CS3009D: NETWORK LABORATORY

Assignment 1 - Network Environments

Adeeb Hadi Seeyad (B190737CS)

Introduction

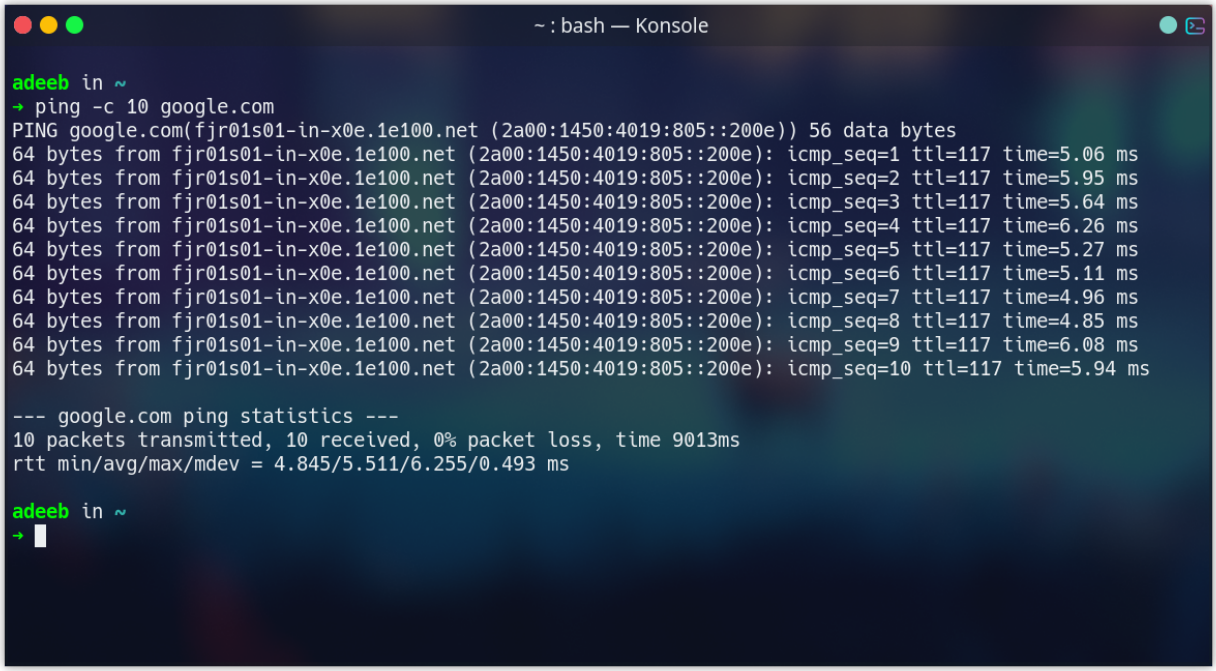
Following tools I used to explore and summarize the network environment available in my system:

1. ping
2. traceroute
3. trancepath
4. ip / ifconfig
5. nslookup
6. whois
7. route
8. tcpdump
9. netstat / ss
10. dstat
11. ifstat
12. wget

1. ping

The ping (Packet Internet Groper) command sends packets of ICMP echo requests to a specific IP address on a network, and then lets you know how long it took to transmit that data and get a response.

