

syntaxe :

tcpdump options expression

options

-a	essaie de convertir les adresses en noms
-c	exit après réception d'un certain nbre de paquets
-d	affiche le code compilé des paquets en clair et stop
-dd	affiche en fragment de programme C
-ddd	affiche le code en nbres décimaux
-e	affiche l'entête de niveau 2 à chaque ligne
-f	affiche les adresses internet étrangères en numérique plutôt qu'en symbolique
-F	utilise un fichier en entrée pour le filtre
-i	écoute sur l'interface précisée
-l	bufféris la sortie standard
-n	ne convertit pas les adresses en noms
-N	n'affiche pas la qualification des noms de domaine sur les noms d'hosts (ex : nic au lieu de nic.ddn.mil)
-O	ne lance pas le code optimiseur de correspondance de paquets
-p	ne met pas l'interface en mode promiscuous (elle peut l'être pour d'autres raisons)
-q	quick : affiche moins d'infos sur les protocoles
-r	lit les paquets d'un fichier qui a été créé avec l'option -w
-s	définit la longueur d'octets à capter
-T	force les paquets sélectionnés par « expression » à être interprétés
-S	affiche les N° de séquence tcp en absolu plutôt qu'en relatif
-t	n'affiche pas de timestamp
-tt	affiche un timestamp non formaté
-v	verbose output (ex : affiche ttl et type de service dans IP)
-vv	encore plus d'infos
-w	écrit les paquets dans un fichier
-x	affiche tous les paquets en hexa

expression

définit le filtre d'affichage des paquets

si non précisé, tous les paquets sont affichés

l'expression consiste en une ou plusieurs primitives

une primitive consiste en un ou plusieurs qualificatifs suivi d'un identificateur « id » (nom ou nbre)

il y a 3 sortes de qualificatifs :

type	les qualificatifs indiquent à quoi le id se réfère (ex : host, net ou port)(par défaut, c'est host)
dir	les qualificatifs indiquent une direction particulière du et/ou vers l'id possibles : src, dst (par défaut : src and dst) ex : src machin
proto	les qualificatifs filtrent un protocole particulier possibles : ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopld, tcp, udp ex : arp net 128.3, ou tcp port 21

primitives possibles :

dst host xxx (xxx est un host, nom ou adr IP)
src host xxx
host xxx
ether dst xxx (xxx est une adresse ethernet)
ether src xxx
ether host xxx
gateway xxx
dst net xxx (xxx est un nom ou une adresse de réseau)
src net xxx
net xxx
net xxx netmask yyy
net xxx/yyy (xxx est un netmask, yyy est une longueur en bits)
dst port xxx
src port xxx
port xxx
les xxx (xxx est une longueur de paquet)
greather xxx
ip proto xxx (xxx=un nbre ou un nom : \icmp, \igrp, \udp, nd ou \tcp)
ether broadcast
ip broadcast
ether multicast
ip multicast
ether proto xxx (xxx= \ip, \arp ou \rarp)
decnet src xxx (xxx est un host)
decnet dst xxx

les primitives peuvent être combinées avec not, and, or

exemples :

tcpdump host sunday (sunday est un nom de host)

tcpdump ip host sunday and not helios (tous les paquets entre sunday et un autre, sauf helios)

exemples de sorties :

arp who has csam tell rtsg	rtsg a envoyé une requête arp demandant l'adresse ethernet de csam
arp reply csam is-at CSAM	csam a répondu son adresse (adr ethernet en minuscules, adr ip en majuscule)

avec tcpdump -n cela donne

arp who has 128.3.254.6 tell 128.3.254.68
arp reply 128.3.254.6 is-at 02 :07 :01 :00 :01 :c4

format général des sorties **tcp** :

src > dst : flags data-segno ack window urgent options