DevOps external course

Networking using Linux. Lection 1

Lecture 6.1

Module 6 **Linux Networking**

Serge Prykhodchenko

Agenda

- Configuring
- Monitoring
- Debugging
- Troubleshooting
- Q&A

CONFIGURING

Configuring

Setting/Changing an IP address

There are several ways to set an IP address in Ubuntu. You can configure the network interface to use dynamic IP using DHCP server or you can manually set a static IP address.

Method #1: Network configuration on the command line

In Ubuntu, you can set IP address through terminal commands.

```
> sudo ifconfig eth0 192.168.0.110 netmask 255.255.255.0
```

Then to add a default gateway, add the below command:

```
> sudo route add default gw 192.168.0.1 eth0
```

Method #2: Network configuration using GUI (NOT OUR WAY)

Configuring

Setting/Changing an IP address

Method #3: Configure the network by editing /etc/interfaces file

- One more method that you can use to configure the IP address. To obtain IP address dynamically, you have to edit ***/etc/network/interfaces***. In ***/etc/network/interfaces***, the basic configuration of interfaces is stored.

Edit the /etc/network/interfaces by entering the following command in terminal.

```
> sudo nano /etc/network/interfaces
```

Then add the following lines:

```
> auto eth1 iface eth1 inet dhcp
```

Save the file and restart networking services using the below command.

```
> sudo systemctl restart networking
>sudo netplan apply
```

Configuring

Method #3: Configure the network by editing /etc/interfaces file

- To set IP address static, you also have to edit /etc/network/interfaces.

Edit the /etc/network/interfaces by entering the following command in terminal.

> sudo nano /etc/network/interfaces

Add the below lines to /etc/network/interfaces.

> auto eth1

> iface eth1 inet static address 192.168.0.111

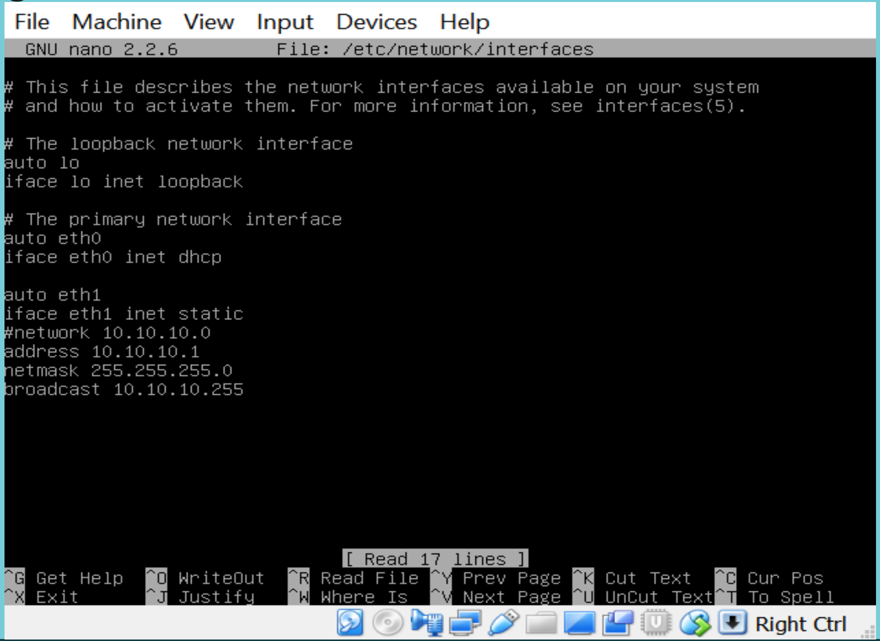
> netmask 255.255.255.0

> gateway 192.168.0.1

> dns-nameservers 8.8.8.8

Save the file and restart networking services using the below command.

> sudo service networking restart



```
  GNU nano 2.2.6           File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
#network 10.10.10.0
address 10.10.10.1
netmask 255.255.255.0
broadcast 10.10.10.255

                                [ Read 17 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

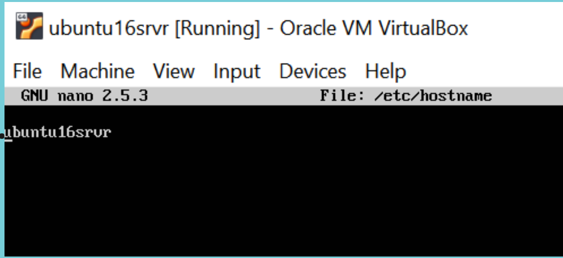
Configuring

Setting up/Changing ***hostname***

The hostname of Ubuntu OS is configured in the file */etc/hostname*.

To edit */etc/hostname*, enter the below command:

> sudo nano /etc/hostname



```
 GNU nano 2.5.3                          File: /etc/hostname

ubuntu16srvr
```

Editing the ***hosts*** file

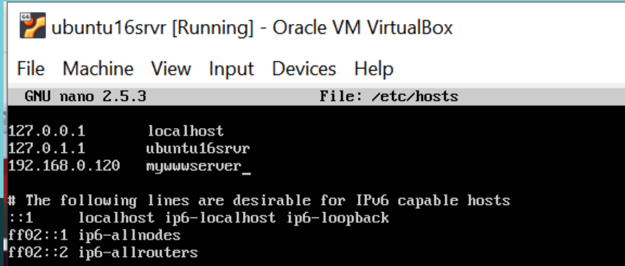
Hosts file maps hostname to IP address locally. For instance, you have a server in your local network, instead of remembering its IP, you can map its IP with a name in your /etc/hosts file. It will allow you to access that machine with a name instead of the IP. To edit a ***hosts*** file, enter:

> sudo nano /etc/hosts

Add the server IP address and name in the hosts file in the following format:

192.168.0.120 mywwwserver

Save the file and reboot the system to apply changes.



```
 GNU nano 2.5.3                          File: /etc/hosts

127.0.0.1       localhost
127.0.1.1       ubuntu16srvr
192.168.0.120   mywwwserver

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Configuring

Enable or Disable Specific Interface

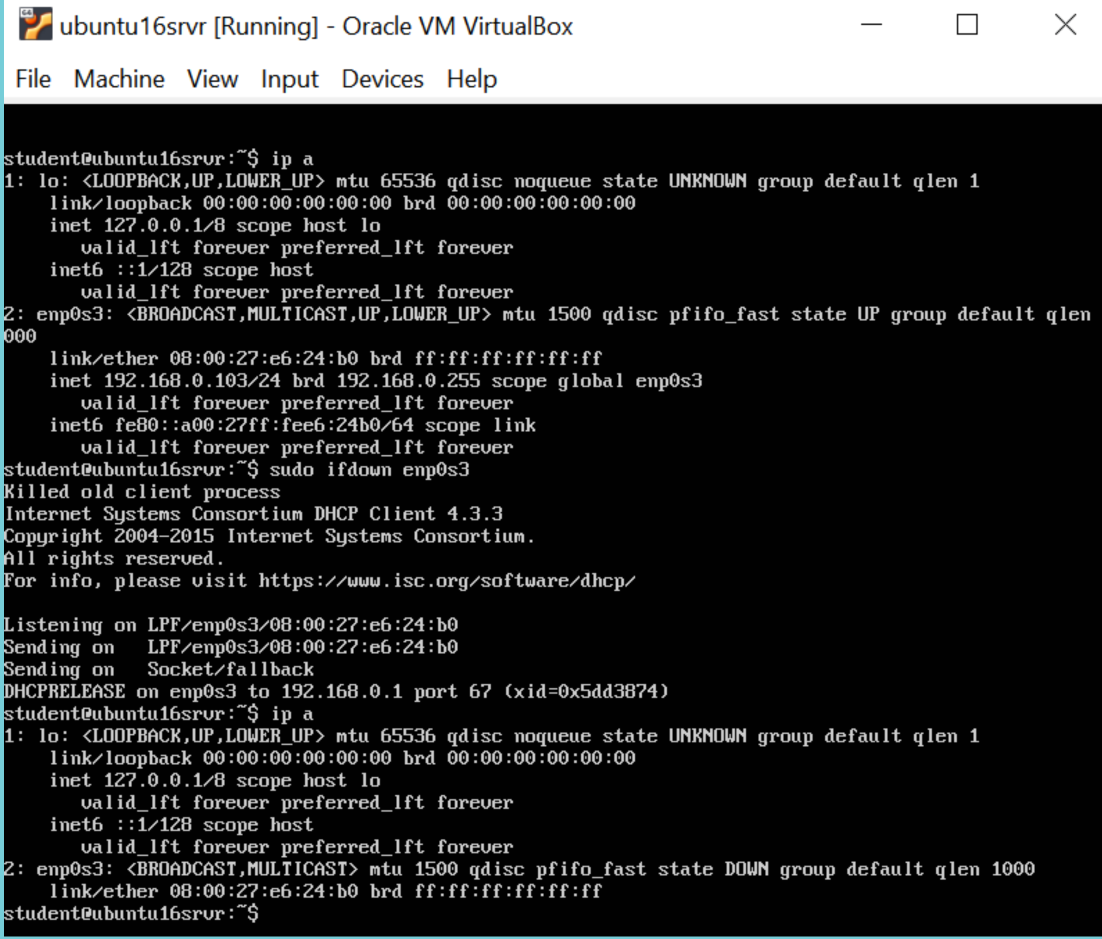
To enable or disable specific Interface, use command as follows.

