Assignment 5: Tutorial

lspci stands for list pci. Think of this command as “ls” + “pci”. This will display information about all the PCI bus in your server.

Apart from displaying information about the bus, it will also display information about all the hardware devices that are connected to your PCI and PCIe bus.

For example, it will display information about Ethernet cards, RAID controllers, Video cards, etc.

1. Default Usage

By default it will display all the device information as shown below. The first field is the slot information in this format: [domain:]bus:device.function

In this example, since all the domain are 0, lspci will not display the domain.

```
# lspci

00:00.0 Host bridge: Intel Corporation 5500 I/O Hub to ESI Port (rev 13)

00:01.0 PCI bridge: Intel Corporation 5520/5500/X58 I/O Hub PCI Express Root Port 1 (rev 13)

00:09.0 PCI bridge: Intel Corporation 7500/5520/5500/X58 I/O Hub PCI Express Root Port 9 (rev 13)

00:14.0 PIC: Intel Corporation 7500/5520/5500/X58 I/O Hub System Management Registers (rev 13)

00:14.1 PIC: Intel Corporation 7500/5520/5500/X58 I/O Hub GPIO and Scratch Pad Registers (rev 13)

00:14.2 PIC: Intel Corporation 7500/5520/5500/X58 I/O Hub Control Status and RAS Registers (rev 13)

00:1a.0 USB controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #4 (rev 02)

00:1c.0 PCI bridge: Intel Corporation 82801I (ICH9 Family) PCI Express Port 1 (rev 02)

00:1d.0 USB controller: Intel Corporation 82801I (ICH9 Family) USB UHCI Controller #1 (rev 02)

00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 92)

00:1f.0 ISA bridge: Intel Corporation 82801IB (ICH9) LPC Interface Controller (rev 02)

00:1f.2 IDE interface: Intel Corporation 82801IB (ICH9) 2 port SATA Controller [IDE mode] (rev 02)

01:00.0 Ethernet controller: Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet (rev 20)
```

01:00.1 Ethernet controller: Broadcom Corporation NetXtreme II BCM5709 Gigabit Ethernet (rev 20)

03:00.0 RAID bus controller: LSI Logic / Symbios Logic MegaRAID SAS 2108 [Liberator] (rev 05)

06:03.0 VGA compatible controller: Matrox Electronics Systems Ltd. MGA G200eW WPCM450 (rev 0a)

2. Detailed Device Information

If you want to look into details of a particular device, use -v to get more information. This will display information about all the devices. The output of this command will be very long, and you need to scroll down and view the appropriate section.

For additional level for verbosity, you can use -vv or -vvv.

In the following example, we have given output of only the RAID controller device.

```
# lspci -v

03:00.0 RAID bus controller: LSI Logic / Symbios Logic MegaRAID SAS 2108 [Liberator] (rev 05)
        Subsystem: Dell PERC H700 Integrated
        Flags: bus master, fast devsel, latency 0, IRQ 16
        I/O ports at fc00 [size=256]
        Memory at df1bc000 (64-bit, non-prefetchable) [size=16K]
        Memory at df1c0000 (64-bit, non-prefetchable) [size=256K]
        Expansion ROM at df100000 [disabled] [size=256K]
        Capabilities: [50] Power Management version 3
        Capabilities: [68] Express Endpoint, MSI 00
        Capabilities: [d0] Vital Product Data
        Capabilities: [a8] MSI: Enable- Count=1/1 Maskable- 64bit+
        Capabilities: [c0] MSI-X: Enable+ Count=15 Masked-
        Capabilities: [100] Advanced Error Reporting
        Capabilities: [138] Power Budgeting <?>
        Kernel driver in use: megaraid_sas
        Kernel modules: megaraid_sas
```

3. Ethtool utility is used to view and change the ethernet device parameters.

List Ethernet Device Properties

When you execute ethtool command with a device name, it displays the following information about the ethernet device.

```
# ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 100Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 1
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: d
        Wake-on: d
        Link detected: yes
```

4. Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships, etc.

