eficiência e tempo de acesso ao meio

» Em *Single Token* com a ≤ 1 ou em *Multiple Token* / *Early Token Release* o tempo de rotação do *token* é dado por

$$T_{rot} = N_a * T_f + \tau$$

» A eficiência pode ser escrita como

$$S = \frac{N_a * T_f}{N_a * T_f + \tau} = \frac{T_{rot} - \tau}{T_{rot}} = 1 - \frac{\tau}{T_{rot}}$$

e portanto

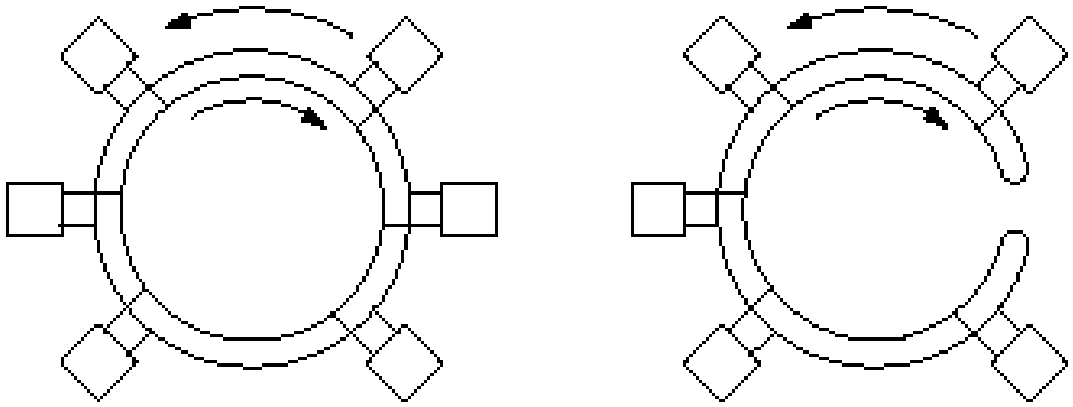
$$T_{rot} = \frac{\tau}{1 - S}$$ (na ausência de tráfego, S = 0 e $T_{rot} = \tau$)

» Pode então concluir-se que o eventual aumento da eficiência é acompanhado de um aumento do tempo de rotação do *token*, e portanto do tempo de acesso de uma estação ao meio (T_{rot} cresce sem limite quando S tende para 1)

» Caso seja necessário limitar o tempo de acesso ao meio (considerando a situação mais desfavorável), isso só se consegue à custa da redução da eficiência

FDDI – Fiber Distributed Data Interface

- *Token Ring* a 100 Mbit/s (ANSI X3T9.5)
- Topologia base – anel duplo
  - Dois anéis unidireccionais (Primário e Secundário), em sentidos opostos
  - Número máximo de estações: 500
  - Número máximo de nós (pontos de acesso): 1000
  - Perímetro máximo (anel Primário): 100 km
  - Distância máxima entre estações: 2 km



FDDI – Fiber Distributed Data Interface

» Todas as estações devem ligar-se ao anel Primário
  – O anel Secundário está normalmente em *standby* (sem tráfego), sendo usado quando for necessário reconfigurar a rede

» Definem-se dois tipos de estações
  – Classe A – ligam-se aos dois anéis
  – Classe B – ligam-se apenas ao anel Primário, ficando isoladas no caso de interrupção deste

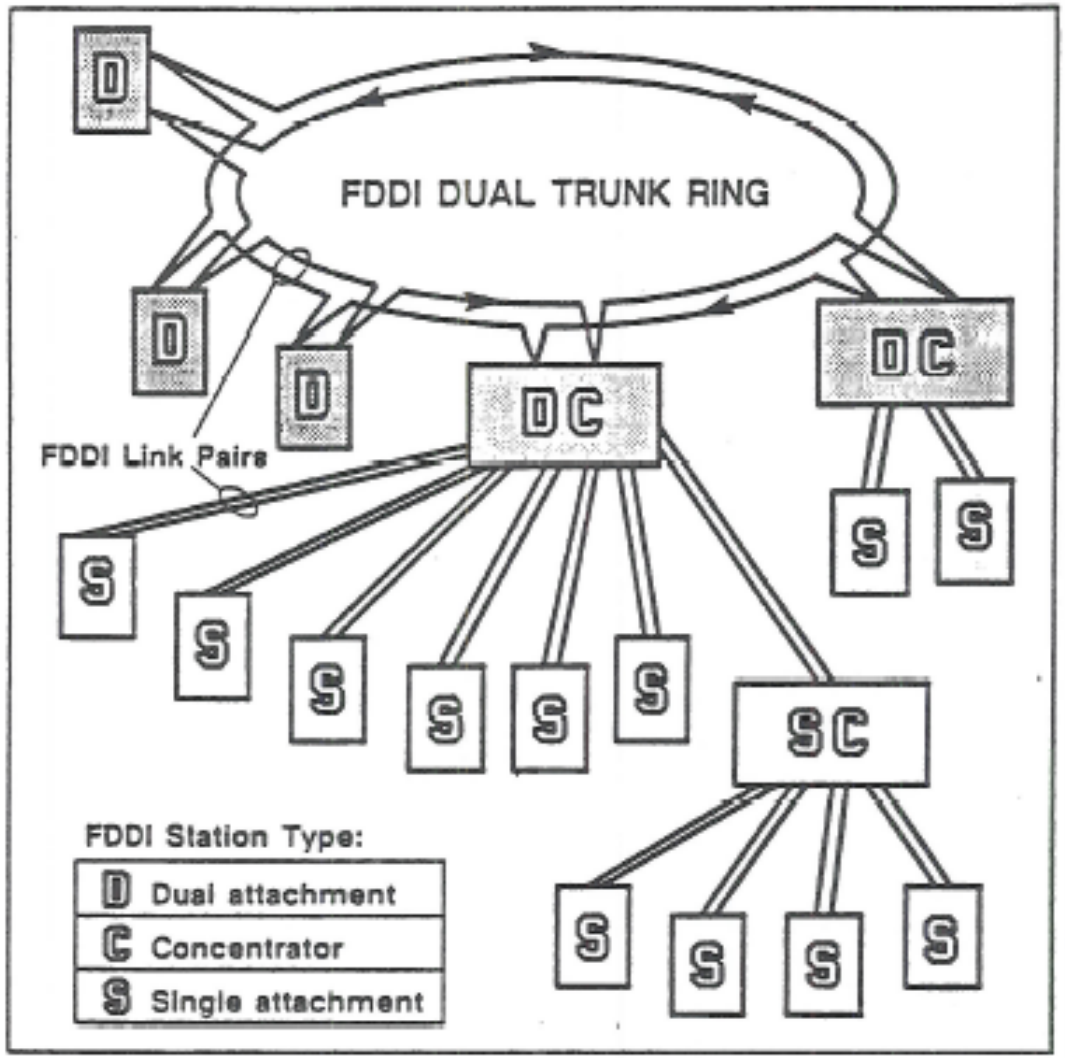
» Tendo em atenção a velocidade de operação e o perímetro máximo possível da rede, normalmente $a > 1$, pelo que em FDDI se usa um protocolo do tipo *Multiple Token*, isto é, o *token* é imediatamente libertado após a transmissão da última trama por parte da estação que o capturou

» Para facilitar o processamento e reduzir a latência de cada estação, o *token* é removido e em seu lugar enviado *idle*, após a sua captura e antes do início efectivo da transmissão de tramas

FDDI – topologia e reconfiguração

- Tal como no *Token Ring* IEEE 802.5, é possível usar *Wiring Concentrators* que facilitam a reconfiguração em caso de interrupção do anel Primário ou de ambos os anéis
- Os concentradores podem ser estações de Classe A (*Dual attachment*) ou de Classe B (*Single attachment*)
- Recorrendo a concentradores, uma rede FDDI pode desenvolver-se numa topologia hierárquica com múltiplos níveis (*Dual Ring of Trees*)
- A rede pode também constituir-se inicialmente com um único concentrador, fechado sobre si próprio, a ligar as estações (*collapsed backbone*)
- Reconfiguração
  - Se houver interrupção apenas do anel Primário, as estações passam a transmitir no anel Secundário
  - Se ocorrer uma interrupção dos dois anéis (no mesmo troço), as estações adjacentes à falha ligam o anel Primário ao Secundário (o perímetro da rede praticamente duplica)
  - Se ocorrerem múltiplas interrupções dos dois anéis, a reconfiguração tem como consequência a formação de várias redes isoladas

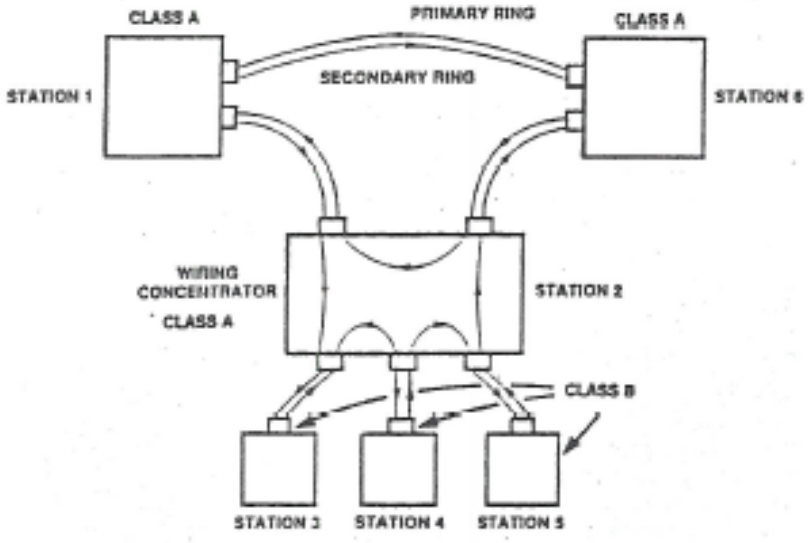
FDDI – topologia (exemplo)

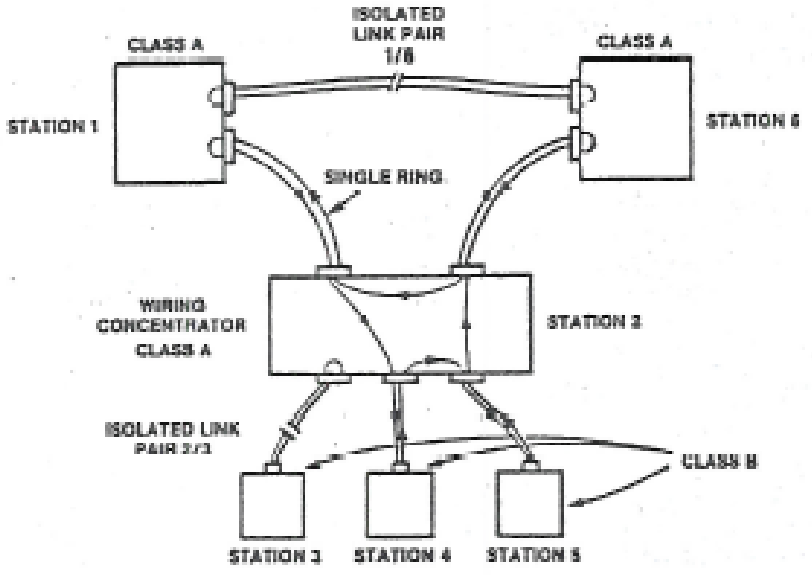


FDDI – reconfiguração

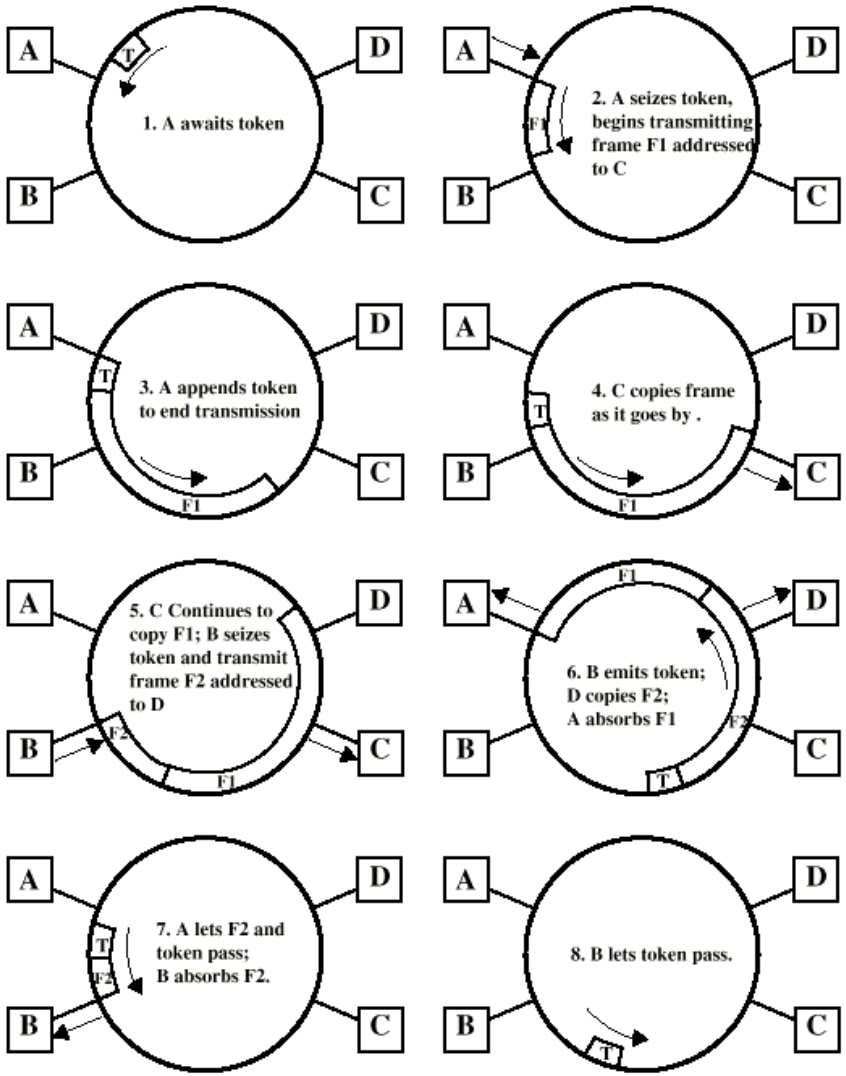
» No caso de interrupção dos dois anéis no mesmo troço, o que afecta a ligação entre duas estações de classe A, as estações adjacentes à falha ligam o anel Primário ao Secundário, reconfigurando a rede sem isolar qualquer estação

» No caso de interrupção de um troço em que exista apenas o anel Primário, o que afecta a ligação de uma estação de classe B a um *Wiring Concentrator*, este reconfigura a rede como no caso básico de um anel simples, isolando a estação em causa

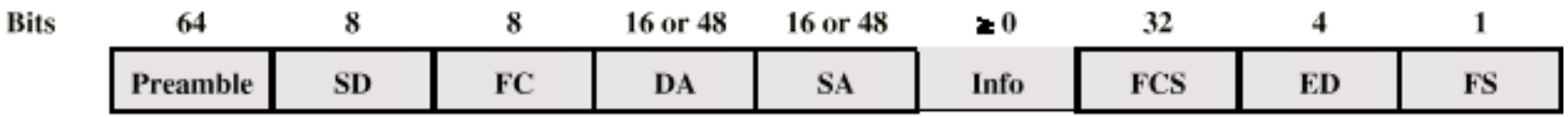




FDDI – exemplo de operação



FDDI – formato das tramas



(a) General Frame Format

(b) Token Frame Format

SD = starting delimiter
FC = frame control
DA = destination address
SA = source address
FCS = frame check sequence
ED = ending delimiter
FS = frame status

FDDI – campos das tramas

- *Preamble* – usado para sincronização
- *Starting Delimiter* (SD) – JK
  - Símbolos de 4 bits não usados para dados (início de trama)
- *Frame Control* (FC) – CLFFZZZZ (bits)
  - C – trama síncrona ou assíncrona
  - L – endereços de 16 ou 48 bits
  - FF – trama de dados LLC, controlo MAC ou reservada
  - *Token* – FC = 10000000 ou FC = 11000000
- *Ending Delimiter* (ED) – T
  - Símbolo (4 bits) não usado para dados (fim de trama)
- *Frame Status* (FS) – EAF
  - Dois símbolos: (1) SET/TRUE; (2) RESET/FALSE
  - E – erro detectado
  - A – endereço reconhecido
  - F – trama copiada

FDDI – tipos de tráfego

» A capacidade disponível é usada para suportar dois tipos de tráfego

  – Síncrono – débito médio e tempo de resposta garantidos; adequado para aplicações em que esses valores são previsíveis com antecedência, permitindo a sua negociação

  – Assíncrono – débito médio e tempo de resposta não garantidos (aplicações de dados em que o tempo de resposta não é crítico); a capacidade disponível (não usada pelo tráfego síncrono) é partilhada de forma dinâmica por tráfego assíncrono

» Durante a inicialização do anel as estações negoceiam um valor do *Target Token Rotation Time* (TTRT) e o menor valor proposto passa a ser o TTRT Operacional (T_Opr) do anel; cada estação mantém dois *timers*

  – TRT – *Token Rotation Timer* (inicializado com o valor T_Opr)
  – THT – *Token Holding Timer* (só para acesso assíncrono)

» Cada estação pode reservar uma fracção da capacidade *R* da rede ($f_i = R_i / R$) para tráfego síncrono, o que lhe confere um tempo máximo de transmissão por cada captura do *token* – $SA_i = f_i$. T_Opr ($\Sigma SA_i < T\_Opr$, pois $\Sigma f_i < 1$)

FDDI – protocolo de acesso

» Quando o *token* chega a uma estação com antecedência (TRT não expirou) é possível transmitir tráfego síncrono e assíncrono; THT é inicializado com o valor TRT corrente e TRT é reinicializado (TRT = T_Opr)

  – Tráfego síncrono: a estação pode transmitir durante SA_i, isto é, de acordo com a fracção da capacidade que lhe foi atribuída (THT inibido)

  – Tráfego assíncrono: a estação transmite até expirar THT, podendo, no entanto, concluir uma transmissão entretanto iniciada

» Quando o *token* chega atrasado, a estação apenas pode transmitir tráfego síncrono (como no caso anterior), mas TRT não é reinicializado

» O protocolo garante

  – Valor médio do tempo de rotação do *token* < T_Opr

  – Valor máximo do tempo de rotação do *token* < 2 **.** T_Opr

Slotted Ring (Empty Slot)

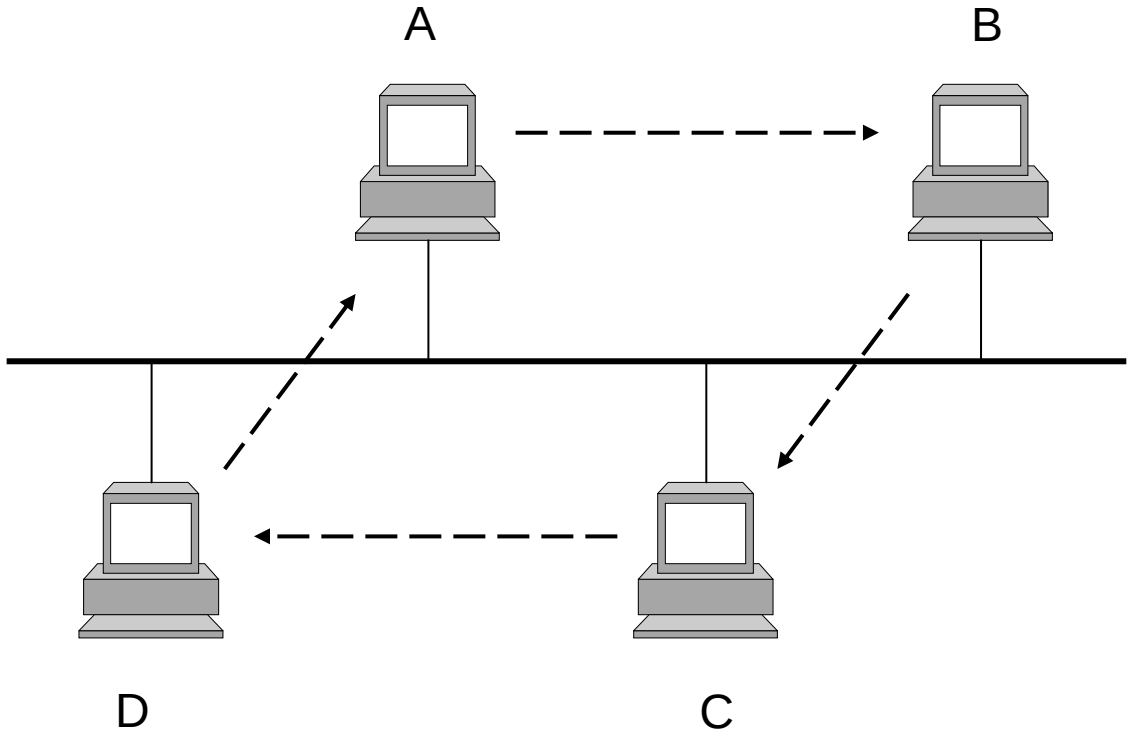
- O anel é dividido num número inteiro de *slots*, de comprimento fixo, que circulam continuamente no anel (o número de slots é igual a *a*)
- Cada *slot* pode ser ocupado por um pacote (ou fragmento)
- O estado de cada *slot* (vazio / ocupado) é indicado por um bit no cabeçalho; os *slots* são inicialmente criados vazios
- Uma estação pronta para transmitir espera a passagem de um *slot* vazio, altera o seu estado para ocupado e insere um pacote no respectivo *slot*
- A libertação do *slot* (alteração do estado para vazio) pode ser feita pela estação de destino (*ORWELL Ring*) ou pela estação de origem (*Cambridge Ring*)
  - A libertação pela estação de origem tem a vantagem de permitir acesso *round robin* a um *slot*
  - A libertação pela estação de destino permite uma melhor utilização do anel, mas requer medidas adicionais para evitar acessos desequilibrados por parte das estações
- Uma vez que os *slots* são independentes, é possível haver acessos simultâneos de várias estações se existirem vários *slots* a circular na rede
- O protocolo de acesso é eficiente, mas essa vantagem perde-se em anéis com baixa latência (*Cambridge Ring*), em que o tamanho dos *slots* é de tal forma pequeno que o *overhead* do cabeçalho (controlo, endereços) é muito elevado

Token Bus – princípio de operação

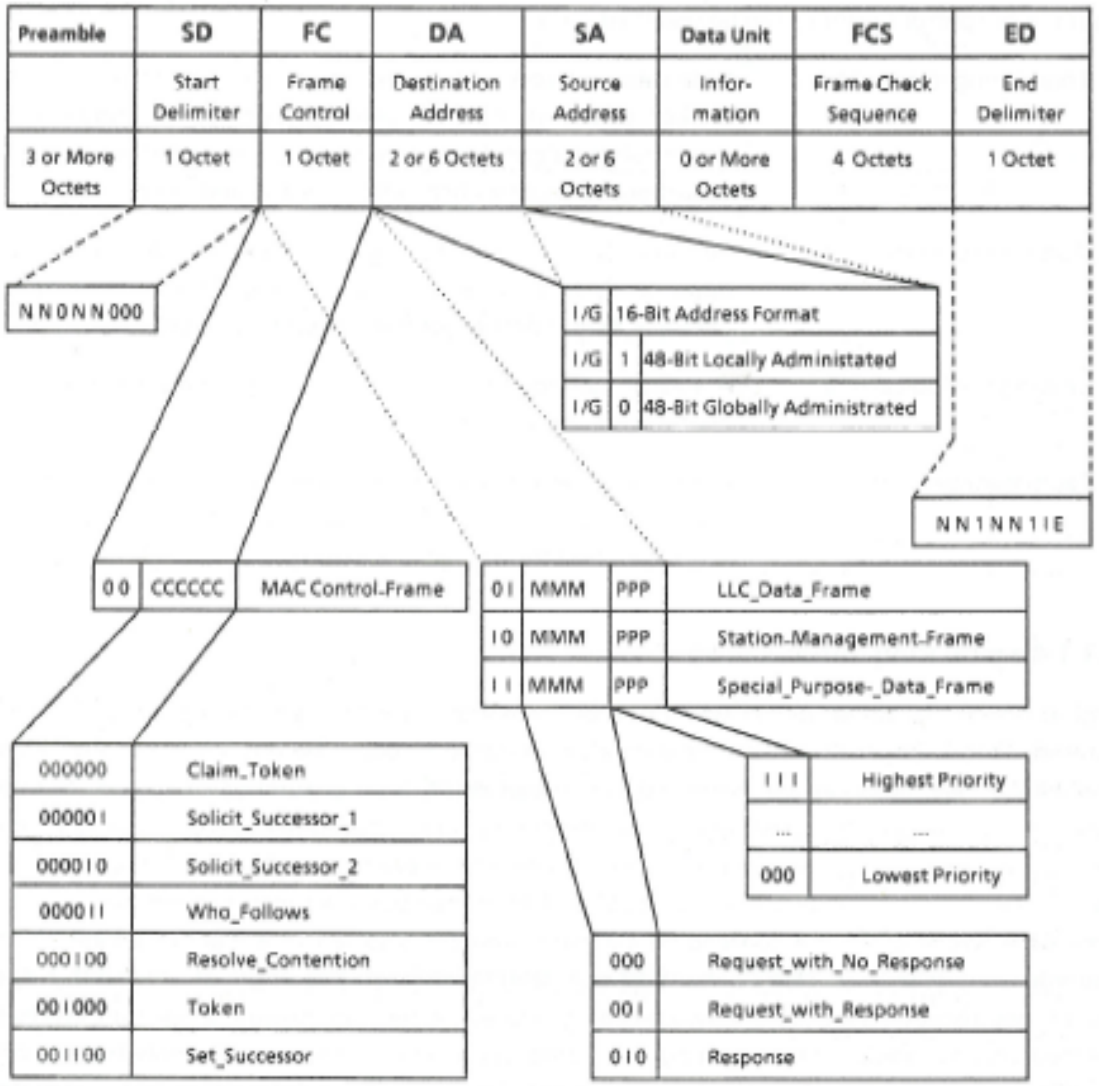
- É possível usar um protocolo do tipo *Control Token* numa rede com topologia em barramento (*Token Bus*), por constituição de um anel lógico
  - É atribuído a cada estação um identificador lógico
  - Cada estação tem um antecessor lógico (do qual recebe o *token*) e um sucessor lógico (ao qual envia o *token*)
- O *token* tem de ser explicitamente passado entre estações, isto é, tem de ser endereçado (endereço MAC do sucessor lógico da estação de posse do *token*)
- Quando de posse do *token*, uma estação deve emitir imediatamente um *token* se não tiver tráfego ou, caso contrário, após concluir a transmissão
- A gestão de uma rede *Token Bus* é complexa
  - Inicialização do anel lógico
  - Adição e remoção de estações do anel lógico
  - Recuperação de erros (interrupção do anel lógico, conflitos na aquisição do *token*, perda do *token*, múltiplos *tokens*, etc.)
- O IEEE especificou uma rede *Token Bus* (IEEE 802.4), tendo em atenção os requisitos de aplicações industriais