Eg. *ping google.com*



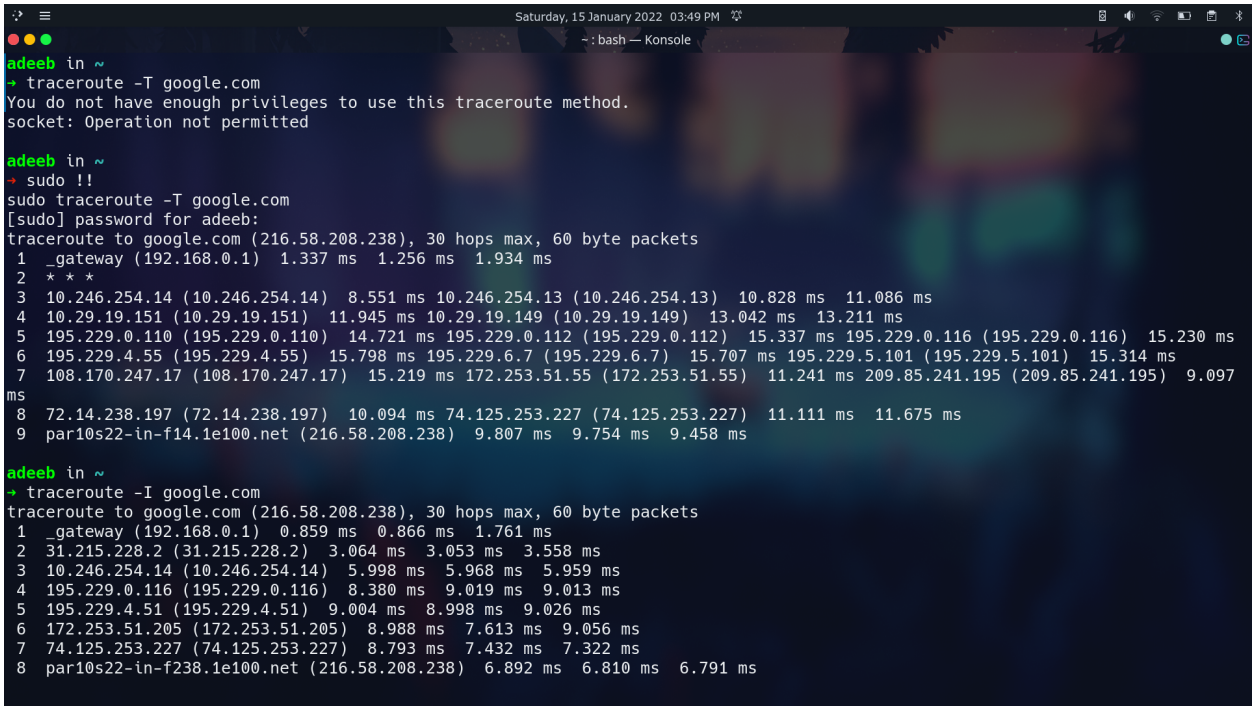
- from : The destination and its IP address.
- icmp_seq : The sequence number of each ICMP packet. Increase by one for every echo request.
- ttl (Time to Live) : represents the number of network hops a packet can take before a router discards it.
- time : The time it took for a packet to reach its destination and come back to the source in milliseconds.

2. traceroute

It sends 3 packets to each intermediate hop to the network host and traces the packets. It displays the ip address of each hop and time taken for the packet to reach each hop. Some of its functionalities require super user privileges.

Eg. *traceroute google.com*

.



- The T flag uses TCP SYN for probs and it requires superuser privileges.
- The I flag uses ICMP ECHO for probs and it does **not** require superuser privileges.

3. tracepath

Tracepath traces a path to a designated network address, reporting on the TTL lag and maximum transmission units (MTU) along the way. This command can be run by any user without superuser privileges unlike traceroute.

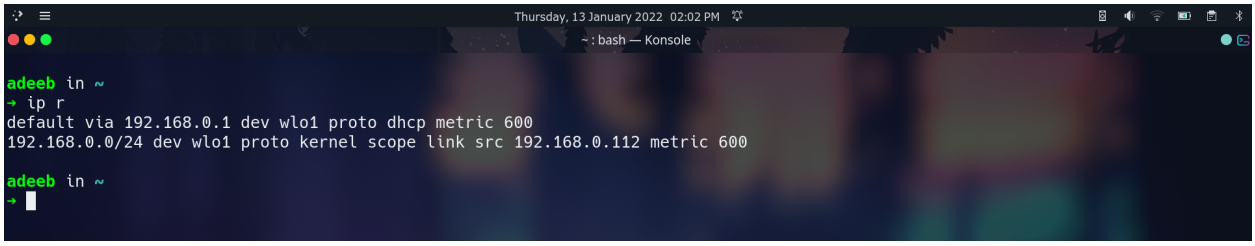
Eg. *tracepath google.com*

4. ip / ifconfig

IP

IP (Internet Protocol) Address is an address of your network hardware. It helps in connecting your computer to other devices on your network and all over the world.

The ip command shows or manipulates routing, network devices, interfaces and tunnels.



ifconfig

Stands for Interface configuration. It is often used for troubleshooting network connectivities. Ifconfig is used at the boot time to set-up the interfaces as necessary.

Eg. *Ifconfig -a* (display all interfaces which are currently available in the system)

5. nslookup

About

The command queries Internet name servers interactively and non-interactively from DNS (Domain Name Server).

