Capítulo 1:

1.1) O que é a internet?

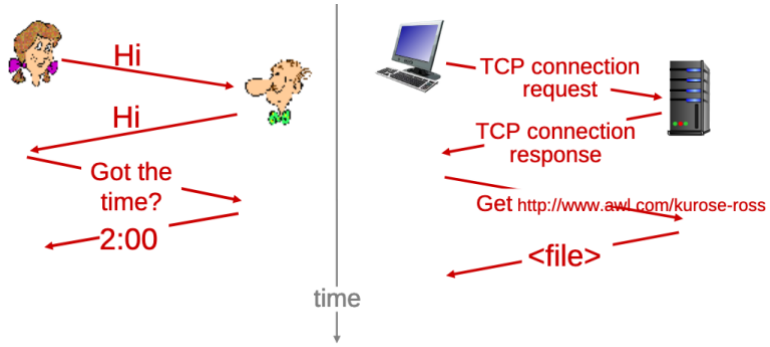
- *Host* ou *end system* pode ser um telemóvel, impressora, qualquer equipamento ligado à rede.
- *Links de comunicação* (ligações) : fibra ótica, cobre, via satélite, etc.
- *Taxa de transmissão:* Largura de banda -> número de bits (informação) que conseguimos transmitir numa dada unidade de tempo (costumamos usar segundo).
- *Routers* e *switches* (*Packet Switches)* conduzem e encaminham o tráfego que os utilizadores geram nas aplicações.

Internet: Rede de redes - Conjunto de protocolos de comunicação/aplicação. TCP e IP são os principais protocolos. TCP assegura a entrega fiável fim a fim (do utilizador A da origem para o utilizador B do fim). Redes IP são responsáveis por fazer o encaminhamento dos dados que geramos por o conjunto de redes interligadas.

Protocolos: Basicamente é um conjunto de regras que regulamentam a comunicação.

Essencialmente definem formatos, ordem de mensagens que são recebidas e enviadas entre as entidades e quais são as ações que devem ser tomadas quando as mensagens são enviadas ou recebidas

Protocolo humano vs Protocolo de redes:



1.2) Periferia de Rede:

Periferia da rede: Hosts (clientes e servidores);
Redes de acesso: Rede por cabo, rede sem cabo;
Core da rede: Equipamento de interligação que assegura o tráfego.

Multiplexagem no domínio da frequência: diferentes canais a transmitirem frequências diferentes (num canal vídeo, noutro áudio, noutro dados, etc).

Os Hosts essencialmente enviam dados. Se tiver uma mensagem de x kBytes, geralmente não é enviado de uma vez para rede. É dividido em pacotes mais pequenos (*packets* de L bits) que vão ser enviados num link de transmissão R (se houver um erro num desse packet, não é preciso reenviar os x kBytes).

$$\text{packet transmission delay} = \text{time needed to transmit } L\text{-bit packet into link} = \frac{L \text{ (bits)}}{R \text{ (bits/sec)}}$$

Meios físicos:

Guiados: cabos de cobre, coaxial, fibra ótica.

Fibras são imunes a ruído eletromagnético (taxa de erro muito inferior), nem causa tanta atenuação como o coaxial por exemplo.

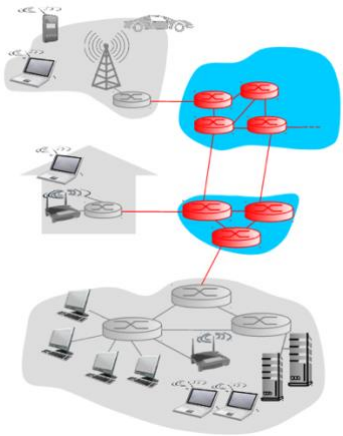
Não-guiados: atmosfera, sinais de radio, etc.

O facto do sinal se propagar num meio aberto causa vários problemas (reflexão, interferência, obstrução por objetos).

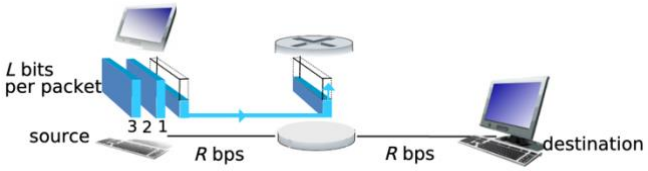
1.3) Core de rede

O core da rede é uma malha de equipamentos de comutação (routers ou switches) conectados entre si.

Recebem os pacotes fragmentos no host do utilizador e encaminham-nos entre si para que o sinal chegue a um servidor destino final. Cada pacote gerado é transmitido SEMPRE à capacidade máxima do link.



Packet Switching:



Demora L/R segundos a transmitir um *packet* de L bits a R bps.

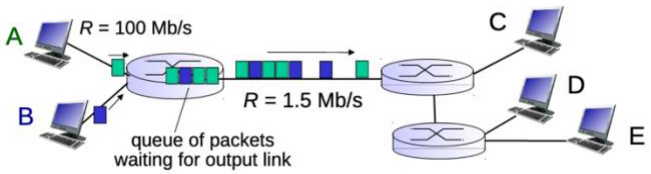
Funciona segundo o princípio *Store and Forward*. Só após receber todo o pacote é que o encaminha para a interface de saída.

Atraso fim a fim: se assumir que o atraso de propagação é 0, na melhor das hipóteses tem-se que o tempo de ida e volta é 2 L/R.

Queueing delay, loss:

Várias entradas, uma saída: se débito de entrada for maior que o débito de saída, os packets vão entrar numa fila de espera e vão ficar à espera até serem transmitidos.

Se a fila está cheia, ocorre *packet drop.*



Routing: determina como é que um pacote é *forwarding* na rede. "Saber encaminhar".

Forwarding: para ocorrer forwarding, é preciso que o routing aconteça. Só depois de todos os routers saberem como encaminhar tráfego é eu o pacote tem possibilidade de chegar ao destino.

Circuit Switching:

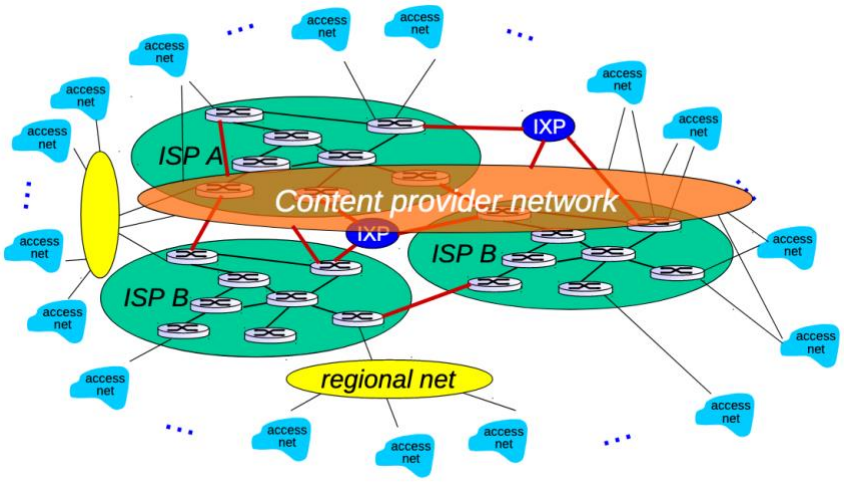
Antes de enviar dados, estabelecer um circuito. (Alocar recursos à cabeça). Se se quer um circuito de A para B de 1gbps, tem que se alocar capacidade de 1 gb para os dois equipamentos.

