

Capítulo 2

Conectando-se

Problemas

- No Capítulo 1, nós vimos que redes consistem de enlaces interconectando nós. Como podemos conectar dois nós?
- Nós também introduzimos o conceito de abstração de “nuvem” para representar uma rede sem revelar suas complexidades internas. Como podemos conectar um host a uma nuvem?

Visão Geral do Capítulo

- Aspectos Gerais sobre Conexões de Nós
- Codificação
- Enquadramento
- Detecção de Erros
- Transmissão Confiável
- Ethernet e Redes de Múltiplos Acessos
- Redes Sem Fio

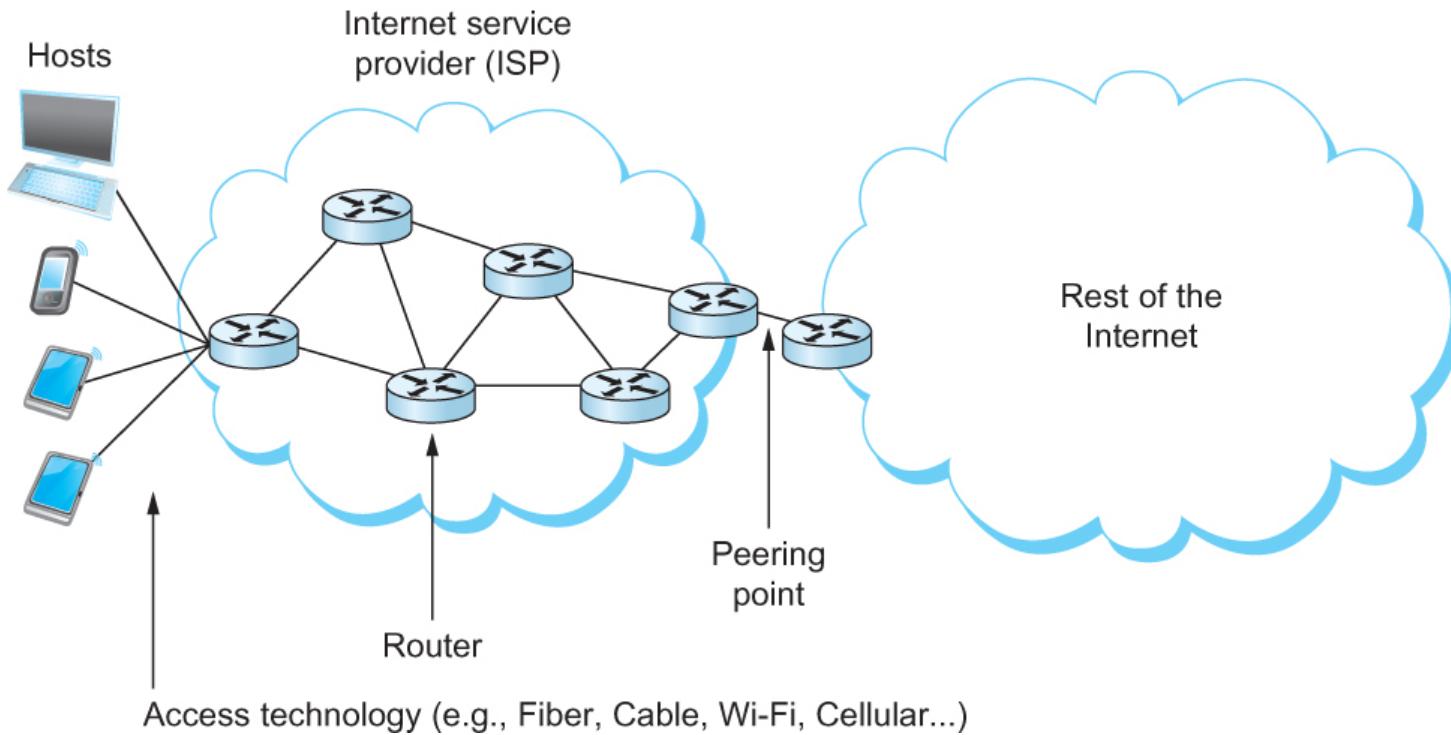
Objetivos do Capítulo

- Explorar diferentes meios de comunicação sobre os quais podemos enviar dados
- Entender o processo de codificação de bits em um meio de transmissão
- Discutir a questão de delimitação de sequências de bits em mensagens que podem ser entregues a um nó
- Discutir diferentes técnicas de detecção de erros e possíveis ações

Objetivos do Capítulo

- Discutir como tornar um enlace confiável apesar de problemas na transmissão
- Introduzir o problema de controle de acesso ao meio (*Media Access Control – MAC*)
- Introduzir redes CSMA (*Carrier Sense Multiple Access*)
- Introduzir redes sem fio com diferentes tecnologias e protocolos

Aspectos Gerais sobre Conexão



Visão da Internet do ponto de vista do usuário final

Capacidade de Enlace e Teorema de Shannon-Hartley

- Define o limite superior de capacidade de um enlace em termos de bits por segundo (bps) como uma função da razão sinal/ruído em decibéis (dB).
- $C = B \log_2(1+S/N)$
 - Em que $B = 3300 - 300 = 3000\text{Hz}$, S é a potência do sinal e N é o ruído médio.
 - A razão sinal/ruído (S/N) é medida em decibéis e está relacionada da seguinte forma $\text{dB} = 10 \times \log_{10}(S/N)$. Se há 30 dB de ruído então $S/N = 1000$.
 - Agora $C = 3000 \times \log_2(1001) = 30\text{kbps}$.
 - Como podemos conseguir 56kbps?

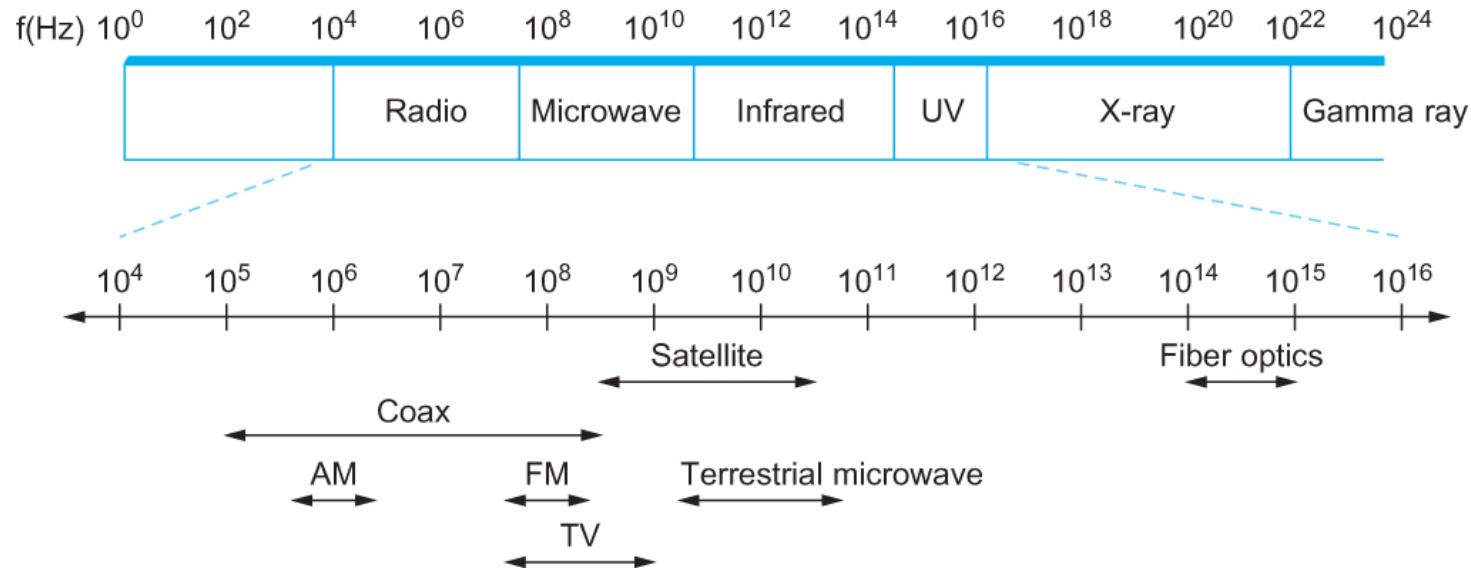
Enlaces (*Links*)

- Todos os enlaces práticos são baseados em algum tipo de radiação eletromagnética que se propaga por um meio ou, em alguns casos, pelo ar livre
- Uma maneira de se caracterizar enlaces, então, é pelo meio que eles utilizam
 - Tipicamente fios de cobre em alguma forma (como par trançado em DSL (*Digital Subscriber Line*) ou cabo coaxial,
 - Fibra óptica (como em enlaces de longa distância na Internet ou última milha de assinantes), ou
 - Ar livre (enlaces de rede sem fio)

Enlaces

- Uma outra característica importante do enlace é a *frequência*
 - Medida em Hertz com a qual as ondas eletromagnéticas oscilam.
- Distância entre pares adjacentes de máximos ou mínimos de uma onda medida em metros é chamada de *comprimento de onda (wavelength)*
 - A velocidade da luz dividida pela frequência determina o comprimento de onda.
 - A frequência em uma cabo de cobre varia de 300Hz a 3300Hz; o comprimento da onda de 300Hz é a velocidade da luz/frequência
 - $2/3 \times 3 \times 10^8 / 300 = 667 \times 10^3$ metros.
- A inserção de dados binários em um sinal é chamada de *codificação (encoding)*.
- Modulação é a modificação de sinais em termos de suas frequências, amplitudes, e fases.

Enlaces



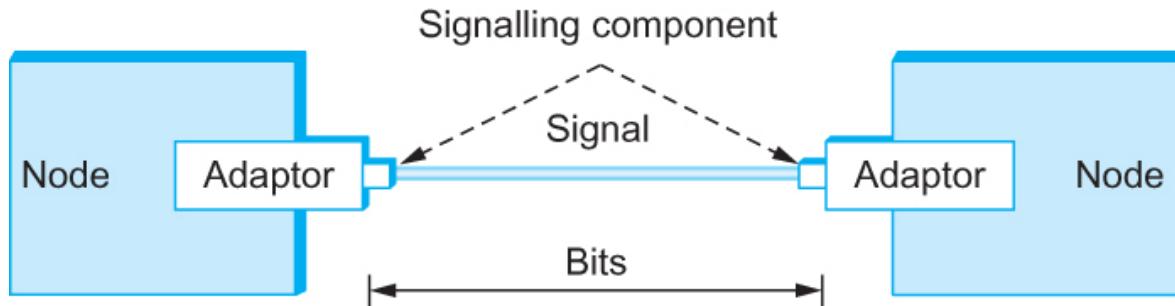
Espectro Eletromagnético

Enlaces

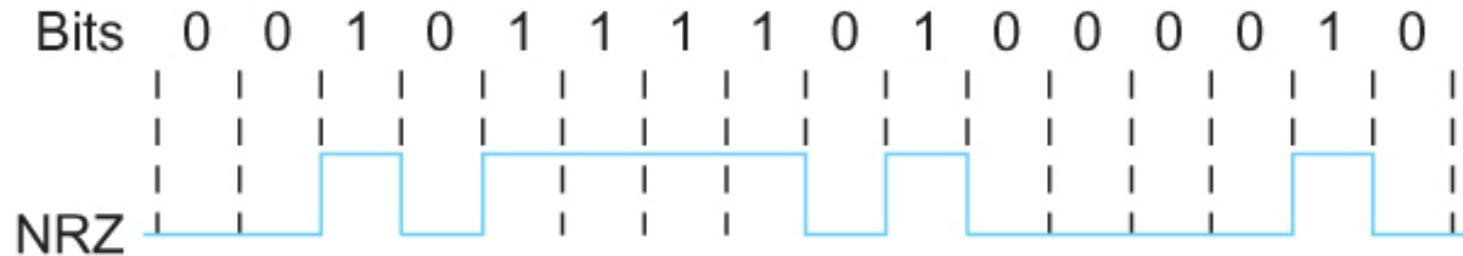
Service	Bandwidth (typical)
Dial-up	28–56 kbps
ISDN	64–128 kbps
DSL	128 kbps–100 Mbps
CATV (cable TV)	1–40 Mbps
FTTH (fibre to the home)	50 Mbps–1 Gbps

Serviços comuns disponíveis para conexão de residências

Codificação



Sinais viajam entre componentes de sinalização; bits fluem entre adaptadores



Codificação NRZ de uma cadeia de bits

Codificação

- Problemas com NRZ (*Non-Return to Zero*)
 - Perda do Sinal Base (*Baseline wander*)
 - O receptor mantém uma média dos sinais recebidos
 - Utiliza a média para distinguir entre nível baixo e alto do sinal
 - Quando o sinal é muito mais baixo que a média, ele é considerado 0, caso contrário ele é considerado 1
 - Vários 0's e 1's consecutivos fazem com que a média modifique significativamente, dificultando a detecção

Codificação

- Problemas com NRZ
 - Recuperação do Relógio (*Clock recovery*)
 - Transições frequentes entre níveis alto e baixo são necessárias para recuperação do relógio
 - Os processos de envio e recepção são guiados por um relógio (assim como o clock de um computador)
 - Em cada ciclo do relógio, o emissor transmite um bit e o receptor o recupera
 - O emissor e o receptor precisam estar sincronizados precisamente

Codificação

- NRZI
 - *Non Return to Zero Inverted*
 - Emissor faz uma transição do sinal corrente para codificar 1 e permanece no mesmo nível para codificar 0
 - Resolve o problema de 1's consecutivos

