Redes de Computadores I

Na aula anterior

- Simulando uma rede 802.11

Na aula de hoje

- Protocolo ARP
- Wireshark

Protocolo ARP

- Vimos que tanto os protocolos Ethernet quanto o WiFi (802.11) utilizam endereços MAC
- Algumas classificações portanto colocam os endereços MAC como parte de uma subcamada própria chamada de “subcamada MAC”

Protocolo ARP

- Na camada acima (“Rede”) vimos que são usados endereços IPs. Então algo precisa interligar endereços IPs e endereços MAC
- Essa interligação é feita por um protocolo chamado de ARP (Address Resolution Protocol)

Protocolo ARP

- Basicamente ele armazena uma tabela contento de um lado endereços IPs e de outro endereços MAC

IP	MAC
192.168.0.1	A6:B4:C2:42:31:14
192.168.0.2	B9:C1:A1:88:31:42
10.10.0.1	A6:C2:A1:89:22:D3
...	...

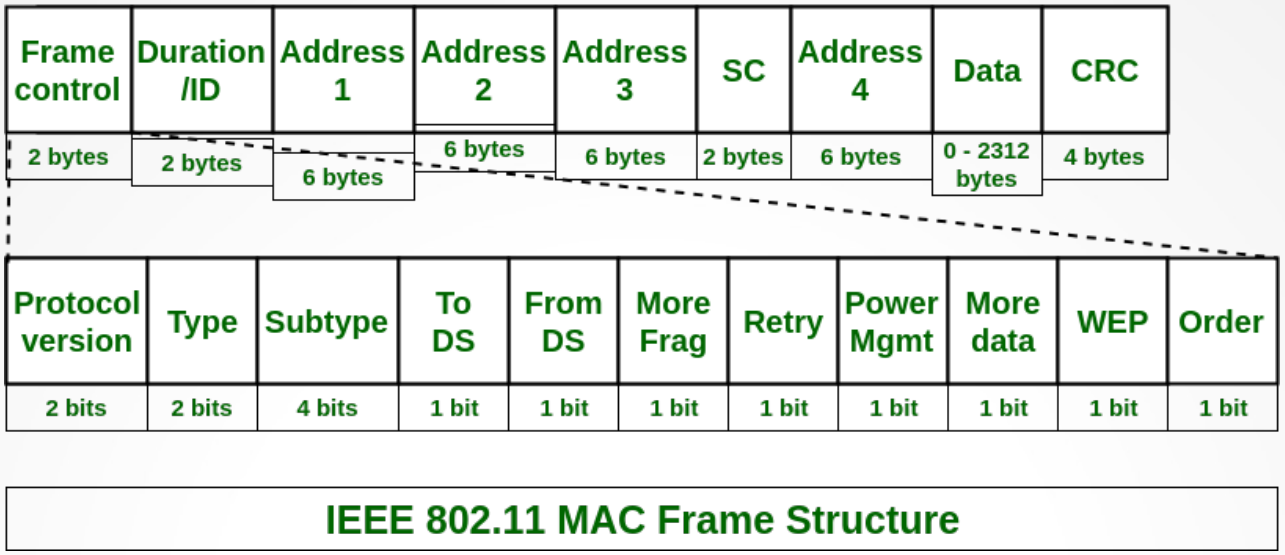
Visualizando informações ARP

- No Windows / Packet Tracer:
  - Visualizar meu endereço ARP

    ipconfig
  - Visualizando minha tabela ARP

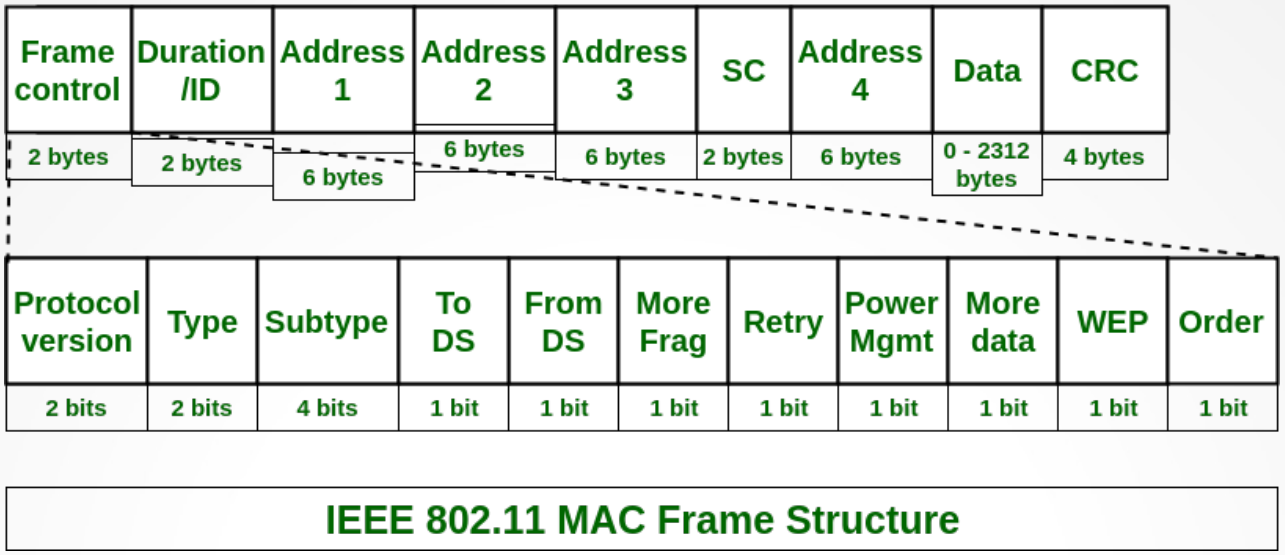
    arp -a

802.11 frame



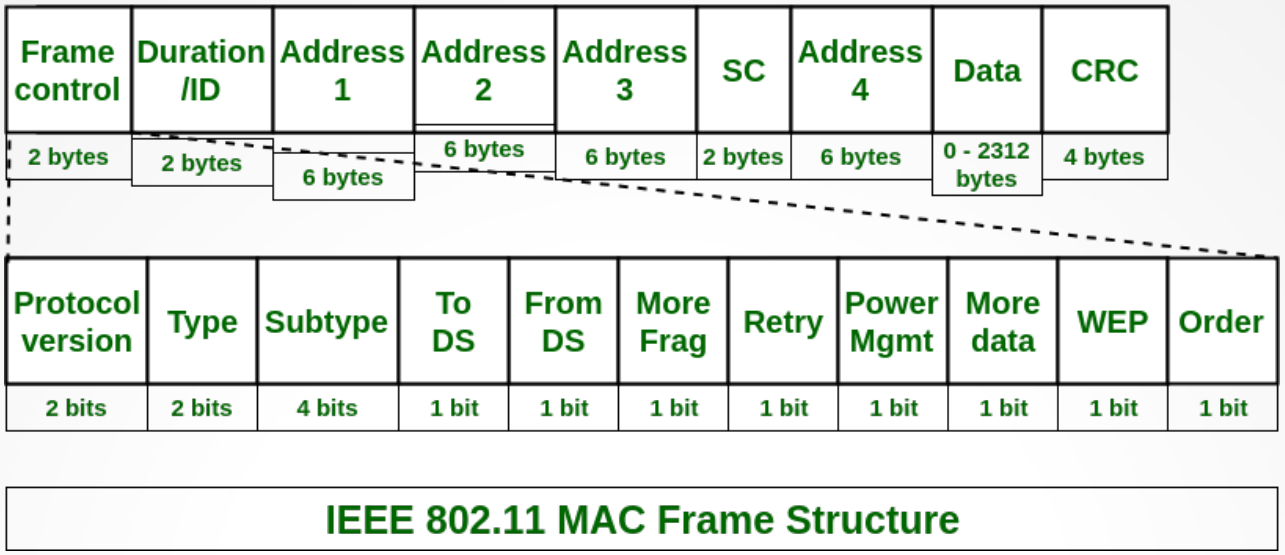
- Framecontrol: além disso existem 7 bits
- To DS / From DS → Sistema de comunicação entre access points
- More frag → Se ele é parte de um conjunto
- Retry → Se é um reenvio

