Nombre	Acción
Mi equipo	host 192.168.0.1
Desde mi equipo	src host 192.168.0.1
Para mi equipo	dst host 192.168.0.1
CiudadWireless	host www.ciudadwireless.com
NO www.xunta.es	! host www.xunta.es
Eth. PC1	ether host 00:30:da:ed:43:ad
Eth. origen PC1	ether src host 00:30:da:ed:43:ad
Eth. destino PC1	ether dst host 00:30:da:ed:43:ad
Eth. PC2	ether host 00:00:00:00:00:01
Eth. Mio ↔ Router	ether host 00:30:da:ed:43:ad && ether host 00:11:d8:12:56:c4
Broadcast	ether broadcast
ARP	arp o ether proto \arp (en caso de hacerlo en línea de comando con tcpdump hay que poner ether proto \\arp para *escapar* la \ que es un símbolo especial
NO ARP	! arp
ICMP	icmp o ip proto \icmp
Puerto 80	port 80
Destino Puerto 80	dst port 80
Origen Puerto 53	src port 53
NO TCP 80	! tcp port 80
UDP 53	udp port 53
TCP	tcp
UDP	udp
Red local	net 192.168.0.0
Red Priv Clase C	net 192.168/16 <-- define una superred que hace referencia a todas las redes de clase C
Web www.edu.xunta.gal	host www.edu.xunta.gal && tcp port 80
https www.edu.xunta.gal	host www.edu.xunta.gal && tcp port 443

TTL < 128	ip[8] < 128
ICMP Echo Request	icmp[0] = 8 o icmp[0]=icmp-echo
ICMP Tiempo Excedido	icmp[0] = 11 o icmp[0]=icmp-timxceed
ICMP Echo	icmp[0]=icmp-echo || icmp[0]=icmp-echoreply
Ping Yo ↔ PC1	(host 192.168.0.1 && host 192.168.0.102) && (icmp[0]=icmp-echo || icmp[0]=icmp-echoreply)
UDP Bien Conocidos	udp[0:2] < 1024 o udp src portrange 0-1023
TCP sólo SYN	tcp[13] = 2
TCP SYN	tcp[13] & 0x02 = 2
NO Fragmentación	ip[6] & 0x40 != 0