# Capture packets using tcpdump

## Description

This article describes how to log packets using tcpdump.

## Installing tcpdump

Before starting, you need to install required packages. **Tcpdump** and **Libpcap**. These packages can be found attached to the article.

To install, you need to upload the packages to your **WCCLite** /tmp/ directory. You can achieve this by using **scp** or any other software that has scp compatibility, for example: WinSCP, PSCP, FileZilla.

We are going to upload using **scp.**

1. Navigate to the directory where **libpcap** is.
2. Open the command terminal in that directory.
3. Execute command: *scp libpcap_1.7.4-1_ar71xx.ipk root@192.168.1.1:/tmp/*
4. It will ask you for the password. Enter the default wcclite password - *wcclite*.

```
~$ scp libpcap_1.7.4-1_ar71xx.ipk root@192.168.71.130:/tmp/
root@192.168.71.130's password:
libpcap_1.7.4-1_ar71xx.ipk                    100%   82KB 844.5KB/s   00:00
```

1. Navigate to the directory where **tcpdump** is.
2. Open the command terminal in that directory.
3. Execute command: *scp tcpdump_4.9.2-1_ar71xx.ipk root@192.168.1.1:/tmp/*
4. It will ask you for the password. Enter the default wcclite password - *wcclite*.

```
$ scp tcpdump_4.9.2-1_ar71xx.ipk root@192.168.71.130:/tmp/
root@192.168.71.130's password:
tcpdump_4.9.2-1_ar71xx.ipk                    100%  305KB   1.0MB/s   00:00
~$
```

After uploading the packages, you need to install them.

1. Connect to the **WCCLite** using an ssh client. We recommend using *putty*
2. Execute command: *opkg install /tmp/libpcap_1.7.4-1_ar71xx.ipk* to install **libpcap**
3. If successful you will get this message.

```
root@wcc-lite0:~# opkg install /tmp/libpcap_1.7.4-1_ar71xx.ipk
Installing libpcap (1.7.4-1) to root...
Configuring libpcap.
root@wcc-lite0:~#
```

Now to install **tcpdump**:

1. Execute: *opkg install /tmp/tcpdump_4.9.2-1_ar71xx.ipk* to install **tcpdump.**
2. If successful you will get this message.

```
root@wcc-lite0:~# opkg install /tmp/tcpdump_4.9.2-1_ar71xx.ipk
Installing tcpdump (4.9.2-1) to root...
Configuring tcpdump.
root@wcc-lite0:~#
```

To check if everything installed correctly, execute this command: *tcpdump --v*

```
root@wcc-lite0:~# tcpdump --v
tcpdump version 4.9.2
libpcap version 1.7.4
root@wcc-lite0:~#
```

Now **Tcpdump** has been successfully installed.

## Running tcpdump

To run **tcpdump** you need to give it specific options. You can find all of them in the manual. Here are some of the more frequent ones:

| Switch | Syntax | Description |
|---|---|---|
| -i any | tcpdump -i any | Capture from all interfaces |
| -i eth0 | tcpdump -i eth0 | Capture from specific interface |
| -D | tcpdump -D | Show available interfaces |
| -w | tcpdump -i eth0 -w capture.pcap | Save capture to file (.pcap for reading it with *Wireshark* or other packet analysis tools) |
| -c | tcpdump -i eth0 -c 100 | Capture first 100 packets and exit |
| -n | tcpdump -n -i eth0 | Do not resolve host names |
| port | tcpdump -i eth0 port 2404 | Capture traffic from a defined port only |
| host | tcpdump host 192.168.1.100 | Capture packets from specific host |

After you write your specific command you execute it via the console.

Here is shown ***tcpdump -i wwan0 -n.*** This command shows all traffic that goes through the gsm interface.

```
root@wcc-lite0:~# tcpdump -i wwan0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wwan0, link-type RAW (Raw IP), capture size 262144 bytes
07:26:00.369477 IP 83.188.95.197.33258 > 193.12.150.64.53: 59154+ A? google.com.
 (28)
07:26:00.370480 IP 83.188.95.197.33258 > 212.247.152.64.53: 59154+ A? google.com
. (28)
07:26:00.507961 IP 0.0.0.0 > 0.0.0.0: truncated-udplength 0
07:26:00.508120 IP 212.247.152.64.53 > 83.188.95.197.33258: 59154 1/4/8 A 142.25
0.74.14 (292)
07:26:00.511667 IP 0.0.0.0 > 0.0.0.0: ICMP echo reply, id 0, seq 0, length 64
07:26:00.582936 IP 142.250.74.14 > 83.188.95.197: ICMP echo reply, id 16671, seq
 0, length 64
```

## Examples

| Command | Description |
|---|---|
| tcpdump -i eth0 -n port 2404 -c 1000 -s0 -w /var/log/2404.dmp | Capture packets that are on port 2404 that go through eth0 interface.Exit after first 1000 and save them to /var/log/2404.dmp file |
| tcpdump -i wwan0 -w /tmp/capture-%H.pcap -G 3600 -C 10000 | Capture packets that go through gsm interface and write a new file to /tmp/capture-<count>.pcap file every 3600 seconds. |
| tcpdump -i any -n port 2404 -w /tmp/capture-%H.pcap -G 3600 | Capture packets that are on port 2404 that go through all interfaces and save a new file to /tmp/capture-<count>.pcap every 3600 seconds. |

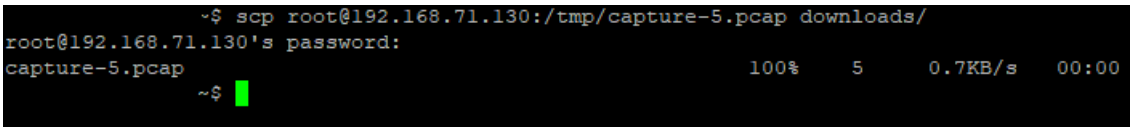
# Downloading packet files

If you save your **tcpdump** files, you need to download them from the **WCCLite.** This can be achieved by using **scp** or any software that has scp compatibility, for example: WinSCP, PSCP, FileZilla.

We are going to use **scp** to download the file.

1. Open the command terminal on your computer.
2. Execute command with the location of your *packet dump* file and directory where to save it. *scp root@192.168.1.1:/<dump directory>/<dump name>  <directory where to save it>*
3. It will ask for the **WCCLite** password. Enter the default password - *wcclite*.
4. If successful the file will appear in the determined location.

Example of the command.




# Files

1. PuTTy ssh software Download
2. WinSCP software Download
3. TCPDump manual
4. Libpcap Download
5. Tcpdump Download

---

Revision #12
★Created 30 July 2021 13:20:03 by Tautvilis
Updated 16 July 2024 14:32:20 by Gabriele