Enable eth0

> sudo ifup eth0

Disable eth0

> sudo ifdown eth0

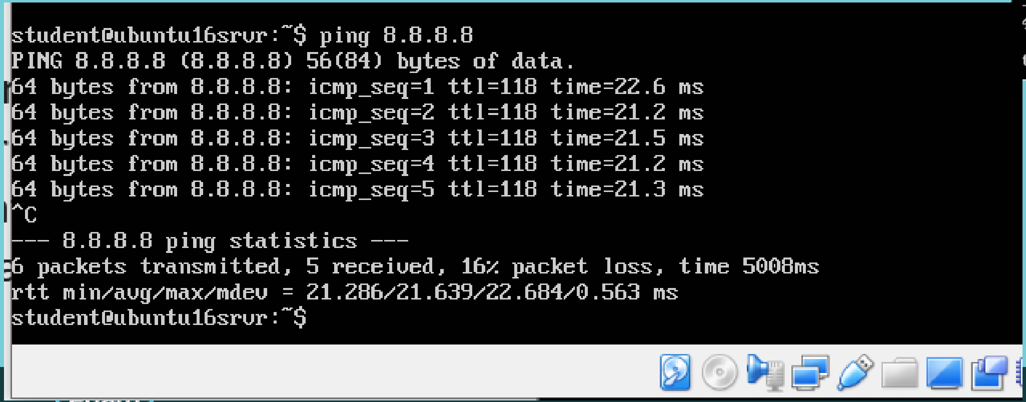

ubuntu16srvr [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
student@ubuntu16srvr:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
000
    link/ether 08:00:27:e6:24:b0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.103/24 brd 192.168.0.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee6:24b0/64 scope link
       valid_lft forever preferred_lft forever
student@ubuntu16srvr:~$ sudo ifdown enp0s3
Killed old client process
Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:e6:24:b0
Sending on   LPF/enp0s3/08:00:27:e6:24:b0
Sending on   Socket/fallback
DHCPRELEASE on enp0s3 to 192.168.0.1 port 67 (xid=0x5dd3874)
student@ubuntu16srvr:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 08:00:27:e6:24:b0 brd ff:ff:ff:ff:ff:ff
student@ubuntu16srvr:~$
```

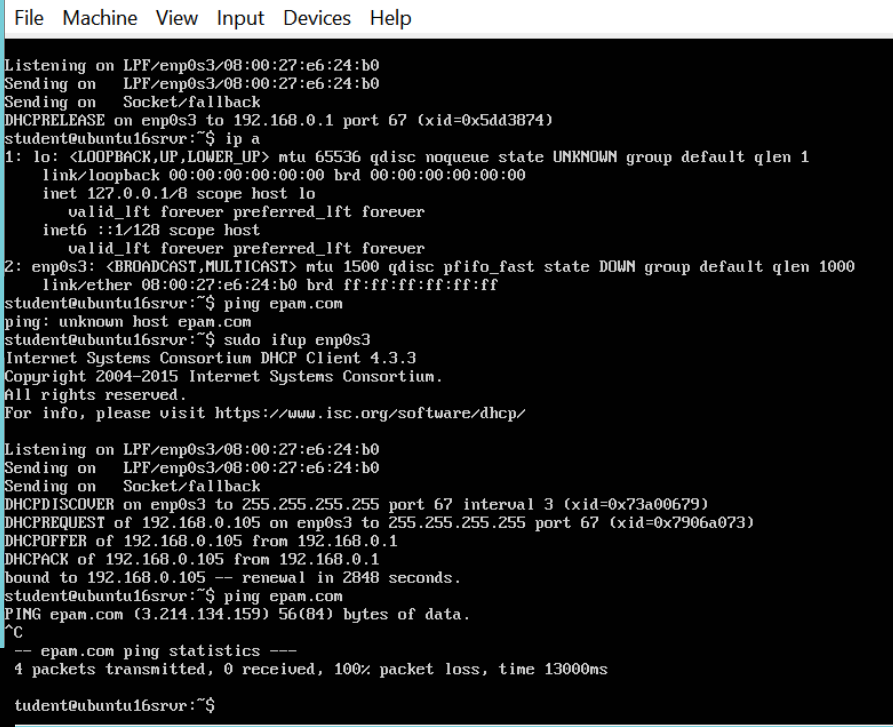
Monitoring / Debugging / Troubleshooting

PING Command

PING (Packet INternet Groper) command is the best way to test connectivity between two nodes. Whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping use ICMP (Internet Control Message Protocol) to communicate to other devices. You can ping host name of ip address using below command.



```
student@ubuntu16srvr:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=22.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=21.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=21.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=21.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=21.3 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 5 received, 16% packet loss, time 5008ms
rtt min/avg/max/mdev = 21.286/21.639/22.684/0.563 ms
student@ubuntu16srvr:~$
```

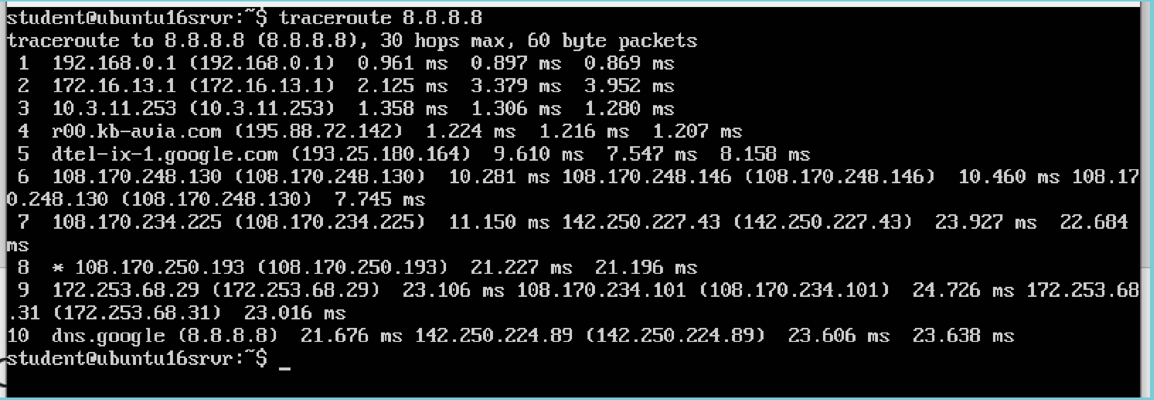


```
Listening on LPF/enp0s3/08:00:27:e6:24:b0
Sending on   LPF/enp0s3/08:00:27:e6:24:b0
Sending on   Socket/fallback
DHCPRELEASE on enp0s3 to 192.168.0.1 port 67 (xid=0x5dd3874)
student@ubuntu16srvr:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 08:00:27:e6:24:b0 brd ff:ff:ff:ff:ff:ff
student@ubuntu16srvr:~$ ping epam.com
ping: unknown host epam.com
student@ubuntu16srvr:~$ sudo ifup enp0s3
Internet Systems Consortium DHCP Client 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:e6:24:b0
Sending on   LPF/enp0s3/08:00:27:e6:24:b0
Sending on   Socket/fallback
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0x73a00679)
DHCPREQUEST of 192.168.0.105 on enp0s3 to 255.255.255.255 port 67 (xid=0x7906a073)
DHCPOFFER of 192.168.0.105 from 192.168.0.1
DHCPACK of 192.168.0.105 from 192.168.0.1
bound to 192.168.0.105 -- renewal in 2848 seconds.
student@ubuntu16srvr:~$ ping epam.com
PING epam.com (3.214.134.159) 56(84) bytes of data.
^C
 -- epam.com ping statistics ---
 4 packets transmitted, 0 received, 100% packet loss, time 13000ms

 tudent@ubuntu16srvr:~$
```

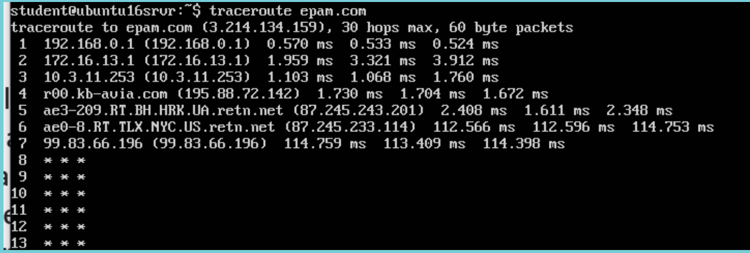
Monitoring / Debugging / Troubleshooting

TRACEROUTE Command

traceroute is a network troubleshooting utility which shows number of hops taken to reach destination also determine packets traveling path. Below we are tracing route to global DNS server IP Address and able to reach destination also shows path of that packet is traveling



