Chapter 03. 네트워크 모니터링

네트워크 설정과 분석 도구

Copyright **FASTCAMPUS** Corp. All Rights Reserved

네트워크 모니터링

- 네트워크 설정 확인 (기본 유틸리티)
  - ipconfig
  - arp
  - route
  - ip
  - netstat
- 네트워크 기본 테스트 (기본 유틸리티)
  - ping
  - traceroute
  - nslookup
- 디버깅도구
  - nmap
  - nc
  - tcpdump
- 네트워크 모니터링 도구 (추가 설치)
  - nload
  - iftop
  - iptraf
  - nethogs
  - bmon
  - …

Copyright **FASTCAMPUS** Corp. All Rights Reserved

네트워크 설정 기초 - ifconfig

네트워크 인터페이스 (NIC, network interface card) 의 설정

- ifconfig
  - 인터페이스 확인
- ifconfig -a
  - 모든 인터페이스 확인

- 사용 예시
  - ifconfig enp0s3 down
  - ifconfig enp0s3 up
  - ifconfig enp0s3 192.168.0.2/24

- 네트워크 인터페이스명
  - 고전적 : eth0, eth1, eth2

  - 현재 (Ubuntu 16.04) : eth0 => enp0s3
    (더 정확히는 Ubuntu 15.10 부터~)
    - 인터페이스 네이밍 기법:
      - 펌웨어/바이오스로부터 할당 : eno1
      - PCI express 슬롯 번호 : ens1
      - 물리적 하드웨어 컨넥터 위치 : enp2s0
    - 배경:
      - https://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames/
    - 결론:
      - enp0s3 = ethernet network peripheral # serial #

Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 설정 기초 - 고정 IP 할당

네트워크 인터페이스 (NIC, network interface card) 의 수동 설정

- 인터페이스 설정파일 수정
  - vim /etc/network/interfaces

```
auto lo
iface lo inet lookback
```

기본값 : 루프백 인터페이스

```
auto enp0s3
iface enp0s3 inet dhcp
```

DHCP 수동 설정

```
auto enp0s3
iface enp0s3 inet static
address 192.168.0.2
netmask 255.255.255.0
gateway 192.168.0.1
dns-nameservers 8.8.8.8 8.8.4.4
```

고정 IP 수동 설정

- 설정 후 네트워크 재설정
  - sudo systemctl restart networking
- 설정 후 특정 인터페이스 재설정
  - sudo ifdown enp0s3
  - sudo ifup enp0s3

Fast campus
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 설정 기초 - arp

인접 디바이스 및 MAC 주소 확인

- arp 테이블 조회
  - arp -an
- arp 주소 삭제
  - arp -d <ip주소>
- arp 주소 고정 추가
  - arp -s <ip주소> <mac주소>

```
user1@user1-VirtualBox:~$ arp -a
? (192.168.56.100) at 08:00:27:07:bd:64 [ether] on enp0s8
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
? (168.126.63.1) at <incomplete> on enp0s3
? (168.126.63.2) at <incomplete> on enp0s3
```

Fast campus
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 설정 기초 - route

route 명령어를 통한 라우팅 테이블 변경

- 라우팅 테이블 조회
  - route -n
- 라우팅 테이블 추가
  - route add
  - route del

```
user1@user1-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.56.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s8
```

- 사용 예시
  - 기본 라우팅 (default gateway) 추가/삭제
    - route add default gw 10.0.2.2
    - route del default gw 10.0.2.2
  - 라우팅 테이블 추가/삭제
    - route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.2.2
    - route del -net 192.168.0.0 netmask 255.255.255.0
    - route add -host 192.168.1.1 dev enp0s3
    - route del -host 192.168.1.1

Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 설정 기초 - ip

IP 주소 확인/설정 관련 통합 명령어

- 인터페이스 확인
  - ip link
  - ip addr
  - ip addr show enp0s3
- 라우팅 확인
  - ip route
- 인접 디바이스 (L2/L3) 확인
  - ip neigh
- 라우팅 정책 확인
  - ip rule

- 사용 예
  - ip rule show
  - ip route show table main
  - ip route get 8.8.8.8
  - ip route get 8.8.8.8 from 10.0.2.15

- PBR (Policy Based Routing) 사용 예 (고급)
  - ip rule add from 192.168.0.0/32 table 1 priority 100
  - ip route add default via 10.0.2.15 table 1
  - ip route show table 1
  - ip route flush cache

