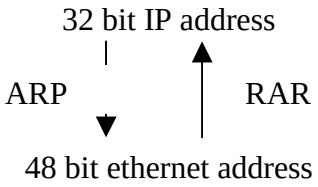
LAB01

Protocolos TCP/IP. Utilização de programas de captura de dados

Neste laboratório ficamos familiarizados com os protocolos fundamentais utilizados numa rede local e na Internet, bem como com programas de captura de dados.

1. Protocolo ARP

Os protocolos ARP (Address Resolution Protocol) e o seu inverso RARP (Reverse Address Resolution Protocol) fazem o mapeamento entre endereços IP e endereços na camada de ligação, os endereços ethernet:



a) olha para a tabela de cache do PC

```
#arp -a
```

Que é que podes concluir?

_____

_____

b) corre o programa de captura de dados tcpdump e captura apenas o tráfego de/para o PC 10.11.160.1

```
#apt-get install tcpdump
#tcpdump -e host 10.11.160.1
```

b) limpa na tabela de cache de endereços MAC esta entrada:

```
#arp -d 10.11.160.1
```

Verifica com o comando anterior que a tabela ficou vazia (ou incompleta) para este IP

d) faz ping a este PC

```
#ping 10.11.160.1
```

Compara o tempo de resposta do primeiro echo relativamente aos seguintes. Que podes concluir? Porquê este comportamento? A captura de dados do tcpdump diz porquê...

_____

_____

e) faz agora ping a um host que não existe

```
#ping 10.11.160.254
```

Consulta a tabela de cache novamente

```
#arp -a
```

Que é que podes concluir da consulta da tabela?

_____

_____

f) Coloca uma entrada fixa na tabela de cache de ARP `/etc/ethers`

```
#echo "10.11.160.55 11:22:33:AA:BB:CC" > /etc/ethers
#arp –f /etc/ethers
```

Consulta a tabela de cache novamente. Que é que podes concluir da consulta da tabela?

_____

_____

Qual é a importância de um PC, um switch ou um router trabalharem com tabelas fixas de endereços ethernet?

_____

_____

2. Protocolos IP e ICMP

Protocolo IP — protocolo fundamental da Internet responsável pelo encaminhamento de todos os dados

Protocolo ICMP — protocolo utilizado para comunicar situações de erro deterministicas na rede, bem como oferecer outra informação (exemplo routing) sobre a rede

a) num terminal de texto (xterm) corre o programa ethereal

```
#apt-get install ethereal
#ethereal &
```

b) configura o filtro de captura (substitui x pelo nº do teu PC)

```
Capture > Start... > Capture Filter: host 10.11.160.x
```

c) faz ping ao PC 10.10.23.29, enviando 3000 bytes de dados (vai haver fragmentação!)

```
#ping -c1 -s3000 10.10.23.29
```

Estuda todos os campos do protocolo IP

- qual o tipo de serviço?

_____

- qual o comprimento total dos 3 pacotes IP?

_____

- qual o offset no primeiro fragmento?_____(em bytes)

- qual o offset no segundo fragmento?_____ (em bytes)

- qual o offset no terceiro fragmento?_____(em bytes)

e) estuda todos os campos do protocolo ICMP

- qual o tipo e o código para "echo request"?

_____

- qual o tipo e o código para "echo reply"?

_____

- qual o tipo e o código para "host unreachable"? (Sugestão: faz ping a um host que não existe por exemplo 10.10.23.254)

_____

3. Protocolo TCP

O protocolo TCP oferece uma ligação segura para transmitir um fluxo de dados

a) corre numa shell (xterm) o programa ethereal e captura o tráfego de/para o teu PC (substitui x pelo nº do teu PC)

```
Capture > Start... > Capture Filter : host 10.11.160.x and tcp
```

b) noutra shell faz telnet para o host 10.10.23.29 e interrompe a ligação imediatamente a seguir ao seu estabelecimento:

```
#telnet 10.10.23.29
^C (Ctrl C)
```

c) estuda o handshake durante o estabelecimento da ligação

- quantos pacotes são necessário para estabelecer a ligação?

_____

- faz um diagrama temporal (nas costas do guião) pondo em evidência os sequence numbers e as flags envolvidas

d) estuda o handshake da terminação da sequência

- quantos pacotes são necessários para terminar a ligação?

_____

e) completa o diagrama temporal (nas costas do guião) pondo em evidência os sequence numbers e as flags envolvidas

f) corre novamente o programa ethereal

```
#ethereal &
```

g) configura o filtro de captura (substitui x pelo nº do teu PC)

```
Capture > Start... > Capture Filter : host 10.11.160.x
```

h) noutra shell faz telnet para o host 10.10.23.29 porta 9 (discard)

```
#telnet 10.10.23.29 9
```

i) com o output do programa ethereal responde às seguintes questões, analisando o 2º pacote que estabelece a ligação:

- Qual o número do porto source?_____
- Qual o número do porto destino?_____
- Qual o sequence number ?_____
- Qual o acknowledgment number ?_____
- Qual o comprimento (em bytes) do cabeçalho?_____
- Qual é o tamanho da janela?_____
- Quais são as opções utilizadas?_____
- Porquê o MSS é de 1460 bytes?_____

4. Programa traceroute

a) numa shell corre o programa ethereal com o filtro de captura host 10.11.160.x (substitui x pelo teu IP)

```
#ethereal &
Capture > Start... > Capture Filter : host 10.11.160.x
```

b) corre o programa traceroute

```
#traceroute –q 1 193.136.224.34
```

c) estuda os campos do cabeçalho IP, UDP e ICMP

- Qual o TTL do 1º pacote?_____
- Qual o TTL do 2º pacote?_____

d) Porque é que há pacotes ICMP enviados de volta pelos routers que se encontram no caminho para o destino?

_____
_____