

Tarefa 1.3.- Wireshark e Ethernet. Ping. Introducción a Packet Tracer.**A) Wireshark e Ethernet. Ping**

O comando **ping** sirve para comprobar se temos conexión desde o equipo no que se executa o comando ata un equipo remoto, que se pode identificar pola súa IP ou pola súa URL.

Podes probar desde o teu equipo, a facer un “ping lpdoteuRouter” (no meu caso 10.200.10.4):

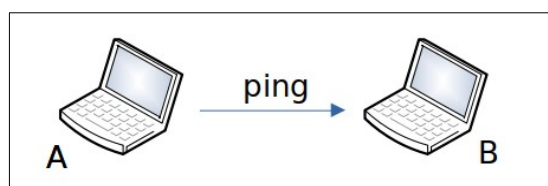
```
onacho@info104:~$ ping 10.200.10.4
PING 10.200.10.4 (10.200.10.4) 56(84) bytes of data.
64 bytes from 10.200.10.4: icmp_seq=1 ttl=64 time=0.119 ms
64 bytes from 10.200.10.4: icmp_seq=2 ttl=64 time=0.066 ms
64 bytes from 10.200.10.4: icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from 10.200.10.4: icmp_seq=4 ttl=64 time=0.064 ms
^C
--- 10.200.10.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.064/0.078/0.119/0.023 ms
```

Ou facer ping a unha dirección URL: www.google.es

```
onacho@info104:~$ ping www.google.es
PING www.google.es (142.250.178.163) 56(84) bytes of data.
64 bytes from mad41s08-in-f3.1e100.net (142.250.178.163): icmp_seq=1 ttl=116 time=10.4 ms
64 bytes from mad41s08-in-f3.1e100.net (142.250.178.163): icmp_seq=2 ttl=116 time=11.0 ms
64 bytes from mad41s08-in-f3.1e100.net (142.250.178.163): icmp_seq=3 ttl=116 time=10.0 ms
64 bytes from mad41s08-in-f3.1e100.net (142.250.178.163): icmp_seq=4 ttl=116 time=10.3 ms
^C
--- www.google.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 10.021/10.414/10.959/0.344 ms
onacho@info104:~$
```

Se o destino recibe o ping e está configurado para responder obtemos resposta, sabendo que temos conexión ata ese equipo.

Wireshark. Executa o wireshark e abre o ficheiro **exemploCapturaTramas.cap**, que mostra unha captura cando un equipo A fai un “ping” a un equipo B, obtendo resposta:



1. Indica o tamaño das 8 tramas en bytes.
2. ¿Son todas tramas Ethernet II?
3. Busca en internet como sería o preámbulo (7 bytes) e o byte delimitador de comezo de trama (FSD). Fíxate que ese preámbulo xa non é mostrado co Wireshark
4. Completa a seguinte táboa seguinte indicando para cada unha das 8 tramas do ficheiro:

Trama número	Tamaño en bytes	MAC orixe	MAC destino	Tipo (Hexadecimal)	Tamaño en bytes dos datos	IP orixe se existe	IP destino se existe
1							
2							
3							
4							
5							
6							
7							
8							

5.- As 2 primeiras tramas e as 2 últimas son tramas do protocolo ARP. ¿Para que se emprega ese protocolo?

B) Packet Tracer

Empregamos Packet Tracer de CISCO como ferramenta de simulación. Para comezar empregaremos os recursos que nos ofrece a páxina de CISCO <https://skillsforall.com/catalog>. Podes comprobar o Catálogo dos cursos que se ofrecen. Por agora centrarémonos no de Packet Tracer

Terás que:

- Crear un usuario nesa plataforma
- Matricularse no curso **Introducción a Cisco Packet Tracer** (no cal descargarás e instalarás Packet Tracer)
- Mostrar un **pantallazo** onde se vexa o teu usuario co curso rematado. (lembra que debes mostrar no pantallazo parte do teu escritorio).

A continuación matricúlate no curso **Exploring Networking with Cisco Packet Tracer**. Deberás facer a primeira actividade (**Set Up Your Small Office Network**), e mostrar un **pantallazo** coa rede da oficina funcionando (lembra que debes mostrar no pantallazo parte do teu escritorio).