```
student@ubuntu16srvr:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.961 ms  0.897 ms  0.869 ms
 2  172.16.13.1 (172.16.13.1)  2.125 ms  3.379 ms  3.952 ms
 3  10.3.11.253 (10.3.11.253)  1.358 ms  1.306 ms  1.280 ms
 4  r00.kb-avia.com (195.88.72.142)  1.224 ms  1.216 ms  1.207 ms
 5  dtel-ix-1.google.com (193.25.180.164)  9.610 ms  7.547 ms  8.158 ms
 6  108.170.248.130 (108.170.248.130)  10.281 ms 108.170.248.146 (108.170.248.146)  10.460 ms 108.17
0.248.130 (108.170.248.130)  7.745 ms
 7  108.170.234.225 (108.170.234.225)  11.150 ms 142.250.227.43 (142.250.227.43)  23.927 ms  22.684
ms
 8  * 108.170.250.193 (108.170.250.193)  21.227 ms  21.196 ms
 9  172.253.68.29 (172.253.68.29)  23.106 ms 108.170.234.101 (108.170.234.101)  24.726 ms 172.253.68
.31 (172.253.68.31)  23.016 ms
10  dns.google (8.8.8.8)  21.676 ms 142.250.224.89 (142.250.224.89)  23.606 ms  23.638 ms
student@ubuntu16srvr:~$ _
```



```
student@ubuntu16srvr:~$ traceroute epam.com
traceroute to epam.com (3.214.134.159), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.570 ms  0.533 ms  0.524 ms
 2  172.16.13.1 (172.16.13.1)  1.959 ms  3.321 ms  3.912 ms
 3  10.3.11.253 (10.3.11.253)  1.103 ms  1.068 ms  1.760 ms
 4  r00.kb-avia.com (195.88.72.142)  1.730 ms  1.704 ms  1.672 ms
 5  ae3-209.RT.BH.HRK.UA.retn.net (87.245.243.201)  2.408 ms  1.611 ms  2.348 ms
 6  ae0-8.RT.TLX.NYC.US.retn.net (87.245.233.114)  112.566 ms  112.596 ms  114.753 ms
 7  99.83.66.196 (99.83.66.196)  114.759 ms  113.409 ms  114.398 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
```

Monitoring / Debugging / Troubleshooting

mtr

MTR (Matt's traceroute) is a program with a command-line interface that serves as a network diagnostic and troubleshooting tool. This command combines the functionality of the ping and traceroute commands. Just like a traceroute, the mtr command will show the route from a computer to a specified host. mtr provides a lot of statistics about each hop, such as response time and percentage. With the mtr command, you will get more information about the route and be able to see problematic devices along the way. If you see a sudden increase in response time or packet loss, then obviously, there is a bad link somewhere.

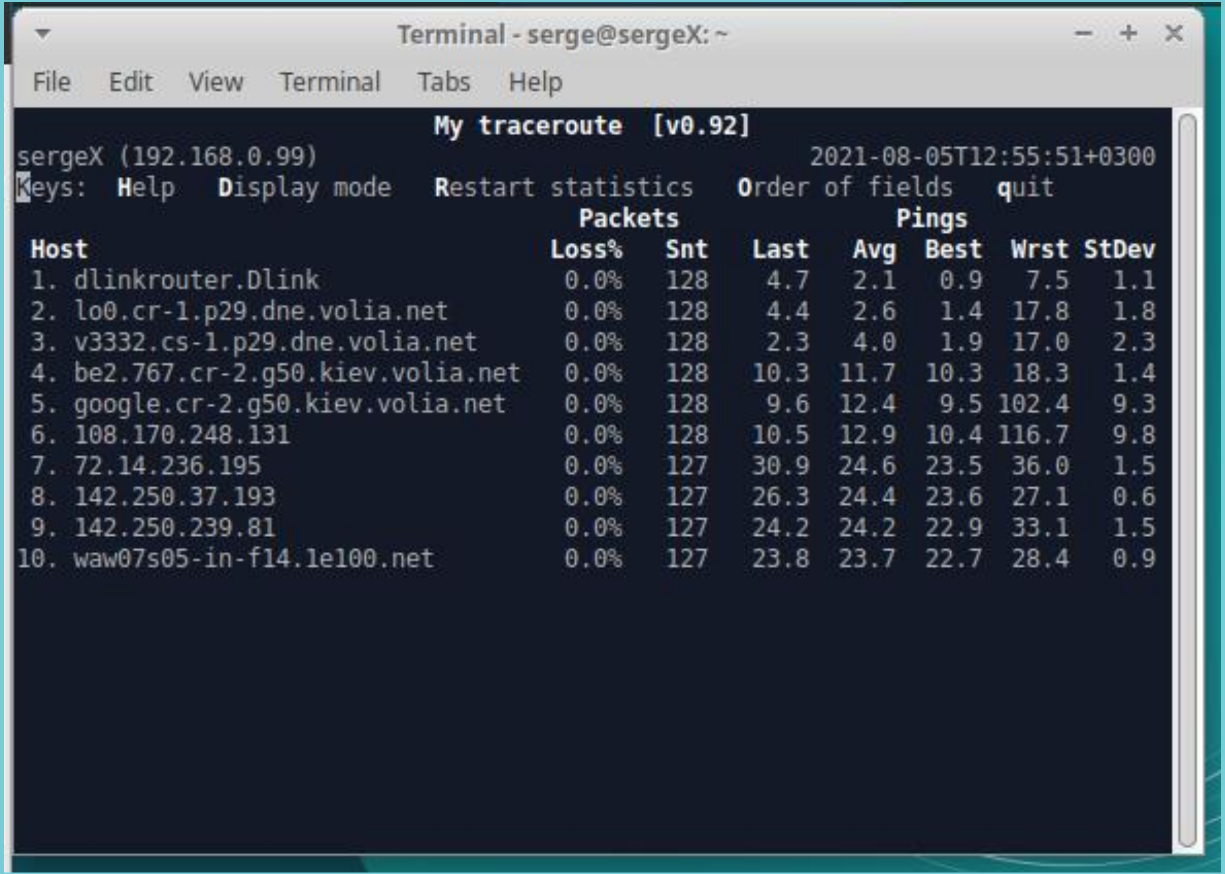
The syntax of the command is as follows:

mtr <options> hostname/IP

Monitoring / Debugging / Troubleshooting

mtr

mtr <options> hostname/IP



```
                         My traceroute  [v0.92]
sergeX (192.168.0.99)                              2021-08-05T12:55:51+0300
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                       Packets               Pings
 Host                                Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. dlinkrouter.Dlink                 0.0%   128    4.7   2.1   0.9   7.5   1.1
 2. lo0.cr-1.p29.dne.volia.net        0.0%   128    4.4   2.6   1.4  17.8   1.8
 3. v3332.cs-1.p29.dne.volia.net      0.0%   128    2.3   4.0   1.9  17.0   2.3
 4. be2.767.cr-2.g50.kiev.volia.net   0.0%   128   10.3  11.7  10.3  18.3   1.4
 5. google.cr-2.g50.kiev.volia.net    0.0%   128    9.6  12.4   9.5 102.4   9.3
 6. 108.170.248.131                   0.0%   128   10.5  12.9  10.4 116.7   9.8
 7. 72.14.236.195                     0.0%   127   30.9  24.6  23.5  36.0   1.5
 8. 142.250.37.193                    0.0%   127   26.3  24.4  23.6  27.1   0.6
 9. 142.250.239.81                    0.0%   127   24.2  24.2  22.9  33.1   1.5
10. waw07s05-in-f14.1e100.net         0.0%   127   23.8  23.7  22.7  28.4   0.9
```

Monitoring / Debugging / Troubleshooting

Show numeric IP addresses (if you use -g, you will get IP addresses (numbers) instead of hostnames):

```
# mtr -g google.com
```

Show the numeric IP addresses and hostnames, too:

