IPv6

- MAIOR eficiência ao nível do desempenho, roteamento e estabilidade de taxas de encaminhamento
- endereços IPv6 têm tempo de vida e são auto-configuráveis

MÉTODOS DE CONFIGURAÇÃO AUTOMÁTICA

↳ STATELESS → configuração determinada pela rede

↳ STATEFULL → configuração determinada pela gestão de rede

Processo:

1. é criado um link local
2. verifica-se a unicidade do endereço de link-local
3. seleciona-se o método de configuração
4. determina-se a informação a ser auto-configurada

WIRELESS

IEEE 802.11

COMPONENTES:

× estações → quaisquer dispositivos que se liguem a uma rede wireless

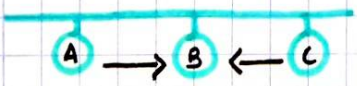
× pontos de acesso → interface wireless que liga à rede wireless (AP's)

> Routers Wireless podem ser pontos de acesso, no entanto, nem todos os pontos de acesso podem ser Routers
>
> NOTA

× basic service set → Rede wireless que permite ligar a um ponto de acesso, diz qual a rede wireless que aquele AP fornece

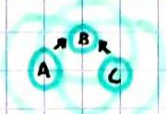
× extended service set → vários pontos de acesso - mesma rede wireless

WIRED × WIRELESS



ETHERNET

→ o PCA e o PCC estão em áreas diferentes a transmitir info para o PCB que se encontra no meio (PCA não sabe que o PCC existe e vice-versa). Isto gera uma colisão em B se A e C enviarem info em simultâneo, e nenhum dos dois irá perceber que houve colisão



WIRELESS LAN

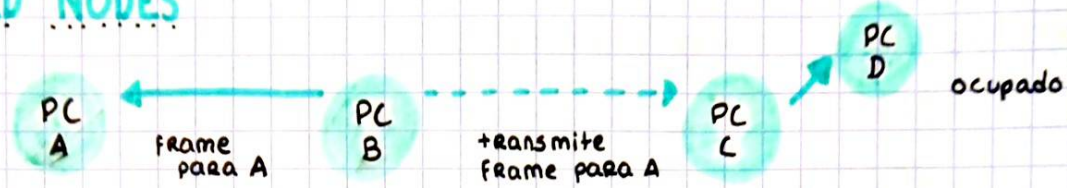
→ as antenas do wireless não detetam colisões, têm de trabalhar em half-duplex - transmissão e recepção de dados acontece alternadamente, enquanto 1 transmite o outro só recebe informações

→ full-duplex - ambos podem transmitir e receber info entre eles em simultâneo.

HIDEN NODES

"nós escondidos", permitem detetar colisões no recetor, através de virtual carrier sensing, o emissor questiona o recetor, se este recebe os pacotes. Se não houver resposta, ele deve assumir que o canal está ocupado

EXPOSED NODES



- Temos então uma situação em que o computador B pretende enviar um pacote para A, para fazer isto numa rede Wireless o PC envia o frame para a rede, não de forma orientada
- Deste modo há o risco do pacote cair num terminal que lhe seja acessível mas cujo pacote não lhe interessa - Risco de encontrar terminais expostos

MACA → multiple access with collision avoidance

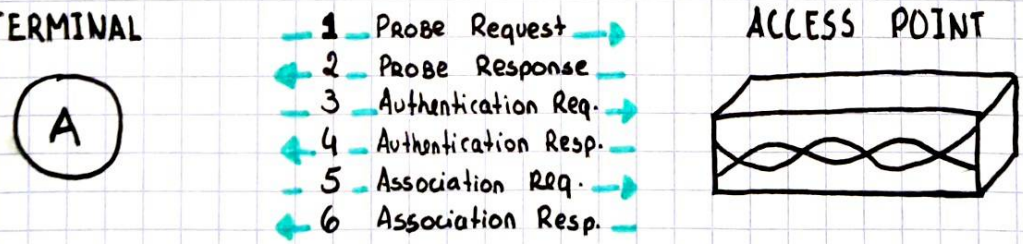
- todos os terminais terão de respeitar o prévio envio de pedidos e permissões para ocupar os canais
- quando um terminal quer enviar um pacote para outro, primeiro deverá enviar um **RTS** (request to send), em resposta a este pedido deve ser enviado um CTS (indica que o canal não está ocupado - clear to send)
- quer o RTS, quer o CTS contêm endereço de destino, origem e tamanho da info a ser enviada

