

Camada de Enlace de Dados

- ❑ O objetivo básico da camada de enlace de dados é permitir uma comunicação eficiente e confiável entre dois computadores adjacentes
- ❑ Estes computadores estão conectados fisicamente entre si através de um canal de comunicação
- ❑ Os protocolos que permitem a comunicação entre estes dois computadores são objetos de estudo na camada de enlace de dados

Camada de Enlace de Dados

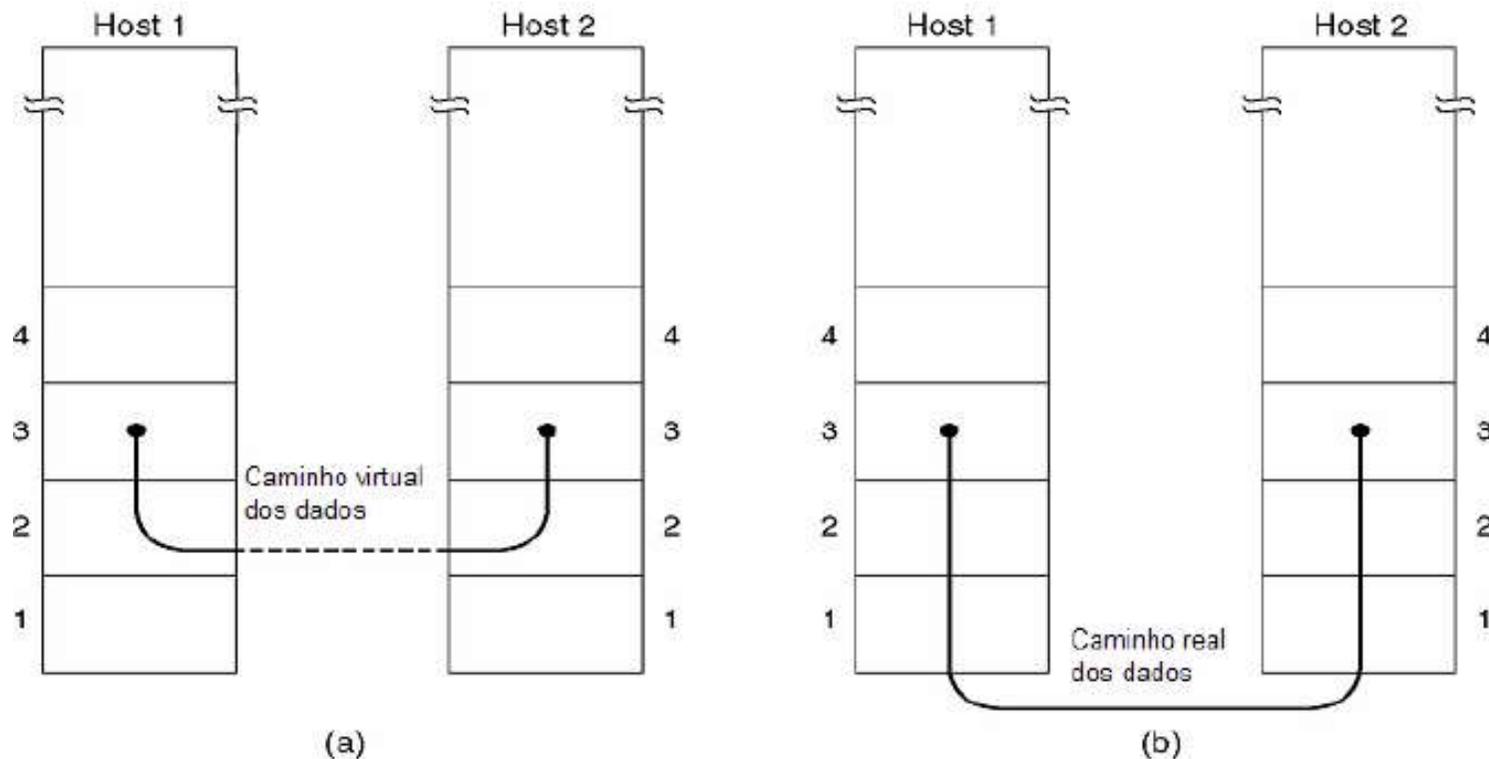
- Principais funções desta camada:
 - Permitir uma comunicação eficiente entre dois computadores adjacentes
 - Fornecer uma interface de serviço, bem definida, à camada de rede
 - Determinar como os bits da camada física serão agrupados em quadros (frames)
 - Permitir uma comunicação confiável, tratando os possíveis erros de transmissão
 - Realizar o controle de fluxo, impedindo que receptores lentos sejam “inundados” por transmissores rápidos
- Os protocolos desta camada devem ser responsáveis por implementar estas funções

Protocolos - Considerações

- Para projetar os protocolos da camada de enlace é necessário fazer algumas considerações:
 - O canal de comunicação (meio físico) produz erros ocasionais
 - O canal de comunicação possui uma taxa de dados finita (capacidade do canal)
 - Existe um retardo de propagação diferente de zero entre o momento em que o bit é enviado e o momento em que ele é recebido.
 - Os bits são transmitidos na ordem exata em que são enviados

Serviços oferecidos

- O principal serviço oferecido à camada de rede é a transferência de dados entre as camadas de rede de origem e destino



(a) Comunicação Virtual

(b) Comunicação Real

Serviços oferecidos

- ❑ Na camada de rede da máquina de origem há uma entidade (um processo) que envia alguns bits à camada de enlace para serem transmitidos à entidade no destino
- ❑ A camada de enlace, por sua vez, prepara estes bits e os envia para a camada física, que será responsável, pela transmissão. No receptor ocorre o processo inverso.
- ❑ O protocolo considera que uma entidade da camada de enlace da origem se comunica com outra entidade da camada de enlace do destino.
- ❑ Entre os serviços oferecidos por esta camada temos:
 - Serviço sem conexão e sem confirmação
 - Serviço sem conexão e com confirmação
 - Serviço orientado à conexão

Sem conexão não confirmado

- ❑ Conexão não é estabelecida entre as entidades
- ❑ Quadros independentes são enviados da origem para o destino que não envia nenhuma confirmação de volta
- ❑ Quadros perdidos são ignorados e tratados pelas camadas superiores
- ❑ Classe de serviço apropriada para Baixa taxa de erro
- ❑ Serviço normalmente usado em LANs.

Sem conexão confirmado

- ❑ Conexão não é estabelecida a priori
- ❑ Quadros enviados pela origem são confirmados pelo destino
- ❑ Origem usa um mecanismo de temporização para reenviar quadros não confirmados
- ❑ Serviço apropriado para canais não confiáveis como comunicação sem fio

Serviço com conexão confirmado

- ❑ Serviço mais sofisticado
- ❑ Serviço possui três fases distintas:
 - Estabelecimento de Conexão - Os dois lados inicializam variáveis e contadores.
 - Transferência de dados – Ocorre a transmissão dos quadros
 - Finalização de conexão – Liberação de buffers, variáveis e outros recursos necessários à conexão.
- ❑ Quadros são numerados e a camada de enlace garante o recebimento de todos os quadros de forma ordenada.
- ❑ Cada quadro enviado é individualmente confirmado
- ❑ Caso não seja confirmado dentro de um intervalo de tempo específico o transmissor pode reenviar o quadro.
- ❑ Este serviço fornece à camada de rede um fluxo de bits confiável.

Enquadramento(Framing)

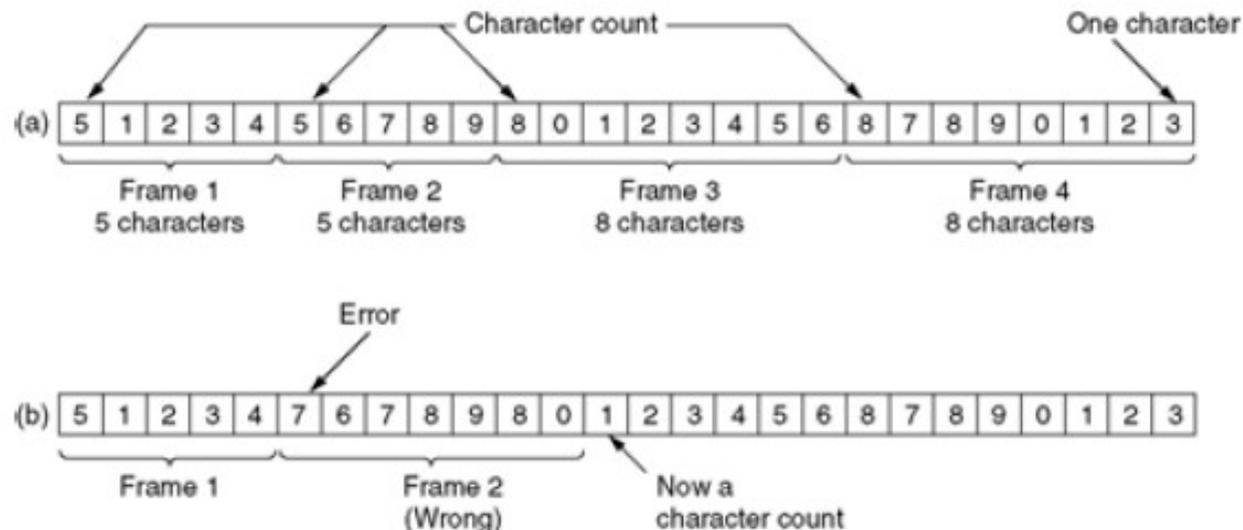
- Problema a ser resolvido:
 - Como agrupar seqüências de bits em quadros para que possam ser processados como unidades de informação?
- Ou
 - Como fazer delimitação de quadros?

Enquadramento - Soluções

- Inserir intervalos de tempo entre transmissões de quadro
- Realizar a contagem de caracteres
 - Em comunicação assíncrona não é viável fazer contagem de caracteres
- Inserir flags (seqüências especiais de bits) de início e fim de quadro com preenchimento (stuffing) de caracteres
- Inserir flags de início e fim de quadro com preenchimento de bits
- Usar violações de código da camada física

Contagem de caracteres

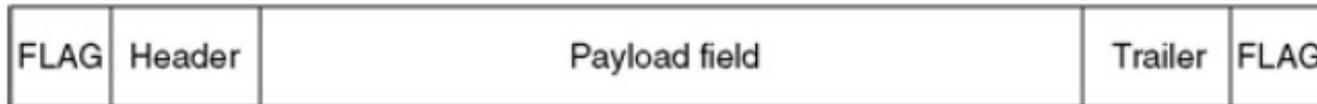
- ❑ Usa-se um campo no cabeçalho para especificar o número de caracteres no quadro
- ❑ Problema: erro nesse campo faz com que o receptor perca a sincronização
- ❑ Não é usado na prática para protocolos da camada de enlace



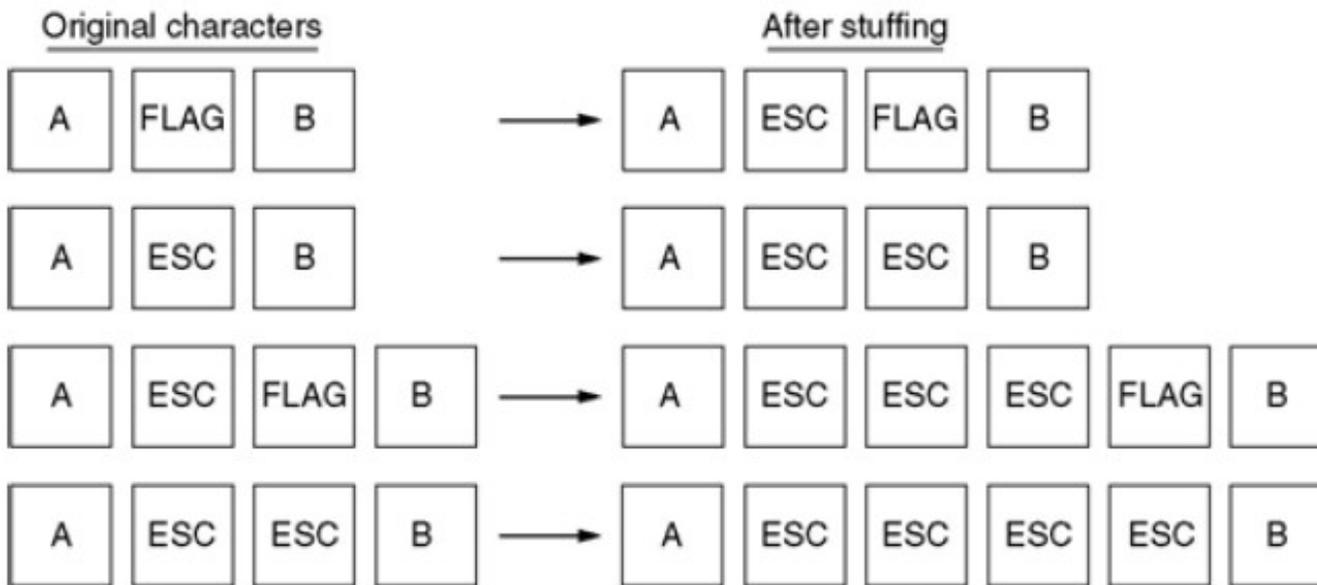
Inserção de Caracteres

- ❑ Quadro é delimitado por caracteres especiais (**FLAG**) que indica o início e o final do mesmo
- ❑ A ocorrência de um caractere **FLAG** no meio da mensagem provoca a inserção de um caractere **ESC**.
- ❑ **Desta forma o caractere FLAG, que é parte da mensagem (payload) não será confundido com um final de quadro**
- ❑ O mesmo processo acontece caso existe uma caractere **ESC** no meio da transmissão. Um novo caractere **ESC** é inserido.
- ❑ No receptor ocorre o processo inverso e caracteres **FLAG** e **ESC** que **foram inseridos pelo transmissor são removidos e a mensagem original é recuperada**
- ❑ Método usado em protocolos orientados a caracteres
- ❑ Neste caso pode-se determinar o próximo (início ou fim) e o destino nunca perde os limites dos outros quadros (frames)