It can also perform reverse lookups, that is, given the ip address it can find the corresponding domain name.

Host is used by default to determine what domain a particular IP address resolves to. It can be changed interactively with the command `*server 8.8.8.8*` (uses google's server to determine the IP address)

DNS (Domain Name System)

The DNS turns domain names into IP addresses, which browsers use to load internet pages.

Command Execution

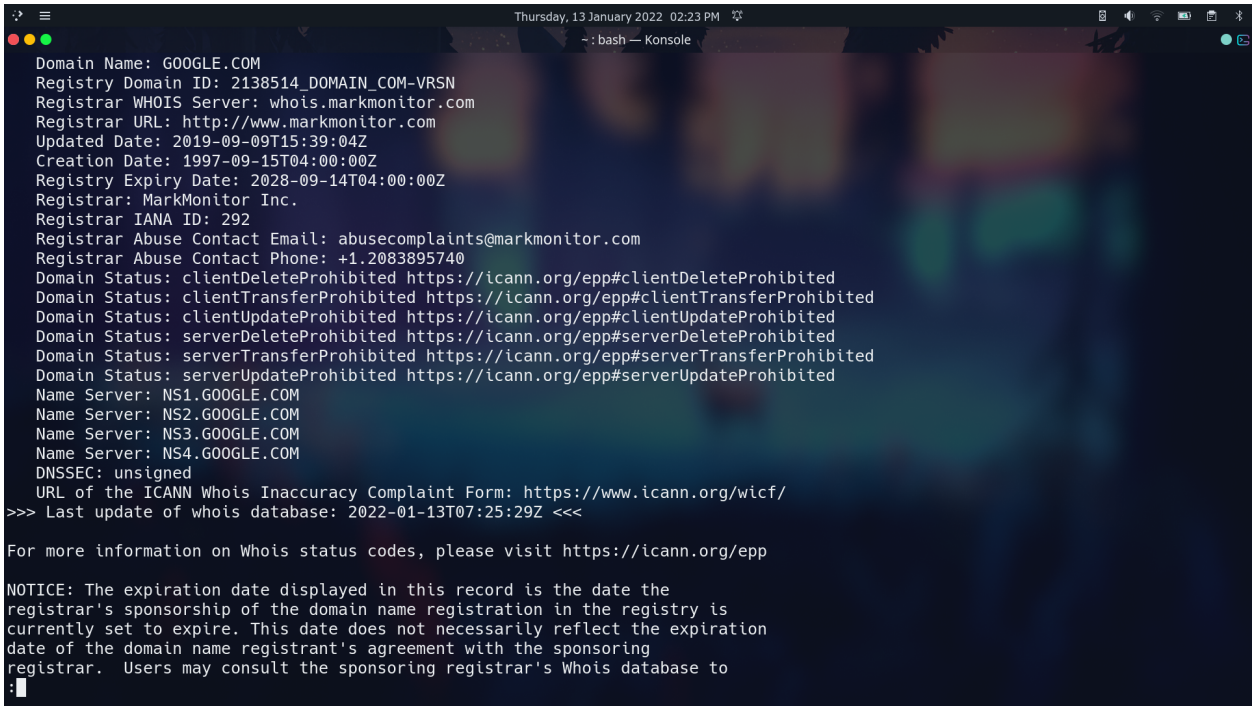
As seen in the first command *nslookup google.com*, it displays both IPv4 and IPv6 address of the domain name, first address being the IPv4 address and second one being the IPv6 address.

The second command performs reverse lookup.

6. whois

This command searches for an object in a RFC 3912 database for listing of records that contain details about the ownership of domains and the owners. The whois client tries to guess the right server to ask for the specified object. If no guess can be made it will connect to *whois.networksolutions.com* for NIC handles or *whois.arin.net* for IPv4 addresses and network names.

Eg. *whois google.com*




Thursday, 13 January 2022 02:23 PM
~ : bash — Konsole
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
:


Thursday, 13 January 2022 02:24 PM
~ : bash — Konsole
https://domains.markmonitor.com/whois
If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.
The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.
By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
(1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
(2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).
MarkMonitor reserves the right to modify these terms at any time.
By submitting this query, you agree to abide by this policy.
MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.
Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
--
(END)

7. route

About

The command shows or manipulates the IP routing table. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with **ifconfig**.

