

tcpdump	nic name	3
		4

tcpdump nic name

```

tcpdump      nic name      .      4.99
nic name      .
RHEL9      4.99      OS

```

```

#!/bin/bash
#=====
=====
#
# FILE: dump.sh
# USAGE: dump.sh [-i interface] [tcpdump-parameters]
# DESCRIPTION: tcpdump on any interface and add the prefix [Interface:xy] in
front of the dump data.
# OPTIONS: same as tcpdump
# REQUIREMENTS: tcpdump, sed, ifconfig, kill, awk, grep, posix regex
matching
# BUGS: ---
# FIXED: - In 1.0 The parameter -w would not work without -i parameter as
multiple tcpdumps are started.
#       - In 1.1 VLAN's would not be shown if a single interface was
dumped.
# NOTES: ---
#       - 1.2 git initial
# AUTHOR: Sebastian Haas
# COMPANY: pharma mall
# VERSION: 1.2
# CREATED: 16.09.2014
# REVISION: 22.09.2014
#
#=====
=====

# When this exits, exit all background processes:
trap 'kill $(jobs -p) &> /dev/null && sleep 0.2 && echo ' EXIT
# Create one tcpdump output per interface and add an identifier to the
beginning of each line:
if [[ $@ =~ -i[[:space:]]?[^[[:space:]]+ ]]; then
    tcpdump -l $@ | sed 's/^[Interface:"${BASH_REMATCH[0]:2}"/' &
else
    for interface in $(ifconfig | grep '^[a-z0-9]' | awk '{print $1}')
    do
        tcpdump -l -i $interface -nn $@ | sed 's/^[Interface:"$interface"/' &
    done
fi
# wait .. until CTRL+C

```

wait

- <https://serverfault.com/questions/224698/how-to-display-interface-in-tcpdump-output-flow>

From:
<https://at1.kr/dokuwiki/> - **AllThatLinux!**

Permanent link:
https://at1.kr/dokuwiki/doku.php/tcpdump_%EC%97%90%EC%84%9C_nic_name_%EC%B6%9C%EB%A0%A5%ED%95%98%EA%B8%B0

Last update: **2024/04/18 07:26**