Token Bus – anel lógico

- Anel lógico: A ➔ B ➔ C ➔ D ➔ A, independente da localização física
- A estação de posse do *token* endereça-o explicitamente ao seu sucessor lógico, mesmo que este não tenha tramas para transmitir
- O protoclo pode funcionar num barramento bidireccional ou unidireccional (*folded bus*) ou numa topologia em estrela, em que o elemento central realiza a difusão de tramas



Token Bus IEEE 802.4 – formato das tramas

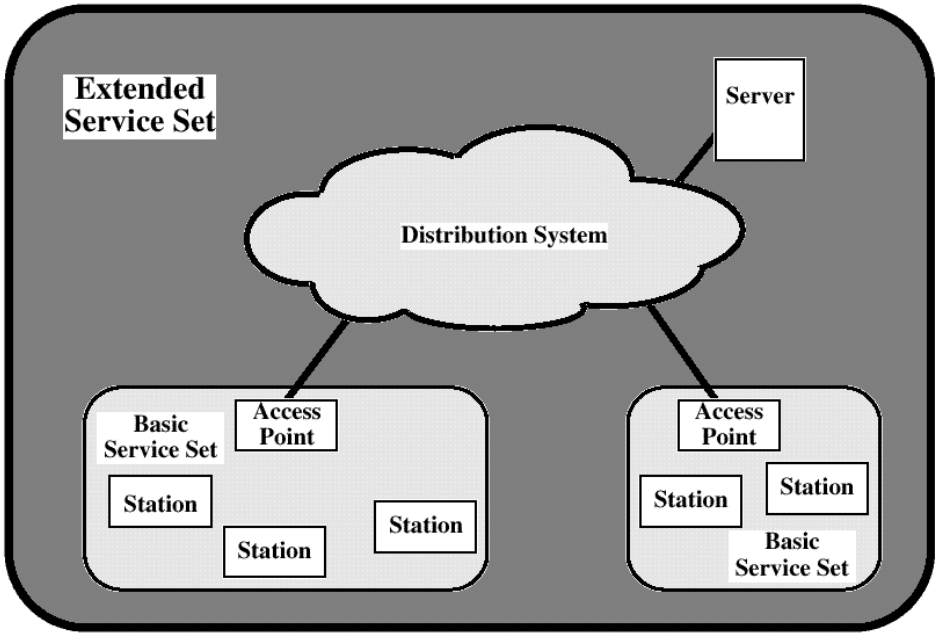


LANs sem fios IEEE 802.11

» IEEE 802.11

» BSS – *Basic Service Set* (célula)
  – Conjunto de estações que usam o mesmo protocolo MAC
  – As estações competem pelo meio de transmissão
  – Interligação
    » Célula isolada
    » Ligação através de *Access Point* (*bridging*)

» ESS – *Extended Service Set*
  – Ligação de 2 ou mais BSS
  – LLC vê uma única LAN lógica



Tipos de mobilidade

» Sem transição
  – Estação estacionária
  – Estação move-se dentro de um BSS

» Transição entre BSS
  – Estação move-se dentro do mesmo ESS

» Transição entre ESS
  – Estação move-se entre BSS em ESS diferentes
  – Interrupção de serviço

Controlo de acesso ao meio – funções

» DWFMAC – *Distributed wireless foundation MAC* (IEEE 802.11*)*

» DCF – *Distributed Coordination Function*

– CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*)

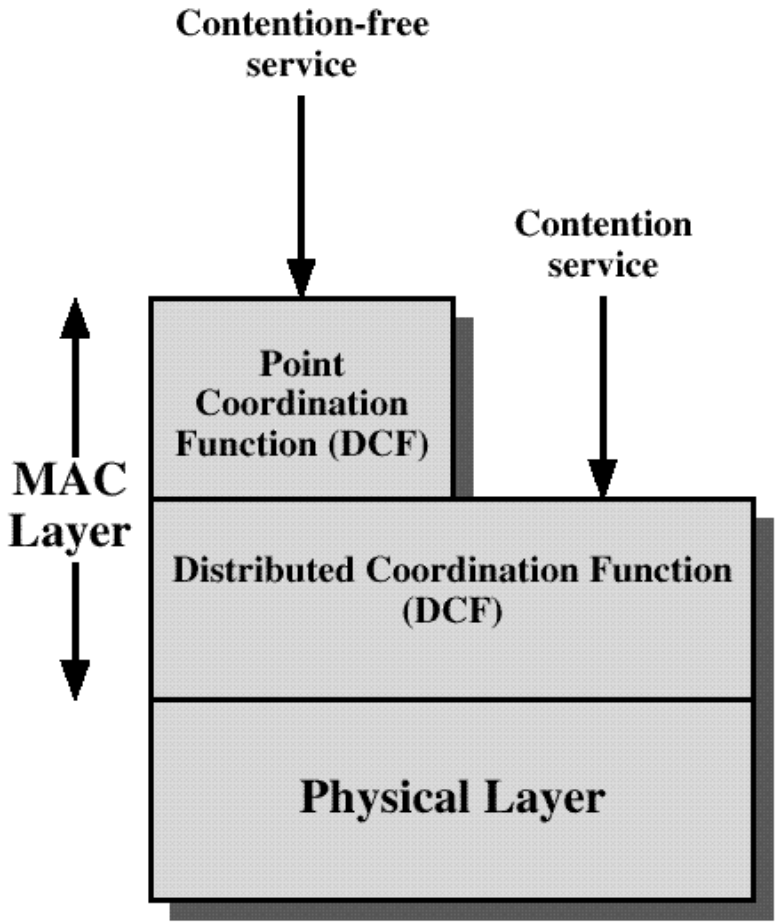
– Sem detecção de colisões (não viável)

» PCF – *Point Coordination Function*

– *Polling* centralizado

– Acesso sem contenção

– Usa serviços DCF



CSMA with Collision Avoidance (CSMA/CA)

- Em LANs sem fios (WLANs) não é possível usar o protocolo CSMA/CD
  - É difícil detectar colisões numa interface rádio, devido a diferenças significativas de potência dos sinais transmitidos e recebidos, perdendo-se assim as vantagens de abortar uma transmissão (possível quando a detecção de colisões é viável)
  - A monitorização do meio durante a transmissão aumentaria a complexidade (e portanto o custo) do sistema
- É necessário usar ACKs para lidar com colisões (como em CSMA), devendo retransmitir-se tramas não confirmadas
  - As retransmissões degradam seriamente o desempenho e portanto mecanismos que reduzam a probabilidade de colisões são essenciais em WLANs
- Estas razões levaram à adopção em WLANs de um protocolo de acesso do tipo *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA)
- Em IEEE 802.11, CSMA/CA é usado pela *Distributed Coordination Function* (DCF), que suporta transferência assíncrona de dados num modo *best-effort* como método básico de acesso, enquanto uma *Point Coordination Function* (PCF) opcional providencia acesso sem conflitos, por meio de *polling*

DCF – CSMA/CA

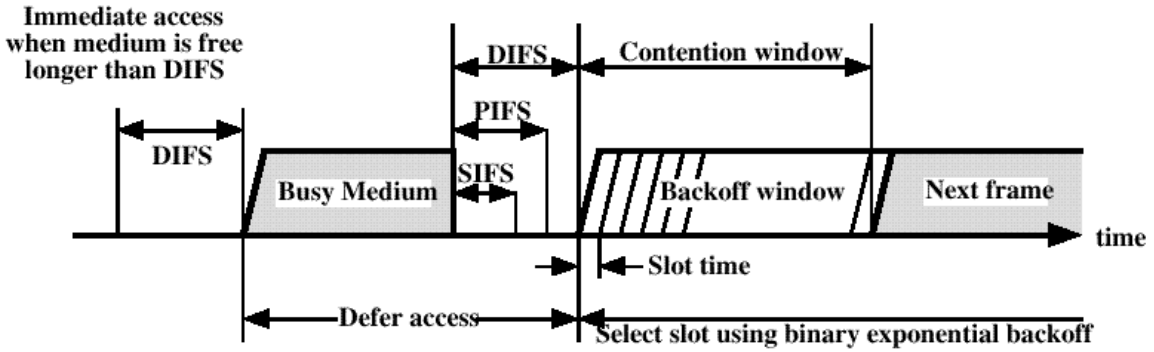
- O protocolo CSMA/CA, usado pela *Distributed Coordination Function* nas redes IEEE 802.11, baseia-se na escuta do meio antes da transmsissão e num mecanismo de deferência do tipo *binary exponential back-off*
- No caso de o meio estar livre, a estação espera durante um intervalo de tempo *Interframe Space* (IFS) e inicia a transmissão se o meio continuar livre
- Se o meio estiver ocupado (ou tiver ficado ocupado durante o intervalo IFS)
  - A estação espera até que o meio fique livre
  - De seguida espera durante IFS e activa um *contention timer* igual ao produto do valor de um *slot* temporal de referência (*aSlotTime*) por uma janela de contenção escolhida aleatoriamente na gama [1, CW], em que $CW = 2^k - 1$ (é definido um valor mínimo de *k* para a primeira tentativa de transmissão de uma trama)
  - Se uma outra transmissão se iniciar antes do *contention timer* expirar, este é inibido até ao fim dessa transmissão e de seguida reactivado
  - Quando o temporizador (*contention timer*) expirar, a estação envia a trama e espera uma confirmação (ACK)
  - Se não for recebida qualquer confirmação, assume-se que a trama se perdeu e é feita uma nova tentativa, após se aumentar *k* de uma unidade (até se atingir um

CSMA/CA – Interframe Space (IFS) e back-off

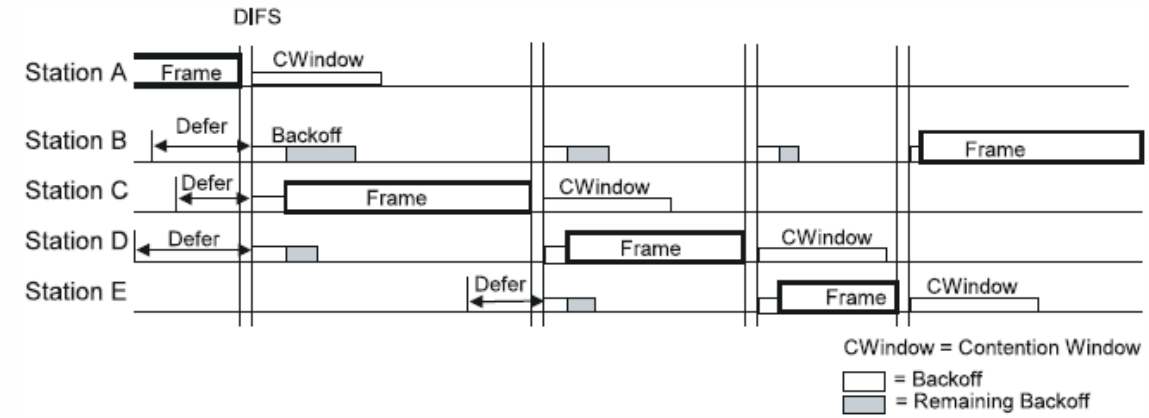
» SIFS (*Short IFS*) – usado por tramas de alta prioridade (e.g., ACK, respostas a *polling*)

» PIFS (*PCF IFS*) – usado pelo *master* para fazer *polling*

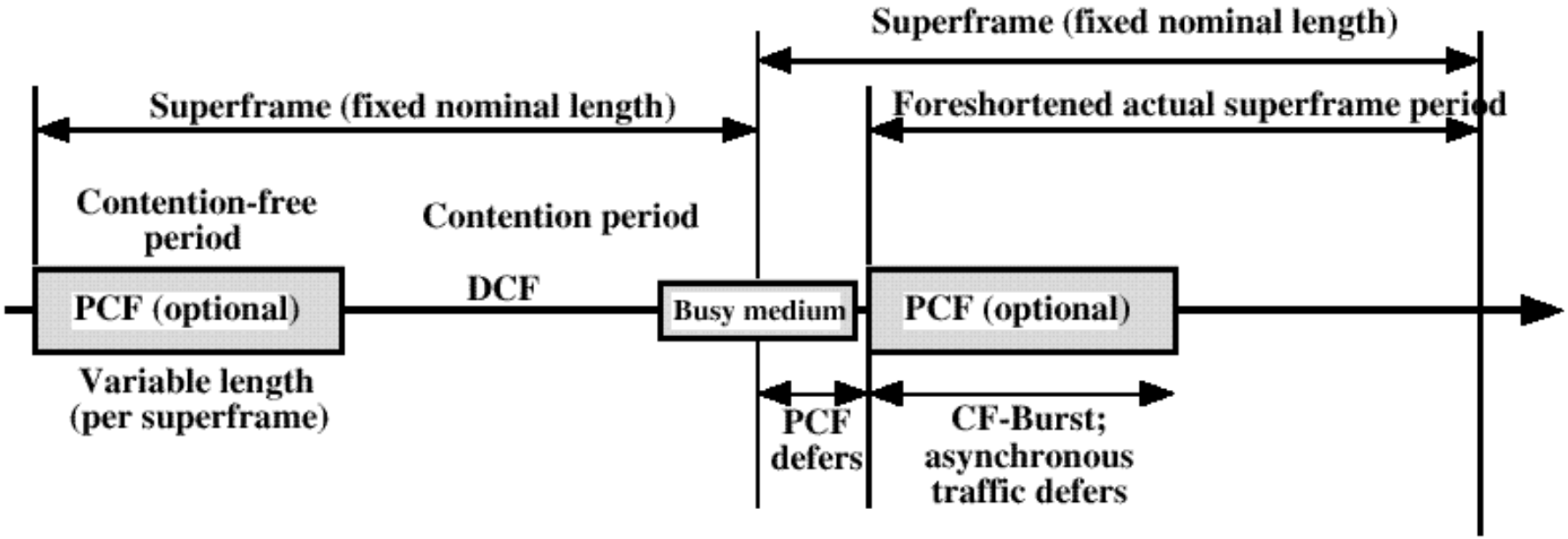
» DIFS (*DCF IFS*) – usado em acessos assíncronos (contenção)



» *Back-off*



PCF – polling


Superframe (fixed nominal length)
Superframe (fixed nominal length)
Foreshortened actual superframe period
Contention-free period
Contention period
PCF (optional)
DCF
Busy medium
PCF (optional)
Variable length (per superframe)
PCF defers
CF-Burst; asynchronous traffic defers

Segmentação física e lógica de LANs

Bridges e bridged LANs

Segmentação física de LANs

» A segmentação de LANs será analisada no contexto das redes IEEE 802.3 e apenas pontualmente será feita referência a soluções adoptadas noutras LANs
  – A referência a dispositivos usados para o efeito e técnicas associadas (*bridging*) usará assim a terminologia adoptada nas redes IEEE 802.3

» Nas LANs IEEE802.3 / Ethernet de primeira geração as estações ligavam-se a um segmento de cabo coaxial (10Base5 e 10Base2)
  – Para aumentar a cobertura geográfica da rede e o número de estações ligadas, os segmentos eram ligados por repetidores, garantindo continuidade a nível físico
» Com a introdução de cablagens estruturadas, as estações passaram a ligar-se a um repetidor multiporta (*hub*) por meio de pares entrançados (*twisted pairs*), podendo vários *hubs* ligar-se a um *hub* num nível hierárquico superior (10Base-T e 100Base-T)
  – Esta solução é logicamente equivalente à primeira (*bus* lógico)
» Nos dois casos podem ocorrer colisões; as estações funcionam no modo *half-duplex* e as colisões são detectadas e resolvidas pelo protocolo CSMA/CD
  – Segmentos ligados por repetidores constituem um domínio de colisão (formando uma LAN, na acepção básica do termo)

Segmentação lógica de LANs com bridges

» Com o aumento do número de estações e do volume de tráfego gerado por cada estação, tornou-se necessário reduzir a dimensão dos domínios de colisão, por meio de filtragem inteligente de tráfego entre segmentos físicos (segmentação lógica)
  – Para o efeito desenvolveu-se um novo tipo de equipamento (*bridge*) que, na versão inicial, interligava segmentos de cabo coaxial, ocupando o lugar de repetidores

» As *bridges* operam na camada MAC (são transparentes a protocolos de nível superior) e filtram ou retransmitem tramas (*forwarding*) com base em endereços MAC, isto é, realizam segmentação lógica da rede na camada MAC
  – Uma *bridge* isola domínios de colisão mas segmentos ligados por *bridges* (*bridged LAN*) formam um único domínio lógico de difusão (na camada MAC) – uma *bridge* não constitui uma barreira à difusão de tramas (não confundir com a difusão ao nível físico)

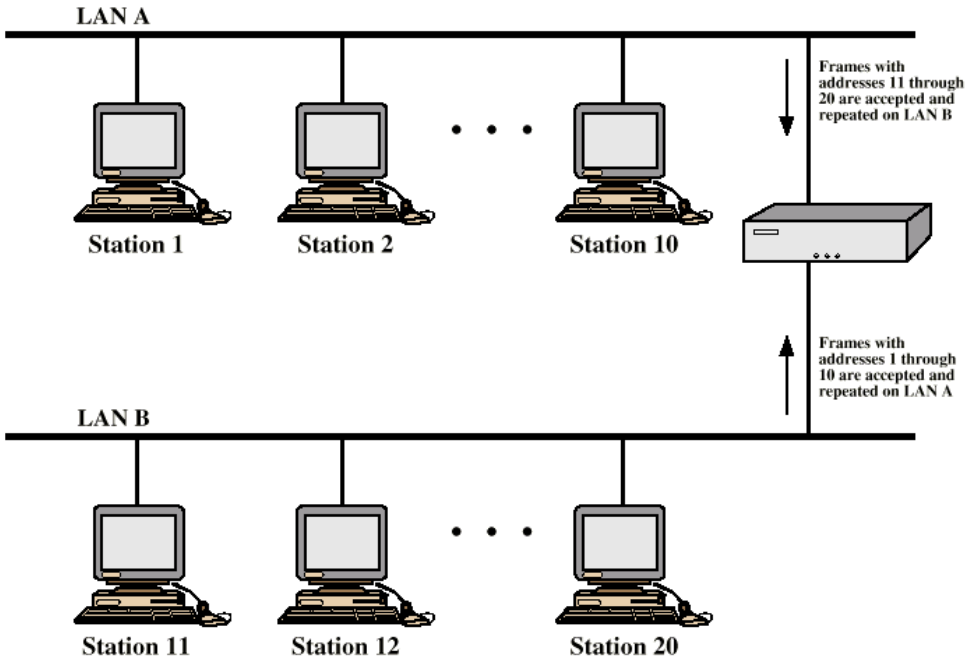
» Nas redes baseadas em cablagens estruturadas, o papel das *bridges* é actualmente desempenhado por comutadores (*LAN switches*), funcionalmente equivalentes às *bridges*, mas mais flexíveis no que se refere à segmentação lógica da rede – os comutadores podem substituir os *hubs*, parcialmente ou na totalidade
  – A designação *bridge* refere-se, por vezes, ao equipamento convencional usado para interligar segmentos de cabo coaxial, mas as funções e mecanismos que suporta (*bridging*) aplicam-se também aos comutadores – nesta acepção, e com a tecnologia actual, uma *bridged LAN* é realizada com comutadores (e a designação *bridge*, em sentido lato, inclui os comutadores)

Bridges – filtragem de tráfego (exemplo simples)

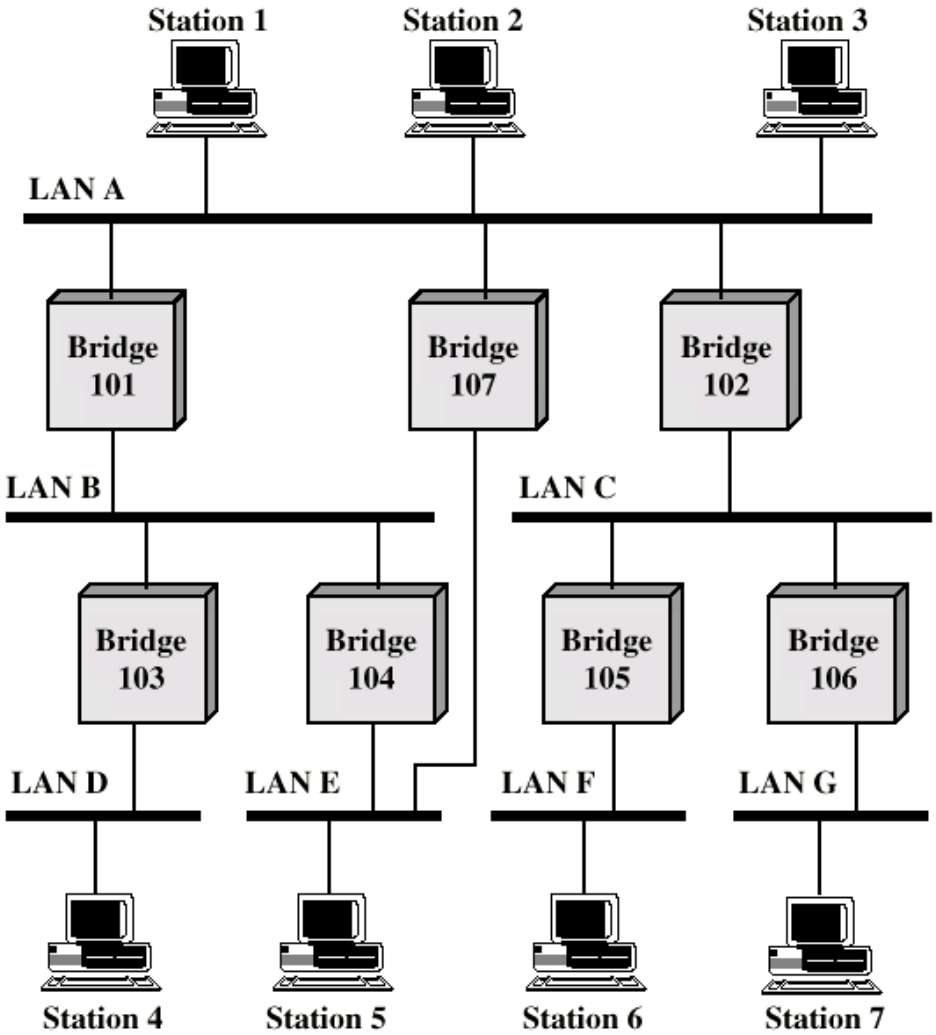
» Ao contrário de um repetidor, a *bridge* não retransmite na LAN B todo o tráfego originado na LAN A, mas apenas as tramas endereçadas a estações na LAN B, assumindo que conhece a respectiva localização – tramas destinadas a estações na LAN A são filtradas e portanto não são retransmitidas pela *bridge* (analogamente, no que se refere a tráfego originado na LAN B)

  – Tramas com endereço de destino *broadcast* ou *multicast* são retransmitidas na outra LAN

» Este processo é particularmente eficiente se uma percentagem significativa de tráfego for local a um segmento