JOINING A BSS

NOTA!
→ Apontamentos página 34

1. a estação têm de achar a rede wireless, pode fazê-lo de modo ativo ou passivo

- scanning passivo → o PC não fez nada, simplesmente ouviu o que o ponto de acesso estava a enviar



- Tanto a autenticação como a associação são necessárias para aceder a um BSS

FASES → | 1 e 2 | 3 e 4 | 5 e 6 |

Não autenticada	Autenticada	Autenticada
Não associada	Não associada	Associada

WLAN FRAMES → Existem 3 tipos de tramas:

1. Controlo → RTS, CTS, ACK
2. Management → Probe Request, Probe Response, Authentication ..., Association...
3. Data

↳ ver análise do gráfico no vídeo

JOINING BSS WITH AP:

SCANNING

↳ Como é que uma estação se liga a uma rede wireless? 1º é necessário fazer o scanning da rede para descobrir onde podem ligar, este scanning pode ser:

PASSIVO → esperas que a rede não esteja escondida e que o ponto de acesso esteja a mandar frames Beacon a dizer a rede e as suas características, e assim o terminal sabe onde está a rede. Frames Beacon são enviados periodicamente pelos pontos de acesso

ATIVO → uma máquina liga-se, já tem um conjunto de redes wireless configuradas e então ~~liga-se~~ tenta achar os APs. Envia um Probe Request, espera que esteja lá um AP e o mesmo responde com um Probe Reply, contendo informação ... etc...

↳ ver análise Beacon Frame + Probe Resp. / Req

JOINING BSS WITH AUTHENTICATION

↳ Assim que um ponto de acesso é encontrado, uma estação passa pela autenticação:

"é uma rede aberta?" "SIM / NÃO" → Caso seja aberta não precisa de + nada

JOINING BSS WITH ASSOCIATION

↳ Assim que uma estação é autenticada, dá-se início à associação

1. Estação —ASSOCIATE REQUEST FRAME→ Address Point

1. O frame tem info sobre o WNIC incluindo "supported data Rates e os SSID da rede a que a estação se quer associar

2. Estação ←ASSOCIATE RESPONSE FRAME— Address Point

2. Aceitação ou rejeição do pedido de associação, contém info como o ID da associação

!!! Só depois da associação estar completa é que a estação consegue transmitir e receber tramas de dados

DATA FRAME ➡ para os dados após a associação temos as tramas de dados

mecanismos de autenticação e autorização

1. Rede Aberta
2. Rede Aberta + MAC
3. Rede Aberta + VPN-gateway
4. Rede Aberta + Web gateways
   ...

-> IEEE 802.111 (WPA 2)
-> VPN

OPEN NETWORKS

- Fornecem endereços IP com DHCP
- Não há autenticação, acesso livre
- Controlo de acesso é complicado
- Não requer software específico

OPEN NETWORKS + MAC AUTHENTICATION

- O controlo da estação MAC address é adicionado
- MAC address pode ser falsificado
- Não pode ser usado em meios públicos

CSMA

Consideremos o cenário onde o PC-A quer enviar um pacote para a rede e, em simultâneo, o PC-B envia outro. **Pode haver colisões!**
Para prevenir colisões existe o mecanismo CSMA/CD

CSMA/CD → faz com que, antes de um pacote ser enviado, verifica se a ligação partilhada está ou não a ser utilizada por outro terminal, bem como verifica se os dados que quer enviar já não se encontram a navegar pelo meio

-> Número de faixas horárias de atraso antes da n-ésima tentativa é uma variável aleatória uniformemente distribuída no terminal, (caso ~~este~~ o terminal para o qual deseja enviar um pacote esteja ocupado, o pacote terá de aguardar um tempo aleatório (**algoritmo de recuo binário exponencial truncado**) e depois enviar

$$0 < R < 2^K, \text{ com } K = \min(n, 10)$$

DURAÇÃO do SLOT → 64 bytes = 512 bits = 51,2 µs (10 Mbps)

exemplo:
- n=1 -> R=0 ou 1 (0 ou 51,2 µs)
- n=2 -> R=0, 1, 2 ou 3 (0; 51,2; 102,4 ou 153,6 µs)
  ...
- n>10

- nº máximo de RETRIES = (16)