# tcpdump syntax as of August 29, 2021

Mahyar TaDini.net
Mahyar@TaDini.net
Github.com/mahyarx
Linkedin.com/in/mahyartajdini
TaDini.net

**-A** — Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.

**-b** — Print the AS number in BGP packets in ASDOT notation rather than ASPLAIN notation.

**-B buffer_size**
or
**--buffer-size=buffer_size** — Set the operating system capture buffer size to buffer_size, in units of KiB (1024 bytes).

**-c count** — Exit after receiving count packets.

**-C file_size** — Before writing a raw packet to a savefile, check whether the file is currently larger than this and, if so, close the current savefile and open a new one. Savefiles after the first savefile will have the name specified with the -w flag, with a number after it, starting at 1 and continuing upward. The default unit of file size is millions of bytes (1,000,000 bytes, not 1,048,576 bytes).

By adding a suffix of k/K, m/M or g/G to the value, the unit can be changed to 1024 ( KiB), 1,048,576 (MiB), or 1,073,741,824 (GiB) respectively.

**-d** — Dump the compiled packet-matching code in a human readable form to standard output and stop.

Please mind that although code compilation is always OS,T-specific, typically it is impossible (and unnecessary) to specify which DLT to use for the dump because tcpdump uses either the DLT of the input interface specified by the -i flag, or the default DLT of the network interface specified with -i, or the particular DLT of the network interface specified with -y and -i respectively. In these cases the dump shows the same exact code that would filter the input file or the network interface without -d.

However, when neither -r nor -i is specified, specifying -d prevents tcpdump from guessing a suitable network interface (see -i and -y). In this case, -y defaults to DVB/PKS and can be set to another valid value manually with -y.

**-dd** — Dump packet-matching code as a C program fragment.

**-ddd** — Dump packet-matching code as decimal numbers (preceded with a count).

**-D**
or
**--list-interfaces** — Print the list of the network interfaces available on the system and on which tcpdump can capture packets. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is displayed. The interface name or the number can be supplied to the -i flag to specify an interface on which to capture.

This can be useful on systems that don't have a command to list them (e.g. Windows systems, or UNIX systems lacking /dev/dlpi -a); the number can be useful on Windows 2000 and later systems, where the interface name is a somewhat complex string.

The -D flag will not be supported if tcpdump was built with an older version of libpcap that lacks the pcap_findalldevs(3PCAP) function.

**-e** — Print the link-level header on each dump line. This can be used, for example, to print MAC layer addresses for protocols such as Ethernet and IEEE 802.11.

**-E** — Use spi@ipaddr algo:secret for decrypting IPsec ESP packets that are addressed to addr and contain Security Parameter Index value spi. This combination may be repeated with comma or newline separation.

Note that setting the secret for IPv4 ESP packets is supported at this time.

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 is the ASCII text for ESP secret key. If preceded by 0x, then a hex value will be read.

The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this option with a true 'secret' key is discouraged. By passing IPsec secret key on the command line all users may see it, other ones could see it if a dump is being made.

In addition to the above syntax, the syntax file name may be used to have tcpdump read the provided file in. The file is opened upon receiving the first ESP packet, so any special permissions that tcpdump may have been given should already have been given up.

**-f** — Print `foreign` IPv4 addresses numerically rather than symbolically (this option is intended to get around serious brain damage in Sun's NIS server — usually it hangs forever translating non-local internet numbers).

The test for `foreign` IPv4 addresses is done using the IPv4 address and netmask of the interface on which capture is being done. If that address or netmask are not available, either because the interface on which capture is being done has no address or netmask or because the capture is being done on the Linux "any" interface, which can capture on more than one interface, this option will not work correctly.

**-F file** — Use file as input for the filter expression. An additional expression given on the command line is ignored.

**-G rotate_seconds** — If specified, rotates the dump file specified with the -w option every rotate_seconds seconds. Savefiles will have the name specified by -w which should include a time format as defined by strftime(3). If no time format is specified, each new file will overwrite the previous file. If the generated filename is not unique, tcpdump will overwrite the pre-existing data, providing a time specification that is coarser than the capture period is therefore not advised.

If used in conjunction with the -C option, filenames will take the form of `file-count+`.

**-h**
or
**--help** — Print the tcpdump and libpcap version strings, print a usage message, and exit.

**--version** — Print the tcpdump and libpcap version strings and exit.

**-H** — Attempt to detect 802.11s draft mesh headers.

**-i interface**
or
**--interface=interface** — Listen. report the list of link-layer types, report the list of time stamp types, or report the results of compiling a filter expression on interface. If unspecified and if the -d flag is not given, tcpdump searches the system interface list for the lowest numbered, configured up interface (excluding loopback). which may turn out to be, for example, `eth0`.

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.

If the -D flag is supported, an interface number as printed by that flag can be used for the interface argument, if no interface on the system has that number as a name.

**-I**
or
**--monitor-mode** — Put the interface in "monitor mode". this is supported only on IEEE 802.3 Wi-Fi interfaces, and supported only on some operating systems.