Função	Rede de Datagramas	Rede de Circuitos Virtuais (VC)
Estabelecimento prévio da conexão (ou circuito)	Não é necessário	É necessário
Endereçamento	Endereço de origem e destino em cada PDU	PDUs contêm o identificador do circuito
Routing / Forwarding	PDUs são encaminhados de forma independente entre si	A rota é estabelecida inicialmente e todos os PDUs utilizam essa rota
Informação de estado	não é necessária	necessária por VC
Falha de um elemento de rede	não é normalmente problemática	todos os VC são terminados
Controlo de tráfego e Controlo de congestão	difícil	fácil, se os recursos atribuídos são suficientes

Packet Switching permite ter mais utilizadores na rede. Circuit Switching permite um melhor desempenho porque há alocação de recursos (maiori. Largura de banda).

Com milhares de redes de acesso, como é que se iria conectá-las entre si?

Utilizam-se milhares de *service providers (ISP's)*, que competem entre si. Para os interconectar existem IXP (*Internet Exhange Point)* e redes regionais.



Este encaminhamento é dinâmico.

1.4) Protocol Layers

Cada camada permite a cooperação entre entidades do mesmo nível protocolar que comunicam entre si, o que cria um contexto comum.

Comunicação por níveis ou camadas:

1) Conjunto de regras que regem a comunicação entre intervenientes;
2) Uma entidade é uma abstração de um ou mais processos computacionais;
3) As regras são implementadas pelas entidades de uma camada protocolar;
4) As função protocolares são variadas e têm âmbitos ou contextos distintos;

Exemplos de funções protocolares:

1) Geração de sinais;
2) Definição de interfaces;
3) Sincronização;
4) Endereçamento;
5) Deteção de erros;
6) Correção de erros;
7) Etc.

O modelo protocolar TCP/IP tem 4 camadas funcionais: aplicação, transporte, rede, ligação, (físico).

Para passar informação da camada da aplicação para o transporte, há um encapsulamento dos dados da aplicação dentro de uma estrutura que tem um *header* próprio.

Capítulo 4: Camada da Rede

Modelos de serviço:

Connectionless – Tipicamente uma rede de datagramas, que são encaminhados de forma independente na rede e sem a necessidade de estabelecer um circuito;

Connection – Circuito Virtual.

Nível de rede organizado a circuitos virtuais implica que a máquina de origem não possa enviar dados sem estabelecer o circuito. Utiliza o endereço de destino para estabelecer o circuito e depois são criados identificadores de circuito.

Tabelas de encaminhamento

IP pega na rota que fizer **match mais longo**. Exemplo:

Destination Address Range	Link interface
11001000 00010111 00010*** *********	0
11001000 00010111 00011000 *********	1
11001000 00010111 00011*** *********	2
otherwise	3

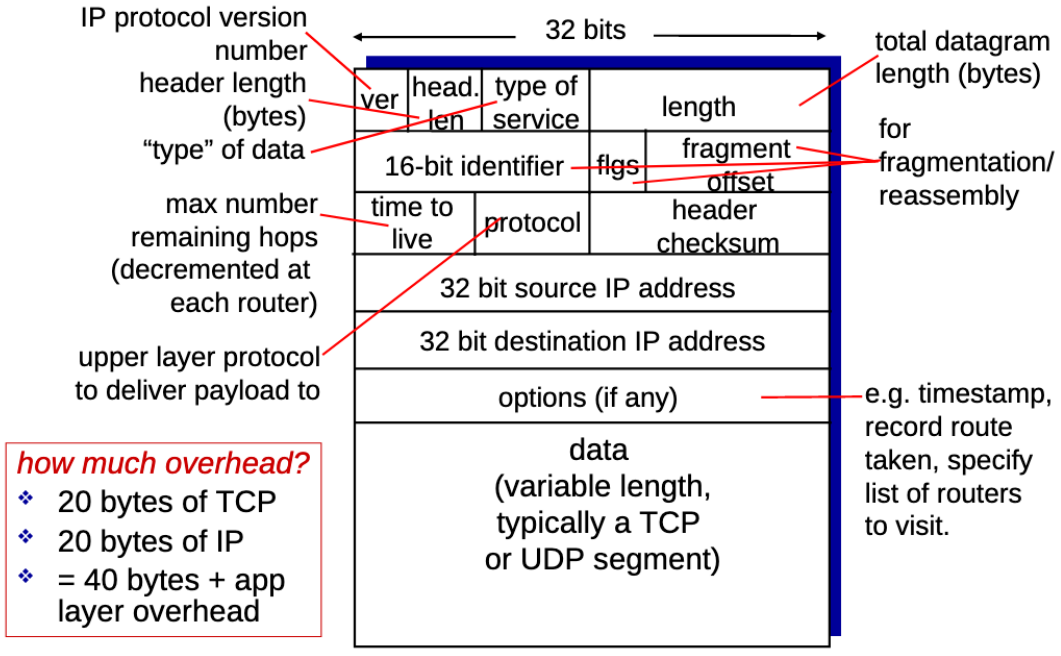
examples:

DA: 11001000 00010111 00011110 10100001 which interface?

DA: 11001000 00010111 00011000 10101010 which interface?

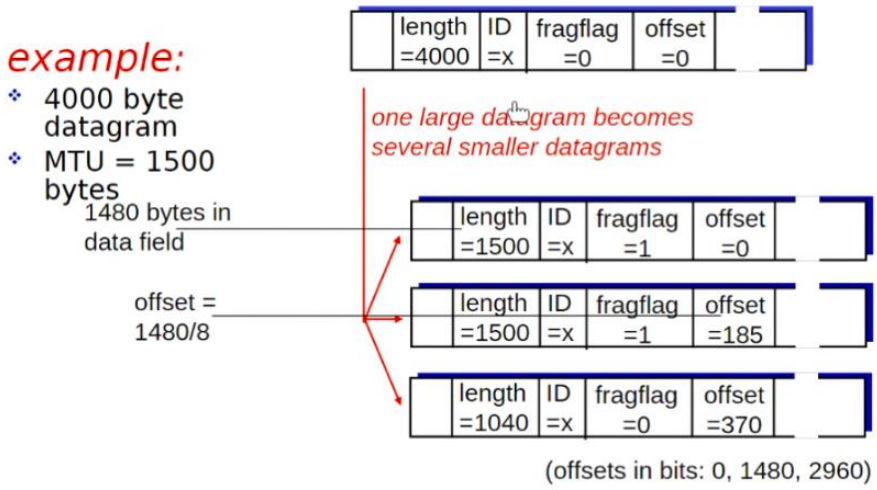
O primeiro exemplo corresponde à interface 2 e o segundo exemplo corresponde à interface 1, apesar de também dar match na interface 2.

