# CAMADA DE REDE

### 4.1. Introdução

Transporta pacotes de um **hospedeiro remetente a um hospedeiro destinatário.**

**Roteador:** repassar datagramas de enlaces de entrada para enlaces de saída.

**Repasse:** Enlace de entrada de um roteador para o enlace de saída apropriado.

**Roteamento**: Rota ou o caminho dos pacotes de um remetente a um destinatário.

**Tabela de Repasse:** cada roteador tem, indica qual das interfaces de enlace do roteador o pacote deve ser repassado. O algoritmo de roteamento determina os valores inseridos.

**Estabelecimento de conexão:** Algumas arquiteturas de camada de rede (ATM, frame-relay e MPLS) exigem que roteadores ao longo do caminho troquem mensagens entre si para estabelecer estado antes que pacotes possam começar a fluir.

A camada de rede da Internet fornece o modelo de serviço **serviço de melhor esforço.**

### 4.2. Redes de Circuitos Virtuais e de Datagramas

##### 4.2.1. Redes de circuitos virtuais (redes de CV)

Serviço **orientado para conexão** (ATM e frame relay).

1. Um caminho (enlaces e roteadores entre hospedeiros de origem e destino);
2. Número de CVs no cabeçalho: um número para cada enlace ao longo do caminho;
3. Registros na tabela de repasse em cada roteador ao longo do caminho

O roteador determina o novo número de CV para um pacote que passa por ele. A tabela de repasse de cada roteador tem a tradução do número de CV. (+ complexo)

**Mantém informação de estado de conexão**

Há três fases que podem ser identificadas em um circuito virtual:

**1. Estabelecimento de CV:** rota determinada e registros colocados nas tabelas de repasse

**2. Transferência de dados.**

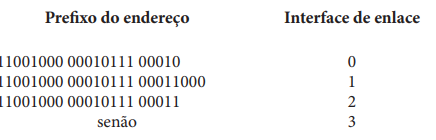
**3. Encerramento do CV:** atualiza as tabelas de repasse tirando os registros

##### 4.2.2. Redes de datagramas

Serviço **NÃO orientado para conexão**

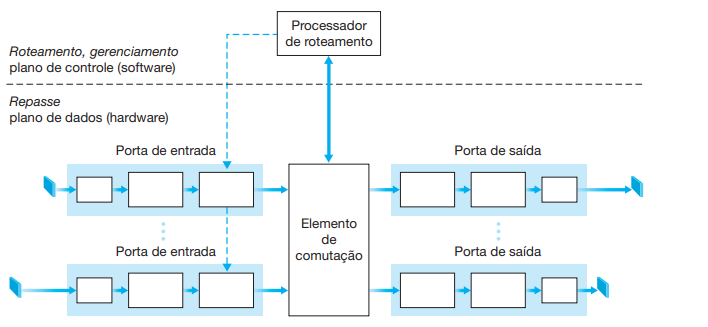
Marca o pacote com o endereço de destino e então o envia para dentro da rede.

Tabela de repasse: Regra da concordância do prefixo mais longo.



As tabelas de repasse podem ser modificadas a qualquer momento, uma série de pacotes pode seguir caminhos diferentes pela rede e chegar fora da ordem.

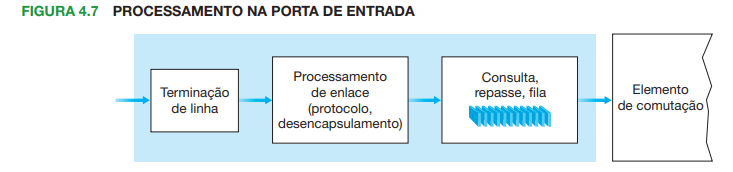
### 4.3. O que há dentro de um roteador?



##### 4.3.1. Processamento de entrada

Terminação de linha e processamento de enlace: funções das camadas física e de enlace.

Pesquisa: Cópia de tabela de repasse determina a porta de saída, evitando gargalo.

Número de versão, soma de verificação e tempo de vida do pacote são verificados, os dois últimos reescritos; contadores usados para o gerenciamento de rede devem ser atualizados.

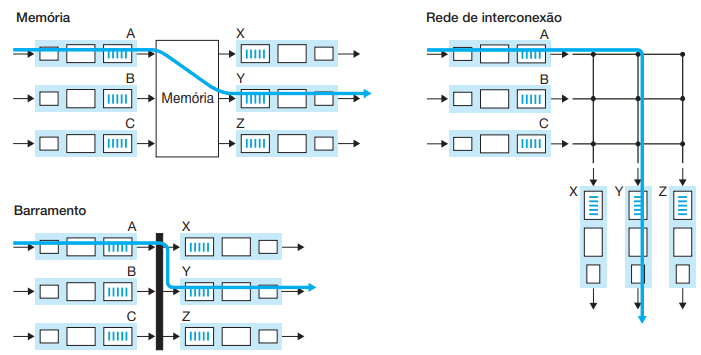
##### 4.3.2. Elementos de comutação

Pacotes são comutados de uma porta de entrada para uma porta de saída.

**Comutação por memória:** primeiros roteadores, computador real. Sinaliza por interrupção, copia para a memória RAM e extrai o endereço de destino, consulta a porta na tabela de repasse e copia nos buffers da porta de saída. Dois pacotes não são repassados ao mesmo tempo. Rot. modernos: consulta do destino e armazenamento pelos processadores nas placas de linha de entrada, parecem com multiprocessadores de memória compartilhada.

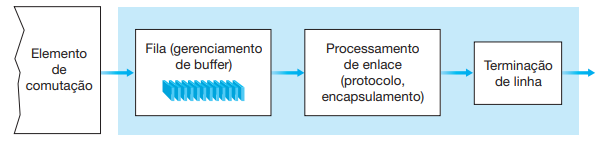
**Comutação por barramento:** barramento compartilhado sem processador de roteamento. Porta de entrada insere um rótulo da porta de destino ao comutador, recebido por todas as portas de saída e a porta do rótulo manterá o pacote. Apenas um pacote pode cruzar o barramento de cada vez: velocidade de comutação limitada à velocidade do barramento.

**Comutação por uma rede de interconexão:** Vários pacotes em paralelo, porém somente um pacote pode ser enviado por barramento de cada vez. 2n barramentos que conectam n portas de entrada com n portas de saída.



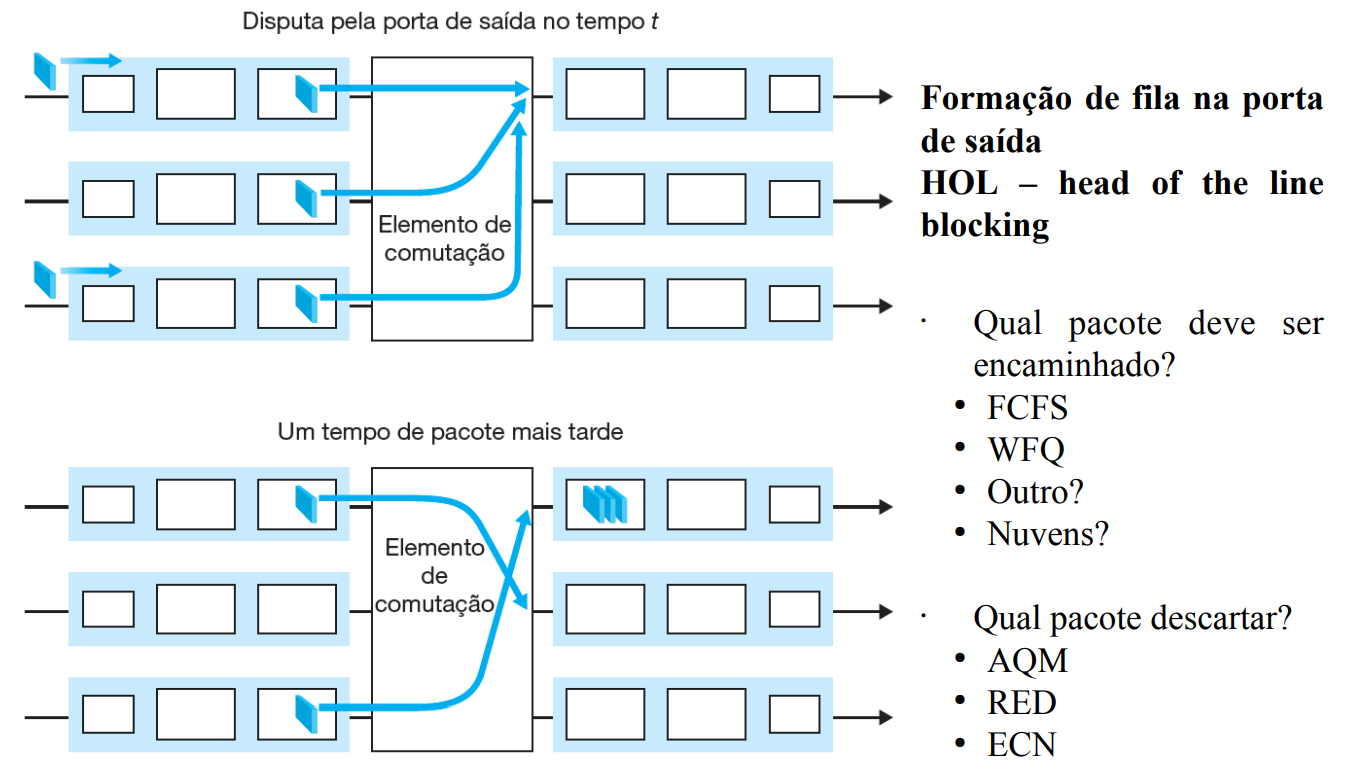
##### 4.3.3. Processamento de saída

Seleção e retirada dos pacotes da fila para transmissão.



##### 4.3.4. Onde ocorre formação de fila?

Filas de pacotes podem se formar nas portas de entrada e saída. O local e a extensão da fila depende da carga de tráfego, velocidade relativa do elemento de comutação e da taxa da linha. B



**Qual pacote encaminhar?** Primeiro a chegar, primeiro a ser atendido (FCFS), fila ponderada justa (WFQ), compartilha o enlace de saída igual entre eles.

**Qual pacote descartar?** (gerenciamento ativo de fila AQM) Detecção aleatória rápida (RED). Definir min e max, se o comprimento médio da fila < min, pacote aceito. média > max, descartado, se estiver entre o intervalo, descartado segundo uma probabilidade.

**Bloqueio de cabeça de fila HOL:** pacote na fila de entrada espera pela transferência mesmo q sua porta de saída esteja livre, pois está bloqueado por um pacote na sua frente. Comprimento da fila de entrada cresce sem limites em determinadas circunstâncias.