Routing Table

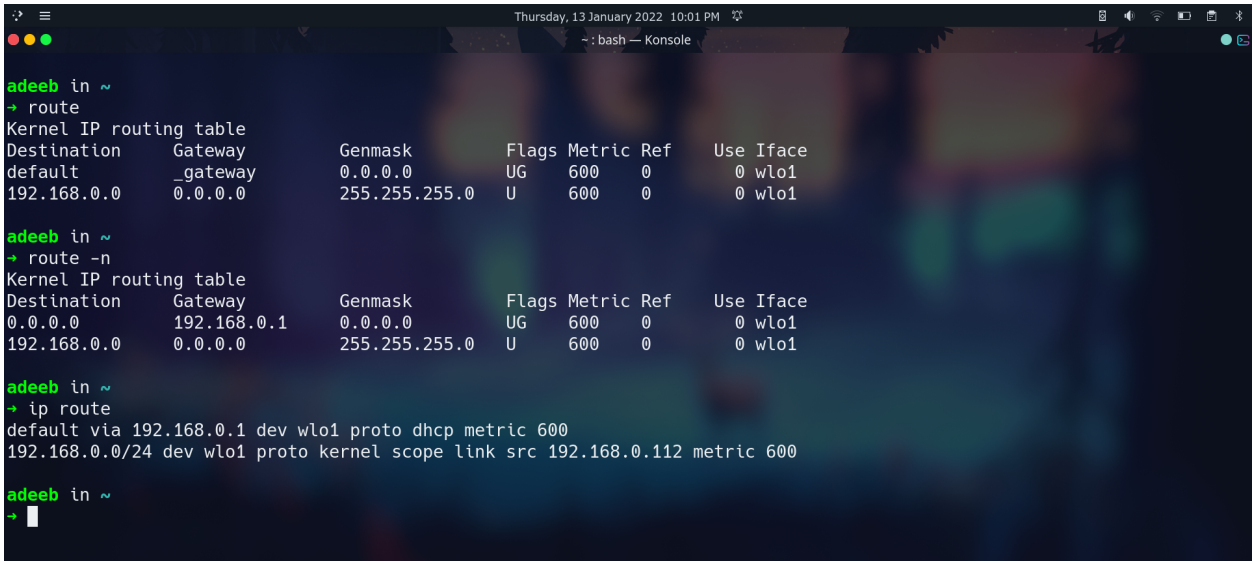
It is a data table stored in a router or a network host that lists the routes to particular network destinations, and in some cases, metrics associated with those routes.

Command Execution

1. *route* - - displays routing table entries.