Copyright **FASTCAMPUS** Corp. All Rights Reserved

네트워크 설정 기초 - ip 명령 #2

ip 명령어를 통한 IP 주소 셋업 및 라우팅 테이블 변경

- 인터페이스 IP 주소 추가/삭제
  - ip addr add 10.0.2.15/24 dev enp0s3
  - ip addr del 10.0.2.15/24 dev enp0s3

- 인터페이스 링크 Up/Down
  - ip link set enp0s3 up
  - ip link set enp0s3 down

- 라우팅 테이블 변경
  - 기본 라우팅 (default gateway) 추가/삭제
    - ip route add default via 10.0.2.2
    - ip route del default via 10.0.2.2

  - 라우팅 테이블 추가/삭제
    - ip route add 192.168.0.0/24 via 10.0.2.2 dev enp0s3
    - ip route del 192.168.0.0/24

- 참고:
  문법이 떠오르지 않을때, 도움말
  - ip route help
  - man ip route

Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 설정 기초 - netstat

시스템 내 열려있는 포트 확인

- 사용법
  - netstat <OPTION>
    - -a : 모든 소켓 정보
    - -r : 라우팅 정보 출력
    - -n : 호스트명 대신 IP 주소를 출력
    - -i : 모든 네트워크 인터페이스 정보 출력
    - -s : 프로토콜별 네트워크 통계
    - -p : 해당 소켓과 관련된 프로세스 표시

- 사용 예
  - 라우팅 테이블 확인
    - netstat -rn
  - 인터페이스 통계 표시
    - netstat -i
  - 모든 소켓과 프로세스 표시
    - netstat -anp
  - 열려있는 TCP 소켓 확인
    - netstat -ant | grep LISTEN

```
user1@user1-VirtualBox:~$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.15:22            10.0.2.2:61546          ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    27656    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    12607    /run/systemd/cgroups-agent
unix  7      [ ]         DGRAM                    12613    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    12888    /run/systemd/journal/syslog
unix  17     [ ]         DGRAM                    12889    /run/systemd/journal/dev-log
unix  3      [ ]         DGRAM                    12606    /run/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     16217
unix  3      [ ]         STREAM     CONNECTED     29252
unix  3      [ ]         STREAM     CONNECTED     30964    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29327
unix  3      [ ]         STREAM     CONNECTED     29224    @/tmp/dbus-aRvjgxS7jE
```

Fast campus
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 기본 테스트 - ping

ICMP 패킷을 통한 네트워크 연결 확인

- 사용법
  - ping <목적지 IP>

- 사용 예
  - ping 8.8.8.8
  - ping 8.8.8.8 -c 3

Copyright **FASTCAMPUS** Corp. All Rights Reserved

네트워크 기본 테스트 - traceroute

네트워크 라우팅 경로 트레이싱 도구

- 사용법
  - traceroute <목적지 IP>
- 설치
  - sudo apt install traceroute
- 사용 예
  - traceroute 8.8.8.8
  - traceroute www.google.com
  - traceroute www.naver.com
  - traceroute www.daum.com
- 참고
  - 중간에 방화벽이 있거나 (VM장비 NAT포함),
    ICMP 응답을 비활성화 해 둔 장비는 응답을 받을 수 없음

```
hyunlove@docker1:~$ traceroute www.google.com
traceroute to www.google.com (173.194.74.106), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  jb-in-f106.1e100.net (173.194.74.106)  0.622 ms * *
hyunlove@docker1:~$ traceroute www.daum.net
traceroute to www.daum.net (211.231.99.80), 30 hops max, 60 byte packets
 1  209.85.252.135 (209.85.252.135)  16.820 ms  16.830 ms 209.85.250.207 (209.85.250.207)  20.179 ms
 2  209.85.252.24 (209.85.252.24)  22.742 ms 209.85.252.126 (209.85.252.126)  22.773 ms 209.85.252.132 (209.85.252.132)  23.136 ms
 3  108.170.229.81 (108.170.229.81)  24.342 ms 72.14.233.198 (72.14.233.198)  24.184 ms 108.170.229.139 (108.170.229.139)  24.324 ms
 4  108.170.249.170 (108.170.249.170)  24.165 ms 108.170.249.106 (108.170.249.106)  24.134 ms 108.170.249.170 (108.170.249.170)  24.129 ms
 5  63-218-69-105.static.pccwglobal.net (63.218.69.105)  24.112 ms  23.976 ms  24.060 ms
 6  Bundle-Ether-41.br03.tok02.pccwbtn.net (63.218.250.85)  157.182 ms  156.858 ms  156.808 ms
 7  63.218.251.110 (63.218.251.110)  154.663 ms  154.605 ms 63-216-242-174.static.pccwglobal.net (63.216.242.174)  156.060 ms
 8  * * *
 9  * 211.231.99.80 (211.231.99.80)  181.757 ms  178.728 ms
hyunlove@docker1:~$
```

Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 기본 테스트 - nslookup

호스트 이름의 IP 주소 변환 도구

- 사용법
  - nslookup <도메인명>
  - nslookup <도메인명> <질의 네임서버>

- 사용 예
  - nslookup www.google.com
  - nslookup www.google.com 8.8.8.8

  - nslookup www.naver.com
  - nslookup www.naver.com 8.8.8.8

- 참고
  - 기본 도메인 서버는 /etc/resolv.conf 참고
  - 설정은 /etc/resolvconf/resolv.conf.d/base 또는 /etc/resolvconf/resolv.conf.d/tail 에 추가 nameserver 8.8.8.8
    수정 후 sudo resolvconf -u 로 갱신

```
user1@user1-VirtualBox:~$ nslookup www.google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.161.68

user1@user1-VirtualBox:~$ nslookup www.google.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.175.100
```

```
user1@user1-VirtualBox:~$ nslookup www.naver.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.naver.com   canonical name = www.naver.com.nheos.com.
Name:   www.naver.com.nheos.com
Address: 125.209.222.142
Name:   www.naver.com.nheos.com
Address: 125.209.222.141

user1@user1-VirtualBox:~$ nslookup www.naver.com 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www.naver.com   canonical name = www.naver.com.nheos.com.
www.naver.com.nheos.com canonical name = www.naver.com.edgekey.net.
www.naver.com.edgekey.net       canonical name = e6030.a.akamaiedge.net.
Name:   e6030.a.akamaiedge.net
Address: 23.50.3.12
```

Fast campus
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 분석 도구 - nmap

네트워크 포트 스캔 / IP 검색 등 다양한 네트워크 스캐닝 도구 (주의. 공격 도구이기도 함)

- 사용법
  - nmap <옵션> <목적지 IP>
    - -sS : TCP SYN 스캔
    - -sT : TCP 연결 스캔
    - -sP : ping 스캔
    - -sU : UDP 스캔
    - -O : 운영체제 확인
    - -v : 상세 출력
    - -F : 빠른 스캔 (fast mode)

- 설치
  - sudo apt install nmap

- 사용 예
  - 내 호스트(localhost) 의 열린 포트 확인
    - nmap localhost
  - 내 네트워크에 존재하는 호스트 확인 (ping scan)
    - nmap -sP 10.0.2.0/24
  - 10.0.2.2 호스트의 열린 포트 확인 (tcp syn scan)
    - nmap -sS 10.0.2.2
  - 10.0.2.15 의 운영체제 확인
    - nmap -O 10.0.2.15

- 10.0.2.0/24 네트워크의 호스트에 TCP 연결 빠른 스켄 및 운영체제 확인
  - nmap -sT -F -O -v 10.0.2.0/24

Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 분석 도구 - nc (netcat)

네트워크 데이터 매뉴얼(수동) 입력 도구

- 사용법
  - nc <옵션> <타겟 호스트> <포트>
    - -n : 호스트 네임과 포트 숫자 입력
    - -v : 상세 결과 출력 (verbose)
    - -l : 서버 모드 (listen)
      - -p : 서버 모드의 포트 (port)

- 사용 예
  - nc localhost 22

  - nc localhost 80
    HEAD / HTTP/1.0\n\n
  - echo -e “HEAD / HTTP/1.0\n\n” | nc localhost 80

  - 서버 모드
    - nc -l -p 1234
    - (다른창에서) nc localhost 1234

Fast campus
Copyright **FASTCAMPUS** Corp. All Rights Reserved

네트워크 분석 도구 - tcpdump

네트워크 트래픽 패킷 덤프 및 분석

- 사용법
  - tcpdump <옵션>
    - -i <nic> : 인터페이스
    - -w : 덤프 파일로 저장
    - -r : 저장된 덤프 파일 로딩
    - -c <cnt> : 캡쳐 할 패킷의 수
    - -s <size> : 패킷 캡쳐 길이 (-s0 은 모든 길이)
    - -v, -vv, -vvv : 패킷 상세 정보 표시
    - -n, -nn : hostname 및 port 에 대한 resolve 끄기(off)