Important Commands:

a) list all ports: netstat -a
b) list all TCP ports: netstat -at
c) list all UDP ports: netstat -au
d) list only listening ports: netstat -l
e) list only listening TCP ports: netstat -lt
f) list only listening UDP ports: netstat -lu
g) list only listening UNIX ports: netstat -lx
h) show statistics for all ports: netstat -s
i) show statistics for TCP ports: netstat -st

j) show statistics for UDP ports: netstat -su

5. lsof stands for List Open Files. It is easy to remember lsof command if you think of it as "ls + of", where ls stands for list, and of stands for open files. It is a command line utility which is used to list the information about the files that are opened by various processes. In unix, everything is a file, (pipes, sockets, directories, devices, etc.). Thus, by using lsof command, you can get the information about any opened files.

Explanation of columns of result obtained on execution of lsof command

a) FD – Represents the file descriptor. Some of the values of FDs are:
   - cwd – Current Working Directory
   - txt – Text file
   - mem – Memory mapped file
   - mmap – Memory mapped device

b) NUMBER – Represent the actual file descriptor. The character after the number i.e '1u', represents the mode in which the file is opened. r for read, w for write, u for read and write.

c) TYPE – Specifies the type of the file. Some of the values of TYPEs are:
   - REG – Regular File
   - DIR – Directory
   - FIFO – First In First Out
   - CHR – Character special file

   For a complete list of FD & TYPE, refer **man lsof**.

6. ifconfig command is used to configure network interfaces. ifconfig stands for interface configurator. Ifconfig is widely used to initialize the network interface and to enable or disable the interfaces.

Some special commands with ifconfig

a) View network settings of an ethernet adaptor: ifconfig eth0
b) Display details of all interfaces including disabled interfaces: ifconfig -a
c) Disable an interface: ifconfig eth0 down
d) Enable an interface: ifconfig eth0 up
e) Assign IP address to an interface: if config eth0 IP-address
f) Change subnet mask of an interface: ifconfig eth0 netmask 255.255.255.0
g) Change broadcast address of the interface: ifconfig eth0 broadcast 192.168.2.255
h) Assign IP address, netmask, and broadcast address at the same time to interface: ifconfig eth0 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255
i) Change MTU of an interface: ifconfig eth0 mtu XX

7. ARP request is a broadcast and an ARP response is a unicast.

Command:

a) Type arp -a: there will be no entry in table because they never communicate with each other.
b) Perform the ping operation: ping 192.168.1.2
c) Type arp -a again. The entries in arp table can be seen in the following format:

Internet Address Physical Address Type

8. traceroute is a network tool used to show the route taken by packets across an IP network. The Traceroute tool will show you each hop sequentially, and total hops required. For each hop, it will display the hop #, roundtrip times, best time (ms), IP address, TTL, and country.
Seeing the traceroute information can help you determine why your connections to a given server might be poor and can help you identify problems. It also shows you how systems are connected to each other, letting you see how your ISP connects to the Internet as well as how the target system is connected.
Command: traceroute www.google.com (equivalent command in windows: tracert)

9. tcpdump command is also called as packet analyzer. tcpdump command will work on most flavors of unix operating system. tcpdump allows us to save the packets that are captured, so that we can use it for future analysis. The saved file can be viewed by the same tcpdump command. We can also use open source software like wireshark to read the tcpdump pcap files.

Commands:

a) Capture packets from a particular ethernet interface: tcpdump -i eth1 (tcpdump captures all the packet flows in the interface eth1 and displays in the standard output).
b) Capture only N number of packets: tcpdump -c 2 -i eth0 (captures only 2 packets from interface eth0).
c) Display captured packets in ASCII: tcpdump -A -i eth0
d) Display captured packets in HEX and ASCII: tcpdump -XX -i eth0
e) Capture the packets and write into a file: tcpdump -w 08232010.pcap -i eth0 (-w option writes the packets into a given file. The file extension should be .pcap, which can be read by any network protocol analyzer).
f) Reading the packets from a saved file: tcpdump -tttt -r data.pcap
g) Capture packets with IP address: tcpdump -n -i eth0