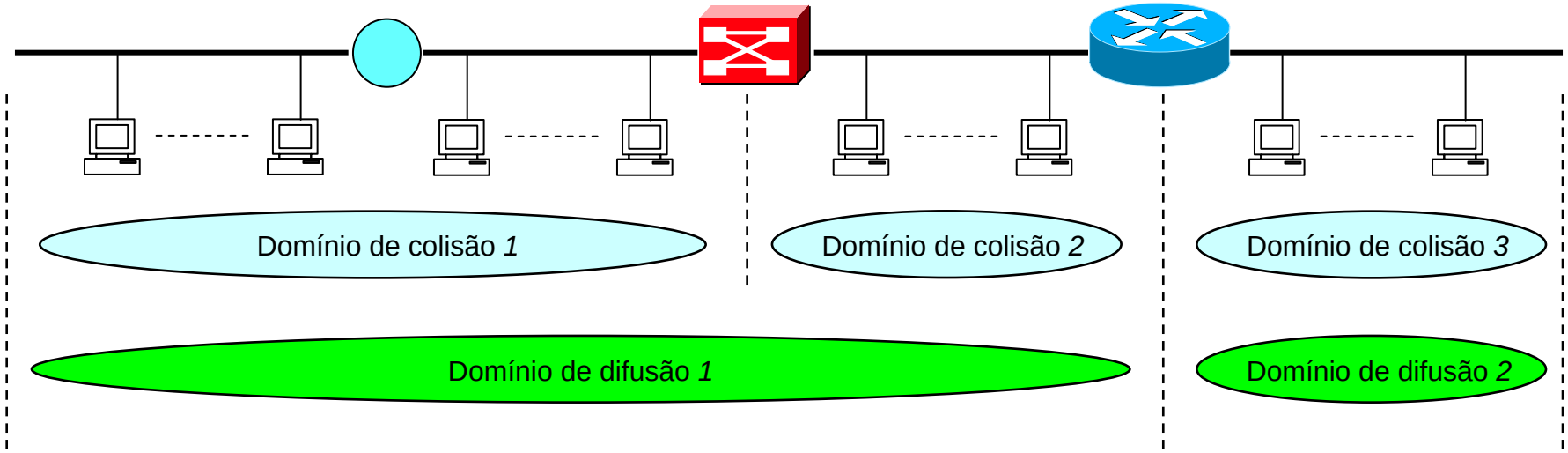
Bridged LAN – exemplo

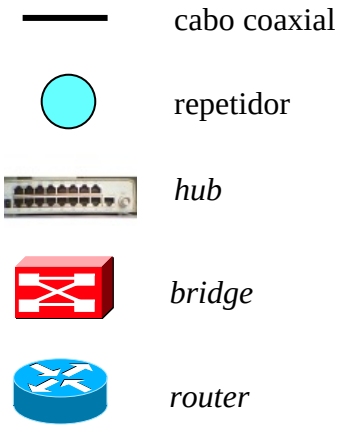


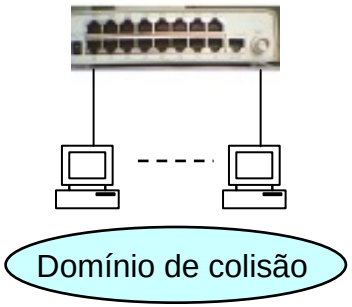
Segmentação lógica de LANs com routers

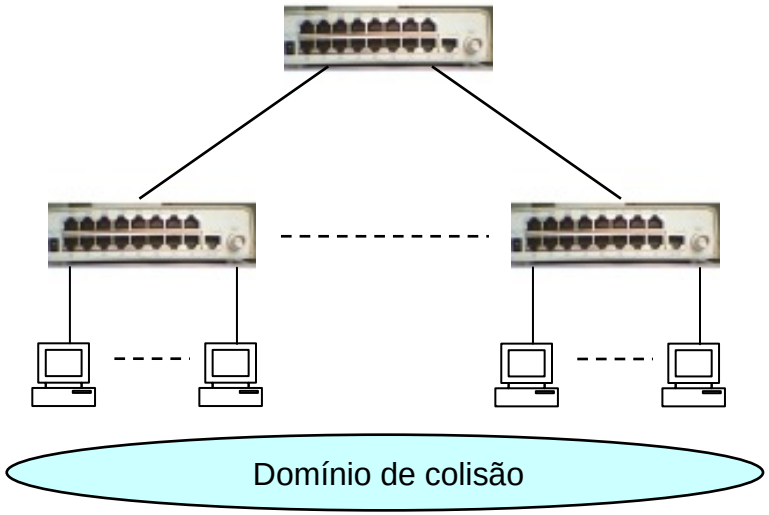
- Domínios de difusão são isolados por meio de *routers*, que providenciam segmentação lógica na camada de Rede (tipicamente IP)
  - A segmentação lógica na camada de Rede pode ser necessária por razões de desempenho, segurança, fiabilidade, ou outras
- A segmentação lógica com *bridges* convencionais e *routers* está condicionada pela localização física das estações (segmentos físicos a que se ligam)
- Com a introdução de comutadores é possível realizar segmentação lógica da rede independentemente da localização física das estações, o que permite suportar o conceito de LAN Virtual (VLAN – *Virtual LAN*) – domínio lógico de difusão transparente à localização física das estações
  - Tipicamente, estações na mesma subrede IP pertencem à mesma VLAN
  - Neste contexto desenvolveu-se uma nova família de equipamentos (designados por vezes *router switches*) – comutam tramas dentro da mesma VLAN e realizam as funções básicas dos *routers*, isto é, encaminham tráfego entre estações em subredes IP / VLANs diferentes, pelo que devem pertencer às VLANs associadas às redes IP que interligam (basta uma única interface física a um comutador, como será discutido, mas é necessário criar múltiplas interfaces virtuais, uma por VLAN)

Domínios de colisão e difusão – exemplos

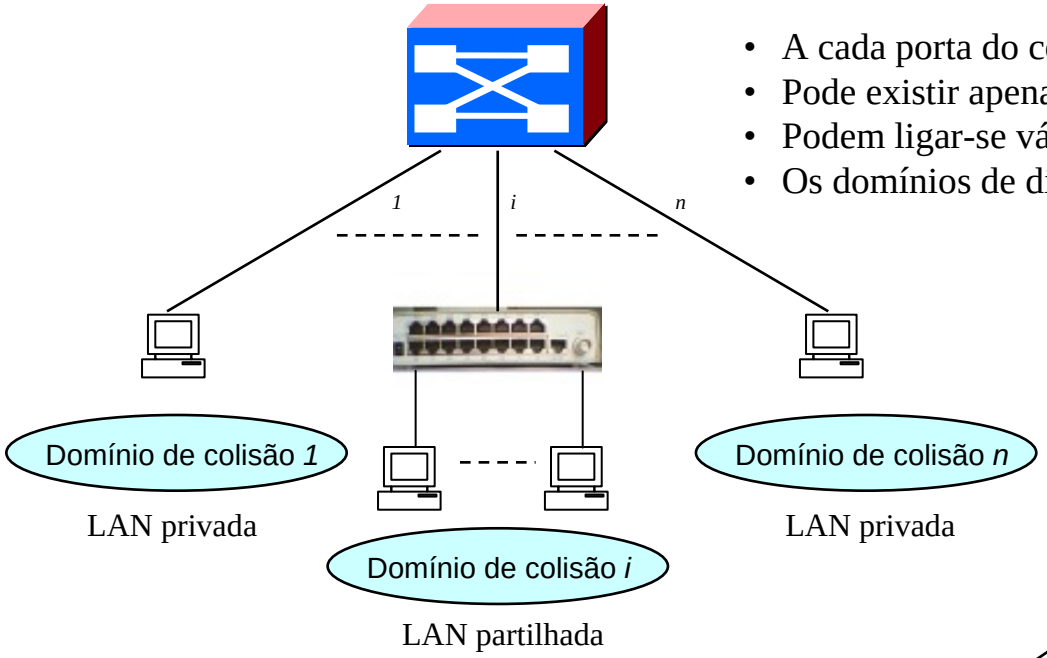




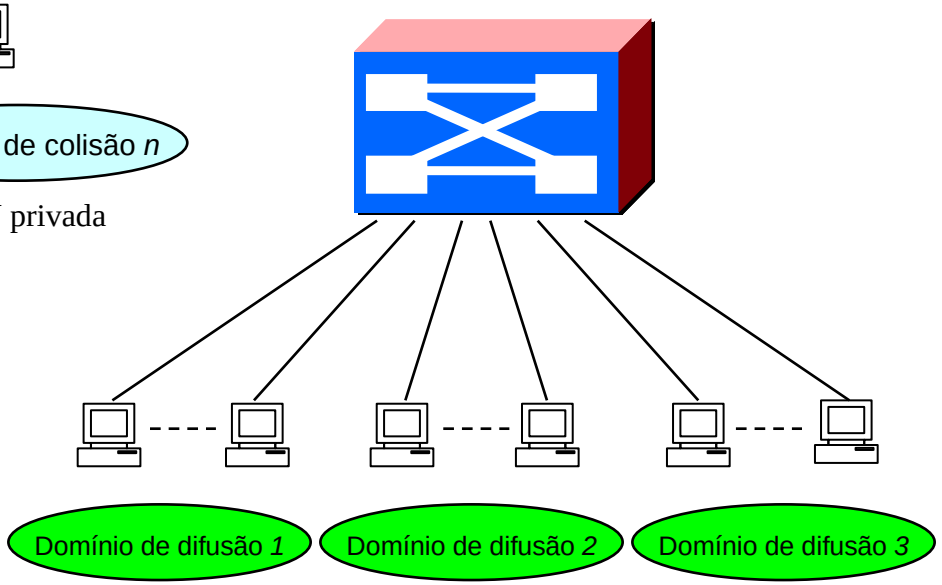




Domínios de colisão e difusão com comutadores



- A cada porta do comutador corresponde um domínio de colisão
- Pode existir apenas um terminal ligado a uma porta (LAN privada)
- Podem ligar-se vários terminais a uma porta através de um *hub*
- Os domínios de difusão são definidos por configuração das portas



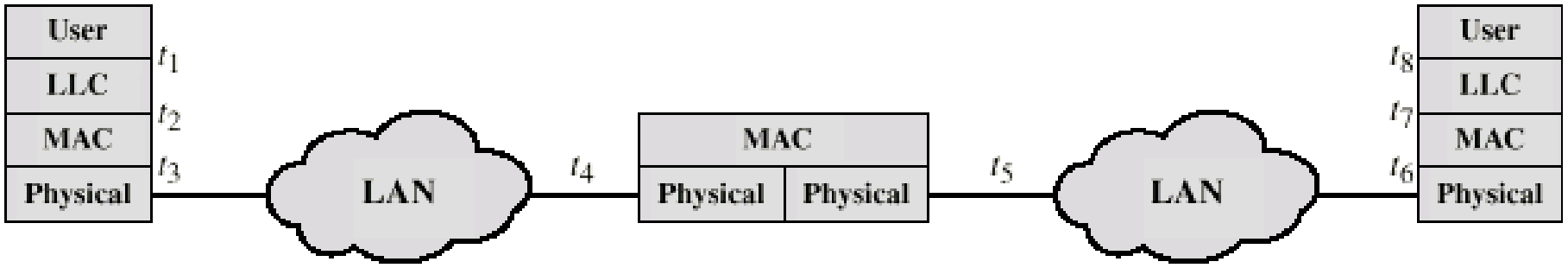
(domínios lógicos de difusão criados por configuração)

hub

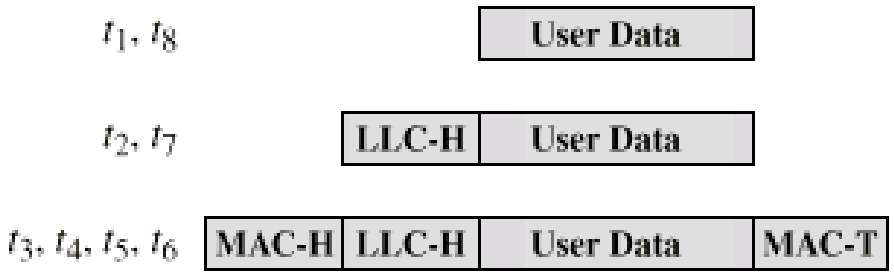
comutador

- Um domínio lógico de difusão constitui uma LAN Virtual (VLAN)
- Uma VLAN pode ser estendida através de vários comutadores
- A comunicação entre VLANs é assegurada por um ou mais *routers*

Bridges IEEE 802 – arquitectura protocolar



(a) Architecture



(b) Operation

LLC-H *LLC Header*
MAC-H *MAC Header*
MAC-T *MAC Trailer*

Bridges IEEE 802 – alternativas

- No casos mais simples uma *bridge* liga segmentos de LANs da mesma tecnologia (mesmo nível físico e MAC)
  - Uma *bridge* deve, de algum modo, reconhecer tramas destinadas a uma ou mais LANs diferentes da LAN de origem e despachá-las, isto é, uma *bridge* tem que decidir se deve retransmitir uma trama (*forwarding*) e, em caso afirmativo, para que segmento(s)
  - Foram definidos dois mecanismos de *bridging* em LANs IEEE 802 – *transparent bridging* em redes Ethernet / IEEE 802.3 (embora a solução normalizada pelo IEEE 802, descrita adiante, tenha carácter genérico) e *source routing* em redes *Token Ring* IEEE 802.5
- Foi ainda considerada a possibilidade de interligar, por meio de *bridges*, LANs de diferentes tecnologias, o que em particular requer a conversão de formatos MAC
  - Para além da dificuldade, nalguns casos, de mapear parâmetros entre tecnologias diferentes (por exemplo, prioridades), esta possibilidade tem actualmente interesse reduzido uma vez que a tecnologia Ethernet / IEEE 802.3 se tornou dominante em LANs
- Foi definida igualmente uma solução para ligar LANs geograficamente afastadas, por meio de *remote bridges*
- Em LANs de grande dimensão é normal providenciar rotas alternativas entre estações (topologia em malha), nomeadamente para garantir redundância em caso de falhas
  - As *bridges* do tipo *source routing* contemplam o envio de tramas por rotas alternativas, mas no mecanimso de *bridging* transparente é necessário criar uma topologia lógica aberta

Source routing e bridges transparentes

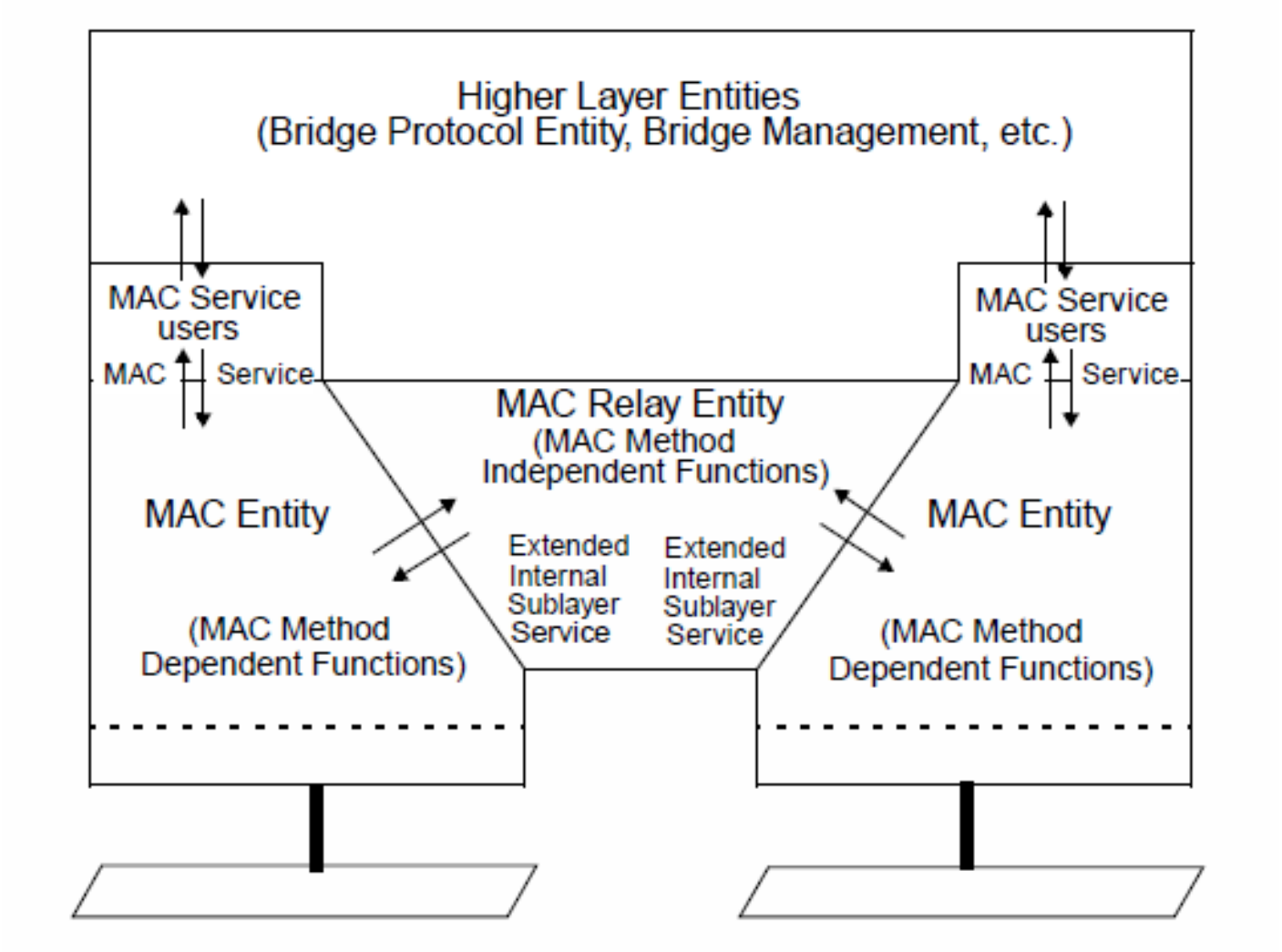
» *Source Routing*
  – As tramas incluem a rota completa desde a estação de origem até à estação de destino, designando as *bridges* no percurso, que se limitam a encaminhar as tramas conforme prescrito
  – Este mecanismo não é transparente para as estações que, por isso, têm de participar activamente no processo de determinação de rotas
  – Este método é usado nas redes *Token Ring* IEEE 802.5

» *Bridges* transparentes (*spanning tree*)
  – No mecanismo de *bridging* transparente, as *bridges* são invisíveis para as estações
  – Ainda que a topologia física seja fechada (rotas alternativas), a topologia lógica tem de ser aberta e cobrir todos os segmentos (*spanning tree*) – as *bridges* cooperam na construção, manutenação e, se necessário, na reconfiguração da topologia lógica (árvore) com base num protocolo que executam entre si (STP – *Spanning Tree Protocol*)
  – Algumas portas das *bridges* são mantidas num estado bloqueado (*blocking*) enquanto que outras participam activamente no mecanismo de comutação (estado *forwarding*)
  – O mecanismo está definido na norma IEEE 802.1D (e igualmente na norma IEEE 802.1Q, que contempla a extensão a VLANs)

Bridges transparentes (IEEE 802.1 D/Q)

- O mecanismo de *bridging* transparente foi inicialmente especificado na norma IEEE 802.1D – a versão mais recente é identificada como IEEE 802.1D-2004
- A norma IEEE 802.1D define uma arquitectura para interligação de LANs abaixo da interface de serviço MAC – as *bridges* MAC permitem comunicação entre estações (*end-stations*) ligadas a diferentes LANs (segmentos) como se estivessem ligadas à mesma LAN (garantindo transparência em relação a protocolos LLC e de Rede)
  - Uma *bridged LAN* é definida como uma concatenação de LANs IEEE 802 ligadas por *bridges* MAC
- O serviço MAC inclui a prioridade de utilizador como parâmetro de QoS
  - A camada MAC mapeia prioridades de utilizador em prioridades de acesso (se a camada MAC das LANs individuais suportar prioridades)
  - As *bridges* mapeiam informação de prioridade transportada em tramas MAC em uma ou mais classes de tráfego (consideradas do ponto de vista da operação dos mecanismos de prioridade e de gestão de filas de espera do processo de despacho)
- A norma IEEE 802.1Q estende os conceitos de *bridging* transparente de forma a incluir a definição e gestão de LANs Virtuais (*Virtual LANs* – VLANs)

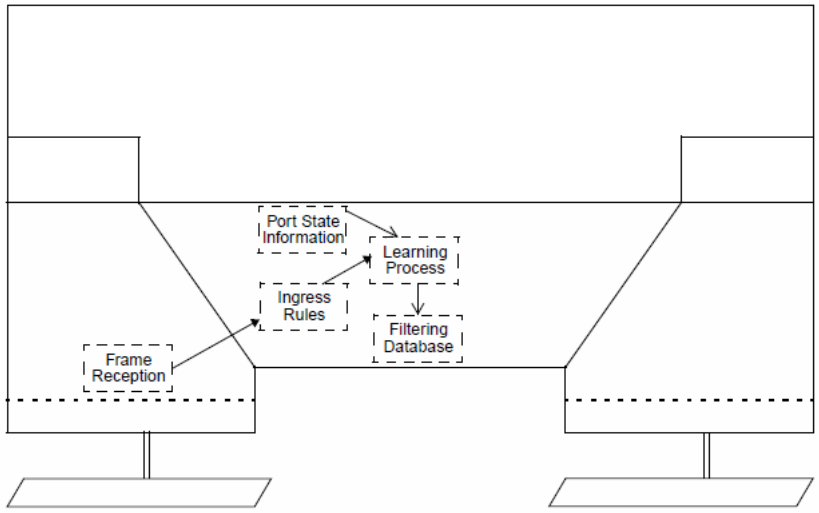
Bridges IEEE 802.1D/Q – arquitectura



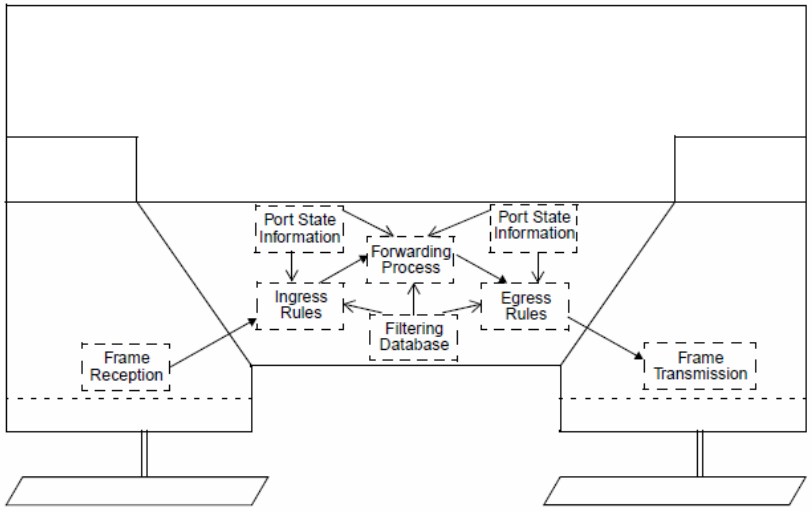
Bridges IEEE 802.1D/Q – learning e forwarding

- As *bridges* transparentes usam um processo de aprendizagem para construir e manter as suas tabelas de comutação de forma automática e dinâmica, adaptando-se deste modo a alterações topológicas (na norma é usada a expressão *filtering database* como sinónimo de *forwarding table*)
- As *bridges* não executam qualquer protocolo de encaminhamento para descoberta de rotas

Learning



Forwarding



Bridges IEEE 802.1D/Q – operação

» Aprendizagem de endereços (*learning*)
  – As entradas da tabela de comutação são construídas com base num processo de aprendizagem que associa endereços MAC a portas
  – Quando uma trama é recebida numa porta, o respectivo endereço MAC de origem (SA) é lido e associado a essa porta na tabela de comutação, significando que essa estação é alcançável através dessa porta (actualiza informação anterior, se presente)
  – As entradas da tabela são mantidas temporariamente, sendo eliminadas após um intervalo de tempo configurado em que não exista actividade da estação correspondente (*ageing*)

» Comutação de tramas (*forwarding*)
  – Tramas com endereço de destino *multicast* ou *broadcast* são difundidas em todas as portas no estado *forwarding*, com excepção da porta de entrada
  – Quando uma trama com endereço MAC de destino (DA) *unicast* é recebida, é consultada a tabela de comutação
    » Se não for encontrada qualquer porta com o endereço DA associado, a trama é enviada para todas as portas no estado *forwarding*, com excepção da porta de entrada
    » Se for encontrada uma porta com o endereço DA associado, a trama é enviada para essa porta, desde que esteja no estado *forwarding* e não seja a porta de entrada
  – As tramas são transmitidas da origem até ao(s) destino(s) ao longo da árvore criada pelo protocolo *spanning tree* (SPT)

Segmentação com bridges transparentes – análise

- Algumas limitações das *bridges* (igualmente aplicável a comutadores)
  - Uma *bridged LAN* não é hierárquica (*flat network*), o que coloca problemas de escalabilidade (não é possível estruturar uma rede apenas com *bridges*)
  - Uma *bridged LAN* não constitui uma barreira à difusão de tramas (que pode ser necessária nalguns casos de tráfego *unicast*, para além de ser obrigatória no caso de tráfego *broadcast / multicast*), o que pode levar a desperdício de recursos
  - Uma *spanning tree* não oferece as melhores rotas para todo o tráfego e não utiliza a capacidade das ligações que não fazem parte da árvore (o que também impede *load sharing* / *balancing*) – para além disso, é necessário ter em conta o tempo de convergência do protocolo aquando de reconfigurações topológicas
- Comparação com *routers*
  - Menor carga de processamento (menos "inteligentes")
    - Mais rápidas (menor latência) / mais baratas
  - Transparentes a protocolos de nível 3
    - Vantagens – suportam protocolos não encaminháveis (*non routable*) e em ambientes multi-protocolo evitam a necessidade de *routers* multi-protocolo
    - Desvantagens – impossível filtrar tráfego com base em protocolos de nível 3
  - Configuração mais simples

