목차

tcpdump 에서 nic name 출력하기

기본적으로 tcpdump에서는 nic name을 출력하는 기능이 없다. 하지만 최근의 4.99 이후 버전부터는 기본적으로 nic name을 출력하도록 변경되었다. 참고

어쨌든 이 기능은 RHEL9 이상에서만 4.99 이상 버전을 사용하므로 이전버전을 사용중인 OS에서는 아래 스크립트를 이용하면 된다.

```
#!/bin/bash
#================================================================================
========
#
# FILE: dump.sh
# USAGE: dump.sh [-i interface] [tcpdump-parameters]
# DESCRIPTION: tcpdump on any interface and add the prefix [Interace: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
```

참조링크

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