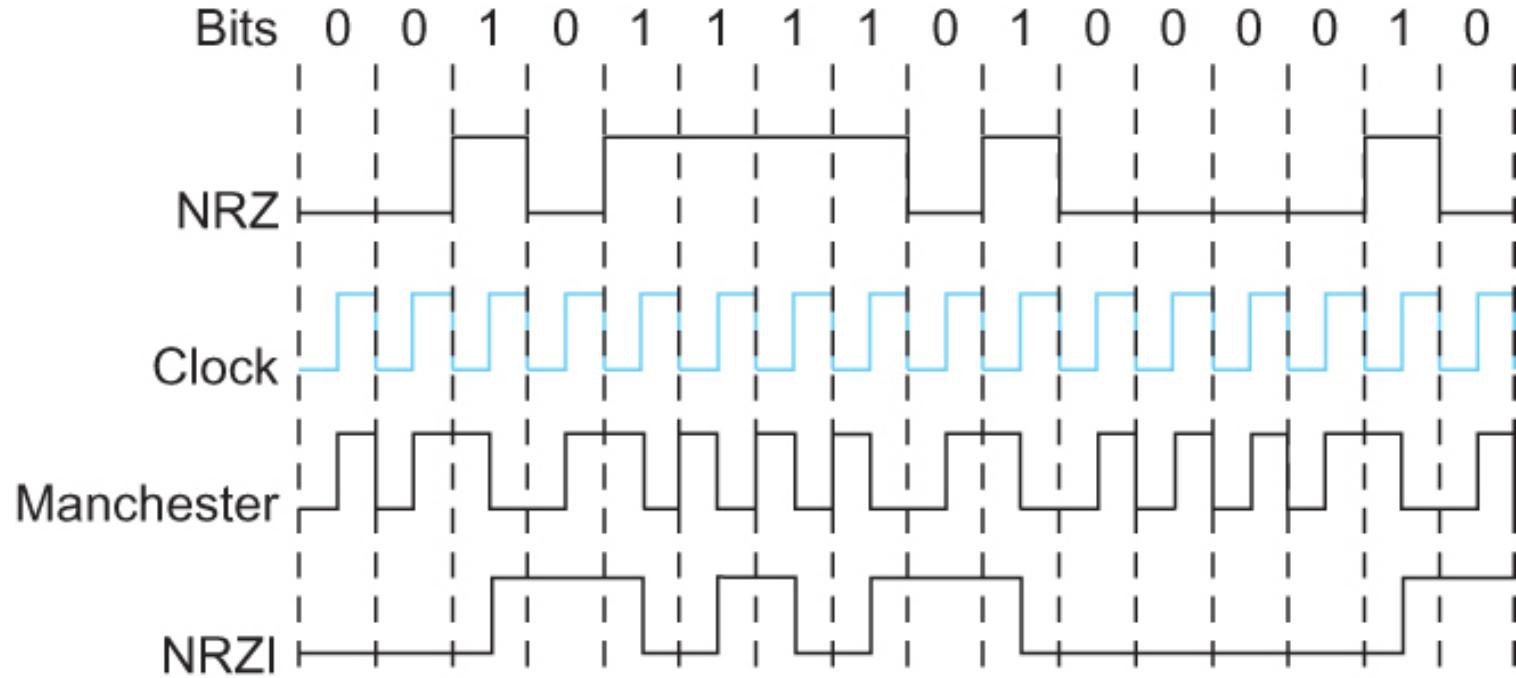
Codificação

- Codificação Manchester
 - Combina o relógio com o sinal enviando OU exclusivo dos dados codificados em NRZ e os níveis do relógio
 - Relógio gera um sinal interno que altera de baixo para alto (um par alto/baixo é considerado um ciclo de relógio)
 - Na codificação Manchester
 - 0: low → high transition
 - 1: high → low transition

Codificação

- Problemas com a codificação Manchester
 - Dobra a taxa de transição do sinal no enlace
 - A taxa em que o sinal muda é chamada de taxa de *baud* do enlace
 - Na codificação Manchester, a taxa de bits é metade da taxa de *baud*

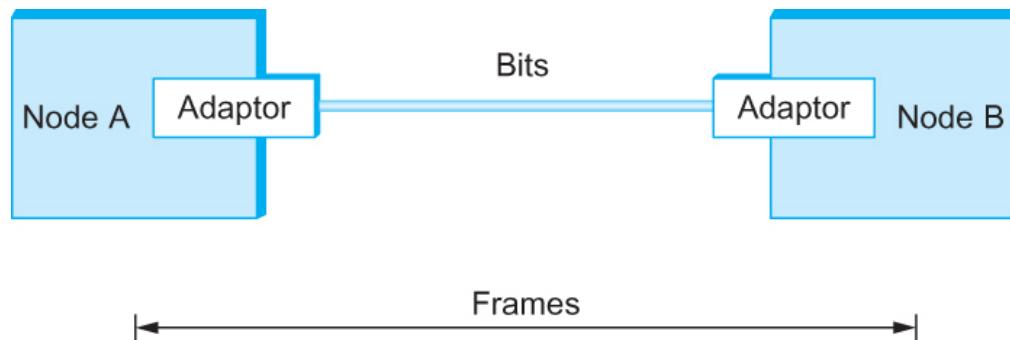
Codificação



Diferentes estratégias de codificação

Enquadramento (*Framing*)

- Nosso foco é em redes comutadas por pacotes, o que significa que blocos de dados (chamados *quadros* – *frames*), e não cadeia de bits, são trocados entre os nós.
- É o adaptador de rede que possibilita a troca de quadros.



Bits fluem entre adaptadores, mas quadros entre nós

Enquadramento

- Quando um nó A deseja transmitir um quadro para um nó B, ele diz ao adaptador para transmitir o quadro que está em sua memória. Isso resulta em sequência de bits enviada no enlace.
- O adaptador no nó B então coleta a sequência de bits que chega no enlace e coloca o quadro correspondente na memória do nó B.
- Saber exatamente qual o conjunto de bits que forma um quadro—ou seja, determinar onde o quadro começa e termina—é o principal desafio enfrentado pelo adaptador.

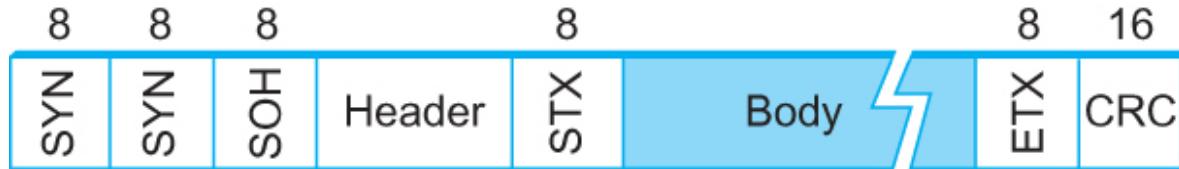
Enquadramento

- Protocolos orientados a Byte
 - Trata cada quadro como uma coleção de bytes (characters) ao invés de bits
 - BISYNC (Binary Synchronous Communication) Protocol
 - Desenvolvido pela IBM (final da década de 1960)
 - DDCMP (Digital Data Communication Protocol)
 - Utilizado na DECNet

Enquadramento

- BISYNC – abordagem de sentinela
 - Quadros são transmitidos a partir do campo mais a esquerda
 - Início do quadro é marcado por um caracter especial SYN (*synchronize*)
 - Parte de dados do quadro está contida entre os caracteres sentinelas especiais STX (start of text) e ETX (end of text)
 - SOH : Start of Header
 - DLE : Data Link Escape (*character or byte stuffing*)
 - CRC: Cyclic Redundancy Check

Enquadramento

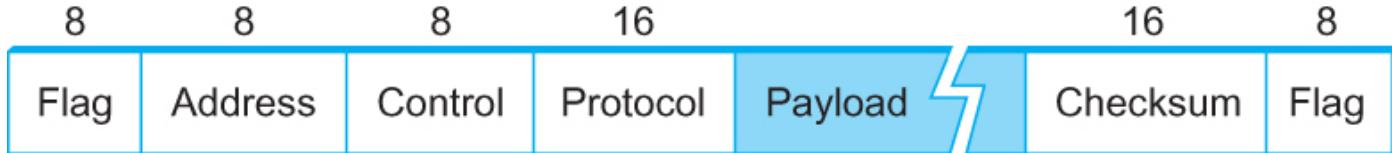


Formato do quadro BISYNC

Enquadramento

- PPP (*Point-to-Point Protocol*), que é utilizado em enlaces da Internet, utiliza a abordagem de sentinela
 - Flag especial para início
 - 0 1 1 1 1 1 1 0
 - Address, control: default numbers
 - Protocol para demultiplexação: IP / IPX
 - Payload: negociado (1500 bytes)
 - Checksum: para detecção erros

Enquadramento

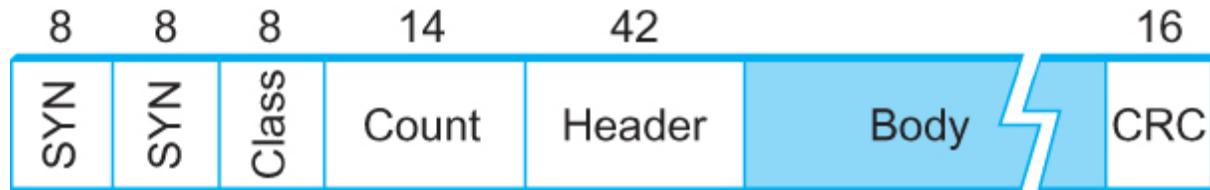


Formato do quadro PPP

Enquadramento

- Abordagem de contagem de Bytes
 - DDCMP
 - *count*: quantos bytes estão contidos no quadro
 - Se *count* for corrompido
 - Erro de enquadramento (*Framing error*)

Enquadramento



Formato do quadro DDCMP

Enquadramento

- Protocolos orientados a Bits
 - HDLC : High Level Data Link Control
 - Sequência de Início e Fim

0 1 1 1 1 1 0



Formato do quadro HDLC

Enquadramento

- Protocolo HDLC
 - No envio, quando uma sequência de cinco 1s consecutivos tiver de ser transmitida no corpo da mensagem
 - O emissor envia um 0 (zero) antes de transmitir o próximo bit
 - Técnica conhecida por *bit stuffing*

Enquadramento

■ Protocolo HDLC

■ No lado do receptor

■ 5 1s consecutivos

■ Próximo bit 0 : Stuffed, descarte-o

1 : Marcador de fim do quadro

OU Erro foi introduzido na cadeia de bits

Olhe para o próximo bit

Se 0 (01111110) → Marcador de fim de quadro

Se 1 (01111111) → Erro, descarte o quadro inteiro

O receptor precisa esperar pelo
próximo 01111110 antes de

receber um quadro novamente

Detecção de Erros

- Erros em bits acontecem em quadros
 - Por causa de interferências elétricas ou ruídos térmicos
- Detecção de Erro
- Correção de Erro
- Duas abordagens quando o receptor detecta um erro
 - Notifica o emissor que a mensagem está corrompida para que o emissor possa reenviá-la.
 - Usa algum algoritmo de detecção e correção de erro para que o receptor reconstrua a mensagem

Detecção de Erros

- Técnicas comuns para detecção de erros de transmissão
 - CRC (Cyclic Redundancy Check)
 - Usado em HDLC, DDCMP, CSMA/CD, Token Ring
 - Outras abordagens
 - Paridade Bi-Dimensional (BISYNC)
 - Checksum (IP)

Detecção de Erros

- Ideia básica da detecção de erros
 - Adicionar informação redundante em um quadro que possa ser usada para determinar se algum erro ocorreu
 - Imagine (Caso Extremo)
 - Transmite duas cópias dos dados
 - Idênticas → Sem erro
 - Diferentes → Erro
 - Esquema pobre???
 - Mensagem com n bits requer n bits de informação redundante
 - Erros podem não ser detectados
 - Em geral, é possível oferecer técnicas mais fortes
 - k bits redundantes, mensagem com n bits, $k \ll n$
 - Em Ethernet, um quadro com até 12.000 bits de dados requer apenas um código CRC de 32 bits

Detecção de Erros

- Bits extras são redundantes
 - Eles não adicionam novas informações a mensagem
 - Derivados da mensagem original utilizando algum algoritmo
 - Tanto emissor quanto receptor conhecem o algoritmo

Emissor



Receptor



Receptor calcula r usando m

Se eles são diferentes, há erro

Se eles são iguais, assume que não há erro

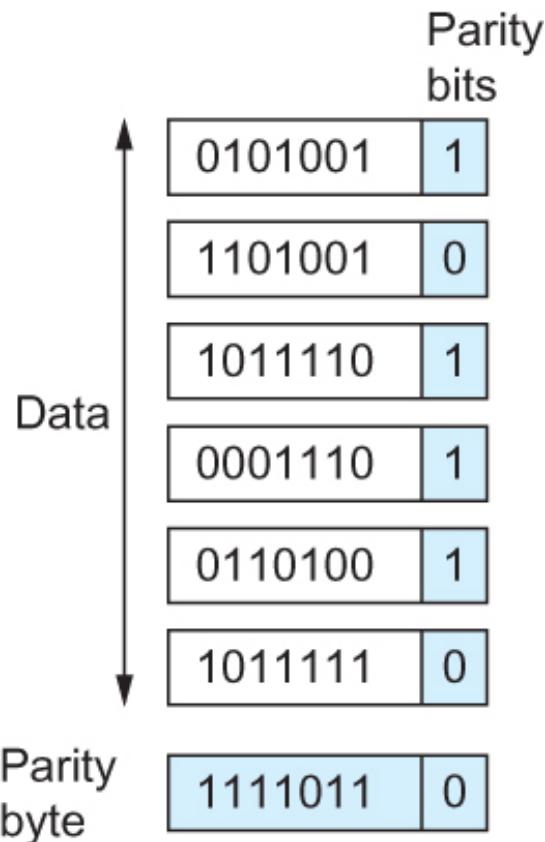
Paridade Bi-Dimensional

- Paridade bi-dimensional é exatamente o que o nome sugere
- É baseada em paridade simples (unidimensional), que consiste em adicionar um bit extra a um conjunto de 7 bits para balancear o número de 1s no byte. Por exemplo,
 - Paridade ímpar atribui 1 ao oitavo bit se necessário para tornar o número de 1s no byte ímpar, e
 - Paridade par atribui 1 ao oitavo bit se necessário para tornar o número de 1s no byte par.

Paridade Bi-Dimensional

- Paridade bi-dimensional faz um cálculo semelhante para cada posição de bit dos bytes contidos em um quadro
- Isso resulta em um byte extra de paridade para o quadro inteiro, além de um bit de paridade para cada byte.
- Paridade bi-dimensional detecta todos os erros de 1, 2 e 3 bits e a maioria dos erros de 4 bits

Paridade Bi-Dimensional



Paridade bi-dimensional

Algoritmo de Checksum da Internet

- Não é utilizado na camada de enlace
- Adiciona todas as palavras (16 bits) que são transmitidas e então transmite o resultado da soma
 - O resultado é chamado *checksum* (soma verificadora)
- O receptor realiza o mesmo cálculo nos dados recebidos e compara o resultado com o checksum recebido
- Se qualquer dado transmitido, incluindo o próprio checksum, é corrompido, então os resultados não batem e o receptor sabe que algum erro ocorreu

Algoritmo de Checksum da Internet

- Considera os dados sendo transmitidos como uma sequência de inteiros de 16 bits (palavras).
- Adiciona as palavras utilizando aritmética de complemento de um e depois calcula o complemento de um do resultado.
- O último número de 16 bits calculado é o checksum.

Algoritmo de Checksum da Internet

- Em aritmética de complemento de um, um inteiro negativo $-x$ é representado como o complemento de x ;
 - Cada bit de x é invertido.
- Quando adicionar número em aritmética de complemento de um, o vai um (*carry*) precisa ser adicionado ao resultado.

Algoritmo de Checksum da Internet

- Considere, por exemplo, a adição de -5 e -3 em aritmética de complemento de um com inteiros de 4 bits
 - $+5$ é 0101, e -5 é 1010; $+3$ é 0011, e -3 é 1100
- Se adicionarmos 1010 e 1100 ignorando o *carry*, obteremos 0110
- Em aritmética de complemento de um, o fato da operação ter causado um *carry* do bit mais significativo exige que o resultado seja incrementado, resultando em 0111, que é a representação em complemento de um de -8 , como esperavamos.

Cyclic Redundancy Check (CRC)

- Reduz o número de bits extras e maximiza a proteção.
- Dada a cadeia de bits 110001, podemos associar um polinômio de uma única variável x a ela.

$$1 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0 = x^5 + x^4 + 1 \text{ cujo grau é } 5.$$

Um quadro de k bits tem grau máximo de $k-1$

- Seja $M(x)$ o polinômio associado à mensagem e $G(x)$ um polinômio gerador.

