

TCPDUMP/WINDUMP OPTIONS CHART

By Mark E. Donaldson

Syntax	<pre>windump [-aBdDeflnNOPqRStvxX] [-c count] [-F file] [-i interface] [-m module] [-r file] [-s snaplen] [-T type] [-w file] [-E algo:secret] [expression]</pre>
Option	Description
-a	Attempt to convert network and broadcast addresses to names.
-c	Exit after receiving count packets.
-d	Dump the compiled packet-matching code in a human readable form to standard output and stop.
-dd	Dump packet-matching code as a C program fragment.
-ddd	Dump packet-matching code as decimal numbers (preceded with a count).
-e	Print the link-level header on each dump line.
-E	Use algo:secret for decrypting IPsec ESP packets. Algorithms may be des-cbc, 3des-cbc, blowfish-cbc, rc3-cbc, cast128-cbc, or none. The default is des-cbc. The ability to decrypt packets is only present if tcpdump was compiled with cryptography enabled. secret the ascii text for ESP secret key. We cannot take arbitrary binary value at this moment. The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this option with truly `secret' key is discouraged. By presenting IPsec secret key onto command line you make it visible to others, via ps(1) and other occasions.
-f	Print `foreign' internet addresses numerically rather than symbolically (this option is intended to get around serious brain damage in Sun's yp server --- usually it hangs forever translating non-local internet numbers).
-F	Use file as input for the filter expression. An additional expression given on the command line is ignored.
-i	Listen on interface. If unspecified, tcpdump searches the system interface list for the lowest numbered, configured up interface (excluding loopback). Ties are broken by choosing the earliest match. In Windows interface can be the name of the adapter, or its number (the one reported by the -D flag). On Linux systems with 2.2 or later kernels, an interface argument of ``any" can be used to capture packets from all interfaces. Note that captures on the ``any" device will not be done in promiscuous mode.
-l	Make stdout line buffered. Useful if you want to see the data while capturing it. E.g., ``tcpdump -l tee dat" or ``tcpdump -l > dat & tail -f dat".
-n	Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.
-N	Don't print domain name qualification of host names. E.g., if you give this flag then tcpdump will print ``nic" instead of ``nic.ddn.mil".
-m	Load SMI MIB module definitions from file module. This option can be used several times to load several MIB modules into tcpdump.
-O	Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer.
-p	Don't put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, ``-p' cannot be used as an abbreviation for `ether host {local-hw-addr} or ether broadcast'.
-q	Quick (quiet?) output. Print less protocol information so output lines are shorter.
-r	Read packets from file (which was created with the -w option). Standard input is used if file is ``-".
-s	Snarf snaplen bytes of data from each packet rather than the default of 68 (with SunOS's NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with ``[[proto]", where proto is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit snaplen to the smallest number that will capture the protocol information you're interested in. Setting snaplen to 0 means use the required length to catch whole packets.

-T	Force packets selected by "expression" to be interpreted the specified type. Currently known types are cnfp (Cisco NetFlow protocol), rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), snmp (Simple Network Management Protocol), vat (Visual Audio Tool), and wb (distributed White Board).
-R	Assume ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified, tcpdump will not print replay prevention field. Since there is no protocol version field in ESP/AH specification, tcpdump cannot deduce the version of ESP/AH protocol.
-S	Print absolute, rather than relative, TCP sequence numbers.
-t	Don't print a timestamp on each dump line.
-tt	Print an unformatted timestamp on each dump line.
-v	(Slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.
-vv	Even more verbose output. For example, additional fields are printed from NFS reply packets.
-vvv	Even more verbose output. For example, telnet SB ... SE options are printed in full. With -X telnet options are printed in hex as well.
-w	Write the raw packets to file rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if file is ``-".
-x	Print each packet (minus its link level header) in hex. The smaller of the entire packet or snaplen bytes will be printed.
-X	When printing hex, print ascii too. Thus if -x is also set, the packet is printed in hex/ascii. This is very handy for analyzing new protocols. Even if -x is not also set, some parts of some packets may be printed in hex/ascii.
-B	Set driver's buffer size to size in Kilobytes. The default buffer size is 1 megabyte (i.e. 1000). If there is any loss of packets during the capture, the suggestion is to increase the kernel buffer size by means of this switch, since the dimension of the driver's buffer influences heavily the capture performance.
-D	Print the list of the interface cards available on the system. For every network adapter, this switch returns the number, the name and the description. The user can start the capture on a specific adapter typing 'Windump -i name' or 'Windump -i number'. If the machine has more than one network adapter, Windump without parameters starts on the first network interface available on the system.
expression	selects which packets will be dumped. If no expression is given, all packets on the net will be dumped. Otherwise, only packets for which expression is `true' will be dumped. The expression consists of one or more primitives. Primitives usually consist of an id (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier: type: dir: proto: