5.9.7 tcpdump Facts

TCPdump is a packet analyzer that runs in a command line utility. It allows the user to view TCP/IP and other packets as they are transmitted and received over on a computer's network. In this lesson, you will learn about:

- Common uses
- Options
- Expression examples

Common Uses

TCPdump prints the contents of network packets. It can read packets from a network interface card or a previously captured packet file. TCPdump can write packets to standard output or a file.

You can TCPdump to intercept and display the network traffic of another user or computer, including user credentials, the content of packets, and other unencrypted information.

Options

These are some of the many configuration options for TCPdump. For a complete list of options refer to the TCPdump MAN (manual) page.

Option	Description
-i any	Listen on all interfaces to check for traffic traffic.
-i eth0	Listen on the eth0 interface.
-D	Show the list of available interfaces.
-n	Don't resolve host names.
-nn	Don't resolve host names or port names.
-q	Be less verbose (more quiet) with your output.
-t	Create a timestamp output humans can read.
-tttt	Create a timestamp output that's maximally readable for humans.
-X	Show the packet's contents in both hex and ASCII.
-XX	Same as -X, but also shows the Ethernet header.
-v, -vv, -vvv	Increase the amount of packet information you get back.
-c	Only receive a certain number of packets and then stop.
-s	Define the snaplength (size) of the capture in bytes. Use -s0 to capture everything unless you are intentionally capturing less.
-S	Print absolute sequence numbers.
-e	Retrieve the Ethernet header.
-q	Show less protocol information.
-E	Decrypt IPsec traffic by providing an encryption key.

Expression Examples

Expressions allow you to filter traffic and find exactly what you need.

There are three main types of expression: type, dir, and proto.

- The type options are host, net (the network address), and port.
- Direction lets you insert the src (source) and dst (destination) commands.
- Protocol lets you designate tcp, udp, icmp, ah, and many more options.

Some examples of uses for TCPdump include the following:

Commands are case sensitive.

TCPdump Example	Description
tcpdump -D	Display the list of interfaces TCPdump can listen to.
tcpdump -n host 192.168.0.1	Capture any packets that list 192.168.0.1 as the source or destination host. Displays IP addresses and port numbers.
tcpdump -i eth0	Listen on interface eth0.
tcpdump -i any	Listen on any available interface.
tcpdump -n dst net 192.168.0.0/24	Capture any packets that list 192.168.0.0/24 as the destination network. Displays IP addresses and port numbers.
tcpdump -n src net 192.168.1.0/24	Capture any packets that list 192.168.1.0/24 as the source network. Displays IP addresses and port numbers.
tcpdump -n dst port 23	Capture any packets that list 23 as the destination port. Displays IP addresses and port numbers.
tcpdump -n "dst host 192.168.1.1 and (dst port 80 or dst port 443)"	Capture any packets that list 192.168.0.1 as the destination IP and 80 or 443as the destination port. Displays IP addresses and port numbers.