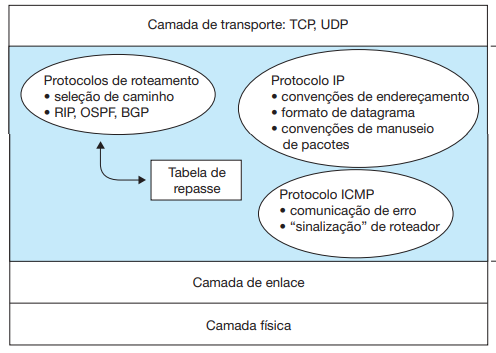
##### 4.3.5. O plano de controle de roteamento

Reside totalmente e é executado em um processador de roteamento dentro do roteador.

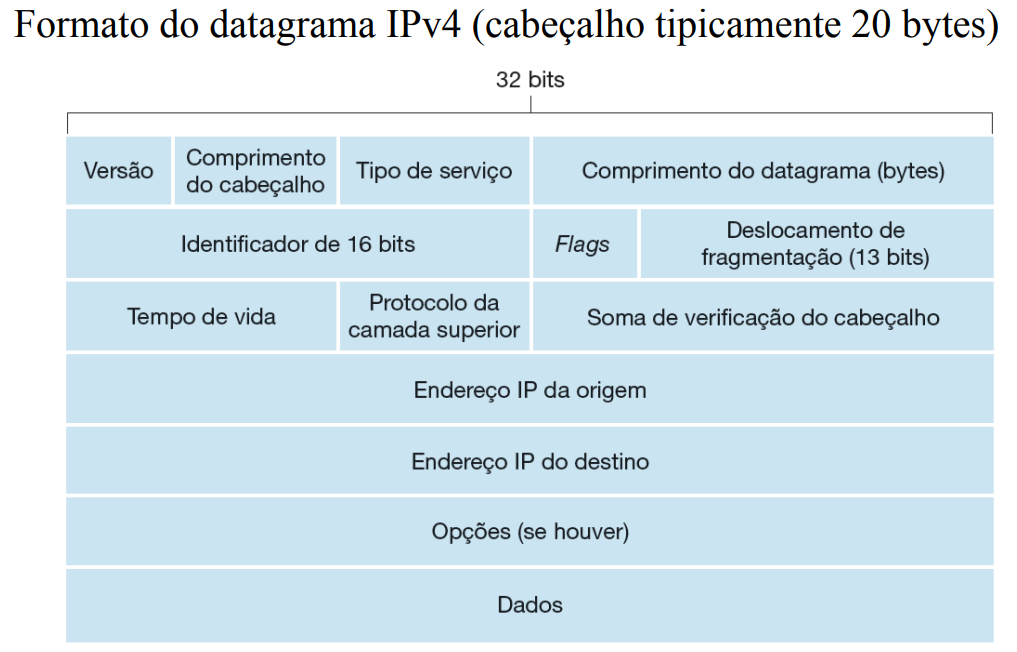
**Descentralizado**, com diferentes partes executando em diferentes roteadores e interagindo pelo envio de mensagens de controle entre si.

### 4.4. O Protocolo da Internet (IP): repasse e endereçamento na Internet

3 componentes principais da camada de rede: protocolo IP, componente de roteamento e o ICMP protocolo de comunicação de erro e de informações da Internet.



##### 4.4.1. Formato de datagrama



**Número da versão:** versão do protocolo IP do datagrama IPv4 ou IPv6

**Comprimento do cabeçalho:** onde os dados começam de fato, típicamente 20 bytes.

**Tipo de serviço:** diferencia diferentes tipos de datagramas (requerem baixo atraso, alta vazão ou confiabilidade)

**Comprimento do datagrama:** comprimento total do datagrama IP (cabeçalho mais dados)

**Identificador, flags, deslocamento de fragmentação**: IPv6 não permite fragmentação.

**Tempo de vida:** TTL-- cada vez que o datagrama é processado por um roteador. Se o TTL==0, o datagrama é descartado.

**Protocolo:** protocolo de camada de transporte ao qual o datagrama deverá ser passado.

**Soma de verificação do cabeçalho:** detecção de erros de bits. Deve ser recalculada e armazenada de novo, pois o campo TTL e campos de opções podem mudar. Calculada só para o cabeçalho IP.

**Endereços IP de origem e de destino**

**Opções:** permite que um cabeçalho IP seja estendido. Descartadas no IPv6

**Dados (carga útil):** contém segmento TCP ou UDP ou mensagens ICMP.

Se carregar um segmento TCP, cada datagrama (não fragmentado) carrega 40 bytes de cabeçalho (20 IP + 20 TCP) junto com a mensagem.

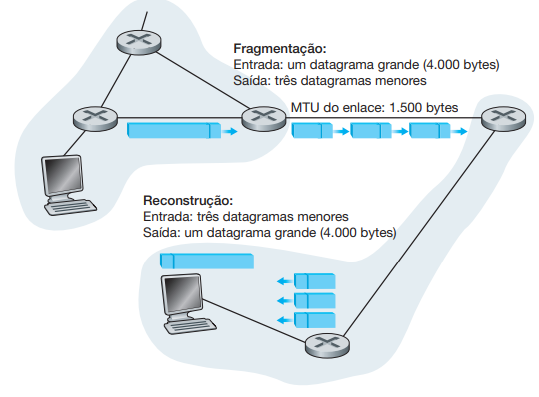
**FRAGMENTAÇÃO DO DATAGRAMA IP**

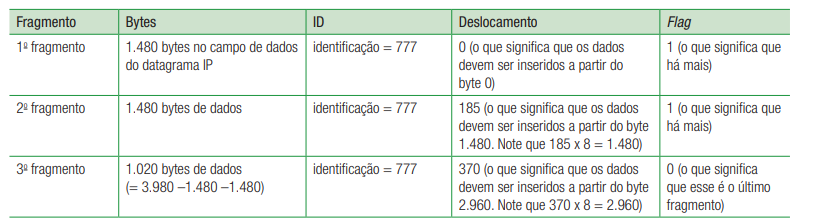
**MTU**: quantidade máxima de dados que a camada de enlace pode carregar. Estabelece um limite para o comprimento de um datagrama. Cada enlace da rota pode ter diferentes MTU.

Simplicidade do núcleo da rede: **reconstrução de datagramas aos sistemas finais.**

*Campos de identificação, flag e deslocamento de fragmentação.*

Datagrama criado -> número de identificação e end. de origem/destino -> cada fragmento tem o end. de origem/destino e o número de identificação original. O último fragmento tem um *bit de flag* = 0. O campo de deslocamento especifica a localização do fragmento.





Quantidade de dados da carga útil original: todos os fragmentos, exceto o último, é um múltiplo de 8 bytes. Valor de deslocamento é especificado em porções de 8 bytes.

Se fragmentos não chegarem, o datagrama incompleto será descartado.

##### 4.4.2. Endereçamento IPv4

**Interface**: fronteira entre o hospedeiro e o enlace físico. 1 IP associado a 1 uma interface.

Cada endereço IP tem comprimento de 32 bits (4 bytes), há 2³² endereços IP possíveis.

193.32.216.9 = 11000001 00100000 11011000 00001001

Uma parte do endereço IP de uma interface é determinada pela **sub-rede**.

**Máscara de sub-rede:** /24 significa que os 24 bits mais à esquerda dos 32 bits definem o endereço da sub-rede.

a.b.c.d/x (x bits mais significativos é o prefixo - num de bits da primeira parte do endereço)

32 - x = equipamentos

**endereço de difusão:** datagrama com endereço de destino **255.255.255.255**, a mensagem é entregue a todos os hospedeiros na mesma sub-rede.

**Exemplo: 192.168.0.0/22**

Quantos equipamentos podem ser endereçados? **32 - 22 = 10 → 2¹⁰ - 2 = 1022**

Endereço da rede? **192.168.0.0**

Endereço de broadcast? **192.168.3.255** (32-22=10, último 8 bits (255) e penúltimo 2 (3)).

O endereço 192.168.34.122 pertence à subrede? Não.

**OBTENÇÃO DE UM BLOCO DE ENDEREÇOS:**

Contatar seu ISP, fornece endereços a partir de um bloco maior de endereços que já estão alocados ao ISP. Por exemplo, o ISP recebe o bloco de endereços 200.23.16.0/20 e divide em oito blocos de endereços contíguos, do mesmo tamanho:



**PROTOCOLO DE CONFIGURAÇÃO DINÂMICA DE HOSPEDEIROS (DHCP):**

O hospedeiro obtém um endereço IP de maneira automática (plug and play) e tenha informações como máscara de sub-rede, o endereço do primeiro roteador (default gateway) e o endereço de seu servidor DNS local. O DHCP é um protocolo cliente-servidor.

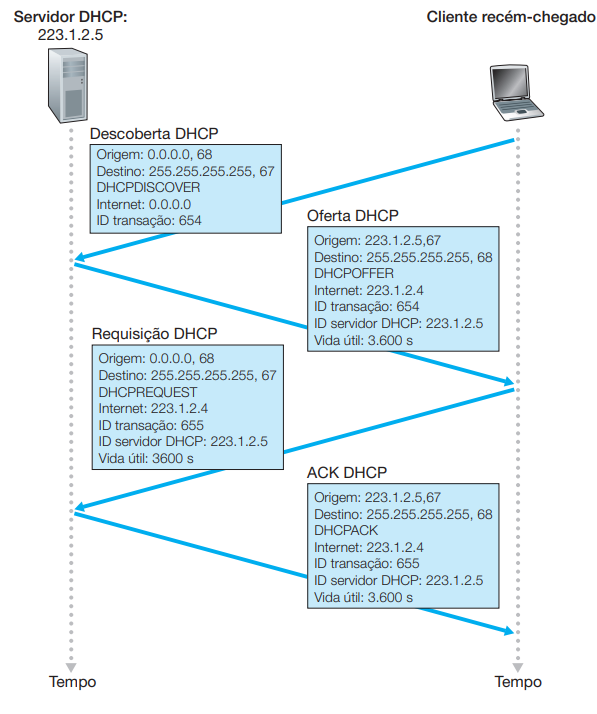
Quatro etapas:

**1. Descoberta do servidor DHCP:** Cliente envia o endereço IP de destino 255.255.255.255 e o endereço IP destinatário 0.0.0.0, transmitindo por difusão à camada de enlace.

**2. Oferta(s) dos servidores DHCP:** Servidor DHCP responde com uma mensagem de oferta utilizando o endereço 255.255.255.255. Contém o ID de transação da mensagem de descoberta recebida, o endereço IP proposto para o cliente, a máscara da rede e o tempo de concessão do endereço IP.

**3. Solicitação DHCP:** O cliente escolhe uma oferta do servidor e responde com uma mensagem de solicitação DHCP, repetindo os parâmetros de configuração.