2. *route -n* - - displays routing table entries in numerical form

3. *ip route* - - displays details of IP routing table



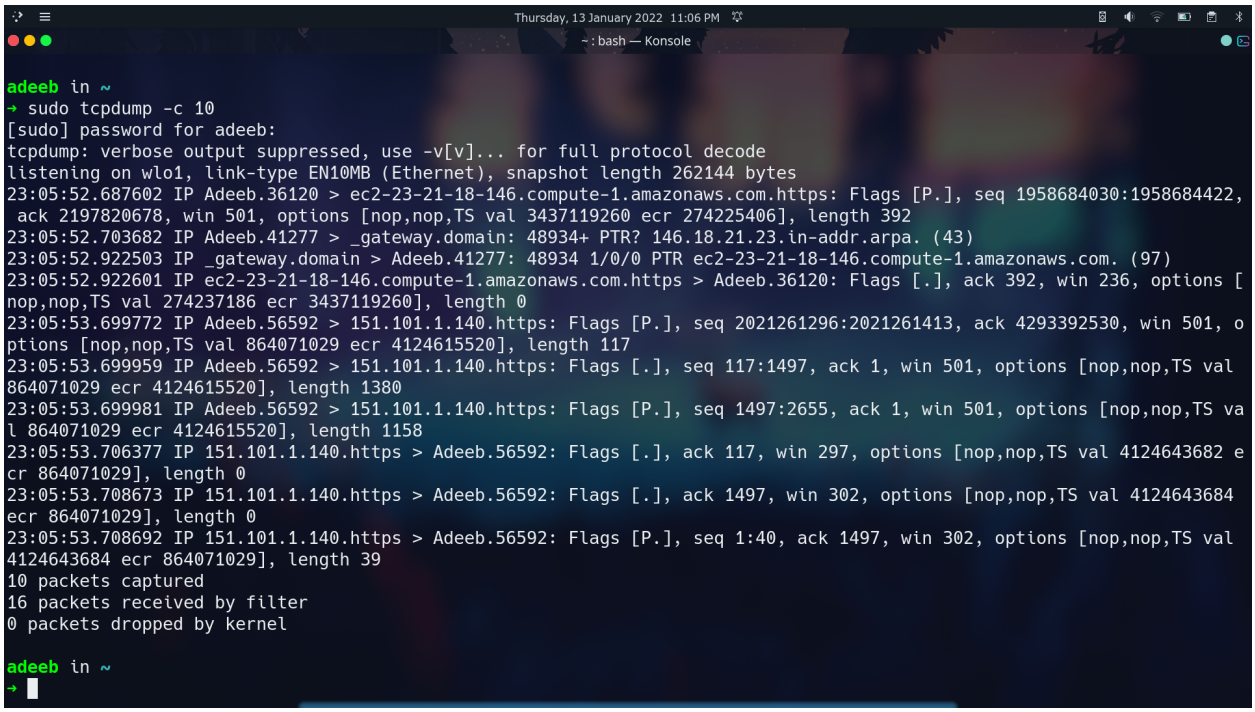
8. tcpdump

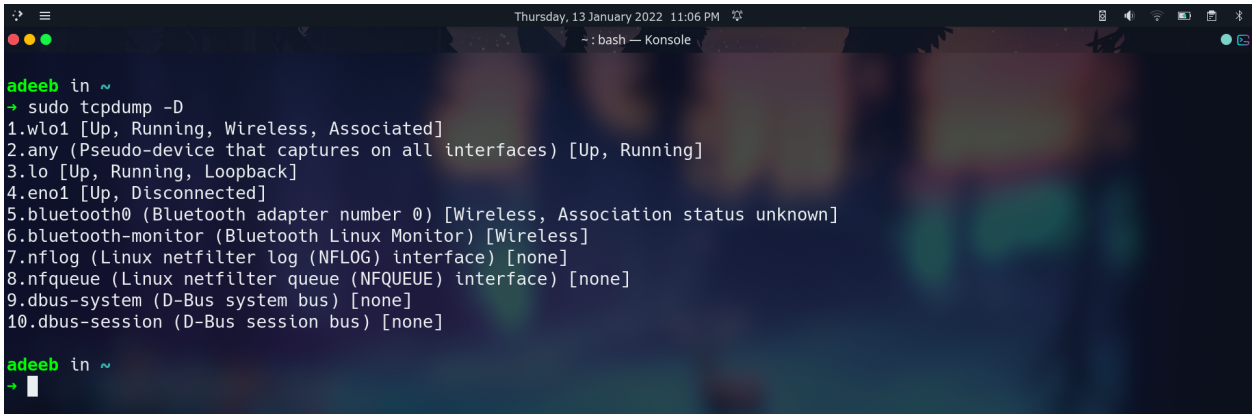
It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

Eg 1. *sudo tcpdump* - - captures packets from the interface of the network through which the system is connected to the internet

Eg 2. sudo tcpdump -D - - print list of networks that this tool can capture packets from

Eg 3. *sudo tcpdump -i any* - - captures packets from the interface of any network





9. netstat / ss

netstat

It displays network connections for TCP/UDP and stats for Interfaces, Network protocols, routing tables, etc