- 사용 예
  - tcpdump -i enp0s3
  - tcpdump -i enp0s3 -w test.pcap
  - tcpdump -i enp0s3 -w test.pcap -c 10
  - tcpdump -i enp0s3 -s0 -nn

```
user1@user1-VirtualBox:~$ sudo tcpdump -i enp0s3 host 8.8.8.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
01:23:57.365673 IP 10.0.2.15 > dns.google: ICMP echo request, id 4763, seq 1, length 64
01:23:57.730512 IP dns.google > 10.0.2.15: ICMP echo reply, id 4763, seq 1, length 64
01:23:58.366658 IP 10.0.2.15 > dns.google: ICMP echo request, id 4763, seq 2, length 64
01:23:58.508577 IP dns.google > 10.0.2.15: ICMP echo reply, id 4763, seq 2, length 64
```

Fast campus
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 분석 도구 - tcpdump #2

네트워크 트래픽 패킷 덤프 및 분석 - 상세 필터링 옵션

- 필터
  - tcpdump <옵션> <필터>
    - host <ip> : 해당 호스트와의 통신
    - src <ip> : 출발지 IP 기준
    - dst <ip> : 목적지 IP 기준
    - net <ip/cidr> : 해당 네트워크 대역 통신
    - port <port> : 특정 (출발지/목적지) 포트
    - src port <port> : 특정 출발지 포트
    - portrange <port-port> : 특정 포트 범위
    - <proto> : 특정 프로토콜 (icmp, tcp, udp)

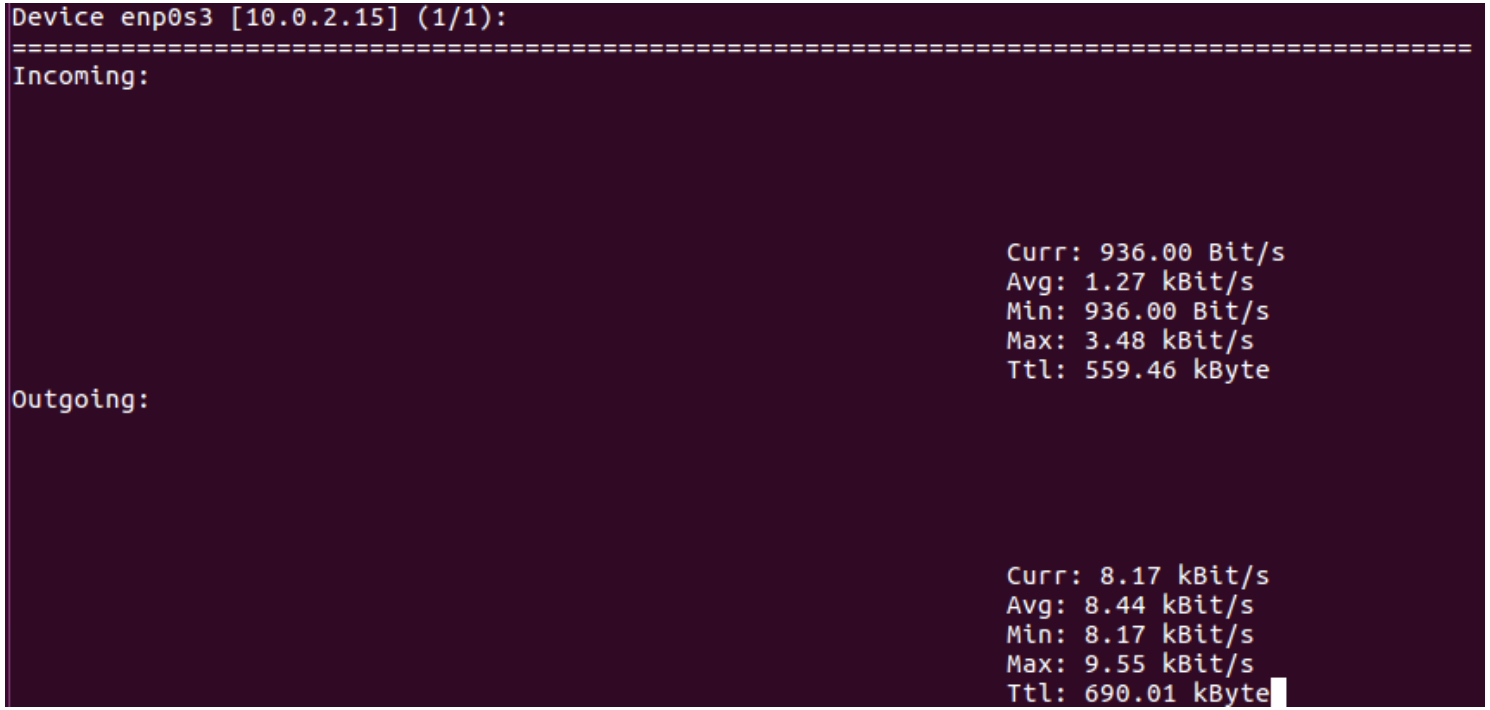
- 사용 예
  - tcpdump -i enp0s3 host 1.2.3.4
  - tcpdump -i enp0s3 src 2.3.4.5
  - tcpdump -i enp0s3 dst 3.4.5.6
  - tcpdump -i enp0s3 net 1.2.3.0/24
  - tcpdump -i enp0s3 port 22
  - tcpdump -i enp0s3 portrange 20-21
  - tcpdump -i enp0s3 icmp
  - tcpdump -i enp0s3 src 1.2.3.4 and dst port 80
  - tcpdump dst 192.168.0.2 and src net and not icmp
  - tcpdump ‘dst 8.8.8.8 and (src net 192.168.0.0/24 or 172.16.0.0/16)’
  - tcpdump ‘src 8.8.8.8 and (dst port 3389 or 22)’

Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 모니터링 도구 - nload

실시간 인터페이스 트래픽 통계

- 사용법
  - nload <인터페이스>
- 설치방법
  - apt install nload



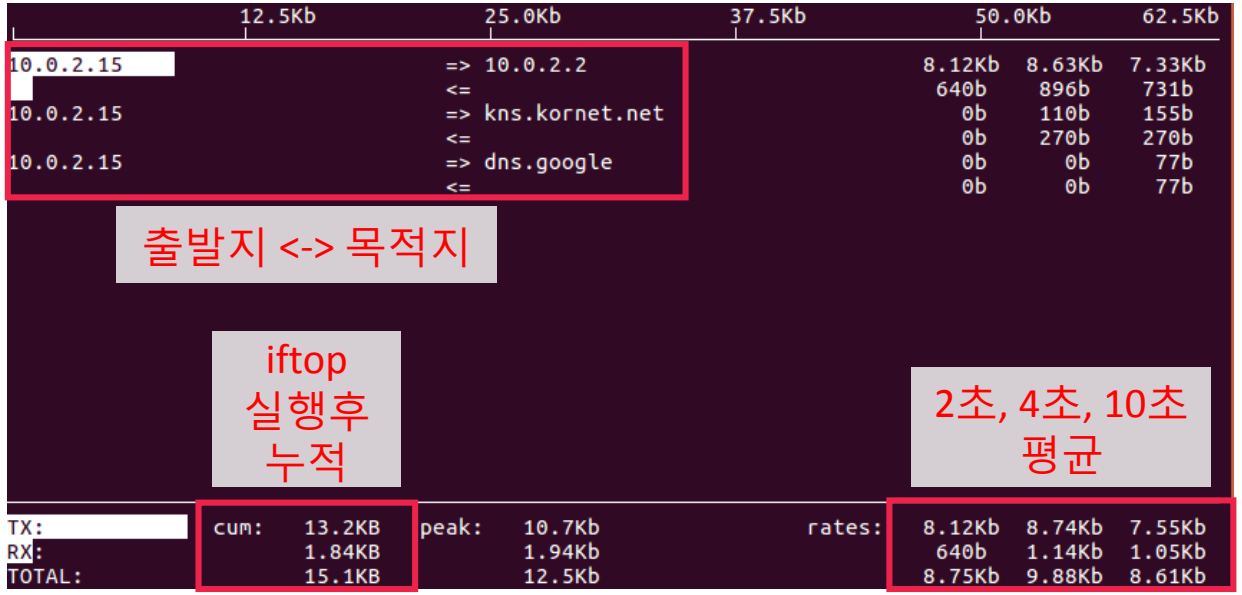
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 모니터링 도구 - iftop

