PROTOCOLOS FUNDAMENTAIS INTERNET

AULA 4 ARP (address resolution Protocol)

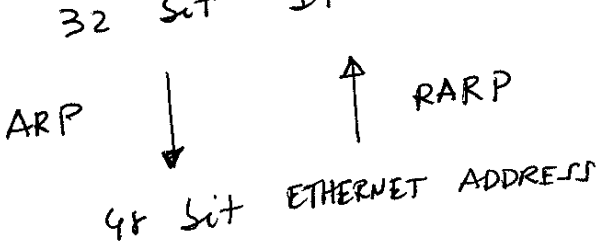
Problema: IP addresses apenas fazem sentido nos IP datagramas — são endereços virtuais

O data link layer precisa de ter endereços reais — os endereços das placas de interface

No caso de rede ethernet é necessário conhecer o endereço da placa de rede — 48 bits que identificam univocamente a placa de rede

ARP (RARP) — faz o mapeamento entre endereços IP e endereços no data link layer

exemplo (ethernet)



exemplo: ftp 10.20.23.29

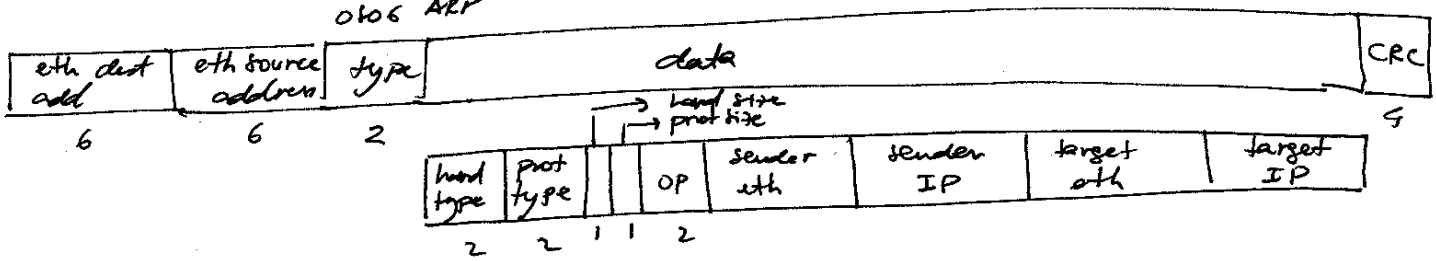
1. who has 10.20.23.29 ? (ARP)
2. arp reply 10.20.23.29 is at 0:0:c0:c2:9B:26 (ARP)
3. 10.20.23.128:1030 > 10.20.23.29:21 (IP/TCP)

ARP CACHE

arp -a — todos os computadores mantem um cache (tabela) com os endereços ethernet já conhecidos

ARP packet (formato) pag 56 stevens

8035 RARP
0806 ARP



eth dest add : FF:FF:FF:FF:FF:FF BROADCAST
(who_has)

hardware type - tipo de hardware (para ethernet = 0001)
protocol type - protocolo a mapear (para IP 0x8000)
hardware address size (para ethernet 6 bytes)
protocol address size (para IP 4 bytes)
Operation ARP request 1 ARP reply 2 RARP request 3 RARP reply 4
sender ethernet
sender IP
target ethernet (para broadcast ff:ff:ff:ff:ff:ff)
target IP

EXEMPLO 1

arp -a (verificar que a tabela de cache não contem o
-d(elete) endereço)

telnet 10.20.23.141 discard

(server discard deita fora tudo o que recebe ...)

tcp dump -e (nosso computador)

tcp dump -e host 10.20.23.141
(captura apenas tráfego de / para este computador)

(reparar no tempo de resposta)

EXEMPLO 2 (non-existent host)

arp -a
date; telnet 10.20.22.24 ; date

tcp dump -e host 10.20.22.24

1 arp who-has 0 seg
2 arp who-has 5 segs depois
3 arp who-has 24 seg depois

arp -a (incomplete entry)

PROXY ARP — routers respondem utilizando a sua tabela de cache

GRATUITIOUS ARP — um computador quando "arranca" faz um broadcast ARP com o seu próprio endereço internet (IP) se alguem responder (com o endereço ethernet) alguem estar a usar o endereço IP!