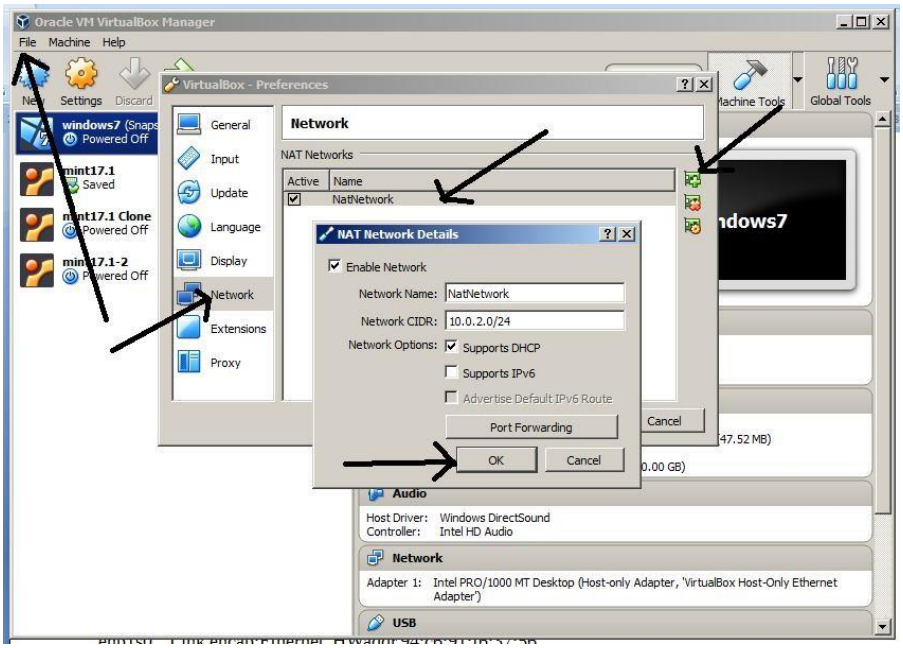
Lab 09 – Network Management Commands

Enable internet on Linux VM.

- **Communicate between Guest and Host using ping command.**

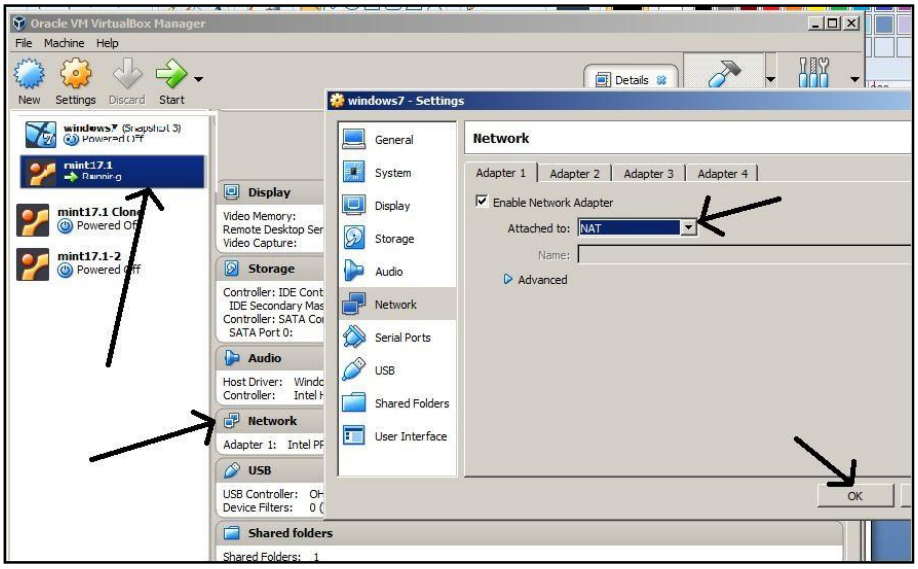
  Host **Virtual Box Manager Settings:**