Cyclic Redundancy Check (CRC)

- Digamos que $M(x)/G(x)$ gere um resto 0.
- Quando $M(x)$ é enviado e $M'(x)$ é recebido, temos $M'(x) = M(x)+E(x)$
- O receptor calcula $M'(x)/G(x)$ e se o resto for diferente de zero, então algum erro ocorreu.
- A única coisa que o emissor e o receptor precisam compartilhar é $G(x)$.

Cyclic Redundancy Check (CRC)

Aritmética Polinomial Modulo 2

- Qual polinômio $B(x)$ pode ser dividido por um divisor polinomial $G(x)$ se $B(x)$ for de grau maior do que $G(x)$.
- Qualquer polinômio $B(x)$ pode ser dividido uma vez por um divisor polinomial $G(x)$ se $B(x)$ for do mesmo grau de $G(x)$.
- O resto da divisão de $B(x)$ por $G(x)$ é obtido subtraindo $G(x)$ de $B(x)$.
- Para subtrair $G(x)$ de $B(x)$, nós realizamos simplesmente a operação de OU-exclusivo (XOR) em cada par de coeficientes equivalentes.

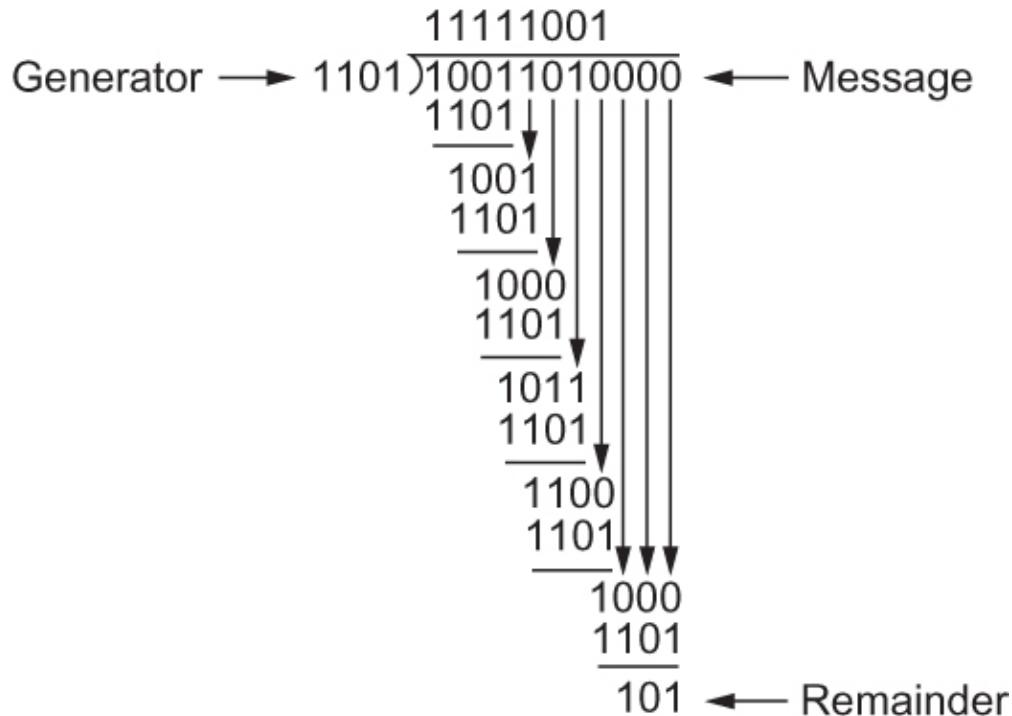
Cyclic Redundancy Check (CRC)

- Seja $M(x)$ um quadro com m bits e um polinômio gerador com menos do que m bits.
- Seja r o grau de $G(x)$. Adicione r bits zero na porção menos significativa do quadro de modo que ele contenha $m+r$ bits e corresponda ao polinômio $x^rM(x)$.

Cyclic Redundancy Check (CRC)

- Divila a cadeia de bits correspondente a $x^rM(x)$ pela cadeia de bits correspondente a $G(x)$ usando divisão módulo 2.
- Subtraia o resto (que possui sempre r ou menos bits) da cadeia correspondente a $x^rM(x)$ usando subtração módulo 2 (adição e subtração são as mesmas operações em módulo 2).
- O resultado é o quadro com checksum a ser transmitido. Chame esse quadro de $M'(x)$.

Cyclic Redundancy Check (CRC)



Cálculo de CRC usando Divisão Polinomial Longa

Cyclic Redundancy Check (CRC)

- Propriedades de Polinômio Gerador
 - Seja $P(x)$ a representação do que o emissor envia e $P(x) + E(x)$ a cadeia recebida. Um valor 1 em $E(x)$ representa que o bit na posição correspondente em $P(x)$ foi invertido.
 - Sabemos que $P(x)/G(x)$ gera um resto 0. mas se $E(x)/G(x)$ também gera um resto 0, então ou $E(x) = 0$ ou $G(x)$ é um fator de $E(x)$.
 - Quando $G(x)$ é um fator de $E(x)$, temos um problema, pois erros não são detectados.
 - Se há erro em um único bit, então $E(x) = x^i$, em que i determina o bit errado. Se $G(x)$ contém dois ou mais termos, ele jamais dividirá $E(x)$. Portanto, todos os erros em um único bit serão detectados.

Cyclic Redundancy Check (CRC)

- Propriedades de Polinômio Gerador
 - Em geral, é possível provar que os seguintes tipos de erro podem ser detectados se $G(x)$ tiver as propriedades listadas
 - Todos os erros de um único bit desde que x^k e x^0 possuam coeficientes diferentes de zero.
 - Todos os erros de dois bits desde que $G(x)$ tenha um fator com pelo menos três termos.
 - Qualquer número de erros ímpar desde que $G(x)$ contenha o fator $(x+1)$.
 - Qualquer erro de “rajada” (i.e., sequência de erros consecutivos) desde que o comprimento da rajada seja menor do que k bits. (A maioria dos erros de rajada maiores do que k bits também pode ser detectada.)

Cyclic Redundancy Check (CRC)

- Seis polinômios geradores que se tornaram padrões internacionais:
 - $\text{CRC-8} = x^8 + x^2 + x + 1$
 - $\text{CRC-10} = x^{10} + x^9 + x^5 + x^4 + x + 1$
 - $\text{CRC-12} = x^{12} + x^{11} + x^3 + x^2 + x + 1$
 - $\text{CRC-16} = x^{16} + x^{15} + x^2 + 1$
 - $\text{CRC-CCITT} = x^{16} + x^{12} + x^5 + 1$
 - $\text{CRC-32} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Transmissão Confiável

- CRC é utilizado para detectar erros.
- Alguns códigos são fortes o suficiente para corrigir erros.
- O overhead é tipicamente muito alto.
- Quadros com erro devem ser descartados.
- Um protocolo de enlace que deseja garantir entrega de quadros deve fazer a recuperação dos quadros descartados
- Isso é possível utilizando a combinação de dois mecanismos fundamentais
 - Confirmações (*Acknowledgements*) e Timeouts

Transmissão Confiável

- Uma confirmação (*acknowledgement* – ACK) é um pequeno quadro de controle que o protocolo envia de volta para o seu par dizendo que o quadro enviado anteriormente foi recebido.
 - Um quadro de controle é um quadro com cabeçalho apenas (i.e., sem dados).
- O recebimento de um ACK indica ao emissor do quadro original que o quadro foi entregue com sucesso.

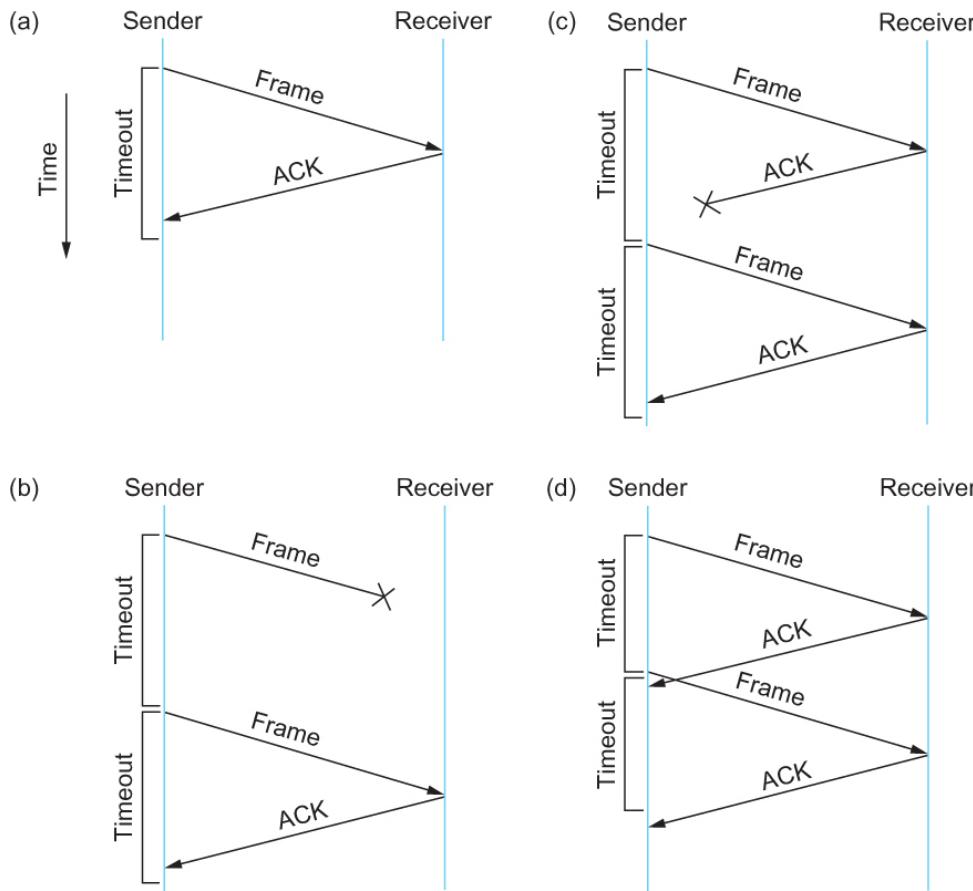
Transmissão Confiável

- Se o emissor não receber o ACK depois de um tempo razoável, ele deve retransmitir o quadro original.
- A ação de esperar por um tempo razoável é chamada de *timeout*.
- A estratégia geral de se utilizar ACKs e timeouts para se implementar entrega confiável é chamada de *Automatic Repeat reQuest (ARQ)*.

Protocolo Stop and Wait

- A ideia do protocolo stop and wait é bem simples
 - Depois de transmitir um quadro, o emissor espera por um ACK antes de transmitir o próximo quadro.
 - Se o ACK não chegar dentro de um certo período de tempo, o emissor “timeout” e retransmite o quadro original.

Protocolo Stop and Wait

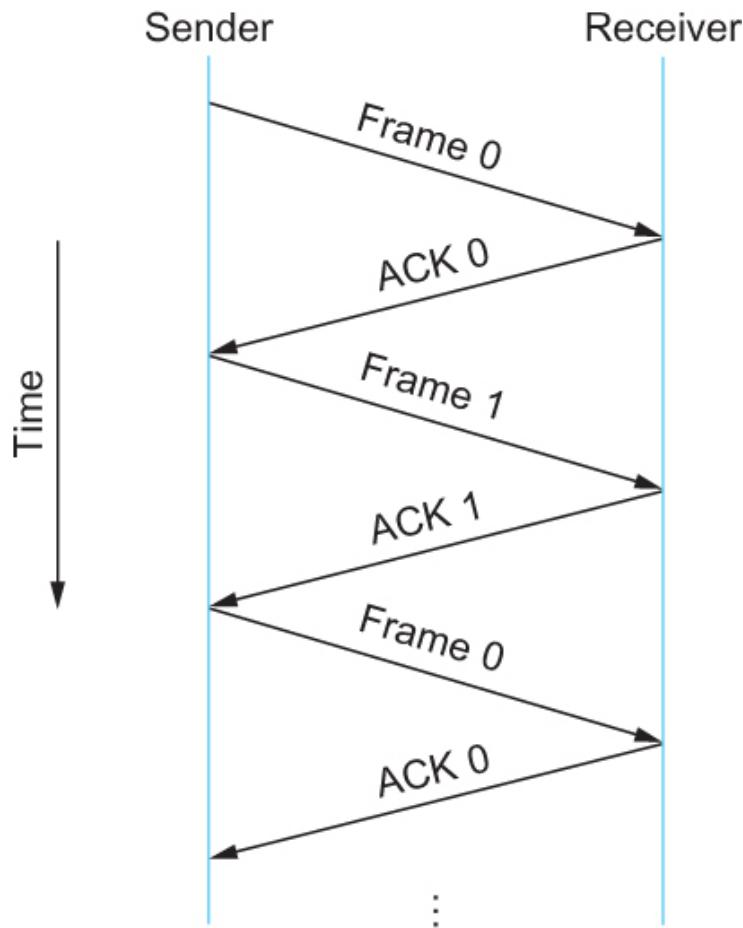


Linha do tempo mostrando quatro cenários diferentes do protocolo stop and wait.
(a) O ACK é recebido antes do timeout expirar; (b) o quadro original é perdido;
(c) o ACK é perdido; (d) o timeout expira antes do ACK chegar

Protocolo Stop and Wait

- Se o ACK for perdido ou chegar atrasado
 - O timer do emissor expira e o emissor retransmite o quadro original, mas o receptor pensará que é o próximo quadro, pois ele recebeu e confirmou o primeiro quadro
 - Como resultado, cópias duplicadas do quadro serão entregues
- Como resolver esse problema?
 - Use um número de sequência de 1 bit (0 ou 1)
 - Quando o emissor retransmite o quadro 0, o receptor pode determinar que está recebendo uma segunda cópia do quadro 0 ao invés da primeira cópia do quadro 1 e, portanto, pode ignorá-lo (o receptor ainda confirma a recepção caso o ACK tenha sido perdido)