IP datagram format



- Datagramas IP maiores do que 1500 bytes, vão ser fragmentados. Uma vez fragmentados, só vão ser reagrupados no destino.

Exemplo fragmentação IP



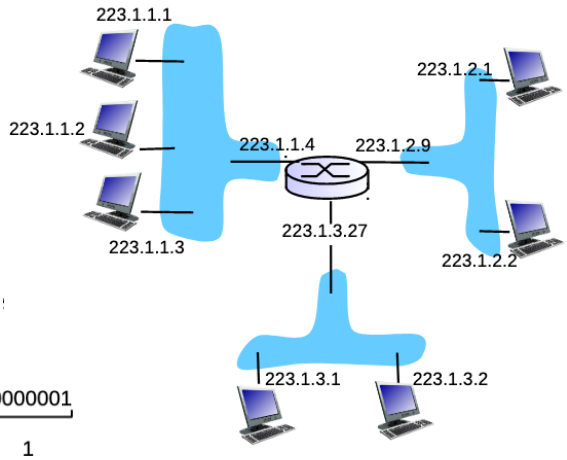
O último fragmento leva o restante do pacote original (daí serem 1040. O datagrama original tem 4000 bytes, ou seja, o payload é 3980 bytes.

IP Addressing

Router -> equipamento interligação nível 3;
Switch -> equipamento interligação nível 2;

Este router possui 3 redes (áreas azuis) e 3 endereços IP cada um associado à sua interface.

- 223.1.1;
- 223.1.2;
- 223.1.3.



Os endereços IP estão associados às interfaces.

exemplo: 223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

Dos 32 bits, há uma parte que identifica a rede (ou sub-rede) e identifica a interface do host.

CIDR – Classless InterDomain Routing

Classe A: máscara /8
Classe B: máscara /16
Classe C: máscara /24

Exemplo:

Considere o IP **130.1.5.1:**

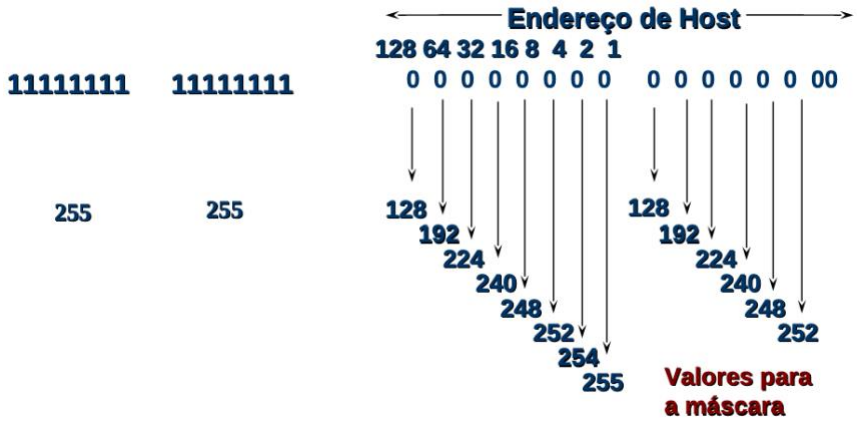
Sabemos que é o endereço **5.1** da rede **130.1.0.0** (classe B).
Máscara por defeito: 255.255.0.0 ou /16.

Considere o IP **130.1.5.1/24:**

É o endereço da estação **1** da sub-rede **130.1.5.0**.
O subnetting é definido no espaço host ID Inicial

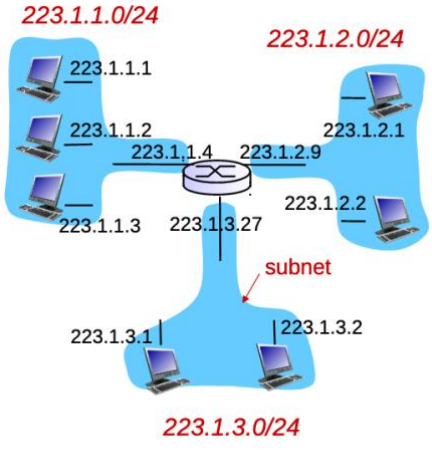
8 bits para subnetting:

- Nº sub-redes: 2^8-2;
- Nº hosts: 2^8-2.



SUB-REDES:

Numa sub-rede os hosts chegam fisicamente entre si sem a intervenção do router. Para determinar as sub-redes, separa-se a ligação ao router, criando redes isoladas. Para ter comunicação entre sub-redes é obrigatório ter um router, com interface para a sua própria rede.



subnet mask: /24

Vantagens vs custo:

- Permite uma melhor organização e gestão dos endereços;
- Permite introduzir mais níveis hierárquicos para routing.

- Reduz espaço de endereçamento (vários endereçamentos passam a não utilizáveis);
- Gestão mais trabalhosa;

Endereços reservados:

- Primeiros 4 bits não podem ser 1;
- 127.x.x.x é reservado para loopback;
- Bits de host a 0's ou 1's;
- Bits de rede /sub-rede a 0's ou 1's.

Endereços privados:

Atribuídos para internets privadas (sem conectividade IP global, não devem ser visíveis, nem são encaminhados na Internet)

- Bloco 192.168.0.0 – 192.168.255.255 /16
- Bloco 172.16.0.0 – 172.31.255.255 /12
- Bloco 10.0.0.0 – 10.255.255.255 /8

Host com várias interfaces é designado de multihomed (múltiplas casas).

Encaminhamento:

- 1ª coluna: Endereço da Rede de destino (mais máscara);
- 2ª coluna: Endereço IP da interface de entrega (next hop);
- N coluna: Indentificador da interface de saída da máquina local;
- Colunas opcionais: flags, tráfego no interface, custo, etc.

```
> netstat -nr
 destination     next_hop        netmask         flags   use         interface
default          192.110.1.254   0.0.0.0         UG      102410      tu0
192.110.1.0      192.110.1.240   255.255.255.0   UH      234576      tu0
.......          ......          ……..           .......  ......      .......
192.168.1.0      192.110.1.253   255.255.255.0   UG      124586      tu0
```

Leitura da última linha: Um datagrama destinado à rede 192.168.1.0 será entregue na interface de endereço 192.110.1.253 saindo pela interface local tu0.