Note that in monitor mode the adapter might disassociate from the network to which it's currently associated, and/or it may not be able to use any wireless networks with that adapter. This could prevent accessing files on a network server, or resolving host names or network addresses, if you are capturing in monitor mode and are not connected to another network with another adapter.

This flag will affect the output of the -L flag. If -I is specified, only those link-layer types available when not in monitor mode will be shown.

**--immediate-mode** — Capture in "immediate mode". In this mode, packets are delivered to tcpdump as soon as they arrive. rather than being buffered for efficiency. This is the default when printing packets rather than saving packets to a `savefile`" if the packets are being printed to a terminal rather than to a file or pipe.

**-j tstamp_type**
or
**--time-stamp-type=tstamp_type** — Set the time stamp type for the capture to tstamp_type. The names to use for the time stamp types are given in pcap-tstamp(7); not all types may be available, and not necessarily be valid for any given interface.

**-J**
or
**--list-time-stamp-types** — List the supported time stamp types for the interface and exit. If the time stamp type cannot be set for the interface, no time stamp types are listed.

**-k** — When capturing, set the time stamp precision for the capture to tstamp_precision. Note that availability of high precision time stamps (nanoseconds) and their actual accuracy is platform and hardware dependent. Also note that when writing captures made with nanosecond accuracy to files, only libpcap/tcpdump/dumpcap files support nanosecond resolution, and the file is written with a different magic number, to indicate that the time stamps are in seconds and nanoseconds; not all programs that read pcap savefiles will be able to read those captures.

**--time-stamp-precision=tstamp_precision**

When reading a savefile, convert time stamps to the precision specified by tmestamp_precision, and display them with that resolution. If the precision specified is less ( for example, nanosecond time stamps in the file, the conversion will lose precision.

The supported values for timestamp_precision are micro for microsecond resolution and nano for nanosecond resolution. The default is microsecond resolution.

**-m module** — Load SMI-MIB module definitions from file module. This option can be used several times to load several MIB modules into tcpdump.

**-M secret** — Use secret as a shared secret for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present.

**-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`.

**-O**
or
**--no-optimize** — Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer.

**-p**
or
**--no-promiscuous-mode** — Don't put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; conversely, this prevents it from being put in promiscuous mode. For a interface, this is usually an abbreviation for `either host (local-hw-addr) or either broadcast`.

**-q** — Quick (quiet?) output. Print less protocol information so output lines are shorter

**-r file** — Read packets from file (which was created with the -w option or by other tools that write pcap or pcapng files). Standard input is used if file is `-`.

**-R** — Assume ESP/AH packets to be in raw format. This is useful for interfaces that perform some or all of those checksum calculation in hardware; otherwise, all outgoing TCP checksums will be flagged as bad.

**-s snaplen**
or
**--snapshot-length=snaplen** — Snarf snaplen bytes of data from each packet rather than the default of 262144 bytes. 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. Note also that taking smaller snapshots will discard data from protocols above the transport layer, which loses information that may be important. NFS and AFS RPC packets, for example, are very large and much of the detail won't be available if a too-short snapshot length is selected.

If you need to reduce the snapshot size below the default, you should limit snaplen to the smallest number that will capture the protocol information you're interested in. Setting snaplen to 0 sets it to the default of 262144, for backwards compatibility with recent older versions of tcpdump.

**-S**
or
**--absolute-tcp-sequence-numbers** — Print absolute, rather than relative, TCP sequence numbers.

**-r file** — Read packets from file (which was created with the -w option or by other tools that write pcap or pcapng files). Standard input is used if file is `-`.

**-q** — Quick (quiet?) output. Print less protocol information so output lines are shorter

**-Q direction**
or
**--direction=direction** — Choose send/receive direction direction for which packets should be captured. Possible values are `in`, `out` and `inout`. Not available on all platforms.

**--print** — Print parsed packet output, even if the raw packets are being saved to a file with the -w flag.

**-t** — Don't print a timestamp on each dump line.

**-tt** — Print an absolute, microsecond or nanosecond resolution timestamp on each dump line. The default is microsecond resolution.

Print the timestamp, as seconds since January 1, 1970, 00:00:00, UTC, and fractions of a second since that time, on each dump line.

**-ttt** — Print a delta (microsecond or nanosecond resolution depending on the -tttttt flag, default is microsecond resolution) between current and previous line on each dump line. The default is microsecond resolution.

**-tttt** — Print a timestamp, as hours, minutes, seconds, and fractions of a second since midnight, preceded by the date, on each dump line.

**-ttttt** — Print a delta (microsecond or nanosecond resolution depending on the -tttttt flag, default is microsecond resolution) between current and first line on each dump line. The default is microsecond resolution.