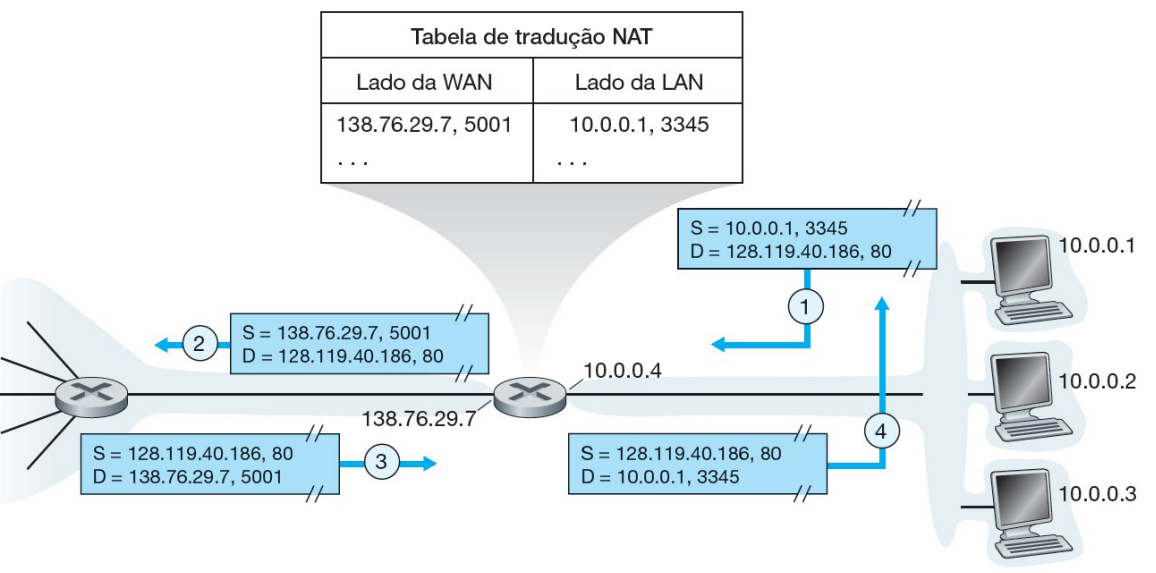
**4. DHCP ACK:** Responde com DHCP ACK, confirmando os parâmetros requisitados.

****

**TRADUÇÃO DE ENDEREÇOS NA REDE: NAT**

O roteador que usa NAT não parece um roteador para o mundo externo, pois se comporta como um equipamento único com *um único endereço IP*.

Tabela de tradução NAT: registros de portas e os IPs.



Críticas:

1- A finalidade dos números de portas é endereçar processos, e não hospedeiros.

2- Roteadores devem processar pacotes até a camada três

3- Viola o argumento fim a fim

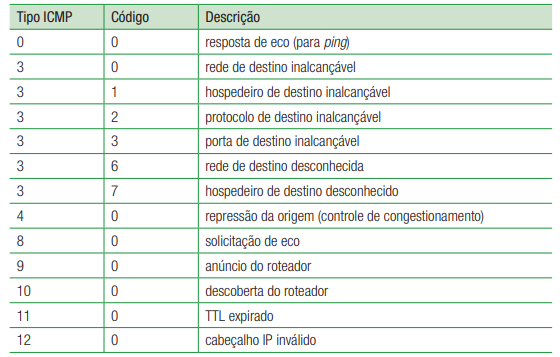
4- Utilização do iPv6

5- Interfere aplicações P2P, pois entre o par, se o B estiver por trás de uma NAT, não poderá agir como um servidor. Mas como um NAT pode ser identificado? UPnP permite que hospedeiros externos iniciem sessões com hospedeiros que utilizam NAT.

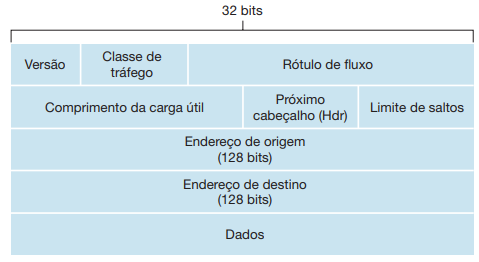
##### 4.4.3. Protocolo de Mensagens de Controle da Internet (ICMP)

O ICMP é usado por hospedeiros e roteadores para **comunicar informações** de camada de rede entre si. A utilização mais comum é para **comunicação de erros.**

Mensagens ICMP têm um campo de tipo e um campo de código. Contém o cabeçalho e os primeiros 8 bytes do datagrama IP que causou a criação da mensagem ICMP.

**

##### 4.4.4. IPv6



**Capacidade de endereçamento expandida:** 128 bits. Introduziu o endereço para qualquer membro do grupo (anycast).

**Cabeçalho fixo de 40 bytes:** campos IPv4 foram descartados ou tornaram-se opcionais. O

**Rotulação de fluxo e prioridade:** fluxos para serviços com tratamento especial.

**Não permite a fragmentação/remontagem.** Se for muito grande, o roteador descartará e devolverá ao remetente uma mensagem de erro ICMP “Pacote muito grande”

**Sem soma de verificação**, pois ocupava muito tempo (recalculado a cada salto no IPv4)

Campo de opções pode ser o próximo (assim como tcp e udp) dentro de um pacote IP.

Nova verão do ICMP foi definida para o IPv6

**Transição do IPv4 para o IPv6:**

1- DNS pode direcionar o tráfego, porém informações podem ser perdidas sobre o fluxo.

2- Implementação de túnel: Quando necessário, IPv6 dentro do Ipv4. Problemas: complexidade, sobrecarga e desempenho.

### 4.5. Algoritmos de roteamento

Em geral um hospedeiro está ligado diretamente a um roteador, o *roteador default*.

**Global:** conhecimento completo da rede. Eu falo com todos.

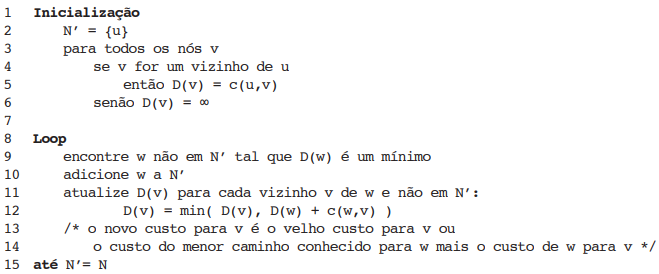
**Descentralizado**: o cálculo é iterativo e distribuído. Vizinhos se falam.

**Estáticos:** rotas mudam muito devagar, às vezes por intervenção humana

**Dinâmicos:** rotas mudam à medida que cargas de tráfego ou a topologia da rede mudam.

**Sensível à carga:** custos variam para refletir o nível de congestionamento no enlace.

##### 4.5.1. O algoritmo de roteamento de estado de enlace (LS) - GLOBAL - Dijkstra

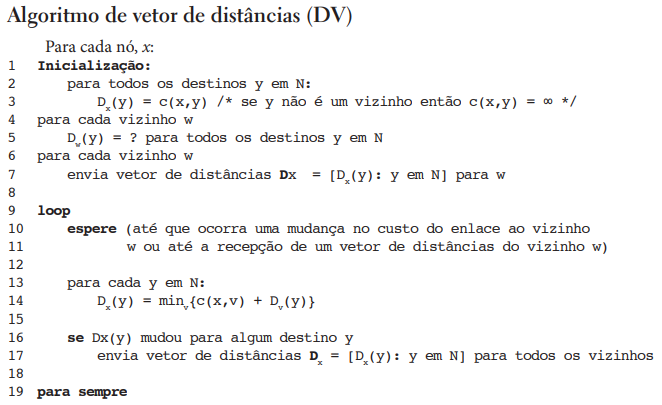


##### 4.5.2. O algoritmo de roteamento de vetor de distâncias (DV) - Descentralizado - fofoqueiro

Iterativo, assíncrono e distribuído.

Seja dx(y) o custo do caminho de menor custo do nó x ao nó y. Então, os menores custos estão relacionados a equação de Bellman-Ford: **dx (y) = minv {c(x,v) + dv (y)}.**

Nó que alcança mínimo é o próximo salto no caminho mais curto ➜ tabela de repasse.



Quando o nó detecta mudança de custo no enlace local, atualiza informação de roteamento, recalcula vetor de distância se DV mudar, notifica vizinhos.

|  | **LS** | **DV** |
| --- | --- | --- |
| **Complexidade da mensagem** | O(nE) | varia muito |
| **Velocidade de convergência** | O(n² ) para O(nE) mensagens | Pode convergir lentamente, ter loops e problema da contagem até o infinito |
| **Robustez** | Erro no cálculo do custo: Cada nó calcula apenas sua própria tabela - isolados - não há muito problema | Erro no cálculo do custo: tabela de cada nó usada por outros, se propaga pela rede!!! |

##### 4.5.3. Roteamento hierárquico

Na prática todos os roteadores com o mesmo algoritmo de roteamento é simplista: escalabilidade (+roteadores +sobrecarga) e autonomia administrativa. Esses problemas podem ser resolvidos agrupando roteadores em **sistemas autônomos (ASs).**

**ASs:** roteadores sob o mesmo controle administrativo com mesmo algoritmo

**Protocolo de roteamento INTRA-AS:** algoritmo de roteamento que roda dentro de um AS.

**Protocolo de roteamento INTER-AS:** Obtém informações sobre as condições de alcance de ASs vizinhos e propagá-las.

Dentro de um AS, os roteadores rodam o mesmo protocolo de roteamento INTRA-AS. Entre eles, os ASs rodam o mesmo protocolo de roteamento INTER-AS.

### 4.6. Roteamento na internet

Protocolo de roteamento intra-AS: como é rodado o roteamento dentro de um AS.

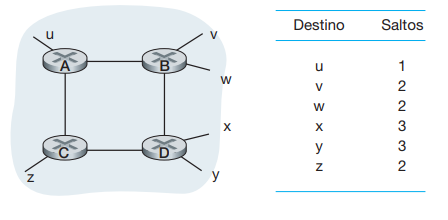
2 usados na Internet: RIP (Routing Information Protocol) e OSPF (Open Shortest Path First)

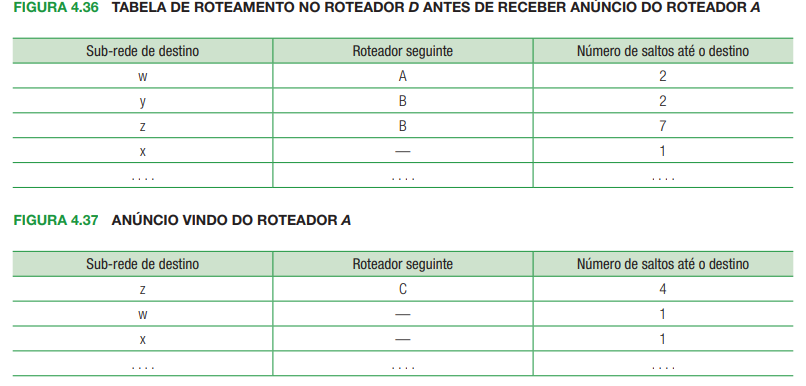
##### 4.6.1. Roteamento intra-AS na Internet: RIP

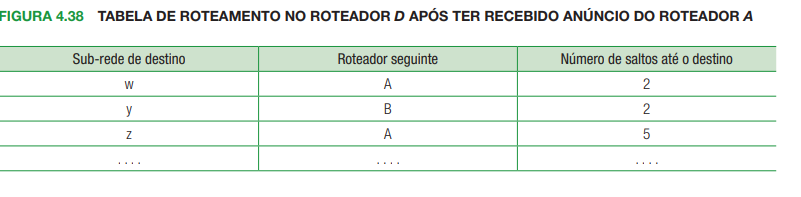
Protocolo de vetor de distâncias. Usa contagem de saltos como métrica de custo, isto é, cada enlace tem um custo 1. O custo máximo de um caminho é limitado a 15 (limitação)

**Mensagem de resposta/anúncios RIP:** distâncias dos caminhos de menor custo.

Cada roteador tem uma tabela RIP de roteamento (vetor de distância + tabela de repasse).