Protocolo Stop and Wait

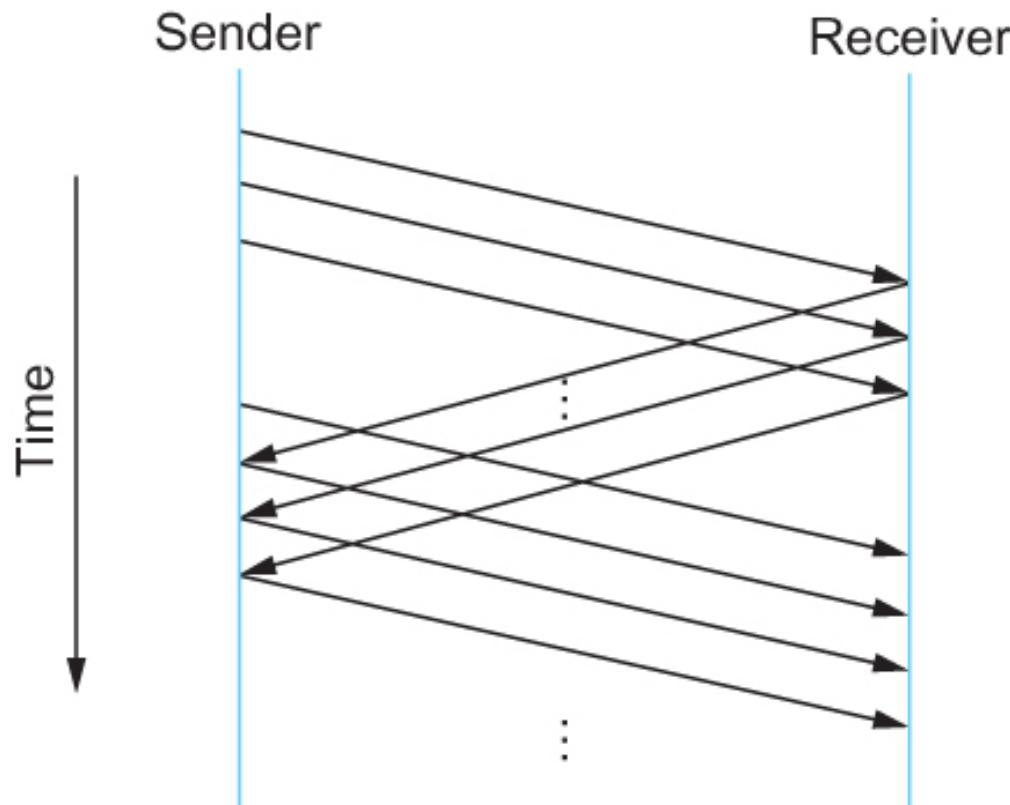


Linha do tempo para stop-and-wait com número de sequência de 1-bit

Protocolo Stop and Wait

- O emissor possui apenas um quadro em trânsito no enlace por vez
 - Isso pode ser bem inferior a capacidade do enlace
- Considere um enlace de 1.5 Mbps com RTT de 45 ms
 - O enlace possui produto atraso \times largura_de_banda de 67.5 Kb ou aproximadamente 8 KB
 - Como o emissor pode enviar apenas um quadro por RTT e assumindo um quadro de tamanho 1 KB
 - Taxa Máxima de Envio
 - Bits per frame \div Time per frame = $1024 \times 8 \div 0.045 = 182$ Kbps
Ou aproximadamente um oitavo da capacidade do enlace
 - Para usar toda a capacidade do enlace, o emissor deve então transmitir até oito quadros antes de ter de esperar por um ACK

Protocolo de Janela Deslizante (*Sliding Window*)



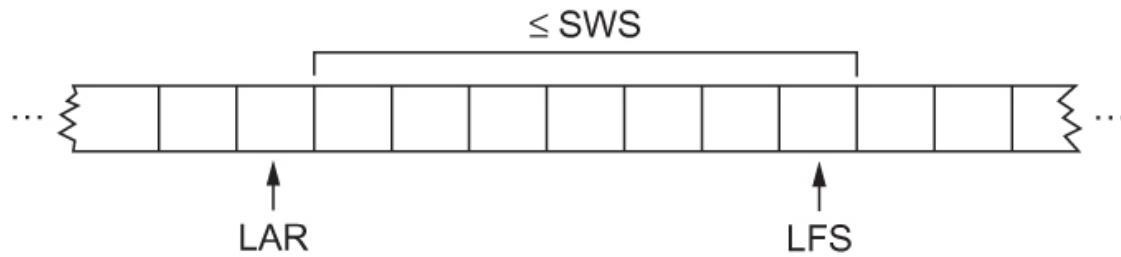
Linha do tempo para o protocolo de janela deslizante

Protocolo de Janela Deslizante (*Sliding Window*)

- O emissor atribui um número de sequência (SeqNum) a cada quadro.
 - Assuma que ele cresça sem limites (até o infinito)
- O emissor mantém três variáveis
 - Tamanho da Janela do Emissor (*Sending Window Size (SWS)*)
 - Limite máximo de quadro em trânsito (sem confirmação) que o emissor pode transmitir
 - Último ACK recebido (*Last Acknowledgement Received (LAR)*)
 - Número de sequência do último ACK recebido
 - Último quadro enviado (*Last Frame Sent (LFS)*)
 - Número de sequência do último quadro enviado

Protocolo de Janela Deslizante (*Sliding Window*)

- O emissor também mantém a seguinte invariante
 $LFS - LAR \leq SWS$



Janela Deslizante no Emissor

Protocolo de Janela Deslizante (*Sliding Window*)

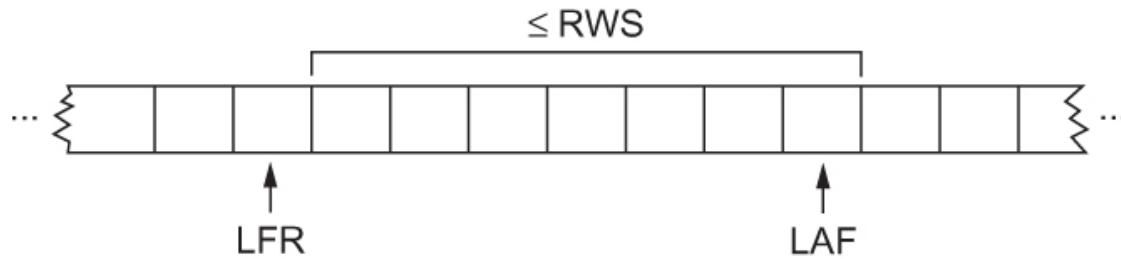
- Quando um ACK chega
 - O emissor move LAR para a direita, permitindo que o emissor transmita um novo quadro
- O emissor também associa um temporizador com cada quadro que ele transmite
 - O emissor retransmite o quadro quando o temporizador expira antes do ACK ser recebido
- Note que o emissor precisa armazenar (buffer) até SWS quadros
 - Por que?

Protocolo de Janela Deslizante (*Sliding Window*)

- O receptor mantém três variáveis
 - Tamanho da Janela do Receptor (*Receiving Window Size (RWS)*)
 - Limite superior no número de quadros fora de ordem que o receptor pode aceitar
 - Maior Quadro Aceitável (*Largest Acceptable Frame (LAF)*)
 - Número de sequência do maior quadro aceitável
 - Último Quadro Recebido (*Last Frame Received (LFR)*)
 - Número de sequência do último quadro recebido

Protocolo de Janela Deslizante (*Sliding Window*)

- O receptor também mantém a seguinte invariante
 $LAF - LFR \leq RWS$



Janela Deslizante no Receptor

Protocolo de Janela Deslizante (*Sliding Window*)

- Quando um quadro com número de sequência SeqNum chega, o que o receptor deve fazer?
 - If $\text{SeqNum} \leq \text{LFR}$ or $\text{SeqNum} > \text{LAF}$
 - Descarte-o (o quadro está fora da janela do receptor)
 - If $\text{LFR} < \text{SeqNum} \leq \text{LAF}$
 - Aceite-o
 - Agora, o receptor precisa decidir se envia ou não um ACK

Protocolo de Janela Deslizante (*Sliding Window*)

- Seja SeqNumToAck
 - O maior número de sequência ainda não confirmado tal que todos os quadros com números de sequência menor ou igual a SeqNumToAck já tenham sido recebidos.
- O receptor confirma o recebimento de SeqNumToAck mesmo que quadros com números de sequência maiores tenham sido recebidos
 - Essa confirmação é conhecida como cumulativa.
- O receptor então atribui
 - LFR = SeqNumToAck e ajusta
 - LAF = LFR + RWS

Protocolo de Janela Deslizante (*Sliding Window*)

Por exemplo, suponha LFR = 5 e RWS = 4

(i.e., o último ACK que o receptor enviou foi para o númer. de seq. 5)

⇒ LAF = 9

Se os quadros 7 e 8 chegarem, eles serão armazenados (buffered) porque eles estão dentro da janela do receptor

Mas nenhum ACK será enviado, uma vez que o quadro 6 ainda não chegou

Quadros 7 e 8 estão fora de ordem

Quadro 6 chega (ele está atrasado porque foi perdido na primeira vez e teve de ser retransmitido)

Agora o receptor confirma o recebimento do quadro 8 e muda LFR para 8 e LAF para 12

Problemas com o protocolo de Janela Deslizante

- Quando um timeout ocorre, a quantidade de dados diminui
 - Porque o emissor não pode avançar sua janela
- Quando uma perda de pacote ocorre, este esquema não mantém o “cano” cheio
 - Quanto mais tempo se leva para detectar a perda de um quadro, mais severos os problemas se tornam
- Como melhorar isso?
 - Negative Acknowledgement (NAK)
 - Additional Acknowledgement
 - Selective Acknowledgement

Problemas com o protocolo de Janela Deslizante

- Negative Acknowledgement (NAK)
 - O receptor envia um NAK para o quadro 6 quando o quadro 7 chega (no exemplo anterior)
 - Entretanto, isso é desnecessário, pois o mecanismo de timeout do emissor será suficiente para detectar essa situação
- Additional Acknowledgement
 - O receptor envia ACK adicional para o quadro 5 quando o quadro 7 chega
 - O emissor usa ACKs duplicados como uma pista para perda de quadros
- Selective Acknowledgement
 - O receptor confirmará exatamente os quadros que ele recebeu, ao invés do de número mais alto
 - O receptor confirmará os quadros 7 e 8
 - O emissor saberá que o quadro 6 foi perdido
 - O emissor pode manter o “cano” cheio, mas a complexidade de implementação aumenta

Problemas com o protocolo de Janela Deslizante

Como selecionar o tamanho da janela

- SWS é fácil de calcular
 - Delay \times Bandwidth
 - RWS pode ser qualquer valor
 - Dois casos comuns
 - RWS = 1
 - Nenhum buffer no receptor para quadros que chegam fora de ordem
 - RWS = SWS
 - O receptor pode armazenar os quadros que o emissor transmite
- Não faz sentido manter RWS > SWS
- Por que?

Problemas com o protocolo de Janela Deslizante

■ Número de Sequência Finito

- O número de sequência do quadro é especificado em um campo do cabeçalho
 - Tamanho finito
 - 3 bits: oito números possíveis: 0, 1, 2, 3, 4, 5, 6, 7
 - É necessário se preocupar com overflow (*wrap around*)

Problemas com o protocolo de Janela Deslizante

- Como distinguir entre duas encarnações diferentes do mesmo número de sequência?
 - O número de possíveis números de sequência deve ser maior que a quantidade de quadros que podem estar em trânsito
 - Stop and Wait: Um quadro em trânsito
 - 2 números de sequência distintos (0 e 1)
 - Seja MaxSeqNum a quantidade de números de sequência disponíveis
 - $SWS + 1 \leq \text{MaxSeqNum}$
 - Isso é suficiente?

Problemas com o protocolo de Janela Deslizante

$SWS + 1 \leq \text{MaxSeqNum}$

- Isso é suficiente?

- Depende de RWS
- If $RWS = 1$, then suficiente
- If $RWS = SWS$, then não é suficiente
- Por exemplo, se tivermos oito números de sequência

0, 1, 2, 3, 4, 5, 6, 7

$RWS = SWS = 7$

O emissor envia 0, 1, ..., 6

O receptor recebe 0, 1, ..., 6

O receptor confirma 0, 1, ..., 6

ACK (0, 1, ..., 6) são perdidos

O emissor retransmite 0, 1, ..., 6

O receptor está esperando 7, 0, ..., 5

Problemas com o protocolo de Janela Deslizante

Para evitar esse problema,

If RWS = SWS

$$\text{SWS} < (\text{MaxSeqNum} + 1)/2$$

Problemas com o protocolo de Janela Deslizante

- A janela deslizante serve para três propósitos diferentes
 - Confiabilidade
 - Preservação da ordem
 - Cada quadro possui um número de sequência
 - O receptor não passa um quadro para a camada superior até que ele tenha passado todos os quadros com números de sequência menores
 - Controle de fluxo
 - O receptor pode diminuir a taxa de envio do emissor (*throttle*)
 - Previne que o emissor sobrecarregue o receptor ao transmitir mais dados que o receptor é capaz de processar

Ethernet

- A tecnologia de rede local de maior sucesso dos últimos 20 anos.
- Desenvolvida em meados de 1970 por pesquisadores do Xerox Palo Alto Research Center (PARC).
- Utiliza tecnologia CSMA/CD
 - Carrier Sense Multiple Access with Collision Detection.
 - Um conjunto de nós envia e recebe quadros sobre um meio compartilhado.
 - *Carrier sense* significa que todos os nós podem distinguir entre um enlace ocupado e ocioso.
 - Detecção de colisão significa que um nó escuta enquanto transmite e pode, portanto, detectar quando um quadro que ele está transmitindo colide com um quadro transmitido por um outro nó.

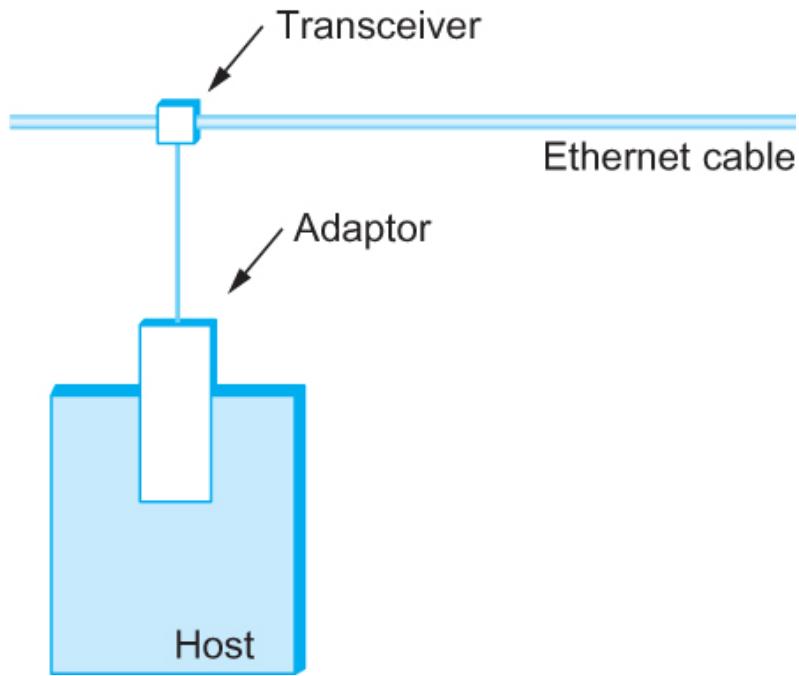
Ethernet

- Utiliza o protocolo ALOHA (*packet radio network*) como seu base para o seu protocolo.
 - Desenvolvido na universidade do Havai para suportar transmissões entre as ilhas havainas.
 - Para ALOHA o meio era a atmosfera, para Ethernet o meio é um cabo coaxial.
- DEC e Intel se juntaram a Xerox para definir um padrão Ethernet de 10 Mbps em 1978 (DIX).
- Esse padrão formou a base para o padrão IEEE 802.3.
- Mais recentemente, o padrão 802.3 foi estendido para incluir uma versão de 100 Mbps chamada Fast Ethernet and uma versão de 1000 Mbps chamada Gigabit Ethernet (Hoje 10 e 40 Gbps já são comuns. Em breve, Ethernet a 100 Gbps deve se tornar acessível).

