Tcpdump

Tcpdump

Stable: 09.10.2019 - 15:36 / Revision: 04.09.2019 - 07:33

Contents

1 Article purpose

This article provides the basic information needed to start using the Linux tool: **tcpdump**[1].

2 Introduction

The following table provides a brief description of the tool, as well as its availability depending on the software packages:

: this tool is either present (ready to use or to be activated), or can be integrated and activated on the software package.

: this tool is not present and cannot be integrated, or it is present but cannot be activated on the software package.

Tool			STM32MPU Embedded Software distribution			STM32MPU Embedded Software distribution for Android™		
Name	Category	Purpose	Starter Package	Developer Package	Distribution Package	Starter Package	Developer Package	Distribution Package
		tcpdump[1] is a common packet analyzer that runs under the						

Tool			STM32MPU Embedded Software distribution			STM32MPU Embedded Software distribution for Android™		
Name	Category	Purpose	Starter Package	Developer Package	Distribution Package	Starter Package	Developer Package	Distribution Package
tcpdump	Monitoring tools	command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is connected.	✓	✓	✓	✓	✓	✓

3 Installing the trace and debug tool on your target board

3.1 Using the STM32MPU Embedded Software distribution

tcpdump is installed by default and ready to be used with all STM32MPU Embedded Software Packages.

```
Board $> which tcpdump
/usr/sbin/tcpdump
```

tcpdump is integrated in weston image distribution through meta-st package: *meta-st/meta-st-openstlinux/recipes-st/packagegroups/packagegroup-framework-tools.bb*.

```
RDEPENDS_packagegroup-framework-tools-network = "\
   tcpdump          \
   iptables         \
   ...
```

3.2 Using the STM32MPU Embedded Software distribution for Android™

tcpdump is installed by default (/system/xbin/tcpdump) and is ready to be used with all STM32MPU software packages for Android™, as soon as debug mode is enable (eng or userdebug build variants). Please see *external/tcpdump/Android.mk*.

```
Board $> which tcpdump
/system/xbin/tcpdump
```

4 Getting started

- Command line description

```
Board $> tcpdump --help
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
               [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
               [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
               [ -Q in|out|inout ]
```

```
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-
command ]
                [ -Z user ] [ expression ]
```

- Dump tcp traffic on eth0 interface (you can use *ip addr show* command to know the list of network interface available)

```
Board $> tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:55:33.107716 IP 10.48.2.165.ssh > 10.201.23.91.52308: Flags [P.], seq 4266254400:
4266254528, ack 3520172211, win 333, options [nop,nop,TS val 57572827 ecr 260374058],
length 128
10:55:33.108933 IP 10.201.23.91.52308 > 10.48.2.165.ssh: Flags [.], ack 128, win 1444,
options [nop,nop,TS val 260374095 ecr 57572827], length 0
...
```

5 To go further

Some usage examples[2].

6 References

- 1.01.1 http://www.tcpdump.org/
- http://www.thegeekstuff.com/2010/08/tcpdump-command-examples

- Useful external links

Document link	Document Type	Description
tcpdump manpage	Standard	linux.die.net
tcpdump (wikipedia.org)	Standard	wikipedia.org