****

RIP trocam anúncios a cada +/- 30s. Se um roteador não ouvir nada de seu vizinho por 180s, será considerado que o enlace de conexão caiu.

##### 4.6.2. Roteamento intra-AS na Internet: OSPF

Foi concebido como sucessor do RIP com uma série de características avançadas.

Usa *Dijkstra*, transmite por difusão informações a todos os roteadores, não só aos vizinhos.

Não impõe uma política para a determinação dos pesos (tarefa do administrador da rede)

Transmite informações quando mudar e periodicamente (30 min), mesmo sem mudança.

**Segurança:** todas as mensagens OSPF autenticadas (para impedir intrusão maliciosa)

**Múltiplos caminhos de mesmo custo** permitidos (apenas um caminho no RIP)

Suporte integrado para roteamento individual e em grupo;

Suporte para hierarquia dentro de um único domínio de roteamento;

##### 4.6.3. Roteamento inter-AS: BGP protocolo de roteador de borda -Border Gateway Protocol

Caminhos para pares origem-destino de vários ASs. Permite que cada sub-rede anuncie sua existência ao restante da Internet.

1- Obter de ASs vizinhos informações de alcançabilidade de sub-redes.

2- Propagar a informação de alcançabilidade a todos os roteadores internos ao AS.

3- Determina rotas boas para sub-redes com base da alcançabilidade e na política do AS.

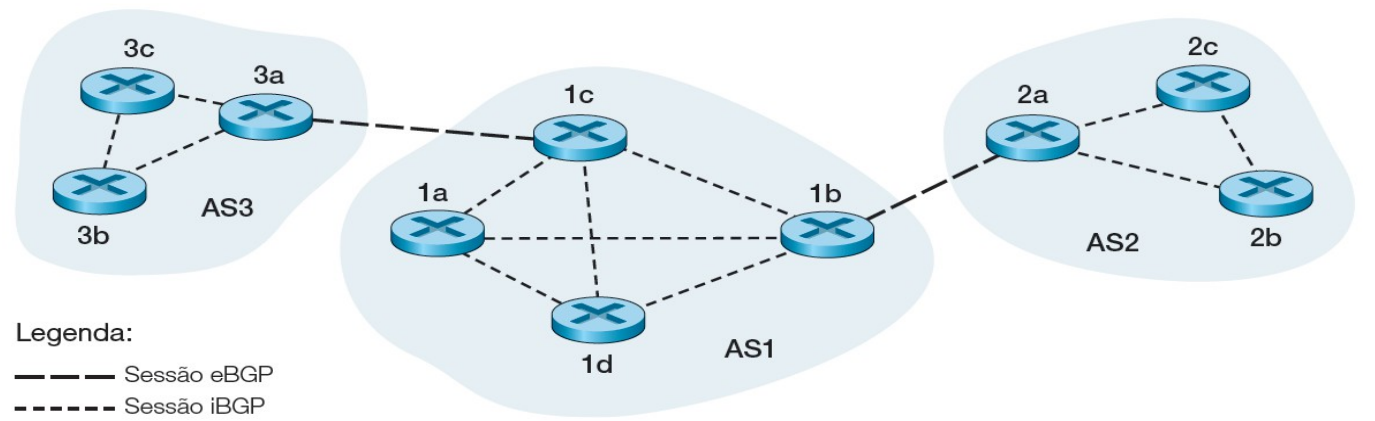
Pares de roteadores trocam informações por conexões TCP semipermanentes na porta 179

**Pares BGP**: dois roteadores nas extremidades da conexão

**Sessão BGP:** conexão TCP, junto com todas as mensagens BGP enviadas pela conexão.

**eBGP**: conexão BGP TCP para enlaces que ligam dois roteadores em ASs diferentes;

**iBGP:** BGP TCP semipermanentes entre roteadores dentro de um AS.



Cada AS conheça quais destinos podem ser alcançados por meio de seus ASs vizinhos.

Os destinos não são hospedeiros, mas prefixos *ciderizados.* Roteadores trocam informações de **alcançabilidade de prefixos** por meio de seus roteadores de borda.

**ATRIBUTOS DE CAMINHO E ROTAS BGP:**

**Número de sistema autônomo (ASN):** identificação exclusiva de um sistema autônomo.

Quando um roteador anuncia um prefixo para uma sessão BGP, inclui vários atributos BGP com o prefixo. **Prefixo + atributos = “Rota”.** 2 atributos importantes:

**AS-PATH:** contém ASs através dos quais o anúncio do prefixo já passou. Evita loops.

**NEXT-HOP:** interface do roteador que inicia o AS-PATH. Indica roteador específico do AS interno para AS do próximo salto (podem ser múltiplos enlaces para AS atual até AS do próximo salto). Usado para configurar suas tabelas de repasse adequadamente.

Quando o roteador de borda recebe anúncio de rota, usa **política de importação para aceitar/declinar.**

**SELEÇÃO DE ROTA DO BGP:**

Um roteador pode conhecer mais do que uma rota para qualquer prefixo determinado.

Invoca sequencialmente as seguintes regras de eliminação, até sobrar apenas uma:

1- Rotas recebem como atributos um **valor de preferência local.** O(s) valore(s) mais altos são selecionados (pode ser mais que um caso sejam iguais).

2- É selecionada a que tenha o AS-PATH mais curto.

3- É selecionada a que tem o roteador NEXT-HOP mais próximo

4- O roteador usa identificadores BGP para selecionar a rota.

### 4.7. Roteamento por difusão e para um grupo

##### 4.7.1. Algoritmos de roteamento por difusão (broadcast)

**Forma simples**: nó remetente envia uma cópia separada do pacote para cada destino.

Vantagens: simples, não precisa novo protocolo, duplicação e funcionalidade de repasse.

Desvantagens: ineficiência, como saber todos os destinatários?

**Inundação não controlada:** nó de origem envia uma cópia para todos os seus vizinhos. Desvantagens: ciclos, se for desconectado nem todos recebem, tempestade de difusão

**Inundação controlada por número de sequência:** nó de origem coloca seu endereço e um número de sequência de difusão em um pacote e envia a seus vizinhos. Cada nó mantém uma lista de endereços e números de sequência para cada pacote que recebeu, duplicou e repassou. Quando um nó recebe um pacote de difusão, verifica se o pacote está nessa lista. Se sim, é descartado; se não, é duplicado e repassado para seus vizinhos.

**Difusão pelo caminho inverso:** O roteador recebe um pacote de difusão de origem x, ele transmite o pacote para seus vizinhos (exceto o que recebeu) somente se o pacote chegou pelo enlace que está em seu próprio caminho individual mais curto de volta ao remetente. Caso contrário, descarta o pacote sem repassá-lo.

**Difusão por spanning tree:** os anteriores não evitam completamente a transmissão de pacotes por difusão redundantes. Uma alternativa é uma a spanning tree mínima.

##### 4.7.2. Serviço para um grupo (multicast)

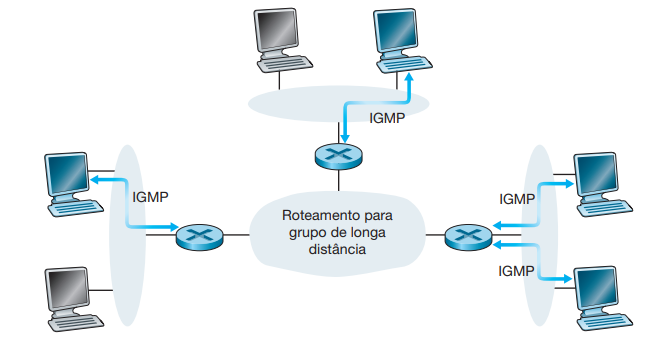
Como identificar os destinatários de um pacote desse tipo e como endereçar um pacote enviado a um desses destinatários?

Um pacote para um grupo é endereçado usando **endereço indireto.** O grupo de destinatários associados a um endereço classe D é denominado **grupo multicast**.

Componentes de grupo: IGMP e protocolos de roteamento para um grupo.

**IGMP:** Opera entre um hospedeiro e o roteador conectado a ele. Oferece meios para um hospedeiro informar ao roteador que uma aplicação quer se juntar a um grupo específico.

**Protocolos de roteamento para um grupo:** encontrar uma árvore de enlaces que conecte todos os roteadores que têm hospedeiros conectados pertencentes ao grupo.



# CAMADA DE ENLACE

### 5.1 Introdução à camada de enlace

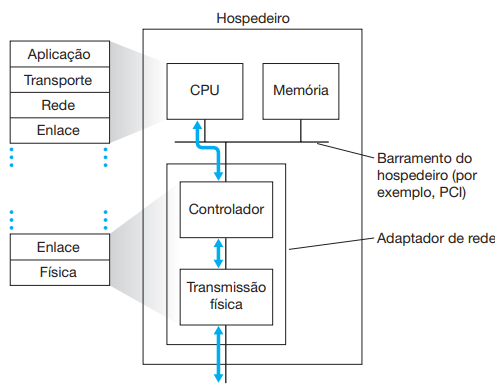
**NÓ:** qualquer dispositivo que rode um protocolo da camada de enlace (hospedeiros, roteadores, comutadores e pontos de acesso Wi-FI)

Nó transmissor encapsula o datagrama em um **quadro da camada de enlace**.

**Serviços oferecidos:** Enquadramento de dados, acesso ao enlace MAC, entrega confiável, detecção e correção de erros.

##### 5.1.2 Onde a camada de enlace é implementada?

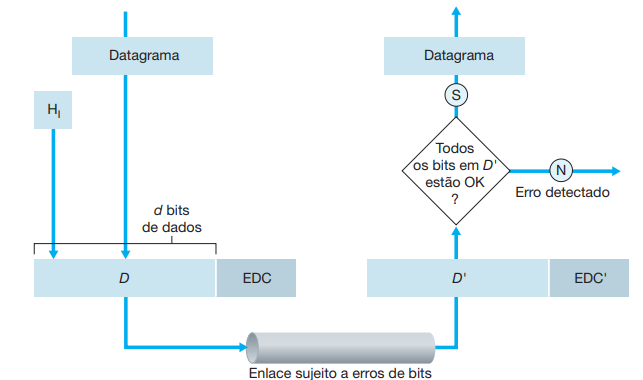
Na maior parte, é implementada em um adaptador de rede/**placa de interface de rede NIC.** No núcleo tem o **controlador**, que executa vários serviços (enquadramento, acesso ao enlace, detecção de erros etc.). Muito da funcionalidade do controlador da camada de enlace é realizada em **hardware**. Software é executada na CPU do hospedeiro



### 5.2 Técnicas de detecção e correção de erros

bits de detecção e de correção (error detection-and-correction — EDC).

