

# Guide for IO Visor Environment

Jungi Lee

2017-07-24

# Type S/C/O (현재 설정 상황)

Type	IP address	OS/Kernel Version
Type S	116.89.190.193	OA 4.2 (Ubuntu 14.04. based) Linux Kernel 4.8.0
Type C	210.114.90.170	Ubuntu 16.04 Linux Kernel 4.8.0
Type O	210.114.90.169	Ubuntu 16.04 Linux Kernel 4.8.0

Upgrade to Linux Kernel 4.5.1 to 4.8.0 (On Type S, Znyx B1's OA4)

- `wget http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.8/linux-headers-4.8.0-040800_4.8.0-040800.201610022031_all.deb`
- `wget http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.8/linux-headers-4.8.0-040800-generic_4.8.0-040800.201610022031_amd64.deb`
- `wget http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.8/linux-image-4.8.0-040800-generic_4.8.0-040800.201610022031_amd64.deb`
- `sudo dpkg -i linux-*.deb`

# Type S 10G Driver Problem (KMJ helped)

- 커널 업그레이드가 진행되며 Parameter 관련 오류 발생
- -> /etc/modprobe.d/ixgbe.conf 의 Parameter 수정해서 해결
- (sudo insmod ixgbe.ko max\_vfs=32)

```
10.865198] ixgbe: Intel(R) 10 Gigabit PCI Express Network Driver - version 4.4.0-k
10.865200] ixgbe: Copyright (c) 1999-2016 Intel Corporation.
10.865452] ixgbe 0000:01:00.0: Enabling SR-IOV VFs using the max_vfs module parameter is deprecated
11.056711] ixgbe 0000:01:00.0 0000:01:00.0 (uninitialized): SR-IOV enabled with 32 VFs
11.080541] ixgbe 0000:01:00.0: Multiqueue Enabled: Rx Queue count = 2, Tx Queue count = 2
11.080669] ixgbe 0000:01:00.0: PCI Express bandwidth of 32GT/s available
11.080670] ixgbe 0000:01:00.0: (Speed:5.0GT/s, Width: x8, Encoding Loss:20%)
11.080751] ixgbe 0000:01:00.0: MAC: 2, PHY: 1, PBA No: FFFFFFFF-OFF
11.080753] ixgbe 0000:01:00.0: e8:8d:f5:10:33:c4
11.182483] ixgbe 0000:01:00.0 eth2: IOV is enabled with 32 VFs
11.182525] ixgbe 0000:01:00.0: Intel(R) 10 Gigabit Network Connection
11.182909] ixgbe 0000:01:00.1: Enabling SR-IOV VFs using the max_vfs module parameter is deprecated
11.368847] ixgbe 0000:01:00.1 0000:01:00.1 (uninitialized): SR-IOV enabled with 32 VFs
11.392675] ixgbe 0000:01:00.1: Multiqueue Enabled: Rx Queue count = 2, Tx Queue count = 2
11.392803] ixgbe 0000:01:00.1: PCI Express bandwidth of 32GT/s available
11.392805] ixgbe 0000:01:00.1: (Speed:5.0GT/s, Width: x8, Encoding Loss:20%)
11.392886] ixgbe 0000:01:00.1: MAC: 2, PHY: 1, PBA No: FFFFFFFF-OFF
11.392887] ixgbe 0000:01:00.1: e8:8d:f5:10:33:c5
11.426816] ixgbe 0000:01:00.1 eth3: IOV is enabled with 32 VFs
```

# Upgrade to Linux Kernel 4.4.0 to 4.8.0 (On Type C, General machines)

- Sudo apt-get -y install linux-image-4.8.0-41-generic linux-image-extra-4.8.0-41-generic
- `sudo apt-get install linux-headers-$(uname -r)`
  