Segmentação com comutadores – análise

- Os comutadores de LAN partilham algumas propriedades das *bridges*
  - Comutação baseada em endereços MAC (e aprendizagem de endereços)
  - Criação de uma topologia lógica aberta (*spanning tree*)
  - Transparência em relação a equipamentos terminais (*end-stations*)
  - Mesmas limitações (ausência de hierarquia, difusão de tramas, *spanning trees*)
- Permitem microsegmentação – redução da dimensão dos domínios de colisão
  - No limite, uma estação por porta – LAN privada
  - Funcionamento *full-duplex* (CSMA/CD inibido) na ligação entre dois comutadores e no caso de uma única estação por porta
- Permitem aumentar de forma significativa a capacidade de comutação
  - A capacidade total cresce com o número de portas e com a velocidade por porta (10 Mbit/s, 100 Mbit/s, 1 Gbit/s, ….)
- Permitem melhorar o desempenho
  - Comutação em *hardware* (menor latência)
  - Suporte de classes de tráfego
- Permitem realizar segmentação lógica da rede, independente da localização física das estações, suportando assim o conceito de LAN Virtual

Segmentação com routers – análise

- Os *routers* são responsáveis pelo encaminhamento de tráfego entre (sub)redes IP (função nuclear) mas desempenham outras funções importantes
  - Estruturação lógica da rede (subredes)
    - Permitem hierarquizar a rede, o que garante escalabilidade
    - Isolam domínios de difusão – controlam *broadcasts*, o que garante estabilidade
    - Permitem criar / separar domínios administrativos
  - Filtragem de tráfego (*firewalls*) de / para o exterior, o que permite implementar políticas de segurança
  - Suporte de QoS
- Comparação com *bridges*
  - Mais complexos / maior *overhead* de processamento
    - Mais caros / mais lentos (maior latência)
  - Configuração mais complexa
- A oferta de *routers* com capacidade de comutação de tramas (*router switches*) permite soluções mais flexíveis, o que atenua algumas das limitações dos *routers* convencionais em ambientes LAN

LANs Virtuais

LANs IP – evolução

» A evolução constante na área da micro-electrónica (aumento da capacidade de processamento e memória, miniaturização, redução de custos, etc.) tem permitido o desenvolvimento de computadores cada vez mais potentes e de novos equipamentos terminais (dotados com múltiplas interfaces de rede, em particular interfaces *wireless*), o que potencia aplicações cada vez mais sofisticadas, que colocam requisitos mais exigentes do ponto de vista da comunicação (e.g., mobilidade e ubiquidade)

» Os equipamentos de rede usados nas LANs de primeiras gerações (*bridges* e *routers*) não conseguiam dar resposta a novos requisitos (desempenho, novos modelos de organização, gestão de recursos, etc.), o que motivou a procura de novas soluções quer arquitectónicas quer tecnológicas

» Neste contexto, constituiu um marco importante a introdução de comutadores de LAN (*LAN switches*) e a possibilidade que abriram para a exploração de LANs Virtuais (VLANs – *Virtual LANs*) e a necessidade de dotar os *routers* com funcionalidades adaptadas a este novo ambiente (e.g., *router switches*)

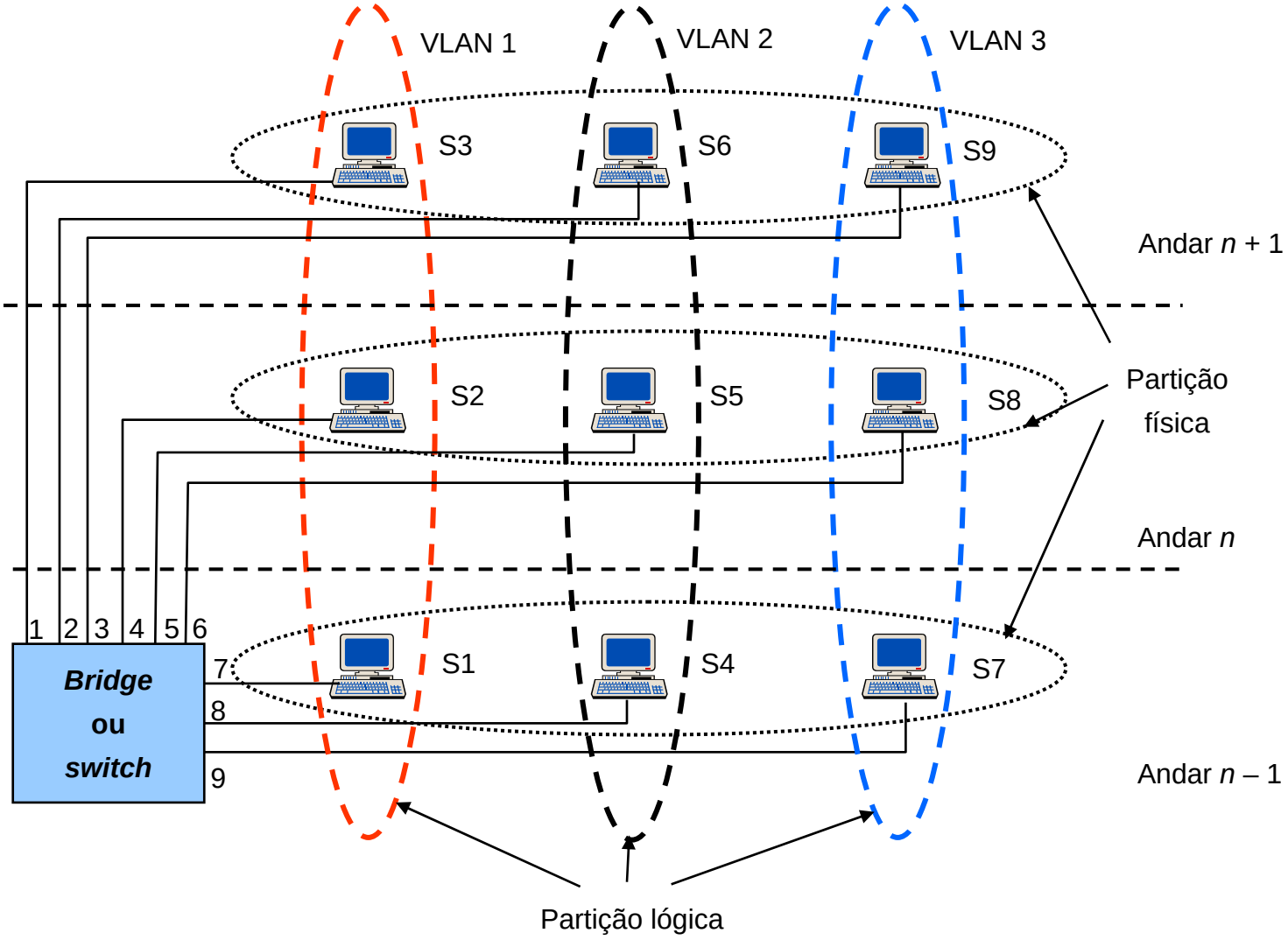
LANs IP – actualização de requisitos

- Desempenho
  - Requisitos de elevado *throughput* e pequena latência
    - Aumento do volume de tráfego – PCs, *workstations*, servidores cada vez mais rápidos
    - Novas aplicações multimédia e aplicações com requisitos de tempo real
- Modelo de organização
  - Grupos de trabalho dinâmicos podem requerer reconfigurações frequentes
    - Mudança de local físico sem mudança de grupo (e inversamente)
    - Pertença a mais do que um grupo
  - Comutação de tráfego dentro do mesmo grupo, em vez de encaminhamento, independentemente da localização física
- Centralização física de recursos
  - Exploração de cablagens estruturadas
  - Segurança, manutenção, redundância (disponibilidade), reconfiguração, partilha
  - Requisitos de maior largura de banda para permitir acessos de mais alta velocidade a recursos partilhados (servidores, *routers* para acesso externo, etc.)
- Acesso externo (Internet)
  - Tráfego com exterior atravessa o *backbone*
- Suporte de Qualidade de Serviço (QoS)
  - Mecanismos de nível 2 e nível 3

LANs Virtuais / Virtual LANs (VLANs)

- Uma VLAN é uma LAN comutada baseada em segmentação lógica, isto é, as estações numa VLAN formam um grupo lógico e pertencem ao mesmo domínio de difusão (na camada MAC), independentemente da respectiva localização física
- A exploração do conceito pressupõe a possibilidade de criar múltiplas VLANs numa rede local, o que coloca vários requisitos
  - Possibilidade de criar múltiplas VLANs num comutador
  - Possibilidade de estender qualquer VLAN a vários comutadores
    - Torna-se assim necessário identificar o tráfego associado a cada VLAN nas ligações entre comutadores – existe actualmente um mecanismo de etiquetagem (*tagging*) normalizado (IEEE 802.1Q)
- Deve também ser possível que uma estação pertença a mais do que uma VLAN – *routers* e servidores são casos típicos (mas não únicos)
  - Esta possibilidade pode ser suportada pelo mecanismo de etiquetagem
- Convém distinguir portas de interligação entre comutadores (*trunk ports*) de portas de acesso
  - No caso de *trunk ports*, a etiquetagem permite facilmente estender VLANs entre comutadores, enquanto que em portas de acesso a necessidade de etiquetagem depende do tipo de estação ligada (que pode ou não suportar etiquetagem)

VLANs – exemplo do conceito



Conectividade entre VLANs em redes IP

- Assumimos que, em LANs IP, estações na mesma subrede IP fazem parte da mesma VLAN (caso contrário não existiria conectividade a nível MAC)
- A conectividade entre estações que pertencem a subredes IP / VLANs diferentes tem de ser garantida por *routers*
- Um *router* tem de fazer parte das várias VLANs associadas às redes IP que interliga
  - Uma solução consiste em ter ligações físicas separadas a portas de um comutador, por cada VLAN envolvida
  - Uma solução mais eficiente consiste numa única ligação física à qual estão associadas várias interfaces virtuais (uma por VLAN) – esta solução é possível, em particular, com *router switches* e requer naturalmente a etiquetagem de tramas
  - Embora se possa justificar a existência de vários *routers*, em casos simples será suficiente um único *router* (*one-armed router*), com as limitações inerentes (e.g., ausência de redundância e sobrecarga de tráfego no *router*)
- Nalguns casos pode não ser necessário envolver *routers* no percurso de dados se uma estação (por exemplo, um servidor) fizer parte de várias VLANs – a comunicação entre o servidor e uma estação pode realizar-se na VLAN comum

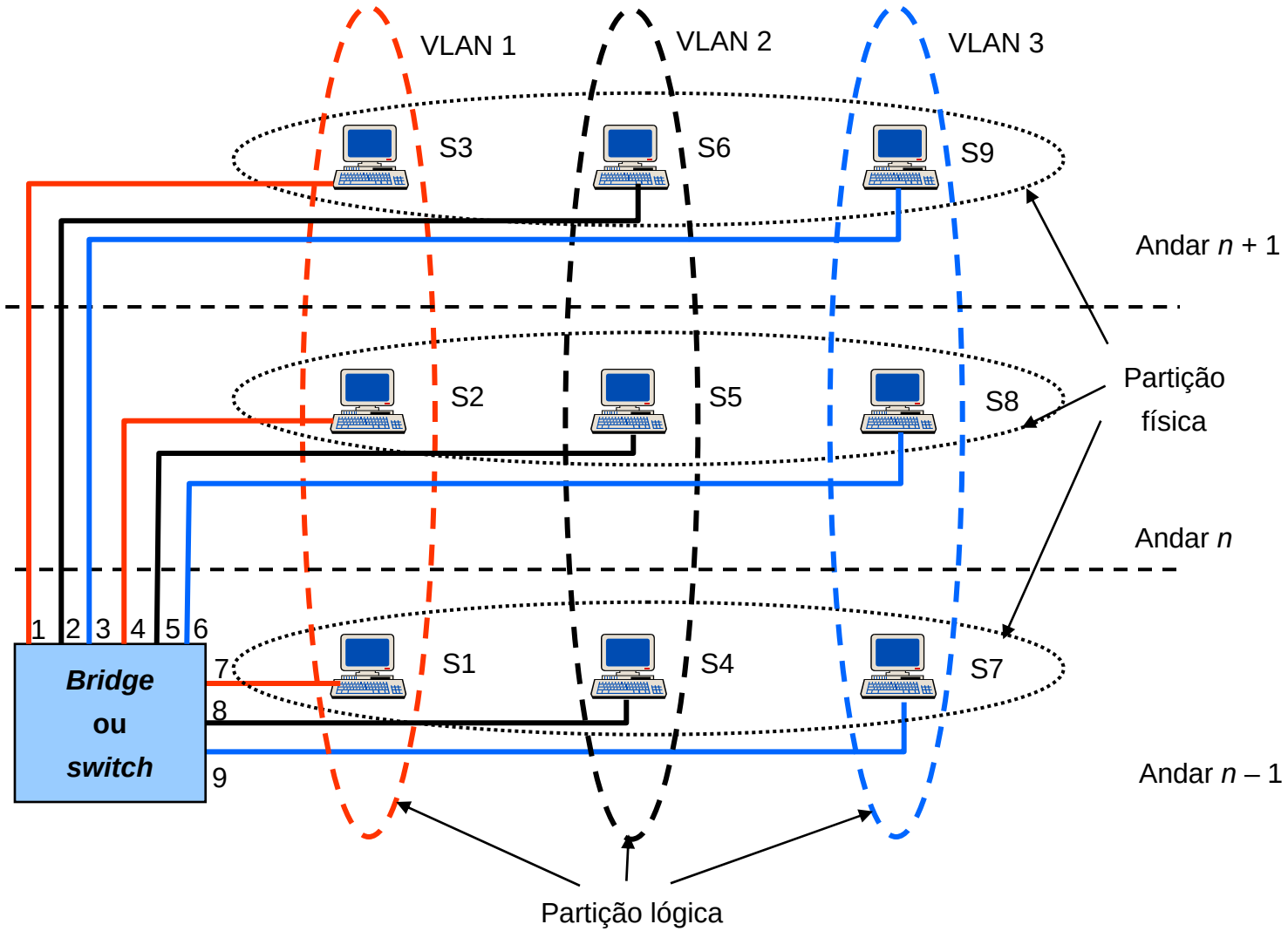
Critérios para formar VLANs

- De entre os vários critérios para formar VLANs que foram propostos e suportados por fabricantes de comutadores destacam-se os seguintes
  - Por porta – uma VLAN é definida como um grupo de portas
  - Por endereço MAC – uma VLAN é definida como um grupo de endereços MAC (*Layer 2 VLAN*)
  - Por subrede lógica (IP) – uma VLAN é definida como um grupo de endereços IP (*Layer 3 VLAN*)
  - Por família / tipo de protocolo
- Nas VLANs do primeiro tipo as associações de estações a VLANs são estáticas e uma porta apenas pode pertencer a uma VLAN
- Nos restantes casos as associações são dinâmicas, uma estação pode pertencer a várias VLANs e uma porta pode ter associadas várias VLANs
- Qualquer que seja o critério adoptado, a operação de comutadores realiza-se na camada MAC e baseia-se em endereços MAC – por exemplo, uma *Layer 3 VLAN* não encaminha pacotes IP, mas define apenas um critério (de nível 3) para formar VLANs

VLANs baseadas em portas

- Começamos por considerar o caso básico em que uma porta não suporta etiquetagem de tramas – uma estação pertence a uma VLAN pelo facto de se ligar a uma porta e não por qualquer atributo próprio (e.g., um endereço MAC ou IP, como noutros tipos de VLANs)
  - Não são associados endereços MAC a VLANs (como em *Layer 2 VLANs*), mas há aprendizagem de endereços MAC para efeito de comutação
- Neste caso, e por esta razão, só é possível associar uma VLAN a cada porta, à qual é atribuído um identificador da VLAN respectiva (PVID – *Port VLAN ID*)
  - Se várias estações estiverem ligadas a uma porta (por exemplo através de um *hub*) todas as estações pertencem à mesma VLAN
- Se uma porta suportar etiquetagem, o respectivo PVID representa a sua VLAN nativa
  - Em tramas etiquetadas a VLAN respectiva é identificada pela etiqueta
  - Tramas não etiquetadas recebidas na porta são associadas à VLAN nativa (PVID)
- A configuração é manual e relativamente fácil, não existindo qualquer processo de "aprendizagem" na formação de VLANs (VLANs estáticas)
- É necessária a intervenção do gestor da rede no caso de reconfigurações (adição, remoção ou alteração da localização de estações)
- A difusão de uma trama é feita apenas nas portas que pertencem à VLAN associada à porta onde a trama foi recebida

VLANs baseadas em portas – exemplo



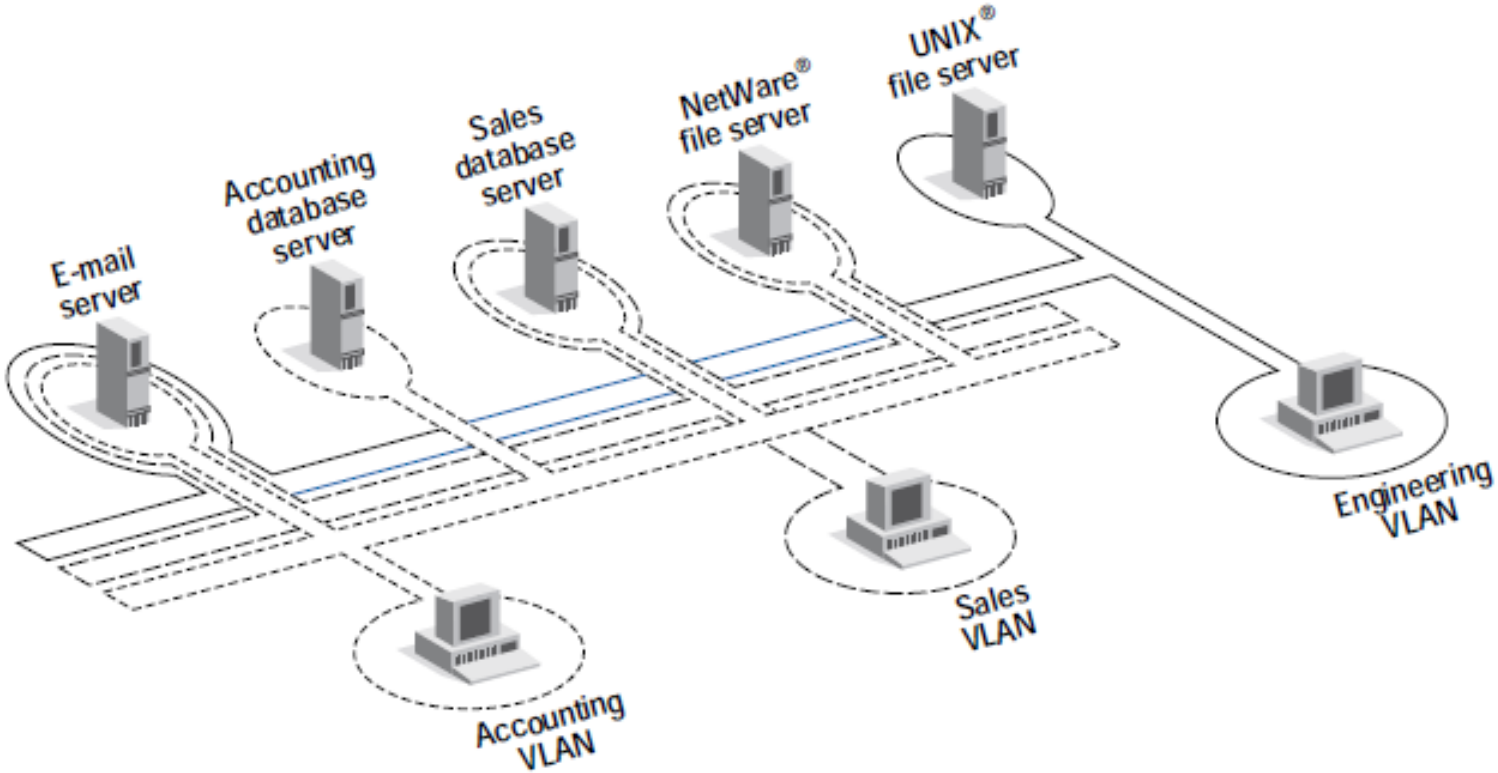
VLANs baseadas em endereços MAC

- O gestor da rede associa endereços MAC a uma ou mais VLANs (esta informação é mantida centralmente)
- A configuração é complexa e sujeita a erros e levanta problemas de escalabilidade (devido ao elevado número de endereços a configurar e ao facto de não serem estruturados)
- Uma estação (endereço MAC) tem de ser explicitamente associada pelo menos a uma VLAN, tendo de repetir-se o processo se houver substituição da carta de interface
- Trata-se de VLANs dinâmicas, uma vez que quando um endereço MAC (de origem) é visto pela primeira vez numa porta, é feita a associação automática da(s) VLAN(s) correspondente(s)
  - A uma porta podem estar associadas múltiplas VLANs, não só porque uma estação pode estar associada a várias VLANs, mas porque a porta pode receber tráfego de diferentes estações (cujos endereços MAC estejam associados a VLANs diferentes)
    - Neste caso, o tráfego de uma VLAN difundido numa porta acaba por ser recebido também por estações que pertencem a outras VLANs associadas a essa porta
- O processo de associação de estações a VLANs é transparente a mudanças de localização física de uma estação (não é necessária qualquer reconfiguração)

VLANs baseadas em subredes IP

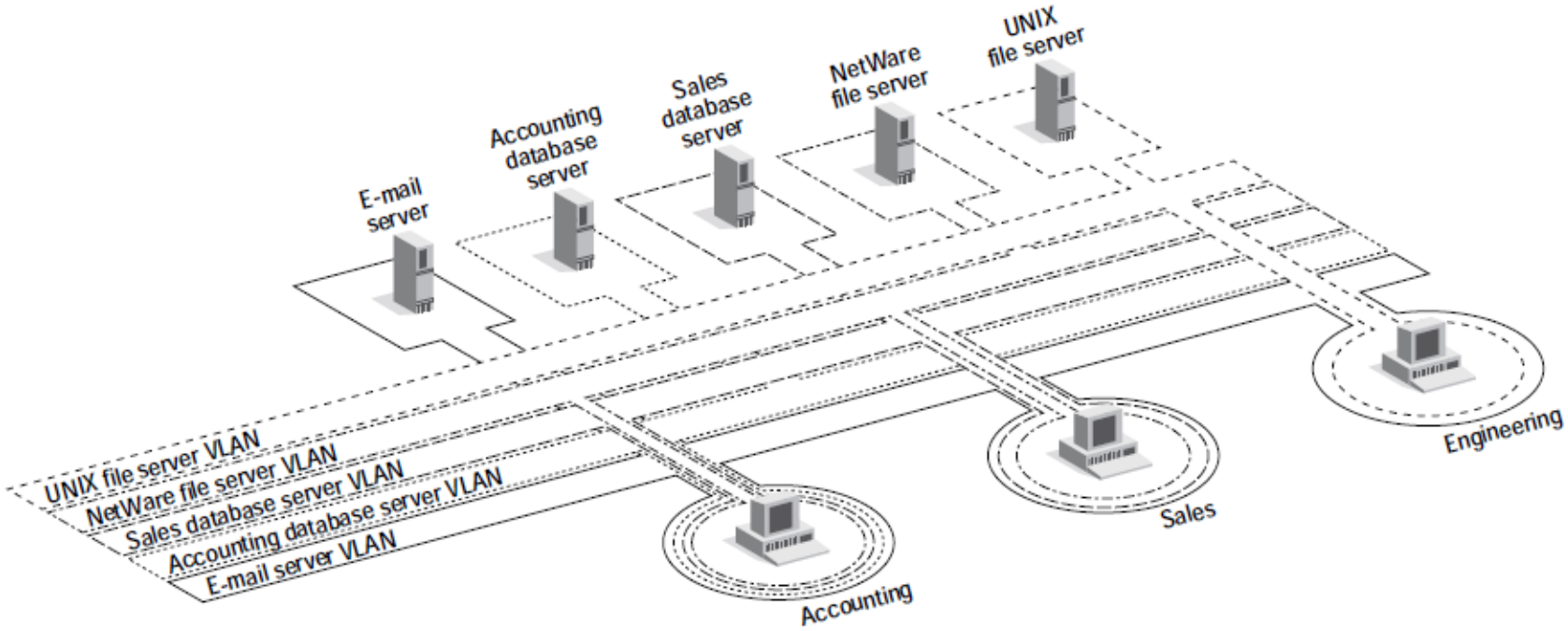
- O processo de associação de subredes IP a VLANs é normalmente realizado pelo gestor da rede (configuração manual), embora alguns fabricantes tenham desenvolvido soluções em que a associação é automática
- Trata-se igualmente de VLANs dinâmicas, uma vez que a associação de uma ou mais VLANs a uma porta se baseia na observação do tráfego recebido na porta (a associação apenas se verifica se o endereço IP de origem pertencer a uma das subredes definidas)
  - A necessidade de processar o cabeçalho dos pacotes, para identificação da VLAN em que as tramas devem ser comutadas ou mesmo difundidas (e não para determinação de rotas), é um factor de degradação de desempenho
- São fáceis de gerir, uma vez que os endereços IP têm estrutura
- São possíveis múltiplas VLANs por estação e múltiplas VLANs por porta
- O processo é transparente à mudança de localização física de uma estação
- A definição de VLANs por um critério de nível 3 pode evitar a necessidade de etiquetagem para transportar, entre comutadores, a informação de pertença a uma VLAN