Determina se D′ é ou não igual ao D original, uma vez que recebeu apenas D′ e EDC′.

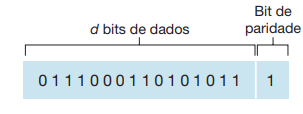


##### 5.2.1 Verificações de paridade

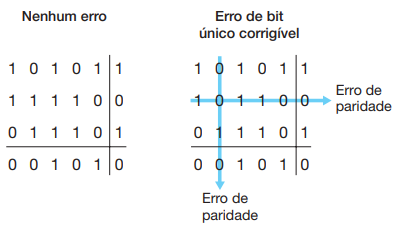
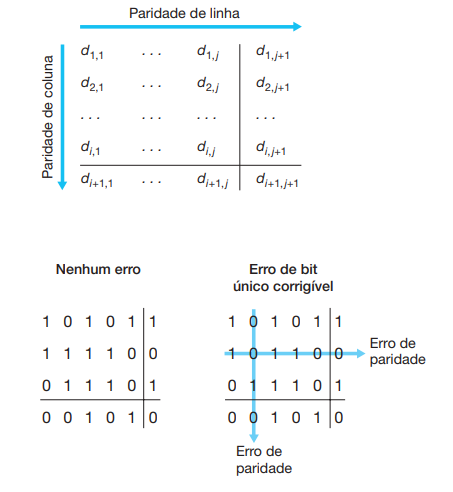
A maneira mais simples de detectar erros.

Um único bit de paridade: paridade par, inclui um bit com valor de modo que o número total de 1’s seja par. Paridade ímpar, o valor é escolhido para ter número ímpar de 1’s.

Se, com paridade par, tiver número ímpar de bits 1’s, há pelo menos um erro de bit. E se ocorrer um número par de erros de bit? Não será detectado. Se a probabilidade de erro de bits for pequena, a chance de vários erros em um pacote é pequena. Em rajada de erros, a probabilidade de haver erros não detectados pode chegar perto de 50%.



**Generalização bidimensional do esquema de paridade de bit único:** os d bits de D são divididos em i linhas e j colunas. Um valor de paridade é calculado para cada linha e para cada coluna. Os i+j+1 bits de paridade resultantes compreendem os bits de detecção de erros do quadro da camada de enlace.



Usa os índices i,j com erros para identificar o bit que foi corrompido e **poder corrigir.**

**Correção de erros antecipada (forward error correction — FEC)**

##### 5.2.2 Métodos de soma de verificação

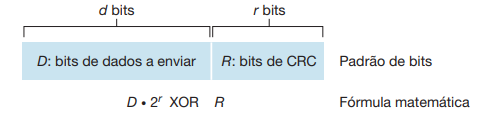
Os *d bits* são tratados como uma sequência de números inteiros de k bits. Soma-os e usa o total como bits de detecção de erro. O complemento de 1 disso forma a soma de verificação da Internet, que é carregada no cabeçalho do segmento. Pouca sobrecarga no pacote.

No IP, a soma de verificação é calculada somente sobre o cabeçalho.

##### 5.2.3 Verificação de redundância cíclica (CRC) - códigos polinomiais

Mais utilizada em na camada de enlace.

O remetente e o receptor concordam com um padrão de r+1 bits, o **gerador G**. Exigencia: bit mais significativo seja 1.



Para a parcela de dados D, o remetente escolhe r bits adicionais (R) e os anexa a D de modo que o padrão de d+r bits resultante (número binário) seja divisível exatamente por G, usando aritmética de módulo 2. Se o resto for diferente de zero, ocorreu um erro; caso contrário, os dados são aceitos como corretos.

### 5.3 Enlaces e protocolos de acesso múltiplo

**Enlace ponto a ponto:** um único remetente em cada extremidade do enlace

**Enlace de difusão:** vários nós remetentes e receptores, todos conectados ao mesmo canal de transmissão único e compartilhado. Quando qualquer nó transmite um quadro, o canal propaga por difusão e cada nó recebe uma cópia. (Ethernet e as LANs sem fio)

**Problema do acesso múltiplo:** como coordenar o acesso de vários nós remetentes e receptores a um canal de difusão compartilhado.

**Protocolos de acesso múltiplo:** através dos quais os nós regulam sua transmissão pelos canais de difusão compartilhados.

Importância de coordenar: transmissão de quadros ao mesmo tempo: nós recebem vários quadros ao mesmo tempo que se colidem, sinais embaralhados. Os quadros envolvidos são perdidos e o canal de difusão é desperdiçado durante o intervalo de colisão.

Idealmente, um protocolo de acesso múltiplo para um canal de difusão com velocidade de R bits por segundo tem as seguintes características desejáveis:

1. Quando apenas um nó tem dados para enviar, esse nó tem uma vazão de R bit/s.

2. Quando M nós têm dados para enviar, cada um tem uma vazão de R/M bits/s.

3. Descentralizado, não há 1 nó mestre que represente 1 único ponto de falha para a rede.

4. O protocolo é simples para que sua implementação seja barata.

##### 5.3.1 Protocolos de divisão de canal

**TDM** divide o tempo em quadros temporais, e divide em N compartimentos de tempo.

**FDM** divide o canal de R bits/s em N canais menores de R/N bits/s

Elimina colisões e é perfeitamente justo. Desvantagens: limitação de R/N bits/s, mesmo quando é o único nó com pacotes para enviar e o nó deve sempre esperar sua vez (TDM)

**CDMA** código diferente a cada nó. Se os códigos forem escolhidos com cuidado, permite que nós diferentes transmitam simultaneamente com entrega correta.

##### 5.3.2 Protocolos de acesso aleatório

Nó transmissor sempre transmite à taxa total do canal R bits/s. Colisão = retransmissão, porém com atrasos aleátorios.

**SLOTED ALOHA**

Suposições:

1- todos os quadros do mesmo tamanho

2- tempo dividido em intervalos de mesmo tamanho (tempo para transmitir 1 quadro, L/R)

3- nós começam a transmitir somente no início dos intervalos

4- nós são sincronizados

5- se 2 ou mais nós transmitem no intervalo, todos os nós detectam colisão

Quando o nó obtém quadro novo, transmite no próximo intervalo. Se não há colisão: nó pode enviar novo quadro no próximo intervalo. Se há colisão: nó retransmite quadro em cada intervalo subsequente com prob. até que haja sucesso.

Decisão de transmitir é tomada por um nó independentemente da atividade dos outros nós ligados ao canal de difusão

**Vantagens:** transmissão R/L, continuo se for o unico ativo, descentralizado e simples.

**Desvantagens:** quando há vários nós ativos, terá colisões, intervalos ociosos

**Eficiência:** fração durante longo tempo de intervalos bem sucedidos (muitos nós, todos com muitos quadros para enviar). Na melhor das hipóteses: canal usado para transmissões úteis **37% do tempo!**

No ALOHA puro, quando um quadro chega pela primeira vez, é imediatamente transmitido ao canal de difusão. Se sofrer colisão, retransmite de imediato. Eficiência máxima do ALOHA puro é metade da eficiência do slotted.

**CSMA**

**detecção de portadora** — um nó ouve o canal antes de transmitir.

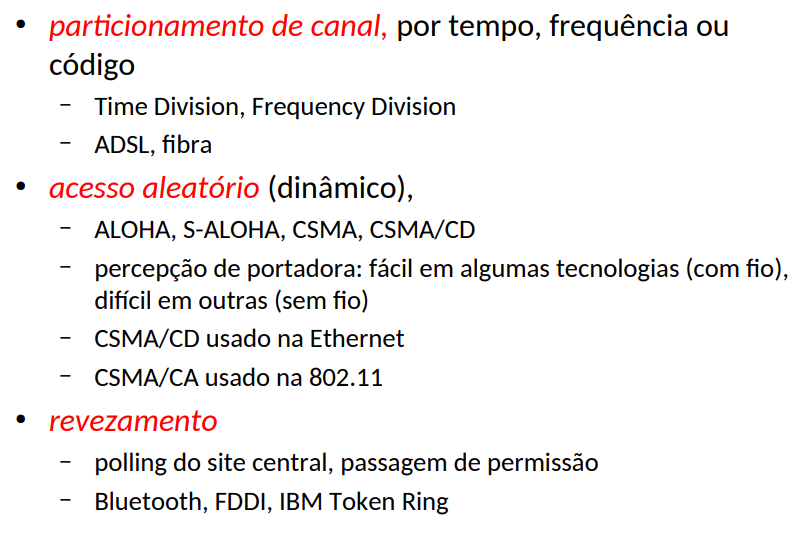
**detecção de colisão —** um nó que está transmitindo ouve o canal enquanto transmite.

Se todos os nós realizam detecção de portadora, por que ocorrem colisões? por causa do tempo que leva para que um sinal se propague de um dos extremos do canal para outro.

##### …………….

##### 5.3.3 Protocolos de revezamento

……………



### 5.4 Redes locais comutadas

Comutadores operam na camada de enlace, eles comutam quadros da camada de enlace (em vez de datagramas da camada de rede).

**Comutador:** transportar datagramas entre hospedeiros e roteadores sem que hospedeiro/roteador tenha que endereçar o quadro explicitamente.

##### 5.4.1 Endereçamento na camada de enlace e ARP

Hospedeiros e roteadores têm endereços da camada de enlace: **Endereços MAC.**

Um hospedeiro tem várias interfaces, então ele possui vários MAC. Porém, os comutadores da camada de enlace não tem MAC associado.

MAC de um adaptador é fixo, tem 6 bytes de comprimento, o que dá 2⁴⁸ endereços.

função: levar quadro de uma interface para outra interface conectada fisicamente.

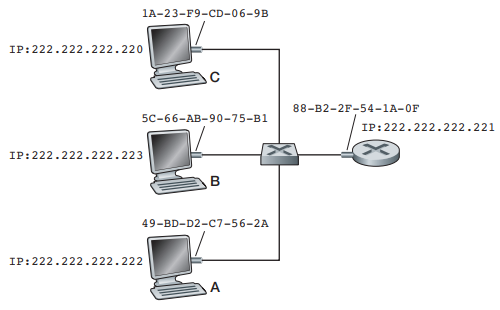
**PROTOCOLO DE RESOLUÇÃO DE ENDEREÇOS ARP (plug-and-play)**

Cada nó IP (hosp., roteador) na LAN tem tabela ARP.

Tabela ARP: mapeamentos de endereço IP/MAC para alguns nós da LAN **<IP, MAC, TTL>**

ARP é um protocolo que fica em cima do limite entre as camadas de enlace e de rede.