```
# mtr -b google.com
```

Set the number of pings that you want to send:

```
# mtr -c 10 google.com
```

Get a report of the mtr command result:

```
# mtr -r -c 10 google.com > mtr-command-google-output
```

or:

```
[root@server ~]# mtr -rw -c 10 google.com > mtr-command-google-output
```

Force the use of the TCP instead of the ICMP:

```
# mtr –tcp google.com
```

Force the use of the UDP instead of the ICMP:

```
# mtr –udp google.com
```

Set the maximum amount of hops:

```
# mtr -m 35 216.58.223.78
```

Define the packet size:

```
# mtr -r -s 50 google.com
```

Print to CSV output:

```
# mtr –csv google.com
```

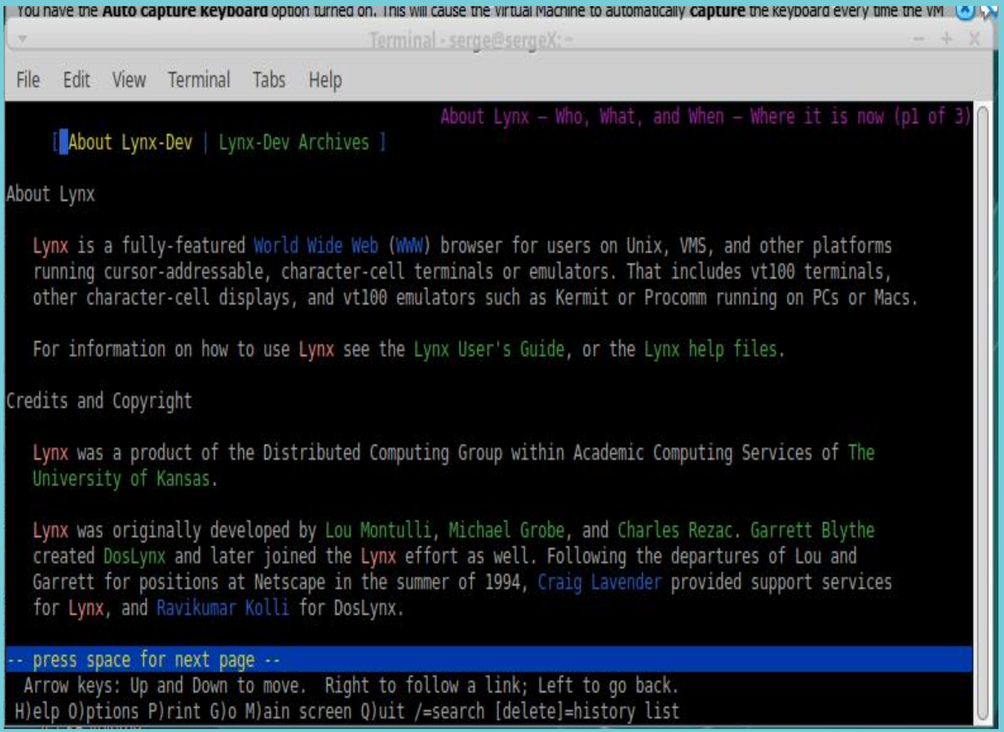
Print to XML output:

```
# mtr –xml google.com
```

Monitoring / Debugging / Troubleshooting

Lynx is a customizable text-based web browser for use on cursor-addressable character cell terminals. As of 2021, it is the oldest web browser still being maintained, having started in 1992.

Links is an open source text and graphic web browser with a pull-down menu system.[3] It renders complex pages, has partial HTML 4.0 support (including tables and frames[4] and support for multiple character sets such as UTF-8), supports color and monochrome terminals and allows horizontal scrolling.

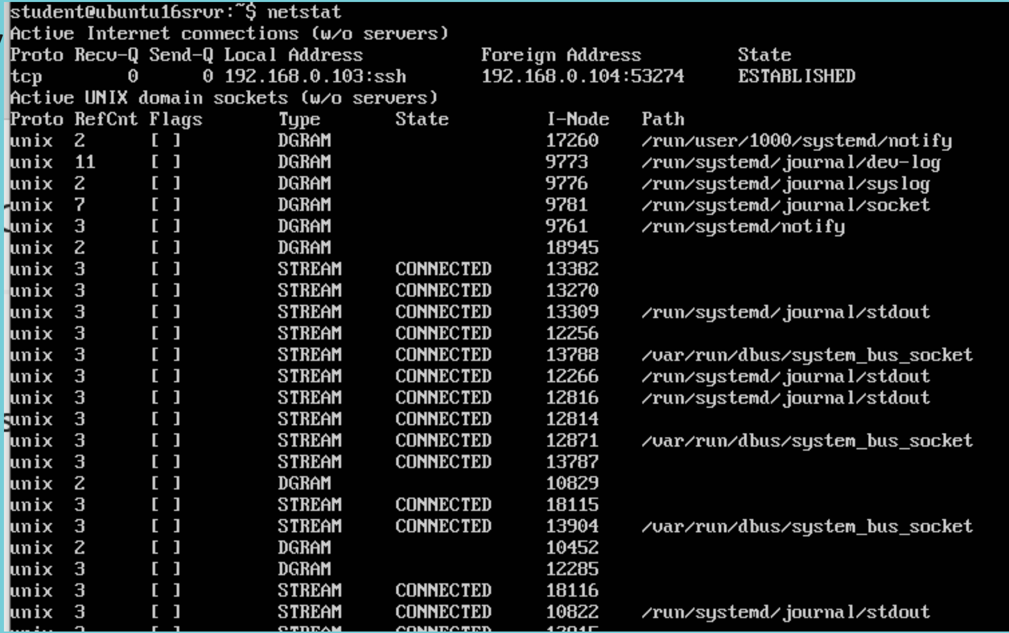


You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM

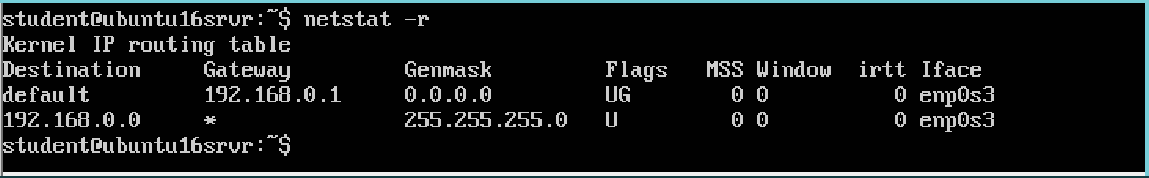
```
                                     About Lynx – Who, What, and When – Where it is now (p1 of 3)
     [ About Lynx-Dev | Lynx-Dev Archives ]

About Lynx

   Lynx is a fully-featured World Wide Web (WWW) browser for users on Unix, VMS, and other platforms
   running cursor-addressable, character-cell terminals or emulators. That includes vt100 terminals,
   other character-cell displays, and vt100 emulators such as Kermit or Procomm running on PCs or Macs.

   For information on how to use Lynx see the Lynx User's Guide, or the Lynx help files.

Credits and Copyright

   Lynx was a product of the Distributed Computing Group within Academic Computing Services of The
   University of Kansas.

   Lynx was originally developed by Lou Montulli, Michael Grobe, and Charles Rezac. Garrett Blythe
   created DosLynx and later joined the Lynx effort as well. Following the departures of Lou and
   Garrett for positions at Netscape in the summer of 1994, Craig Lavender provided support services
   for Lynx, and Ravikumar Kolli for DosLynx.

-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Monitoring / Debugging / Troubleshooting

Netstat (Network Statistic) command display connection info, routing table information etc. To displays routing table information use option as **-r**.



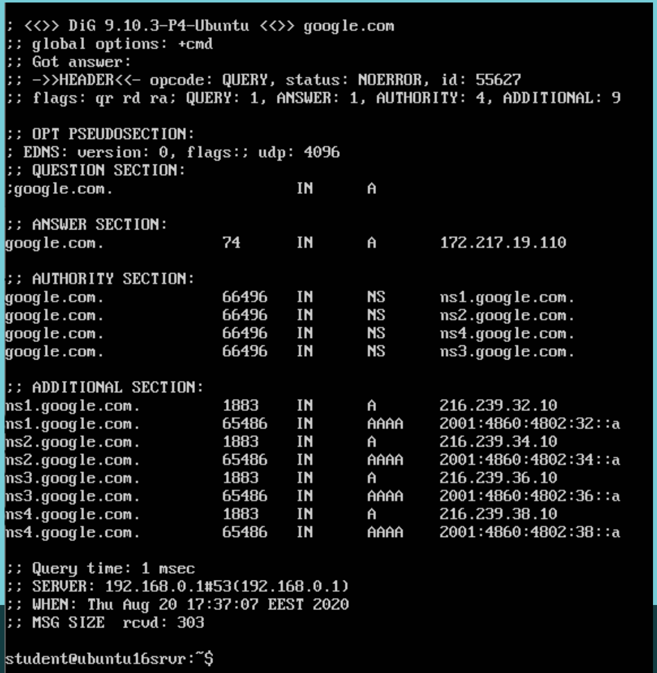
```
student@ubuntu16srvr:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.0.103:ssh       192.168.0.104:53274     ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    17260    /run/user/1000/systemd/notify
unix  11     [ ]         DGRAM                    9773     /run/systemd/journal/dev-log
unix  2      [ ]         DGRAM                    9776     /run/systemd/journal/syslog
unix  7      [ ]         DGRAM                    9781     /run/systemd/journal/socket
unix  3      [ ]         DGRAM                    9761     /run/systemd/notify
unix  2      [ ]         DGRAM                    18945
unix  3      [ ]         STREAM     CONNECTED     13382
unix  3      [ ]         STREAM     CONNECTED     13270
unix  3      [ ]         STREAM     CONNECTED     13309    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12256
unix  3      [ ]         STREAM     CONNECTED     13788    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     12266    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12816    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     12814
unix  3      [ ]         STREAM     CONNECTED     12871    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     13787
unix  2      [ ]         DGRAM                    10829
unix  3      [ ]         STREAM     CONNECTED     18115
unix  3      [ ]         STREAM     CONNECTED     13904    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    10452
unix  3      [ ]         DGRAM                    12285
unix  3      [ ]         STREAM     CONNECTED     18116
unix  3      [ ]         STREAM     CONNECTED     10822    /run/systemd/journal/stdout
```



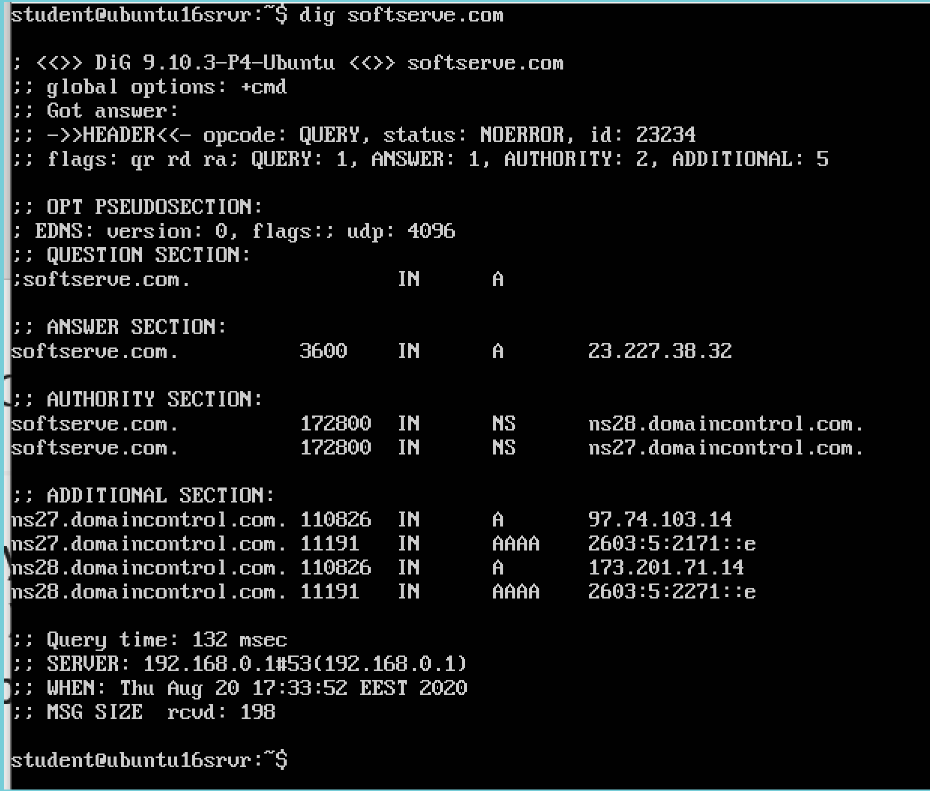
```
student@ubuntu16srvr:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.0.1     0.0.0.0         UG        0 0          0 enp0s3
192.168.0.0     *               255.255.255.0   U         0 0          0 enp0s3
student@ubuntu16srvr:~$
```

Monitoring / Debugging / Troubleshooting

Dig (domain information groper), ***dig*** query DNS Related information like A Record, CNAME, MX Record etc. This command mainly use to troubleshoot DNS related query



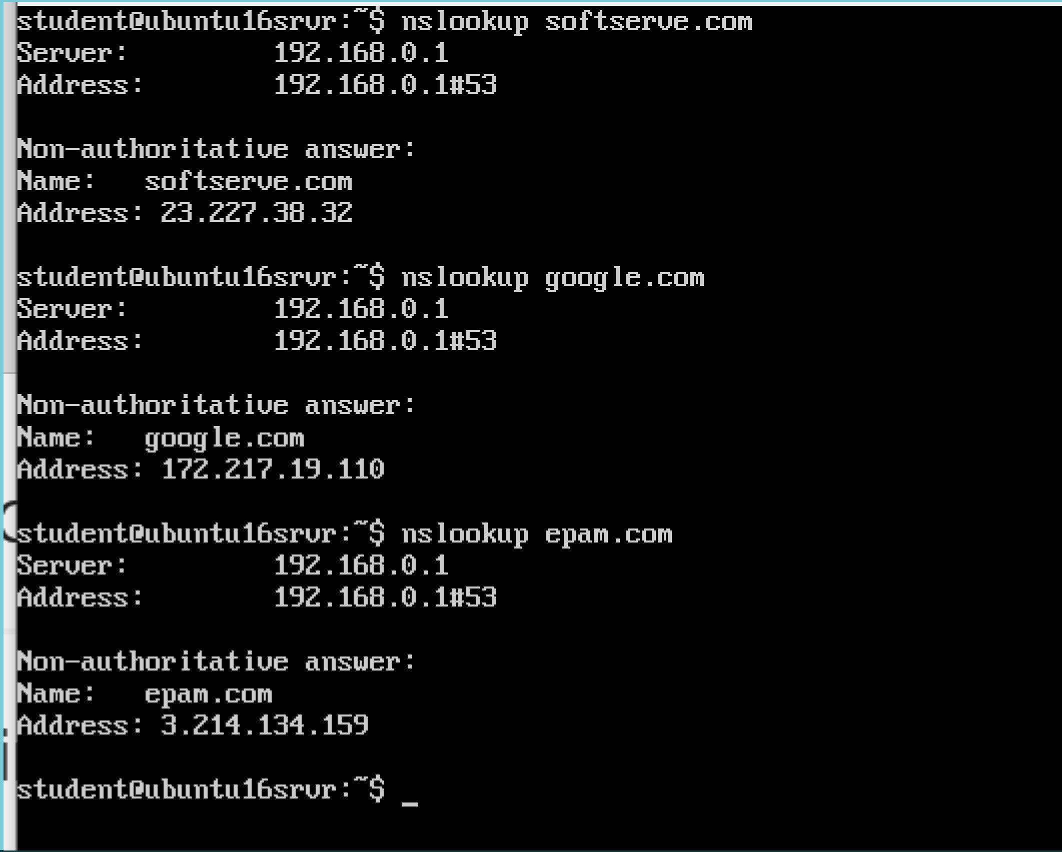
```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55627
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             74      IN      A       172.217.19.110

;; AUTHORITY SECTION:
google.com.             66496   IN      NS      ns1.google.com.
google.com.             66496   IN      NS      ns2.google.com.
google.com.             66496   IN      NS      ns4.google.com.
google.com.             66496   IN      NS      ns3.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         1883    IN      A       216.239.32.10
ns1.google.com.         65486   IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         1883    IN      A       216.239.34.10
ns2.google.com.         65486   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         1883    IN      A       216.239.36.10
ns3.google.com.         65486   IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         1883    IN      A       216.239.38.10
ns4.google.com.         65486   IN      AAAA    2001:4860:4802:38::a

;; Query time: 1 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Aug 20 17:37:07 EEST 2020
;; MSG SIZE  rcvd: 303

student@ubuntu16srvr:~$
```



```
student@ubuntu16srvr:~$ dig softserve.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> softserve.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23234
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;softserve.com.                 IN      A

;; ANSWER SECTION:
softserve.com.          3600    IN      A       23.227.38.32

;; AUTHORITY SECTION:
softserve.com.          172800  IN      NS      ns28.domaincontrol.com.
softserve.com.          172800  IN      NS      ns27.domaincontrol.com.

;; ADDITIONAL SECTION:
ns27.domaincontrol.com. 110826  IN      A       97.74.103.14
ns27.domaincontrol.com. 11191   IN      AAAA    2603:5:2171::e
ns28.domaincontrol.com. 110826  IN      A       173.201.71.14
ns28.domaincontrol.com. 11191   IN      AAAA    2603:5:2271::e

;; Query time: 132 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Thu Aug 20 17:33:52 EEST 2020
;; MSG SIZE  rcvd: 198

student@ubuntu16srvr:~$
```