Inserção de Caracteres



(a)



(b)

Inserção de bits

- ❑ Semelhante à inserção de caracteres, neste caso um flag (**01111110**) de bits é colocado no início e no final de cada
- ❑ O flag é utilizado para realizar o enquadramento.
- ❑ Durante a montagem dos quadros, sempre que o transmissor encontra 5 bits de valor **1**, **consecutivos**, um bit **0**, é inserido (bit stuffing) nos dados a serem enviados.
- ❑ Desta forma o padrão de bits do flag não se repete dentro dos dados e somente irá aparecer no final do quadro.
- ❑ O receptor deverá fazer o processo inverso e sempre que bits de valor 1 forem encontrados o próximo bit, que foi inserido no receptor deverá ser removido.

Inserção de bits - Exemplo

a) Dados Originais

011011111111111111110010

b) Dados enviados pelo meio físico

01111110 01101111 011111 011111 010010 01111110

Flag
(Início do quadro)

bits inseridos

Flag
(Final do quadro)

c) Dados recebidos após remoção dos bits inseridos e dos flags

011011111111111111110010

Controle de Erros

- ❑ A camada de enlace deve permitir uma comunicação eficiente e confiável entre dois computadores adjacentes
- ❑ Uma série de fatos podem levar a erros durante a transmissão pelo meio físico. Entre estes podemos citar: Ruídos; Atenuação; Ecos
- ❑ Os erros causados podem danificar um quadro. Neste caso o quadro é recebido, porém a informação do mesmo está incorreta.
- ❑ Os erros podem levar a uma perda completa do quadro devido a uma rajada de bits (ruído)
- ❑ A forma como o controle de erros é efetuado depende do tipo de serviço oferecido pela camada.

Controle de Erros

□ QUADROS PERDIDOS

- Utilização de um retorno (feedback) para o transmissor.
- Este retorno pode ser feito através de QUADROS DE CONTROLE especiais que indicam uma confirmação positiva (ACK) ou negativa (NACK) de recebimento entre as entidades parceiras
- As informações de controle permitem a comunicação sobre o estado da transmissão entre os parceiros.

□ QUADROS DANIFICADOS

- Utiliza-se códigos para DETECÇÃO DE ERROS;
- Podem também ser utilizados códigos para CORREÇÃO DE ERROS.
- A detecção e correção de erros é baseada na redundância, ou seja, bits adicionais devem ser anexados ao quadro.

Quadros Perdidos

- ❑ No caso de quadros perdidos, o transmissor ficará a confirmação positiva (ACK) ou negativa (NACK) e enquanto esta não chega o mesmo ficará suspenso!
- ❑ Neste caso uma solução é o uso de TIMERS (TEMPORIZADORES).
- ❑ Se a confirmação não for recebido em um tempo pré-determinado um novo quadro será enviado.
- ❑ Após o envio do quadros os temporizadores iniciam sua contagem. O mesmo é ajustado para aguardar um período de tempo (t).
- ❑ Este período deve ser necessário para que o quadro chegue ao destino, seja processado e a confirmação seja enviada.
- ❑ Se a confirmação é recebida antes do tempo (t) o timer é cancelado.
- ❑ Caso a confirmação não seja recebida, após o tempo ajustado do temporizador (t) o mesmo será disparado e um novo quadro deverá ser enviado ao receptor.
- ❑ Esta técnica pode gerar o envio de QUADROS DUPLICADOS ao receptor.
- ❑ Par resolver este problema são acrescentados NÚMERO DE SEQUÊNCIA aos quadros

Quadros Danificados

- ❑ Um quadro é danificado quando alguns de seus bits estão incorretos.
- ❑ Na DETECÇÃO DE ERRO é possível apenas identificar o erro.
- ❑ Neste caso o receptor poderia enviar uma confirmação negativa (NACK), solicitando o reenvio do quadro.
- ❑ Na CORREÇÃO DE ERRO o receptor pode identificar o erro e além disso corrigi-lo.
- ❑ Em ambos os casos são utilizadas técnicas e algoritmos para tal fim.
- ❑ Estas técnicas se baseiam na REDUNDÂNCIA, ou seja, bits são adicionados no quadro. Estes bits serão utilizados pelos algoritmos.
- ❑ Quando maior a REDUNDÂNCIA maior a possibilidade de correção.

Quadros Danificados

- ❑ Um tipo de erro que acontece na prática é o erro em rajada (burst). Neste caso uma série de bits são corrompidos em seqüência.
- ❑ Ruídos; ecos; interferências; etc. são as causas principais dos erros em rajadas.
- ❑ Dependendo do nível da rajada o erro o quadro pode inclusive ser completamente danificado.
- ❑ As técnicas para detecção e correção de erros são projetadas a fim de lidar com erros em rajadas.

Controle de Erros

- ❑ Como o controle de erros é baseado em redundância é necessário acrescentar bits a palavra de dados (quadro) que será enviado.
- ❑ Um quadro possui m bits de dados (palavra de dados – **data word**)
- ❑ Acrescenta-se ao quadro r bits adicionais que serão utilizados no controle de erros
- ❑ A seqüência de bits a ser transmitida possui então um tamanho n ($n = m + r$).
- ❑ Esta seqüência é conhecida como palavra código (**code word**)
- ❑ Se o número r de bits redundantes for suficientemente grande além da CORREÇÃO é possível também a DETECÇÃO de erros

Quadros Danificados

- ❑ Para lidar com quadros danificados por erros a camada de enlace possui algoritmos para controle de erros
- ❑ DETECÇÃO DE ERRO
 - BIT DE PARIDADE
 - CRC – Cyclic Redundance Code (Código de Redundância Cíclica)
- ❑ CORREÇÃO DE ERRO
 - Código de Hamming

Bit de Paridade

- ❑ Consiste em **acrescentar à palavra de dados um bit** adicional
- ❑ Caso o número de bits 1 seja ímpar o bit de paridade é igual a 1. E caso seja par o bit de paridade será 0.

Palavra de dados	01	11
Palavra código	01 1	11 0

- ❑ O bit de paridade não é utilizado na camada de enlace, mas este método simples, indica como é a filosofia para detecção e correção de erros através da **redundância**.

Cyclic Redundancy Code

- ❑ CRC é um método baseado na adição de bits de check a uma primitiva
- ❑ Os bits adicionados garantem que na ausência de erros de comunicação, a primitiva mais os bits de check são **divisíveis** por um dado fator
- ❑ O método específico de divisão e o fator usado determinam o quais de erros de transmissão que podem ser detectados
- ❑ Uma sequência de 'n' bits pode ser interpretado como um polinômio de grau 'n-1':

$$\sum_{i=0}^{N-1} b_i \cdot x^i$$

- ❑ onde:
 - b_i : coeficiente do bit na posição i
 - x_i : presente indica bit valor 1

Exemplo

- Por exemplo, a sequencia 10011 define o polinômio: $x^4 + x + 1$
- Relembremos as operações binárias:
 - $0 + 0 = 0 - 0 = 0$
 - $0 + 1 = 0 - 1 = 1$
 - $1 + 0 = 1 - 0 = 1$
 - $1 + 1 = 1 - 1 = 0$
- Não há “transporte” de bit na adição e nem “empréstimo” na subtração
- Para todo ‘i’, $x^i + x^i = 0$
- Para multiplicar dois códigos, basta multiplicar os polinômios

Exemplo de Multiplicações

- Considere a primitiva com 3 bits abaixo. A coluna código indica os bits que serão enviados.

Primitiva	Polinômio	Fator	Produz	Código
0 0 0	0	$x+1$	0	0 0 0 0
0 0 1	1	$x+1$	$x+1$	0 0 1 1
0 1 0	x	$x+1$	x^2+x	0 1 1 0
0 1 1	$x+1$	$x+1$	x^2+1	0 1 0 1
1 0 0	x^2	$x+1$	x^3+x^2	1 1 0 0
1 0 1	x^2+1	$x+1$	x^3+x^2+x+1	1 1 1 1
1 1 0	x^2+x	$x+1$	x^3+x	1 0 1 0
1 1 1	x^2+x+1		$x+1$ x^3+1	1 0 0 1

Exercício

- Calcular o polinômio:
- Primitiva= (1 0 0 1 1) Fator= (1 1 0 0)
- $(x^4 + x + 1) \times (x^3 + x^2) = x^7 + x^6 + x^4 + x^2$
- Este mecanismo pode facilmente ser utilizado para definir o código

CRC

- ❑ Polinômios podem ser objetos de todas as operações aritméticas.
- ❑ Como a primitiva é multiplicada por um fator para criar o código a ser transmitido, então no destino deve-se aplicar o processo inverso, ou seja, usar o fator como divisor.

CRC

- ❑ Considere-se o polinômio $x^7 + x^6 + x^4 + x^3 + x^2$ quando dividido pelo fator $x^5 + x^2 + 1$ resultará x
- ❑ Para fazer o polinômio divisível pelo fator basta subtrair o resto dele
- ❑ Neste caso, o receptor será capaz de detectar o erro mas não será capaz de recuperar a primitiva a partir do código recebido.
- ❑ Então o mais indicado é usar o resto como um checksum, onde o resto da divisão será enviado como verificação.

Soma de Verificação (checksum)

- ❑ Para se calcular o o *checksum* de um quadro com m bits, transforma-se a palavra de dados (quadro) no polinômio $M(x)$
- ❑ Defina r como sendo o grau de $G(x)$. Acrescente r bits zero à extremidade de baixa ordem (direita) do quadro, de modo que ele passe a conter $m+r$ bits e que corresponda ao polinômio $N(x)$
- ❑ Isto equivale a uma multiplicação de $M(x)$ por um polinômio x^r
- ❑ Faça a divisão polinomial de $N(x) / G(x)$
- ❑ Subtraia o resto $[R(x)]$ de $N(x)$. O resultado será chamado
- ❑ $T(x)$ que deverá ser enviado
- ❑ $T(x) = N(x) - R(x)$ (subtração em módulo 2)

Soma de Verificação (checksum)

- Na recepção podem ocorrer duas situações:
 - A. Caso chegue o polinômio – $T(x)$:
 - Ao dividir $T(x) / G(x)$ no receptor o resto é zero.
 - Neste caso não houve erro de transmissão
 - B. Caso chegue o polinômio – $T(x) + E(x)$
 - Ao dividir $[T(x) + E(x)]/G(x)$ o resto é diferente de zero
 - Neste caso houve erro de transmissão.