Ethernet

- Um segmento Ethernet é implementado em um cabo coaxial de até 500 m.
 - Esse cabo é semelhante ao tipo utilizado em TV a cabo exceto que sua impedância é de 50 ohms ao invés de 75 ohms do cabo de TV.
- Hosts se conectam ao segmento Ethernet por interposição no cabo.
- Um *transceiver* detecta quando a linha está ociosa e codifica os dados quando o host está transmitindo.
- O *transceiver* também recebe sinais transmitidos no segmento.
- O *transceiver* é conectado ao adaptador Ethernet que esta conectado em um host.
- O protocolo é implementado no adaptador.

Ethernet

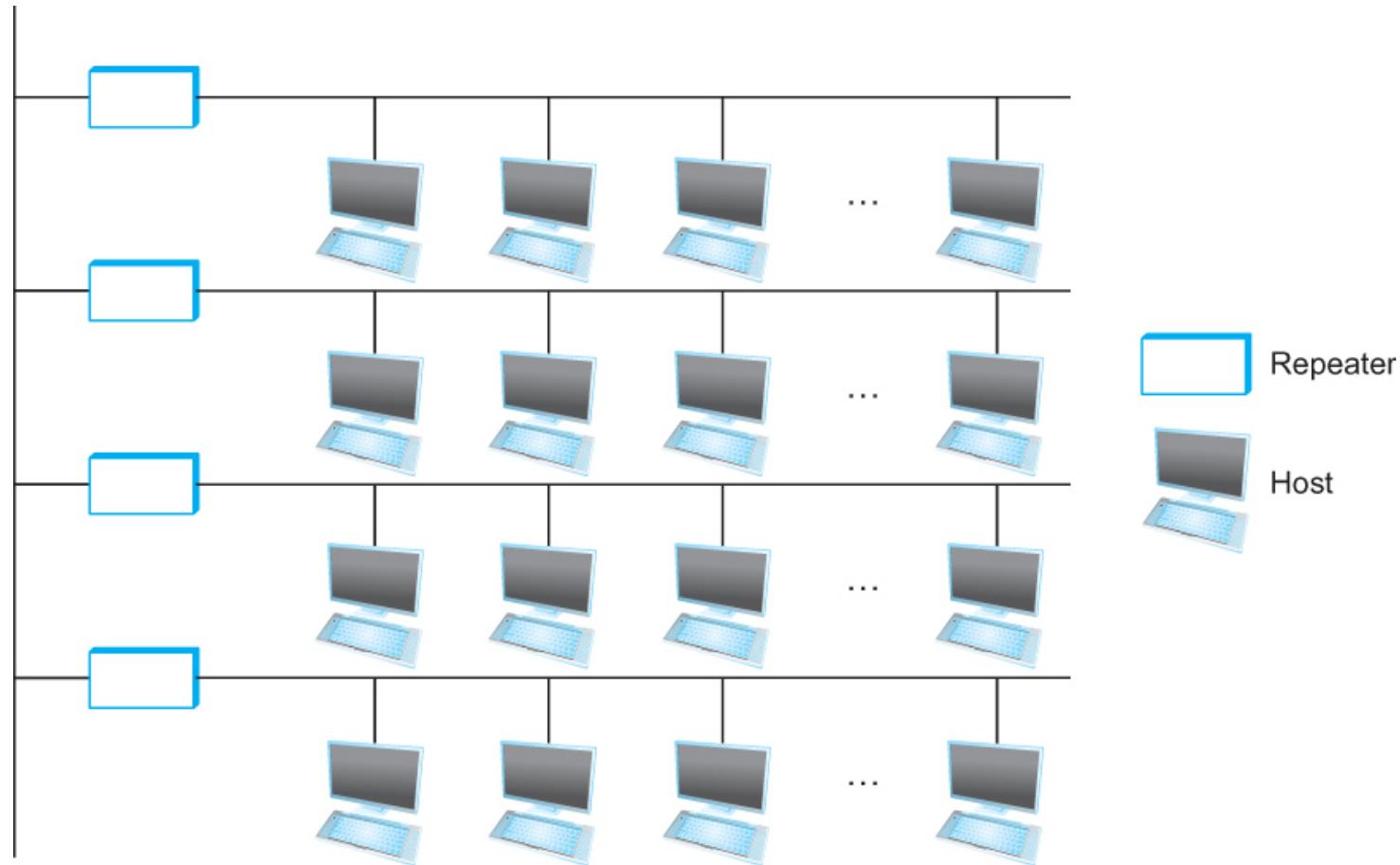


Transceiver e adaptador Ethernet.

Ethernet

- Múltiplos segmentos Ethernet podem ser conectados por *repetidores (repeaters)*.
- Um *repetidor* é um dispositivo que simplesmente repassa os sinais digitais.
- Não mais do que quatro repetidores podem ser posicionados entre qualquer par de hosts.
 - Uma rede Ethernet possui, portanto, um comprimento máximo de apenas 2500 m.

Ethernet



Repetidores Ethernet.

Ethernet

- Qualquer sinal transmitido por um host em uma rede Ethernet é enviado para toda a rede (broadcast).
 - O sinal é propagado em ambas direções.
 - Os repetidores repassam o sinal para todos os outros segmentos
 - Os terminadores conectados ao final de cada segmento absorvem o sinal.
- Ethernet utiliza codificação Manchester.

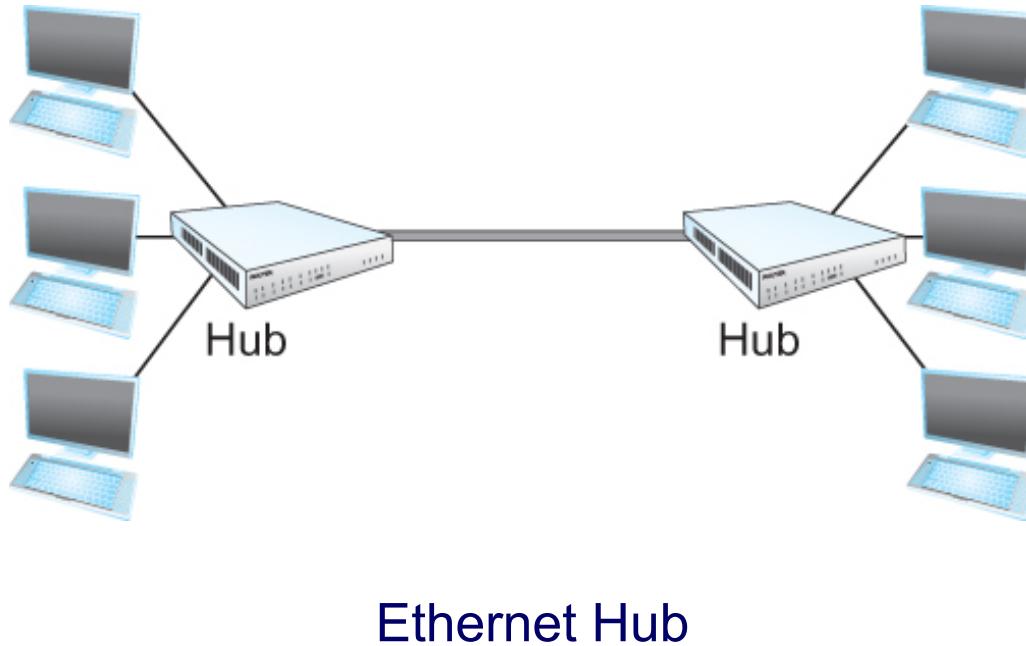
Ethernet

- Novas tecnologias em Ethernet
 - Ao invés de usar cabo coaxial, uma rede Ethernet pode ser construída com um cabo mais fino conhecido como 10Base2 (o original era 10Base5)
 - 10 significa que a rede opera a 10 Mbps
 - Base significa que o cabo é usado em um sistema de banda base
 - 2 significa que um dado segmento não pode ser maior do que 200 m

Ethernet

- Novas tecnologias em Ethernet
 - Uma outra tecnologia de cabo é a 10BaseT
 - T significa par trançado (*twisted pair*)
 - Limitada a 100 m de comprimento
 - Com 10BaseT, a configuração comum é ter vários segmento ponto-a-ponto saindo de um repetidor multiponto, chamado *Hub*

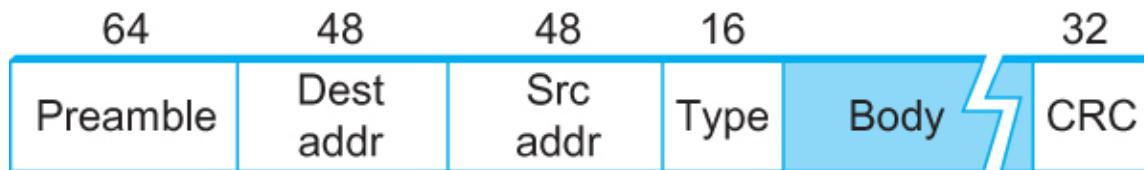
Ethernet



Protocolo de Acesso Ethernet

- O algoritmo é chamado de Controle de Acesso ao Meio Ethernet (*Ethernet's Media Access Control (MAC)*).
 - É implementado em Hardware no adaptador de rede.
- Formato do quadro
 - Preâmbulo (64 bits): permite que o receptor sincronize com o sinal (sequência alternada de 0s e 1s).
 - Endereços de origem e destino (48 bits cada).
 - Tipo do pacote (16 bits): age como uma chave de demultiplexação para identificar o protocolo de nível acima.
 - Dados (até 1500 bytes)
 - Um quadro deve conter no mínimo 46 bytes de dados.
 - O quadro deve ser grande o suficiente para se detectar colisões.
 - CRC (32 bits)

Quadro Ethernet



Formato do quadro Ethernet

Endereços Ethernet

- Cada host em uma rede Ethernet (de fato, cada host Ethernet no mundo) possui um endereço Ethernet único.
- O endereço pertence ao adaptador e não ao host.
 - É geralmente gravado em ROM.
- Endereços Ethernet são geralmente representados em um formato legível a humanos
 - Como uma sequência de seis números separados por dois pontos.
 - Cada número corresponde a 1 byte do endereço de 6 bytes e é representado como um par de dígitos hexadecimais, um para cada nibble do byte.
 - Zeros à esquerda não são geralmente mostrados.
 - Por exemplo, 8:0:2b:e4:b1:2 corresponde a
 - 00001000 00000000 00101011 11100100 10110001 00000010

Endereços Ethernet

- Para assegurar que cada adaptador receba um endereço único, cada fabricante de dispositivos Ethernet recebe um prefixo diferente que deve ser utilizado nos endereços de cada adaptador que ele construa
 - À AMD foi atribuído o prefixo de 24 bits 8:0:20

Endereços Ethernet

- Cada quadro transmitido em uma rede Ethernet é recebido pelos demais adaptadores conectados na mesma rede.
- Cada adaptador repassa para a camada de cima apenas os quadros com endereço de destino igual ao do adaptador.
- Além do endereço *unicast*, um endereço com todos os bits iguais a 1 é tratado como endereço de *broadcast*.
 - Todos adaptadores passam para camada de cima quadros com endereço de *broadcast*.
- Um endereço que o bit menos significativo do primeiro byte é igual a 1 é chamado de endereço de *multicast*.
 - Um host pode programar seu adaptador para aceitar um conjunto de endereços *multicast*.
 - 01:00:0C-CC-CC-CD – *Cisco shared spanning tree protocol address*

Endereços Ethernet

- Em resumo, um adaptador Ethernet recebe todos os quadros e aceita
 - Quadros endereçados para o seu próprio endereço.
 - Quadros endereçados para o endereço de broadcast.
 - Quadros para um endereço *multicast* desde que tenha sido programado para receber quadros desse endereço.

Algoritmo de Transmissão Ethernet

- Quando o adaptador tem um quadro para enviar e o canal está ocioso, ele transmite o quadro imediatamente.
 - O limite máximo de 1500 bytes no quadro significa que o adaptador pode ocupar o canal por um comprimento máximo fixo de tempo.
- Quando o adaptador tem um quadro para transmitir e o canal está ocupado, ele espera até que o canal fique ocioso e então transmite imediatamente.
- O algoritmo de transmissão Ethernet é conhecido como 1-persistente porque um adaptador transmite um quadro com probabilidade 1 sempre que o canal está ocioso.

Algoritmo de Transmissão Ethernet

- Uma vez que não há controle centralizado, é possível que dois (ou mais) adaptadores comecem a transmitir ao mesmo tempo,
 - Porque ambos encontraram o canal ocioso,
 - Ou, ambos estavam esperando por um canal ocupado se tornar ocioso.
- Quando isso acontece, dizemos que os dois (ou mais) quadros *colidiram* na rede.

Algoritmo de Transmissão Ethernet

- Como Ethernet suporta a detecção de colisões, cada emissor é capaz de determinar se uma colisão está acontecendo.
- No momento que um adaptador detecta que seu quadro está colidindo com um outro, ele primeiro transmite uma sequência de interferência de 32 bits (*32-bit jamming sequence*) e então para de transmitir.
 - Assim, um transmissor transmitirá no mínimo 96 bits em caso de colisão
 - 64 bits de preâmbulo + 32 bits da sequência de interferência (*jamming sequence*)

Algoritmo de Transmissão Ethernet

- Uma situação em que um adaptador transmitirá apenas 96 bits (chamado de quadro anão – *runt frame*) é quando os dois hosts estão muito próximos um do outro.
- Se eles estiverem mais distantes,
 - Eles terão de transmitir por mais tempo, e portanto enviar mais bits, antes de detectar a colisão.

Algoritmo de Transmissão Ethernet

- O pior caso ocorre quando dois hosts estão em extremos opostos da rede Ethernet.
- Para ter certeza que um quadro enviado não colidiu com um outro, um transmissor tem de transmitir no mínimo 512 bits.
 - Todo quadro Ethernet deve ter pelo menos 512 bits (64 bytes).
 - 14 bytes do cabeçalho + 46 bytes de dados + 4 bytes de CRC

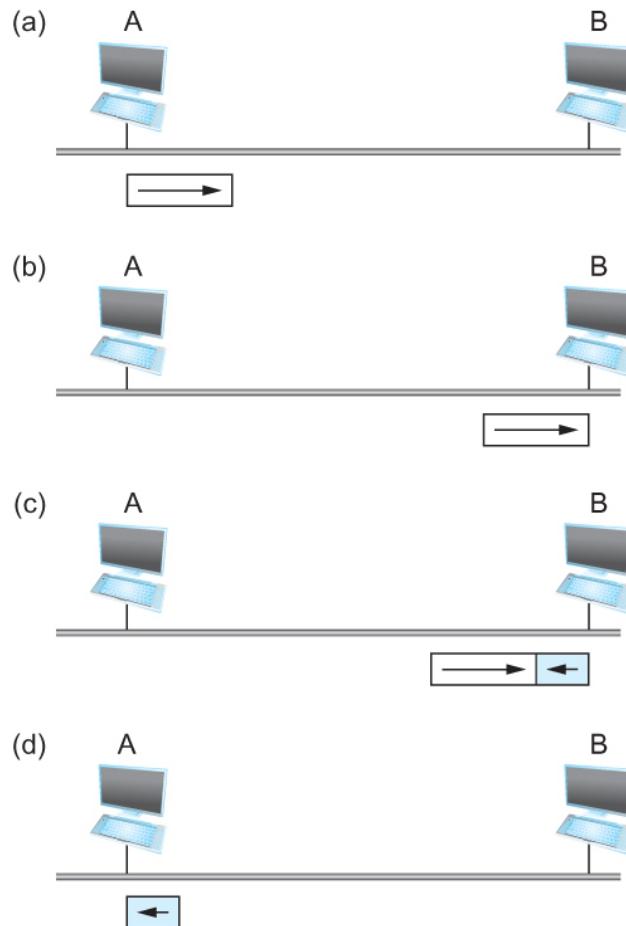
Algoritmo de Transmissão Ethernet

- Por que 512 bits?
 - Por que o comprimento é limitado a 2500 m?
- Quanto mais distantes dois nós estão, mais tempo leva para um quadro enviado por um nó chegar ao outro, o que torna a rede mais vulnerável a colisões durante esse período.