Monitoring / Debugging / Troubleshooting

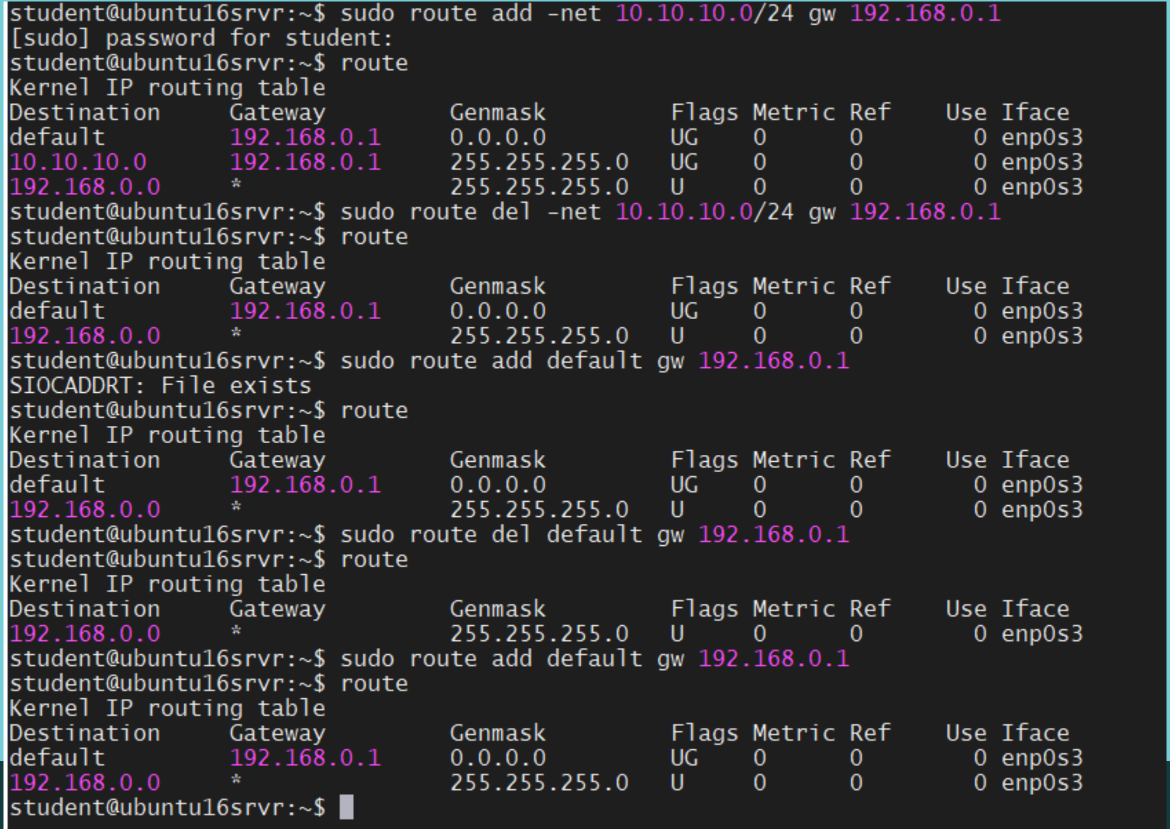
nslookup command also use to find out **DNS** related query



```
student@ubuntu16srvr:~$ nslookup softserve.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   softserve.com
Address: 23.227.38.32

student@ubuntu16srvr:~$ nslookup google.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.19.110

student@ubuntu16srvr:~$ nslookup epam.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   epam.com
Address: 3.214.134.159

student@ubuntu16srvr:~$ _
```

Monitoring / Debugging / Troubleshooting

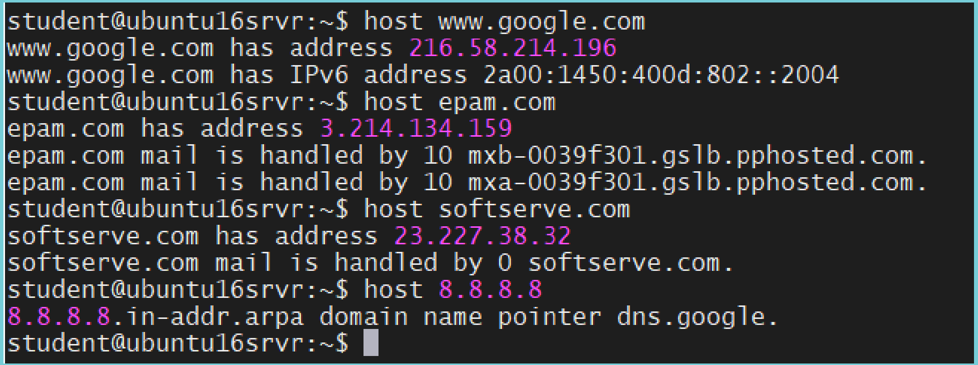
route command also shows and manipulate ip routing table.



```
student@ubuntu16srvr:~$ sudo route add -net 10.10.10.0/24 gw 192.168.0.1
[sudo] password for student:
student@ubuntu16srvr:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.1     0.0.0.0         UG    0      0        0 enp0s3
10.10.10.0      192.168.0.1     255.255.255.0   UG    0      0        0 enp0s3
192.168.0.0     *               255.255.255.0   U     0      0        0 enp0s3
student@ubuntu16srvr:~$ sudo route del -net 10.10.10.0/24 gw 192.168.0.1
student@ubuntu16srvr:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.1     0.0.0.0         UG    0      0        0 enp0s3
192.168.0.0     *               255.255.255.0   U     0      0        0 enp0s3
student@ubuntu16srvr:~$ sudo route add default gw 192.168.0.1
SIOCADDRT: File exists
student@ubuntu16srvr:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.1     0.0.0.0         UG    0      0        0 enp0s3
192.168.0.0     *               255.255.255.0   U     0      0        0 enp0s3
student@ubuntu16srvr:~$ sudo route del default gw 192.168.0.1
student@ubuntu16srvr:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     *               255.255.255.0   U     0      0        0 enp0s3
student@ubuntu16srvr:~$ sudo route add default gw 192.168.0.1
student@ubuntu16srvr:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.1     0.0.0.0         UG    0      0        0 enp0s3
192.168.0.0     *               255.255.255.0   U     0      0        0 enp0s3
student@ubuntu16srvr:~$ 
```

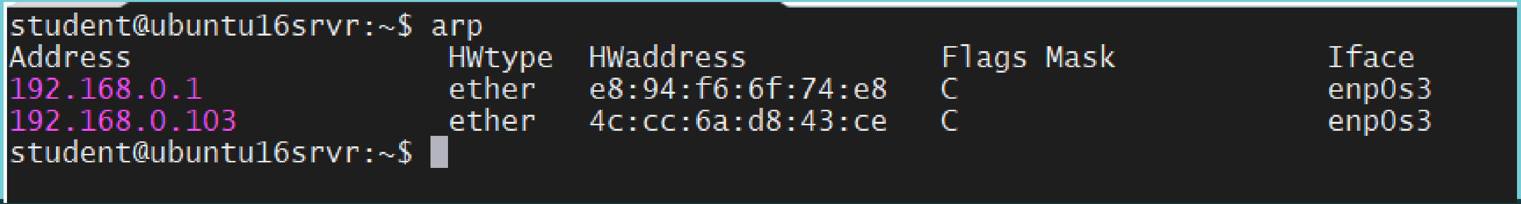
Monitoring / Debugging / Troubleshooting

host command to find name to IP or IP to name in IPv4 or IPv6 and also query DNS records.



```
student@ubuntu16srvr:~$ host www.google.com
www.google.com has address 216.58.214.196
www.google.com has IPv6 address 2a00:1450:400d:802::2004
student@ubuntu16srvr:~$ host epam.com
epam.com has address 3.214.134.159
epam.com mail is handled by 10 mxb-0039f301.gslb.pphosted.com.
epam.com mail is handled by 10 mxa-0039f301.gslb.pphosted.com.
student@ubuntu16srvr:~$ host softserve.com
softserve.com has address 23.227.38.32
softserve.com mail is handled by 0 softserve.com.
student@ubuntu16srvr:~$ host 8.8.8.8
8.8.8.8.in-addr.arpa domain name pointer dns.google.
student@ubuntu16srvr:~$
```

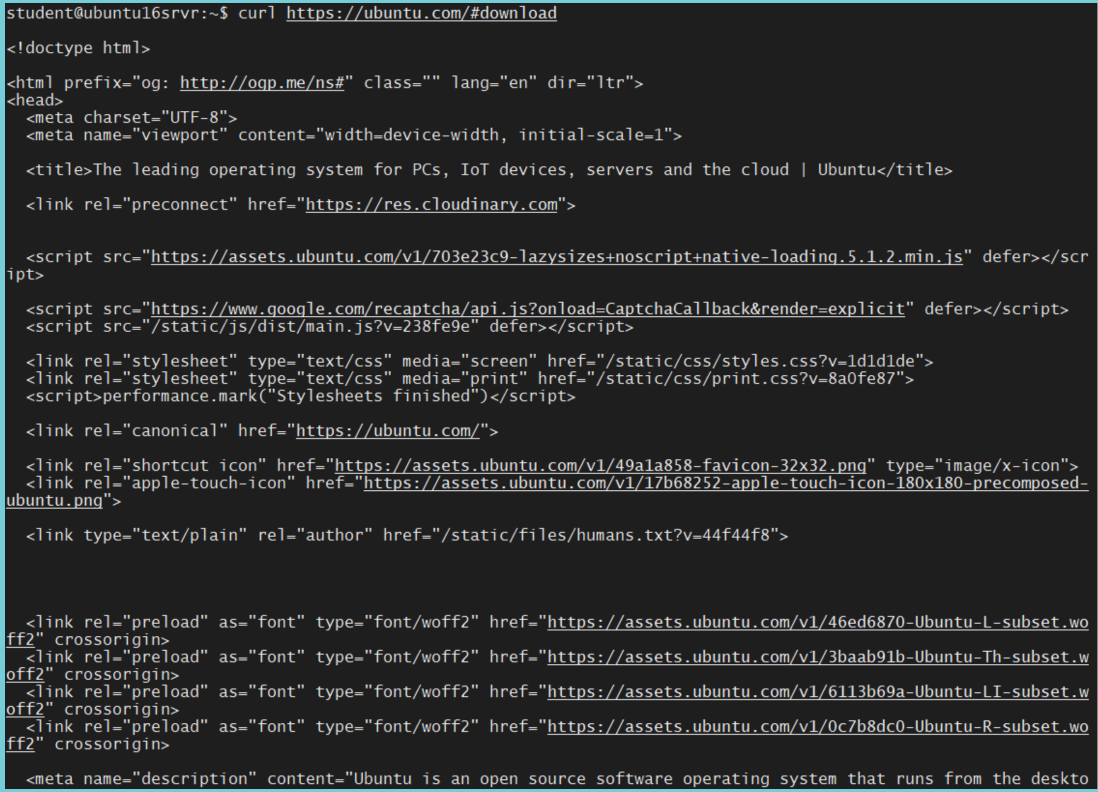
ARP (Address Resolution Protocol)
arp is useful to view / add the contents of the kernel's ARP tables. To see default table use the command as



```
student@ubuntu16srvr:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.1              ether   e8:94:f6:6f:74:e8   C                     enp0s3
192.168.0.103            ether   4c:cc:6a:d8:43:ce   C                     enp0s3
student@ubuntu16srvr:~$
```

Monitoring / Debugging / Troubleshooting

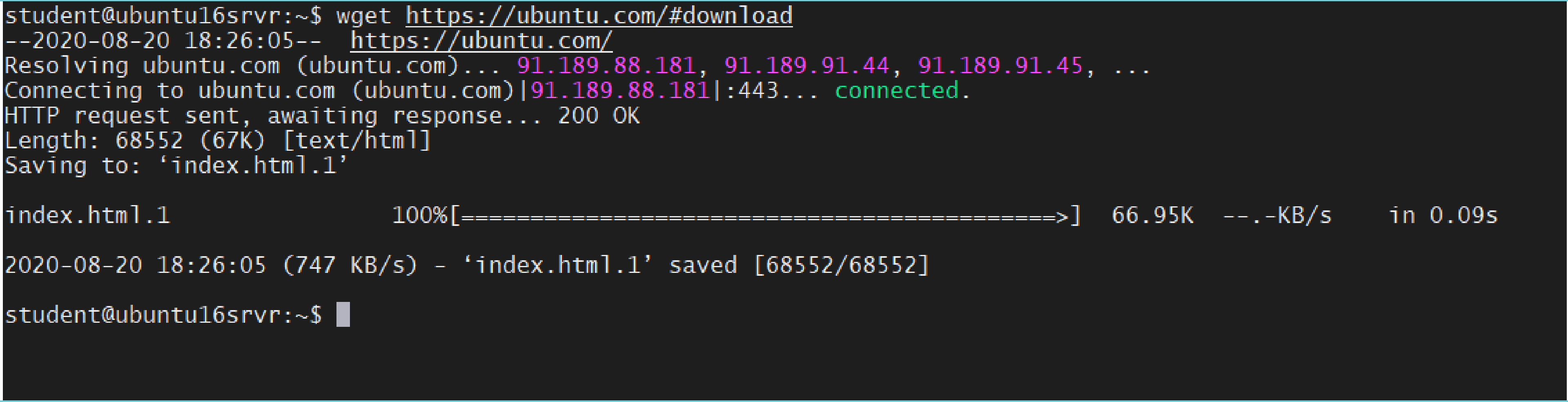
(cURL) ***curl*** is a command-line tool for getting or sending data including files using URL syntax. Since cURL uses libcurl, it supports every protocol libcurl supports



```
student@ubuntu16srvr:~$ curl https://ubuntu.com/#download

<!doctype html>

<html prefix="og: http://ogp.me/ns#" class="" lang="en" dir="ltr">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">

  <title>The leading operating system for PCs, IoT devices, servers and the cloud | Ubuntu</title>

  <link rel="preconnect" href="https://res.cloudinary.com">


  <script src="https://assets.ubuntu.com/v1/703e23c9-lazysizes+noscript+native-loading.5.1.2.min.js" defer></scr
ipt>

  <script src="https://www.google.com/recaptcha/api.js?onload=CaptchaCallback&render=explicit" defer></script>
  <script src="/static/js/dist/main.js?v=238fe9e" defer></script>

  <link rel="stylesheet" type="text/css" media="screen" href="/static/css/styles.css?v=1d1d1de">
  <link rel="stylesheet" type="text/css" media="print" href="/static/css/print.css?v=8a0fe87">
  <script>performance.mark("Stylesheets finished")</script>

  <link rel="canonical" href="https://ubuntu.com/">

  <link rel="shortcut icon" href="https://assets.ubuntu.com/v1/49a1a858-favicon-32x32.png" type="image/x-icon">
  <link rel="apple-touch-icon" href="https://assets.ubuntu.com/v1/17b68252-apple-touch-icon-180x180-precomposed-
ubuntu.png">

  <link type="text/plain" rel="author" href="/static/files/humans.txt?v=44f44f8">




  <link rel="preload" as="font" type="font/woff2" href="https://assets.ubuntu.com/v1/46ed6870-Ubuntu-L-subset.wo
ff2" crossorigin>
  <link rel="preload" as="font" type="font/woff2" href="https://assets.ubuntu.com/v1/3baab91b-Ubuntu-Th-subset.w
off2" crossorigin>
  <link rel="preload" as="font" type="font/woff2" href="https://assets.ubuntu.com/v1/6113b69a-Ubuntu-LI-subset.w
off2" crossorigin>
  <link rel="preload" as="font" type="font/woff2" href="https://assets.ubuntu.com/v1/0c7b8dc0-Ubuntu-R-subset.wo
ff2" crossorigin>

  <meta name="description" content="Ubuntu is an open source software operating system that runs from the deskto
```