SuperNetting

Tratar das redes diretamente ligadas, tráfego interno, e rota por defeito! A rota por defeito tem de garantir acesso ao à rede onde o router está ligado. Neste caso é RTR. Nas redes internas só precisamos de saber que são acessíveis via RTR2 (neste caso). Especificamos isso através do IP de RTR2.

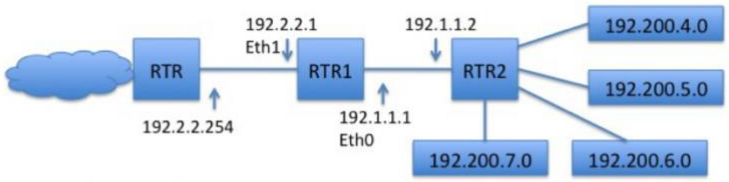


Tabela de encaminhamento de RTR1 - sem Supernetting

Destino	Próximo Nó	Máscara	Interface
192.2.2.0	192.2.2.1	255.255.255.0	Eth1
192.1.1.0	192.1.1.1	255.255.255.0	Eth0
192.200.4 (0000 0100).0	**192.1.1.2**	**255.255.255.0**	**Eth0**
192.200.5 (0000 0101).0	**192.1.1.2**	**255.255.255.0**	**Eth0**
192.200.6 (0000 0110).0	**192.1.1.2**	**255.255.255.0**	**Eth0**
192.200.7 (0000 0111).0	**192.1.1.2**	**255.255.255.0**	**Eth0**
Default	192.2.2.254	0.0.0.0	Eth1
192.200.4(0000 0100).0	**192.1.1.2**	**255.255.252 (11111100).0**	**Eth0**

As conexões internas partilham o mesmo próximo salto, o que permite fazer agregação de rotas. Para agregação de notas precisamos de alterar a máscara. Se olharmos para a parte em binário, há uma parte comum. Logo os dois últimos bits são irrelevantes para a forma de encaminhar. Abdicando deles, não criamos ambiguidades, mas temos uma só entrada na tabela de encaminhamento com a máscara 255.255.252.0. Reduz-se 4 entradas para 1 entrada.

As bridges (e switches) são equipamentos nível 2 e, por isso, não é visível a nível 3. Isto é, quando definirmos as redes IP's, não as consideramos. (Não criam sub-redes).

IP Estático:

Rota estática, é o administrador que as configura e são imutáveis. É um esquema bastante rígido, pouco flexível, mas simples e consegue reduzir o tráfego na rede.

IP Dinâmico:

Rota dinâmica, e atualizada ao longo do tempo. Os routers trocam informação de routing entre si. Implementam protocolos específicos (RIP, OSPF, BGP, etc). Tem uma grande flexibilidade e adapta-se de forma automática a falhas ou mudanças na configuração da rede. O tráfego da atualização pode causar sobrecarga na rede.

Caminho por defeito é a rota a seguir caso não exista uma entrada específica na table para a rede de destino. Caso particular de encaminhamento estático.

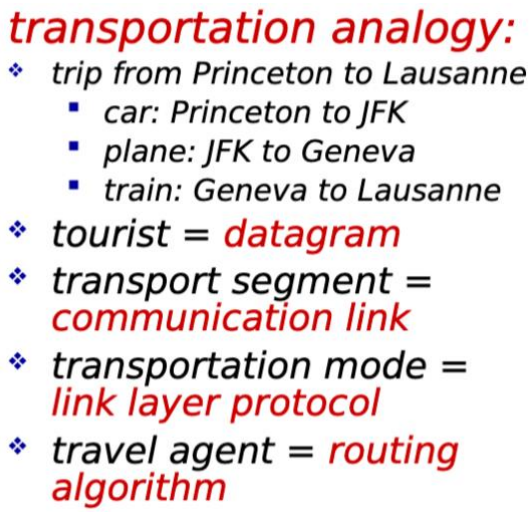
Computação dinâmica das rotas:

Centralizada: cada router, conhecendo a topologia da área, determina o melhor caminho para os possíveis destinos dessa rede;

Distribuída: cada router envia informação de encaminhamento que conhece aos routers seus vizinhos (redes a que dá acesso).

Capítulo 5: Link Layer – Nível de ligação de dados

Responsabilidade é diferente do nível do IP. Transfere um datagrama de um nodo para outro que seja fisicamente adjacente.



Framing: encapsular o que o nível 3 passa numa unidade de dados nível 2 (frame).

Endereço MAC é também endereço físico.

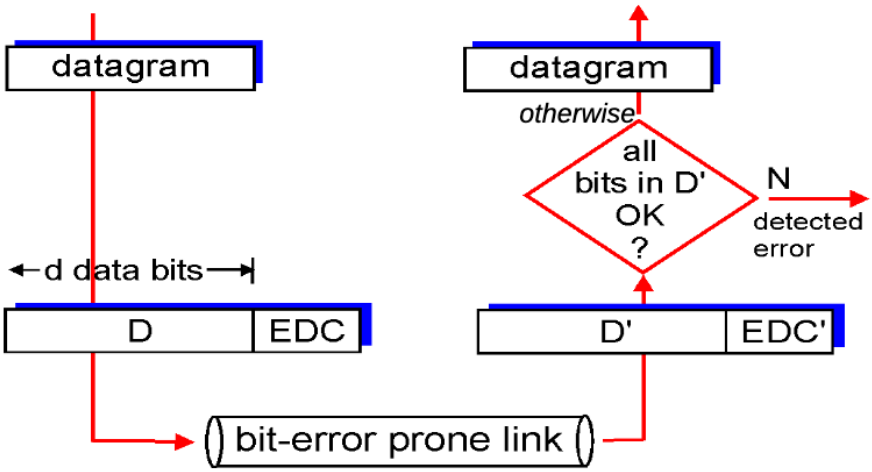
Controlo de fluxo: Serviço genérico que pode existir no nível 2. Regula a cadência entre nós adjacente. Um que envia e outro que recebe.

Controlo de erros: 2 tarefas : deteção e correção. Posso receber uma entrega não fiável e simplesmente descartar, sem corrigir. Códigos de correção são muito pouco usados porque possuem overhead muito grande. Utilizam-se então códigos de retransmissão.

Redes cabeladas têm muitos poucos erros e é possível que nem tenham código de deteção de erros. Redes WiFi, como o meio é muito mais suscetível a erros, o código de deteção de erros está sempre presente.

Half-duplex e Full-duplex: Half-duplex são bidirecionais alternadas (ou transmite um ou transmite outra) e Full-duplex são simultâneas.

Error detection



Mac Address e ARP

Endereços únicos na rede local. Isto é, só podemos ter acesso a eles se for adjacente à nossa rede local.