Organização de VLANs por departamento



- Um servidor (serviço) é associado a uma ou mais VLANs – ocorre *overlap* apenas a nível de servidores (recursos partilhados)
- Administração simples
- Solução adaptada a organizações com fronteiras claras entre departamentos

Organização de VLANs por serviço



- Cada servidor (serviço) define uma VLAN
- Os utilizadores de serviços podem pertencer a mais do que uma VLAN
- Relações de pertença difíceis de gerir

VLANs IEEE 802.1Q

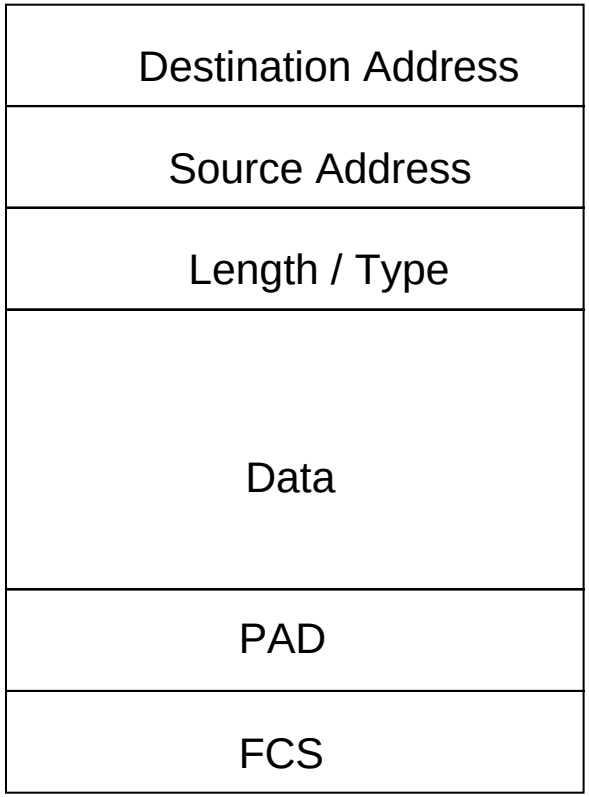
- A versão mais recente da norma é identificada como IEEE 802.1Q-2005
- A norma IEEE 802.1Q estende os conceitos de *bridging* e filtragem na camada MAC com o objectivo de suportar a definição e gestão de LANs Virtuais (*Virtual LANs* – VLANs)
- A especificação de *VLAN bridging* é idependente de IEEE 802.1D, mas contém (reutiliza) muitos dos elementos desta especificação
- A norma IEEE 802.1Q define um formato de trama que permite transportar um identificador de VLAN e informação de prioridade de utilizador, sendo esta informação útil em LANs que não suportam prioridades nativamente (por exemplo, IEEE 802.3 / Ethernet)
  - Estende o mecanismo de prioridade definido em IEEE 802.1D, fazendo uso da capacidade de tramas VLAN transportarem informação de prioridade extremo a extremo, através de MACs concatenados, independentemente da capacidade de sinalização de prioridade por parte de cada tipo particular de MAC

IEEE 802.1Q – etiquetagem (tagging)

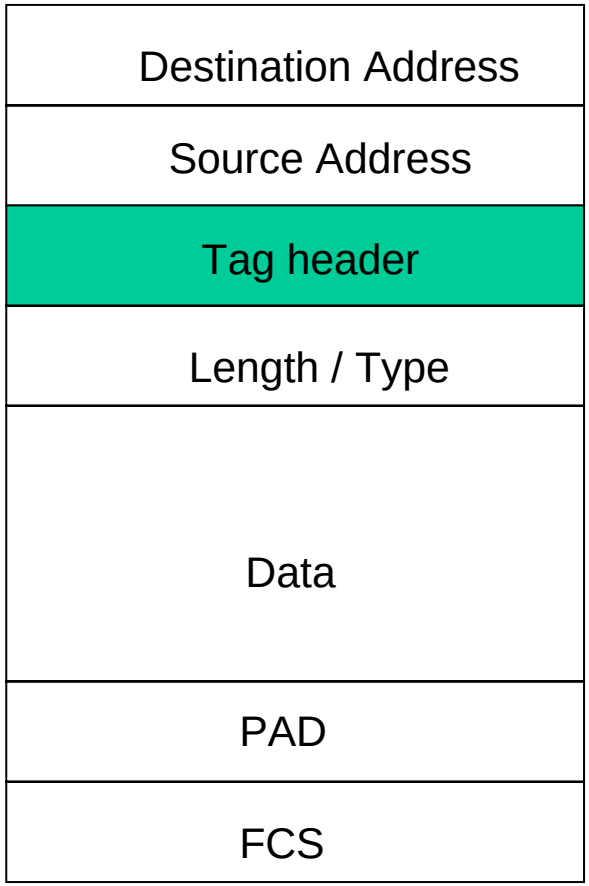
- Uma trama etiquetada (*tagged frame*) é uma trama que contém um *tag header* inserido após o campo de endereço MAC de origem (ou o campo *Routing Information*, caso exista)
  - O *tag header* transporta informação de prioridade e, opcionalmente, a identificação da VLAN associada à trama
- O *tag header* inclui
  - Um *Tag Protocol Identifier* (TPID)
  - *Tag Control Information* (TCI)
- Existem dois tipos de tramas etiquetadas
  - *Priority-tagged frame* – o *tag header* transporta informação de prioridade, mas não informação de identificação de VLAN
  - *VLAN-tagged frame* – o *tag header* transporta informação de identificação de VLAN e informação de prioridade
- As *bridges* podem ser
  - *VLAN-aware* – reconhecem tramas do tipo *VLAN-tagged* e podem inserir e remover *tag headers*
  - *VLAN-unaware* – não reconhecem tramas do tipo *VLAN-tagged*

Tramas IEEE 802.3 / Ethernet etiquetadas e não etiquetadas

Untagged frame



Tagged frame



A presença de um *Tag Header* é indicada por um valor específico a seguir ao campo *Source Address*, na posição habitualmente ocupada pelo campo *Length* / *Type*

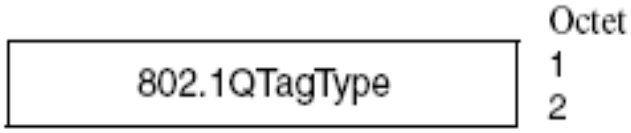
Tag Protocol Identifier (TPID)

» Formato

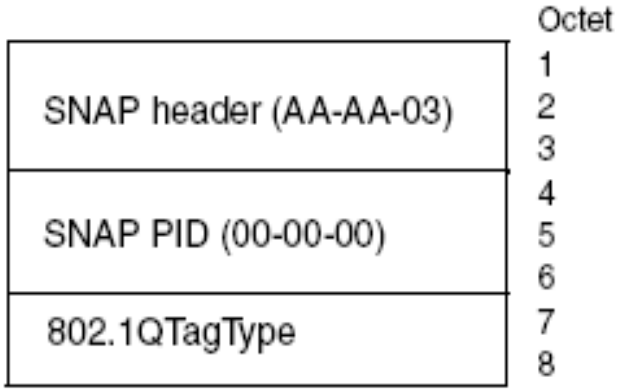
– A estrutura deste campo difere conforme se usar codificação Ethernet ou SNAP (SNAP é usado em IEEE 802.5 e FDDI)

– O TPID transporta um valor de tipo (*Ethernet Type*) igual a 81-00 que identifica a trama como etiquetada (*802.1QTagType*)

Ethernet-encoded TPID format

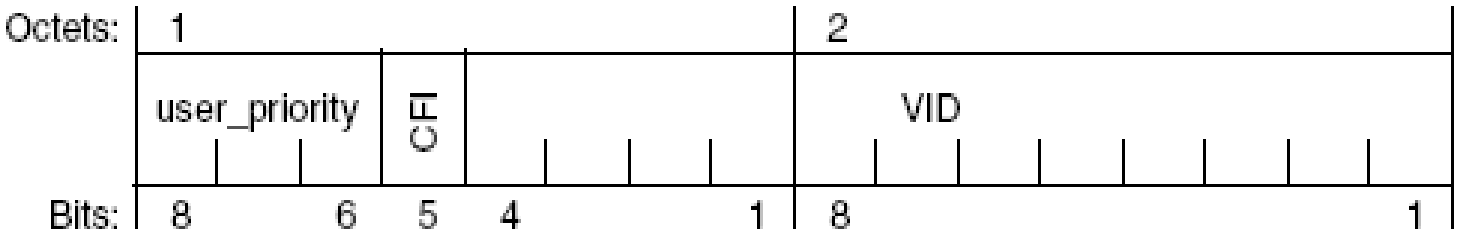


SNAP-encoded TPID format



Tag Control Information (TCI)

» Formato
  – Prioridade de utilizador – são usados 3 bits para representar até 8 níveis de prioridade
  – *Canonical Format Indicator* (CFI) – 1 bit (*flag*)
  – *VLAN Identifier* (VID) – 12 bits para identificar a VLAN a que a trama pertence
    » Uma trama *priority-tagged* é identificada por um valor nulo no campo VID



Classificação de tramas e associação a VLANs

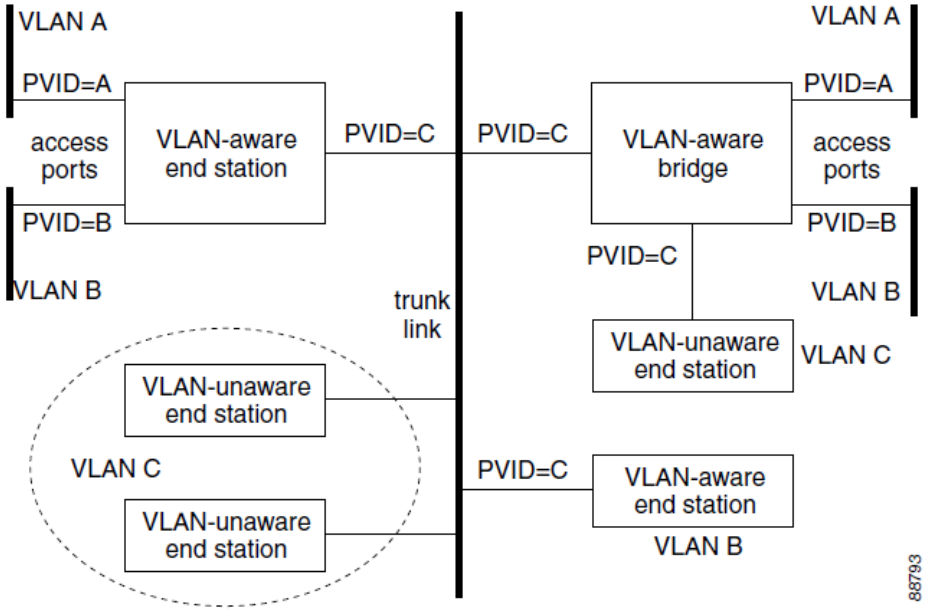
- Uma *bridge* IEEE 802.1Q (*VLAN bridge*) suporta classificação de VLANs com base em portas (*Port-based VLAN*)
  - Pode adicionalmente suportar classificação baseada em porta e protocolo (*Port-and-Protocol-based VLAN*)

- Cada trama recebida e admitida numa porta duma *VLAN bridge* tem de ser associada a uma e uma só VLAN (é-lhe associado um VID)
  - Se se tratar duma trama *VLAN-tagged*, a própria trama transporta um VID (etiquetagem explícita)
  - Caso contrário (*Untagged* ou *Priority-tagged*) a etiquetagem é implícita
    - Se se tratar de uma *Port-based VLAN*, a associção (classificação) é determinada pela porta, o que requer que cada porta tenha associado um PVID (*Port VLAN Identifier*)
    - Se se tratar de uma *Port-and-Protocol-based VLAN*, a associação é determinada pela porta e pelo identificador de protocolo transportado na trama – para além do PVID é necessário que a porta tenha associados múltiplos VIDs (*VID Set*), sendo cada VID associado a um *Protocol Group Identifier*

VLAN nativa e etiquetagem

» Numa rede podem coexistir estações / *bridges* sensíveis e não sensíveis a VLANs (*VLAN-aware* e *VLAN-unware*, respectivamente)
  – O PVID associado a uma porta funciona como uma etiqueta para as tramas não etiquetadas recebidas pela porta e representa a VLAN nativa

» No exemplo, as duas estações *VLAN-unware* ligadas ao *trunk* estão associadas à VLAN C uma vez que as portas das *VLAN-aware bridges* ligadas ao *trunk* têm PVID = C – todas as tramas não etiquetadas recebidas nessas portas são associadas à VLAN C



Parâmetros associados a uma porta

- Cada porta de uma VLAN *bridge* deve suportar os seguintes parâmetros
  - *Acceptable Frame Types*, que pode ser configurado para
    - Admitir apenas tramas do tipo *VLAN-tagged*
    - Admitir apenas tramas do tipo *Untagged* e *Priority-tagged*
    - Admitir todas as tramas
  - PVID (*Port VLAN Identifier*) para classificação do tipo *Port-based*
- Pode ainda suportar o parâmetro
  - *VID Set*, para classificação do tipo *Port-and-Protocol-based*

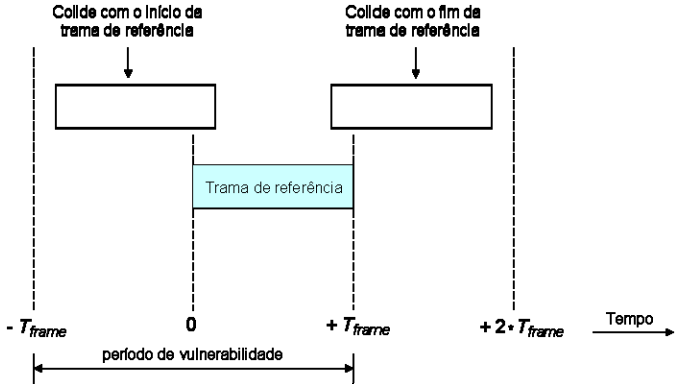
- A aceitação de uma trama para despacho pela *bridge* depende do tipo de trama e da configuração destes parâmetros na porta respectiva

Anexo

ALOHA – eficiência

» S – tráfego relativo transportado
- λ_{rx} – Taxa de pacotes transmitidos com sucesso
- $S = \lambda_{rx} \times T_{frame}$

» G – tráfego relativo oferecido
- λ – Taxa de pacotes transmitidos com e sem sucesso
- $G = \lambda \times T_{frame}$



» Modelo de tráfego
- Processo de Poisson com população infinita e tramas com tamanho fixo

» $S = G\,P_0$
- P_0 – probabilidade de nenhum outro pacote ser gerado em $2xT_{frame}$ (período de vulnerabilidade)

$$P_k = P[k\_pacotes\_oferecidos\_em\_2\times T_{frame}] = \frac{(\lambda 2T_{frame})^k e^{-\lambda 2T_{frame}}}{k!} = \frac{(2G)^k e^{-2G}}{k!}$$

$$P_0 = \frac{(2G)^0 e^{-2G}}{0!} = e^{-2G}$$

$$\max\left(\frac{S}{G}\right) \rightarrow \frac{dS}{dG} = 0 \Leftrightarrow e^{-2G}(1-2G) = 0 \Leftrightarrow G = \frac{1}{2} \qquad S_{\max} = \frac{1}{2e} = 18{,}4\%$$

Slotted ALOHA – eficiência

» Período de vulnerabilidade – T_{frame}

$$P_k^{'} = P[k\_pacotes\_oferecidos\_em\_T_{frame}] = \frac{(\lambda T_{frame})^k e^{-\lambda T_{frame}}}{k!} = \frac{(G)^k e^{-G}}{k!}$$

$$P_0^{'} = \frac{(G)^0 e^{-G}}{0!} = e^{-G}$$

$$S = GP_0^{'} = Ge^{-G}$$

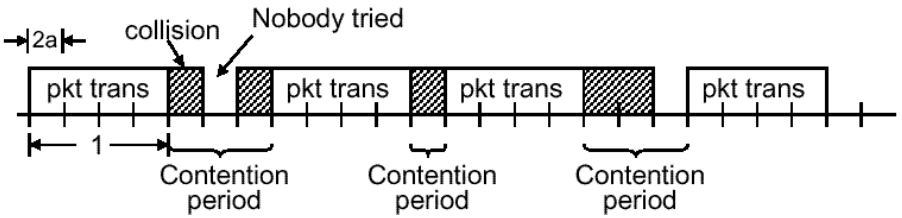
$$\max\left(\frac{S}{G}\right) \rightarrow \frac{dS}{dG} = 0 \Leftrightarrow G = 1 \qquad S_{\max} = \frac{1}{e} = 36{,}8\%$$

CSMA/CD – eficiência

» Eficiência $S = \dfrac{n_{tx}}{n_{tx} + E[n_{cont}]}$

$T_{slot} = 2 \times T_{prop}$

$$n_{tx} = \frac{T_{frame}}{T_{slot}} = \frac{T_{frame}}{2 \times T_{prop}} = \frac{1}{2a}$$



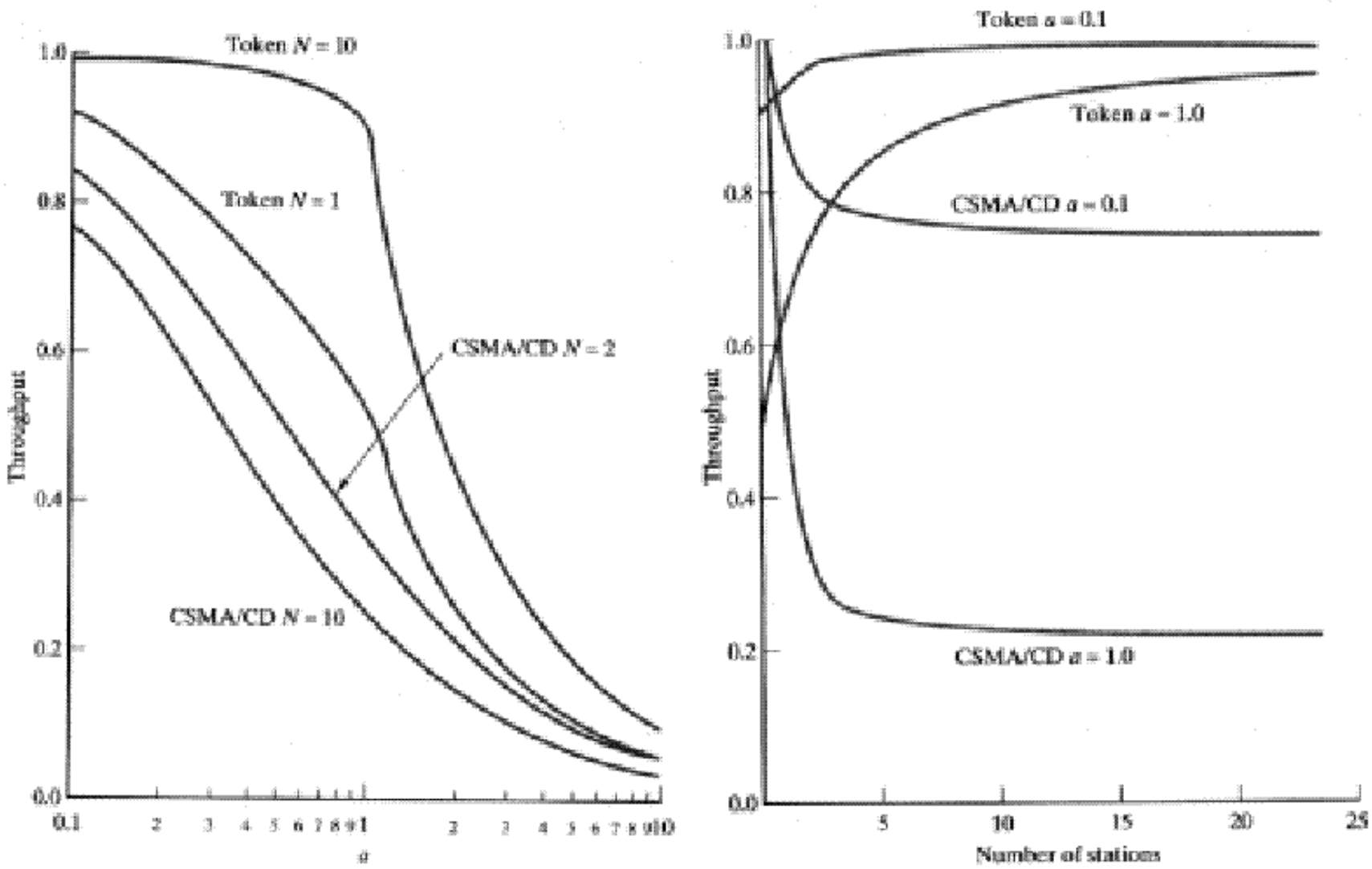
» $A = \binom{N}{1} P^1 (1-P)^{N-1} = NP(1-P)^{N-1}$

- P – Probabilidade de uma estação transmitir num *slot*
- A – Probabilidade de exactamente uma estação transmitir num *slot* e adquirir o meio

» $E[n_{cont}] = \sum_{i=1}^{+\infty} i(1-A)^i A = \dfrac{1-A}{A}$ $\quad \Rightarrow S = \dfrac{1/2a}{1/2a + (1-A)/A} = \dfrac{1}{1 + 2a(1-A)/A}$

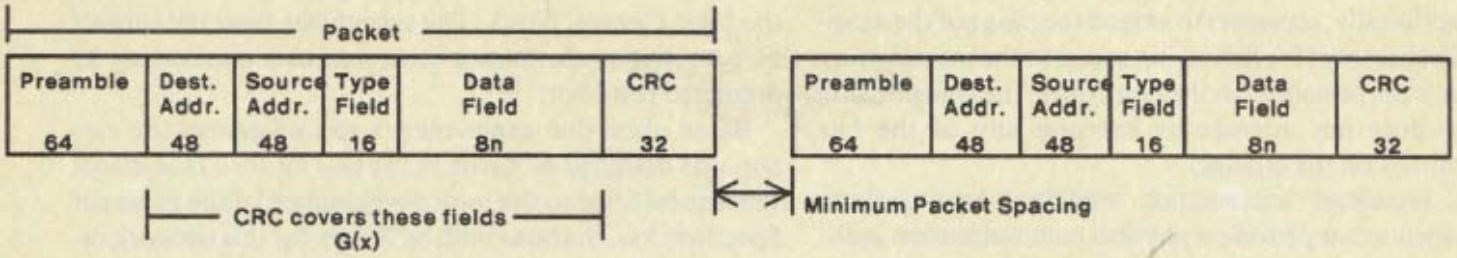
» P=1/N ➔ $A_{MAX} = \left(1 - \dfrac{1}{N}\right)^{N-1}$ $\quad \lim_{N\to\infty}\left(1 - \dfrac{1}{N}\right)^{N-1} = \dfrac{1}{e} \quad \Rightarrow \lim_{N\to\infty} S = \dfrac{1}{1 + 3.44a}$

CSMA/CD vs. Token Ring – eficiência



Ethernet 1.0 Technical Summary (1) *(*)*

Packet Format



Stations must be able to transmit and receive packets on the common coaxial cable with the indicated packet format and spacing. Each packet should be viewed as a sequence of 8-bit bytes; the least significant bit of each byte (starting with the preamble) is transmitted first.

Maximum Packet Size: 1526 bytes (8 byte preamble + 14 byte header + 1500 data bytes + 4 byte CRC)

Minimum Packet Size: 72 bytes (8 byte preamble + 14 byte header + 46 data bytes + 4 byte CRC)

Preamble: This 64-bit synchronization pattern contains alternating 1's and 0's, ending with two consecutive 1's. The preamble is: 10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101011.

Destination Address: This 48-bit field specifies the station(s) to which the packet is being transmitted. Each station examines this field to determine whether it should accept the packet. The first bit transmitted indicates the type of address. If it is a 0, the field contains the unique address of the one destination station. If it is a 1, the field specifies a logical group of recipients; a special case is the broadcast (all stations) address, which is all 1's.

Source Address: This 48-bit field contains the unique address of the station that is transmitting the packet.

Type Field: This 16-bit field is used to identify the higher-level protocol type associated with the packet. It determines how the data field is interpreted.

Data Field: This field contains an integral number of bytes ranging from 46 to 1500. (The minimum ensures that valid packets will be distinguishable from collision fragments.)

Packet Check Sequence: This 32-bit field contains a redundancy check (CRC) code, defined by the generating polynomial:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

The CRC covers the address (destination/source), type, and data fields. The first transmitted bit of the destination field is the high-order term of the message polynomial to be divided by G(x) producing remainder R(x). The high-order term of R(x) is the first transmitted bit of the Packet Check Sequence field. The algorithm uses a linear feedback register which is initially preset to all 1's. After the last data bit is transmitted, the contents of this register (the remainder) are inverted and transmitted as the CRC field. After receiving a good packet, the receiver's shift register contains 11000111 00000100 11011101 01111011 (x^{31}, ... ,x^{0}).

Minimum Packet Spacing: This spacing is 9.6 usec, the minimum time that must elapse after one transmission before another transmission may begin.

Round-trip Delay: The maximum end-to-end, round-trip delay for a bit is 51.2 usec.

Collision Filtering: Any received bit sequence smaller than the minimum valid packet (with minimum data field) is discarded as a collision fragment.