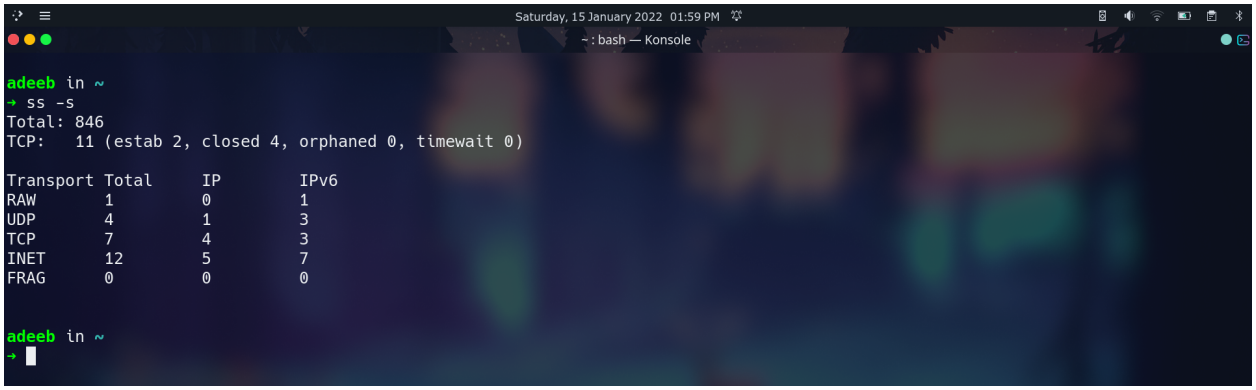
ss

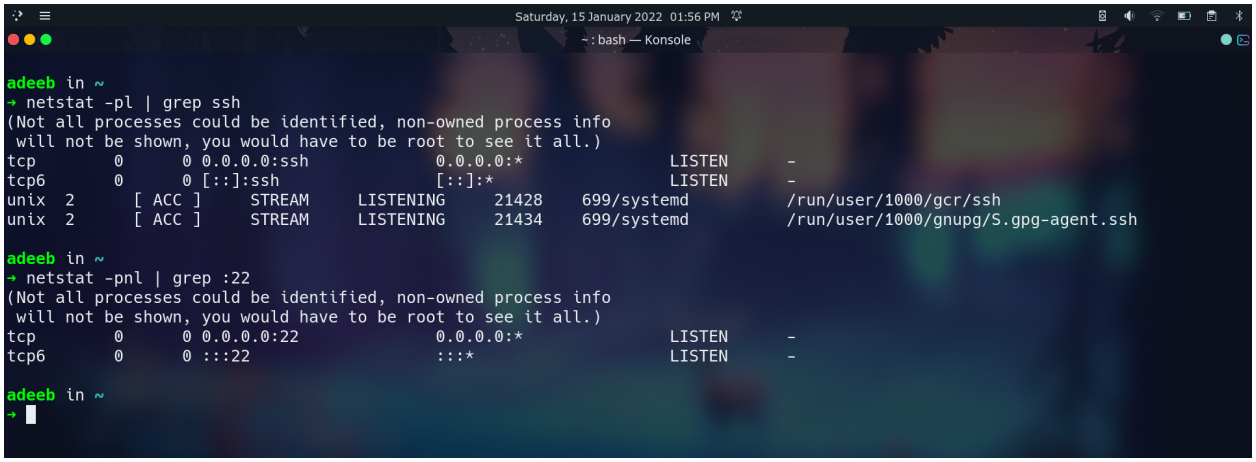
It's another utility to investigate sockets, replacing netstat. ss command tool which dumps socket stats and displays information similarly but it is faster than netstat. Usually used in troubleshooting network problems.

Command Execution

1. *ss -s - - displays summary stats*
2. *ss -t - - displays all TCP connections*
3. *ss -u - - displays all UDP connections*
4. *ss -x - - displays all unix connections*
5. *netstat -ie - - displays all the network interfaces (similar to ifconfig with a flag)*
6. *netstat -pnl | grep <port number> - - Check if specific port is listening*


Saturday, 15 January 2022 01:58 PM
~ : bash — Konsole
adeeb in ~
→ ss -t
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
ESTAB 0 0 192.168.0.112:43794 44.226.241.1:https
ESTAB 0 0 192.168.0.112:43428 89.187.162.107:dynamid
adeeb in ~
→ ss -u
Recv-Q Send-Q Local Address:Port Peer Address:Port Process
0 0 192.168.0.112%wlo1:bootpc 192.168.0.1:bootps
0 0 [::1]:48425 [::1]:48425
adeeb in ~
→ ss -x
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
u_dgr ESTAB 0 0 /run/systemd/notify 13752 * 0
u_dgr ESTAB 0 0 /run/systemd/journal/dev-log 13776 * 0
u_dgr ESTAB 0 0 /run/systemd/journal/socket 13778 * 0
u_seq ESTAB 0 0 @00004 23421 * 23420
u_seq ESTAB 0 0 @00005 24981 * 24982
u_seq ESTAB 0 0 @00006 24983 * 24984
u_seq ESTAB 0 0 @00001 23420 * 23421
u_seq ESTAB 0 0 @00002 24343 * 24344
u_seq ESTAB 0 0 @00003 24344 * 24343
u_str ESTAB 0 0 * 24625 * 24626
u_str ESTAB 0 0 @/tmp/.ICE-unix/799 17339 * 17338
u_str ESTAB 0 0 /run/systemd/journal/stdout 16015 * 17279
u_str ESTAB 0 0 * 70306 * 70307
u_str ESTAB 0 0 * 21492 * 23037
u_str ESTAB 0 0 * 30653 * 38921
u_str ESTAB 0 0 * 23114 * 19354
u_str ESTAB 0 0 * 11716 * 17218