Endereço IP -> muda de acordo com a rede "hospedeira";
MacAddress -> não muda.

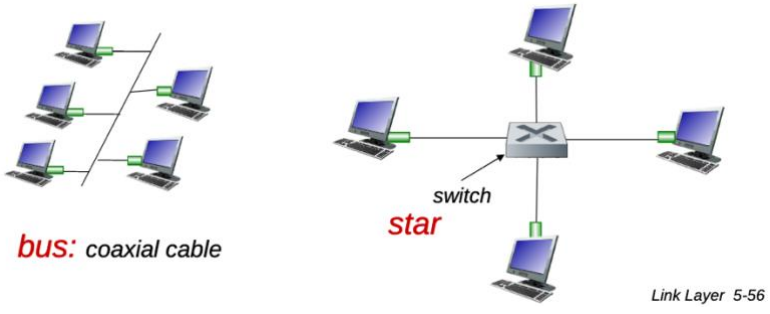
Protocolo ARP permite saber o endereço Mac através do seu IP.

Se A quer enviar uma trama para B, mas o endereço MAC do B não está na tabela ARP do A, A tem de fazer um ARP request, que contém o endereço IP de B. O endereço MAC destino utilizado é o endereço de broadcast layer-2 (ff-ff-ff-ff-ff-ff). Quando uma trama possui esse endereço, TODOS os sistemas nessa LAN vão processar essa trama. Vão desencapsular, processar o pacote IP, e ver se o seu IP é igual ao IP pedido. A máquina com o IP correspondente, vai responder a A com uma primitiva "ARP reply" com o seu endereço MAC. E nessa altura o A pode atualizar a sua tabela ARP com a informação recebida.

Ethernet

Bus: todos os nós no mesmo domínio de colisão. Podem colidir uns com os outros. Popular até os anos 90.

Start: Switch no centro. Não há colisão. Usada nos dias de hoje.



Unreliable, Connectionless

ConnectionLess: Não orientadas à conexão. Basta que sinta um meio em silencio para enviar as tramas; não há qualquer negociação entre um MAC de origem e um MAC de destino.

Unreliable: Não há confirmações entre NIC's dizendo se a trama chegou bem ou não. Se algo corre mal, as NIC's descartam a trama e depois tentam recuperar de colisão.

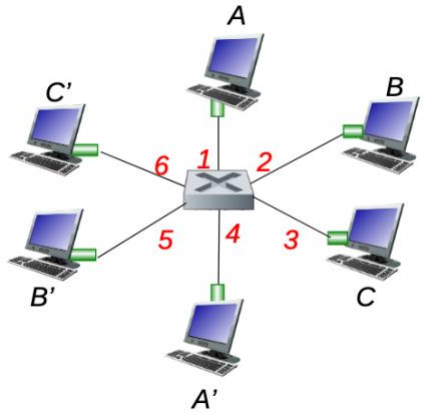
Switches:

Equipamento nível 2.

O switch é capaz de paralelismo, **Store and Forward** das frames. Em situações de contenção, duas tramas a chegar ao switch por portas diferentes destinadas à mesma porta, primeiro comuta uma e depois comuta a outra. Examina o MAC Address da trama que está a chegar e seletivamente encaminha essa trama por uma ou mais portas de saída. É **transparente**, isto é, os hosts não sabem da presença de switches. Têm a **capacidade de aprendiza**gem, não precisa de muita configuração (apenas a básica necessária).

Permite também transmissões simultâneas sem colisões.

A para A' e B para B', mesmo que em simultâneo, é capaz de fazer a comutação e ocorrem transmissões em paralelo. Permite isolar qualquer problema elétrico só afeta o seu domínio de colisão. Isto é, se a ligação A -> switch tiver com problemas, o resto da rede continua a funcionar.



Como é que o switch sabe que o A' é alvancável através da interface 4 e que o B' é alcancável através da interface 5?

Tem uma tabela que faz o mapeamento com o endereço **Mac do host, a interface para alcançar esse host e um tempo** associado.

Como é que estas entradas são criadas e mantidas na tabela?

R: **O switch aprende**

O switch vai aprendendo à medida que o tráfego vai fluindo. Quando o switch envia uma trama, ele aprende a localização de quem envia. Se ele não sabe determinado MAC destino, envia para todas as portas.

Ex: quando A envia tráfego, ele na tabela regista que A chega pela interface 1.

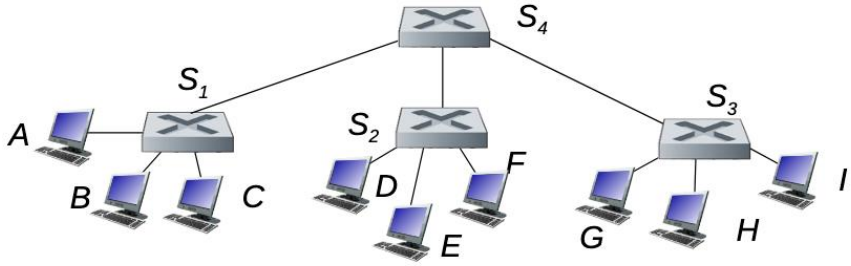
MAC addr	*interface*	*TTL*
A	*1*	*60*

Switch table (initially empty)

Quando uma trama é recebida:

1. Regista por qual interface é que chegou a trama e o endreço MAC de quem envia;
2. Indexa a tabela usando o MAC destino. E depois ou esse endereço existe ou não na tabela;
3. Se a entrada existir, ele vai primeiro validar se o destino está num segmento diferente daquele onde chega a trama; (situações com topoligias com múltiplos switches, ter a certeza que a trama não é reenviada no link onde está a chegar;
4. Se sim, então descarta a trama;
5. Se não, faz o forward da trama pela interface indicada na entrada (MAC destino);
6. Se a entrada não existir na tabela, faz **flood**. Envia a trama para todas as interfaces à exceção daquela onde chega a trama.

Switches interconectados:



S1, S2, S3 e S4 são redes comutáveis.

Se quisermos enviar uma trama de A para G, aplica-se na mesma o **algoritmo de auto aprendizagem.**

À medida que o tráfego vai fluindo, a tabela de comutação de S4 pode ter numa só entrada o A, o B e o C na porta 1. O que as tabelas têm é uma lista de endereços MAC que são atingidos a partir de uma determinada porta.

Switch vs router

- Ambos são store-and-forward;

- Router – NetWork Layer: Trata endereços IP e questões de encaminhamento;
- Switch – Link Layer.

- Router – Tabelas de encaminhamento atualizadas por protocolos de encaminhamento ou estaticamente;
- Switch – Tabelas de comutação feitas com base em aprendizagem e lidam com endereços MAC em vez de endereços IP.

Capítulo 6

Redes sem fios: modo **infraestruturado** – obrigatoriamente uma ligação a uma infraestrutura. Há a possibilidade entre àreas.

