Parte 1

Camada de Enlace

Conteúdo

Fundamentos

Como pacotes são enviados pelos *enlaces individuais* no caminho de comunicação fim a fim?

Como os datagramas da camada de rede são encapsulados nos quadros da camada de enlace para transmissão por um único enlace?

Diferentes protocolos da camada de enlace são usados em diversos enlaces no caminho de comunicação?

Como os conflitos de transmissão nos enlaces de difusão podem ser resolvidos?

Existe endereçamento na camada de enlace e, se houver, como este endereçamento opera com o endereçamento da camada de rede?

Qual a diferença entre um comutador (switch) e um roteador?

Fundamentos

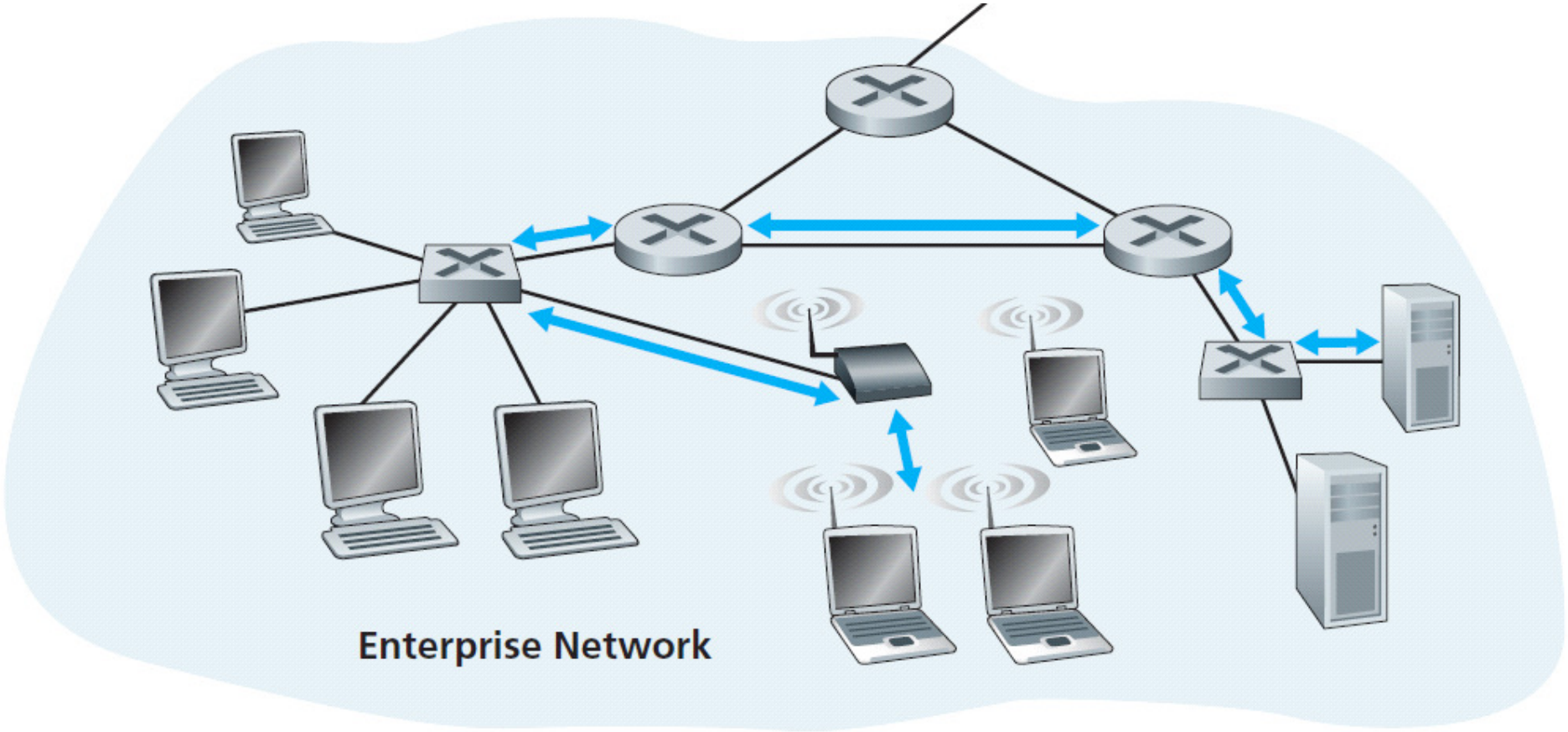
- **Terminologia**:
  - **Nó**: Qualquer dispositivo que rode um protocolo da camada de enlace. Os nós incluem hosts, roteadores, switches e pontos de acesso Wi-Fi;
  - **Enlaces**: Canais de comunicação que conectam nós adjacentes nos caminhos de comunicação;
- Para levar um datagrama de um host origem até um destino, o datagrama tem de ser transportado sobre cada um dos **enlaces individuais** existentes no caminho fim a fim;
- Considerando dado enlace, um nó transmissor encapsula o datagrama em um **quadro da camada de enlace** e o transmite para dentro do enlace.

Fundamentos

- **Analogia**: Sistema de transporte entre minha casa em Fortaleza até um hotel nos Alpes Suíços
  - Turista ➜ datagrama;
  - Trecho de transporte (casa-aeroporto, aeroporto-aeroporto, aeroporto-hotel) ➜ Enlace de comunicação;
  - Meio de transporte (táxi, avião, trem) ➜ Protocolo da camada de enlace;
  - Agente de viagens ➜ Protocolo de roteamento.

Fundamentos

Seis saltos da camada de enlace entre host sem fio e servidor



Conteúdo

Serviços Fornecidos pela Camada de Enlace

Serviço básico oferecido pela camada de enlace

Mover um datagrama de um nó até outro nó adjacente por um único enlace de comunicação.

- **Enquadramento de dados**:
  - Quase todos os protocolos encapsulam cada datagrama da camada de rede dentro de um quadro da camada de enlace antes de transmiti-lo pelo enlace;
  - O quadro consiste de um campo de dados e um campo de cabeçalho.
- **Acesso ao enlace**:
  - Um protocolo de Controle de Acesso ao Meio (*Medium Access Control* - MAC) especifica as regras segundo as quais um quadro é transmitido pelo enlace;
  - **Enlaces ponto-a-ponto**: problema simples;
  - **Enlaces de difusão**: problema interessante (problema de múltiplo acesso).

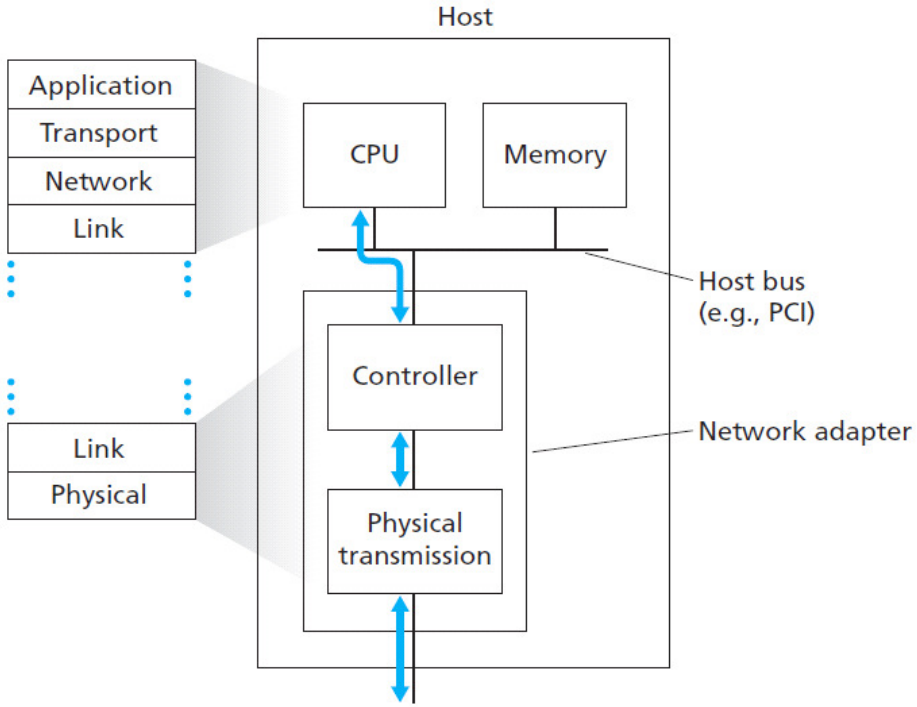
Serviços Fornecidos pela Camada de Enlace

- **Entrega confiável**:
  - Reconhecimentos e retransmissões;
  - Usado para enlaces que costumam ter altas taxas de erros (por ex. enlaces sem fio);
  - Sobrecarga para enlaces com baixa taxas de erro (por ex. enlaces com fio).
- **Detecção e correção de erros**:
  - Erros de bits são introduzidos por atenuação de sinal e ruído eletromagnético;
  - O nó transmissor envia bits de detecção de erros no quadro e o nó receptor realiza uma verificação de erros;
  - A **detecção** de erros na camada de enlace é mais sofisticada do que as implementadas nas camadas de transporte e rede, e é executada em hardware;
  - A **correção** de erros determina exatamente em que lugar do quadro o erro ocorreu, e então o corrige.

Conteúdo

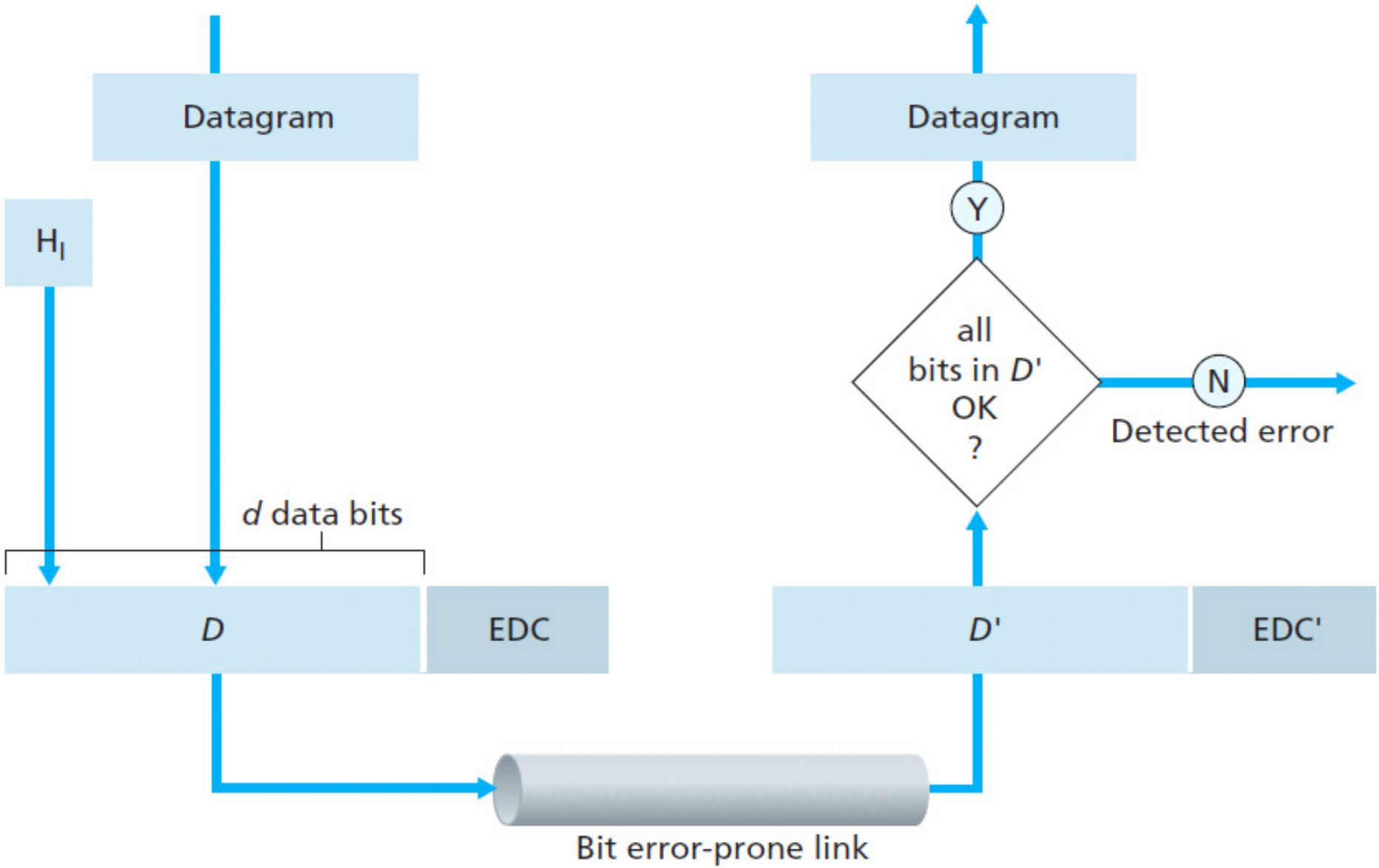
Onde a Camada de Enlace é Implementada?

- A camada de enlace é implementada em um **adaptador de rede** (placa de interface de rede);
- A maior parte da camada de enlace é implementada em **hardware**;
- Parte dela também é implementada em **software** que é executada na CPU do host.



Conteúdo

Técnicas de Detecção e Correção de Erros



Técnicas de Detecção e Correção de Erros

- Técnicas de detecção e correção de erros permitem que o receptor descubra a ocorrência de erros de bits às vezes, **mas não sempre**;
- O receptor pode não perceber que a informação recebida contém erros de bits: **erros de bits não detectados**;
- É preciso escolher um esquema de detecção de erros para o qual a **probabilidade** dessas ocorrências seja pequena;
- **Trade-off**: eficiência x complexidade.

Técnicas de Detecção e Correção de Erros

Correção de Erros Antecipada (Forward Error Correction - FEC)

Quais os benefícios de se utilizar técnicas de correção de erros antecipada?

Técnicas de Detecção e Correção de Erros

Correção de Erros Antecipada (Forward Error Correction - FEC)

Quais os benefícios de se utilizar técnicas de correção de erros antecipada?

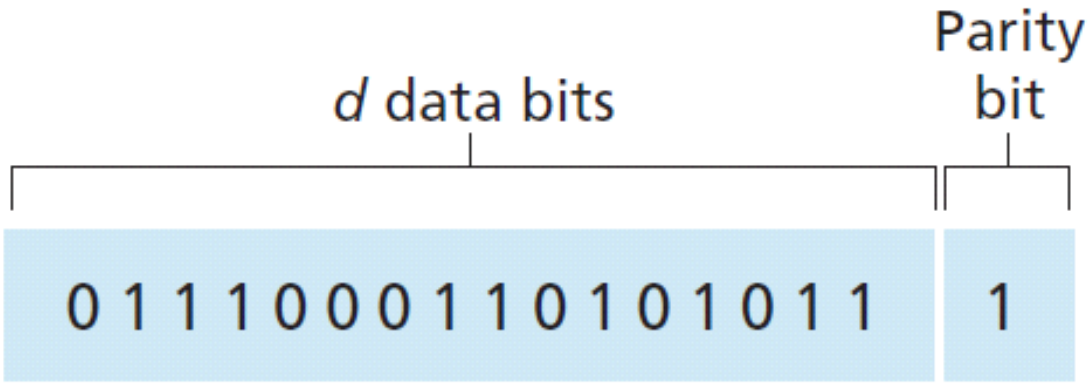
- Permitem imediata correção de erros no receptor;
- Podem reduzir o número exigido de retransmissões do remetente;
- Reduz o atraso fim-a-fim: benefício importante para aplicações multimídia em tempo real e enlaces com longo atraso de propagação (*Delay-Tolerant Networks*).

- Técnicas de detecção e correção:
  - **Verificação de paridade**;
  - **Soma de verificação**;
  - **Verificação de Redundância Cíclica (CRC)**.