실시간 세션 모니터링

- 사용법
  - iftop <옵션>
    - -i : 인터페이스
    - -n : 호스트네임 변환 안함
    - -f : 필터 (pcap filter)
- 설치방법
  - apt install iftop
- 사용 예
  - iftop
  - iftop -i enp0s3 -n
  - iftop -f ‘ip dst 8.8.8.8’
  - iftop -f ‘dst port 22’

- 런타임 옵션
  - p : port 표시
  - P : 잠시 중단 (Pause)
  - t : rx only, tx only, both
  - b : bar 그래프 on/off
  - L : linear / log scale
  - n : name resolve
  - h : help

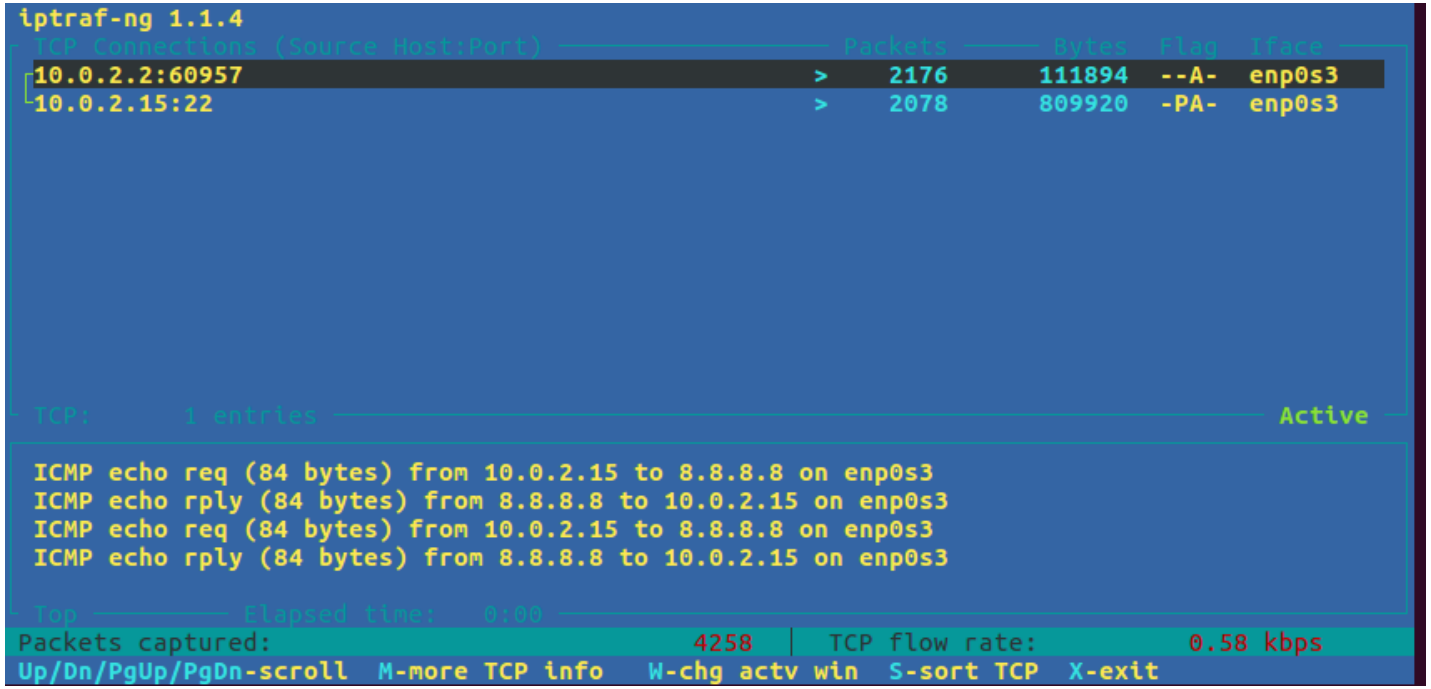


Fast campus
Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 모니터링 도구 - iptraf-ng (iptraf 의 개선된 버전)

네트워크 트래픽 실시간 모니터링 도구

- 사용법
  - iptraf <옵션>
    - -i : 인터페이스
- 설치방법
  - apt install iptraf-ng
- 사용 예
  - iptraf