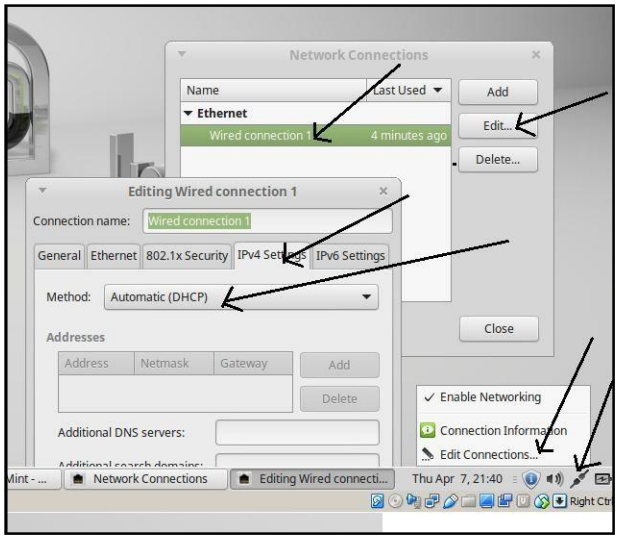
  5. In Virtual Box Manager, Select "**File**", → "**Preferences**" → Network → Host only Networks (Tab).
  6. Select icon for adding "**New Host only Networks**" (See vboxnet0 gets added"
  7. Change the properties of vboxnet0
  8. By default network CIDR is 10.0.2.0/24. Click OK.



Guest **VBM Settings in Virtual Box:**

- Select Guest OS in Virtual Box. Select settings for Network.
- Change the settings for Network. - Select "**Adapter 1**" Tab – Change "**Attached to**" to "**NAT**"
- Go to Guest OS. And make sure that in Guest OS, setting has been made in network connection, as obtain IP address in DHCP mode..


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details
windows7 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Enable Network Adapter
Attached to: NAT
Name:
Advanced
OK
mint17.1
mint17.1 Clone
mint17.1-2
Display
Storage
Audio
Network
USB
Shared folders


Network Connections
Name
Last Used
Add
Ethernet
Wired connection 1
4 minutes ago
Edit...
Delete...
Editing Wired connection 1
Connection name: Wired connection 1
General Ethernet 802.1x Security IPv4 Settings IPv6 Settings
Method: Automatic (DHCP)
Addresses
Address Netmask Gateway
Add
Delete
Additional DNS servers:
Close
Enable Networking
Connection Information
Edit Connections...
Network Connections
Editing Wired connecti...
Thu Apr 7, 21:40

=== * ===

Test and manage network using following commands

ifconfig:

- **ifconfig**(interface configuration) is used to configure the kernel-resident network interfaces.

Example 1: ifconfig -a

- **-a :** This option is used to display all the interfaces available, even if they are down.
- **Output: ifconfig -a**

```
enp1s0    Link encap:Ethernet  HWaddr 94:c6:91:f6:37:56
          inet addr:172.16.20.107  Bcast:172.16.20.255  Mask:255.255.255.0
          inet6 addr: fe80::ef4b:1b1d:5c61:d9c6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61890 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44175 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24167103 (24.1 MB)  TX bytes:6512965 (6.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:15869 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15869 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1729018 (1.7 MB)  TX bytes:1729018 (1.7 MB)
```

Example 2: ifconfig –s

- **-s :** Display a short list, instead of details.
- **Output: ifconfig -s**

Iface	MTU	Met	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
enp1s0	1500	0	62065	0	0	0	44236	0	0	0	BMRU
lo	65536	0	15869	0	0	0	15869	0	0	0	LRU

iwconf ig:

- **iwconfig** command in Linux is like **ifconfig** command, in the sense it works with kernel-resident network interface but it is dedicated to wireless networking interfaces only.

ethtool:

- ethtool utility is used to view and change the ethernet device parameters.

Example 1: List Ethernet Device Properties

- When user executes ethtool command with a device name, it displays the following information about the Ethernet device.

- **ethtool enp1s0**

```
Settings for enp1s0:
        Supported ports: [ TP MII ]
        Supported link modes: 10baseT/Half 10baseT/Full
                              100baseT/Half 100baseT/Full
                              1000baseT/Half 1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Advertised link modes: 10baseT/Half 10baseT/Full
                               100baseT/Half 100baseT/Full
                               1000baseT/Full
        Advertised pause frame use: Symmetric Receive-only
        Advertised auto-negotiation: Yes
        Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                             100baseT/Half 100baseT/Full
                                             1000baseT/Full
        Link partner advertised pause frame use: No
        Link partner advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: MII
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: pumbg
        Wake-on: g
        Current message level: 0x00000033 (51)
                               drv probe ifdown ifup
        Link detected: yes
```

Example 3: Use ethtool -S option to display the bytes transferred, received, errors, etc

- **ethtool -S enp1s0**

```
NIC statistics:
    tx_packets: 42257
    rx_packets: 57556
    tx_errors: 0
    rx_errors: 33
    rx_missed: 0
    align_errors: 0
    tx_single_collisions: 0
    tx_multi_collisions: 0
    unicast: 42095
    broadcast: 11512
    multicast: 3949
```

arpwatch:

- **arpwatch** is an open source computer software program that helps user to monitor **Ethernet** traffic activity (like **Changing IP** and **MAC Addresses**) on network and maintains a database of **ethernet/ip** address pairings.
- This tool is especially useful for **Network administrators** to keep a watch on **ARP activity** to detect **ARP spoofing** or unexpected **IP/MAC** addresses modifications.