Conteúdo

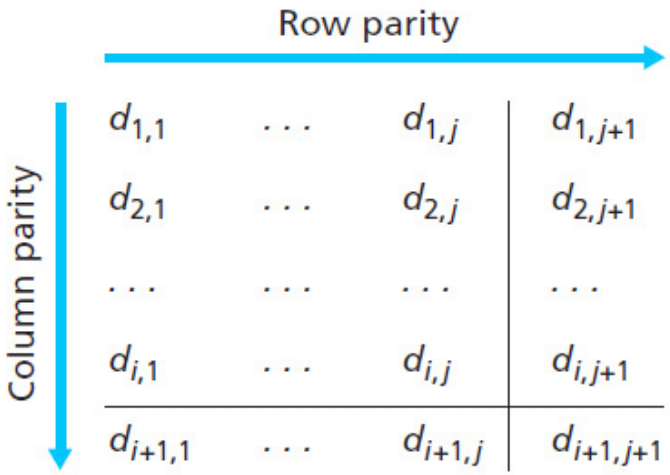
Verificação de Paridade

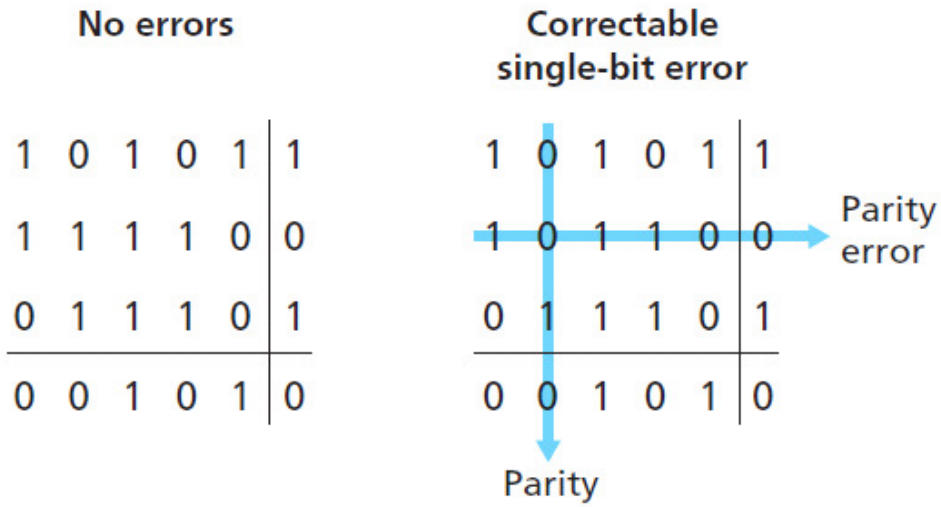
- A maneira mais simples de detectar erros é utilizar um único **bit de paridade**;
- Esquemas de paridade par e ímpar;
- Em um esquema de paridade par, o remetente escolhe o valor do bit de paridade de modo que o número total de "1"s nos $d + 1$ bits seja par;
- Em um esquema de paridade par, se um receptor contar um número ímpar de "1"s, saberá que ocorreu pelo menos um erro de bit (mais precisamente, um número ímpar de erros de bit);
- Problemas de detecção de erros em rajada.



Verificação de Paridade

Paridade Par Bidimensional





Conteúdo

Soma de Verificação

- A **soma de verificaçao da Internet** é baseada nessa técnica;
- Bytes de dados são tratados como **inteiros de k bits** (por ex. 16 bits) e somados;
- O **complemento 1** dessa soma forma a soma de verificação;
- O receptor verifica se houve erros somando as palavras recebidas e o checksum, e averiguando se o resultado contém somente bits 1;
- Oferece **proteção um tanto baixa** contra erros comparado com a técnica CRC;
- **Exemplo**:
  - Palavra 1.....0110011001100000
  - Palavra 2.....0101010101010101
  - Palavra 3.....1000111100001100
  - Soma.....0100101011000010
  - Complemento 1.....1011010100111101
  - Soma no receptor..1111111111111111

Soma de Verificação

Por que os protocolos TCP/IP utilizam soma de verificação e a camada de enlace utiliza CRC?

Soma de Verificação

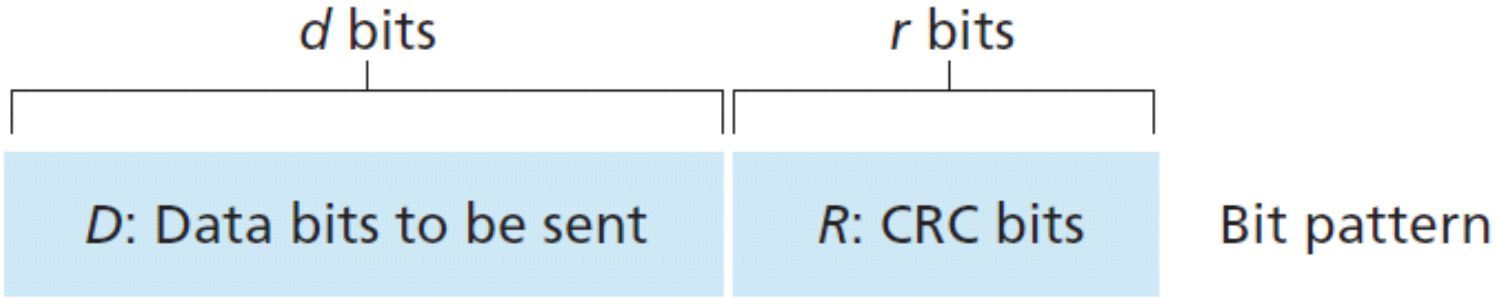
Por que os protocolos TCP/IP utilizam soma de verificação e a camada de enlace utiliza CRC?

A detecção de erros na camada de transporte é executada em software, portanto necessita ser mais simples. A detecção de erros na camada de enlace é executada em hardware, portanto as técnicas podem ser mais complexas.

Conteúdo

Verificação de Redundância Cíclica (CRC)

- **Códigos de Verificação de Redundância Cíclica** (Cyclic Redundancy Check - CRC);
- **Códigos polinomiais**: a cadeia de bits a ser enviada é considerada como um polinômio cujos coeficientes são os valores 0 e 1 na cadeia (aritmética polinomial);
- O remetente e o receptor devem, primeiro, concordar com um padrão de $r + 1$ bits, conhecido como um **gerador** G;
- Para cada parcela de dados de d bits, D, o remetente escolherá r bits adicionais, R, de modo que o padrão de $d + r$ bits resultante seja divisível exatamente por G, usando aritimética de módulo 2;
- O receptor divide os $d + r$ bits recebidos por G; se o resto for diferente de zero, o receptor saberá que ocorreu um erro;



Verificação de Redundância Cíclica (CRC)

- Padrões internacionais foram definidos para geradores G de 8, 12, 16 e 32 bits;
- Cada padrão de CRC pode detectar erros de rajada de até r bits e pode detectar qualquer número ímpar de erros de bits.

Enlaces e Protocolos de Acesso Múltiplo

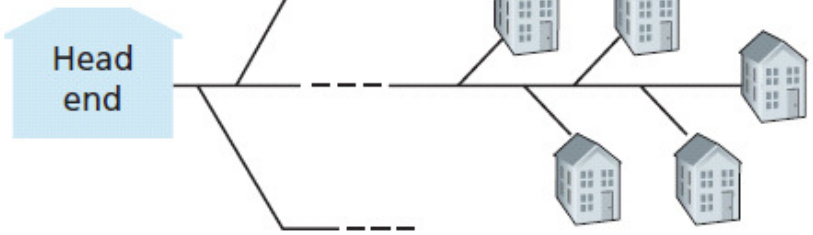
- Há dois tipos de enlaces de redes:
  - **Enlace ponto a ponto**: Consiste em um único remetente em uma extremidade do enlace e um único receptor na outra. Exemplos: protocolo ponto a ponto (PPP) e controle de ligação de dados de alto nível (HDCL);
  - **Enlace de difusão**: Pode ter vários nós remetentes e receptores, todos conectados ao mesmo canal de transmissão único e compartilhado. Exemplos: ethernet e WiFi.

Problema do Múltiplo Acesso

Como coordenar o acesso de vários nós remetentes e receptores a um canal de difusão compartilhado.

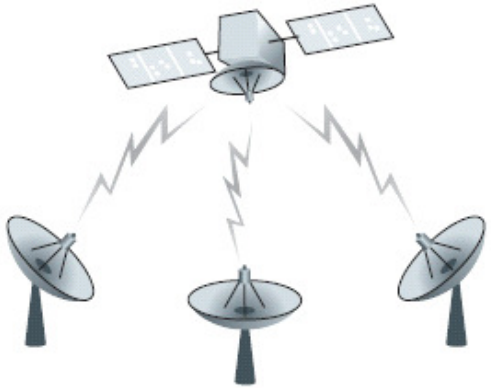
Exemplos de Canais de Acesso Múltiplo

Shared wire
(for example, cable access network)

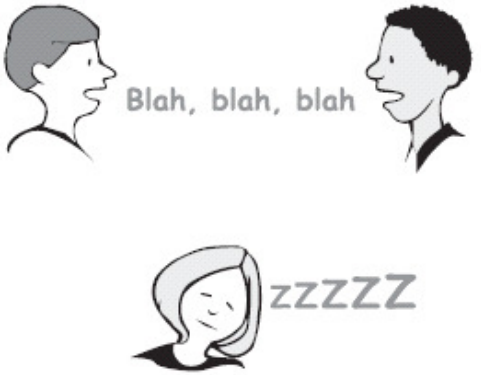


Shared wireless
(for example, WiFi)

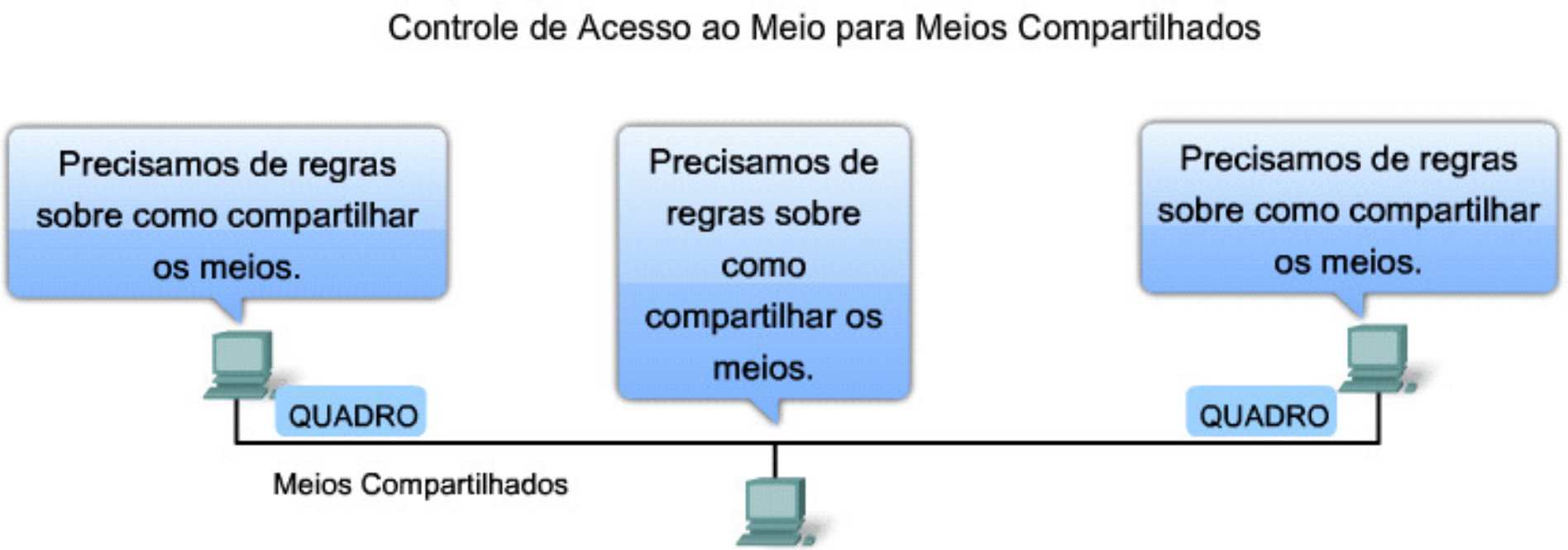
Satellite



Cocktail party



Controle de Acesso ao Meio para Meios Compartilhados

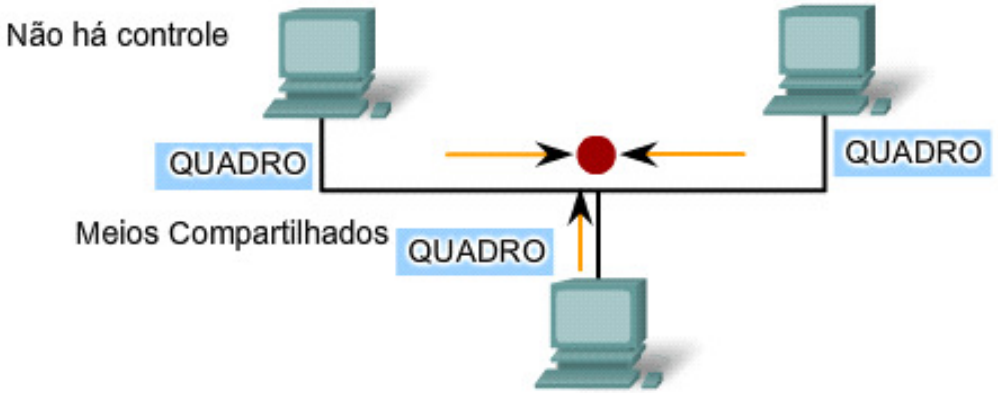


1. Dê a todos uma oportunidade de falar;
2. Não fale até que alguém fale com você;
3. Não monopolize a conversa;
4. Levante a mão se tiver uma pergunta a fazer;
5. Não interrompa uma pessoa quando ela estiver falando;
6. Não durma quando alguém estiver falando.

Controle de Acesso ao Meio para Meios Compartilhados

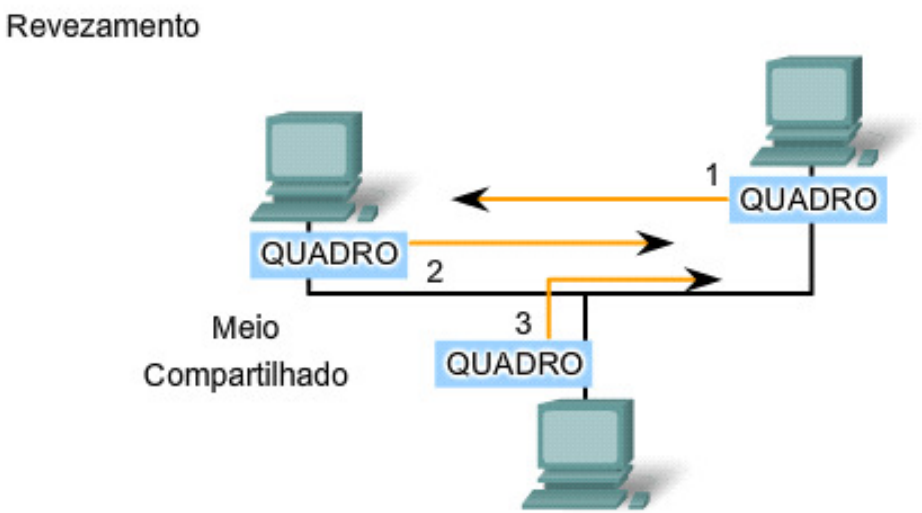
Métodos de Controle de Acesso ao Meio

Nenhum controle resultará em várias colisões.
As colisões resultam em quadros corrompidos que devem ser reenviados.



Os métodos que exigem um alto nível de controle previnem as colisões, mas o processo tem um custo elevado.

Os métodos que exigem um baixo nível de controle têm custo reduzido, mas as colisões são mais frequentes.