Checksum – Exemplo

- Quadro: 1101011011 ($x^9+x^8+x^6+x^4+x^3+x+1$) □ $M(x)$
- Gerador: 10011 (x^4+x+1) □ $G(x)$
- 1. Grau do polinômio gerador(r) = 4
- 2. Mensagem a ser transmitida $N(x)=1101011011$ **0000**
- 3. $N(x) = x^{13}+x^{12}+x^{10}+x^8+x^7+x^5+x^4$
- 4. $x^{13}+x^{12}+x^{10}+x^8+x^7+x^5+x^4 \begin{array}{l} \underline{\phantom{x^{13}+x^{12}+x^{10}+x^8+x^7+x^5+x^4} x^4+x+1} \end{array}$
- 5. $x^3 - 3x^2 + x$ $x^9+x^8-2x^5+x^3+2x^2$
- 6. Neste caso o resto é o polinômio $r(x)=1110$
- 7. Subtração de $N(x) - R(x)$: 11010110111110
- 8. Mensagem a ser transmitida $T(x) = 1101011011$ **1110**

Polinômios Geradores

- ❑ Projetar polinômios geradores para detectar a maior classe possível de erros de comunicação não é uma tarefa fácil.
- ❑ Além disso, em sistemas distribuídos isto tem de ser comunicado a todos os envolvidos, ou seja o polinômio deve ser **padronizado**.
- ❑ Veremos que um bom polinômio gerador tem pelo menos um fator $(x + 1)$
- ❑ CRC-12 é um polinômio largamente utilizado, para gerar checksum de 12 bits:

$$x^{12}+x^{11}+x^3+x^2+1$$

CRC-CCITT

- A CCITT (hoje ITU-T) recomenda o seguinte polinômio gerador de 16 bits:

$$x^{16}+x^{12}+x^5+1$$

- O grau é 16, então este código pode detectar rajadas de erros de até 16 bits
- Em aritmética binária, este código pode ser escrito como:

$$(x+1)(x^{15}+x^{14}+x^{13}+x^{12}+x^4+x^3+x^2+x+1)$$

- Pode-se ver que qualquer polinômio multiplicado pelo fator $(x+1)$ tem um número par de parcelas (i.e., bits não zero)

CRC-CCITT

- ❑ Isto significa que todo **E com um número ímpar de** parcelas, produzido por um número ímpar de erros de bits é detectável
- ❑ CRC-CCITT detecta:
- ❑ 100% dos erros simples, duplos, com um número ímpar de bits com erro e erros em rajada com até 16 bits.
- ❑ 99,997% em caso de rajadas de 17 bits
- ❑ 99,998% em rajadas maiores que 17 bits.
- ❑ O comitê IEEE 802 padronizou um CRC-32 bits:

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

Distância Hamming

- O número de bits diferentes entre duas “palavras código” é chamado de distância Hamming (1950).
 - Código Origem: 00110101
 - Código Destino: 0**1**010101
 - Neste caso distância de Hamming (D) = 2
- A distância de Hamming equivale ao número de bits incorretos entre duas palavras
- Para **detectar d erros e distância de Hamming** entre a palavra de dados e a palavra de código deve ser igual a **d+1**
- Para **corrigir d erros a distância de Hamming** entre a palavra de dados e a palavra de código deve ser igual a **2d+1**
- O bit de paridade apresenta distância de Hamming igual a 2, logo pode corrigir 1 único bit incorreto!

Palavra de dados	01
Palavra código enviada	011
Palavra código recebida	1 10

Distância de Hamming = 2

Código de Hamming

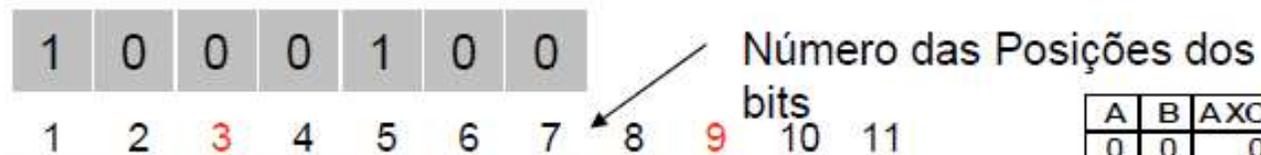
- ❑ Algoritmo que permite proteger primitivas contra erros de comunicação
- ❑ No mínimo o código permite a detecção de erros de comunicação
- ❑ Bits de verificação são colocados no quadro de tal modo que a palavra recebida indica onde ocorreu o erro.
- ❑ Algoritmo enumera os bits da primitiva de 1 a $m+r$, onde r é o número de bits de verificação.

Código de Hamming

- ❑ I-ésimo bit de verificação é colocado na posição 2^i para todo i , tal que $0 \leq i \leq \log_2(m+r)$
- ❑ Desta forma os bits de verificação são colocados nas posições: 2^0 ; 2^1 ; 2^2 ; 2^3 ; 2^4 ...
- ❑ Em seguida é feito um XOR com o valor das posições dos bits iguais a 1. O resultado deste XOR é colocado nos bits de verificação.
- ❑ Os bits do resultado do XOR são numerados da direita para a esquerda.
- ❑ número da posição indica a posição deste bit na palavra código
- ❑ Na recepção é feito um XOR com as posições dos bits iguais a 1.
- ❑ Caso seja diferente de zero então esta é a posição do erro.

Transmissão de 1000100

□ Palavra de dados



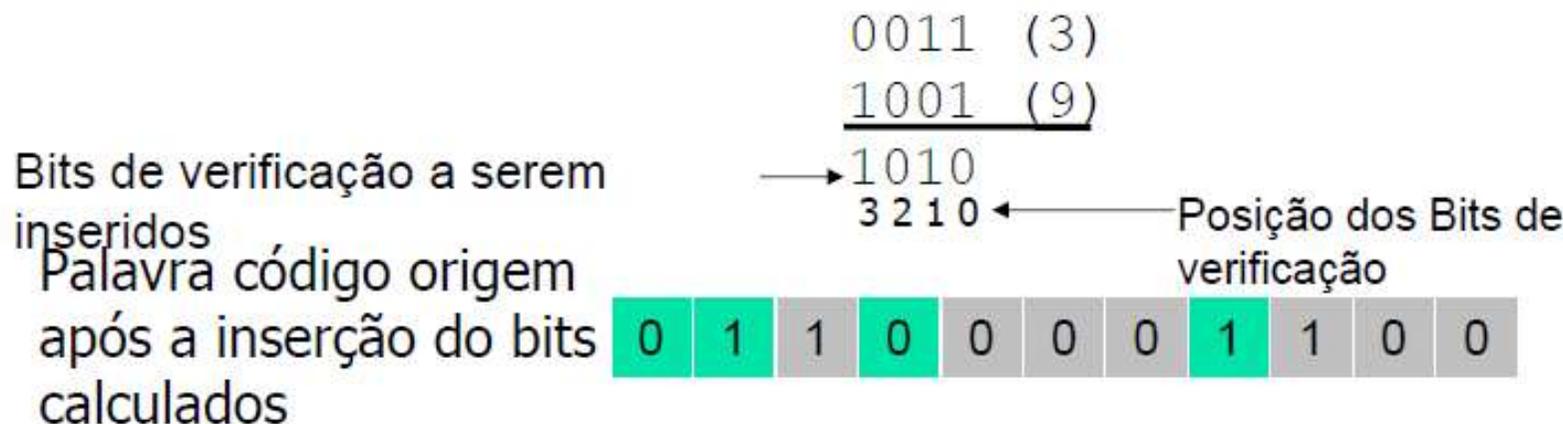
□ Palavra código origem



A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

□ Para calcular os bits de verificação é feito uma operação XOR entre os números das posições dos bits iguais a 1. Neste exemplo a posição 3 (0011) e 9 (1001), possuem na origem bits iguais a 1

□ Os bits resultantes desta operação são numerados da direita para a esquerda e este número indica a posição que em este bit será colocado



Transmissão de 1000100

□ Palavra código enviada

1	2	3	4	5	6	7	8	9	10	11
0	1	1	0	0	0	0	1	1	0	0

□ Palavra código Recebida

0	1	1	0	0	0	1	1	1	0	0
---	---	---	---	---	---	---	---	---	---	---

□ Na recepção é feito um XOR entre os números das posições dos bits iguais a 1. Neste caso temos:

2(0010); 3(0011); 7(0111); 8(1000) e 9(1001)

□ O resultado da operação equivale à posição do bit com erro!

□ Caso não houvesse erro o XOR seria entre os valores:

2(0010); 3(0011); 8(1000) e 9(1001)

□ Neste caso o resultado seria 0000 (zero) indicando que não houve erro na transmissão.

XOR

0010 (2)

0011 (3)

0111 (7)

1000 (8)

1001 (9)

0111

Resultado da operação XOR

O número indica a posição do bit com erro: 7 (0111)

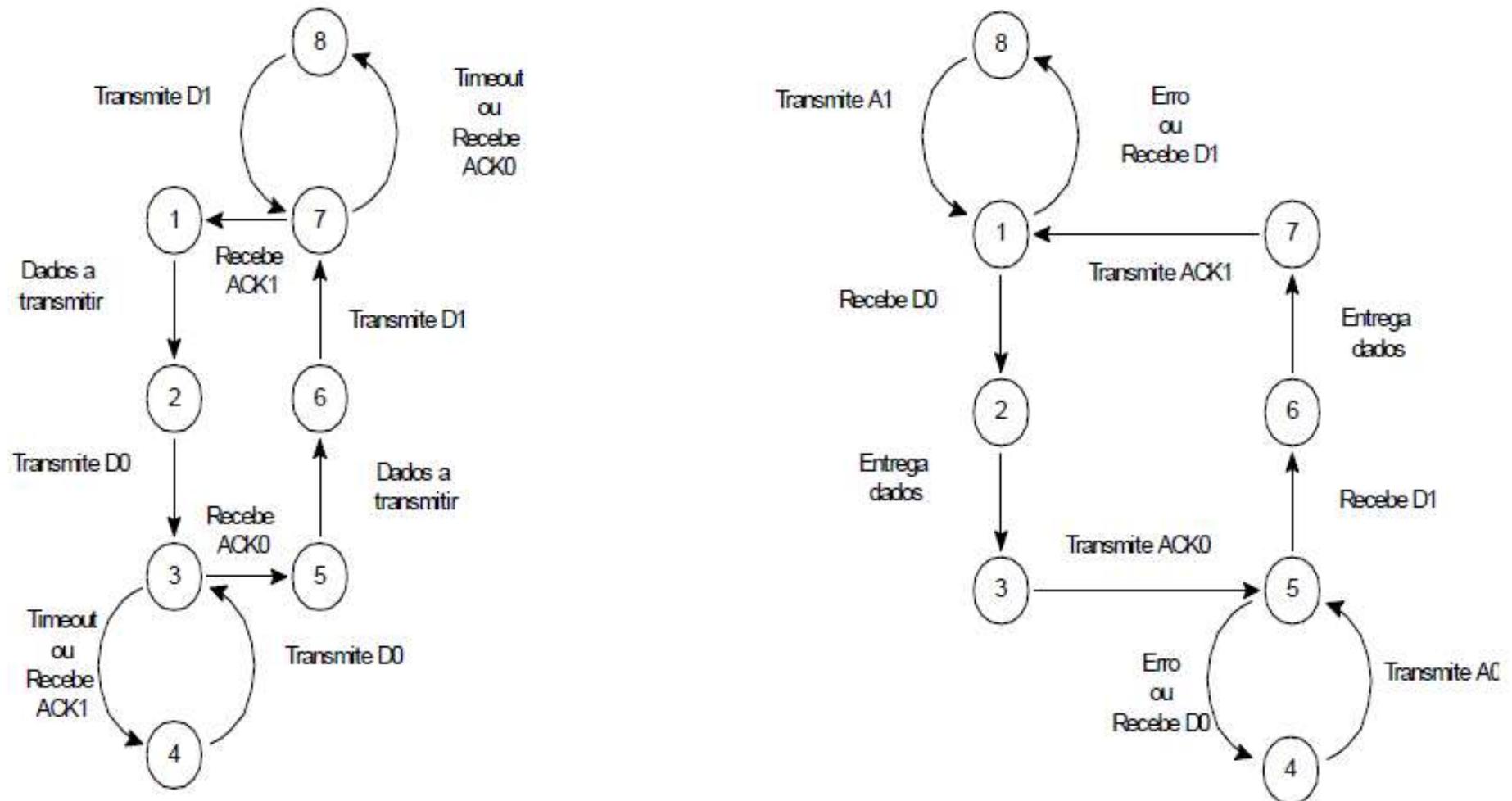
Protocolos de Enlace de Dados

- ❑ Realizam tanto o controle de erros como o controle de fluxo
- ❑ Utilizam timeouts e números de sequencia nos quadros
- ❑ A transmissão pode ser simplex ou duplex