Monitoring / Debugging / Troubleshooting

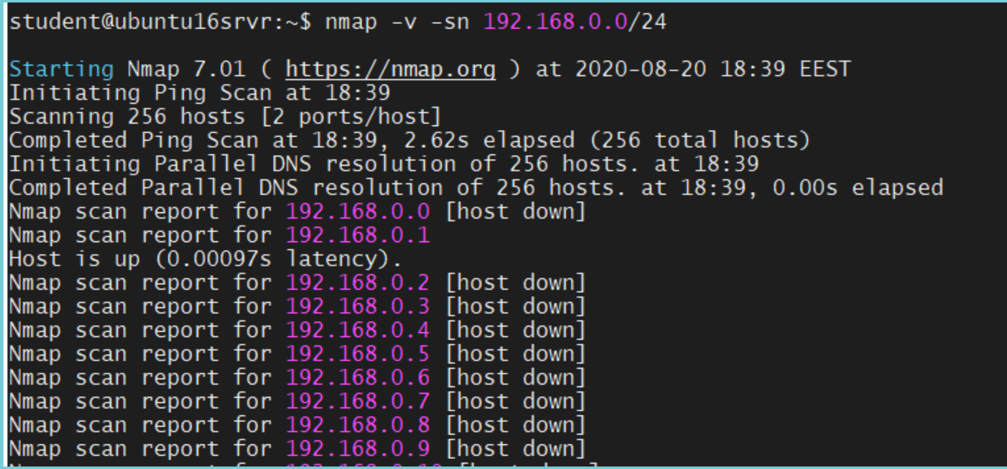
GNU **Wget** is a free utility for non-interactive download of files from the Web. It supports HTTP, HTTPS, and FTP protocols, as well as retrieval through HTTP proxies.
Wget is non-interactive, meaning that it can work in the background, while the user is not logged on.
This allows you to start a retrieval and disconnect from the system, letting Wget finish the work. By contrast, most of the Web browsers require constant user’s presence, which can be a great hindrance when transferring a lot of data.



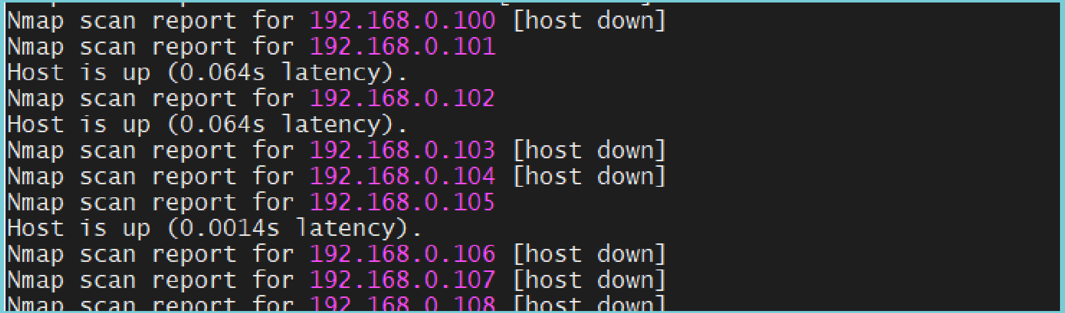
```
student@ubuntu16srvr:~$ wget https://ubuntu.com/#download
--2020-08-20 18:26:05--  https://ubuntu.com/
Resolving ubuntu.com (ubuntu.com)... 91.189.88.181, 91.189.91.44, 91.189.91.45, ...
Connecting to ubuntu.com (ubuntu.com)|91.189.88.181|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68552 (67K) [text/html]
Saving to: ‘index.html.1’

index.html.1                100%[===========================================>]  66.95K  --.-KB/s    in 0.09s

2020-08-20 18:26:05 (747 KB/s) - ‘index.html.1’ saved [68552/68552]

student@ubuntu16srvr:~$ 
```

Monitoring / Debugging / Troubleshooting

Nmap ("Network Mapper"), ***nmap*** is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.



```
student@ubuntu16srvr:~$ nmap -v -sn 192.168.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2020-08-20 18:39 EEST
Initiating Ping Scan at 18:39
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 18:39, 2.62s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 18:39
Completed Parallel DNS resolution of 256 hosts. at 18:39, 0.00s elapsed
Nmap scan report for 192.168.0.0 [host down]
Nmap scan report for 192.168.0.1
Host is up (0.00097s latency).
Nmap scan report for 192.168.0.2 [host down]
Nmap scan report for 192.168.0.3 [host down]
Nmap scan report for 192.168.0.4 [host down]
Nmap scan report for 192.168.0.5 [host down]
Nmap scan report for 192.168.0.6 [host down]
Nmap scan report for 192.168.0.7 [host down]
Nmap scan report for 192.168.0.8 [host down]
Nmap scan report for 192.168.0.9 [host down]
```

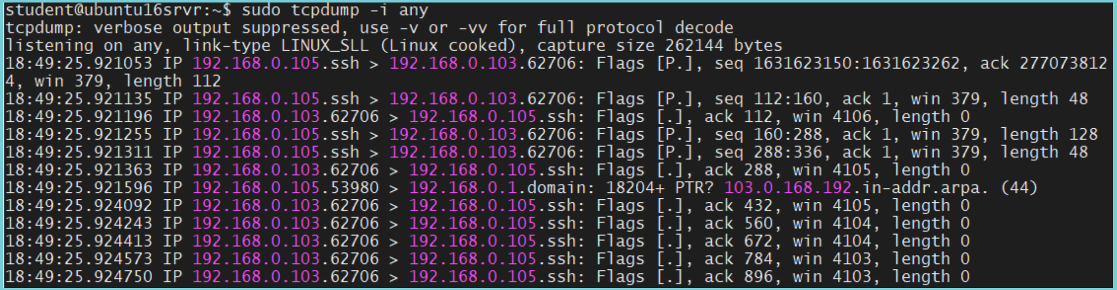


```
Nmap scan report for 192.168.0.100 [host down]
Nmap scan report for 192.168.0.101
Host is up (0.064s latency).
Nmap scan report for 192.168.0.102
Host is up (0.064s latency).
Nmap scan report for 192.168.0.103 [host down]
Nmap scan report for 192.168.0.104 [host down]
Nmap scan report for 192.168.0.105
Host is up (0.0014s latency).
Nmap scan report for 192.168.0.106 [host down]
Nmap scan report for 192.168.0.107 [host down]
Nmap scan report for 192.168.0.108 [host down]
```

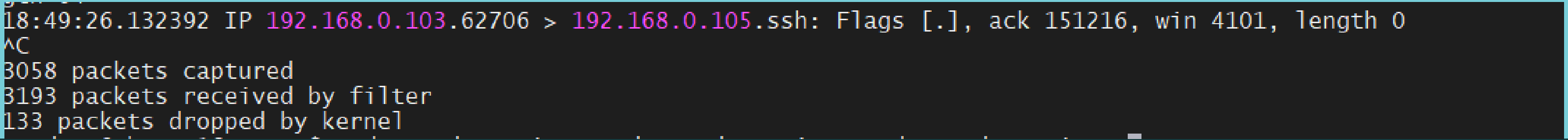
Monitoring / Debugging / Troubleshooting

tcpdump is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool.

A powerful and versatile tool that includes many options and filters, tcpdump can be used in a variety of cases. Since it's a command line tool, it is ideal to run in remote servers or devices for which a GUI is not available, to collect data that can be analyzed later. It can also be launched in the background or as a scheduled job using tools like cron.



```
student@ubuntu16srvr:~$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
18:49:25.921053 IP 192.168.0.105.ssh > 192.168.0.103.62706: Flags [P.], seq 1631623150:1631623262, ack 277073812
4, win 379, length 112
18:49:25.921135 IP 192.168.0.105.ssh > 192.168.0.103.62706: Flags [P.], seq 112:160, ack 1, win 379, length 48
18:49:25.921196 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 112, win 4106, length 0
18:49:25.921255 IP 192.168.0.105.ssh > 192.168.0.103.62706: Flags [P.], seq 160:288, ack 1, win 379, length 128
18:49:25.921311 IP 192.168.0.105.ssh > 192.168.0.103.62706: Flags [P.], seq 288:336, ack 1, win 379, length 48
18:49:25.921363 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 288, win 4105, length 0
18:49:25.921596 IP 192.168.0.105.53980 > 192.168.0.1.domain: 18204+ PTR? 103.0.168.192.in-addr.arpa. (44)
18:49:25.924092 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 432, win 4105, length 0
18:49:25.924243 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 560, win 4104, length 0
18:49:25.924413 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 672, win 4104, length 0
18:49:25.924573 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 784, win 4103, length 0
18:49:25.924750 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 896, win 4103, length 0
```



```
18:49:26.132392 IP 192.168.0.103.62706 > 192.168.0.105.ssh: Flags [.], ack 151216, win 4101, length 0
^C
3058 packets captured
3193 packets received by filter
133 packets dropped by kernel
```

How to connect

- https://www.youtube.com/watch?v=8V4Ez4NUHAk
- https://stackoverflow.com/questions/44238395/connect-two-virtualbox-machine
- https://www.virtualbox.org/manual/ch06.html

QUESTIONS & ANSWERS

THANK YOU!