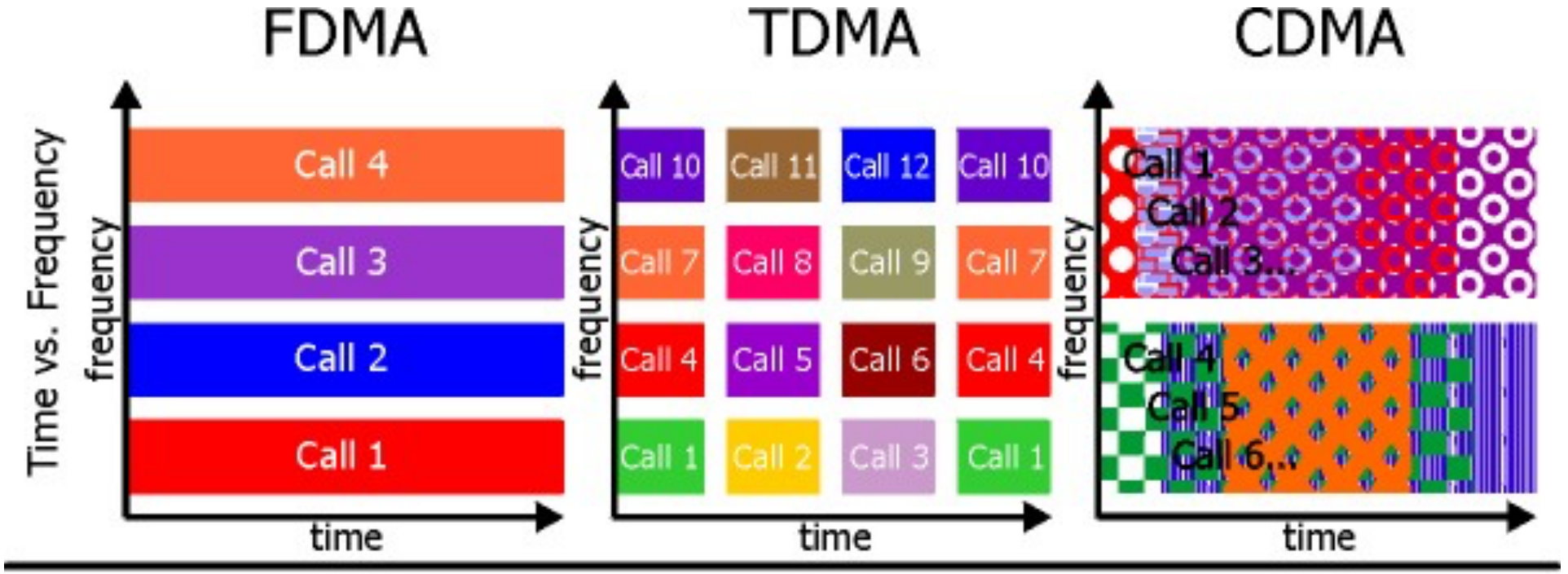


Controle de Acesso ao Meio para Meios Compartilhados

Características Desejáveis de um Protocolo de Múltiplo Acesso a um Enlace de R bps

1. Quando apenas um nó tem dados para enviar, esse nó tem uma vazão de R bps;
2. Quando M nós tem dados para enviar, cada um desses nós tem uma vazão média de R/M bps;
3. O protocolo é descentralizado;
4. O protocolo é simples para que sua implementação seja barata.

Protocolos de Divisão de Canal



Conversation Analogy

Everyone talks in a different room to prevent interference. Since the conversation can't be heard from another room, it can be filtered from the other by going to the other room.

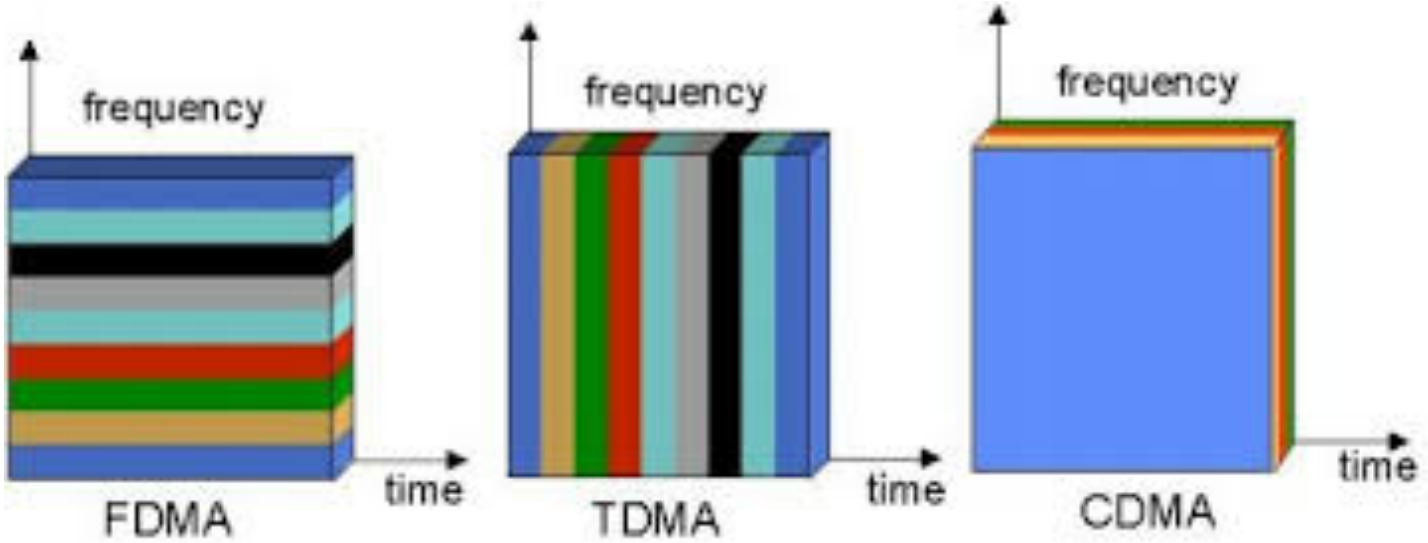
Within each room, everyone takes turns talking to prevent interference. Within each room, one person is talking at once, so they must talk fast to say everything.

Everyone speaks a different language at the same time in the same room. Since each language is unique, one may be filtered from another.

Protocolos de Divisão de Canal

Múltiplo Acesso por Divisão de Frequência (Frequency Division Multiple Access - FDMA)

- Divide o canal de R bps em N frequências diferentes, cada uma com uma largura de banda de R/N bps;
- Cada frequência é atribuída a um dos N nós;

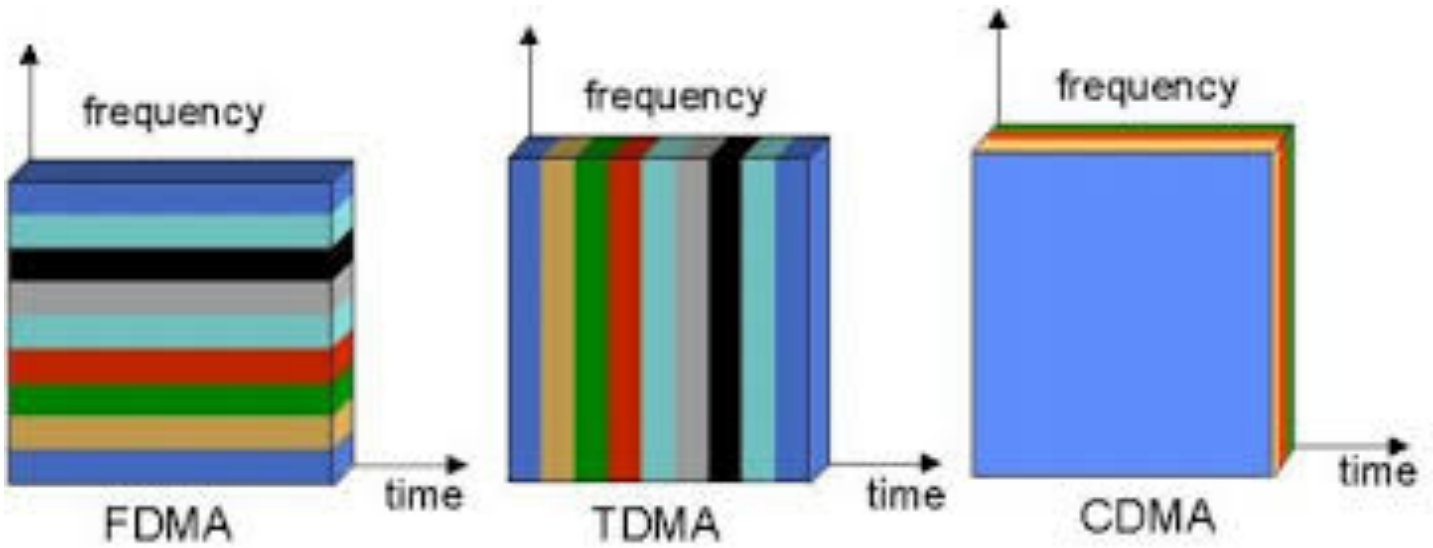


Quais as vantagens e desvantagens do FDMA?

Protocolos de Divisão de Canal

Múltiplo Acesso por Divisão de Frequência (Frequency Division Multiple Access - FDMA)

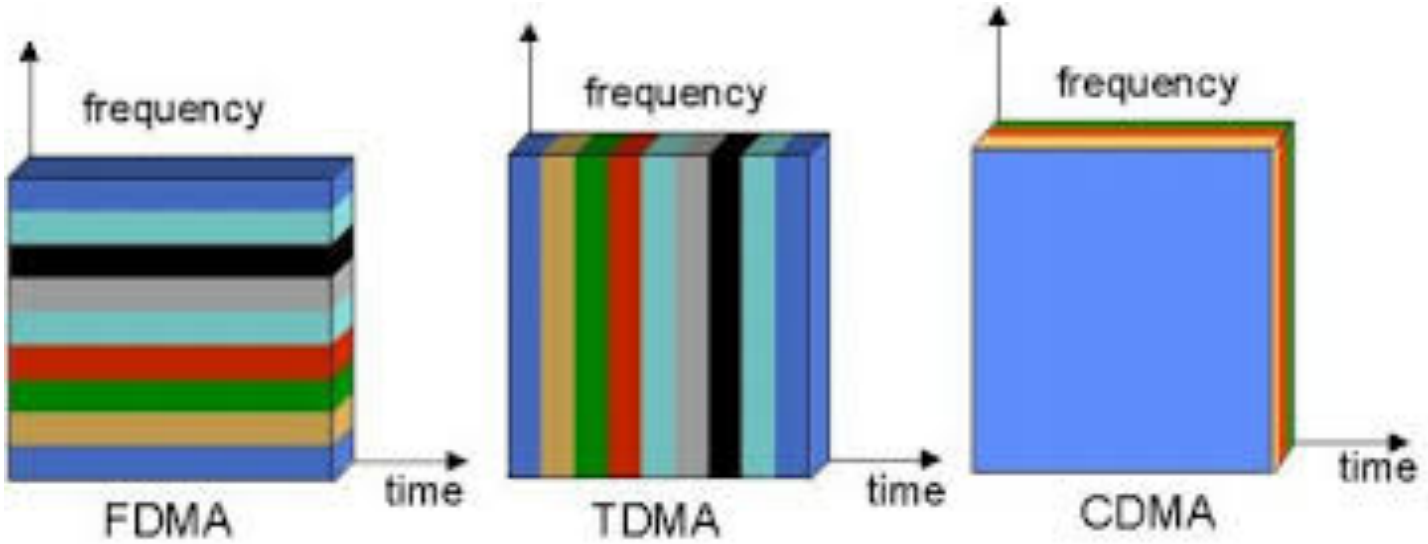
- **Vantagens**
  - Elimina colisões;
  - É perfeitamente justo: cada nó ganha uma velocidade de transmissão dedicada de R/N bps.
- **Desvantagens**
  - Um nó fica limitado a uma velocidade média de R/N bps, mesmo quando ele é o único nó com pacotes para enviar.



Protocolos de Divisão de Canal

Múltiplo Acesso por Divisão de Tempo (Time Division Multiple Access - TDMA)

- Divide o tempo em **quadros temporais**, os quais depois divide em N **compartimentos de tempo** (slots);
- Cada slot é atribuído a um dos N nós;



Quais as vantagens e desvantagens do TDMA?

Protocolos de Divisão de Canal

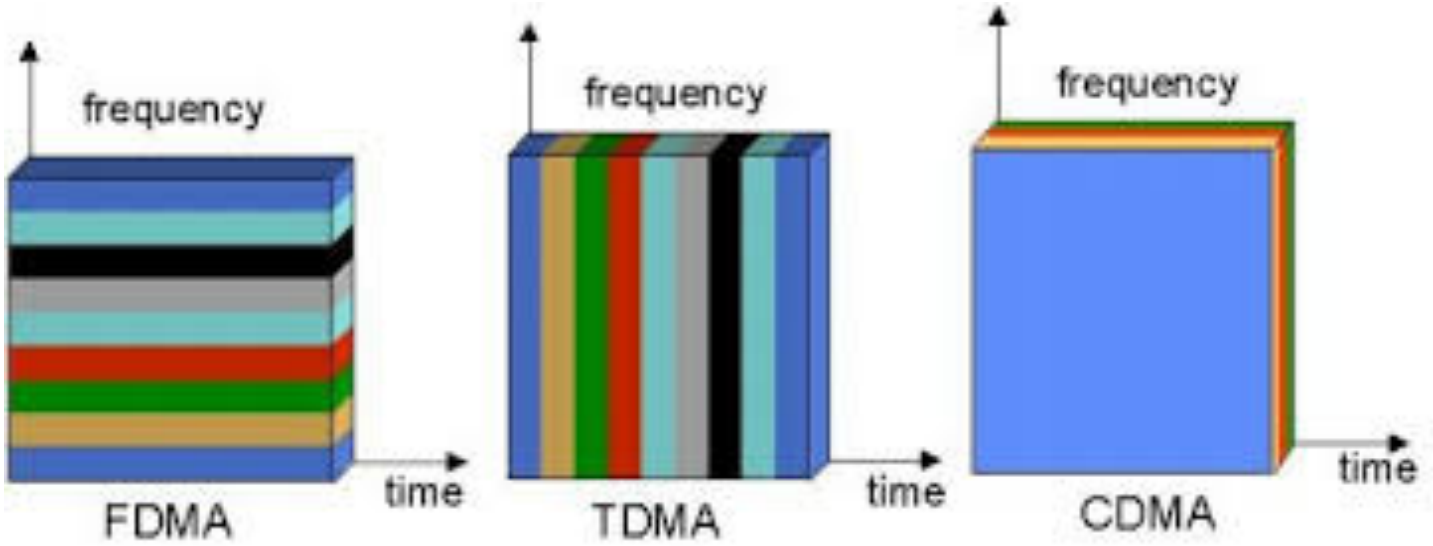
Múltiplo Acesso por Divisão de Tempo (Time Division Multiple Access - TDMA)

- **Vantagens**
  - Elimina colisões;
  - É perfeitamente justo: cada nó ganha uma velocidade de transmissão dedicada de R/N bps durante cada quadro temporal.
- **Desvantagens**
  - Um nó fica limitado a uma velocidade média de R/N bps, mesmo quando ele é o único nó com pacotes para enviar;
  - Um nó deve sempre esperar sua vez na sequência de transmissão, mesmo quando ele é o único com dados a enviar.

Protocolos de Divisão de Canal

Acesso Múltiplo por Divisão de Código (Code Division Multiple Access - CDMA)

- Atribui um **código** diferente a cada nó; cada nó usa seu código exclusivo para codificar os bits de dados que envia.
- **Vantagens**
  - Nós diferentes podem transmitir simultaneamente a despeito das interferências causadas pelas transmissões dos outros nós.