Protocolo Stop-and-Wait

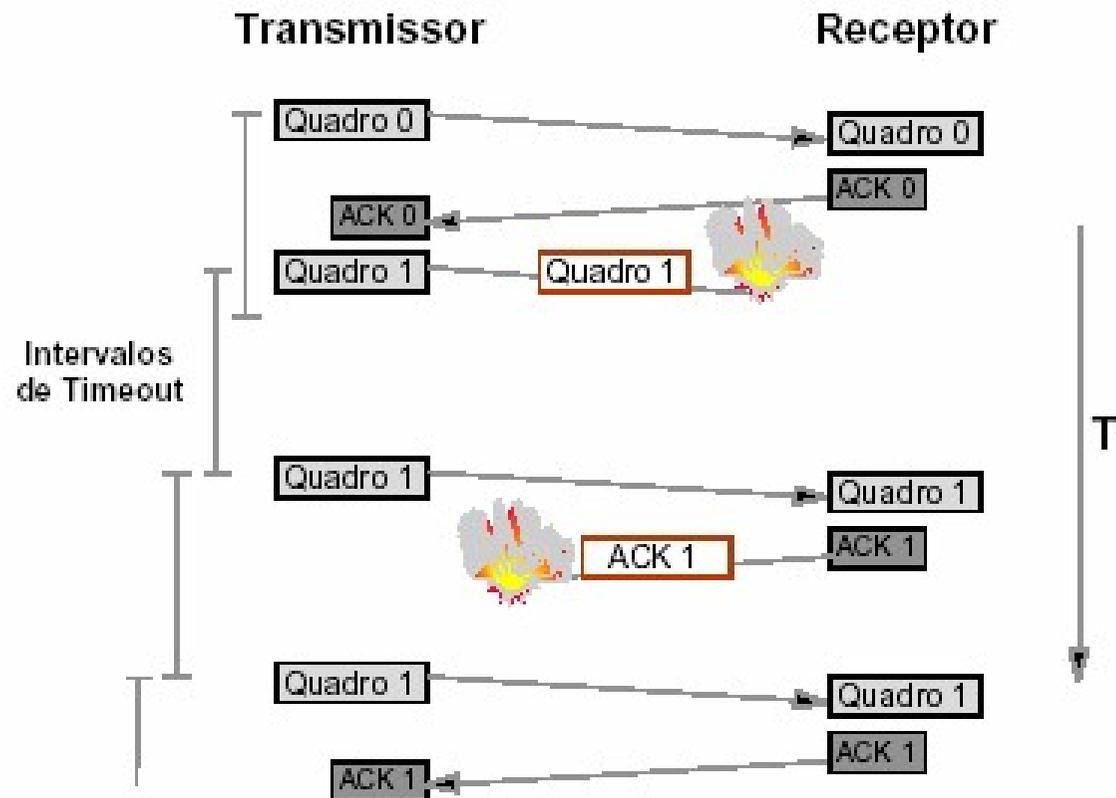
- ❑ Também conhecido como protocolo de bit alternado.
- ❑ O transmissor só envia um novo quadro quando recebe a confirmação do quadro enviado anteriormente (ACK)
- ❑ Como os quadros podem ser transmitidos mais de uma vez é necessário numerá-los para que o receptor possa diferenciá-los.
- ❑ Apenas um bit é utilizado para numerar os quadros, pois o transmissor somente envia o próximo do quadro depois do recebimento da sua confirmação.
- ❑ O primeiro quadro é numerado com bit 0 e o segundo com o bit 1
- ❑ Esta técnica é ineficiente em relação ao controle de erro, visto que enquanto o transmissor aguarda pelas confirmações (ACK) o canal não é utilizado

- A figura a seguir mostra o funcionamento do protocolo



Protocolo Stop-and-Wait

□ Diagrama Temporal do Protocolo



Protocolo com Janela

- A fim de aumentar a eficiência do uso do canal este protocolo transmite diversos quadros, mesmo sem ter recebido o seu reconhecimento.
- Os quadros são então numerados seqüencialmente
- O número máximo de quadros (W) que podem ser enviados sem reconhecimento é chamado “**Janela de Transmissão**”
- No caso de erro duas técnicas são utilizadas:
 - Retransmissão Integral (Go Back n)
 - Retransmissão Seletiva (Selective Repeat)

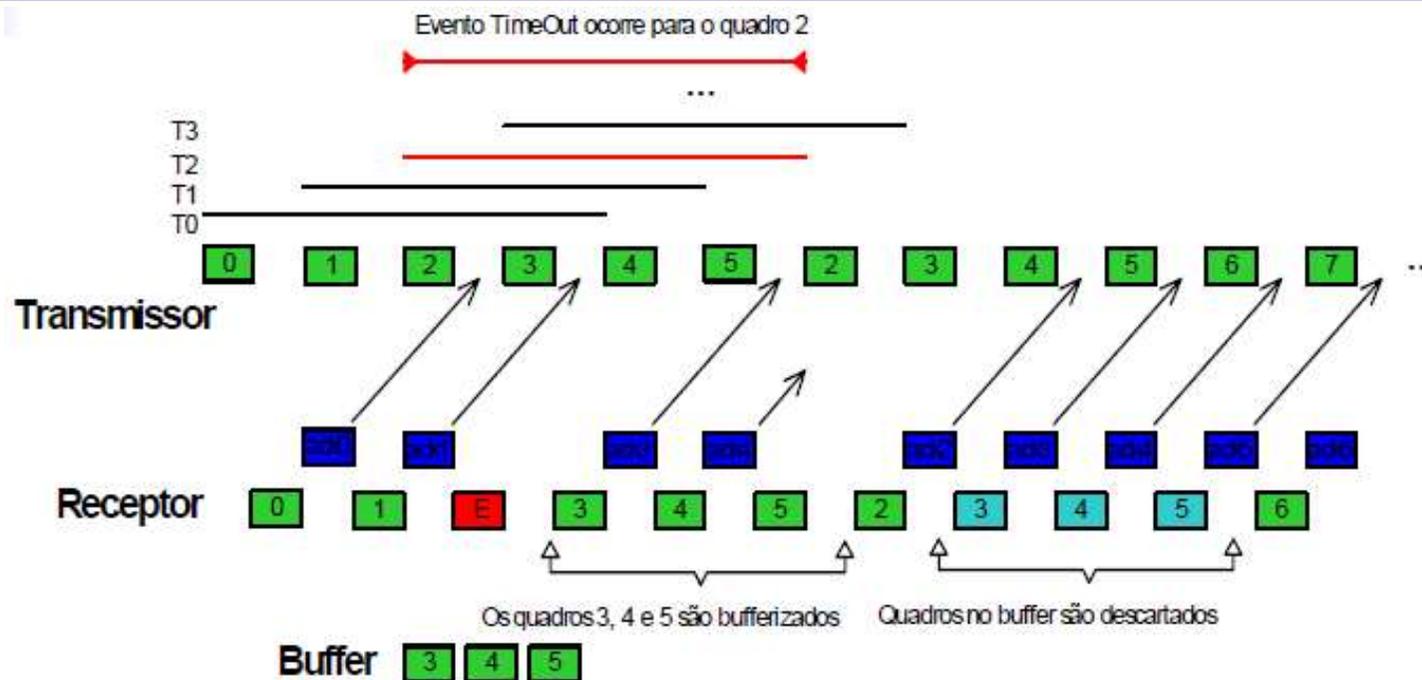
Protocolo “Go Back n”

- ❑ Também conhecido como Retransmissão Integral
- ❑ Neste caso todos os quadros a partir do que não foi reconhecido são retransmitidos
- ❑ A medida que um quadro é enviado um timer para este quadro é disparado
- ❑ Uma possibilidade para aumentar a eficiência na utilização do canal é o receptor enviar o reconhecimento do quadro de número N, ou seja o último da seqüência
- ❑ Quando o transmissor receber o reconhecimento do quadro N ele conclui que todos os outros foram recebidos corretamente.

Protocolo “Selective Repeat”

- ❑ Também conhecido como Retransmissão Seletiva
- ❑ Sempre que um quadro é enviado um timer é associado ao mesmo.
- ❑ A medida que os quadros são recebidos, em em caso de confirmação positiva, o quadro é armazenado em um buffer.
- ❑ Em caso de erro, o protocolo retransmite todos os quadros a partir do quadro cujo erro aconteceu.
- ❑ Porém neste caso, como o reconhecimento dos quadros foi armazenado e somente os quadros não reconhecidos e que são recebidos novamente.

Protocolo “Selective Repeat”



- ❑ Neste exemplo, ocorre um erro na transmissão do quadro 2. Enquanto o transmissor aguarda o ACK deste quadro os quadros seguintes são enviados.
- ❑ Como o ACK não chega o timeout acontece e desta forma todos os quadros enviados após o quadro 2, são reenviados.
- ❑ Porém ao reenviar todos os quadros após o quadro 2, somente aqueles que não estão no buffer serão recebidos, neste caso os quadros 3, 4 e 5 serão descartados

Protocolos Janela Deslizante

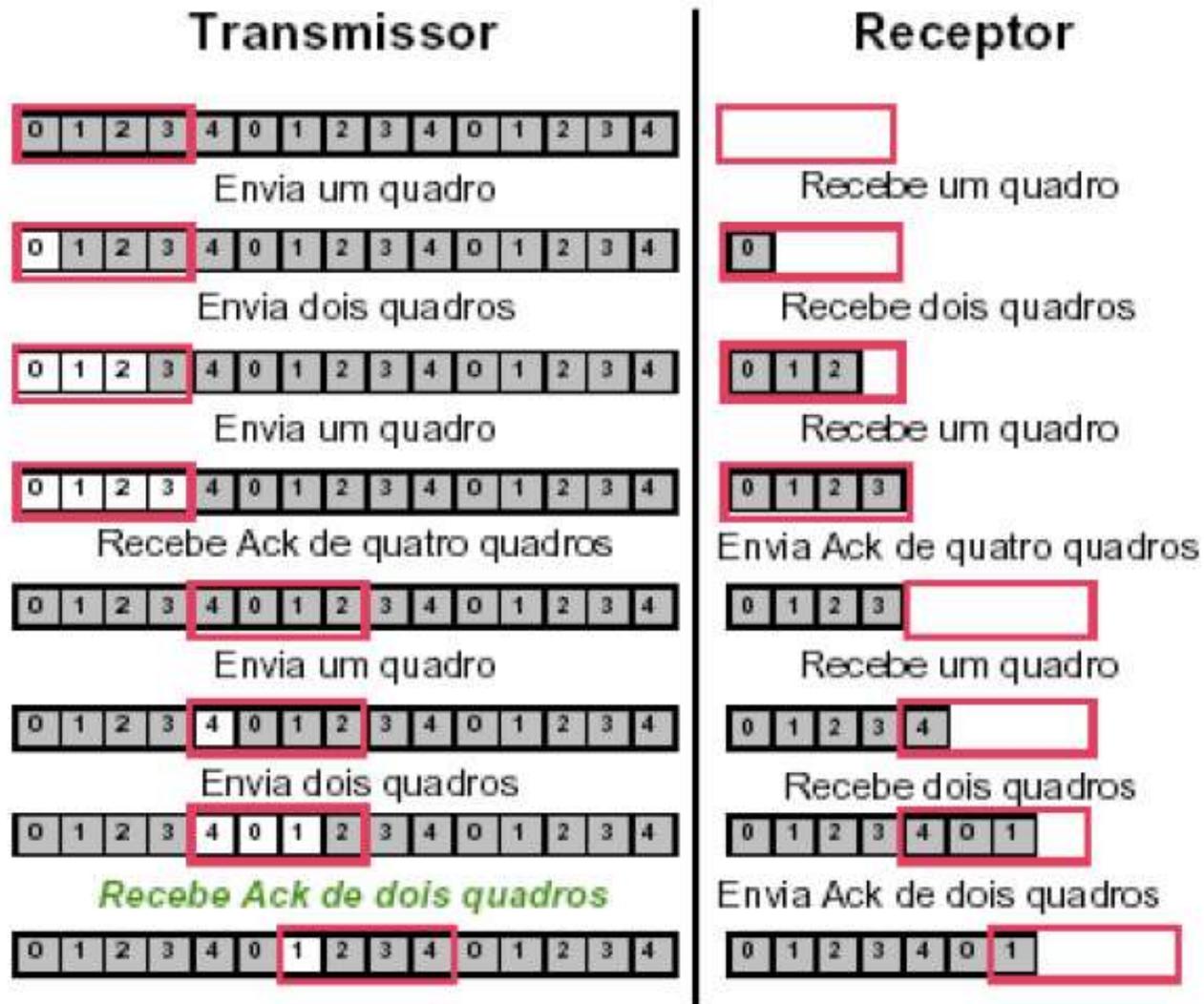
- ❑ Também conhecidos como “**sliding windows**”
- ❑ Quando a janela **W** é maior que 1, o controle de fluxo é feito com base em quadros especiais e em janelas de transmissão e recepção
- ❑ O número máximo (**T**) de quadros que o transmissor pode enviar, sem receber um reconhecimento é determinado pela largura da janela.
- ❑ Após enviar **T quadros sem receber reconhecimento** o transmissor suspende o envio dos dados
- ❑ Os dados serão transmitidos somente após o recebimento de um reconhecimento
- ❑ Este quadro de reconhecimento indica que o receptor está pronto para processar novos quadros e que todos enviados foram recebidos em erros.