Algoritmo de Transmissão Ethernet

- Suponha que A comece a transmitir um quadro no tempo t
- E que d represente a latência do enlace em um sentido
- O primeiro bit do quadro de A chega a B no tempo $t + d$
- Suponha que um instante antes do quadro de A chegar, o host B comece a transmitir o seu quadro
- O quadro de B vai colidir imediatamente com o quadro de A e a colisão será detectada por B
- O host B enviará a sequência de interferência de 32 bits (*32-bit jamming sequence*)
- O host A não saberá que a colisão ocorreu até que o quadro de B chegue a ele, o que só acontecerá no tempo $t + 2 * d$
- O host A deve continuar transmitindo até esse tempo para que ele detecte a colisão
 - O host A deve transmitir por pelo menos $2 * d$ para ter certeza que ele detecte todas as possíveis colisões.

Algoritmo de Transmissão Ethernet



Cenário de pior caso: (a) A envia um quadro no tempo t ; (b) O quadro de A chega a B no tempo $t + d$; (c) B começa a transmitir no tempo $t + d$ e colide com o quadro de A; (d) O quadro anão de B (*runt frame*) de 32 bits chega a A no tempo $t + 2d$.

Algoritmo de Transmissão Ethernet

- Como o comprimento máximo de uma rede Ethernet é de 2500 m (incluindo até quatro repetidores), o RTT máximo foi definido em 51.2 μ s
 - Em redes Ethernet de 10 Mbps corresponde a 512 bits
- Outra maneira de olhar essa situação,
 - Precisamos limitar a latência máxima a um valor bem pequeno (51.2 μ s) para que o algoritmo de acesso funcione
 - Portanto, o comprimento máximo de uma rede Ethernet deve ser na ordem de 2500 m.

Algoritmo de Transmissão Ethernet

- Quando um adaptador detecta uma colisão e para sua transmissão, ele deve esperar um certo tempo para tentar novamente.
- Toda vez que o adaptador tenta transmitir e falha, ele dobra o tempo que ele espera antes de tentar novamente.
- Essa estratégia de dobrar o intervalo entre cada tentativa de retransmissão é conhecida como recuo exponencial (*Exponential Backoff*).

Algoritmo de Transmissão Ethernet

- Na primeira tentativa, o adaptador espera 0 ou 51.2 μ s, selecionados de forma aleatória.
- Se essa tentativa falha, ele então seleciona aleatoriamente um tempo de espera entre os seguintes valores 0, 51.2, 102.4, 153.6 μ s antes de tentar novamente;
 - Isso é $k * 51.2$ para $k = 0, 1, 2, 3$
- Após a terceira colisão, o adaptador espera $k * 51.2$ para $k = 0 \dots 2^3 - 1$ (novamente selecionando de forma aleatória).
- Em geral, o algoritmo seleciona um k aleatório entre 0 e $2^n - 1$ e espera por $k * 51.2 \mu$ s, em que n é o número de colisões ocorridas até o momento.

Experiência com Ethernet

- Ethernet funciona melhor em condições de baixo tráfego.
 - Em alto tráfego, muita capacidade da rede é desperdiçada em colisões.
- Ethernet é, geralmente, utilizada de forma conservadora.
 - Tem menos de 200 hosts, o que é bem menor do que o máximo permitido de 1024.
- A maioria é bem menor do que 2500m com um RTT mais próximo de 5 μ s do que de 51.2 μ s.
- Ethernets são fáceis de administrar e manter.
 - Não há switches que possam falhar e não há necessidade de se manter tabelas de roteamento atualizadas.
 - É fácil de adicionar um novo host a rede.
 - É barata.
 - O cabo é barato e o único custo adicional é o adaptador de cada host.

Enlaces Sem Fio (*Wireless Links*)

- Enlaces sem fio transmitem sinais eletromagnéticos
 - Rádio, microondas, infravermelho
- Enlaces sem fio compartilham o mesmo meio
 - O desafio é compartilhar o meio eficientemente sem interferir um com outro
 - A maioria dos compartilhamentos é feita dividindo-se o meio ao longo das dimensões de frequência e espaço
- Uso exclusivo de uma frequência específica em região geográfica pode ser alocado a uma entidade, como uma empresa

Enlaces Sem Fio (*Wireless Links*)

- Essas alocações são determinadas por agências governamentais, como a FCC (*Federal Communications Commission*) nos EUA e a Anatel no Brasil
- Algumas faixas de frequência são alocadas para usos específicos.
 - Algumas faixas são reservadas para uso governamental.
 - Outras faixas são reservadas para rádios AM e FM, televisões, comunicações via satélite e telefones celulares.
 - Frequências específicas nessas faixas são alocadas para organizações individuais para uso dentro de uma certa área geográfica (rádios FM podem ter a mesma frequência em cidades diferentes).
 - Finalmente, há várias faixas de frequência que não precisam de licença para uso (Telefone sem fio e Wi-Fi).

Enlaces Sem Fio (*Wireless Links*)

- Dispositivos que usam frequências livres ainda estão sujeitos a certas restrições
 - O primeiro é o limite de potência do transmissor
 - Isso limita o alcance do sinal, evitando a interferência com um outro sinal
 - Por exemplo, telefone sem fio pode ter um alcance máximo de 100 pés (~30 metros).

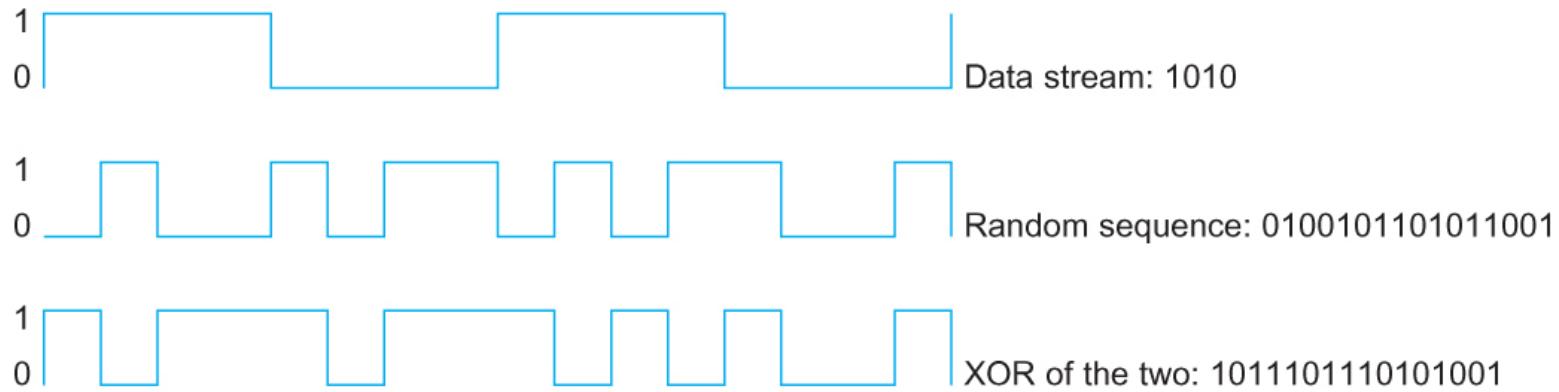
Enlaces Sem Fio (*Wireless Links*)

- A segunda restrição requer o uso da técnica de **Spread Spectrum**
 - A ideia é espalhar o sinal sobre uma faixa de frequência maior
 - Para minimizar o impacto da interferência de outros dispositivos
 - Técnica originalmente projetada para uso militar.
 - **Salto de Frequência (Frequency hopping)**
 - Transmite o sinal sobre uma sequência aleatória de frequências
 - Primeiro transmite em uma frequência, depois em uma segunda, depois em uma terceira, ...
 - A sequência de frequências não é verdadeiramente aleatória, ao invés é computada algorítmicamente por um gerador de números pseudo-aleatórios
 - O receptor usa o mesmo algoritmo que o emissor, inicializa-o com a mesma semente, e é
 - Capaz de saltar as frequências em sincronismo com o transmissor para receber corretamente o quadro

Enlaces Sem Fio (*Wireless Links*)

- Uma segunda técnica de spread spectrum é chamada **sequência direta (*direct sequence*)**
 - Representa cada bit no quadro em múltiplos bits no sinal transmitido.
 - Para cada bit que o transmissor quer transmitir
 - Ele envia o OU exclusivo do bit e n bits aleatórios
 - A sequência de bits aleatórios é gerada por um gerador de números pseudo aleatórios conhecido pelo transmissor e pelo receptor.
 - Os valores transmitidos, conhecidos como **código de fragmentação de n bits (n -bit chipping code)**, espalha o sinal por uma faixa de frequência que é n vezes mais larga.

Enlaces Sem Fio (*Wireless Links*)



Exemplo de uma sequência 4-bit chipping

Enlaces Sem Fio (*Wireless Links*)

- Tecnologias de rede sem fio diferem em várias dimensões
 - Quanta largura de banda elas oferecem
 - Quão distante dois nós que querem se comunicar podem estar
- Quatro tecnologias populares de rede sem fio
 - Bluetooth
 - Wi-Fi (formalmente conhecida como 802.11)
 - WiMAX (802.16)
 - 3G (telefones celulares)

Enlaces Sem Fio (*Wireless Links*)

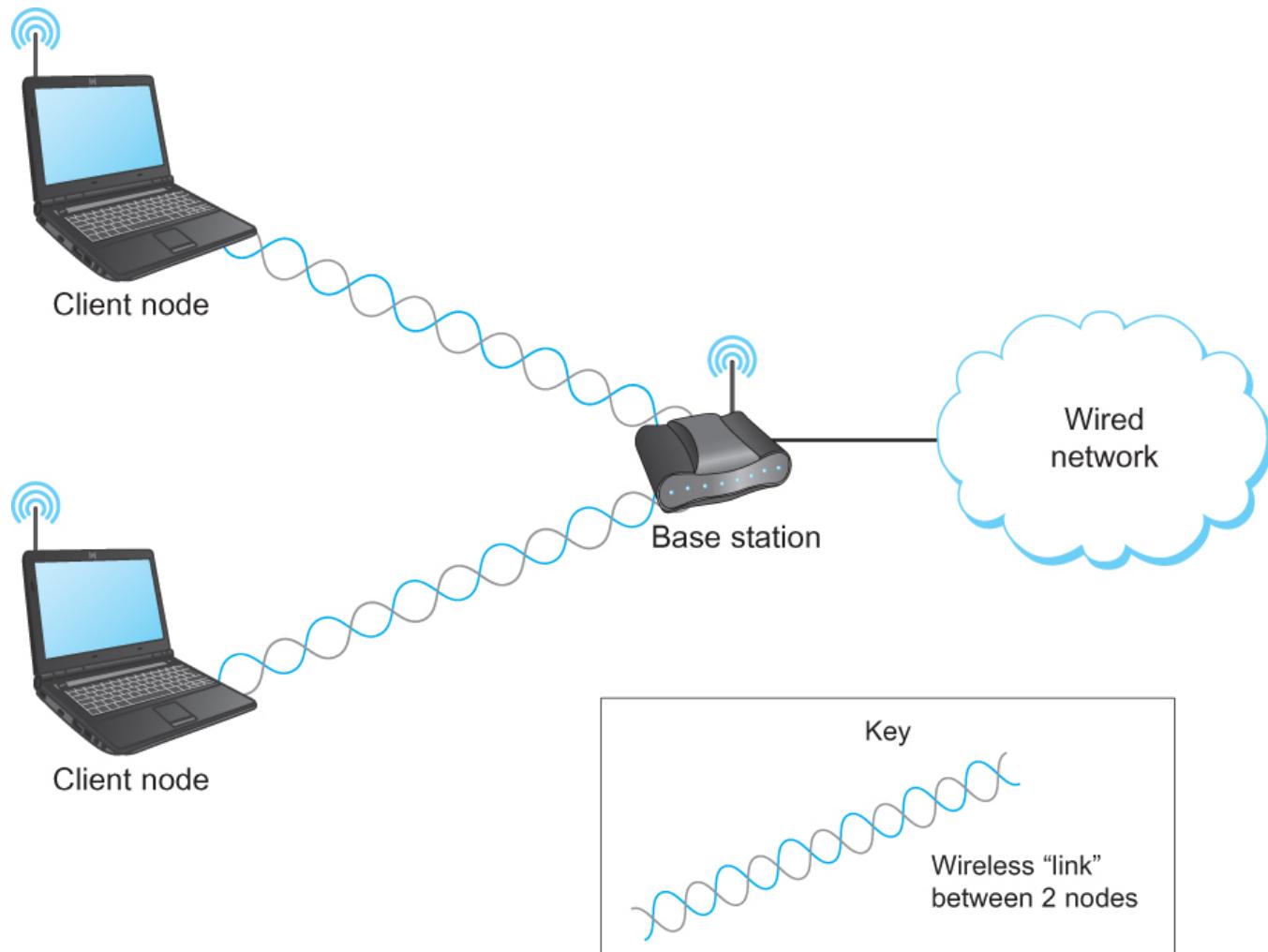
	Bluetooth (802.15.1)	Wi-Fi (802.11)	3G Cellular
Typical link length	10 m	100 m	Tens of kilometers
Typical data rate	2 Mbps (shared)	54 Mbps (shared)	Hundreds of kbps (per connection)
Typical use	Link a peripheral to a computer	Link a computer to a wired base	Link a mobile phone to a wired tower
Wired technology analogy	USB	Ethernet	DSL

Visão geral das principais tecnologias de rede sem fio

Enlaces Sem Fio (*Wireless Links*)

- Os enlaces sem fio são geralmente assimétricos
 - Os dois extremos são geralmente de tipos diferentes de nós
 - Um extremo geralmente é fixo e possui uma conexão cabeada com a Internet (conhecido como estação base - *base station*)
 - O nó no outro extremo é geralmente móvel