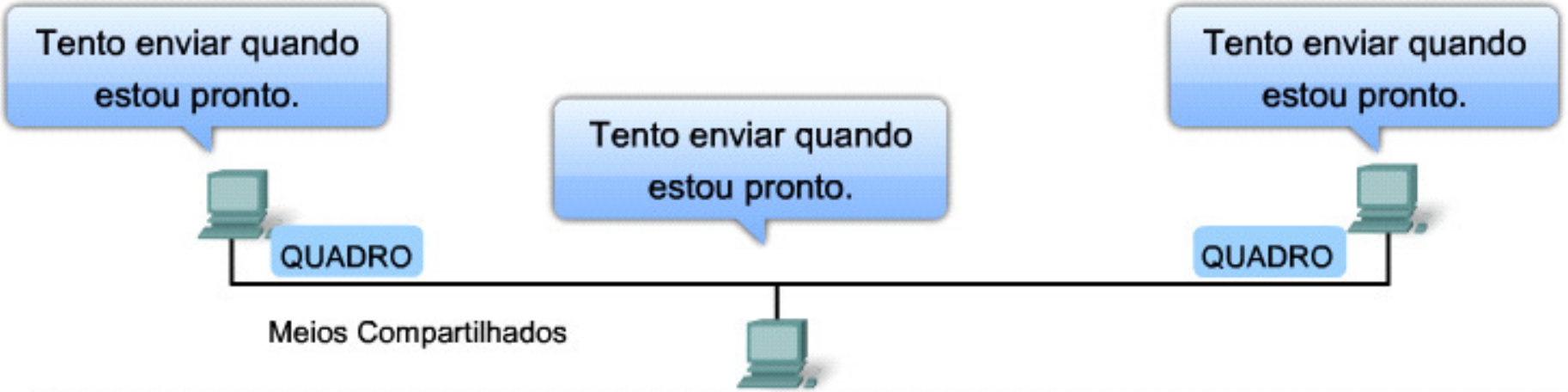
Protocolos de Acesso Aleatório

- Um nó transmissor sempre transmite à **taxa total** do canal, i.e. R bps;
- Quando há uma **colisão**, cada nó envolvido nela **retransmite repetidamente** seu pacote até que este passe sem colisão;
- Quando um nó sofre uma colisão, ele espera um **tempo aleatório independente** dos demais antes de retransmitir o pacote;
- Dois exemplos clássicos de protocolos de acesso aleatório:
  - **Aloha**: Aloha puro, Slotted Aloha;
  - **Carrier Sense Multiple Access (CSMA)**: CSMA/CD (Collision Detection), CSMA/CA (Collision Avoidance).

Protocolos de Acesso Aleatório

Controle de Acesso ao Meio para Meios Compartilhados

Acesso com Base em Contenção (Disputa)



Método	Características	Exemplo

Acesso com Base em Contenção (Disputa)	• Estações podem transmitir a qualquer momento
	• Há colisões
	• Há mecanismos para resolver a contenção ou disputa:
	  • CSMA/CD para redes Ethernet
	  • CSMA/CA para redes sem fio 802.11
		• Ethernet
		• Sem Fio

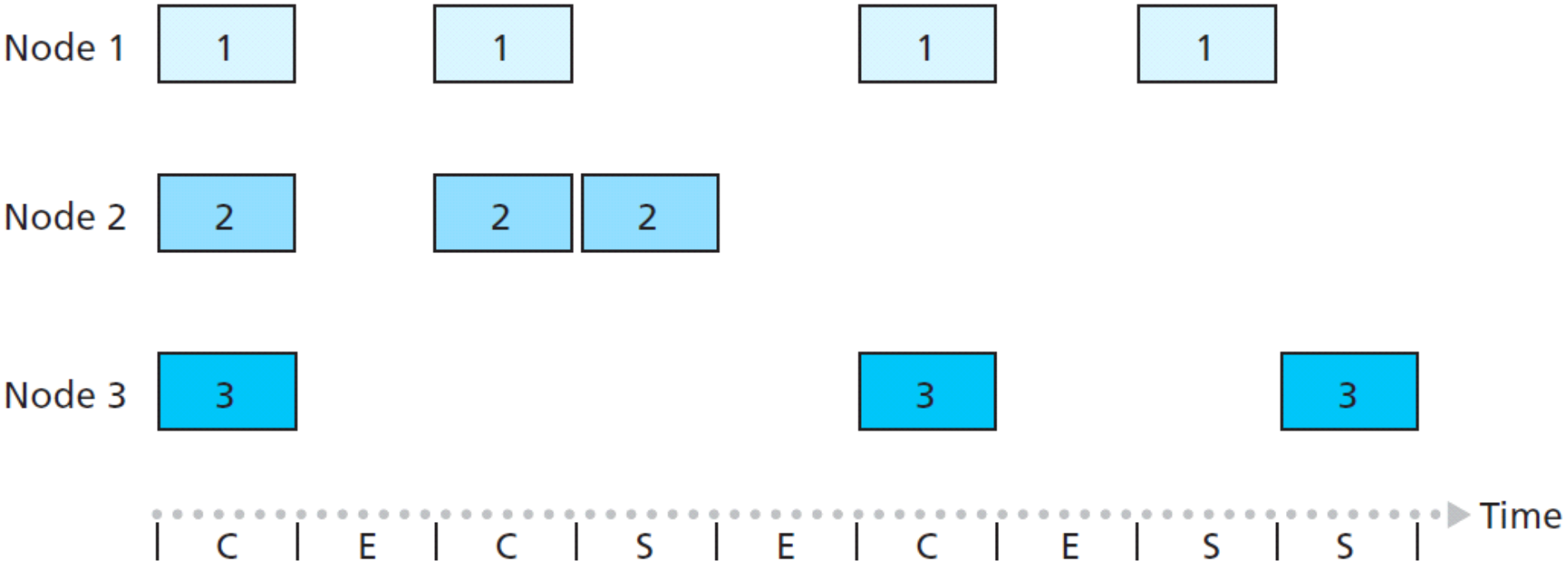
Protocolos de Acesso Aleatório

Protocolo Slotted Aloha

- O tempo é dividido em **intervalos (slots)**;
- Os nós são **sincronizados** de modo que cada nó sabe onde os intervalos começam;
- Quando o nó tem um novo pacote para enviar, espera até o início do próximo intervalo e transmite o pacote inteiro no intervalo;
- Se não houver colisão, o nó terá transmitido seu quadro com sucesso;
- Se houver uma colisão, o nó a detectará antes do final do intervalo; ele retransmitirá seu quadro em cada intervalo subsequente com **probabilidade** p até que o quadro seja transmitido sem colisão.

Protocolos de Acesso Aleatório

Protocolo Slotted Aloha



Key:

C = Collision slot

E = Empty slot

S = Successful slot

Protocolos de Acesso Aleatório

Protocolo Slotted Aloha

Quais as vantagens e desvantagens do Slotted Aloha?

Protocolos de Acesso Aleatório

Protocolo Slotted Aloha

Vantagens

- Permite que um único nó transmita continuamente à **taxa total** do canal R bps, quando ele for o único nó ativo;
- Protocolo altamente **descentralizado**;
- Protocolo extremamente **simples**.

Desvantagens

- Requer que os intervalos sejam **sincronizados** nos nós;
- Quando há vários nós ativos, certa fração dos intervalos terá colisões e, portanto, será "**desperdiçada**";
- Outra fração dos intervalos estará **vazia** porque todos os nós ativos evitarão transmitir como resultado da política probabilística de transmissão.

Protocolos de Acesso Aleatório

Protocolo Slotted Aloha

- Os únicos intervalos "não desperdiçados" serão aqueles em que exatamente um nó transmite (**intervalo bem-sucedido**);
- Cálculo da eficiência de um protocolo de múltiplo acesso com intervalos
  - Definida como a fração (calculada durante um longo tempo) de intervalos bem-sucedidos;
  - Suposições:
    - Existe um grande número de nós ativos;
    - Cada nó tem sempre um grande número de pacotes a enviar.

Protocolos de Acesso Aleatório

Protocolo Slotted Aloha

- Derivação da eficiência máxima do protocolo Slotted Aloha
  - Cada nó tenta transmitir um pacote em cada intervalo com probabilidade p (pacote novo ou retransmissão);
  - A probabilidade de que determinado intervalo seja bem-sucedido é a probabilidade de que um dos nós transmita (p) e os restantes $N-1$ nós, não ($(1-p)^{N-1}$);
  - Portanto, a probabilidade de um nó arbitrário ter sucesso é $Np(1-p)^{N-1}$;
  - Para obtermos a eficiência máxima para N nós ativos, temos de encontrar um $p^{\star}$ que maximize essa expressão;
  - Para obter a eficiência máxima para um grande número de nós ativos, consideramos o limite de $Np^{\star}(1-p^{\star})^{N-1}$ quando N tende ao infinito;
  - Eficiência máxima do Slotted Aloha: $E = 1/e = 0.37$.

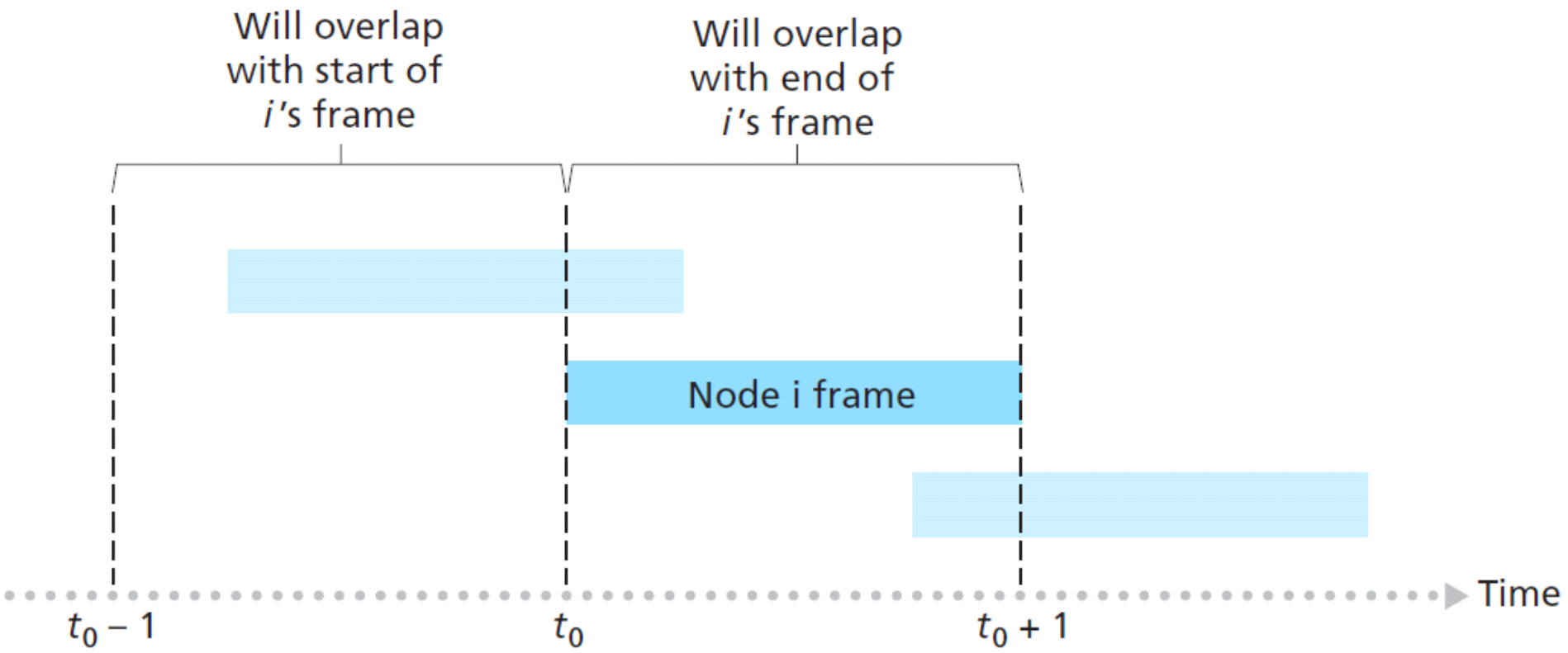
Protocolos de Acesso Aleatório

Protocolo Aloha

- Quando o nó tem um novo pacote para enviar, imediatamente transmite o pacote inteiro ao canal de difusão;
- Se não houver colisão, o nó terá transmitido seu quadro com sucesso;
- Se houver uma colisão, o nó retransmitirá de imediato o pacote com probabilidade p (após ter concluído a transmissão total do quadro que sofreu a colisão);
- Caso contrário, o nó esperará por um tempo de transmissão de pacote;
- Após essa espera, ele então retransmite o pacote com probabilidade p ou espera (permanecendo ocioso) por outro tempo de pacote com probabilidade $1 - p$;
- Eficiência máxima do Aloha puro: $E = 1/2e = 0.185$.

Protocolos de Acesso Aleatório

Protocolo Aloha



Protocolos de Acesso Aleatório

Protocolo CSMA

- Duas regras importantes a serem consideradas:
  - **Ouça antes de falar**: **detecção de portadora**;
  - **Se alguém começar a falar ao mesmo tempo que você, pare de falar**: **detecção de colisão**.
- Essas duas regras estão incorporadas na família de protocolos de **Múltiplo Acesso com Detecção de Portadora** (CSMA - Carrier Sense Multiple Access) e CSMA com **detecção de colisão** (CSMA/CD).

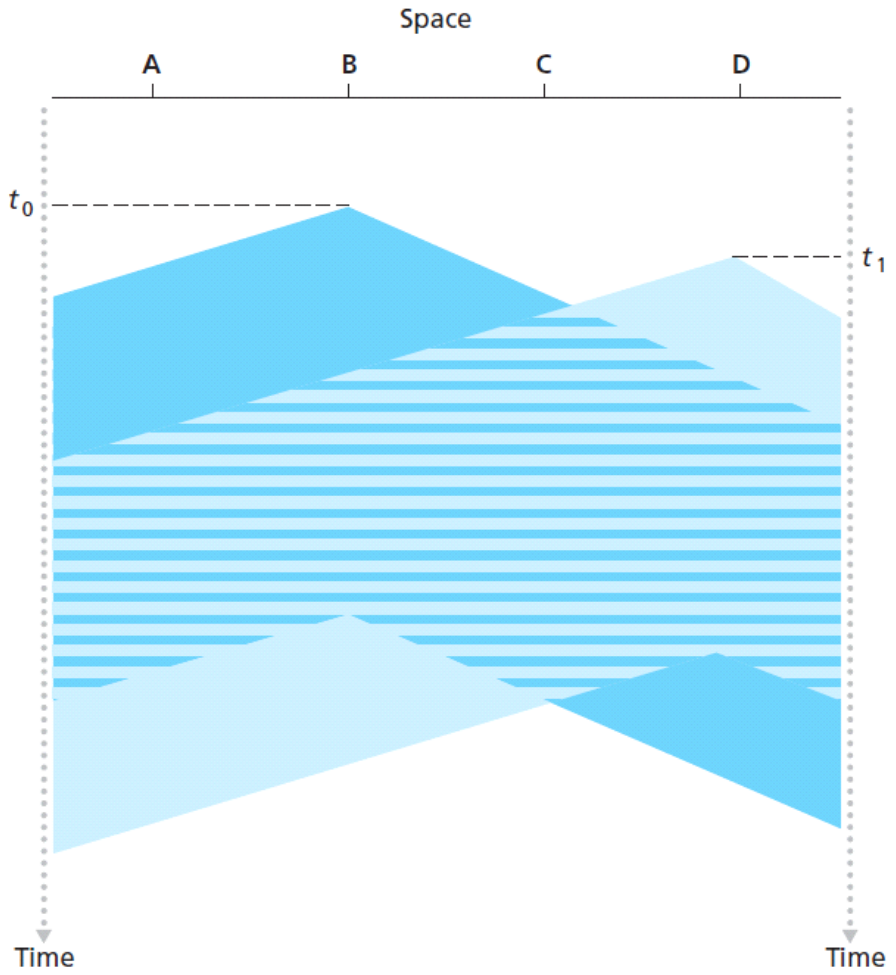
Se todos os nós realizam detecção de portadora, por que ocorrem colisões?