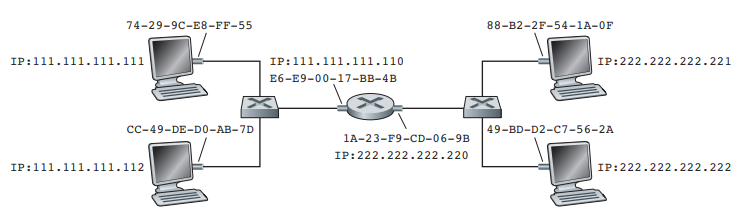
**APENAS PARA A SUB-REDE!!**



222.220 quer mandar um datagrama IP para 222.222. Ele dá a seu adaptador o datagrama IP e o MAC do destino, monta um quadro com o MAC do receptor e envia para a LAN. Ele usa o ARP para saber o MAC do IP 222.222, como não está na tabela, monta um pacote ARP: Destino FF-FF-FF-FF-FF-FF perguntando: qual o MAC de 222.222? Envia para broadcast. Apenas o destinatário responde para a origem.

Mensagem de consulta ARP enviada dentro de um quadro de difusão e a mensagem de resposta ARP é enviada dentro de um quadro padrão.

**ENVIO DE UM DATAGRAMA PARA FORA DA SUB-REDE**



111 quer enviar um datagrama IP ao 222. Remetente deve indicar o MAC de destino DO ROTEADOR 110 BB-4B (roteador do primeiro salto no caminho até o destino final). A tabela de repasse indica a interface que o datagrama deve ser repassado (222.220), passa para o seu adaptador, que encapsula o quadro e envia pra subrede2, com destino MAC do 222.222

| REDE | Origem: 111  Destino: 222 | Origem: 111  Destino: 222 | Origem: 111  Destino: 222 |
| --- | --- | --- | --- |
| ENLACE | 110?  BB-48 | Origem: FF-55  Destino: BB-48 | Origem: 06-9B  Destino: 56-2A |

##### 5.4.2 Ethernet - não orientado a conexão - não confiável

Primeira LAN de alta velocidade amplamente disseminada, versões que funcionam a velocidades iguais, ou mais altas, hardware para a tecnologia com custo baixo.

Adaptador encapsula o datagrama IP em um quadro Ethernet, que passa para a camada física. Adaptador recebe da camada física, extrai o datagrama IP e o passa para a rede.



**Dados** (46/1500bytes): carrega datagrama IP. MTU Ethernet é 1.500 byte (fragmentação).

**Endereço de destino** (6 bytes): MAC do adaptador de destino. Se recebe um quadro Ethernet para ele ou difusão, passa o conteúdo do campo de dados para a camada de rede.

**Endereço de origem** (6 bytes): MAC do adaptador que transmite o quadro para a LAN.

**Campo de tipo** (2 bytes): Para qual protocolo da camada de rede ele deve passar o conteúdo do campo de dados (IP, Novell IPX, AppleTalk, ARP)

**Verificação de redundância cíclica (CRC)** (4 bytes): Permitir que o adaptador receptor detecte se algum erro de bit foi introduzido no quadro.

**Preâmbulo** (8 bytes): Despertar os adaptadores receptores e sincronizar os relógios (10Mbps, 100Mbps, 1000Mbps).

Gigabit Ethernet: CSMA/CD para canais de difusão compartilhados, permite operação full-duplex, enlaces ponto a ponto.

##### 5.4.3 Comutadores da camada de enlace

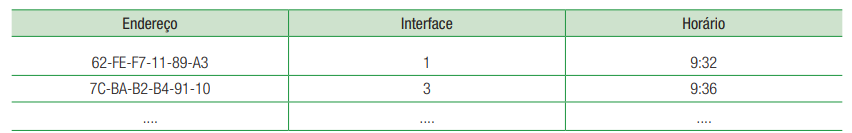
Recebe quadros da camada de enlace e repassa para os enlaces de saída.

**Transparente** aos hospedeiros e roteadores na sub-rede (um nó endereça um quadro a outro nó em vez de endereçar o quadro ao comutador)

**Filtragem**: a capacidade de um comutador que determina se um quadro deve ser repassado ou se deve apenas ser descartado.

**Repasse**: a capacidade de um comutador que determina as interfaces para as quais um quadro deve ser dirigido e então dirigir o quadro a essas interface

Filtragem e repasse de comutadores são feitos com uma tabela de comutação:



Quando um pacote chega, há 3 opções:

1- Não há entrada na tabela, envia para todas as interface menos a que ele veio (difusão).

2- Existe entrada na tabela associando a interface que veio: filtragem ao descartar o quadro

3- Existe entrada na tabela com uma interface diferente da que veio: envia p/ interface certa

Autoaprendizagem: monta sua tabela de modo automático, dinâmico e autônomo

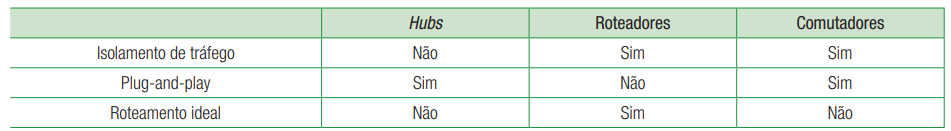
Vantagens: Eliminação de colisões e desperdício de banda, enlaces heterogêneos, gerenciamento.

**Comutadores vs roteadores**

Ambos são dispositivos de armazenamento e repasse.

**Comutadores**: plug-and-play, velocidades altas de filtragem e repasse, processam quadro apenas até a camada 2. Porém, topologia restrita a spanning tree, uma rede grande exige de hospedeiros e roteadores tabelas ARP grandes, suscetíveis a tempestade de difusão.

**Roteadores:** não ficam restritas a spanning tree e podem usar o melhor trajeto entre origem e destino, proteção de firewall contra as tempestades de difusão. Porém não são plug-and-play e tempo de processamento por pacote maior (até a camada 3)

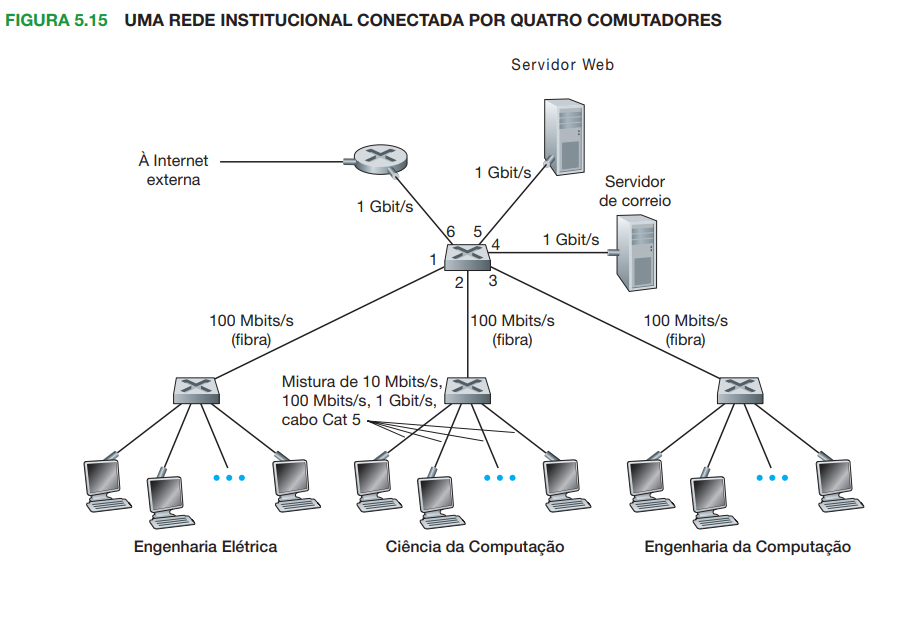


**Redes pequenas**, algumas centenas de hospedeiros: **comutadores**, pois localizam o tráfego e aumentam a vazão sem exigir nenhuma configuração de endereços IP.

**Redes maiores,** com milhares de hospedeiros, **roteadores** (além de comutadores), pois fornecem isolamento de tráfego mais robusto, controlam tempestades de difusão e usam rotas “mais inteligentes” entre os hospedeiros da rede.

##### 5.4.4 Redes locais virtuais (VLANs)

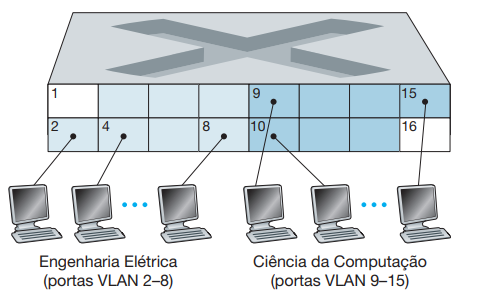
LANs institucionais com frequência são configuradas hierarquicamente:



**Desvantagens:** Falta de isolamento do tráfego (de difusão arp ou dhcp). Por questão de segurança e privacidade (qualquer um dos grupos podem acessar pacotes alheios) seria melhor limitar esse tráfego (roteadores).

Isso pode ser resolvido com um comutador que suporte **Redes Locais Virtuais (VLANs)**. Várias redes locais virtuais executadas por 1 infraestrutura física de uma rede local virtual.

VLAN baseada em portas: portas divididas em grupos 5.5 Virtualização de enlace: uma rede como camada de enlace

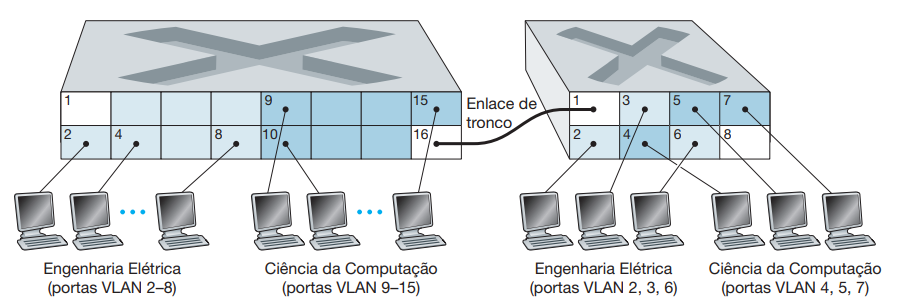


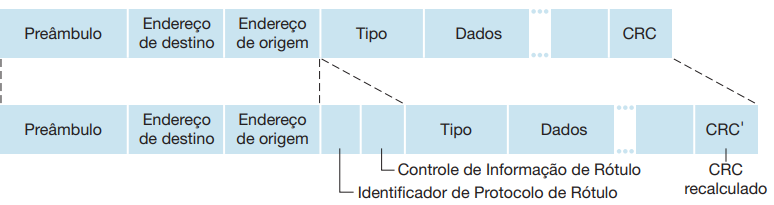
Mas se isolados, como o tráfego do EE pode ser enviado para o CC? **conectar uma porta de comutação da VLAN a um roteador externo**, configurando aquela porta para que pertença às VLANs de ambos os departamentos. Fornecedores de comutadores facilitam montando um dispositivo que contém um comutador VLAN e um roteador.