(*) Extraído de *IEEE Computer, August 1982, pp. 14-15*

Ethernet 1.0 Technical Summary (2)

Control Procedure

The control procedure defines how and when a station may transmit packets into the common cable. The key purpose is fair resolution of occasional contention among transmitting stations.

Defer: A station must not transmit into the coaxial cable when carrier is present or within the minimum packet spacing time after carrier has ended.

Transmit: A station may transmit if it is not deferring. It may continue to transmit until either the end of the packet is reached or a collision is detected.

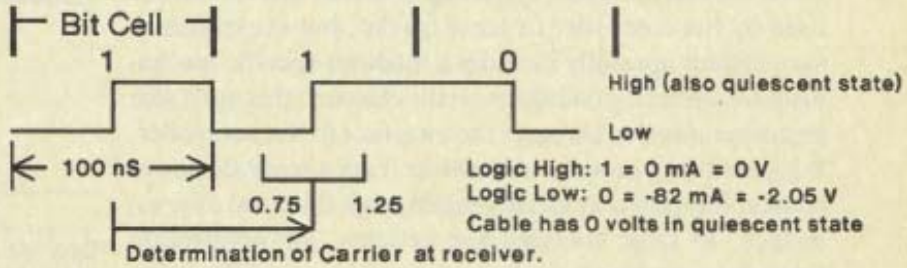
Abort: If a collision is detected, transmission of the packet must terminate, and a *jam* (4-6 bytes of arbitrary data) is transmitted to ensure that all other participants in the collision also recognize its occurrence.

Retransmit: After a station has detected a collision and aborted, it must wait for a random *retransmission delay*, defer as usual, and then attempt to retransmit the packet. The random time interval is computed using the backoff algorithm (below). After 16 transmission attempts, a higher level (e.g. software) decision is made to determine whether to continue or abandon the effort.

Backoff: Retransmission delays are computed using the *Truncated Binary Exponential Backoff* algorithm, with the aim of fairly resolving contention among up to 1024 stations. The delay (the number of time units) before the n^{th} attempt is a uniformly distributed random number from [0 to 2^n-1] for $0 < n \leq 10$ ($n = 0$ is the original attempt). For attempts 11-15, the interval is *truncated* and remains at [0 to 1023]. The unit of time for the retransmission delay is 512 bit times (51.2 usec).

Channel Encoding

Manchester encoding is used on the coaxial cable. It has a 50% duty cycle, and insures a transition in the middle of every bit cell ("data transition"). The first half of the bit cell contains the complement of the bit value, and the second half contains the true value of the bit.



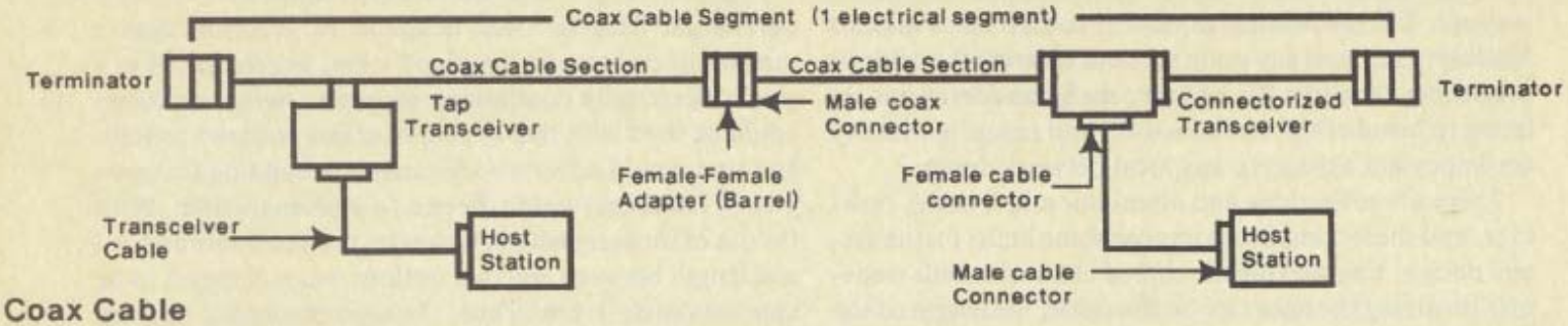
Data Rate

Data rate is 10 M bits/sec = 100 nsec bit cell ± 0.01%.

Carrier

The presence of data transitions indicates that carrier is present. If a transition is not seen between 0.75 and 1.25 bit times since the center of the last bit cell, then carrier has been lost, indicating the end of a packet. For purposes of deferring, carrier means any activity on the cable, independent of being properly formed. Specifically, it is any activity on either receive or collision detect signals in the last 160 nsec.

Ethernet 1.0 Technical Summary (3)



Coax Cable

Impedance: 50 ohms ± 2 ohms (Mil Std. C17-E). This impedance variation includes batch-to-batch variations. Periodic variations in impedance of up to ± 3 ohms are permitted along a single piece of cable.

Cable Loss: The maximum loss from one end of a cable segment to the other end is 8.5 db at 10 MHz (equivalent to ~500 meters of low loss cable).

Shielding: The physical channel hardware must operate in an ambient field of 2 volts per meter from 10 KHz to 30 MHz and 5 V/meter from 30 MHz to 1 GHz. The shield has a transfer impedance of less than 1 milliohm per meter over the frequency range of 0.1 MHz to 20 MHz (exact value is a function of frequency).

Ground Connections: The coax cable shield shall not be connected to any building or AC ground along its length. If for safety reasons a ground connection of the shield is necessary, it must be in only one place.

Physical Dimensions: This specifies the dimensions of a cable which can be used with the *standard tap*. Other cables may also be used, if they are not to be used with a tap-type transceiver (such as use with connectorized transceivers, or as a section between sections to which standard taps are connected).

Center Conductor:	0.0855" diameter solid tinned copper
Core Material:	Foam polyethylene or foam teflon FEP
Core O.D.:	0.242 " minimum
Shield:	0.326" maximum shield O.D. (>90% coverage for outer braid shield)
Jacket:	PVC or teflon FEP
Jacket O.D.:	0.405"

Coax Connectors and Terminators

Coax cables must be terminated with male N-series connectors, and cable sections will be joined with female-female adapters. Connector shells shall be insulated such that the coax shield is protected from contact to building grounds. A sleeve or boot is acceptable. Cable segments should be terminated with a female N-series connector (can be made up of a barrel connector and a male terminator) having an impedance of 50 ohms ± 1%, and able to dissipate 1 watt. The outside surface of the terminator should also be insulated.

Ethernet 1.0 Technical Summary (4)

Transceiver

CONNECTION RULES

Up to 100 transceivers may be placed on a cable segment no closer together than 2.5 meters. Following this placement rule reduces to a very low (but not zero) probability the chance that objectionable standing waves will result.

COAX CABLE INTERFACE

Input Impedance: The resistive component of the impedance must be greater then 50 Kohms. The total capacitance must be less than 4 picofarads.

Nominal Transmit Level: The important parameter is average DC level with 50% duty cycle waveform input. It must be -1.025 V (41 mA) nominal with a range of -0.9 V to -1.2 V (36 to 48 mA). The peak-to-peak AC waveform must be centered on the average DC level and its value can range from 1.4 V P-P to twice the average DC level. The voltage must never go positive on the coax. The quiescent state of the coax is logic high (0 V). Voltage measurements are made on the coax near the transceiver with the shield as reference. Positive current is current flowing out of the center conductor of the coax.

Rise and Fall Time: 25 nSec $\pm$ 5 nSec with a maximum of 1 nSec difference between rise time and fall time in a given unit. The intent is that dV/dt should not significantly exceed that present in a 10 MHz sine wave of same peak-to-peak amplitude.

Signal Symmetry: Asymmetry on output should not exceed 2 nSec for a 50-50 square wave input to either transmit or receive section of transceiver.

TRANSCEIVER CABLE INTERFACE

Signal Pairs: Both transceiver and station shall drive and present at the receiving end a 78 ohm balanced load. The differential signal voltage shall be 0.7 volts nominal peak with a common mode voltage between 0 and +5 volts using power return as reference. (This amounts to shifted ECL levels operating between Gnd and +5 volts. A 10116 with suitable pulldown resistor may be used). The quiescent state of a line corresponds to logic high, which occurs when the + line is more positive than the - line of a pair.

Collision Signal: The active state of this line is a 10 MHz waveform and its quiescent state is logic high. It is active if the transceiver is transmitting and another transmission is detected, or if two or more other stations are transmitting, independent of the state of the local transmit signal.

Power: +11.4 volts to +16 volts DC at controller. Maximum current available to transceiver is 0.5 ampere. Actual voltage at transceiver is determined by the interface cable resistance (max 4 ohms loop resistance) and current drain.

ISOLATION

The impedance between the coax connection and the transceiver cable connection must exceed 250 Kohms at 60 Hz and withstand 250 VRMS at 60 Hz.

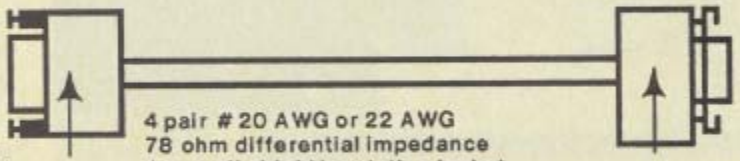
Transceiver Cable and Connectors

Maximum signal loss = 3 db @ 10 MHz. (equivalent to ~50 meters of either 20 or 22 AWG twisted pair).

Transceiver Cable Connector Pin Assignment

1.	Shield*		
2.	Collision +	9.	Collision -
3.	Transmit +	10.	Transmit -
4.	Reserved	11.	Reserved
5.	Receive +	12.	Receive -
6.	Power Return	13.	+ Power
7.	Reserved	14.	Reserved
8.	Reserved	15.	Reserved

*Shield must be terminated to connector shell.



Male 15 pin D-Series connector with lock posts.

4 pair # 20 AWG or 22 AWG
78 ohm differential impedance
1 overall shield insulating jacket
4 ohms max loop resistance for power pair

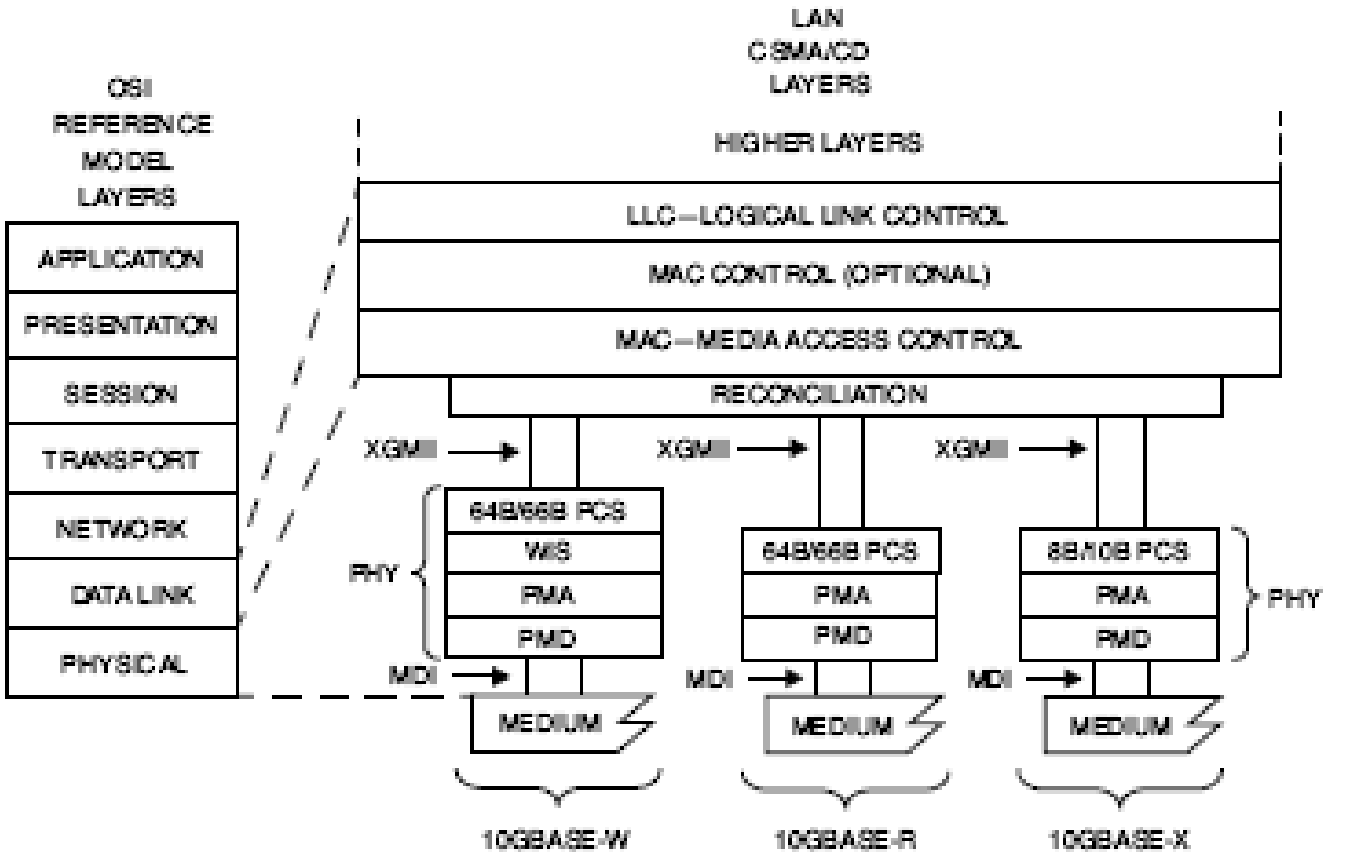
Female 15 pin D-Series connector with slide lock assembly.

10 Gigabit Ethernet

» A norma Ethernet a 10 Gbit/s especifica
  – Apenas o modo de funcionamento *full-duplex*
  – Apenas fibra óptica como meio de transmissão
    » A adopção de diferentes tipos de fibra permite atingir vários objectivos de alcance máximo, em ambientes de redes locais e metropolitanas

» A camada física é dividida em duas subcamadas – PMD (*Physical Media Dependent*) e PCS (*Physical Coding Sublayer*)
  – São suportados vários tipos de PMD
  – São especificadas várias interfaces LAN (10GBASE-R e 10GBASE-X) e WAN (10GBASE-W)

10 Gigabit Ethernet – arquitectura



MDI = MEDIUM DEPENDENT INTERFACE
PCS = PHYSICAL CODING SUBLAYER
PHY = PHYSICAL LAYER DEVICE
PMA = PHYSICAL MEDIUM ATTACHMENT
PMD = PHYSICAL MEDIUM DEPENDENT
WIS = WAN INTERFACE SUBLAYER
XGMII = 10 GIGABIT MEDIA INDEPENDENT INTERFACE

10 Gigabit Ethernet – camada física (PMD e PCS)

- Foram definidos 4 tipos de PMD
  - 850 nm Série
    - Fibra multimodo
  - 1310 nm WWDM (*Wide Wavelength Division Multiplexing*)
    - Fibra multimodo / monomodo
  - 1310 nm Série
    - Fibra monomodo
  - 1550 nm Série
    - Fibra monomodo
- WWDM é usado apenas em LANs (10GBASE-X), enquanto os três restantes tipos podem ser usados em interfaces LAN (10GBASE-R) ou WAN (10GBASE-W)
- A subcamada PCS inclui funções de codificação (8B/10B e 64B/66B), serialização ou multiplexagem e ainda WIS (*WAN Interface Sublayer*) para adaptação da trama MAC ao payload SONET/SDH em interfaces WAN (10GBASE-W)

10 Gigabit Ethernet – interfaces LAN

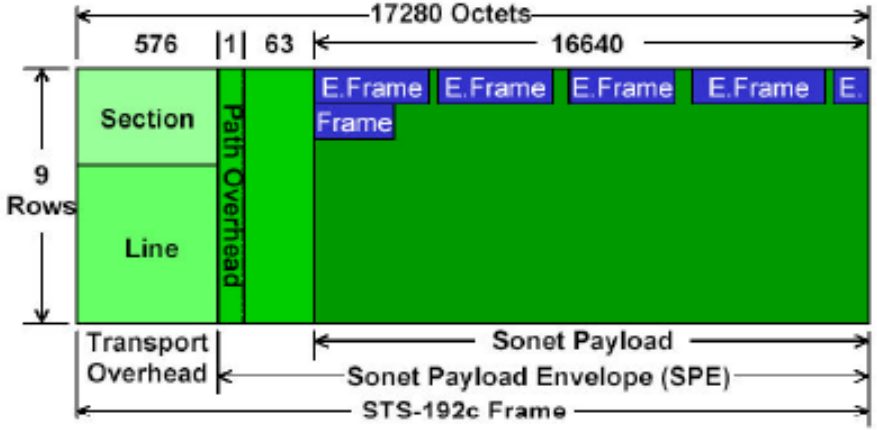
» 10GBASE-LX4
  – Interface WWDM (*Wide Wavelength Division Multiplexing*)
    » São usados 4 comprimentos de onda na janela de 1310 nm
    » Fibras multimodo (alcance 300 m) ou monomodo (alcance 10 km)
  – Código de linha 8B/10B
    » *Line rate* (*baud rate*): 4 * 3.125 Gbaud = 12.5 Gbaud
    » *MAC rate*: 8 / 10 * 12.5 = 10 Gbit/s

» 10GBASE-R
  – Interface série
    » 10GBASE-SR – janela 850 nm, fibra multimodo, alcance: 30 / 300 m
    » 10GBASE-LR – janela 1310 nm, fibra monomodo, alcance: 10 km
    » 10GBASE-ER – janela 1550 nm, fibra monomodo, alcance: 40 km
  – Código de linha 64B/66B
    » *Line rate* (*baud rate*): 10.3125 Gbaud
    » *MAC rate*: 64 / 66 * 10.3125 = 10 Gbit/s

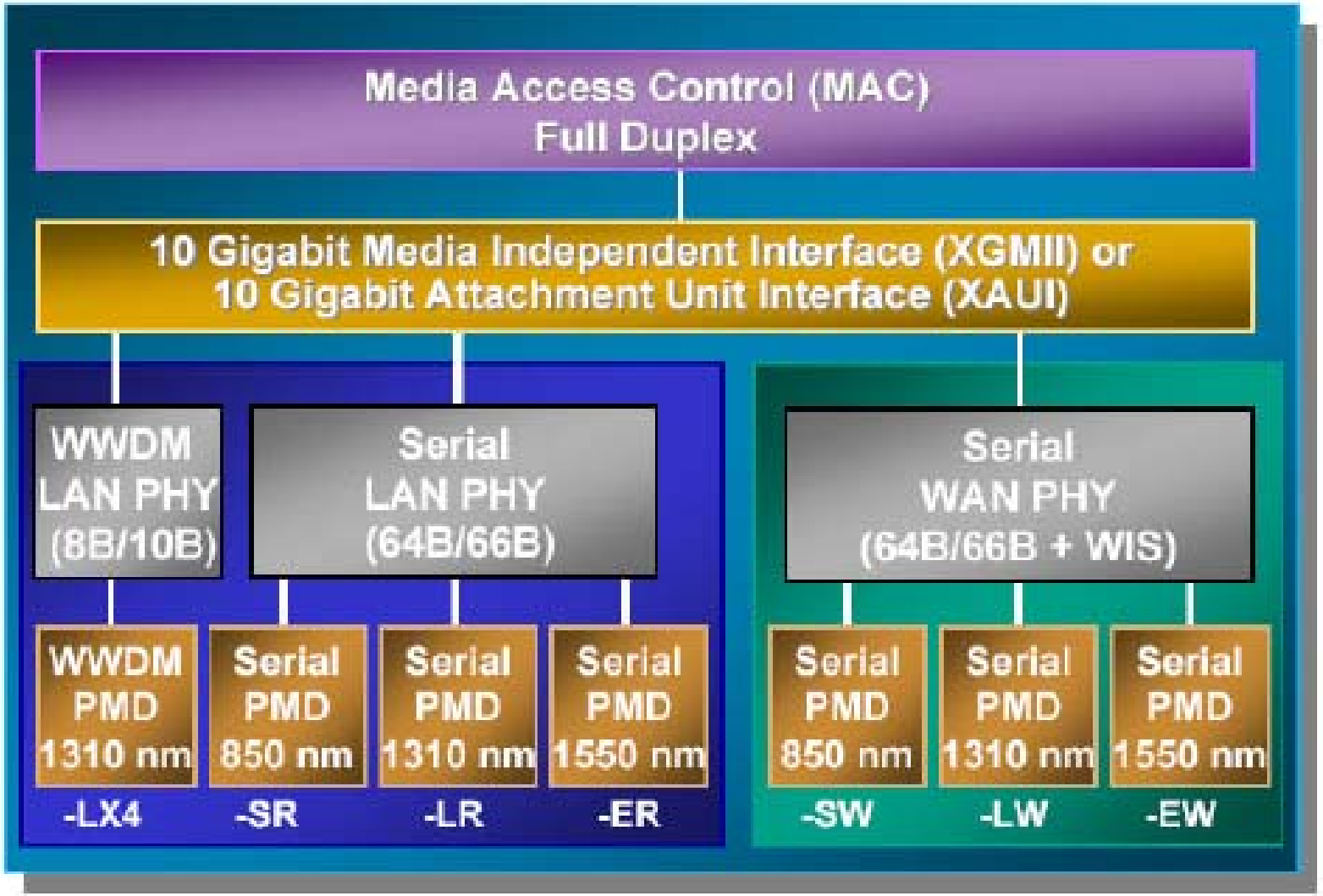
10 Gigabit Ethernet – interfaces WAN

» 10GBASE-W
  – Interface série
    » 10GBASE-SW, 10GBASE-LW, 10GBASE-EW (os mesmos PMDs que em 10GBASE-R)
  – A subcamada PCS inclui uma função de adaptação da trama MAC ao *payload* SONET/SDH (WIS – *WAN Interface Sublayer*)
    » *SONET Physical Rate*: 9.95328 Gbit/s
    » *SONET Payload Rate*: 26 / 27 * 9.95328 = 9.58464 Gbit/s
  – Código de linha 64B/66B
    » *MAC rate*: 64 / 66 * 9.58464 = 9.2942 Gbit/s

SONET STS-192c
SDH STM-64



10 Gigabit Ethernet – opções no nível físico



10 Gigabit Ethernet – opções no nível físico

Device	8B/10B PCS	64B/66B PCS	WIS	850nm Serial	1310nm WWDM	1310nm Serial	1550nm Serial
10GBASE-SR		✓		✓			
10GBASE-SW		✓	✓	✓			
10GBASE-LX4	✓				✓		
10GBASE-LR		✓				✓	
10GBASE-LW		✓	✓			✓	
10GBASE-ER		✓					✓
10GBASE-EW		✓	✓				✓

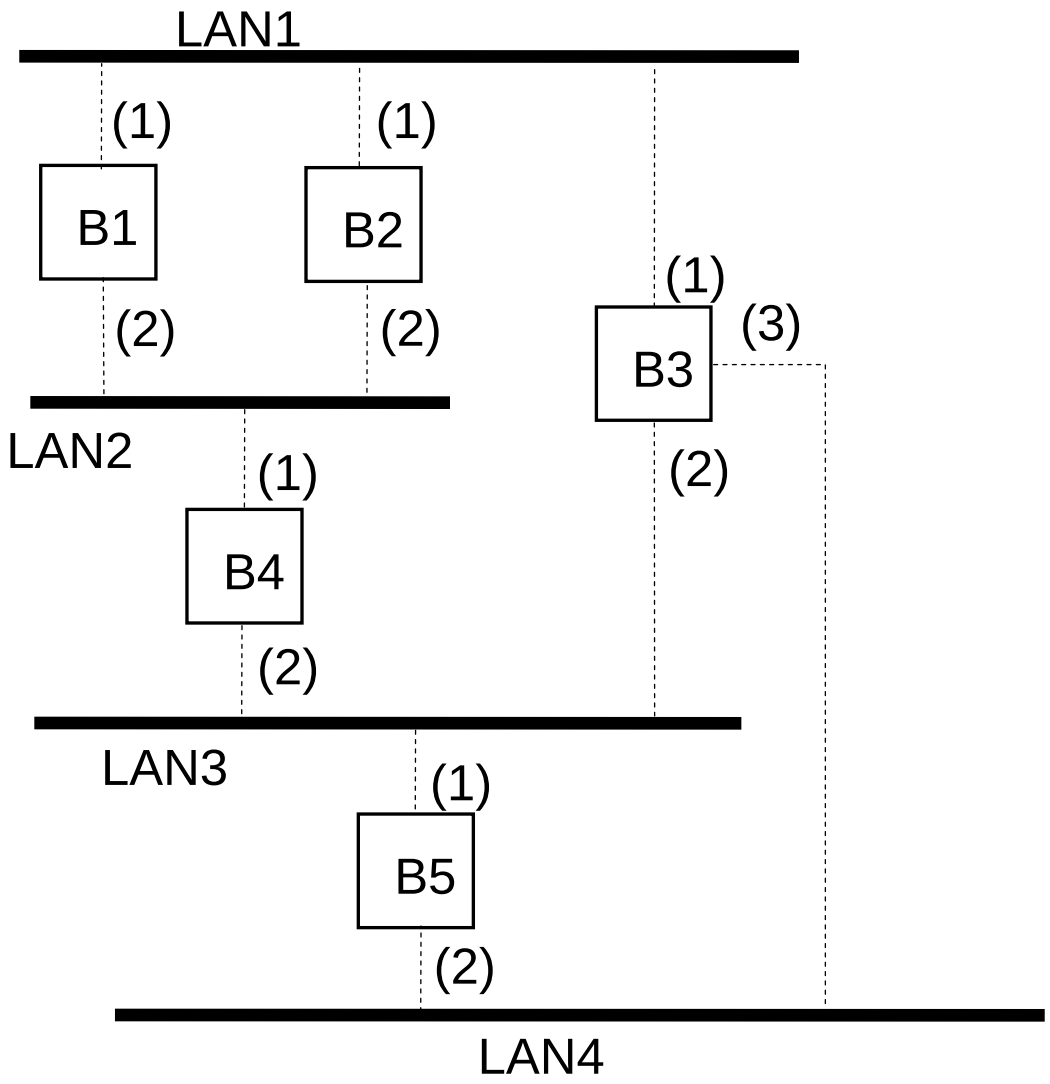
10GBASE-W **10GBASE-R**	PMD série 850 nm	PMD série 1310 nm	PMD série 1550 nm
Fibra	Multimodo 62 / 50 μm	Monomodo	Monomodo
Distância máxima	30 / 300 m	10 km	40 km