- CONFIG\_BPF=y
- CONFIG\_BPF\_SYSCALL=y
- # [optional, for tc filters]
- CONFIG\_NET\_CLS\_BPF=m
- # [optional, for tc actions]
- CONFIG\_NET\_ACT\_BPF=m
- CONFIG\_BPF\_JIT=y
- CONFIG\_HAVE\_BPF\_JIT=y
- # [optional, for kprobes]
- CONFIG\_BPF\_EVENTS=y

# Type S/C/O kernel Version 4.8.0

```
Connecting to 116.89.190.193:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to ZNYX OpenArchitect 4.2 (Ubuntu 14.04 LTS) (GNU/Linux 4.8.0-040800-generic x86_64)

* Documentation:  https://help.ubuntu.com/
Last login: Wed Jul 19 11:10:42 2017 from 203.237.53.71
znyx@S1-GJ1S:~$
```

```
-----
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-41-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

36 packages can be updated.
21 updates are security updates.
```

```
Connecting to 210.114.90.169:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-58-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

5 packages can be updated.
0 updates are security updates.
```

# Install IO Visor – Build Dependencies

- # Trusty and older
- VER=trusty
- echo "deb http://llvm.org/apt/\$VER/ llvm-toolchain-\$VER-3.7 main
- deb-src http://llvm.org/apt/\$VER/ llvm-toolchain-\$VER-3.7 main" | ~~W~~ sudo tee /etc/apt/sources.list.d/llvm.list
- wget -O - http://llvm.org/apt/llvm-snapshot.gpg.key | sudo apt-key add -
- sudo apt-get update
  
- # All versions
- sudo apt-get -y install bison build-essential cmake flex git libedit-dev libllvm3.7 llvm-3.7-dev libclang-3.7-dev python zlib1g-dev libelf-dev

# Install IO Visor – Install and compile BCC

- `git clone https://github.com/iovisor/bcc.git`
- `mkdir bcc/build; cd bcc/build`
- `cmake .. -DCMAKE_INSTALL_PREFIX=/usr`
- `make`
- `sudo make install`



# Packet tracing

- \$sudo python packet\_tracing.py
- Working on Type S/C/O

```
2017-07-19 11:39:07.919817
4 116.89.190.193 203.237.53.71 13
Suspicious IP detected
2017-07-19 11:39:07.919938
4 116.89.190.193 203.237.53.71 13
Suspicious IP detected
2017-07-19 11:39:07.920064
4 116.89.190.193 203.237.53.71 13
Suspicious IP detected
2017-07-19 11:39:07.920188
4 116.89.190.193 203.237.53.71 13
Suspicious IP detected
2017-07-19 11:39:07.920310
4 116.89.190.193 203.237.53.71 13
^CTraceback (most recent call last):
  File "packet_tracing.py", line 143, in <module>
    f = open("list.txt", "r")
KeyboardInterrupt
znyx@SL-GJ1S:~/packet$
```

```
2017-07-19 20:39:50.037906
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038007
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038116
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038232
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038374
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038464
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038552
4 210.114.90.170 203.237.53.71 191
Suspicious IP detected
2017-07-19 20:39:50.038684
^CTraceback (most recent call last):
  File "packet_tracing.py", line 139, in <module>
    print("%3s%20s%20s%9s" % (str(int(ipversion, 2)), srcAddr, dstAddr,
KeyboardInterrupt
netcs@KOREN-Cloud:~/packet$
```

```
2017-07-19 20:40:46.932831
4 210.114.90.169 203.237.53.71 236
Suspicious IP detected
2017-07-19 20:40:46.932940
4 210.114.90.169 203.237.53.71 236
Suspicious IP detected
2017-07-19 20:40:46.933015
4 210.114.90.169 203.237.53.71 236
Suspicious IP detected
2017-07-19 20:40:46.933110
4 210.114.90.169 203.237.53.71 236
Suspicious IP detected
2017-07-19 20:40:46.933220
^CTraceback (most recent call last):
  File "packet_tracing.py", line 143, in <module>
    f = open("list.txt", "r")
KeyboardInterrupt
netcs@Type-0-Test:~/packet$
```