802.11 frame



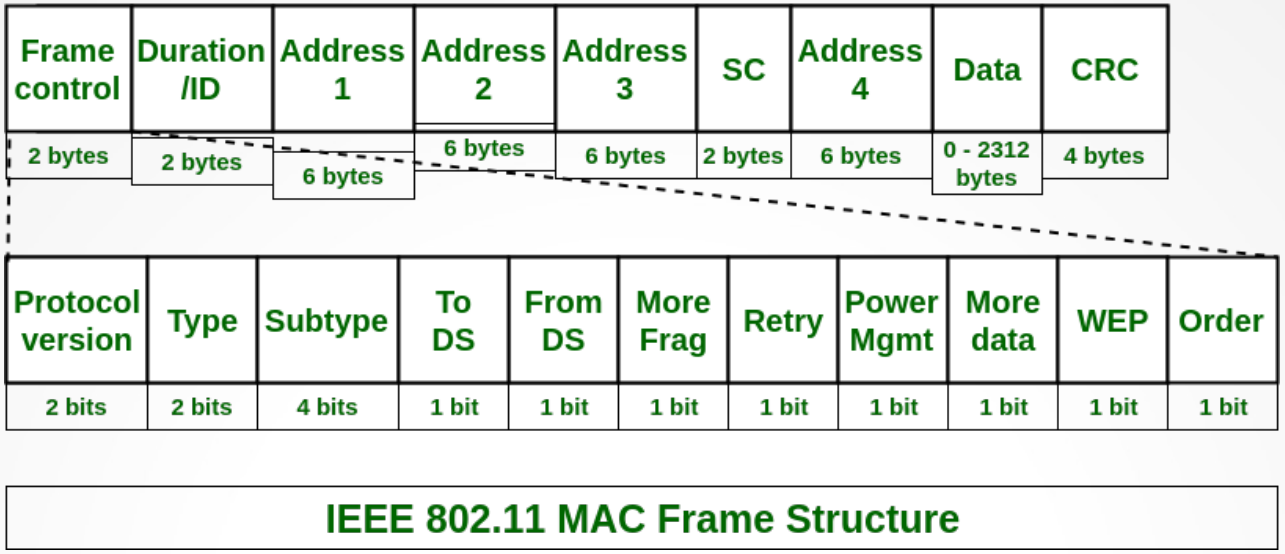
- Framecontrol: além disso existem 8 bits
- To DS / From DS → Sistema de comunicação entre access points
- More frag → Se ele é parte de um conjunto
- Retry → Se é um reenvio

802.11 frame



- Economia de energia → Se a estação vai entrar em economia de energia após o envio
- More data → Se após aquele frame existirão outros do mesmo conjunto (ou aquele é o último?)
- WEP → Se o mecanismo de segurança é o WEP
- Order → Se for 1 a ordem de recebimento deve ser obedecida

802.11 frame



- Duração → Tempo necessário para o envio
- Endereços 1 à 4 → Um mesmo frame pode ser enviado para até 3 destinatários ao mesmo tempo
- SC → Sequence Control: Identificador da ordem dos quadros
- Data → Dados em si
- CRC → Controle de erros

Mecanismos de segurança

- Principais mecanismos
  - WEP → Mecanismo original do WiFi. É melhor do que não usar nenhuma segurança mas é desaconselhado hoje
  - WAP → Substituto do WEP mas também considerado inseguro hoje
  - WAP2 → Versão melhorada do WAP. É o mínimo nível de segurança aceitável hoje

Modos do WPA2

- Pessoal (utiliza uma chave compartilhada)
  - Mais fácil de configurar
  - Menos seguro
- Modo ‘enterprise’
  - Mais difícil de configurar: requer um servidor de autenticação
  - Mais seguro

SSID

- Sigla para Service Set Identifier
- É basicamente o nome da rede que aparece aos usuários
- Pode ser configurado para ficar oculto
  - Nesse modo o cliente é que tem que informar que quer começar a se comunicar (o access point fica “esperando” um pedido)

SSID oculto?

- Vantagens
  - Usuários “comuns” não veem a rede
  - Afasta curiosos sem conhecimento técnico
- Desvantagens
  - Softwares específicos podem detectar a comunicação, afinal ela está no ar
  - Hackers podem se sentir desafios “Por que ocultaram essa rede?”
  - Pode gerar uma falsa sensação de segurança

Referências

- Conteúdo
- https://www.cbtnuggets.com/blog/technology/networking/what-is-ethernet-frame-format
- https://embarcados.com.br/a-evolucao-do-protocolo-wi-fi-ieee-802-11/
- https://www.geeksforgeeks.org/ieee-802-11-mac-frame/
- https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ssid
-
  - Amaral et al. Redes de Computadores I – Aula 7. Disponível em: https://proedu.rnp.br/handle/123456789/623
  - https://pt.wikipedia.org/wiki/Paridade_(telecomunica%C3%A7%C3%B5es)
- Imagens (exceto slides 4 e 18)
  - Amaral et al. Redes de Computadores I – Aula 7. Disponível em: https://proedu.rnp.br/handle/123456789/623