Mas e se quiser manter os mesmos grupos sabendo que há EE e CC em um prédio extra?

1- Entrada pertencente à VLAN CS em cada comutador (e da mesma forma para EE) e conectá-las umas às outras, porém, isso não permite crescimento.

2- **Entroncamento de VLANS:** porta especial em cada comutador configurada como uma porta de tronco que interconecta as VLANs, por meio de um quadro estendido: Quadro Ethernet original (no alto); quadro VLAN Ethernet 802.1Q-tagged (embaixo)





### 5.5 Virtualização de enlace: uma rede como camada de enlace

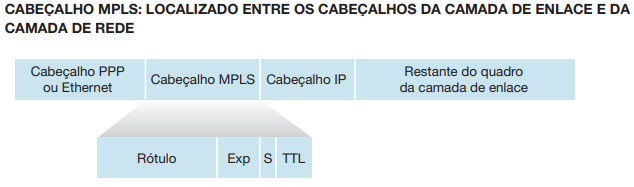
##### 5.5.1 Comutação de Rótulos Multiprotocolo (MPLS)

Redes de comutação de pacotes por circuitos virtuais: um rótulo de tamanho fixo.

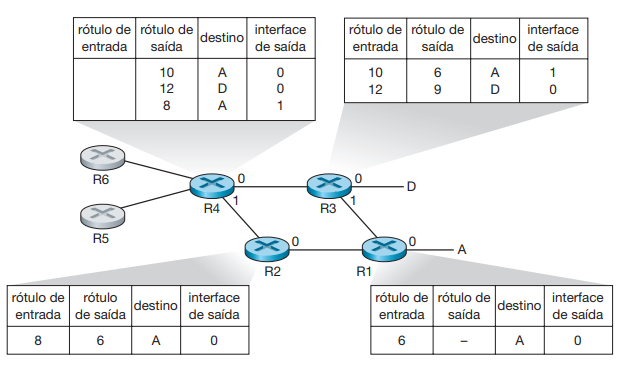
Não abandonar a infraestrutura de repasse de datagramas IP

Manipulado por um roteador habilitado para MPLS. Não precisa extrair o endereço de destino e buscar com o prefixo mais longo na tabela de repasse.

Executa comutação com base em rótulos, sem precisar considerar o IP de um pacote.



**Rótulo**: identificador de circuito virtual. **3 bits para uso experimental**, um único bit, **S**, indica o final de uma série de rótulos MPLS “empilhados” e um campo de **tempo de vida**.



### 5.6 Redes do datacenter

O datacenter tem sua própria rede que interconecta seus hospedeiros e liga-o à Internet.

**Lâminas:** hospedeiros empilhados em estantes. No topo tem o **comutador do topo da estante (TOR),** que interconecta os hospedeiros entre si e com outros comutadores.

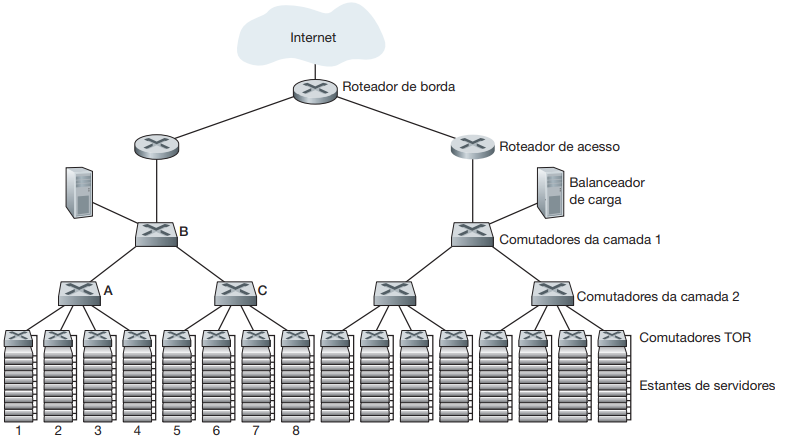
Dois tipos de tráfego: clientes externos/hospedeiros internos (roteadores de borda), e entre hospedeiros internos.

Solicitações externas vão primeiro a um **balanceador de carga**, que distribui as solicitações aos hospedeiros. Oferece uma função tipo NAT, traduzindo IP externo para o IP interno.

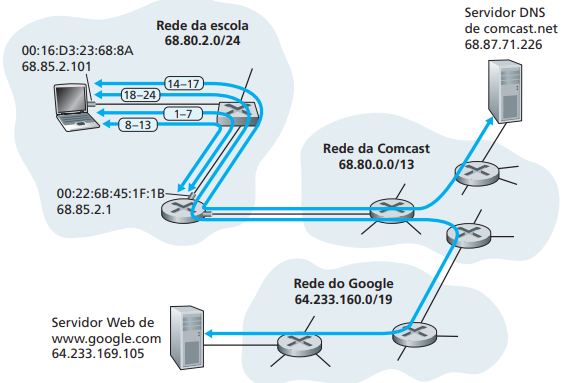
Para escalar, emprega uma **hierarquia de roteadores e comutadores**.

**Desvantagens:** capacidade limitada de hospedeiro-a-hospedeiro

**Tendências:** novas arquiteturas de interconexão e protocolos de rede que contornem as desvantagens dos projetos hierárquicos tradicionais (como a topologia totalmente conectada) datacenters modulares (MDCs) baseados em contêineres.



### 5.7 Um dia na vida de uma solicitação de página Web



##### 5.7.1 Começando: DHCP, UDP, IP e Ethernet

Bob conecta seu notebook via cabo Ethernet ao comutador Ethernet da escola.

1. Solicitação DHCP em segmento UDP com porta de destino 67 e origem 68. É colocado em um datagrama IP destino difusão (255….255) e origem 0.0.0.0, já que ainda não tem um endereço IP. Colocado em um quadro Ethernet com endereço de destino MAC FF:...:FF (transmitido a todos conectados ao comutador) e origem 68:8A.
2. O quadro de difusão Ethernet com a solicitação DHCP é enviado para o comutador, que transmite para todas as portas de saída, incluindo ao roteador.
3. O roteador recebe o quadro Ethernet e o datagrama IP é extraído, demultiplexado até o UDP, e a mensagem de solicitação é extraída.
4. O servidor DHCP designa o endereço 68.85.2.101. Cria uma mensagem de ACK DHCP, dentro de um segmento UDP -> datagrama IP -> quadro Ethernet, com endereço de origem (00:22:6B:45:1F:1B) e destino (00:16:D3:23:68:8A).
5. Enviado pelo roteador ao comutador, que já sabe a interface para enviar para Bob.
6. O notebook do Bob recebe o quadro Ethernet, extrai o datagrama IP, UDP e a mensagem ACK DHCP. Grava seu endereço IP (68.85.2.101) e o do seu servidor DNS (68.87.71.226). Instala o endereço do roteador de borda default (68.85.2.1) em sua tabela de repasse de IP. **Enviará todos os datagramas com destino fora de sua sub-rede 68.85.2.0/24 à saída-padrão.**

##### 5.7.2 Ainda começando: DNS, ARP

Bob digita o URL *www*.*google*.*com* em seu navegador.

1. S.O cria mensagem de consulta DNS perguntando “[www.google.com](http://www.google.com)”. UDP (porta de destino 53) -> IP endereço de destino 68.87.71.226 (DNS) e origem 68.85.2.101 -> Ethernet, enviado ao roteador de borda. Sabe o endereço IP do roteador de borda, **mas não o endereço MAC**.
2. Cria uma mensagem de consulta ARP ao endereço IP 68.85.2.1, coloca em um quadro Ethernet e transmite por difusão ao endereço de destino (FF:...:FF) e envia ao comutador, que entrega o quadro a todos os dispositivos.
3. Roteador de borda recebe, vê que o endereço IP de destino é o IP de sua interface. Responde, indicando que o seu endereço MAC 00:22:6B:45:1F:1B corresponde ao endereço IP 68.85.2.1. Coloca em um quadro Ethernet, com o endereço de destino 00:16:D3:23:68:8A e envia ao comutador, que entrega ao notebook de Bob.
4. O notebook de Bob recebe e extrai o endereço MAC do roteador de borda (00:22:6B:45:1F:1B).
5. **Pode agora endereçar o quadro Ethernet com a consulta DNS ao MAC do roteador de borda.** Observe que o **datagrama** nesse quadro tem o endereço IP de destino 68.87.71.226 **(servidor DNS)**, enquanto o **quadro** tem o endereço de destino 00:22:6B:45:1F:1B (**roteador de borda**). O notebook de Bob envia esse quadro ao comutador, que entrega o quadro ao roteador de borda

##### 5.7.3 Ainda começando: roteamento intradomínio ao servidor DNS

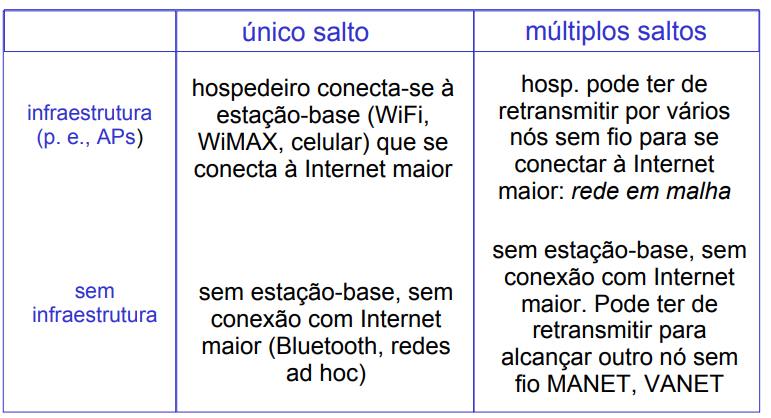
1. O roteador de borda recebe o quadro. Procura o IP de destino e vê na sua tabela de encaminhamento a interface a ser mandada. O roteador na rede comcat faz o mesmo.
2. Datagrama chega ao servidor DNS, que responde com o IP do site requisitado.

# REDES SEM FIO E REDES MÓVEIS

Estação base: responsável pelo envio e recebimento de dados (torres celulares e pontos de acesso em uma LAN). Quando hospedeiros estão associados com uma estação base, estão operando em modo de infraestrutura;

Modo ad-hoc: sem estações-base, nós só transmitem dentro da cobertura do enlace, nós se organizam em uma rede (roteiam entre si mesmos)

Podemos classificar as redes sem fio de acordo com dois critérios: (i) pacote na rede sem fio atravessa exatamente **um salto único** sem fio ou **múltiplos saltos** sem fio, e (ii) se **há infraestrutura** na rede, como uma estação-base:



### 6.2 Características de enlaces e redes sem fio

Erros de bits mais comuns em enlaces sem fio pois:

**-Redução da força do sinal:** Radiações eletromagnéticas atenuadas quando atravessam algum tipo de matéria, resultando na redução de sua força **(atenuação de percurso)**.