Example 1: To watch a specific interface, type the following command with '-i' and device name.

- **arpwatch -i enp1s0**
    - So, whenever a new MAC is plugged or a particular IP is changing his MAC address on the network, user can notice **syslog** entries at '**/var/log/syslog**' or '**/var/log/message**' file.
- **Output:**

tail -10 /var/log/syslog

tail -10 /var/log/syslog

Apr 4 11:34:21 admincs-To-be-filled-by-O-E-M arpwatch: reaper: pid 4547, exit status 1

Apr 4 11:38:23 admincs-To-be-filled-by-O-E-M arpwatch: new station 172.16.20.26 e2:7b:55:83:d3:a1 enp1s0

Apr 4 11:38:23 admincs-To-be-filled-by-O-E-M arpwatch: new station 172.16.20.52 e2:7b:55:83:d3:a1 enp1s0

Apr 4 11:38:23 admincs-To-be-filled-by-O-E-M arpwatch: execl: /usr/lib/sendmail: No such file or directory

Apr 4 11:38:23 admincs-To-be-filled-by-O-E-M arpwatch: reaper: pid 4587, exit status 1

Apr 4 11:38:23 admincs-To-be-filled-by-O-E-M arpwatch: execl: /usr/lib/sendmail: No such file or directory

Apr 4 11:38:23 admincs-To-be-filled-by-O-E-M arpwatch: reaper: pid 4588, exit status 1

Apr 4 11:42:37 admincs-To-be-filled-by-O-E-M cinnamon-screensaver-pam-helper: pam_ecryptfs: seteuid error

Apr 4 11:43:10 admincs-To-be-filled-by-O-E-M kernel: [1664.202203] device enp1s0 entered promiscuous mode

Apr 4 11:43:10 admincs-To-be-filled-by-O-E-M arpwatch: listening on enp1s0

- User can also check current **ARP** table, by using following command.

    arp -a

    ? (172.16.20.38) at 90:0f:0c:e3:df:07 [ether] on enp1s0

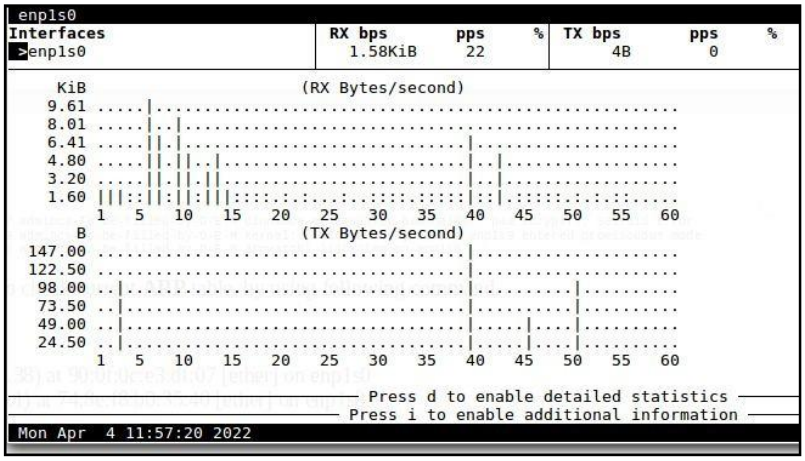
    ? (172.16.20.1) at 74:8e:f8:b0:35:40 [ether] on enp1s0

bmon:

- **bmon** is a simple yet powerful, text-based network monitoring and debugging tool for Unix-like systems, which captures networking related statistics and displays them visually in a human friendly format.

Example 1: bmon -p enp1s0

To view more detailed graphical statistics/information of bandwidth usage, press d key Press [Shift + ?] to view the quick reference. To exit the interface, press **[Shift + ?]** again.