Enlaces Sem Fio (*Wireless Links*)



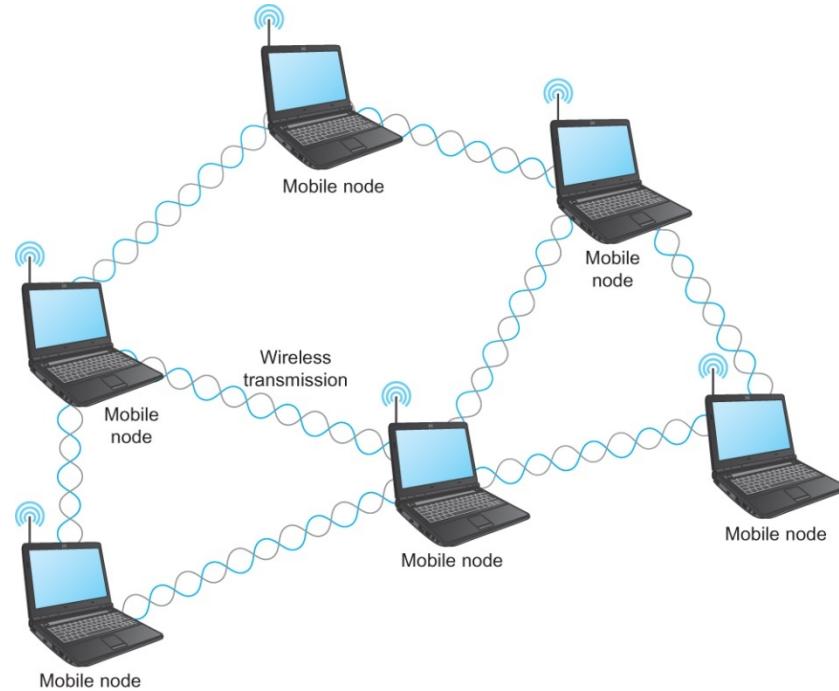
Uma rede sem fio utilizando uma estação base

Enlaces Sem Fio (*Wireless Links*)

- Comunicação sem fio suporta comunicação ponto-a-multiponto
- Comunicação entre os nós móveis (clientes) é roteada via estação base
- Três níveis de mobilidade para os clientes
 - Nenhuma mobilidade: o receptor deve estar em uma posição fixa para receber a transmissão direcional da estação base (versão inicial de WiMAX)
 - Mobilidade é limitada ao alcance da base (Bluetooth)
 - Mobilidade entre bases (Telefones celulares e Wi-Fi)

Enlaces Sem Fio (*Wireless Links*)

- Redes em Malha (*Mesh*) ou Ad-hoc
 - Os nós são pares
 - As mensagens podem ser repassadas via uma cadeia de nós pares



Uma rede sem fio ad-hoc ou malha (*mesh*)

IEEE 802.11

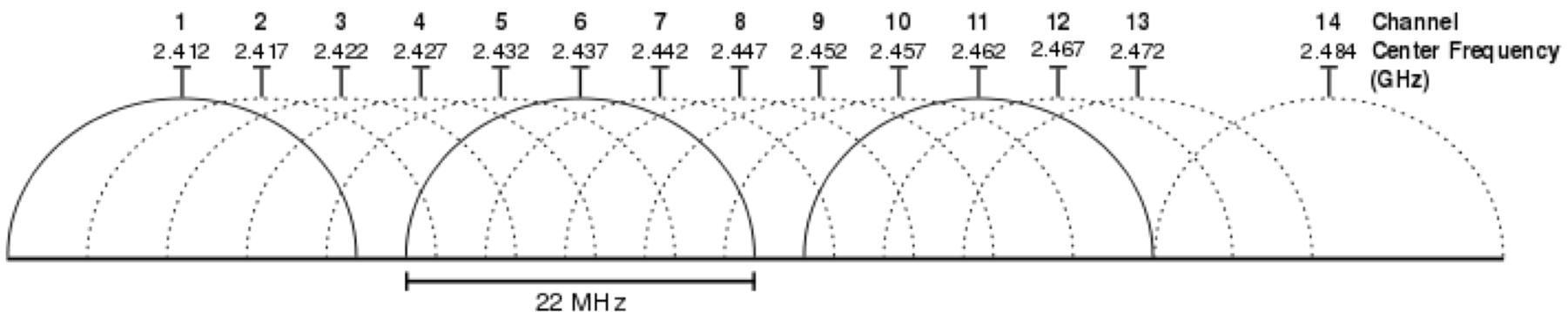
- Também conhecido como Wi-Fi
- Assim como a Ethernet, 802.11 foi projetado para uso em área geográfica limitada (casa, escritórios, campus)
 - O principal desafio é mediar o acesso a um meio de comunicação compartilhado – neste caso, sinais propagando pelo ar
- 802.11 suporta algumas funcionalidades adicionais
 - Gerenciamento de energia e
 - Mecanismos de segurança

IEEE 802.11

- O 802.11 original definiu dois padrões para a camada física baseada em rádio.
 - Um usando *frequency hopping*.
 - Mais de 79 faixas de 1-MHz de largura.
 - E o segundo usando *direct sequence*.
 - Usando 11-bit *chipping sequence*.
 - Ambos os padrões funcionam 2.4-GHz e oferecem até 2 Mbps.
- Depois, a camada física 802.11b foi adicionada.
 - Usa uma variante de *direct sequence*, o 802.11b oferece até 11 Mbps.
 - Usa a faixa de frequência livre de 2.4-GHz.
- Depois veio o 802.11a que suporta até 54 Mbps usando OFDM.
 - 802.11a usa faixa livre de 5-GHz.
- Depois veio o padrão 802.11g que é compatível com o 802.11b.
 - Usa a faixa de 2.4 GHz, OFDM (*Orthogonal Frequency Division Multiplexing*) e entrega até 54 Mbps.
 - O padrão mais recente é o 802.11n que pode chegar a 600 Mbps.

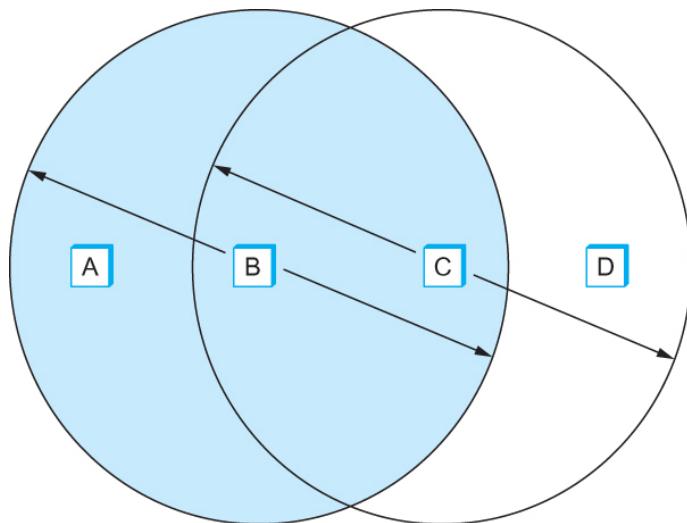
Enlaces Sem Fio (*Wireless Links*)

- Divisão em canais em 802.11 a 2.4GHz



IEEE 802.11 – Prevenção de Colisão

- Considere a situação na figura abaixo em que cada um dos quatro nós é capaz de enviar e receber sinais dos nós imediatamente à esquerda e à direita
 - Por exemplo, B pode trocar quadros com A e C, mas ele não pode alcançar D
 - C pode alcançar B e D, mas não A

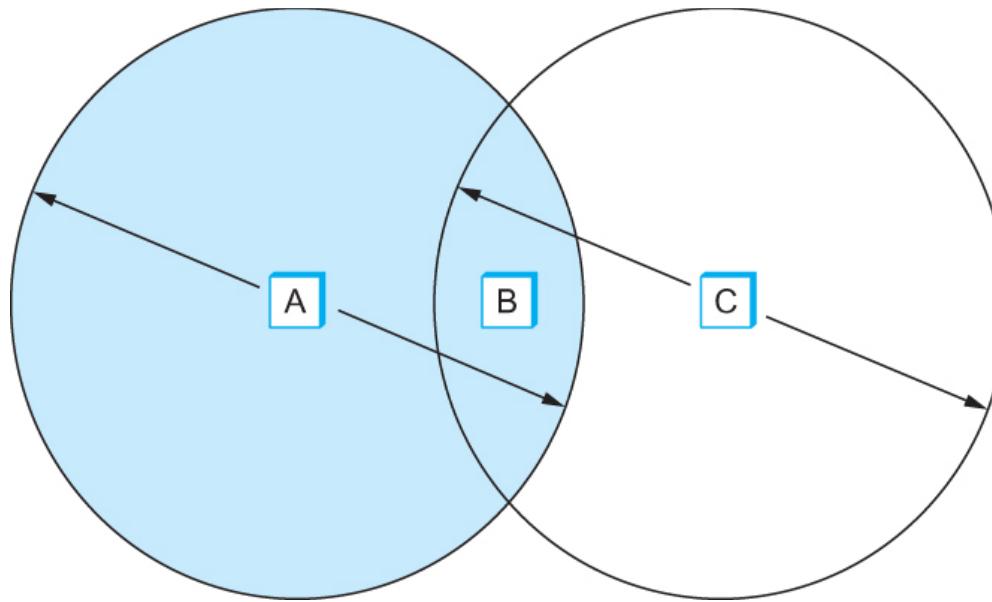


Exemplo de uma rede sem fio

IEEE 802.11 – Prevenção de Colisão

- Suponha que tanto A quanto C queiram se comunicar com B para enviar um quadro
 - A e C não sabem da existência um do outro porque seus sinais não atravessam a distância entre os dois
 - Esses dois quadros colidem um com outro em B
 - Mas, diferente de Ethernet, nem A nem C detectam essa colisão
 - A e C são conhecidos como *nós escondidos* (*hidden nodes*) um relação ao outro

IEEE 802.11 – Prevenção de Colisão

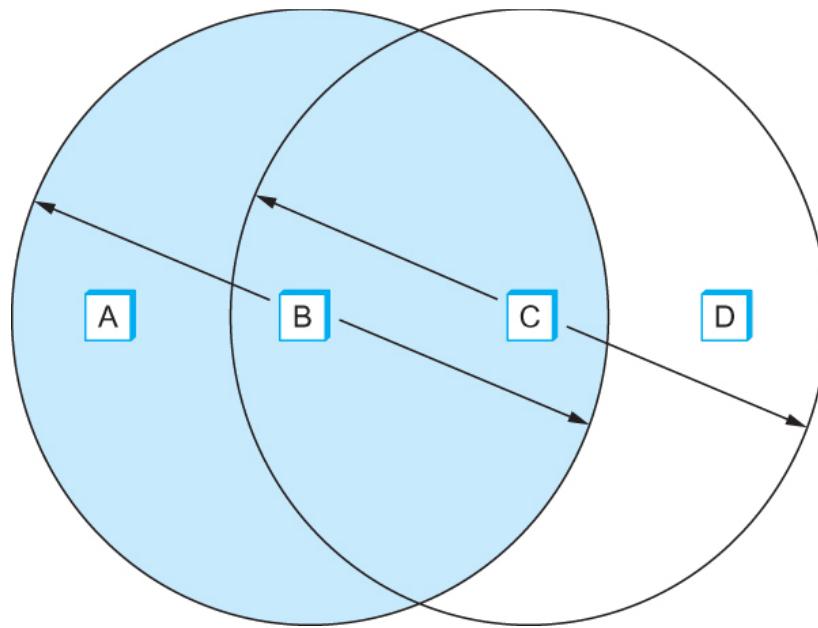


O problema do “Nó Escondido”. Embora A e C estejam escondidos um do outro, seus sinais colidem em B. (O alcance de B não é mostrado.)

IEEE 802.11 – Prevenção de Colisão

- Um outro problema chamado *nó exposto* (*exposed node*) pode ocorrer
 - Suponha que B está enviando para A. O nó C está ciente dessa transmissão porque ele recebe a transmissão de B.
 - Seria um engano de C concluir que ele não pode transmitir para nenhum outro nó só porque ele escuta a transmissão de B.
 - Suponha que C queira transmitir para o nó D.
 - Isso não é um problema, pois a transmissão de C para D não interferirá com a capacidade de A receber o sinal de B.

IEEE 802.11 – Prevenção de Colisão



Problema do Nô Exposto. Embora B e C estejam expostos aos sinais um do outro, não há interferência se B transmitir para A enquanto C transmite para D. (Os alcances de A e D não são mostrados.)

IEEE 802.11 – Prevenção de Colisão

- 802.11 resolve esses dois problemas com um algoritmo chamado *Multiple Access with Collision Avoidance* (MACA).
- Ideia básica
 - Transmissor e receptor trocam quadros de controle antes do transmissor iniciar uma transmissão de dados.
 - Essa troca informa a todos os nós vizinhos que uma transmissão está para começar.
 - O transmissor envia um quadro *Request to Send* (RTS) para o receptor.
 - O quadro RTS possui um campo que indica por quanto tempo o transmissor quer acesso ao meio
 - Comprimento do quadro de dados a ser transmitido
 - O receptor responde com um quadro *Clear to Send* (CTS)
 - Este quadro também contém o comprimento solicitado

IEEE 802.11 – Prevenção de Colisão

- Qualquer nó que recebe o quadro CTS sabe que
 - Está perto do receptor e, portanto,
 - não pode transmitir pelo período de tempo que se leva para transmitir o quadro de comprimento especificado
- Qualquer nó que recebe o quadro RTS mas não recebe o quadro CTS
 - Não está próximo suficiente do receptor para interferir com sua transmissão e, portanto,
 - está livre para transmitir

IEEE 802.11 – Prevenção de Colisão

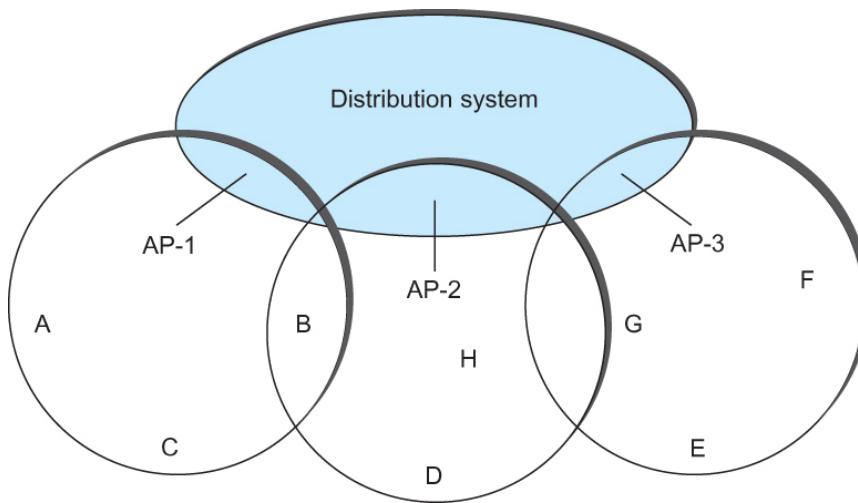
- Utilização de ACK em MACA
 - Proposto em MACAW: MACA para Wireless LANs
- O receptor envia um ACK para o transmissor depois de receber um quadro
- Todos os nós devem esperar por esse ACK antes de tentar transmitir
- Se dois ou mais nós detectam um enlace ocioso e tentarem transmitir um quadro RTS ao mesmo tempo
 - Seus quadros RTS colidirão um com o outro
- 802.11 não suporta detecção de colisão
 - O transmissor percebe que houve colisão quando ele não recebe o quadro CTS depois de um certo tempo
 - Neste caso, os nós envolvidos na colisão esperam um tempo aleatório antes de tentar novamente.
 - O tempo que um determinado nó espera é definido pelo mesmo algoritmo de recuo exponencial definido para Ethernet.