**-Interferência de outras fontes:** Várias fontes de rádio transmitindo na mesma banda de frequência sofrerão interferência umas das outras. O ruído eletromagnético presente no ambiente também pode causar interferência.

**-Propagação multivias:** partes da onda eletromagnética se refletem em objetos e no solo e tomam caminhos de comprimentos diferentes entre um emissor e um receptor. Isso resulta no embaralhamento do sinal recebido no destinatário.

**Sinal eletromagnético**: combinação de uma forma degradada do sinal original e um ruído de fundo no ambiente. A relação sinal-ruído (SNR): quanto maior, facilita para o destinatário extrair o sinal transmitido de um ruído de fundo.

**BER - taxa de erro de bits** (bit error rate)

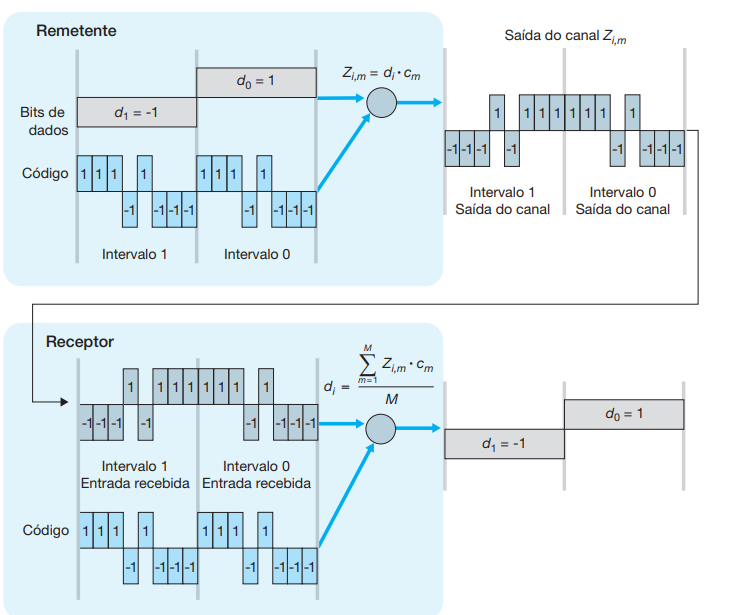
**Quanto mais alta for a SNR, mais baixa será a BER.** Desvantagens do aumento da potência de transmissão: mais energia gasta e mais interferência.

Para determinada SNR, uma **técnica de modulação com uma taxa de transmissão de bit maior terá uma BER maior.**

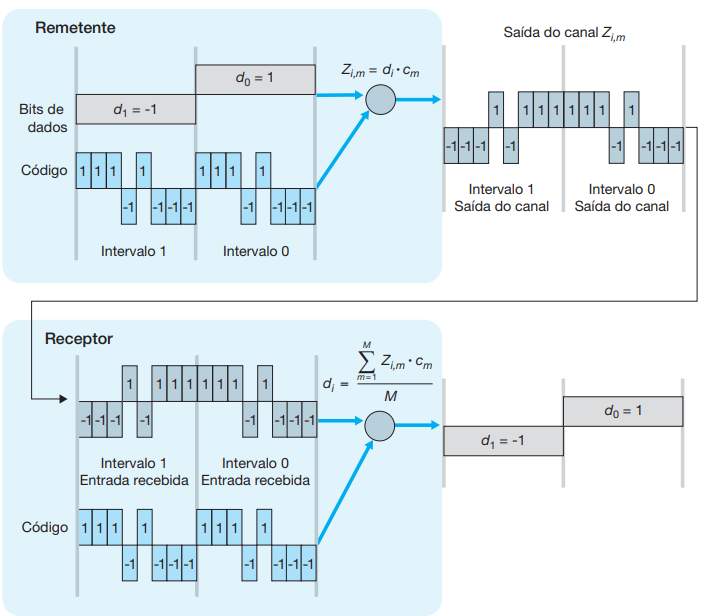
A seleção dinâmica da técnica de modulação da camada física pode ser usada para adaptar a técnica de modulação para condições de canal.

##### 6.2.1 CDMA

Cada bit que está sendo enviado é codificado pela multiplicação do bit por um sinal (o código) que muda a uma velocidade muito maior (conhecida como taxa de chipping) do que a sequência original de bits de dados. **bit 0 = -1.**



Como recuperar bits de dados de um remetente quando são embaralhados por varias transmissões? hipótese de que os sinais de bits são **aditivos**.



### 6.3 Wi-Fi: LANs sem fio 802.11

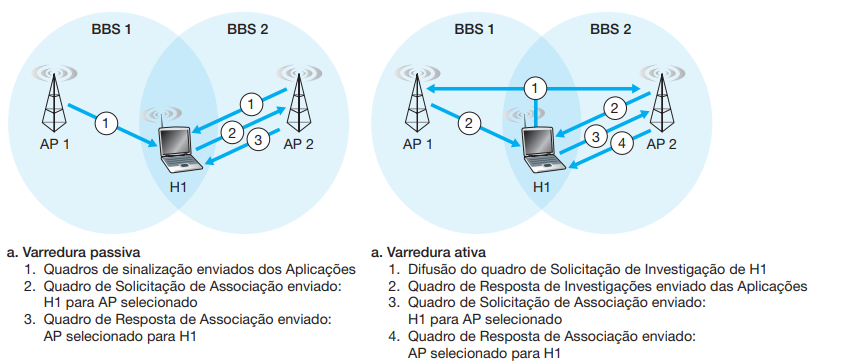
Há diversos padrões 802.11 (b, a, g, a/g e a/b/g). Todos usam CSMA/CA, mesma estrutura de dados, capacidade de reduzir sua taxa de transmissão para alcançar distâncias maiores e permitem modo de infraestrutura e o modo ad-hoc.

Conjunto básico de serviço (**BSS**): contém **uma ou mais estações sem fio** e uma estação-base central/**ponto de acesso (AP)**.

Cada estação sem fio 802.11 e cada AP tem um endereço MAC.

Cada estação sem fio precisa se associar com um AP, o qual tem um **Identificador de Conjunto de Serviços (SSID)** composto de uma ou duas palavras e um **número de canal.**

**Selva de Wi-Fis:** localização que recebe sinal suficientemente forte de dois ou mais APs.

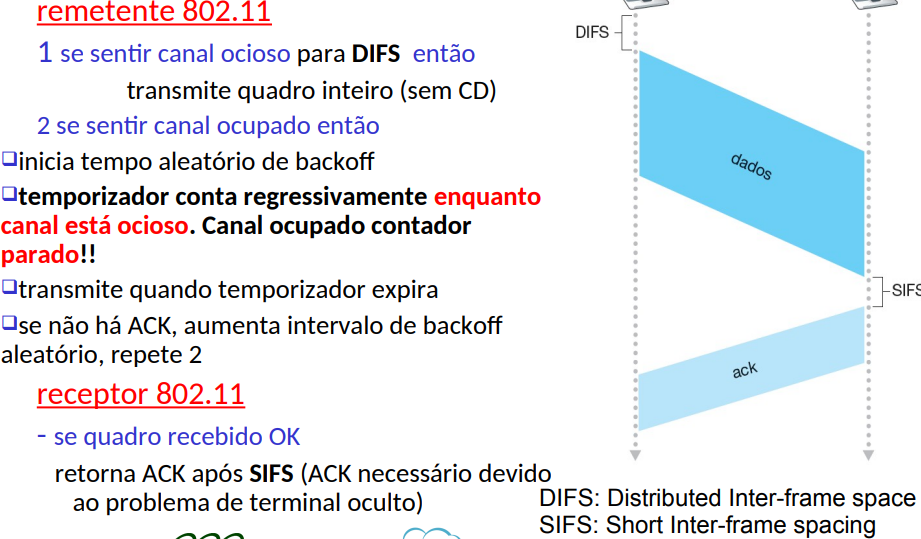
****

**CSMA/CA:** acesso múltiplo por detecção de portadora com **prevenção de colisão**. Diferente do CD (detecta colisão) pois em rede sem fio o meio de transmissão é muito mais lento, então demoro mais pra detectar colisão.

**CSMA/CA:** usa esquema de reconhecimento/retransmissão ARQ da camada de enlace.

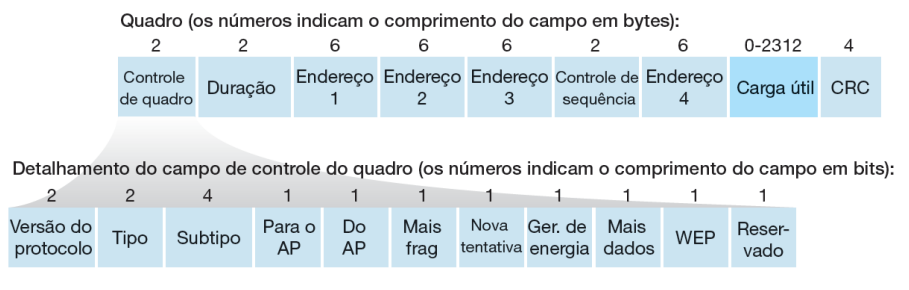
Só posso transmitir tendo certeza que ninguém vai me interromper. Aviso que vou falar, e espero alguém se pronunciar o contrário. Aviso antes!!!

**Reconhecimento na camada de enlace**: estação de destino recebe um quadro, ela espera um curto período de tempo (SIFS) e devolve um quadro de reconhecimento. Se a estação transmissora não receber um reconhecimento em dado período de tempo, admitirá que um erro e retransmitirá. Se não receber reconhecimento após número fixo de retransmissões, desistirá e descartará o quadro.



Tratando de terminais ocultos: **RTS e CTS:** reservam um canal.

Remetente quer enviar, envia um quadro RTS ao AP indicando o tempo total requerido para transmitir e o quadro de reconhecimento (ACK). Quando o AP recebe o quadro RTS, responde por difusão de um quadro CTS.

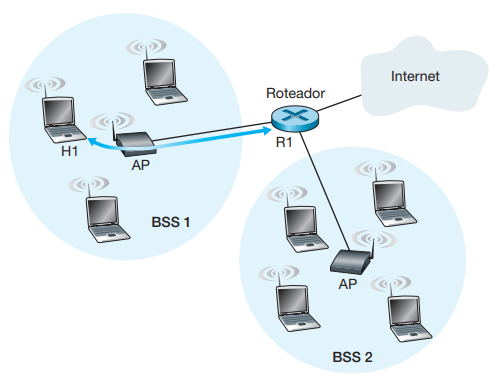


**4 campos de endereços MAC:** 3 para interconexão em rede e um para APs modo ad hoc.

**Endereço 2:** estação que transmite o quadro.

**Endereço 1:** estação sem fio que deve receber o quadro.

**Endereço 3:** endereço da interface de roteador.



**Adaptação da taxa 802.11** escolhe de maneira adaptável a técnica de modulação da camada física.

**Gerenciamento de energia/potência:** permite que os nós minimizem o tempo de suas funções de: percepção, transmissão e recebimento.

Gerenciamento da mobilidade: princípios