Protocolos de Acesso Aleatório

Protocolo CSMA

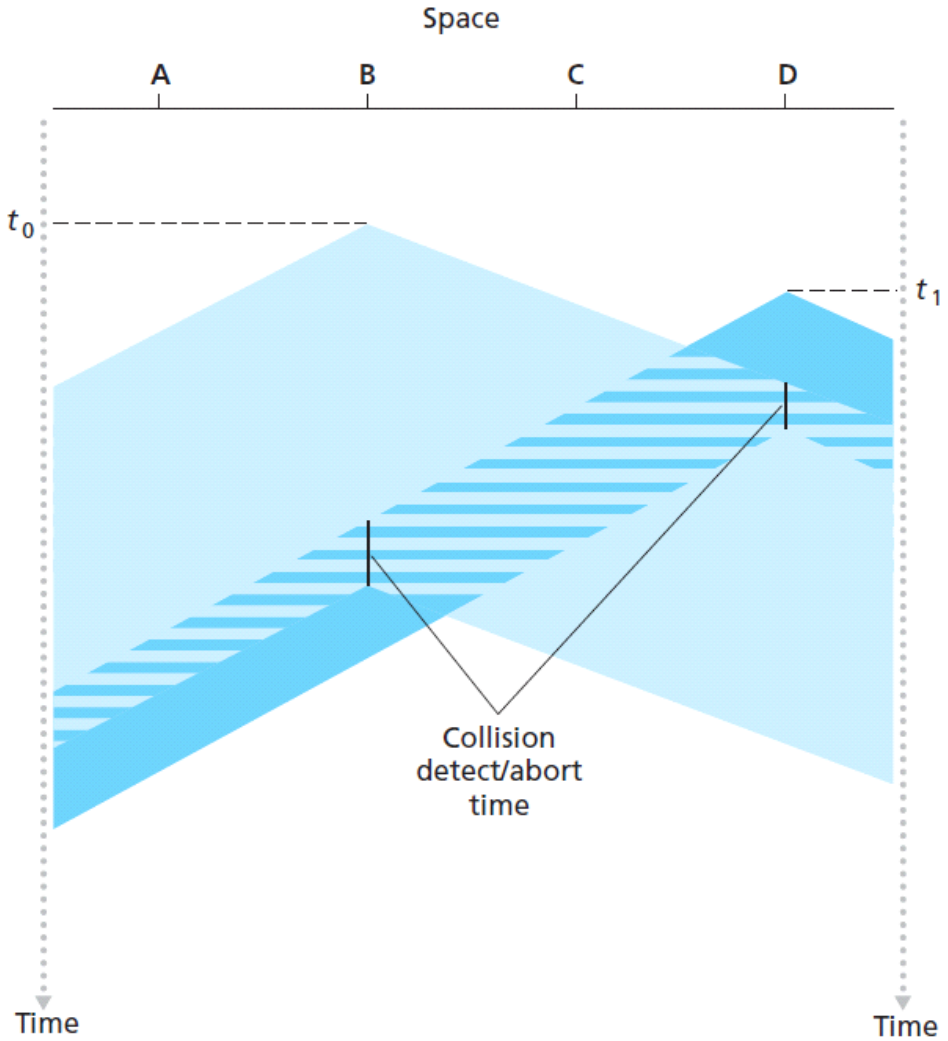
Se todos os nós realizam detecção de portadora, por que ocorrem colisões?

Por causa do atraso de propagação fim a fim de canal.



Protocolos de Acesso Aleatório

Protocolo CSMA/CD



Protocolos de Acesso Aleatório

Protocolo CSMA/CD

1. O adaptador obtém um datagrama da camada de rede, prepara um quadro da camada de enlace e coloca o quadro no buffer do adaptador;
2. Se o adaptador detectar que o canal está ocioso (ou seja, não há energia de sinal entrando nele a partir do canal), ele começa a transmitir o quadro. Caso contrário, ele espera até que não detecte energia de sinal, para então começar a transmitir o quadro;
3. Enquanto transmite, o adaptador monitora a presença de energia de sinal vinda de outros adaptadores usando o canal de difusão;
4. Se transmitir o quadro inteiro sem detectar energia de sinal de outros adaptadores, o adaptador terá terminado com o quadro. Caso contrário, ele aborta a transmissão;
5. Depois de abortar, o adaptador espera por um tempo aleatório e depois retorna à etapa 2.

Protocolos de Acesso Aleatório
Protocolo CSMA/CD

- Se o intervalo for grande e o número de nós colidindo for pequeno, é provável que o canal permaneça muito tempo ocioso;
- Se o intervalo for pequeno e o número de nós colidindo for grande, é provável que os valores aleatórios escolhidos sejam quase os mesmos, e os nós transmitindo colidirão de novo.

Qual seria um bom valor para o tempo de espera aleatório?

Protocolos de Acesso Aleatório

Protocolo CSMA/CD

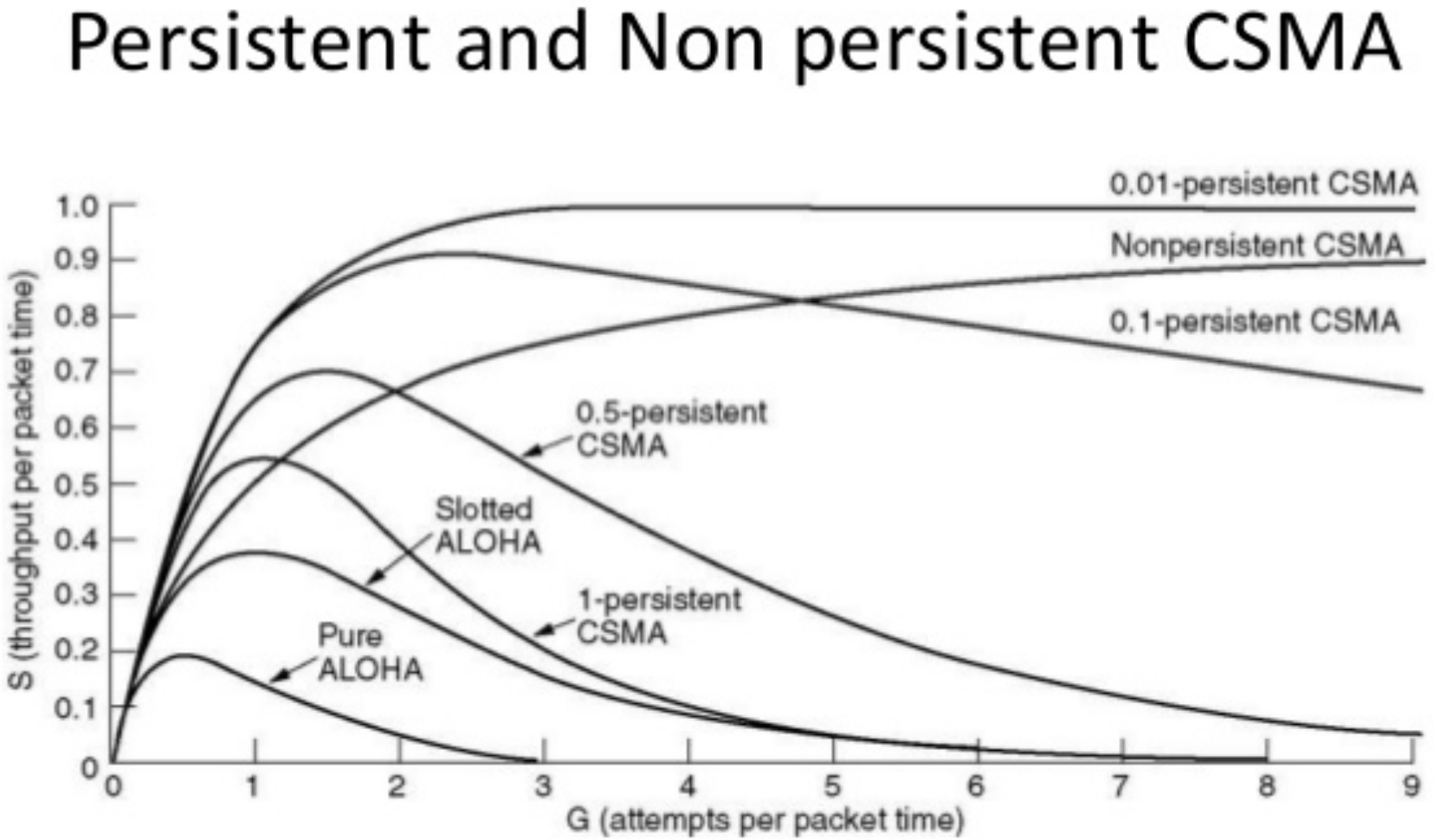
Qual seria um bom valor para o tempo de espera aleatório?

Algoritmo de recuo exponencial binário.

- Ao transmitir um quadro que já tenha experimentado n colisões, um nó escolhe o valor de K (tempo de espera) aleatoriamente a partir de $\{0, 1, 2, \cdots, 2^n - 1\}$;
- Quanto mais colisões um pacote experimentar, maior o intervalo do qual K é escolhido;
- **Exemplo**
  - Um nó transmite um pacote pela primeira vez, mas detecta uma colisão;
  - K é escolhido com probablidade igual entre $\{0, 1\}$. Se escolher $K = 0$, então ele de imediato começa a detectar o canal. Se escolher $K = 1$, ele espera um intervalo antes de iniciar o ciclo de detectar-e-transmitir-quando-ocioso;
  - Após uma segunda colisão, K é escolhido com probablidade igual entre $\{0, 1, 2, 3\}$;
  - Após uma terceira colisão, K é escolhido com probablidade igual entre $\{0, 1, 2, 3, 4, 5, 6, 7\}$;
  - Etc.

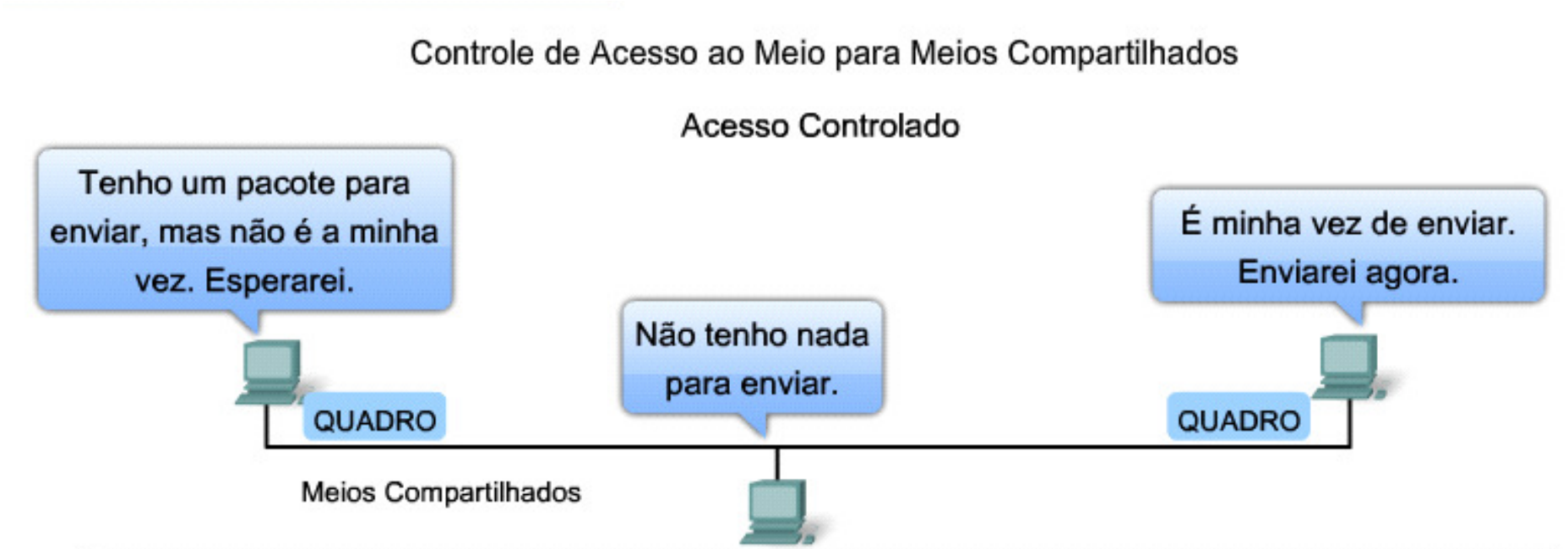
Protocolos de Acesso Aleatório

Comparação entre os Protocolos Aloha e CSMA



Comparison of the channel utilization versus load for various random access protocols

Protocolos de Revezamento



Método	Características	Exemplo
Acesso Controlado	• Apenas uma estação transmite por vez • Dispositivos que desejam transmitir devem esperar a sua vez • Nenhuma colisão • Algumas redes determinísticas utilizam passagem de token	• Token Ring • FDDI

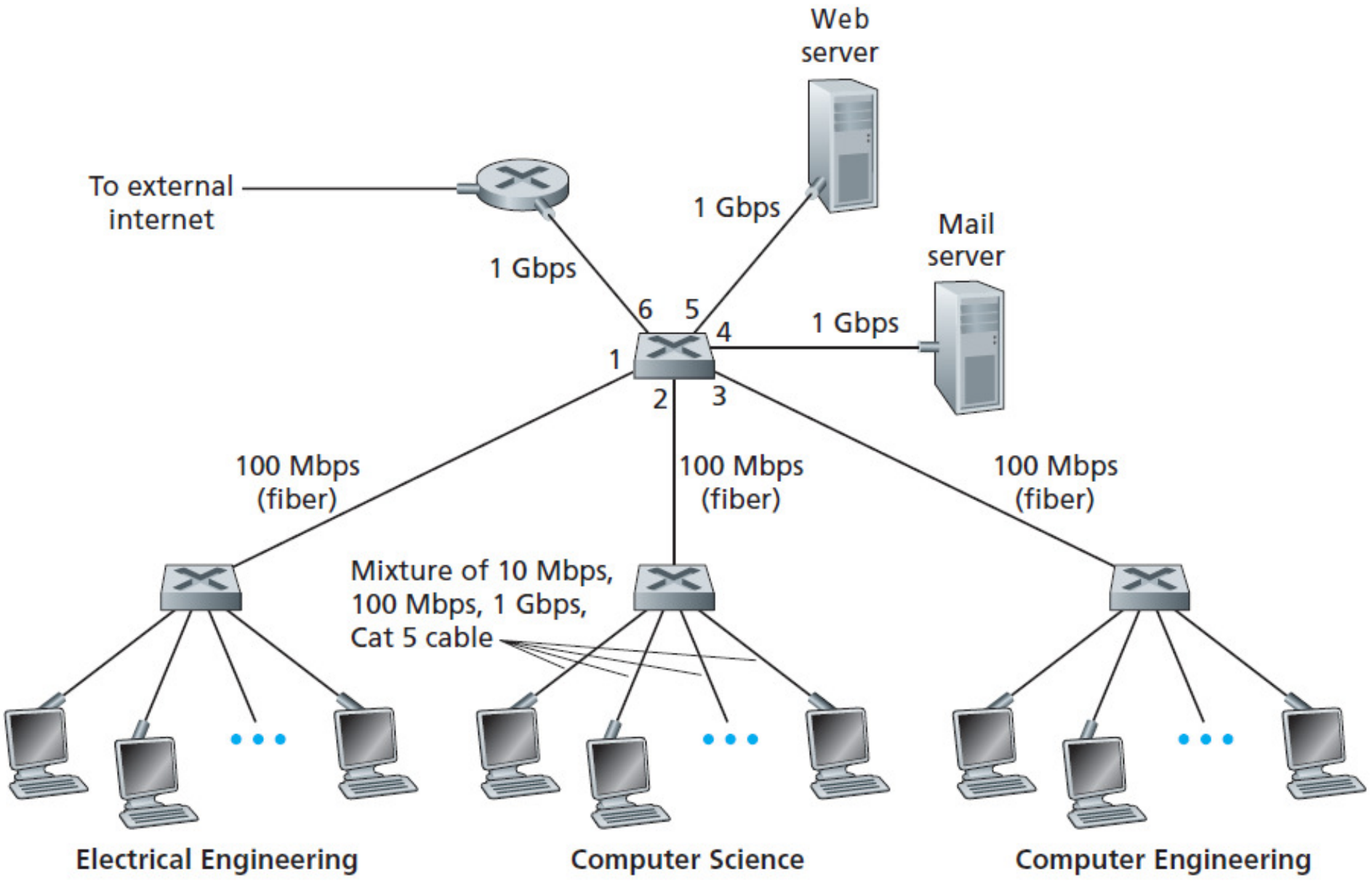
Protocolos de Revezamento

- **Protocolo de Polling (Seleção)**
  - Requer que um dos nós seja designado como mestre;
  - O mestre seleciona cada um dos nós por alternância circular;
  - Elimina as colisões e os intervalos vazios;
  - Introduz um atraso de seleção;
  - Se o nó mestre falhar, o canal inteiro ficará inoperante.