IEEE 802.11 – Sistema de Distribuição

- 802.11 é apropriado para uma configuração ad-hoc de nós que podem ou não se comunicar com todos os outros nós.
- Os nós são livres para se movimentar.
- O conjunto de nós alcançáveis pode mudar ao longo do tempo.
- Para lidar com mobilidade e conectividade parcial,
 - 802.11 define estruturas adicionais em um conjunto de nós.
 - Ao invés de tratar todos os nós como iguais,
 - alguns nós podem se mover
 - alguns nós estão conectados a uma infraestrutura de rede cabeada
 - Estes nós são chamados de Pontos de Acesso (*Access Points* – AP) e são conectados uns aos outros por um sistema de distribuição

IEEE 802.11 – Sistema de Distribuição

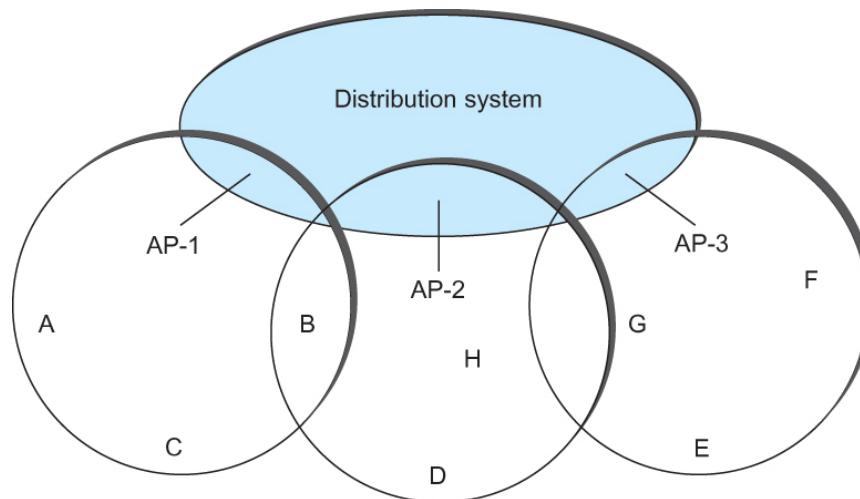
- A figura a seguir ilustra um sistema de distribuição que conecta três APs, em que cada um serve nós de uma determinada região
- Cada uma dessas regiões é análoga a uma célula em sistema de telefonia celular em que os APs exercem o mesmo papel das estações bases
- O sistema de distribuição opera na camada 2 da arquitetura ISO



APs conectados a uma rede de distribuição

IEEE 802.11 – Sistema de Distribuição

- Embora dois nós possam se comunicar diretamente se eles estiverem dentro de seus alcances, a ideia por trás dessa configuração é que
 - Cada nó se associa a um AP
 - Para o nó A se comunicar com o nó E, A primeiro envia um quadro para o seu AP-1 que repassa o quadro para o AP-3 por meio do sistema distribuição. O AP-3 é quem transmite o quadro para E.



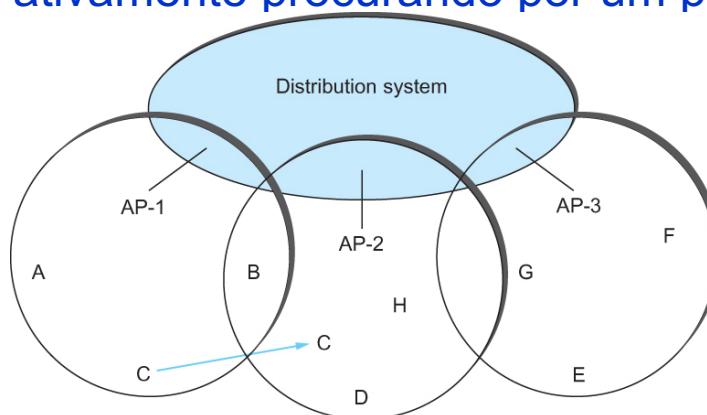
APs conectados a uma rede de distribuição

IEEE 802.11 – Sistema de Distribuição

- Como os nós selecionam seus APs?
- O que acontece quando um nó move de uma célula para outra?
- A técnica para selecionar um AP é chamada *varredura (scanning)*
 - O nó envia uma quadro de *Probe*
 - Todos os APs dentro da área de alcance respondem com um quadro *Probe Response*
 - O nó seleciona um dos APs e envia um quadro *Association Request*
 - O AP responde com um quadro *Association Response*
- Um nó utiliza esse protocolo sempre que
 - ele se junta a uma rede, bem como
 - quando ele se torna insatisfeito com o seu AP atual.
 - Isto pode acontecer, por exemplo, quando o sinal do AP atual fica fraco porque o nó se distanciou do AP
 - Sempre que um nó muda para um novo AP, o novo AP notifica o AP antigo da mudança via o sistema de distribuição

IEEE 802.11 – Sistema de Distribuição

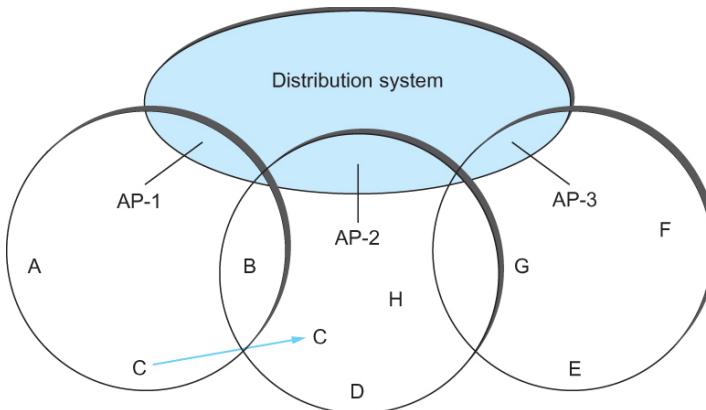
- Considere a situação mostrada na figura abaixo quando o nó C move da célula servida pelo AP-1 para a célula servida pelo AP-2.
- Conforme ele se move, ele envia quadros *Probe*, que eventualmente resulta em um quadro *Probe Responses* do AP-2.
- Em um determinado momento, C passa a preferir AP-2 ao invés de AP-1, e se associa a ele como ponto de acesso.
 - Este processo é chamado de *varredura ativa (active scanning)*, uma vez que o nó está ativamente procurando por um ponto de acesso.



Mobilidade de um nó

IEEE 802.11 – Sistema de Distribuição

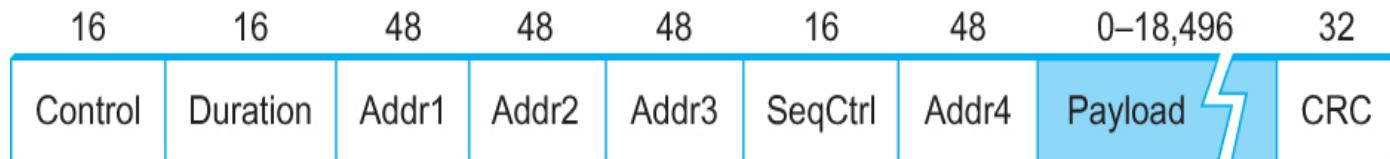
- Os APs também enviam periodicamente quadros *Beacon* que anunciam as características do AP; isso inclui as taxas de transmissão suportadas pelo AP.
 - Este processo é chamado de *varredura passiva (passive scanning)*
 - Um nó pode mudar para esse AP baseado no quadro *Beacon* simplesmente enviando um quadro *Association Request* de volta para o AP.



Mobilidade de um nó

IEEE 802.11 – Formato do Quadro

- Endereços Origem e Destino: 48 bits cada
- Dados: até 2312 bytes
- CRC: 32 bits
- Campo de controle: 16 bits
 - Contém três subcampos de interesse
 - 6 bit **Type**: indica se é um quadro RTS ou CTS ou está sendo usado pelo algoritmo de rastreamento
 - Um par de campos de 1 bit : chamados **ToDS** e **FromDS**



Formato do Quadro

IEEE 802.11 – Formato do Quadro

- Quadro contém quatro endereços
- Como esses endereços são interpretados, depende dos valores de **ToDS** e **FromDS** no campo de controle do quadro.
- Isso é para considerar a possibilidade do quadro ter sido repassado pelo sistema de distribuição, o que significaria que,
 - O transmissor original não é necessariamente o mesmo que o nó transmissor mais recente
- O mesmo ocorre para o endereço de destino
- Caso mais simples
 - Quando um nó está enviando diretamente para um outro, ambos os bits DS são iguais a 0, Addr 1 identifica o endereço de destino e Addr2 o endereço de origem.

IEEE 802.11 – Formato do Quadro

- Caso mais complexo
 - Ambos os bits DS são iguais a 1
 - Indica que o quadro partiu de um nó sem fio para o sistema de distribuição e depois do sistema de distribuição para um outro nó sem fio.
 - Quando os dois bits são iguais a 1,
 - Addr1 identifica o destino final,
 - Addr2 identifica o transmissor mais recente (o nó que repassou o quadro do sistema de distribuição para o destino final)
 - Addr3 identifica o nó intermediário (o nó que aceitou o quadro da rede sem fio e repassou pelo sistema de distribuição)
 - Addr4 identifica a origem inicial.
- Addr1: E, Addr2: AP-3, Addr3: AP-1, Addr4: A

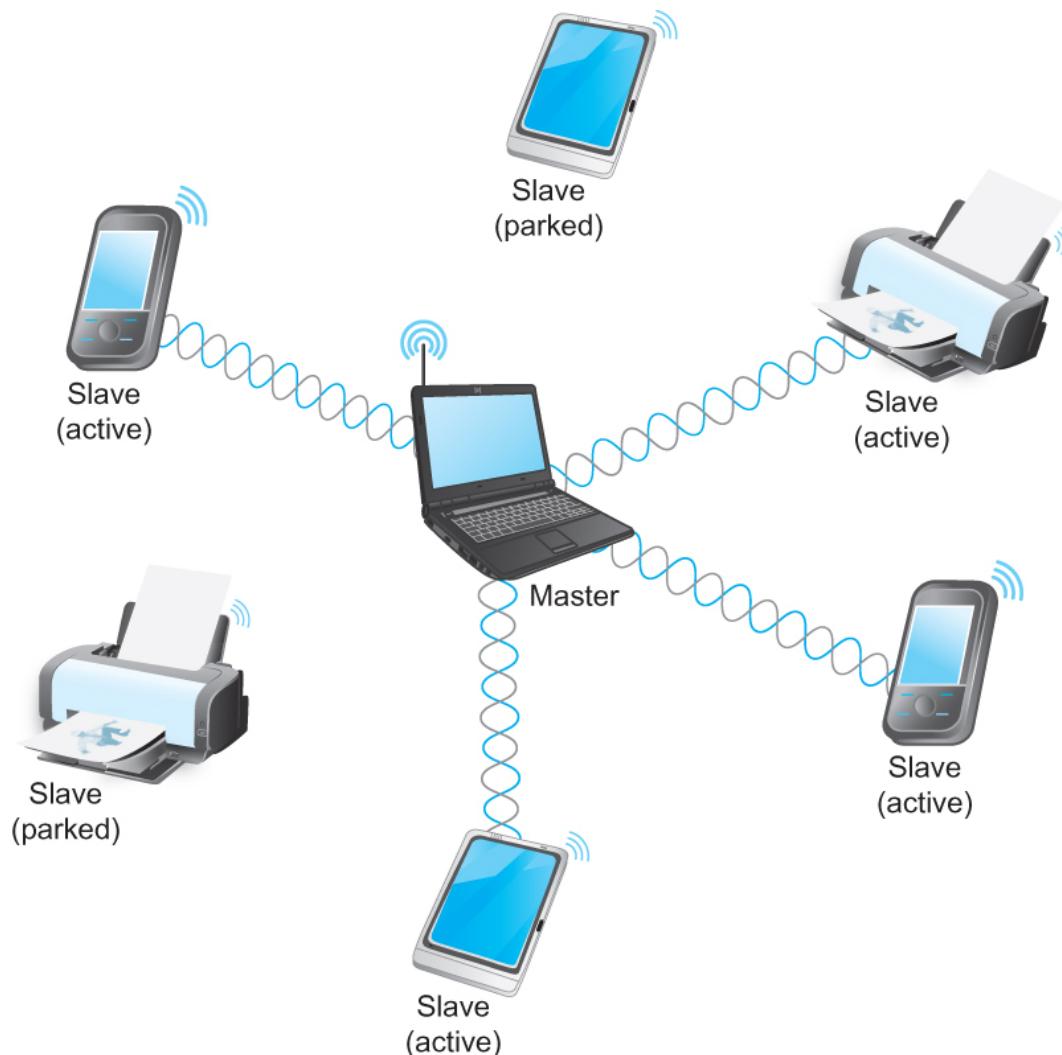
Bluetooth

- Usado para comunicações em distâncias curtas entre celulares, PDAs, notebooks e outros dispositivos pessoais.
- Opera na faixa livre de 2.45 GHz
- Possui um alcance de apenas 10 m
- Os dispositivos normalmente pertencem a um indivíduo ou um grupo
 - Normalmente chamado de *Personal Area Network (PAN)*
- A versão 2.0 oferece velocidade de até 2.1 Mbps
- O consumo de energia é baixo

Bluetooth

- Bluetooth é especificado por um consórcio industrial chamado Bluetooth Special Interest Group
- Especifica um conjunto completo de protocolos, indo além da camada de enlace para definir protocolos de aplicação, que são chamados de *perfis (profiles)*.
 - Existe um perfil para sincronizar um PDA com um computador pessoal
 - Um outro perfil serve para dar acesso a um dispositivo móvel a uma rede local cabeada.
- A configuração básica de rede Bluetooth é chamada de uma *piconet*
 - Consiste de um dispositivo mestre e até sete dispositivos escravos
 - Qualquer comunicação é sempre entre o mestre e um escravo
 - Os escravos não se comunicam diretamente

Bluetooth



Uma Piconet Bluetooth

Resumo

- Nós introduzimos vários tipos de enlaces que são usados para conectar usuários a redes existentes e para se construir redes maiores do zero.
- Nós estudamos cinco questões chaves que devem ser consideradas para que dois ou mais nós conectados a um meio possam trocar quadros entre si.
 - Codificação
 - Enquadramento
 - Deteção de Erros
 - Confiabilidade
 - Enlaces de Acessos Múltiplos
 - Ethernet
 - Wireless 802.11, Bluetooth