**-T type** — Force packets selected by "expression" to be interpreted the specified type. Currently known types are aarp, ah, ahcp, ancp (Ancp Protocol) Distance Vector protocol, carp (Common Address Redundancy Protocol), cnfp (Cisco NetFlow protocol), domain (Domain Name Service), lmp (Link Management Protocol), pgm (Pragmatic General Multicast), pgm_zmtp1 (ZMTP/1.0 inside PGM/EPGM), ptp (Precision Time Protocol), radius (RADIUS), rpcap (BBDis Serialization Protocol), rpc (Remote Procedure Call), rtcp (Real-Time Applications control protocol), rtp (Real-Time Applications protocol), rtpevent (Real-Time Applications Protocol) payload, rtpcrypt (SCRM),RP, rtp (Trivial File Transfer Protocol), vat (Visual Audio Tool), vrrp (Virtual eXtensible Local Area Network), vxlan (Virtual eXtensible Local Area Network), wb ( distributed White Board) and zmtp1 (ZeroMQ Message Transport Protocol 1.0).

Note that the pgm type above affects UDP interpretation only, the native PGM is always recognised as IP protocol 113 regardless. UDP-encapsulated PGM is often called "EPGM" or "PGM/UDP".

Note that the pgm_zmtp1 type above affects interpretation of both native PGM and UDP at once. During the native PGM decoding the application data of an ODATA/RDATA packet would be decoded as a ZeroMQ datagram with ZMTP/1.0 frames. During the UDP decoding in addition to that any UDP packet would be treated as an encapsulated PGM packet.

**-u** — Print unbuffered NFS handles.

**-U**
or
**--packet-buffered** — If the -w option is not specified, or if it is specified but the --print flag is also specified, make the printed packet output `packet-buffered`; i.e., as the description of the contents of each packet is printed, it will be written to the standard output, and, on systems that do, it will be written to a terminal. being written only when the output buffer fills.

If the -w option is specified, make the saved raw packet output `packet-buffered`; i.e., as each packet is saved, it will be written to the output file, rather than being written only when the output buffer fills.

The -U flag will not be supported if tcpdump was built with an older version of libpcap that lacks the pcap_dump_flush(3PCAP) function.

**-v** — Verbose output. For example, in the default format, the IP packet time to live, IP fragmentation and 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, and SMB packets are fully decoded.

**-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 file** — 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 `-`

This output will be buffered if written to a file or pipe, so a program reading from the file or pipe may not see packets for an arbitrary amount of time after they are received. Use the -U flag to cause packets to be written as soon as they are received.

The MPHE type application/vnd.tcpdump.pcap has been registered with IANA for pcap files. The filename extension .pcap appears to be the most commonly used along with .cap and .dmp. Tcpdump itself doesn't check the extension when reading capture files and doesn't add an extension when writing them ( it uses magic numbers in the file header instead). However, many operating systems and applications will use the extension if it is present and adding one (e.g. .pcap) is recommended.

See pcap-savefile(5) for a description of the file format.

**-W filecount** — Used in conjunction with the -C option, this will limit the number of files created to the specified number, and begin creating files from the beginning, thus creating a 'rotating' buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly.

Used in conjunction with the -G option, this will limit the number of rotated dump files that get created, exiting with status 0 when reaching the limit.

If used in conjunction with both -C and -G, the -W option will currently be ignored, and will only affect the file name.

**-V file** — Read a list of filenames from file. Standard input is used if file is `-`.

**-v** — Verbose output. For example, in the default format, the IP packet time to live, IP fragmentation and 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.

When writing to a file with the -w option and at the same time not reading from a file with the -r option, report to stderr, once per second, the number of packets captured. In Solaris, FreeBSD and possibly other operating systems this periodic update currently can cause loss of captured packets on their way from the kernel to tcpdump.

**-x** — When parsing and printing, produce (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.

**-xx** — When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, including its link level header, in hex and ASCII.

**-X** — When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analyzing new protocols. In the current implementation this flag may have the same effect as -XX if the packet is truncated.

**-XX** — When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, including its link level header, in hex and ASCII.

**-y datalinktype**
or
**--linktype=datalinktype** — Set the data link type to use while capturing packets (see -L) or while compiling and dumping packet-matching code (see -d) to datalinktype.

**-z postrotate-command** — Used in conjunction with the -C or -G options, this will make tcpdump run "postrotate-command file " where file is the savefile being closed after each rotation. For example, if -W is also used, this will run the compress each savefile using gzip or bzip2.

Note that tcpdump will run the command in parallel to the capture, using the lowest priority so that this doesn't disturb the capture process.

And in case you would like to use a command that itself takes flags or different arguments, you can always write a shell script that will take the savefile name as the only argument, make the flags & arguments arrangements and execute the command that you want.

**-z** — Used in conjunction with the -C option, this will limit the number of files created to the specified number, and begin creating files from the beginning, thus creating a 'rotating' buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly.

Used in conjunction with the -G option, this will limit the number of rotated dump files that get created, exiting with status 0 when reaching the limit.

If used in conjunction with both -C and -G, the -W option will currently be ignored, and will only affect the file name.

**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.

For the expression syntax, see pcap-filter(7).

**-Z user**
or
**--relinquish-privileges=user** — If tcpdump is running as root, after opening the capture device or input savefile, but before opening any savefiles for output, change the user ID to user and the group ID to the primary group of user.

This behavior can also be enabled by default at compile time.