Proctolos Janela Deslizante

- ❑ O tamanho da janela deve ser igual ao número máximo de seqüência dos quadros
- ❑ O número máximo (**R**) **que o receptor pode receber** sem que nenhum seja entregue ao nível superior (rede) é o tamanho da janela de recepção.
- ❑ Os quadros são armazenados em um buffer de recepção
- ❑ Se o buffer está cheio um quadro especial – `receive_not_ready` é enviado ao transmissor que suspende o processo de envio

Protocolos Janela Deslizante

Exemplo

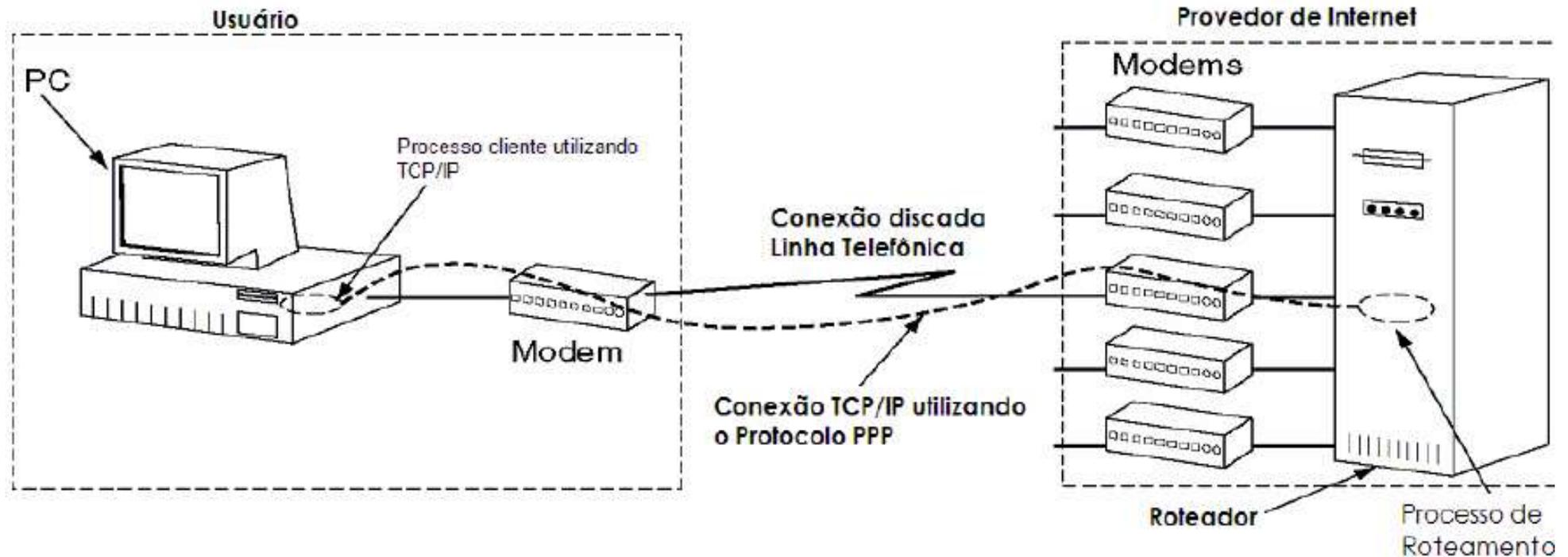


Protocolo PPP

- ❑ O protocolo PPP (Point-to-Point Protocol – Protocolo Ponto a ponto) é um protocolo utilizado para conectar computadores domésticos à Internet
- ❑ Este é um protocolo de enlace de dados que trata as funções de enquadramento, controle de erros entre outras
- ❑ O protocolo é definido pela RFC (Request For Comments) 1661 e mais elaborado em várias outras RFCs (por exemplo, as RFCs 1662 e 1663)
- ❑ Através de uma mesma ligação, o protocolo PPP pode transportar diferentes tipos de pacotes vindos da camada de rede através de uma mesma ligação
- ❑ A ligação é full-duplex e considera-se que os quadros são entregues de forma ordenada

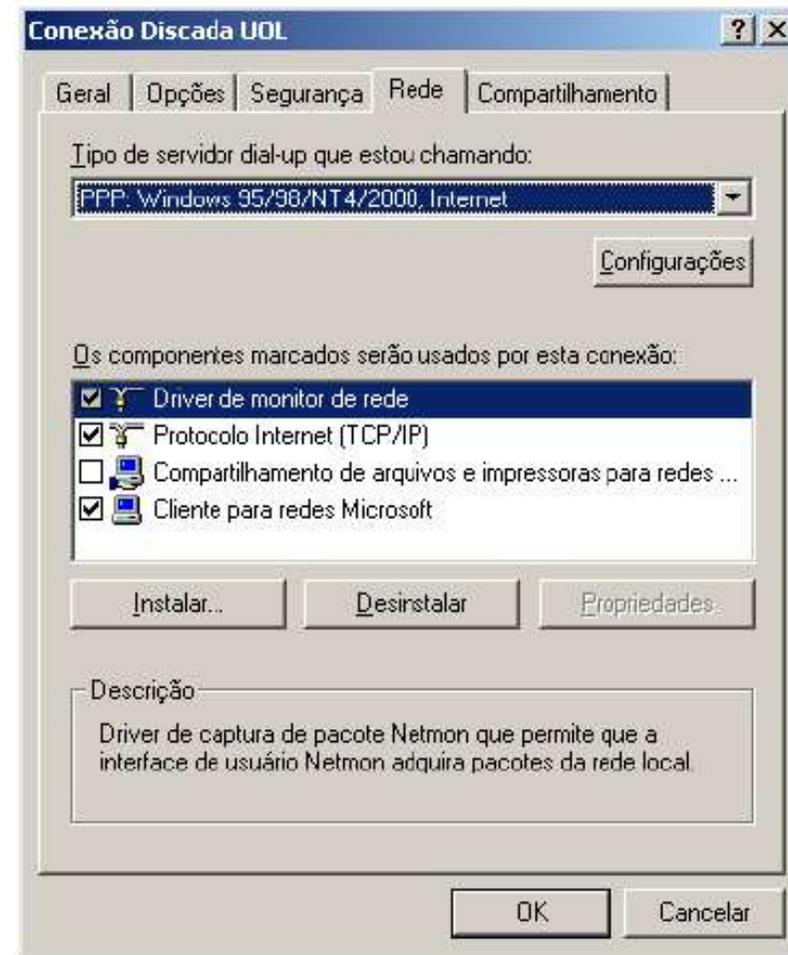
Protocolo PPP

- Protocolo PPP utilizado na conexão internet



Protocolo PPP

- ❑ O protocolo PPP é utilizado nas conexões discadas à internet e deve ser configurado



Protocolo PPP

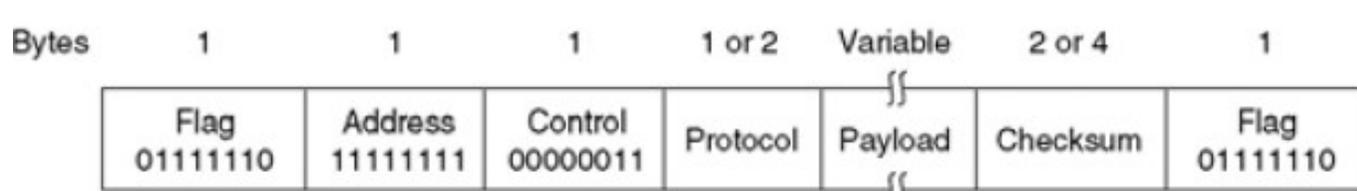
- ❑ O PPP possui três componentes básicos:
- ❑ Um método responsável pelo enquadramento através da inserção de caracteres e um controle de erro através de checksum
- ❑ Um protocolo de controle de enlace, chamado LCP (Link Control Protocol) usado para ativar linhas, testá-las, negociar opções e desativá-las novamente quando não forem mais necessárias.
- ❑ Uma maneira de negociar as opções da camada de rede de modo independente do protocolo da camada de rede a ser utilizado.
 - Para isto existe uma família de NCPs (Network Control Protocol — protocolo de controle de rede) para cada diferente protocolo de rede utilizado.

Exemplo de Utilização

- ❑ Computador doméstico de conectando à Internet utilizando TCP/IP
 1. PC chama o roteador do provedor por meio de um modem
 2. Modem do roteador atende ao telefone e estabelece uma conexão física
 3. PC envia ao roteador uma série de pacotes LCP no campo de carga útil de um ou mais quadros PPP. Esses pacotes e suas respostas selecionam os parâmetros PPP a serem utilizados.
 4. Após esta definição uma série de pacotes NCP é enviada para configurar a camada de rede.
 5. O NCP para o IP atribui os endereços IP, desta forma o Pc irá receber um endereço IP de forma dinâmica.
 6. Nesse momento, o PC passa a ser um host da Internet e pode enviar e receber pacotes IP, da mesma forma que os hosts fisicamente conectados.
 7. Ao final da conexão o NCP é utilizado para desativar a conexão da camada de rede e liberar o endereço IP.
 8. O LCP encerra a conexão da camada de enlace de dados.
 9. Finalmente, o PC solicita que o modem desligue o telefone, liberando a conexão da camada física.

Quadro PPP

- O quadro PPP é orientado a bytes e é composto da seguinte forma:
 - Campo Flag – 1 byte; Responsável pelo enquadramento
 - Campo Endereço – 1 byte, sempre com o valor 11111111. Todas as estações devem aceitar o quadro
 - Campo Controle – 1 Byte. Valor padrão é 00000011 indicando que o quadro é não numerado. Neste modo o PPP não oferece transmissão confiável com números de seqüência
 - Campo Protocolo – Informa o tipo de pacote existente no quadro carga. Seus valores indicam os protocolos LCP, NCP, IP, IPX, AppleTalk entre outros. 2 bytes
 - Campo Carga (Payload) – Tamanho variável e negociado através do LCP, possui valor padrão de 1500 bytes. Ocorre o preenchimento (padding) caso necessário
 - Campo CheckSum – 2 bytes. Utilizado para controle de erros através do CRC
- Como Endereço e Controle são constantes o LCP negocia entre ambas as partes a sua omissão



Subcamada de Acesso ao Meio

- As Redes podem ser divididas em duas categorias quanto à sua tecnologia de transmissão:
 - Redes Ponto a Ponto (Point to Point)
 - Meio de transmissão dedicado
 - Sem disputa (contention) pelo acesso ao meio
 - Sem necessidade de endereçamento
 - Apenas um destino possível para cada transmissão
 - Exemplo: Conversa ao telefone
 - Redes de Difusão (BroadCast)
 - Meio de transmissão compartilhado
 - É necessário disciplinar o acesso ao meio
 - Cada estação possui um endereço único
 - A mesma transmissão pode ser recebida por várias estações
 - Exemplo: Palestra em uma sala de aula

Subcamada de Acesso ao Meio

- Nas redes de difusão (Broadcast) existe um importante problema a ser resolvido:
 - Determinar quem tem direito de usar o canal quando há uma disputa pelo mesmo
- A subcamada de acesso ao meio (Medium Access Control – MAC) é parte integrante da camada de Enlace de dados e contém os protocolos de acesso ao meio
- Esta camada é particularmente importante para as redes locais (LAN) visto estas são redes de difusão

Alocação do Canal

- ❑ O problema básico consiste em várias estações competindo pelo meio físico.
- ❑ Existem duas abordagens possíveis para alocação do canal de comunicação
- ❑ Alocação Estática – Consiste em dividir a banda do canal ou o tempo de acesso ao mesmo entre as várias estações
- ❑ Alocação Dinâmica – Neste caso todo o canal é alocado para a transmissão de forma aleatória por cada estação que deseja transmitir

Alocação Estática

- ❑ Na alocação estática o canal é dividido entre todas as estações.
- ❑ Basicamente existem duas formas de realizar esta alocação:
 - **Multiplexação por Divisão de Frequência (FDM – Frequency Division Multiplexing)**
 - ❑ Se existem N usuários, a largura de banda é dividida em N partes do mesmo tamanho, desta forma cada estação utiliza uma faixa de frequência diferente para transmissão.
 - **Multiplexação por Divisão de Tempo (TDM - Time Division Multiplexing)**
 - ❑ Neste caso o uma faixa de tempo t (time slot), é cedido para cada estação realizar a sua transmissão
 - ❑ Em ambas as abordagens não existe disputa
 - ❑ Quando alguma estação ficar inativa o uso do canal será desperdiçado, pois o uso do canal não pode ser remanejado
 - ❑ Desta forma resultam em uma baixa utilização do canal

Alocação Dinâmica

- ❑ Na alocação dinâmica uma estação utiliza toda a sua capacidade para transmissão dos quadros.
- ❑ Neste caso haverá disputa (contention) pelo uso do meio de transmissão
- ❑ Ocorre a possibilidade de colisões, ou seja, duas ou mais estações transmitindo dados ao mesmo tempo.

Alocação Dinâmica - Premissas

□ Estações

- Autônomas – geram tráfego independentemente umas das outras
- Mono-programadas - uma vez iniciada a transmissão de um quadro, a estação permanece bloqueada até que a transmissão se complete com sucesso
- No que se refere ao hardware, todas as estações são equivalentes, embora um software de protocolo possa atribuir prioridades a elas para acesso ao canal

□ Canal de transmissão

- Um único canal é utilizado para transmissão e recepção por todas as estações

Alocação Dinâmica - Premissas

- Colisões
 - Ocorrem quando dois (ou mais) quadros são transmitidos simultaneamente
 - Todas as estações podem detectar a ocorrência de colisões
 - Um quadro que tenha sofrido colisão deverá ser retransmitido posteriormente
 - Não há outros erros além dos gerados por colisões.
- Uso do tempo
 - O tempo pode ser utilizado de duas formas
 - Tempo contínuo
 - Transmissão de quadros pode ter início em qualquer instante
 - Tempo demarcado (slotted time)
 - Um relógio mestre divide o tempo em intervalos discretos (slots)
 - Transmissão de quadros só pode começar no início de um slot

Alocação Dinâmica - Premissas

- Detecção do estado do canal
 - Existem duas diferentes abordagens baseadas detecção de portadora. Portadora (carrier) se refere ao sinal elétrico enviado pelo cabo
 - Com Detecção de Portadora (carrier sensing)
 - Estações verificam se o canal está sendo usado antes de tentarem transmitir
 - Reduz a probabilidade de colisões
 - Método geralmente usado em redes locais
 - Sem Detecção de Portadora
 - Quando a monitoração prévia do estado do canal não é prática. Por exemplo, em redes sem fio, devido ao fato de nem toda estação estar na mesma faixa de rádio das outras.
 - Estações transmitem sem verificar se o canal está livre
 - Detectam a colisão e retransmitem

Protocolos de Acesso Múltiplo

- ❑ Existem vários protocolos para alocar um canal de acesso múltiplo.
- ❑ Os vários protocolos diferem em funcionamento; eficiência e no tipo de meio físico a ser utilizados
- ❑ Protocolos
 - ALOHA
 - ALOHA com Tempo Demarcado (Slotted ALOHA)
 - Protocolos com monitoramento do meio (CSMA)
 - Protocolos livres de colisão
 - Protocolos de Disputa Limitada
 - Protocolos de múltiplo acesso com divisão do comprimento de onda
 - Protocolos para rede local sem fio

ALOHA

- ❑ Desenvolvido na década de 70 (Norman Abramson) em uma Universidade do Havaí
- ❑ Estações transmitem quadros sempre que houver dados a serem enviados sem monitorar o estado do meio
- ❑ Colisões são frequentes e quadros são perdidos mesmo que apenas o primeiro ou último bit tenha colidido
- ❑ Transmissor detecta a colisão e retransmite o quadro
 - Detecção da colisão é feita através da escuta da saída do canal. Caso não seja possível escutar o canal é necessário confirmações (ACK)
 - No caso de colisão, retransmite após um intervalo aleatório de tempo para tentar evitar novas colisões

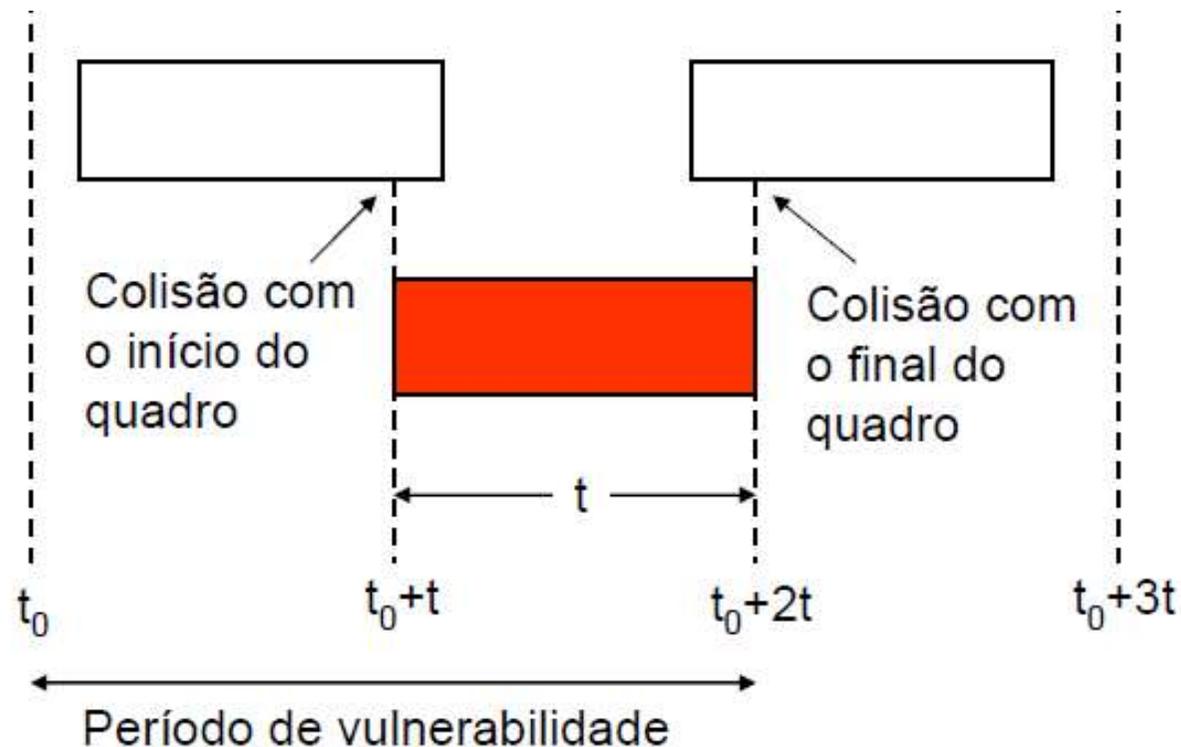
ALOHA

- ❑ Quadros transmitidos pelo protocolo ALOHA. Os hachurados foram perdidos devido às colisões.



ALOHA

- Sendo t o tempo de envio de um quadro.
- Qualquer quadro gerado nos intervalos $(t_0 ; t_0+t)$ e no intervalo $(t_0+2t; t_0+2t)$ irá colidir com o quadro sombreado



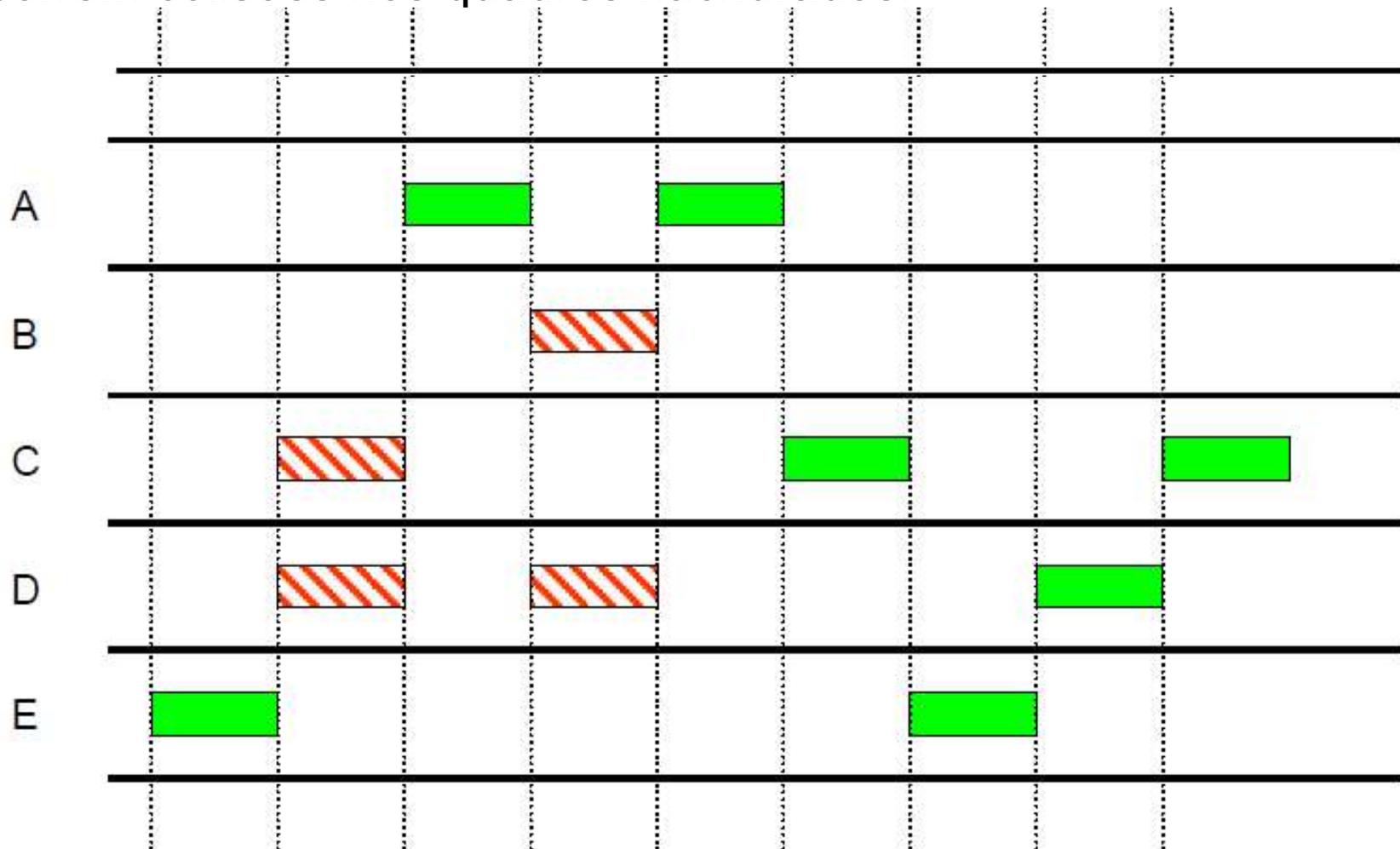
ALOHA - Eficiência

- ❑ A eficiência decresce com o aumento do número de estações tentando transmitir ao mesmo tempo
- ❑ Isto gera mais colisões, que por sua vez geram mais retransmissões, produzindo um efeito cascata
- ❑ Eficiência máxima do protocolo é de 18%, ou seja, apenas 18% da capacidade do canal é utilizada

SLOTTED ALOHA

- ❑ Publicado em 1972(Roberts, L.)
- ❑ Tempo é dividido em intervalos discretos
- ❑ Cada intervalo é equivalente ao tempo de transmissão de um quadro, considerando os que todos os quadros possuem tamanho fixo
- ❑ Sincronização é feita por uma estação especial transmite um sinal periódico de temporização para marcar o início dos slots
- ❑ Estação transmissora precisa esperar o início de um novo slot para que possa transmitir
- ❑ Reduz pela metade o período de vulnerabilidade
- ❑ Dobra a eficiência: 36%

- Ocorrem colisões nos quadros hachurados.