10GBASE-X	PMD WWDM 1310 nm
Fibra	Multimodo / Monomodo
Distância máxima	300 m / 10 km

Bridging – algoritmo spanning tree

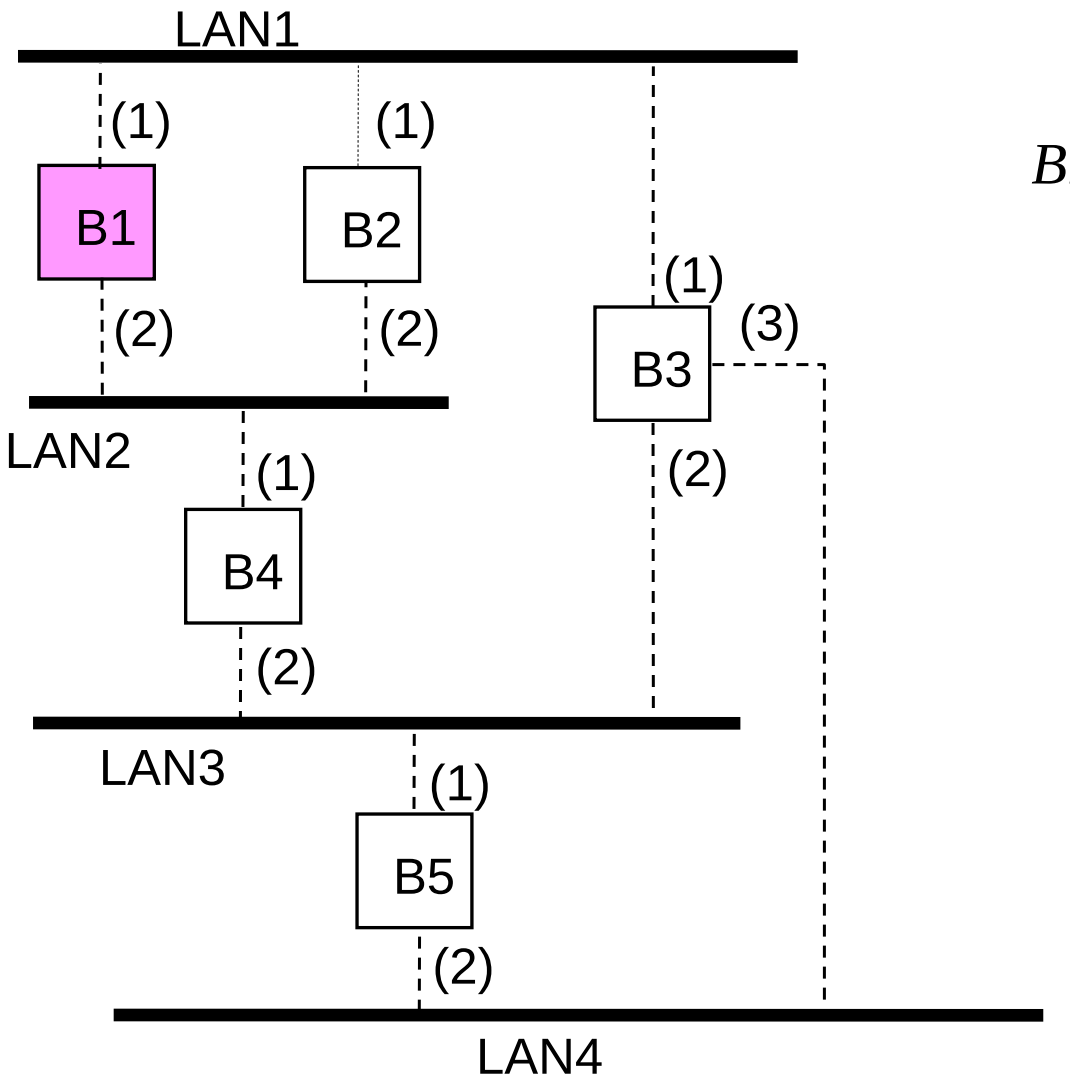
1. Seleccionar a *root bridge* entre todas as *bridges*
   - A *root bridge* é a *bridge* com o menor *bridge ID*
2. Determinar a *root port* para cada *bridge* (excepto a *root bridge*)
   - A *root port* é a porta com o percurso de menor custo para a *root bridge*
   - A *root bridge* não tem *root ports*
3. Seleccionar a *designated bridge* para cada LAN
   - A *designated bridge* é a *bridge* que oferece o percurso de menor custo da LAN para a *root bridge*
   - A *designated port* liga a LAN à *designated bridge*
   - Todas as portas da *root bridge* são *designated ports*
4. Todas as *root ports* e todas as *designated ports* são colocadas no estado *forwarding*
   - Estas são as únicas portas autorizadas a despachar tramas
   - As restantes portas são colocadas no estado *blocking*

Exemplo – topologia física



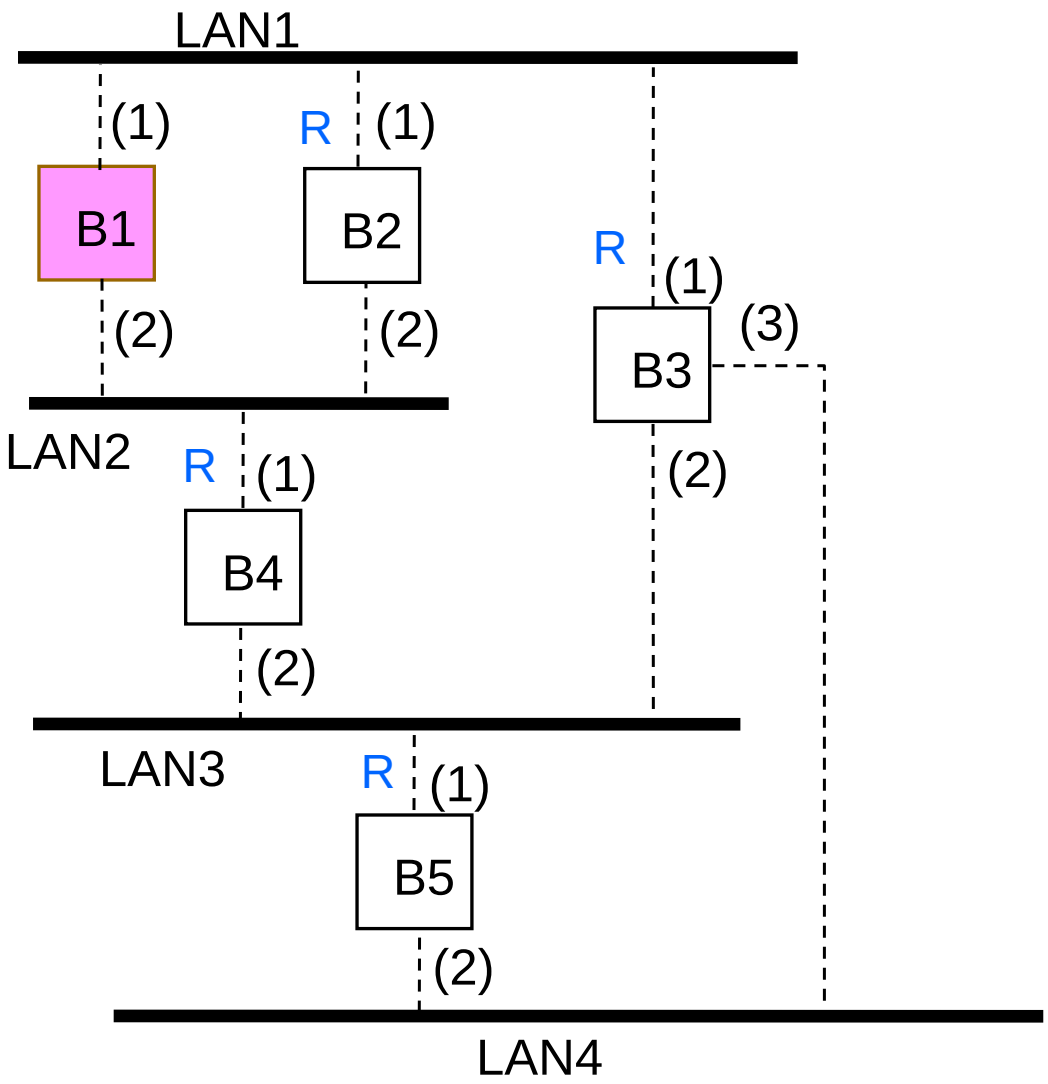
Assume-se que os custos associados às portas das *bridges* são iguais

Exemplo – passo 1



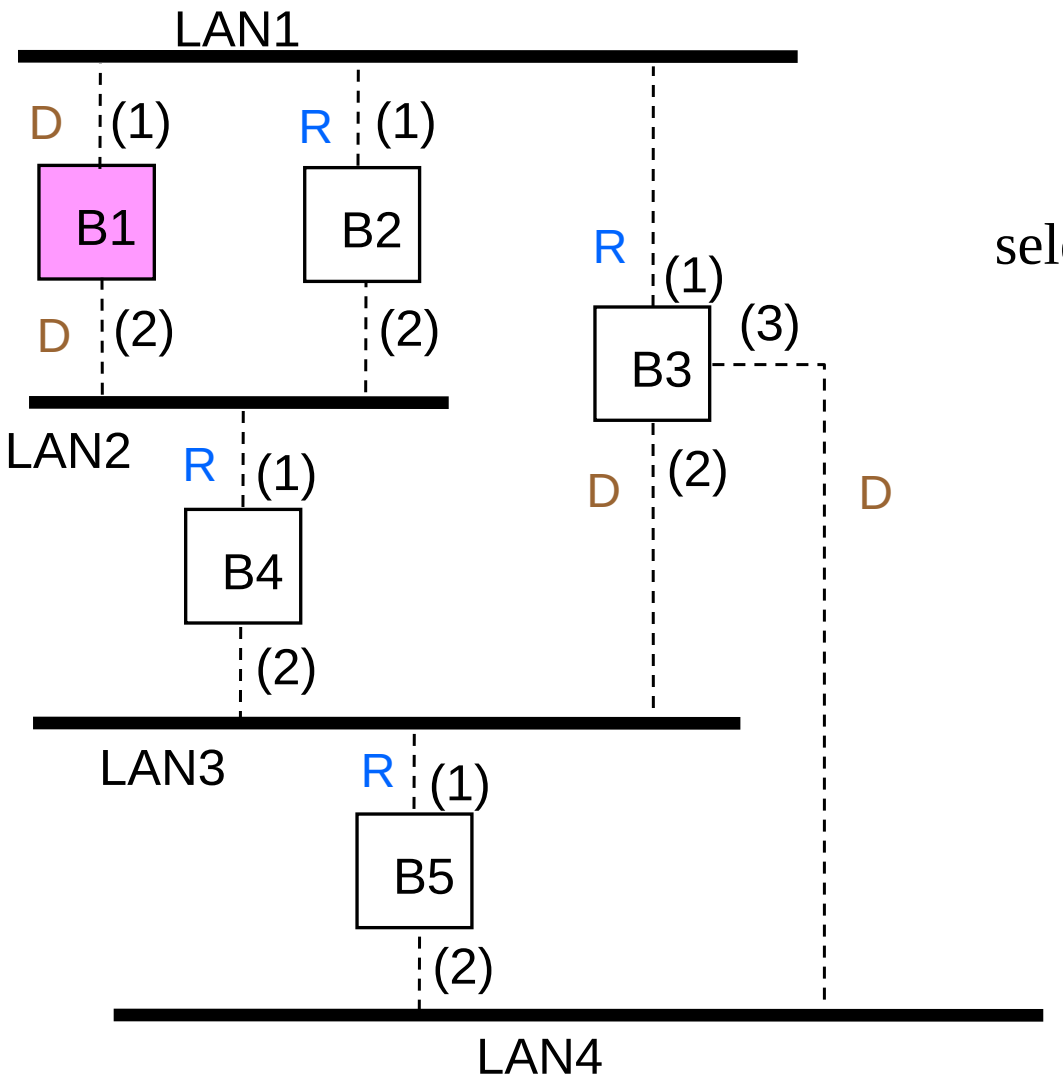
Bridge 1 seleccionada como *root bridge*

Exemplo – passo 2



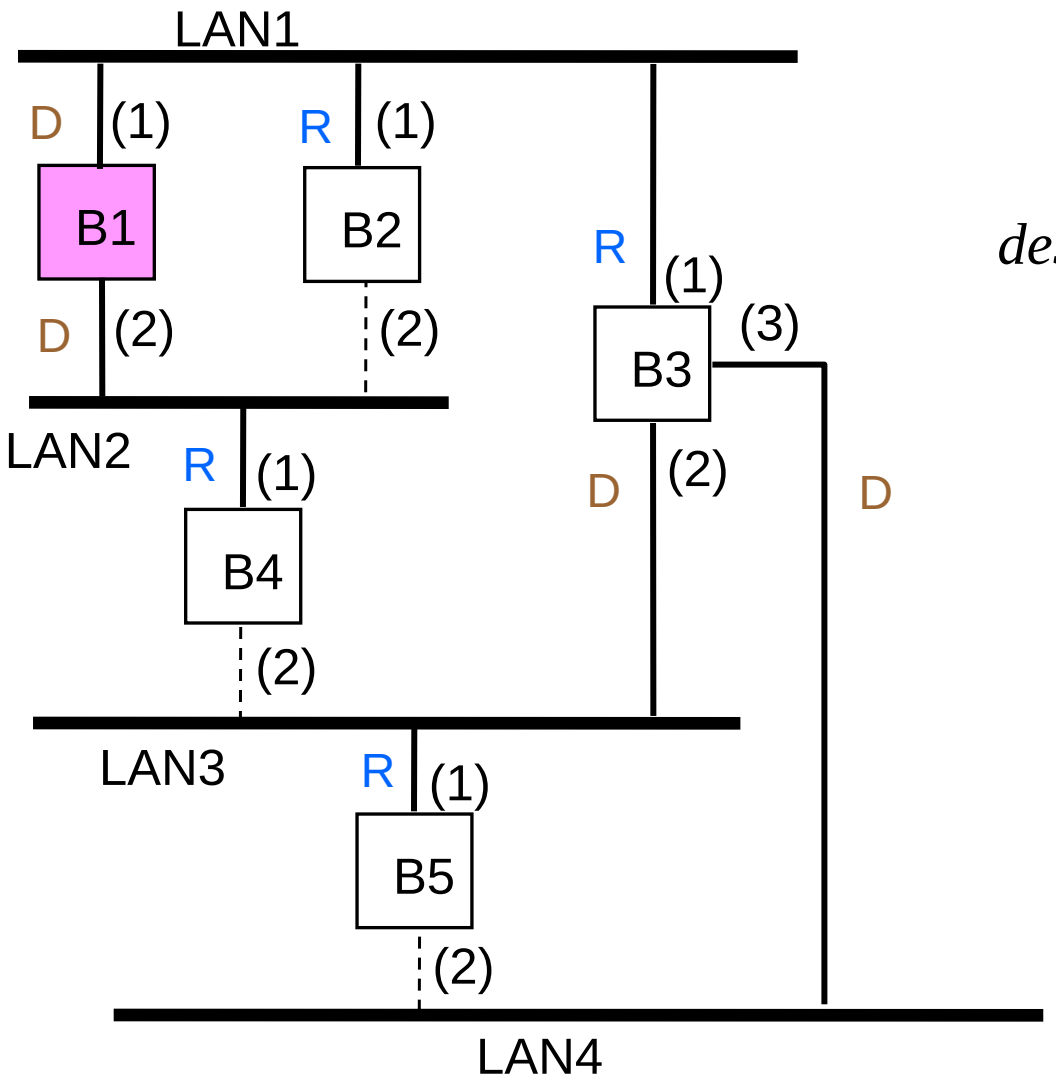
Root port seleccionada
para cada *bridge*
(excepto *root bridge*)

Exemplo – passo 3



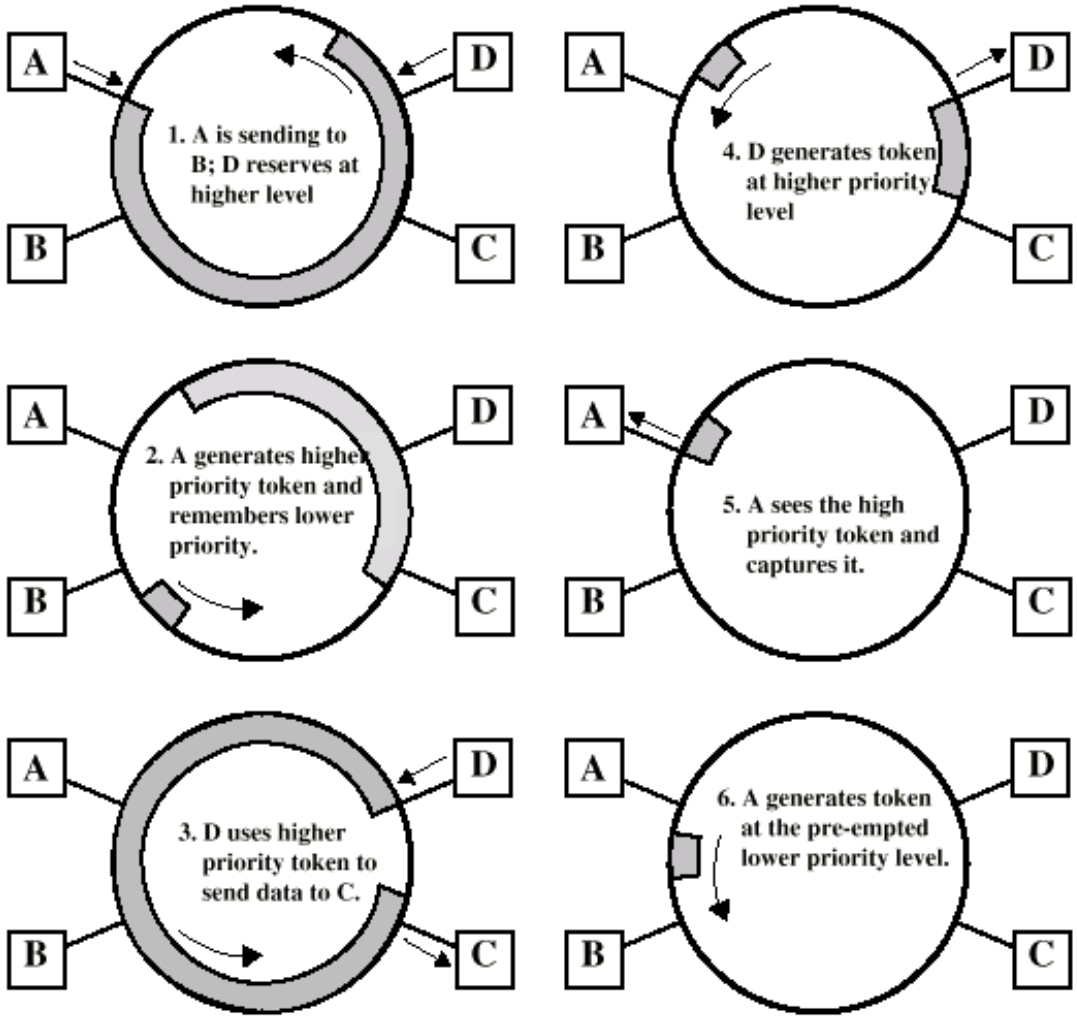
Designated bridge
seleccionada para cada LAN

Exemplo – passo 4



Todas as *root ports* e *designated ports* colocadas no estado *forwarding*

Token Ring – mecanismo de prioridades



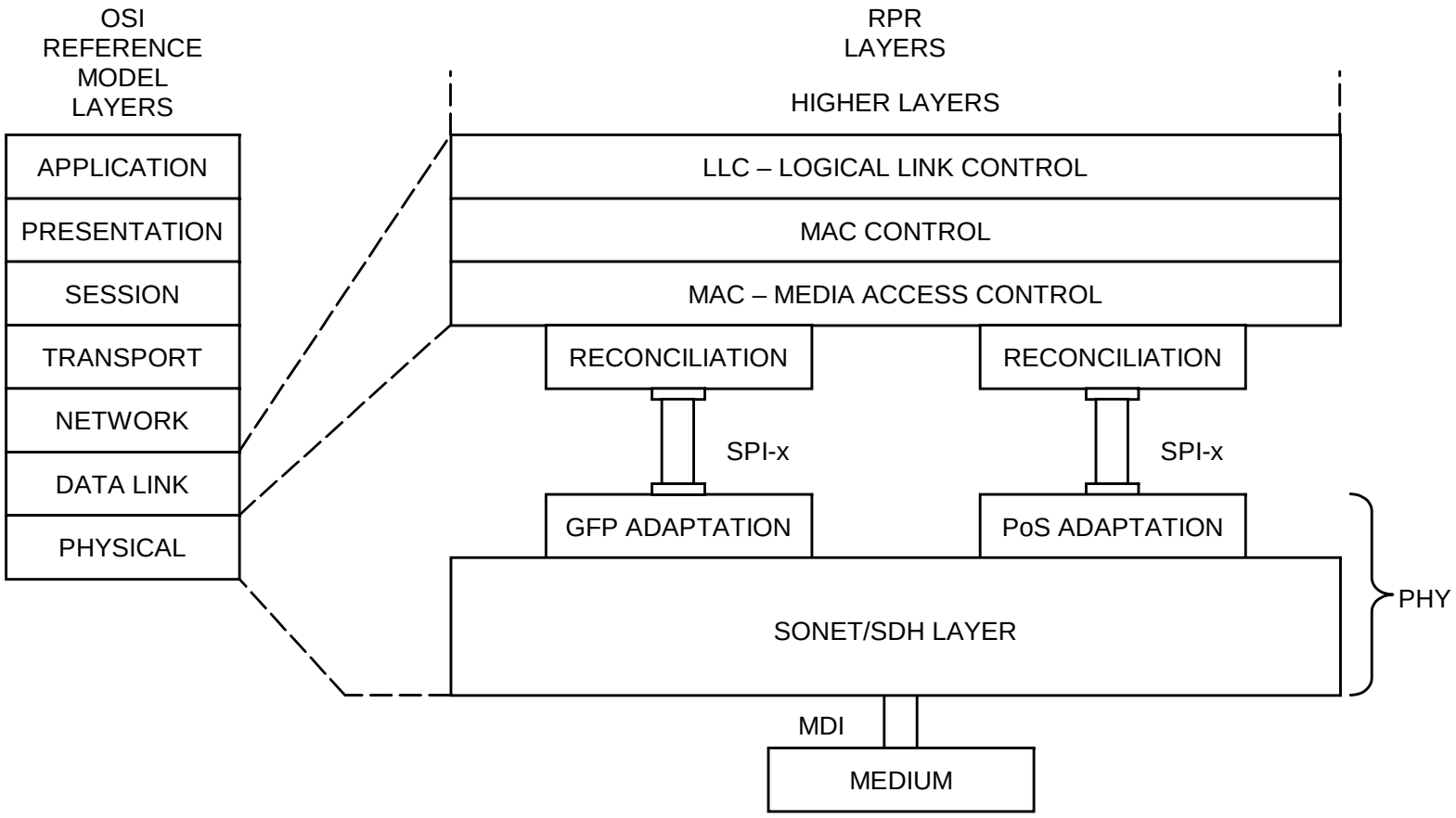
Resilient Packet Ring – características

- Tecnologia normalizada – IEEE 802.17
  - Especifica níveis físico e MAC para uso em LANs, MANs e WANs
- Tira partido da infraestrutura instalada de anéis SONET/SDH, embora possa ser usada com outras camadas físicas (GbE, 10GbE, WDM)
  - Beneficia dos mecanismos de protecção SONET/SDH (tempos de reconfiguração inferiores a 50 ms)
- Protocolo optimizado para tráfego de dados, o que permite eficiência muito superior à da reserva de circuitos TDM (SONET/SDH)
  - Capacidade do anel partilhada por tráfego dos utilizadores (pacotes)
    - Gestão dinâmica e distribuída da largura de banda (multiplexagem estatística / *oversubscription*)
  - Optimização da largura de banda – remoção pelo destino (*spatial reuse*)
  - *Fairness* (algoritmo distribuído)
  - Diferenciação de níveis de qualidade de serviço (prioridades)