Copyright FASTCAMPUS Corp. All Rights Reserved

네트워크 모니터링 도구 - nethogs

사용자별/프로세스별 네트워크 트래픽 이용량 실시간 모니터링

- 사용법
  - nethogs <옵션>
    - -d <sec> : 갱신 주기
- 설치방법
  - apt install nethogs
- 사용 예
  - nethogs

```
NetHogs version 0.8.1

    PID USER     PROGRAM                                  DEV        SENT      RECEIVED
   8088 user1    curl                                     enp0s3     0.606     45.668 KB/sec
   3341 user1    sshd: user1@pts/19                       enp0s3    58.292      8.947 KB/sec
      ? root     10.0.2.15:57032-125.209.222.142:80                  0.000      0.000 KB/sec
      ? root     unknown TCP                                         0.000      0.000 KB/sec

  TOTAL                                                             58.897     54.615 KB/sec
```

Fast campus

Copyright FASTCAMPUS Corp. All Rights Reserved

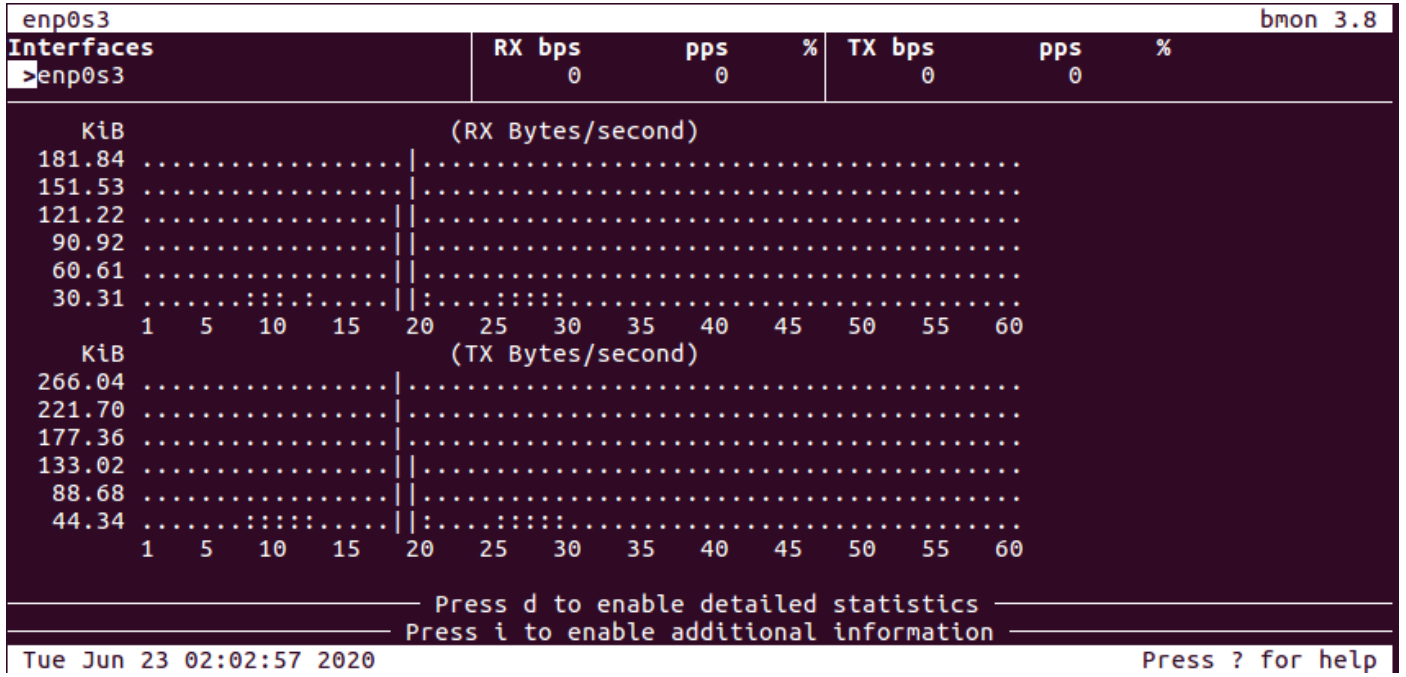
네트워크 모니터링 도구 - bmon

그래피컬 실시간 뷰 네트워크 모니터링

- 사용법
  - bmon <옵션>
    - -p : 인터페이스
    - -r <sec> : 그래프 당 초 주기
    - -o : 출력 포멧 (ascii, format)

- 설치방법
  - apt install bmon

- 사용 예
  - bmon -r 5 -p enp0s3



Copyright FASTCAMPUS Corp. All Rights Reserved