Protocolos CSMA

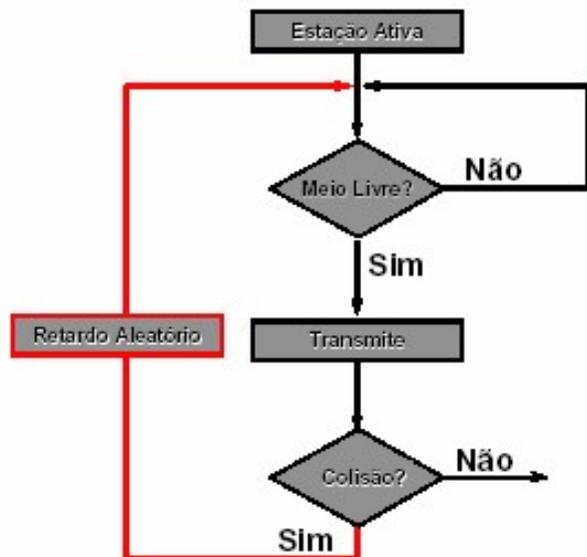
- ❑ Estes protocolos de múltiplo acesso (Multiple Access) baseiam-se na detecção da portadora (Carrier Sense)
- ❑ A detecção é feita através do monitoramento do meio
- ❑ Em redes locais, é possível uma estação monitorar a atividade das demais
- ❑ Antes de efetuar uma transmissão a estação deve observar o meio
- ❑ Possui uma melhor eficiência de utilização do meio, em relação aos protocolos ALOHA/Slotted ALOHA devido à maior disciplina no acesso.

CSMA 1-Persistente

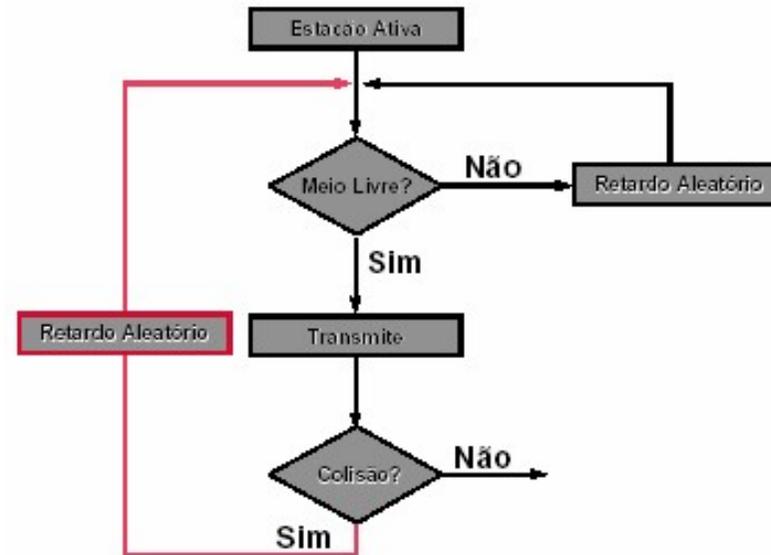
- Estação recebe dados da camada superior para a transmissão, e desta forma segue os seguintes passos:
 - Inicialmente “escuta” o meio de transmissão
 - Se livre
 - Estação transmite o quadro imediatamente
 - Se ocupado
 - Estação continua escutando o canal
 - Ao detectar que o meio ficou livre, transmite o quadro imediatamente
 - Se houver colisão, estação aguarda um tempo aleatório e repete o protocolo
- Esse protocolo é denominado 1-persistente, porque a estação transmite com probabilidade 1 sempre que encontra o canal desocupado, ou seja, realiza a transmissão imediata

CSMA funcionamento

□ CSMA 1-Persistente



□ CSMA Não Persistente



CSMA 1-Persistente Desempenho

- É afetado pelo atraso de propagação. Quanto maior o atraso aumenta a probabilidade de que duas estações percebam o meio de transmissão livre e comecem a transmitir “simultaneamente”, gerando colisão
- Exemplo:
 - Estação A transmite um quadro
 - Estação B escuta o meio mas o sinal transmitido por A ainda não se propagou até ela então B pensa que o meio está livre e começa a transmitir



CSMA Não Persistente

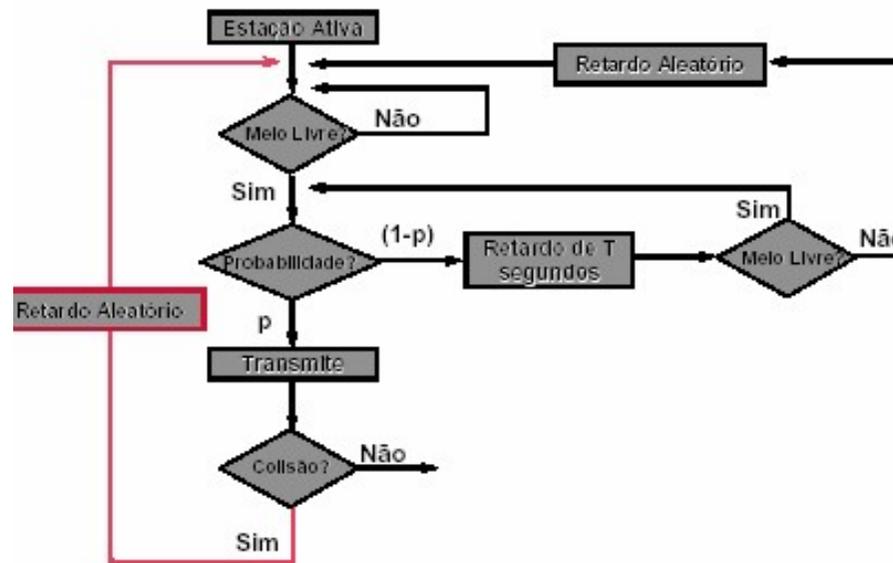
- Antes de transmitir, estação “escuta” o meio
- Se livre:
 - Inicia transmissão do quadro imediatamente
- Se ocupado:
 - Estação na fica escutando o canal, mas ao invés disso, espera um intervalo de tempo aleatório
 - Recomeça novamente o protocolo
- Melhor utilização do meio visto que gera um número menor de colisões
- Requer um tempo maior para transmitir um quadro

CSMA p-Persistente

- Protocolo com tempo demarcado em intervalos (slots)
- Antes de transmitir, estação “escuta” o meio
- Se livre:
 - Se probabilidade igual a **p então:**
 - Transmite o quadro
 - Se probabilidade igual a **q ($q = 1 - p$) então:**
 - Aguarda um tempo aleatório (T) e verifica novamente se o meio está livre
 - Caso o meio esteja ocupado realiza um retardo aleatório
- Se ocupado:
 - realiza um retardo aleatório
 - espera próximo slot e recomeça
- Baseado em tempo discreto
- Eficiência: 85% para $p = 0.1$

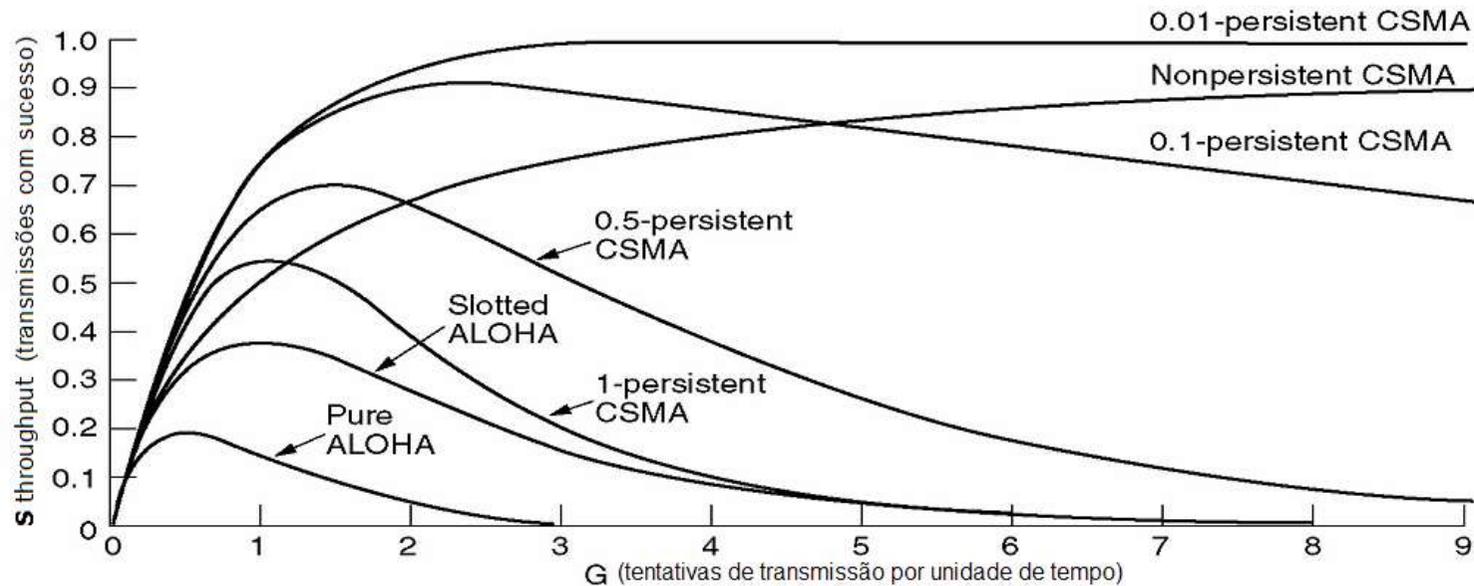
CSMA p-Persistente

❑ Funcionamento



Comparação de Eficiência

- Comparação do uso do canal x a carga para os vários protocolos de acesso múltiplo



Comparação de Eficiência

- ❑ S (Rendimento / Throughput)– Número de transmissões com sucesso por unidade de Tempo.
- ❑ Para simplificação o tempo de de transmissão de um pacote será igual a 1. Logo o número máximo de transmissões é igual a 1.
- ❑ G (Carga / Load) – Número esperado de transmissões e tentativas de retransmissões de todas as estações por unidade de tempo

CSMA Considerações

- Quanto menos persistente:
- melhor a eficiência de utilização do meio
- Por outro lado, a diminuição do fator p resulta em um maior atraso de transmissão para cada quadro individual
- Portanto, deve-se chegar a um equilíbrio entre estes dois requisitos
 - eficiência de utilização do meio
 - tempo máximo de transmissão de um quadro

CSMA/CD

- ❑ Protocolo CSMA com Detecção de Colisão (Collision Detection)
- ❑ Melhoria sobre os protocolos CSMA originais
- ❑ Estações interrompem a transmissão de seus quadros caso detectem uma colisão
- ❑ Economizam tempo e largura de banda, uma vez que os quadros já foram comprometidos
- ❑ Detecção de colisões:
 - Estação transmissora “escuta” o meio, medindo a potência ou comprimento dos pulsos de sinal recebidos, comparando com o sinal transmitido
 - Em meios de difusão (broadcast) uma estação “escuta” suas próprias transmissões

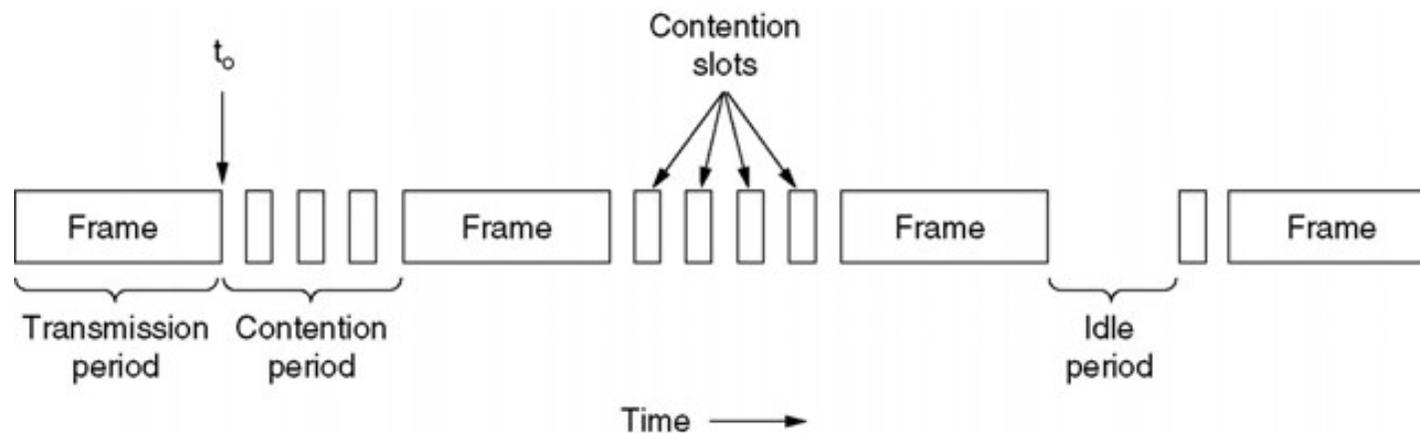
CSMA/CD

□ Algoritmo

- Uma ou mais estações têm quadros para transmitir (anterior ao instante t_0)
- Cada estação “escuta” o meio
- Quando o meio se torna livre (t_0):
 - Cada estação inicia a transmissão de seu quadro
- Estações continuam “escutando” o meio
- Caso detectem uma colisão:
 - param a transmissão
 - esperam um intervalo de tempo aleatório
 - tentam novamente