Resilient Packet Ring – topologia

- Anel duplo – *dual counter rotating ring*
- Ambos os anéis transportam tráfego (ao contrário de FDDI ou de anéis SONET/SDH em que 50% da capacidade é reservada para protecção)
- Cada nó selecciona o anel que oferece o percurso mais curto para o destino
  - Os nós mantêm um mapa topológico da rede, sendo a topologia da rede descoberta com base em tráfego de controlo
  - O tráfego de controlo relativo ao tráfego de dados num anel é transportado no outro anel
    - Os pacotes de controlo são usados para descoberta da topologia, para protecção inteligente e controlo da largura de banda
- Esquemas de protecção (reconfiguração)
  - *Wrapping*
  - *Steering*

RPR – arquitectura sobre SONET/SDH

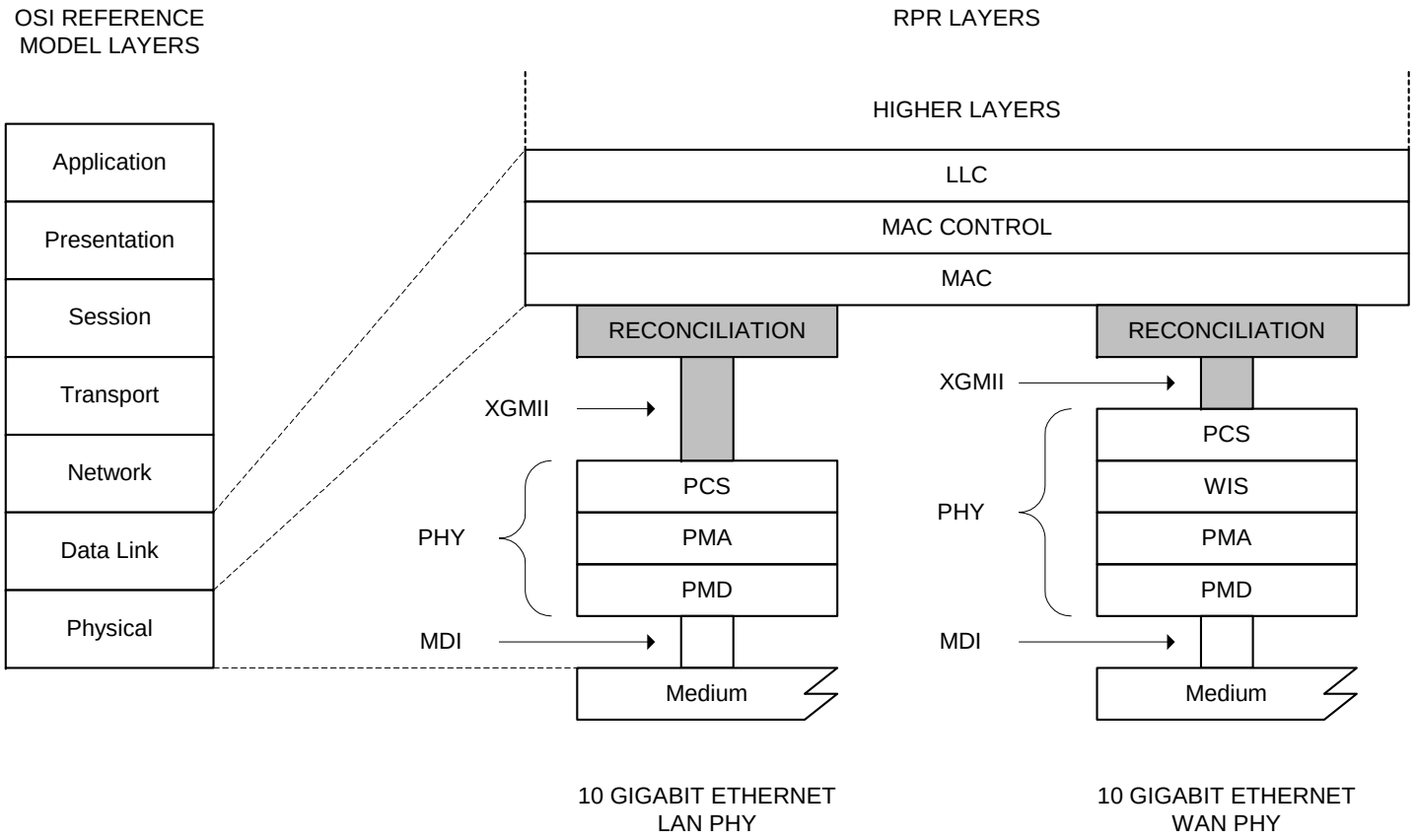


MDI – MEDIUM DEPENDENT INTERFACE

SPI – SYSTEM PACKET INTERFACE

GFP – GENERIC FRAMING PROTOCOL

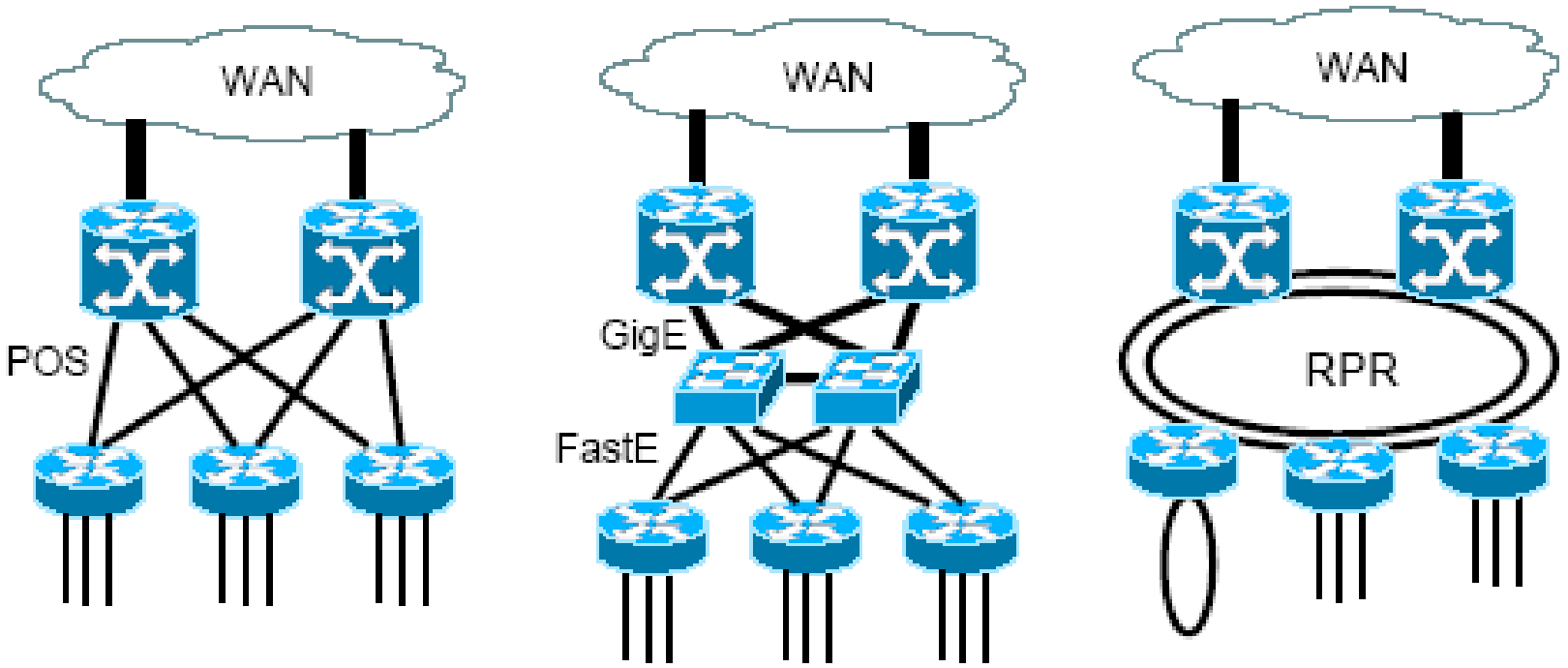
RPR – arquitectura sobre 10 Gigabit Ethernet



LLC = LOGICAL LINK CONTROL
MAC = MEDIA ACCESS CONTROL
MDI = MEDIUM DEPENDENT INTERFACE
PCS = PHYSICAL CODING SUBLAYER
PHY = PHYSICAL LAYER ENTITY

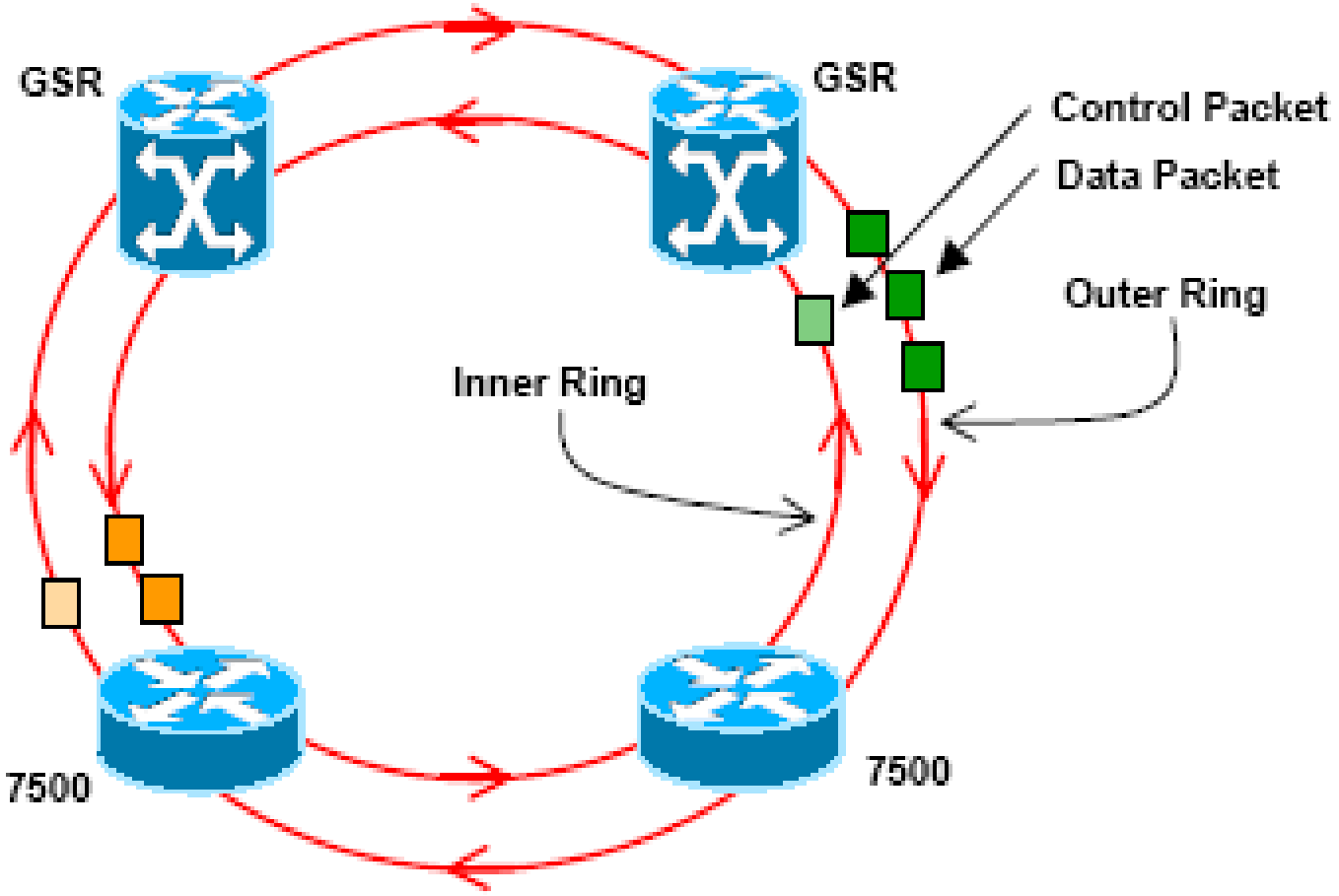
PMA = PHYSICAL MEDIUM ATTACHMENT
PMD = PHYSICAL MEDIUM DEPENDENT
WIS = WAN INTERFACE SUBLAYER
XGMII = 10 GIGABIT MEDIA INDEPENDENT INTERFACE

RPR – agregação de tráfego e alternativas

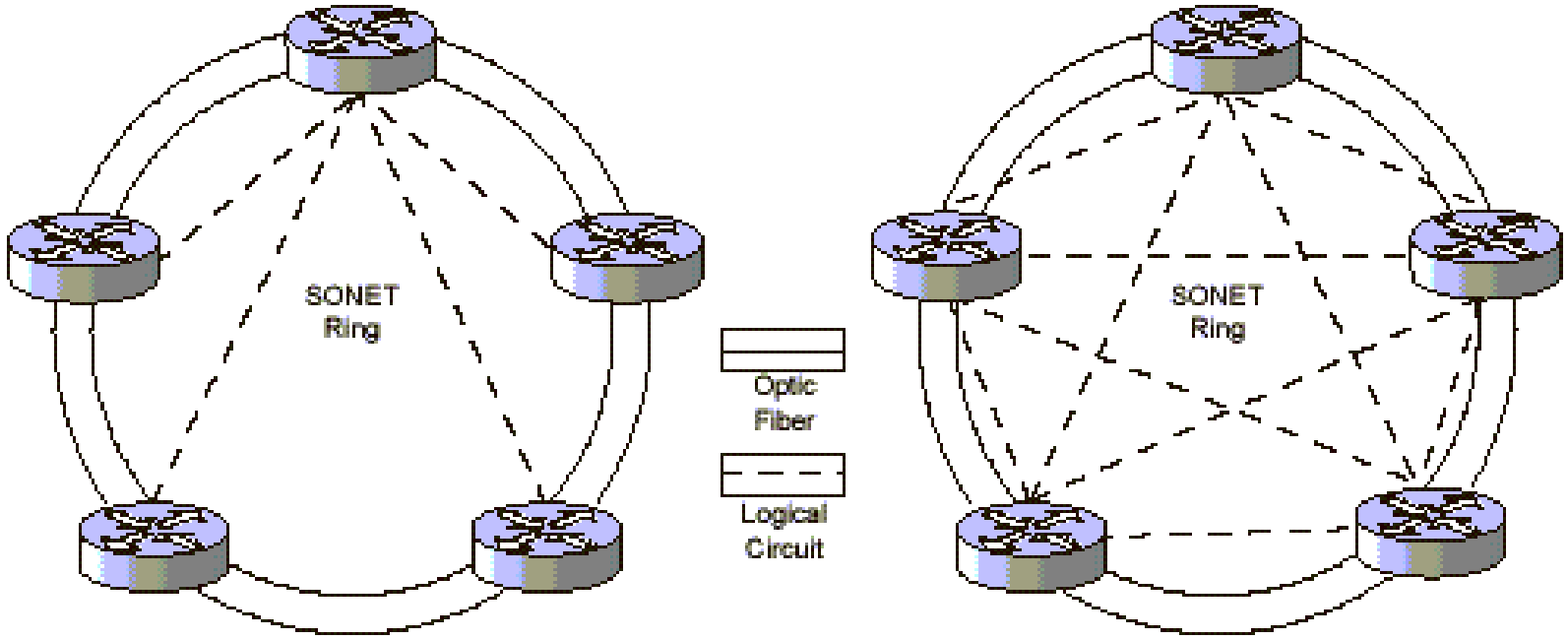


- Agregação directa (POS – *Packet over SONET*) – é necessário implementar políticas complexas nos *routers* de *backbone* e exige um número elevado de portas
- Comutação de nível 2 – os *routers* de *backbone* são menos complexos, mas aumenta o número de sistemas e o número total de portas
- RPR – a agregação não requer sistemas adicionais nem definição de políticas complexas

Anéis RPR – tráfego de dados e de controlo



Comparação de RPR com TDM em SONET/SDH



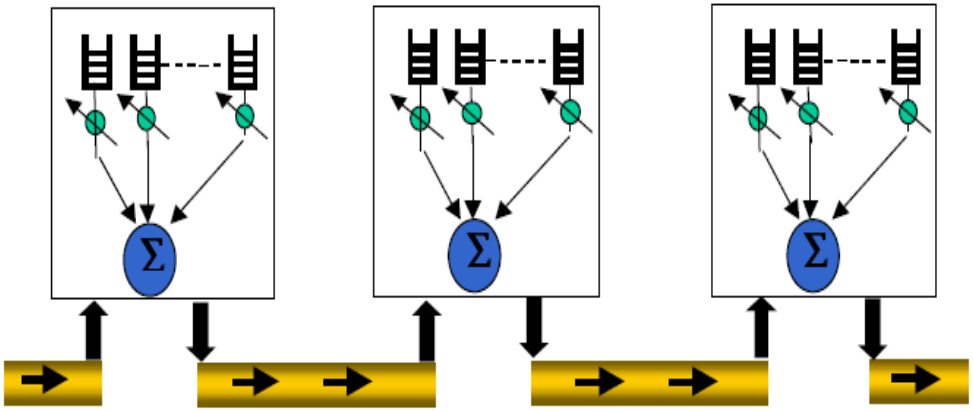
No exemplo com cinco nós

» Topologia lógica em estrela (*hub*), típica de redes de acesso – com TDM é necessário disponibilizar quatro circuitos ponto a ponto

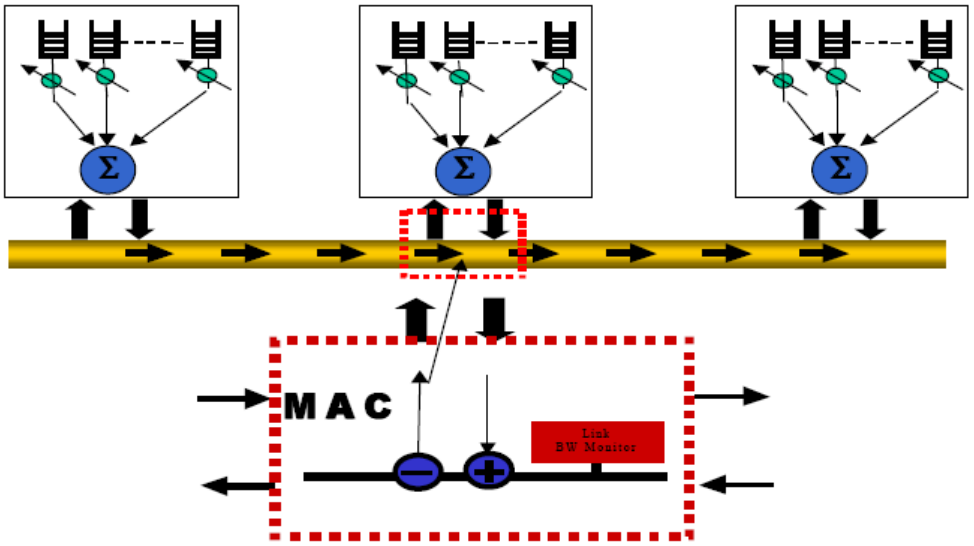
» Topologia lógica em malha (*mesh*), típica de redes de núcleo (*core*) – com TDM é necessário disponibilizar dez circuitos ponto a ponto

Comparação de RPR com Ethernet

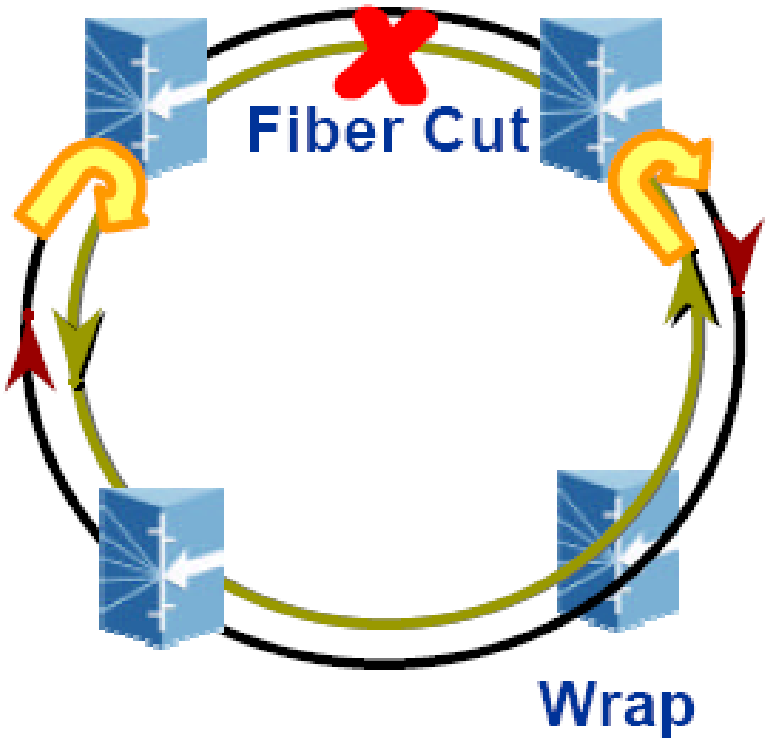
Ethernet – os nós são ligados por circuitos ponto-a-ponto; cada pacote é processado por cada nó no percurso entre a origem e o destino

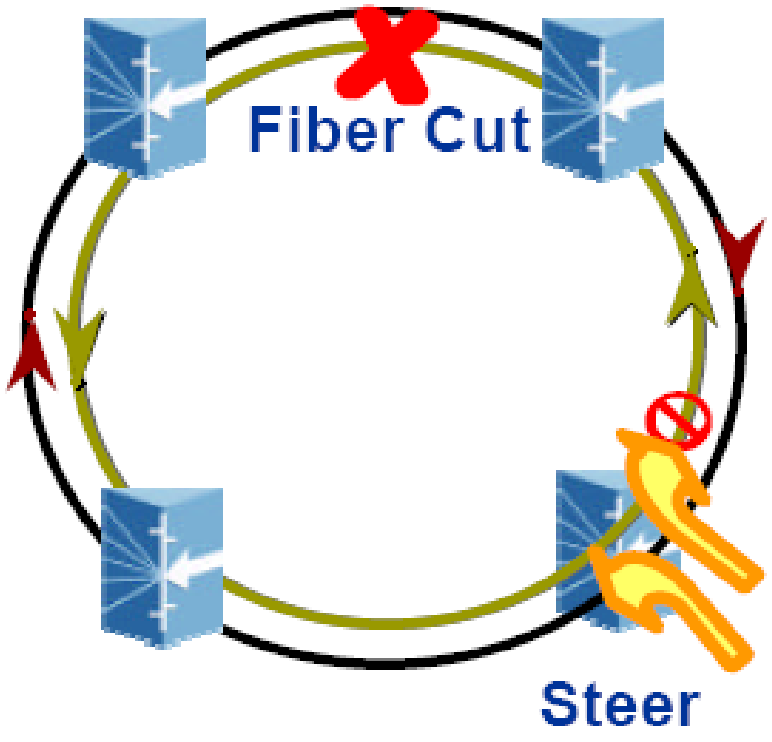


RPR – os nós funcionam como ADM (*add-drop multiplexers*) ligados a um meio partilhado; pacotes em trânsito não são processados nos nós intermédios



RPR – reconfiguração (wrapping e steering)





Encapsulamento baseado em LLC

- Encapsulamento de protocolos “encaminháveis” (*routed ISO protocols*)
  - Identificado por DSAP = SSAP = 0xFE
  - O primeiro octeto do campo de Dados é NLPID (*Network Layer Protocol Identifier*), administrado por ISO / ITU
    - NLPID é também usado em encapsulamento não baseado em LLC
  - Valores de NLPID
    - 0x00 *Null Network Layer* / *Inactive Set*
    - 0x08 ITU-T Q.933
    - 0x80 SNAP (*Subnetwork Access Protocol*)
      - Usado em encapsulamento não baseado em LLC quando o protocolo não tem NLPID associado
      - LLC suporta encapsulamento LLC/SNAP
    - 0x81 ISO CLNP
    - 0x82 ISO ES-IS
    - 0x83 ISO IS-IS
    - 0xCC IP
      - IP não é protocolo ISO mas tem NLPID associado
      - IP é normalmente encapsulado com base em LLC/SNAP (LANs, IP sobre ATM, LANE)
- Encapsulamento LLC/SNAP
  - Identificado por DSAP = SSAP = 0xAA

Encapsulamento LLC/SNAP

» O campo SNAP é constituído por cinco octetos
  – OUI *Organizationally Unique Identifier* (3 octetos)
  – PID *Protocol Identifier*, normalmente designado *Ether Type* (2 octetos)

» Tipos de encapsulamento
  – *Routed non ISO PDUs* OUI = 0x000000
  – *Bridged IEEE 802 PDUs* OUI = 0x0080C2

» *Routed non ISO PDUs – PID*
  – 0x0800 IPv4
  – 0x0806 ARP
  – 0x0807 XNS
  – 0x6003 DECnet
  – 0x8035 RARP
  – 0x809B AppleTalk
  – 0x8137 IPX
  – 0x86DD IPv6
  – 0x8847 MPLS

» *Bridged IEEE 802 PDUs – PID*
  – 0x0001/0007 IEEE 802.3
  – 0x0002/0008 IEEE 802.4
  – 0x0003/0009 IEEE 802.5
  – 0x0004/000A FDDI
  – 0x000E BPDUs