Example 2: bmon -r 5 -p enp1s0 -o ascii

- The output can be viewed in ascii mode also, the output could be collected at regular interval also.
- **Output**

IInterfaces	RX bps	pps	%	TX bps	pps	%
enp1s0	0	0	0	0		
Interfaces	RX bps	pps	%	TX bps	pps	%
enp1s0	5.53KiB	16		0	0	
Interfaces	RX bps	pps	%	TX bps	pps	%
enp1s0	1.85KiB	10		0	0	
Interfaces	RX bps	pps	%	TX bps	pps	%
enp1s0	1.05KiB	10		0	0	
Interfaces	RX bps	pps	%	TX bps	pps	%
enp1s0	4.55KiB	16		41B	0	

wget:

- **wget** is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.
- **Examples:**
  - To simply download a webpage:
    - **wget https://www.google.com/index.html**
  - To download the file in **background**
    - **wget -b https://www.rediff.com/index.html**

netstat

- netstat is a command line utility for Linux that prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
- netstat can be used to diagnose network issues and service problems.
- **Important Options used:**
  - -a: all listening and non-listening ports, -t tcp ports
  - -u udp ports, -l listening ports
  - -s Statistics of ports, -r Kernel Routing Information

Example 1: netstat -at | head // To list all tcp ports.

```
admincs-To-be-filled-by-O-E-M ~ # netstat -at | head
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:smtp          *:*                     LISTEN
tcp        0      0 localhost:submission    *:*                     LISTEN
tcp        0      0 admincs-To-be-fi:domain *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        1      0 172.16.20.107:38096     172.16.20.116:ssh       CLOSE_WAIT
tcp        0      0 172.16.20.107:39984     104.18.72.113:https     ESTABLISHED
```

Example 2: netstat -s // To list the statistics for all ports.

Ip:
102865 total packets received
14 with invalid addresses
0 forwarded
19 with unknown protocol
0 incoming packets discarded
97399 incoming packets delivered

70224 requests sent out
24 outgoing packets dropped
2 dropped because of missing route

Icmp:
77 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
destination unreachable: 77
258 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
destination unreachable: 258

Example 3: netstat -r // Kernel Routing Information

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
default	172.16.20.1	0.0.0.0	UG	0	0	0	enp1s0
link-local	*	255.255.0.0	U	0	0	0	enp1s0
172.16.2.2	172.16.20.1	255.255.255.255	UGH	0	0	0	np1s0
172.16.20.0	*	255.255.255.0	U	0	0	0	enp1s0

ping

- **ping** (Packet Internet Groper) command is used to check the network connectivity between host and server/host.
    - -c : Number of packets to be transfered
    - -w : deadline, with in this seconds, continuesly send the packets ICMP Packets.
    - -s : Packe size

Example 1: **ping -c 5 -s 100 172.16.20.116**

- Will send 5 ICMP Packets to test wheter machine 100.172.16.116 is alive or not, and each packet size data is 100 bytes, total packet size is 108 (8 bytes of header).

Example 2: **ping -w 5 172.16.20.115**

- Will continuously send the ICMP packets within 5 seconds.

traceroute:

- **traceroute** command in Linux prints the route that a packet takes to reach the host.
- This command is useful when user want to know about the route and about all the hops that a packet takes.

Example 1: **traceroute www.google.com**

traceroute to www.google.com (142.250.195.196), 30 hops max, 60 byte packets
1 172.16.20.1 (172.16.20.1) 0.761 ms 1.407 ms 1.973 ms
2 172.16.1.100 (172.16.1.100) 0.137 ms 0.137 ms 0.140 ms
3 117.236.190.194 (117.236.190.194) 7.500 ms 9.117 ms 8.384 ms
4 172.24.64.138 (172.24.64.138) 2.385 ms 2.380 ms 136.232.204.173.static.jio.com (136.232.204.173) 3.082 ms
5 * * *
6 72.14.218.250 (72.14.218.250) 19.051 ms 18.964 ms 19.297 ms
7 * * *
8 216.239.59.230 (216.239.59.230) 20.538 ms maa03s42-in-f4.1e100.net (142.250.195.196) 17.921 ms 216.239.59.230 (216.239.59.230) 20.029 ms

- The first column corresponds to the **hop count**. The second column represents **the address of that hop** and after that, three space-separated time in milliseconds.
    - *traceroute* command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop.