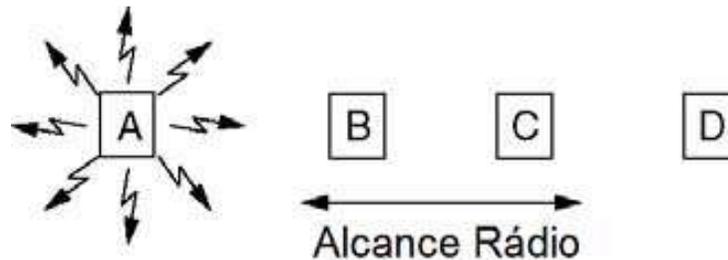
CSMA/CD

- Sistema alterna entre os seguintes estados:
 - Contention(Disputa): estações tentando ganhar acesso ao meio
 - Transmission(Transmissão): uma estação transmite um quadro
 - Idle(Inativo) : nenhuma estação tem quadros a transmitir



Protocolo para Redes sem Fio

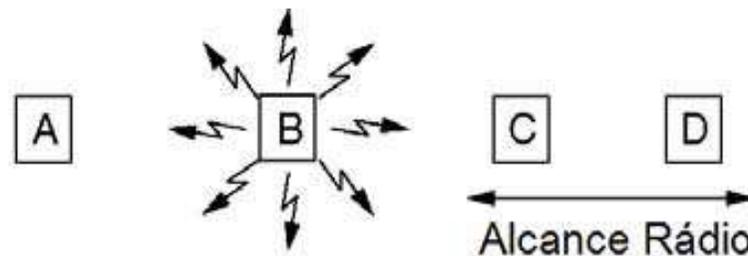
- Em um primeiro momento podemos supor que um protocolo CSMA seria suficiente para uma rede sem fio
- Porém Em redes sem fio esta abordagem não funciona devido as suas peculiaridades
- **Problema da estação oculta**
 - A está transmitindo para B. C deseja transmitir para B, porém A está fora de seu alcance
 - Neste caso, apenas por ouvir o canal, C irá concluir que o canal está disponível, e irá iniciar a transmissão para B, gerando colisões



Protocolo para Redes sem Fio

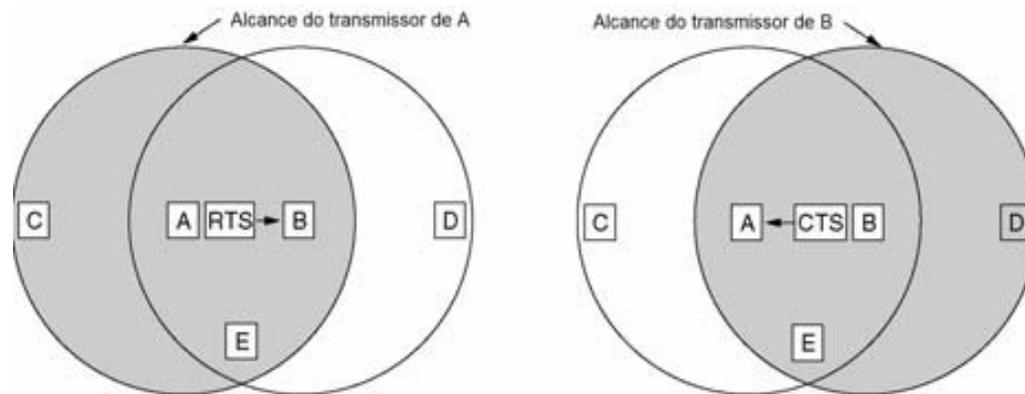
□ Problema da estação exposta

- Supondo agora que B está transmitindo para A e que C deseja transmitir para D
- Neste caso, apenas por ouvir o canal, C irá concluir que o canal está ocupado, pois está no alcance do rádio da estação B
- Então C, irá concluir de forma errada, que a transmissão para D não pode ser efetuada, pois o meio está sendo ocupado



Protocolos para Redes sem Fio

- ❑ Protocolo **MACA (Multiple Access with Collision Avoidance – Acesso Múltiplo com Abstenção de Colisão)**
 - Um dos primeiros (1990) protocolos para redes sem fio
 - Neste protocolo o transmissor estimula o receptor a emitir um pequeno quadro, a fim de avisar as estações que estão em seu (receptor) alcance que o mesmo irá receber quadro, evitando assim novas transmissões
- ❑ Protocolo **MACAW (Maca for Wireless, 1994), possui alguns melhoramentos em relação ao MACA**



Protocolo para Redes sem Fio

- Protocolo MACA (Multiple Access with Collision Avoidance)
 - A deseja enviar um quadro para B
 - Inicialmente A envia um pequeno (30 bytes) quadro **RTS (Request do Send)** para B. Este quadro contém em um de seus campos o tamanho do quadro que será enviado em seguida por A
 - B responde para A com um quadro **CTS (Clear to Send)**. Este quadro também contém o tamanho do quadro que B irá receber.
 - Assim que receber o quadro **CTS, A, irá iniciar a transmissão do quadro para B**
 - Qualquer estação que estiver no alcance de A irá ouvir o **RTS e então não** utilizará o canal por um período suficiente para que A receba o **CTS de volta**
 - Da mesma forma qualquer estação no alcance de B, irá receber o **CTS e ficará** em silêncio para aguardar o quadro que será transmitido em seguida.
 - Mesmo assim ainda ocorrem colisões, por exemplo B e C podem enviar quadros
 - **RTS para A no mesmo instante.**
 - No caso de uma colisão o transmissor que não obtiver o **CTS em um intervalo de** tempo esperado, aguarda um intervalo aleatório a fim de realizar uma nova tentativa

Protocolo para Redes sem Fio

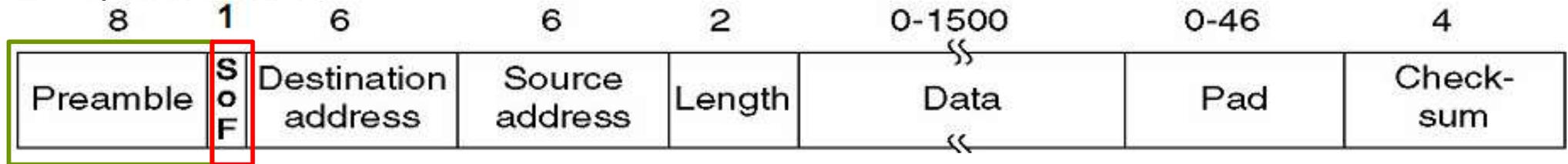
- Protocolo MACA (Multiple Access with Collision Avoidance – Acesso Múltiplo com Cancelamento de Colisão)
 - Um dos primeiros (1990) protocolos para redes sem fio
 - Neste protocolo o transmissor estimula o receptor a emitir um pequeno quadro, a fim de avisar as estações que estão em seu (receptor) alcance que o mesmo irá receber quadro, evitando assim novas transmissões

Padrão Ethernet

- ❑ Padrão 802.3 (Ethernet) e Padrão 802.11 (LAN sem fio)
- ❑ O 802.3 e o 802.11 têm camadas físicas diferentes e subcamadas MAC diferentes
- ❑ Convergem para a mesma subcamada de controle de enlace lógico (LLC - definida no padrão 802.2), e portanto têm a mesma interface para a camada de rede
- ❑ O protocolo da subcamada MAC do padrão 802.3 é baseado no protocolo de acesso CSMA/CD 1-persistente

Protocolo MAC IEEE 802.3

□ Quadro MAC



□ Preâmbulo:

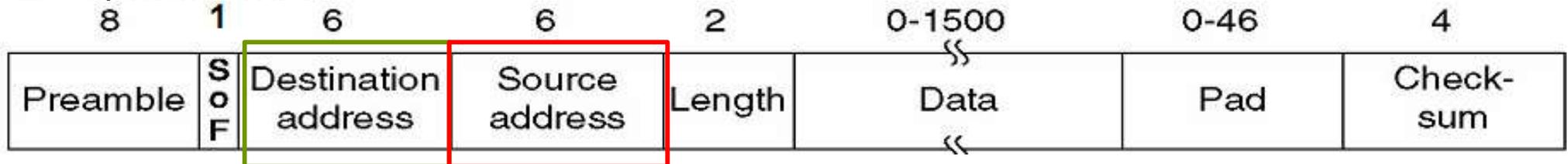
- 7 bytes contendo o padrão de bits 1 0 1 0 1 0 1 0. Este padrão produz uma onda quadrada a fim de permitir a sincronização entre o clock do receptor e o clock do transmissor

□ Delimitador de início de quadro

- 1 byte contendo o padrão 1 0 1 0 1 0 1 1

Protocolo MAC IEEE 802.3

□ Quadro MAC



□ Endereços de destino e fonte (2 ou 6 Bytes)

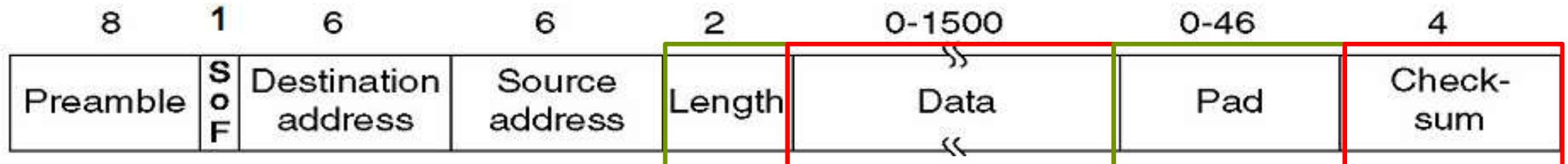
- Bit de mais alta ordem: 0 → endereço único; 1 → endereço de grupo
 - Multidifusão (Multicast): transmissão de um mesmo pacote para um grupo de estações
 - Difusão (Broadcast): todos os bits do endereço de destino iguais a 1
- Bit 46
 - Endereços globais: atribuídos pelo IEEE, globalmente únicos (7×10^{13})
 - Endereços locais: atribuídos pelo administrador local

Endereços MAC IEEE 802.3

- 6 bytes, expressos em hexadecimal
- Formato: xx:xx:xx:xx:xx:xx
- Placas de rede possuem endereços permanentemente associados
 - Não há duas placas com o mesmo endereço MAC (global)
 - Fabricantes compram, do IEEE, pacotes de 224 endereços: 3 bytes menos significativos do endereço
- Endereços com estrutura “plana”
 - Sem estrutura hierárquica
 - Independentes da rede em que se localiza a estação ou placa de rede
- Endereço de broadcast: FF:FF:FF:FF:FF:FF

Protocolo MAC IEEE 802.3

□ Quadro MAC



- Comprimento do campo de dados
 - Especifica o número de bytes contidos no campo de dados do quadro
 - Mínimo de 0, máximo de 1500
- Campo de enchimento (Pad)
 - Evita quadros menores que 64 bytes
- Tamanho mínimo de um quadro: para garantir a detecção de colisões (a 10Mbps: 64 bytes = 51,2µs = tempo de ida-e-volta)
- Campo de checksum
 - Código de checagem de erro polinomial
 - CRC 32 bits

Dispositivos de Enlace de Dados

□ Hub

- Opera na camada física
- Manipula bits individuais
- Nada mais que **repetidor com várias portas**
- Único domínio de colisões

□ Switch

- Dispositivo de camada de enlace
- Manipula quadros
- Cada porta forma um domínio de colisões independente
- Capacidade de encaminhar os quadros apenas para a porta à qual está ligada a estação de destino
- Aumenta o vazão global da rede