Protocolos de Revezamento

- **Protocolo de Passagem de Permissão (Token)**
  - Um pequeno quadro de finalidade especial conhecido como uma **permissão** (*token*) é passado entre os nós obedecendo a uma determinada ordem fixa;
  - Quando um nó recebe uma permissão, ele a retém apenas se tiver dados para transferir, caso contrário, imediatamente a repassa para o nó seguinte;
  - A passagem de permissão é descentralizada e tem uma alta eficiência;
  - A falha de um nó pode derrubar o canal inteiro;
  - Se um nó acidentalmente se descuida e não libera a permissão, é preciso chamar algum procedimento de recuperação para recolocar a permissão em circulação.

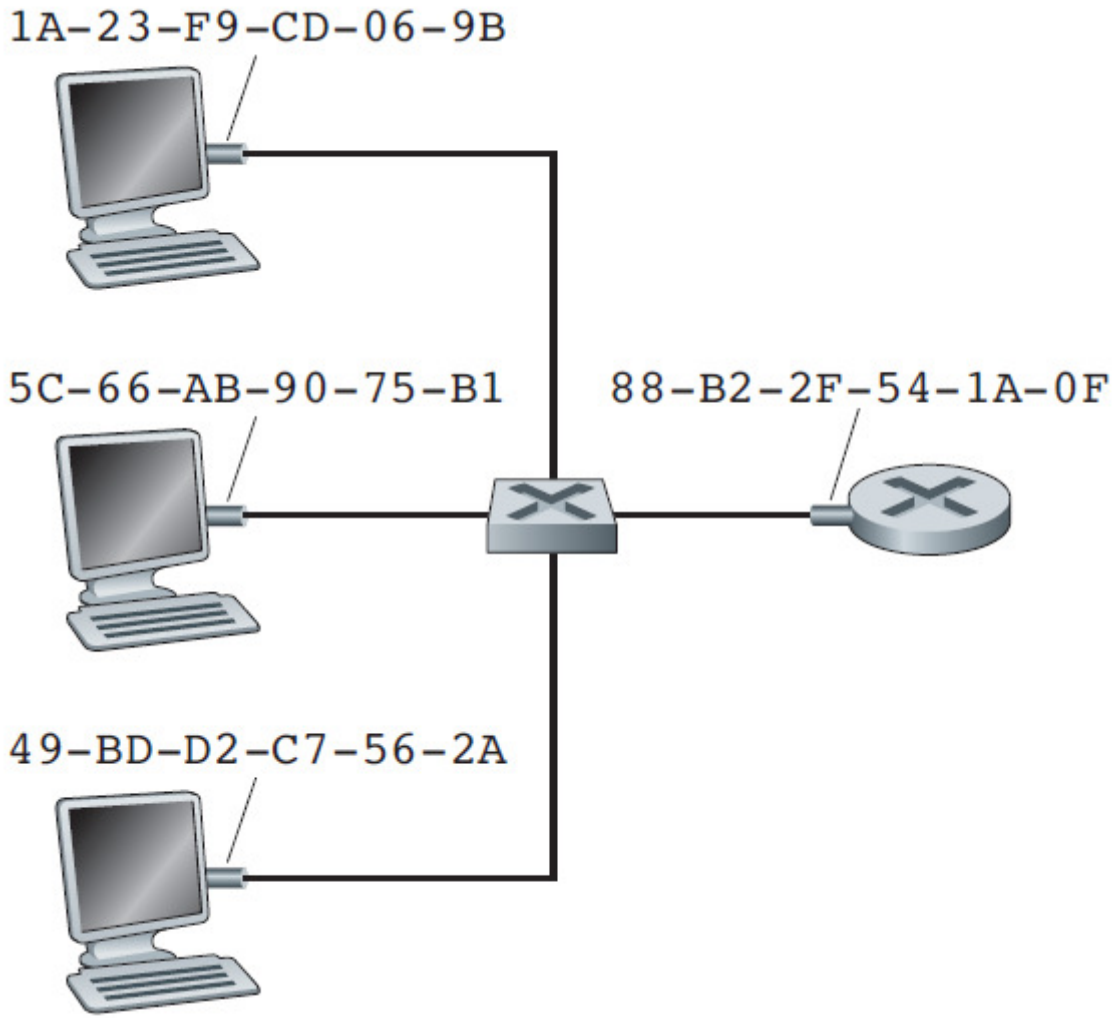
Endereçamento da Camada de Enlace



Endereçamento da Camada de Enlace

- Hosts e roteadores podem ter várias interfaces de rede (adaptadores), cada um possuindo um endereço da camada de enlace (endereço MAC);
- No entanto, os comutadores da camada de enlace (switches) não têm endereços da camada de enlace associados às suas interfaces, que se conectam aos hosts e roteadores;
- Os switches fazem o seu trabalho de modo transparente, sem que o host ou roteador tenha que endereçar o quadro explicitamente para o switch intermediário;
- O endereço MAC tem 6 bytes (notação hexadecimal), o que dá 2^{48} endereços MAC possíveis; atualmente se pode mudar o endereço MAC de um adaptador via software, mas o normal é que ele seja permanente;
- O endereço FF-FF-FF-FF-FF-FF é o endereço de difusão MAC especial.

Endereçamento da Camada de Enlace

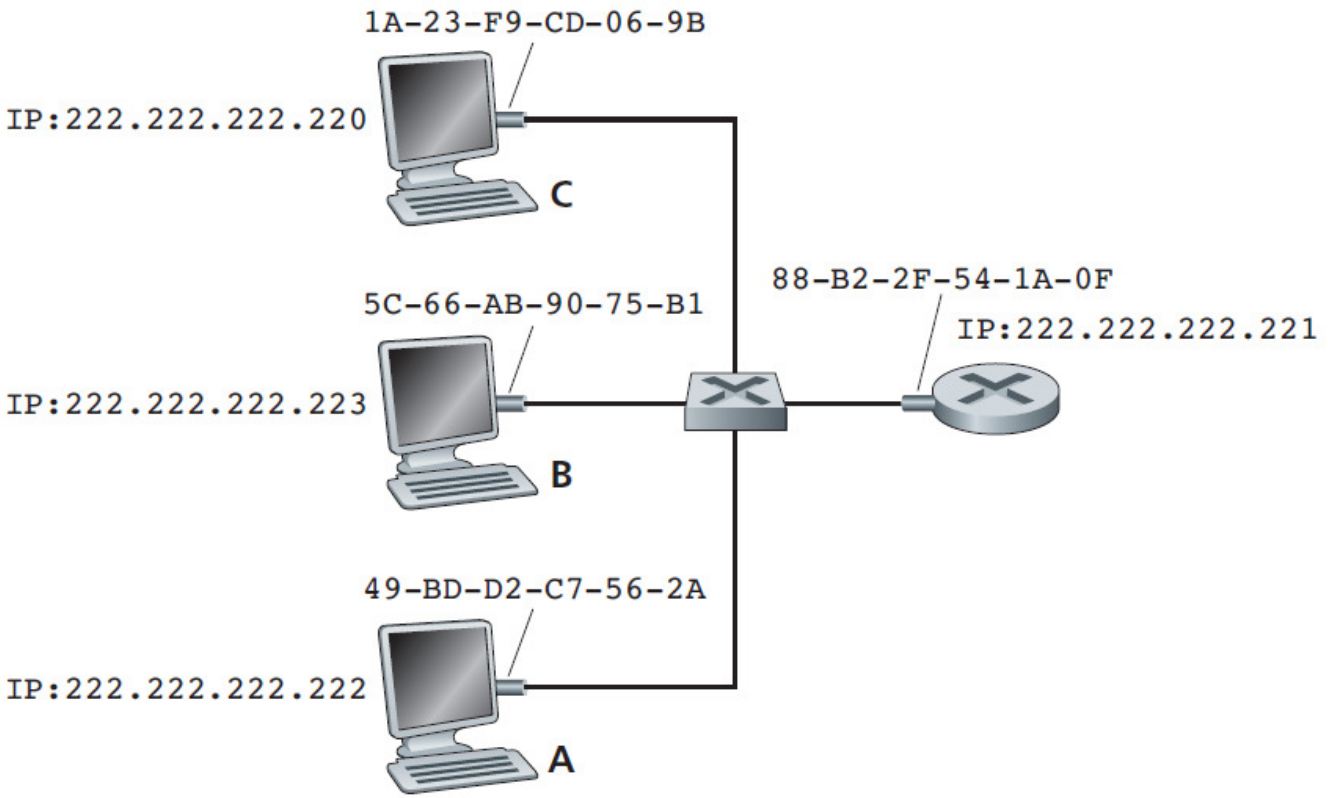


Endereçamento da Camada de Enlace

- O endereço **MAC tem uma estrutura linear**, enquanto o endereço **IP tem uma estrutura hierárquica**;
- Analogia: endereço MAC ➜ CPF; endereço IP ➜ endereço postal;
- O endereço postal de uma pessoa pode mudar se ela muda de cidade, mas seu CPF não;
- Quando um adaptador quer enviar um quadro para algum adaptador de destino, o remetente insere no quadro o endereço MAC de destino e envia o quadro para dentro da LAN;
- Quando um adaptador receber um quadro, ele verificará se o endereço MAC de destino combina com o seu próprio endereço MAC:
  - Se sim, o adaptador extrairá o datagrama encerrado no quadro e o passará para cima na pilha de protocolos;
  - Se não, o adaptador descartará o quadro.

Endereçamento da Camada de Enlace e ARP

Por que é preciso ter endereços na camada de rede e na camada de enlace?



Endereçamento da Camada de Enlace

Por que é preciso ter endereços na camada de rede e na camada de enlace?

- LANs são projetadas para protocolos da camada de rede arbitrários, o protocolo IP não é o único padrão;
- Se adaptadores usassem endereços de camada de rede, em vez de endereços MAC, o endereço de rede teria que ser armazenado na RAM do adaptador e reconfigurado toda vez que este mudasse de local (ou fosse ligado);
- Se não existissem endereços MAC, a tarefa de verificação de combinação de endereço deveria ser feito pela camada de rede; dessa forma a camada de rede do host teria que ser interrompida por cada quadro enviado à LAN;
- Para que as camadas sejam blocos de construção praticamente independentes em uma arquitetura de rede, diferentes camadas precisam ter seu próprio esquema de endereçamento.

Protocolo ARP

- O **Protocolo de Resolução de Endereços** (*Address Resolution Protocol* - ARP) é responsável por fazer a tradução entre endereços da camada de enlace e da camada de rede;
- Cada nó (host ou roteador) tem em sua RAM uma tabela ARP que contém mapeamentos de endereços IP para endereços MAC;
- A tabela ARP é dinâmica; um tempo de remoção típico para um registro é de 20 minutos;
- O protocolo ARP é *plug-and-play*.

Quais as semelhanças e diferenças entre os protocolos ARP e DNS?

Protocolo ARP

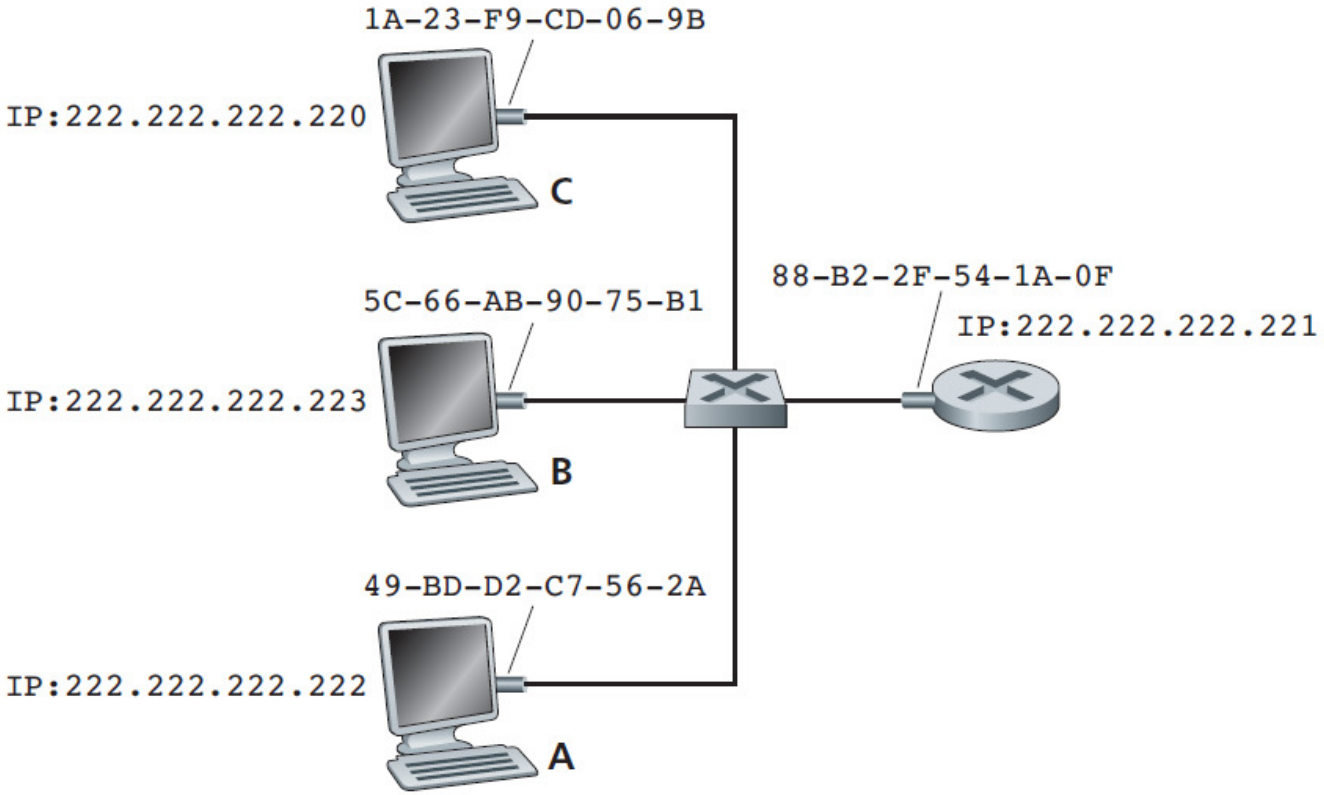
- O Protocolo de Resolução de Endereços (Address Resolution Protocol - ARP) é responsável por fazer a tradução entre endereços da camada de enlace e da camada de rede;
- Cada nó (host ou roteador) tem em sua RAM uma tabela ARP que contém mapeamentos de endereços IP para endereços MAC;
- A tabela ARP é dinâmica; um tempo de remoção típico para um registro é de 20 minutos;
- O protocolo ARP é *plug-and-play*.

Quais as semelhanças e diferenças entre os protocolos ARP e DNS?