Example 2: **traceroute 172.16.2.10** **//local server**

traceroute to 172.16.2.10 (172.16.2.10), 30 hops max, 60 byte packets
1 172.16.20.1 (172.16.20.1) 0.624 ms 1.013 ms 1.428 ms
2 172.16.2.10 (172.16.2.10) 0.212 ms !X 0.206 ms !X 0.186 ms !X

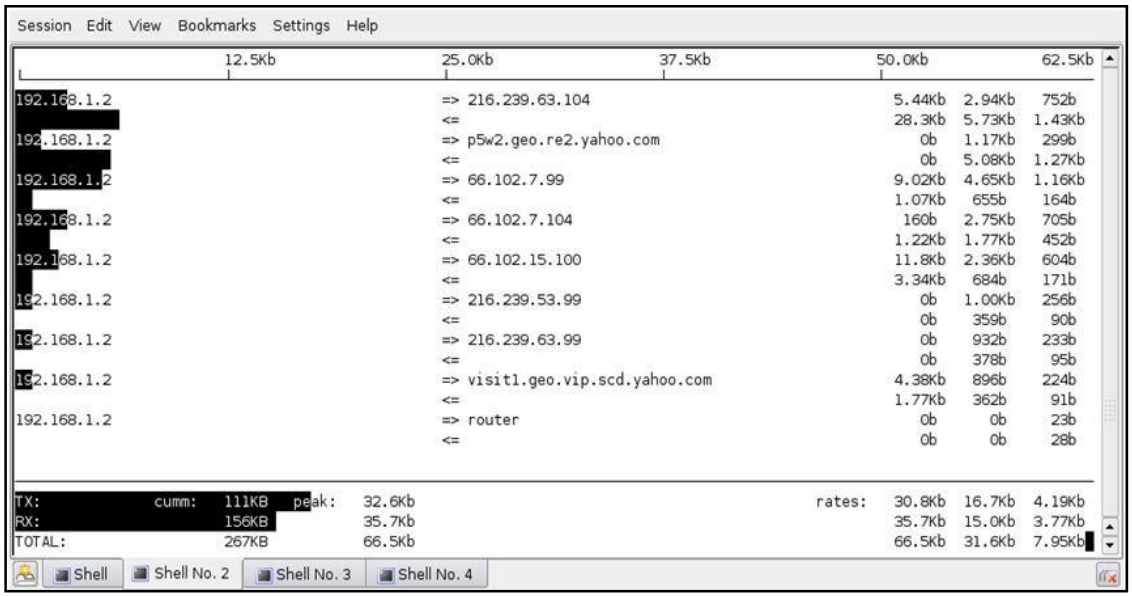
Example 2: traceroute 127.0.0.1 **//local machine**

traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 60 byte packets
1 localhost (127.0.0.1) 0.034 ms 0.010 ms 0.010 ms

iftop

- The **iftop** command listens to network traffic on a named network interface, or on the first interface, it can find which looks like an external interface if none is specified, and **displays a table of current bandwidth usage by pairs of hosts**.

Example 1: iftop -i enp1s0



nload

- **nload** is a Linux command-line tool used to monitor network traffic and bandwidth usage in real time, using insightful graphs and traffic statistics.
- Output of nload is in paragraph, one for each *device*.
  Example: nload -m // -m for multiple devices.
- Output:

```
Device enp1s0 [172.16.20.107] (1/2):
=====================================
Incoming:                Outgoing:
Curr: 1.61 kBit/s          Curr: 0.00 Bit/s
Avg: 1.82 kBit/s           Avg: 456.00 Bit/s
Min: 0.00 Bit/s           Min: 0.00 Bit/s
Max: 34.95 kBit/s            Max: 15.07 kBit/s
Ttl: 76.13 MByte           Ttl: 8.84 MByte

Device lo [127.0.0.1] (2/2):
=====================================
Incoming:                Outgoing:
Curr: 1.30 kBit/s          Curr: 1.30 kBit/s
Avg: 808.00 Bit/s          Avg: 808.00 Bit/s
Min: 0.00 Bit/s           Min: 0.00 Bit/s
Max: 20.16 kBit/s            Max: 20.16 kBit/s
Ttl: 1.53 MByte            Ttl: 1.53 MByte
```

ss

- The **ss** command is a tool used to dump socket statistics
- With ss, user get very detailed information about how Linux machine is communicating with other machines, networks, and services; details about network connections, networking protocol statistics, and Linux socket connections.
- **Some options used:**
  - -t Display TCP sockets, -u Display UDP sockets,
  - -a All Sockets, -l Only Listening Sockets,
  - -4 ipv4 Packets only.