Podem também funcionar em modo **ad hoc:** nós só podem comunicar se tiverem dentro da area de cobertura.

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Os sinais através do ar e obstáculos são significamente atenuados, há um decréscimo da força de sinal (contrariamente ao que acontece a sinais cabelados). E, portanto, este meio é mais suscetíveis a sofrer interferências.

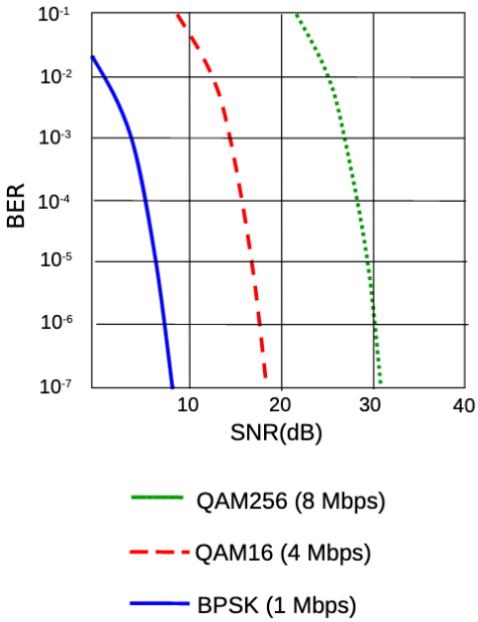
A banda de 2.4 GHz é uma banda onde funcionam muitos dispositivos, havendo uma grande interferência.

O sinal de radio reflete-se em paredes, obstáculos, etc, chegando ao destino com pequenos desfaçamentos – **Multipath Propagation**

SNR – Relação sinal ruído. Quanto mais forte for o sinal, mais fácil é extrair o ruido e ficar com o sinal limpo.

BER - Bit Error Ratio – bits errados face aos bits trasmitidos. O objetivo é que seja o mais baixo possível.

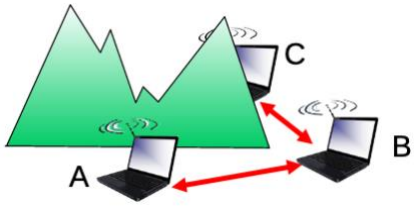
É possivel diminuir o BER se se aumentar a potência do sinal. Mas também é possível reduzir o débito (banda) de forma a manter o BER em níveis baixos.



Problemas

Terminal escondido:

A escuta o B, o B escuta o C mas o A não escuta o C. A e C podem transmitir simultaneamente e pode ocorrer interferência em B.



IEEE 802.11 wireless LANs ("Wi-Fi")

802.11b
- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer

802.11a
- 5-6 GHz range
- up to 54 Mbps

802.11g
- 2.4-5 GHz range
- up to 54 Mbps

802.11n: multiple antennae (4)
- 2.4-5 GHz range
- up to 200-600 Mbps

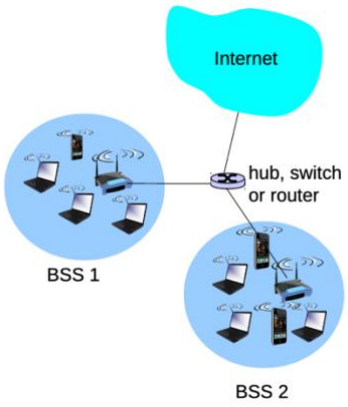
802.11ac: multiple antennae (8)
- aka Gigabit Wi-Fi
- 5.8 GHz band
- up to 7 Gbps

802.11ax: (under development)
- aka Wi-Fi 6, large # of users
- 2.4-5 GHz range
- up to ~10 Gbps

Todas usam **CSMA/CA** para acesso múltiplo. É um método controlo de acesso específico de redes Wi-Fi.

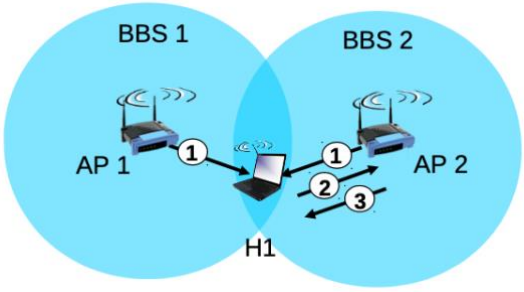
Base Station = Access Point (AP);

Basic Service Set (BSS) -> Area de cobertura que está a ser servida por um particular AP.

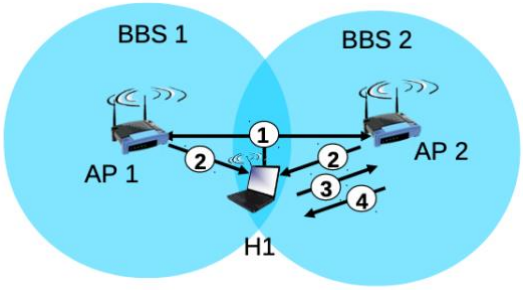


Um host para poder operar tem de se associar ao AP. Faz **scanning** dos vários canais ou então pode ir recebendo "beacon frames"(beacons) que são enviadas pelos AP que informam sobre o nome do AP (SSID) e o MAC adress. O host, após a receção de beacons, seleciona um AP à qual se vai associar.

Scanning passivo: feito quando o host H1 toma conhecimento das caracteristicas da BSS através de beacons. Estes são enviados do AP para as STA's. Com base nesses beacons, a estação H1 escolhe qual o AP que se vai associar.



Scanning ativo: o host H1 envia um probe request em broadcast e os AP's que estão nas imediações respondem – probe response.



Acessos múltiplos

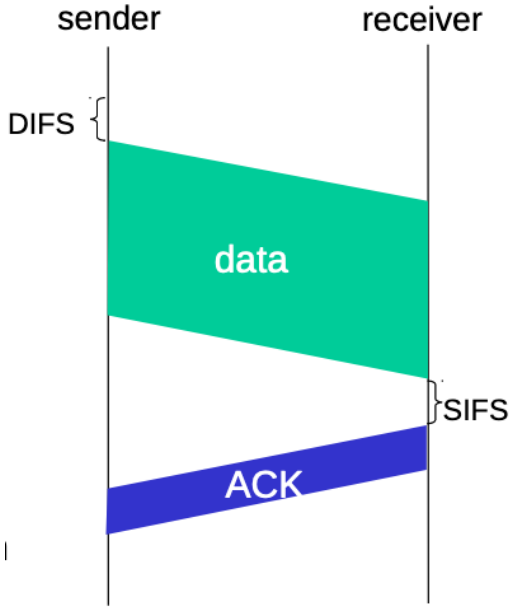
CSMA, escutar o meio antes de transmitir. Há situações em que a colisão não é detetada de forma eficaz.