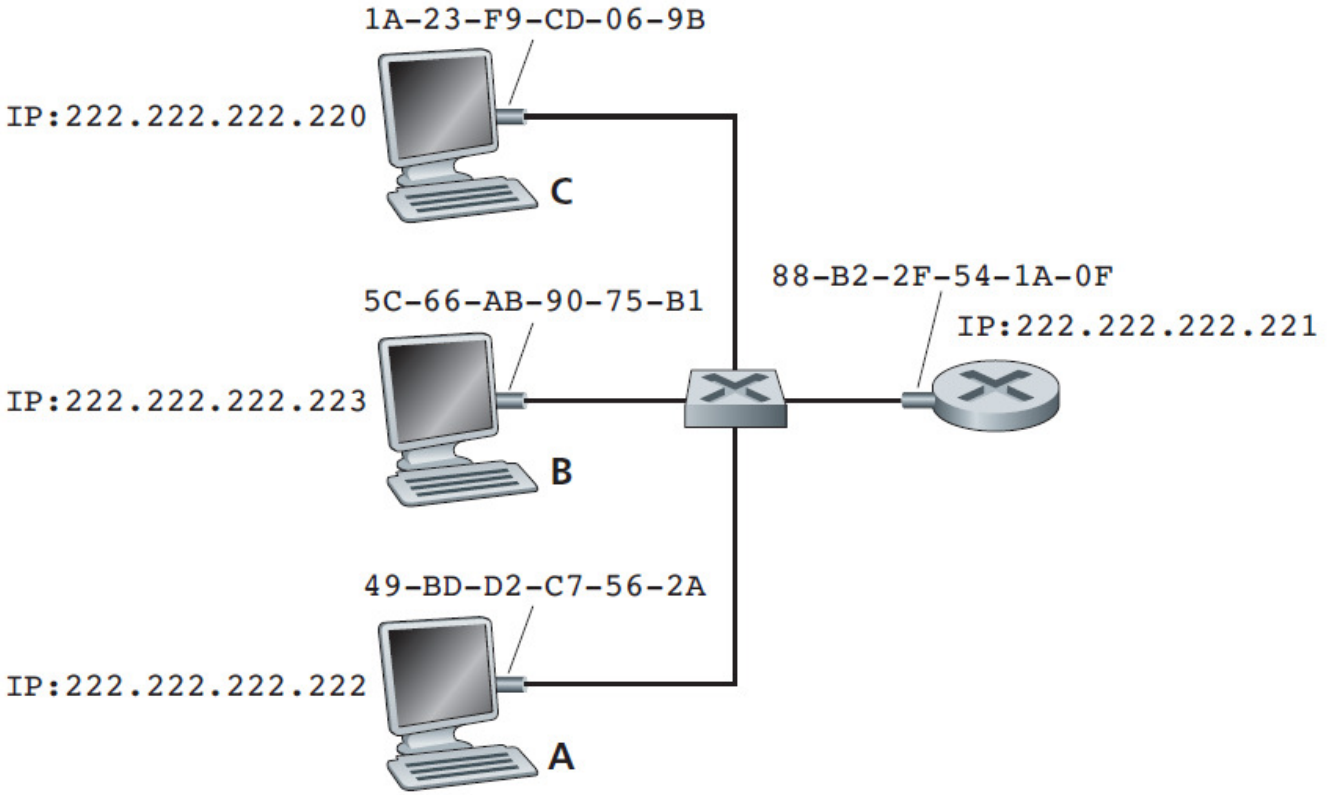
- O DNS converte nomes de hosts para endereços IP, enquanto que o ARP converte endereços IP em endereços MAC;
- O DNS faz a conversão para máquinas em qualquer lugar do mundo, ao passo que o ARP faz a conversão apenas para nós na mesma sub-rede.

Protocolo ARP

Como o host com endereço IP 222.222.222.220 consegue enviar um datagrama IP para o host 222.222.222.222?



Protocolo ARP

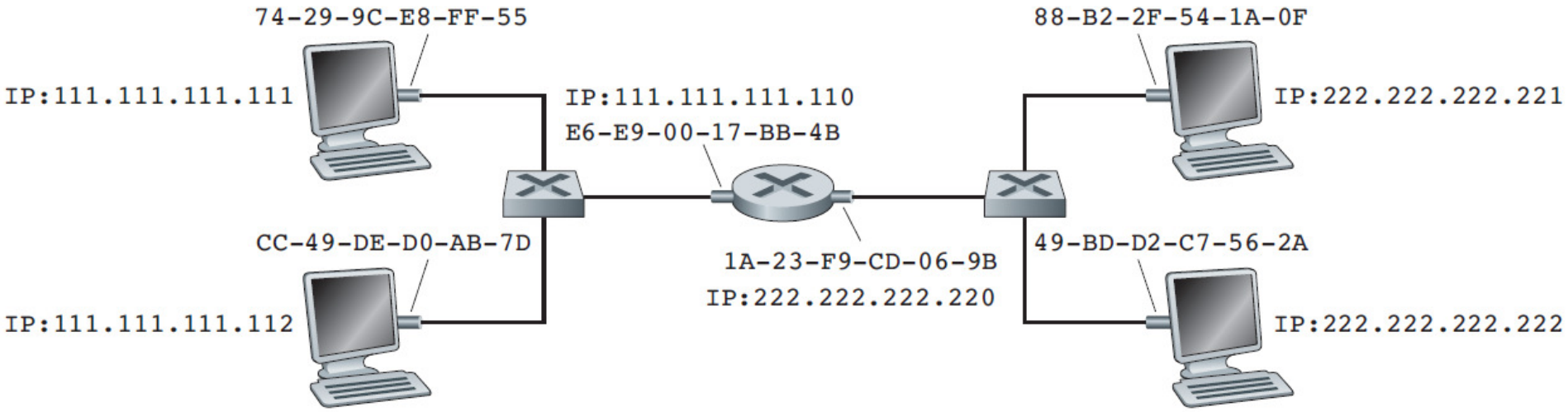


IP Address	MAC Address	TTL
222.222.222.221	88-B2-2F-54-1A-0F	13:45:00
222.222.222.223	5C-66-AB-90-75-B1	13:52:00

Endereçamento da Camada de Enlace e ARP

Como o host com endereço IP 111.111.111.111 consegue enviar um datagrama IP para o host 222.222.222.222?

Duas sub-redes interconectadas por um roteador

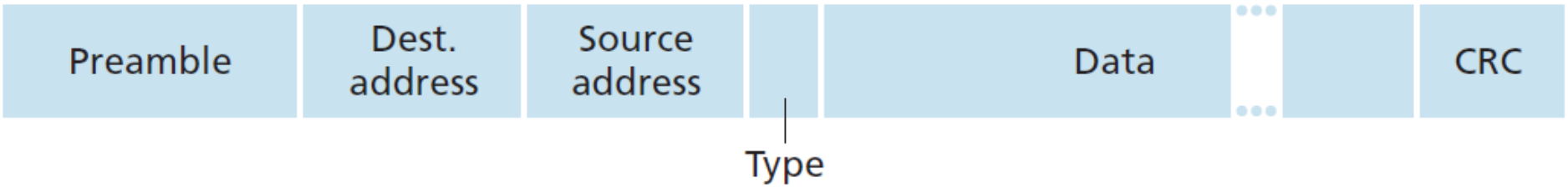


Ethernet

- A Ethernet tornou-se o padrão dominante nas redes locais;
- Atualmente, a Ethernet é para a rede local o que a Internet é para a rede global;
- Razões para o sucesso da Ethernet:
  - Foi a primeira LAN de alta velocidade amplamente disseminada;
  - É mais barata e menos complexa que seus concorrentes, por ex. token ring, FDDI e ATM.
- Evolução da Ethernet:
  1. Década de 70: Topologia em barramento, cabo coaxial, CSMA/CD;
  2. Metade da década de 90: Topologia em estrela com hub, cabo de par trançado, CSMA/CD;
  3. Começo dos anos 2000: Topologia em estrela com comutador (switch), cabo de par trançado e fibra óptica, comutação de pacotes (armazenar-e-repassar).

Ethernet

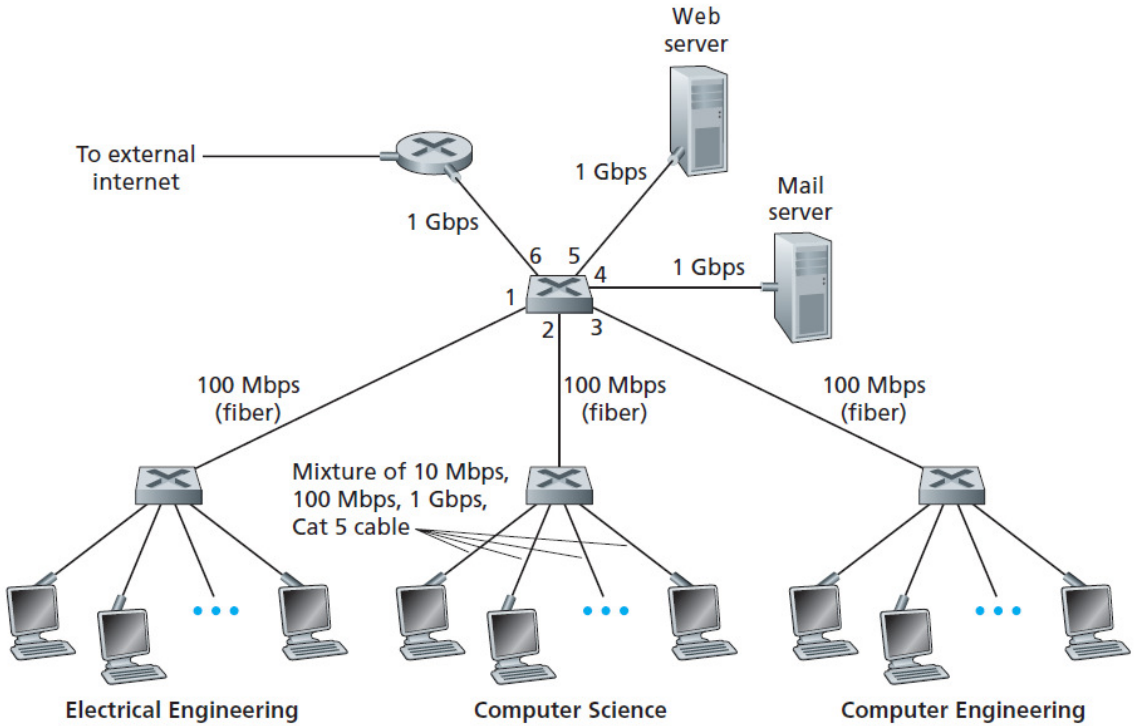
- A Ethernet fornece serviço não orientado para conexão à camada de rede;
- A Ethernet fornece um serviço não confiável à camada de rede;
- Se houver lacunas por causa de quadros Ethernet descartados, aplicações que usam UDP verão as lacunas, enquanto as que usam TCP solicitarão uma retransmissão do segmento TCP.



Comutadores da Camada de Enlace

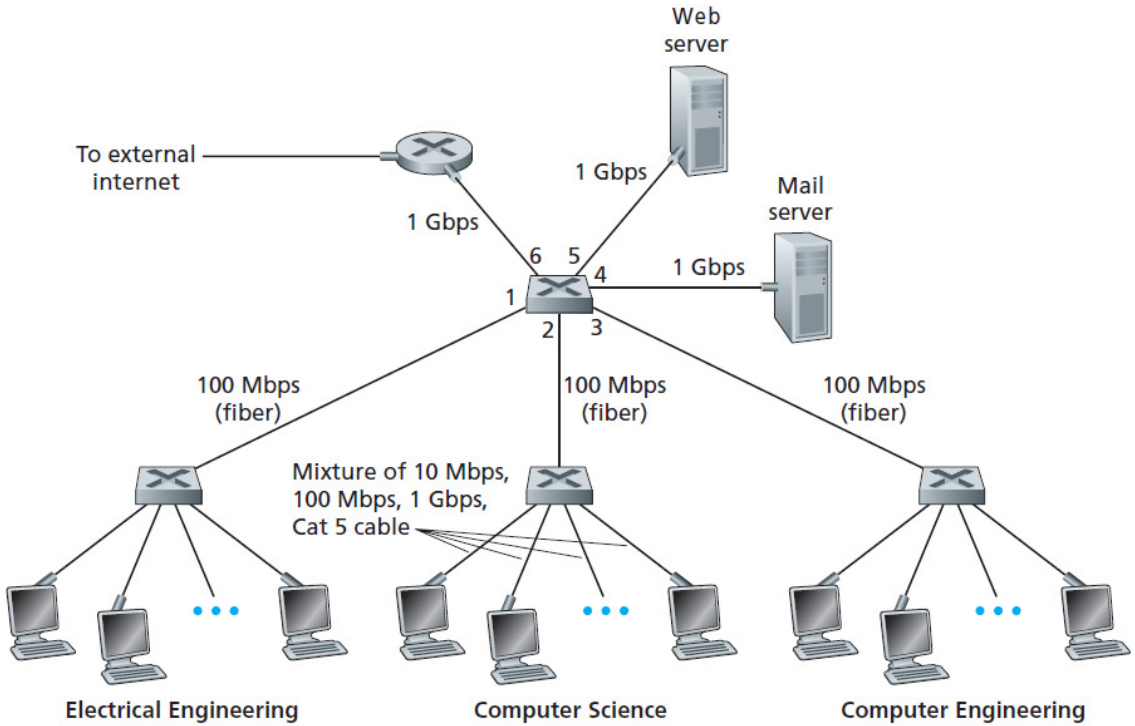
- **Filtragem** é a capacidade de um comutador que determina se um quadro deve ser repassado para alguma interface ou se deve apenas ser descartado;
- **Repasse** é a capacidade de um comutador que determina as interfaces para as quais um quadro deve ser dirigido e então dirigir o quadro a essas interfaces;
- Filtragem e repasse por comutadores são feitos com uma **tabela de comutação**;
- Comutadores são **autodidatas**, são dispositivos ***plug-and-play***, e utilizam comunicação **full-duplex**.

Comutadores da Camada de Enlace



Address	Interface	Time
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
....	....	....

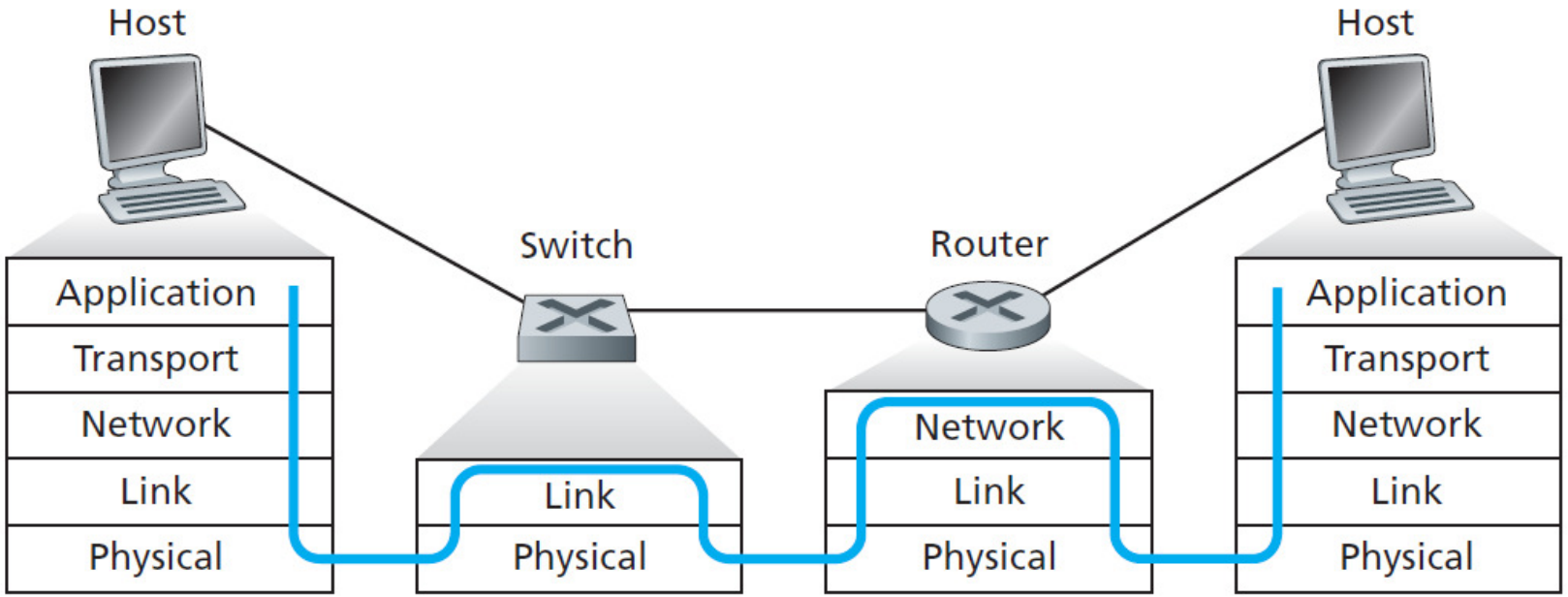
Comutadores da Camada de Enlace



Address	Interface	Time
01-12-23-34-45-56	2	9:39
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36

Comutadores da Camada de Enlace

- Propriedades de comutação da camada de enlace
  - Eliminação de colisões;
  - Enlaces heterogêneos;
  - Maior segurança.
  - Facilidade de gerenciamento;



Comutadores da Camada de Enlace

Quais as semelhanças e diferenças entre um comutador (switch) e um roteador?