Example 1: ss –t

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	0	172.16.20.107:57818	142.250.182.46:https
ESTAB	0	0	172.16.20.107:48336	34.107.221.82:http
ESTAB	0	0	172.16.20.107:48334	34.107.221.82:http
ESTAB	0	0	172.16.20.107:49542	34.213.33.47:https

tcpdump

- **tcpdump** is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux.It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through system.
- **tcpdump -i enp1s0**
- **Importatnt Options used:**
  - –c Specifice Number of Packets captured
  - –e Print the link-level header on each dump line.

Example 3: tcpdump -c 5 -i enp1s0

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:46:05.519973 IP 172.16.20.63.51082 > 239.255.255.250.1900: UDP, length 173
13:46:05.521176 IP 172.16.20.107.42602 > dns.google.domain: 39493+ PTR?
250.255.255.239.in-addr.arpa. (46)
13:46:05.521196 IP 172.16.20.107.42602 > dns.google.domain: 39493+ PTR?
250.255.255.239.in-addr.arpa. (46)
13:46:05.521206 IP 172.16.20.107.42602 > 172.16.1.100.domain: 39493+ PTR?
250.255.255.239.in-addr.arpa. (46)
13:46:05.521400 IP 172.16.1.100.domain > 172.16.20.107.42602: 39493 NXDomain* 0/0/0 (46)
5 packets captured
17 packets received by filter
7 packets dropped by kernel
```

dstat

- **dstat** is a tool that is used to retrieve information or statistics form components of the system such as network connections, IO devices, or CPU, etc.

- **Some options used:**
  - -c enable cpu stats (system, user, idle, wait, hardware interrupt, software interrupt)
  - **-d**, --disk enable disk stats (read, write) -g, --page enable page stats (page in, page out)
  - **-i**, --int enable interrupt stats -m, --mem enable memory stats (used, buffers, cache, free)
  - -n, --net enable network stats (receive, send) --nocolor
- **Output:**

dstat -n

```
-net/total-
recv     send
  0        0
216B     0
336B   84B
632B     0
6297B   54B
584B    54B
697B   0 ^C
```

dstat -c

```
----total-cpu-usage----
usr sys idl wai hiq siq
  4   1  95   0   0   0
  1   0  98   0   0   0
  2   0  98   0   0   0
  2   1  97   0   0   0^C
```

```
        0x0050:  2627 2829 2a2b 2c2d 2e2f 3031 3233 3435  &'()*+,-./012345
        0x0060:  3637                                     67
1 packet captured
1 packet received by filter
0 packets dropped by kernel
admincs-To-be-filled-by-O-E-M ~ # dstat
You did not select any stats, using -cdngy by default.
----total-cpu-usage---- -dsk/total- -net/total- ---paging-- ---sys
usr sys idl wai hiq siq| read  writ| recv  send|  in   out | int
  4   1  95   0   0   0| 113k  103k|    0     0 |  75B 1199B| 410
  6   5  88   0   0   0|    0     0 | 275B    0 |   0     0 | 467
  2   0  98   0   0   0|    0     0 |    0     0 |   0     0 | 179
  2   1  98   0   0   0|    0     0 | 259B    0 |   0     0 | 164
  2   0  98   0   0   0|    0     0 | 240B  162B|   0     0 | 222
  2   0  98   0   0   0|    0     0 | 276B    0 |   0     0 | 235
  4   0  96   1   0   0|    0    40k| 582B  294B|   0     0 | 278
  3   1  97   0   0   0|    0    96k|6218B  384B|   0     0 | 250
  2   0  98   0   0   0|    0     0 | 216B    0 |   0     0 | 199
  2   0  98   0   0   0|    0     0 | 579B  441B|   0     0 | 259
 11   1  88   0   0   0| 4096B|5879B  147B|   0     0 | 684
  5   1  94   0   0   0|    0     0 | 726B  660B|   0     0 | 329
  6   1  93   0   0   0|    0     0 |    0     0 |   0     0 | 507
  4   2  94   1   0   0|    0    40k|3932B 2443B|   0     0 | 318
 14   2  84   0   0   1|    0     0 | 421B   54B|   0     0 |1035
 15   1  82   0   0   1|    0     0 | 215B    0 |   0     0 |1261
  4   1  95   0   0   0|    0   668k| 386B  171B|   0     0 | 357
 15   3  82   0   0   1|    0     0 |  75k 3585B|   0     0 |1868
```