Num meio wireless, não conseguimos ter garantia da qualidade do sinal que a estação recetora está a ter uma vez que se podem receber sinais muito fracos. Portanto, o que o 802.11 decidiu foi que não iam fazer deteção de colição mas sim **evitar colisões: (CSMA/C(collision)A(voidance)).**

802.11 sender: há um tempo inicial que o sender tem de esperar antes de começar a transmitir. (DIFS: 28 – 50 micro segundos)

Depois desta espera, transmite a trama integralmente sem fazer deteção de colisão.

Se o meio está ocupado, a estação não fica de forma persistente a tentar enviar o sinal. Começa o "random backoff time" e o timer conta enquanto o canal está inativo. Se não recebeu o ACK, aumenta o "backoff time" e volta a entrar no ciclo de espera.

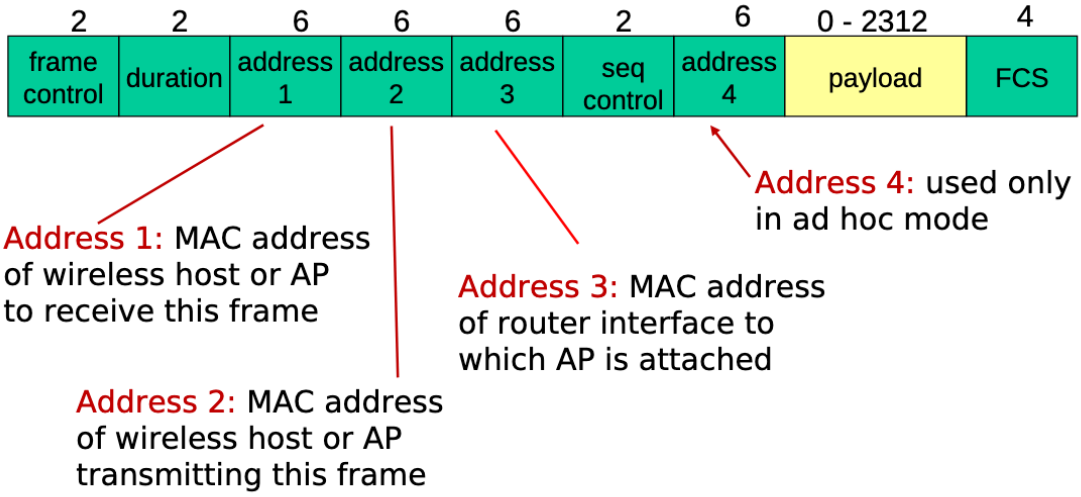


802.11 receiver: espera SIFS (10 - 16 micro segundos) e se a trama é recebida, envia um positivo ackoledgment. Se este ACK não chega, é porque houve erro.

Apesar de haver tempos de espera, pode de facto ocorrer colisões (devido ao nó escondido, por exemplo). Portanto, antes de enviar dataframes, usar tramas de mais curta duração que fazem um pedido de acesso ao meio. A STA (station), antes de começar a enviar uma trama longa, usa pequenas tramas que pedem o acesso ao meio (RTS – request to send). Não remove totalmente as colisões porque podemos ter colisões a nível dos RTS, mas uma vez que uma STA ganha acesso ao meio, não existem mais colisões. Depois da estação enviar o RTS, o AP faz um broadcast do CTS (clear to send). O CTS é enviado a todos os nós.

Este método (RTS/CTS) permite reservar o canal, e é bastante importante no sentido de remover na totalidade a colisão entre tramas porque uma vez que uma STA ganha acesso ao meio, durante esse periodo tem o meio reservado só para ela.

A probabilidade de haver colisões entre RTS é muito baixa. Caso ocorra, acontece CSMA/CA. (backoff durante algum tempo e voltam a enviar o sinal).



toDS	fromDS	addr1	addr2	addr3	addr4	obs.
0	0	DA	SA	BSSID	-	ad hoc
0	1	DA	BSSID	SA	-	do AP
1	0	BSSID	SA	DA	-	para AP
1	1	RA	TA	DA	SA	dentro DS

A semantica dos endereços depende do tipo de trama e da sua direcionalidade.
toDS e fromDS:

(0,0) -> não vai nem vem do sistema de distribuição. Não tem de ser exclusivamente um cenário de uma rede ad hoc. São tramas que ficam na BSS.;

(0,1) -> vem do sistema de distribuição;

(1,0) -> vai para o sistema de distribuição;

(1,1) -> dentro do sistema de distribuição. Mais complexa.

Management frames – used to perform supervisory functions such as joining and leaving wireless networks and moving associations from AP to AP.

Control frames - used in conjunction with data frames to perform control operations such as channel acquisition and carrier-sensing maintenance functions, and positive acknowledgment of received data. Control frames allow to deliver data reliably from STA to STA.

Data frames - used to send data from STA to STA. Several different data frame may occur, depending on the network.

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

Power managment:

Quando a estação ou o AP levantam o bit de power management, o que permite é quer ao nó, quer ao AP, fazer uma gestão mais eficiente da transferência de dados entre ambos. “Im going to sleep” até ao próximo beacon interval.

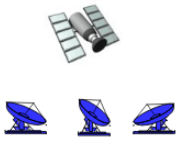
Do lado do AP para a estação, o AP dá a indicação à estação se essa estação tem ou não dados para receber. Se tiver mantem-se acordada, senão “volta a dormir”.

Capitulo 5 – Acessos múltiplos e protocolos

O maior desafio é quando há um meio de difusão: um meio partilhado em que qualquer estação pode aceder ao meio e uma vez acedendo ao meio, todas as outras têm a possibilidade de ouvir e receber a trama que está a ser transmitida.

shared wire (e.g., cabled Ethernet)

shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

humans at a cocktail party (shared air, acoustical)

Colisão: se um nodo recebe 2 ou mais sinais ao mesmo tempo. As tramas vão ser recebidas com erro.

Para regulamentar este acesso, utilizam-se **protocolos de acesso múltiplo.** Uma regra base é que este controlo seja feito usando o próprio canal de comunicação. “In-band channel”.

Taxonomia – esquema de classificação dos protocolos

3 classes genéricas:

- Channel Partition: canal é dividido em pequenas unidades. Os protocolos alocam pequenos troços de capacidade da ligação para uso exclusivo de um determinado nodo.
- Random access: canal não é dividido e, não sendo dividido, há a possibilidade de ocorrerem colisões. Vai haver uma forma de recuperar dessas colisões.
- Taking turns: passagem de “tokens” de uns nodos para outros.

Channel Partition:

TDMA:

Método livre de contenção. A capacidade do canal é, numa primeira estância, dividida em "time frames", e cada time frame dividida em slots.