Comutadores da Camada de Enlace

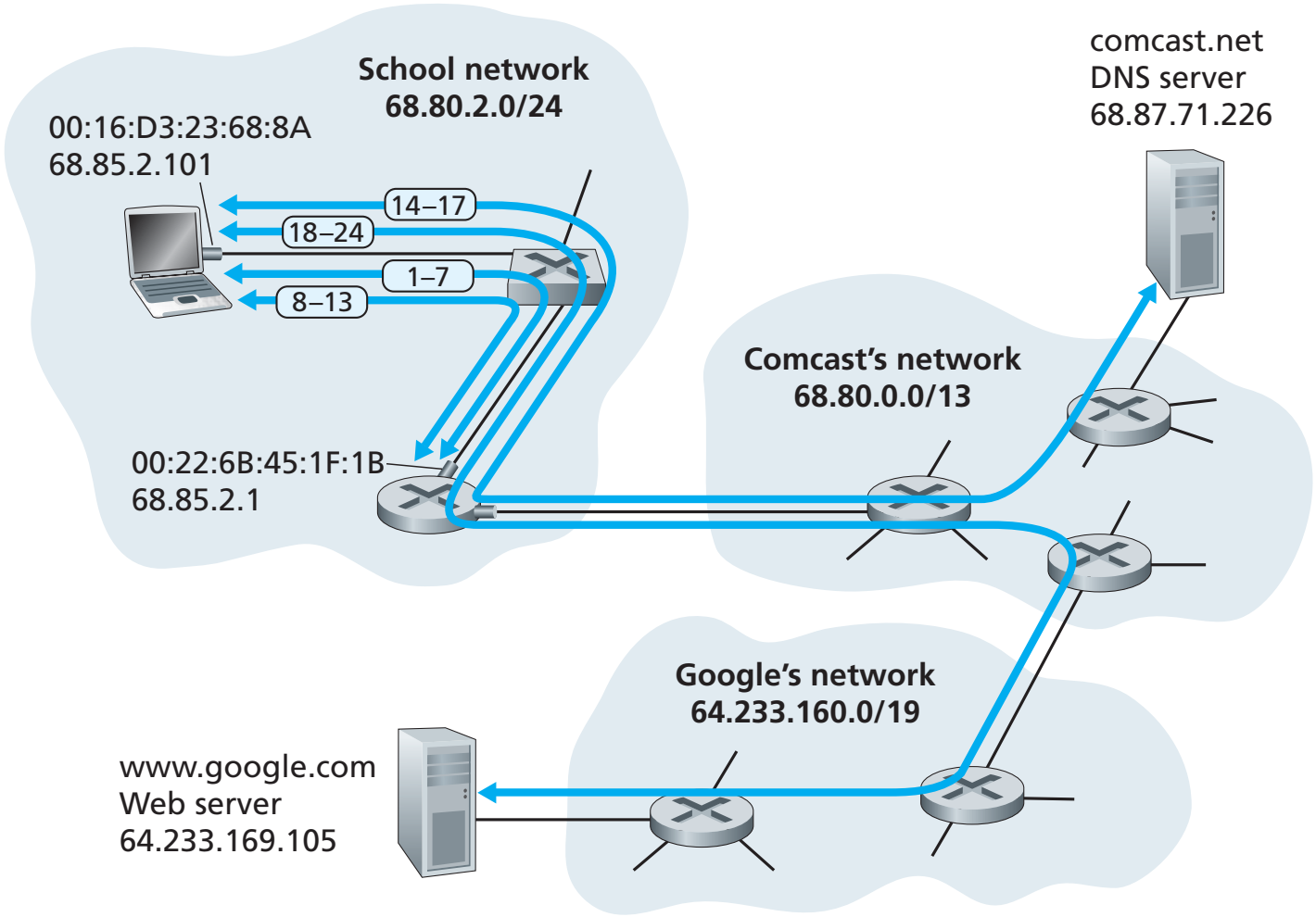
Quais as semelhanças e diferenças entre um comutador (switch) e um roteador?

- Ambos são comutadores de pacotes do tipo armazena-e-repassa;
- Um roteador é um comutador de pacotes da camada 3, enquanto que um comutador opera com protocolos da camada 2 (comutadores são mais rápidos);
- Ambos permitem isolamento de tráfego, mas o isolamento dos roteadores é mais robusto;
- Comutadores são plug-and-play, enquanto que os roteadores não;
- Roteadores usam rotas "mais inteligentes" entre os hosts da rede;
- Roteadores oferecem proteção de firewall contra as tempestades de difusão da camada 2.

De um modo geral, comutadores são usados em redes locais com algumas centenas de hosts, enquanto que roteadores (além de comutadores) são usados em redes com milhares de hosts.

Um Dia na Vida de uma Solicitação de Página Web

Bob conecta seu notebook ao switch Ethernet da sua escola e faz o download da página web www.google.com.



Um Dia na Vida de uma Solicitação de Página Web

Fase 1

DHCP, UDP, IP e Ethernet

Um Dia na Vida de uma Solicitação de Página Web

1. The operating system on Bob's laptop creates a **DHCP request message** and puts this message within a **UDP segment** with destination port 67 (DHCP server) and source port 68 (DHCP client). The UDP segment is then placed within an **IP datagram** with a broadcast IP destination address (255.255.255.255) and a source IP address of 0.0.0.0, since Bob's laptop doesn't yet have an IP address.

Um Dia na Vida de uma Solicitação de Página Web

2. The IP datagram containing the DHCP request message is then placed within an Ethernet frame. The **Ethernet frame** has a destination MAC addresses of FF:FF:FF:FF:FF:FF so that the frame will be broadcast to all devices connected to the switch (hopefully including a DHCP server); the frame's source MAC address is that of Bob's laptop, 00:16:D3:23:68:8A.

Um Dia na Vida de uma Solicitação de Página Web

3. The broadcast Ethernet frame containing the DHCP request is the first frame sent by Bob's laptop to the Ethernet switch. The switch broadcasts the incoming frame on all outgoing ports, including the port connected to the router.

Um Dia na Vida de uma Solicitação de Página Web

4. The router receives the broadcast Ethernet frame containing the DHCP request on its interface with MAC address 00:22:6B:45:1F:1B and the IP datagram is extracted from the Ethernet frame. The datagram's broadcast IP destination address indicates that this IP datagram should be processed by upper layer protocols at this node, so the datagram's payload (a UDP segment) is thus **demultiplexed** up to UDP, and the DHCP request message is extracted from the UDP segment. The DHCP server now has the DHCP request message.

Um Dia na Vida de uma Solicitação de Página Web

5. Let's suppose that the DHCP server running within the router can allocate IP addresses in the **CIDR** block 68.85.2.0/24. In this example, all IP addresses used within the school are thus within Comcast's address block. Let's suppose the DHCP server allocates address 68.85.2.101 to Bob's laptop. The DHCP server creates a **DHCP ACK message** containing this IP address, as well as the IP address of the DNS server (68.87.71.226), the IP address for the default gateway router (68.85.2.1), and the subnet block (68.85.2.0/24) (equivalently, the "network mask"). The DHCP message is put inside a UDP segment, which is put inside an IP datagram, which is put inside an Ethernet frame. The Ethernet frame has a source MAC address of the router's interface to the home network (00:22:6B:45:1F:1B) and a destination MAC address of Bob's laptop (00:16:D3:23:68:8A).

Um Dia na Vida de uma Solicitação de Página Web

6. The Ethernet frame containing the DHCP ACK is sent (unicast) by the router to the switch. Because the switch is **self-learning** and previously received an Ethernet frame (containing the DHCP request) from Bob's laptop, the switch knows to forward a frame addressed to 00:16:D3:23:68:8A only to the output port leading to Bob's laptop.

Um Dia na Vida de uma Solicitação de Página Web

7. Bob's laptop receives the Ethernet frame containing the DHCP ACK, extracts the IP datagram from the Ethernet frame, extracts the UDP segment from the IP datagram, and extracts the DHCP ACK message from the UDP segment. Bob's DHCP client then records its IP address and the IP address of its DNS server. It also installs the address of the default gateway into its **IP forwarding** table. Bob's laptop will send all datagrams with destination address outside of its subnet 68.85.2.0/24 to the default gateway. At this point, Bob's laptop has initialized its networking components and is ready to begin processing the Web page fetch. Note that only the last two DHCP steps are actually necessary.)

Um Dia na Vida de uma Solicitação de Página Web

Fase 2

DNS e ARP

Um Dia na Vida de uma Solicitação de Página Web

8. The operating system on Bob's laptop thus creates a **DNS query message**, putting the string "www.google.com" in the question section of the DNS message. This DNS message is then placed within a UDP segment with a destination port of 53 (DNS server). The UDP segment is then placed within an IP datagram with an IP destination address of 68.87.71.226 (the address of the DNS server returned in the DHCP ACK in step 5) and a source IP address of 68.85.2.101.

Um Dia na Vida de uma Solicitação de Página Web

9. Bob's laptop then places the datagram containing the DNS query message in an Ethernet frame. This frame will be sent (addressed, at the link layer) to the gateway router in Bob's school's network. However, even though Bob's laptop knows the IP address of the school's gateway router (68.85.2.1) via the DHCP ACK message in step 5 above, it doesn't know the gateway router's MAC address. In order to obtain the MAC address of the gateway router, Bob's laptop will need to use the **ARP protocol**.

Um Dia na Vida de uma Solicitação de Página Web

10. Bob's laptop creates an **ARP query** message with a target IP address of 68.85.2.1 (the default gateway), places the ARP message within an Ethernet frame with a broadcast destination address (FF:FF:FF:FF:FF:FF) and sends the Ethernet frame to the switch, which delivers the frame to all connected devices, including the gateway router.

Um Dia na Vida de uma Solicitação de Página Web

11. The gateway router receives the frame containing the ARP query message on the interface to the school network, and finds that the target IP address of 68.85.2.1 in the ARP message matches the IP address of its interface. The gateway router thus prepares an **ARP reply**, indicating that its MAC address of 00:22:6B:45:1F:1B corresponds to IP address 68.85.2.1. It places the ARP reply message in an Ethernet frame, with a destination address of 00:16:D3:23:68:8A (Bob's laptop) and sends the frame to the switch, which delivers the frame to Bob's laptop.

Um Dia na Vida de uma Solicitação de Página Web

12. Bob's laptop receives the frame containing the ARP reply message and extracts the MAC address of the gateway router (00:22:6B:45:1F:1B) from the ARP reply message.

Um Dia na Vida de uma Solicitação de Página Web

13. Bob's laptop can now (finally!) address the Ethernet frame containing the DNS query to the gateway router's MAC address. Note that the IP datagram in this frame has an IP destination address of 68.87.71.226 (the DNS server), while the frame has a destination address of 00:22:6B:45:1F:1B (the gateway router). Bob's laptop sends this frame to the switch, which delivers the frame to the gateway router.

Um Dia na Vida de uma Solicitação de Página Web

Fase 3

Roteador Intradomínio ao Servidor DNS

Um Dia na Vida de uma Solicitação de Página Web

14. The gateway router receives the frame and extracts the IP datagram containing the DNS query. The router looks up the destination address of this datagram (68.87.71.226) and determines from its forwarding table that the datagram should be sent to the leftmost router in the Comcast network in the figure. The IP datagram is placed inside a link-layer frame appropriate for the link connecting the school's router to the leftmost Comcast router and the frame is sent over this link.

Um Dia na Vida de uma Solicitação de Página Web

15. The leftmost router in the Comcast network receives the frame, extracts the IP datagram, examines the datagram's destination address (68.87.71.226) and determines the outgoing interface on which to forward the datagram towards the DNS server from its forwarding table, which has been filled in by Comcast's intra-domain protocol (such as RIP, OSPF or IS-IS) as well as the Internet's inter-domain protocol, BGP.

Um Dia na Vida de uma Solicitação de Página Web

16. Eventually the IP datagram containing the DNS query arrives at the DNS server. The DNS server extracts the DNS query message, looks up the name www.google.com in its DNS database, and finds the DNS resource record that contains the IP address (64.233.169.105) for www.google.com. (assuming that it is currently cached in the DNS server). Recall that this cached data originated in the authoritative DNS server for google.com. The DNS server forms a DNS reply message containing this hostname-to-IP address mapping, and places the DNS reply message in a UDP segment, and the segment within an IP datagram addressed to Bob's laptop (68.85.2.101). This datagram will be forwarded back through the Comcast network to the school's router and from there, via the Ethernet switch to Bob's laptop.

Um Dia na Vida de uma Solicitação de Página Web

17. Bob's laptop extracts the IP address of the server www.google.com from the DNS message. Finally, after a lot of work, Bob's laptop is now ready to contact the www.google.com server!

Um Dia na Vida de uma Solicitação de Página Web

Fase 4

Interação Cliente-Servidor Web: TCP e HTTP

Um Dia na Vida de uma Solicitação de Página Web

18. Now that Bob's laptop has the IP address of www.google.com, it can create the TCP socket that will be used to send the HTTP GET message to www.google.com. When Bob creates the TCP socket, the TCP in Bob's laptop must first perform a three-way handshake with the TCP in www.google.com. Bob's laptop thus first creates a TCP SYN segment with destination port 80 (for HTTP), places the TCP segment inside an IP datagram with a destination IP address of 64.233.169.105 (www.google.com), places the datagram inside a frame with a destination MAC address of 00:22:6B:45:1F:1B (the gateway router) and sends the frame to the switch.

Um Dia na Vida de uma Solicitação de Página Web

19. The routers in the school network, Comcast's network, and Google's network forward the datagram containing the TCP SYN towards www.google.com, using the forwarding table in each router, as in steps 14-16 above. Recall that the router forwarding table entries governing forwarding of packets over the interdomain link between the Comcast and Google networks are determined by the BGP protocol.

Um Dia na Vida de uma Solicitação de Página Web

20. Eventually, the datagram containing the TCP SYN arrives at www.google.com. The TCP SYN message is extracted from the datagram and demultiplexed to the welcome socket associated with port 80. A connection socket is created for the TCP connection between the Google HTTP server and Bob's laptop. A TCP SYNACK segment is generated, placed inside a datagram addressed to Bob's laptop, and finally placed inside a link-layer frame appropriate for the link connecting www.google.com to its first-hop router.

Um Dia na Vida de uma Solicitação de Página Web

21. The datagram containing the TCP SYNACK segment is forwarded through the Google, Comcast, and school networks, eventually arriving at the Ethernet card in Bob's laptop. The datagram is demultiplexed within the operating system to the TCP socket created in step 18, which enters the connected state.

Um Dia na Vida de uma Solicitação de Página Web

22. With the socket on Bob's laptop now(finally!) ready to send bytes to www.google.com, Bob's browser creates the HTTP GET message containing the URL to be fetched. The HTTP GET message is then written into the socket, with the GET message becoming the payload of a TCP segment. The TCP segment is placed in a datagram and sent and delivered to www.google.com as in steps 18-20 above.

Um Dia na Vida de uma Solicitação de Página Web

23. The HTTP server at www.google.com reads the HTTP GET message from the TCP socket, creates an HTTP response message, places the requested Web page content in the body of the HTTP response message, and sends the message into the TCP socket.

Um Dia na Vida de uma Solicitação de Página Web

24. The datagram containing the HTTP reply message is forwarded through the Google, Comcast, and school networks, and arrives at Bob's laptop. Bob's Web browser program reads the HTTP response from the socket, extracts the html for the Web page from the body of the HTTP response, and finally (finally!) displays the Web page!