O acesso vai sendo feito dentro de cada time frame. Cada estação obtém a um time slot fixo, que normalmente corresponde ao tempo de transimssão do pacote. Slots que não sejam usados por estações não são reusados por outras estações. Vão para um estado de "idle".

Pros: Não possui colisões e é um sistema justo. Não há nenhuma estação a bloquear as outras e quando quer transmitir, pode fazê-lo.

Cons: Pode conduzir a perda de capacidade de comunicação.

FDMA:

O canal é dividido em múltiplas frequências e cada estação é atribuida uma frequência.

Random access:

Quando uma estação acede ao meio, tem a capacidade de utilizar toda a capacidade existente para transmitir.

Preocupam-se em tentar detetar ou tentar evitar as colisões.

Ex: slotted ALOHA; ALOHA; CSMA; CSMA/CD; CSMA/CA(usada em wireless)

Slotted ALOHA:

<u>Princípios:</u>

-Todas as tramas têm o mesmo tamanho;

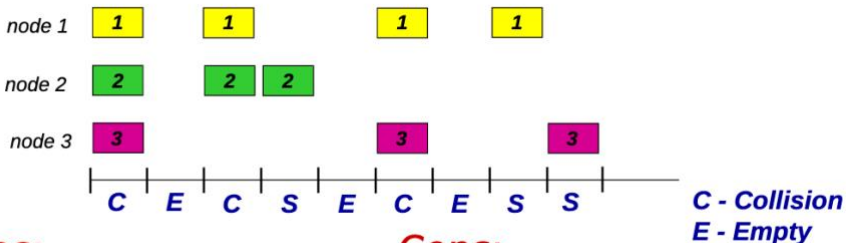
-Slots cuja duração é o tempo necessário para transmitir uma trama;

-Nodos começam a transmitir só no inicio do slot e que estão sincronizados;

-Pode haver colições.

<u>Operações:</u>

Qualquer estação que sinta um slot livre pode transmitir, e se tiver mais tramas para transmitir, pode transmitir imediamente no proximo slot.



Pros:

- *single active node can continuously transmit at full rate of channel*
- *highly decentralized: only slots in nodes need to be in sync; each node detects and solves collision*
- *simple*

Cons:

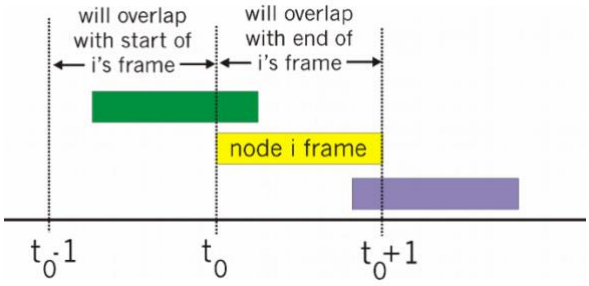
- *collisions, wasting slots*
- *idle slots*
- *nodes may be able to detect collision in less than time to transmit packet*
- *clock synchronization*

A eficiencia é, no máximo, 37%, é baixa.

Pure ALOHA:

Não considera slots, logo não tem sincronização.

A probabilidade de colisões aumenta uma vez que uma trama enviada em t0 pode colidir com uma enviada em t0-1 e t0+1.

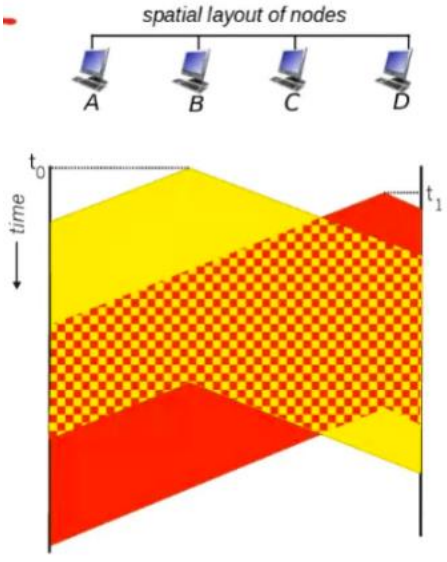


Eficiência de 18%.

CSMA:

Neste método escuta-se o meio antes de começar a transmitir. Para a analogia humana é "Se alguem fala, eu não vou interromper".

Pode ocorrer colisões devidido ao "delay" . Um nodo B pode começar a transmitir e um nodo D pode começar a transmitir uma vez que ainda não ouviu o B.



Há uma interferencia do sinal amarelo com o sinal vermelho que corrompe a trama.

CSMA/CD (collision detection):

Num meio partilhado **cabelado** é possivel detetar colisões porque a rede que está a transmitir faz simultaneamente a análise ao meio e apercebe-se que o sinal que está a colocar no meio deixa de ser igual aquele que está a transmitir. E, portanto, em redes cabeladas, é facilmente detetada a colisão. Em redes wi-fi não é fácil devido ao fading, redes escondidas, etc. Por isso é que se usa o CSMA/CA.

Em meios cabelados, as estações quando detetam uma colisão abortam a transmissão para otimizar o desperdicio do uso de canal.

Se a colisão é detetada, as estações reforçam a colisão (geram um ruído para a linha) e abortam a colisão. Depois de abortar, fazem backoff.

1. *NIC receives datagram from network layer, creates frame*
2. *If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.*
3. *If NIC transmits entire frame without detecting another transmission, NIC is done with frame !*
4. *If NIC detects another transmission while transmitting, aborts and sends jam signal*
5. *After aborting, NIC enters binary (exponential) backoff:*
   - *after mth collision, NIC chooses K at random from {0,1,2, …, 2^m-1}. NIC waits K·512 bit times, returns to Step 2*
   - *longer backoff interval with more collisions*

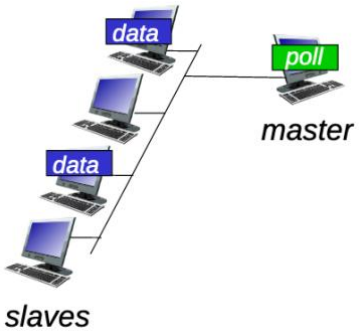
Taking turns:

Polling:

Um primário e vários secundários e é um primário que coordena. Fazer polling às estações e só depois é que a estação envia dados.

Problemas:

- Polling overhead;
- Latencia;
- Ponto de falha (master).



Token passing:

Um token cirucla na rede e só a estação que tem o token consegue transmitir.

Problemas:

- Token overhead;
- Latencia;
- Ponto de falha (token).

Resumo:

channel partitioning, by time, frequency or code
- *Time Division, Frequency Division*

random access (dynamic),
- *ALOHA, S-ALOHA, CSMA, CSMA/CD*
- *carrier sensing: easy in some technologies (wire), hard in others (wireless)*
- *CSMA/CD used in Ethernet*
- *CSMA/CA used in 802.11*

taking turns
- *polling from central site, token passing*
- *bluetooth, FDDI, token ring*