Saturday, 15 January 2022 01:59 PM
~ : bash — Konsole
adeeb in ~
→ ss -s
Total: 846
TCP: 11 (estab 2, closed 4, orphaned 0, timewait 0)
Transport Total IP IPv6
RAW 1 0 1
UDP 4 1 3
TCP 7 4 3
INET 12 5 7
FRAG 0 0 0
adeeb in ~
→


Saturday, 15 January 2022 01:56 PM
~ : bash — Konsole
adeeb in ~
→ netstat -pl | grep ssh
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp 0 0 0.0.0.0:ssh 0.0.0.0:* LISTEN -
tcp6 0 0 [::]:ssh [::]:* LISTEN -
unix 2 [ACC] STREAM LISTENING 21428 699/systemd /run/user/1000/gcr/ssh
unix 2 [ACC] STREAM LISTENING 21434 699/systemd /run/user/1000/gnupg/S.gpg-agent.ssh
adeeb in ~
→ netstat -pnl | grep :22
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp6 0 0 :::22 :::* LISTEN -
adeeb in ~
→

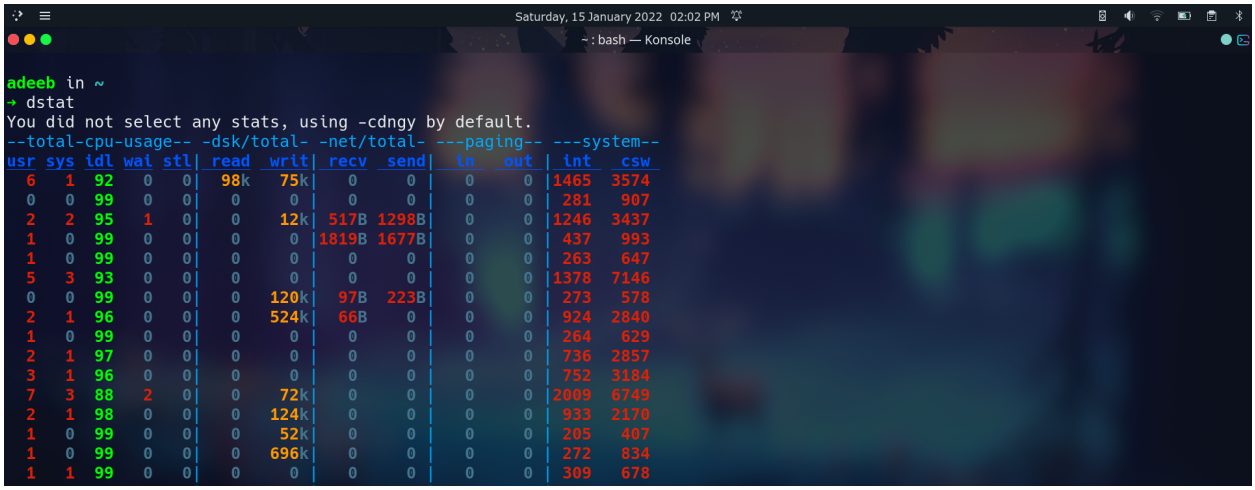
10. dstat

About

Dstat allows you to view all of your system resources instantly, you can eg. compare disk usage in combination with interrupts from your IDE controller, or compare the network bandwidth numbers directly with the disk throughput (in the same interval).

Command Execution

1. dstat



Column	Meaning
CPU Stats	CPU usage by user, system processes and number of idle processes, and number of waiting processes, hardware and software interrupts.
Disk Stats	Total number of read and write operations on the disk.
Network Stats	Total amount of Bytes received and sent on network interfaces.
Paging Stats	Number of times information is copied into and moved out of memory.
System Stats	Number of interrupts and context switches.

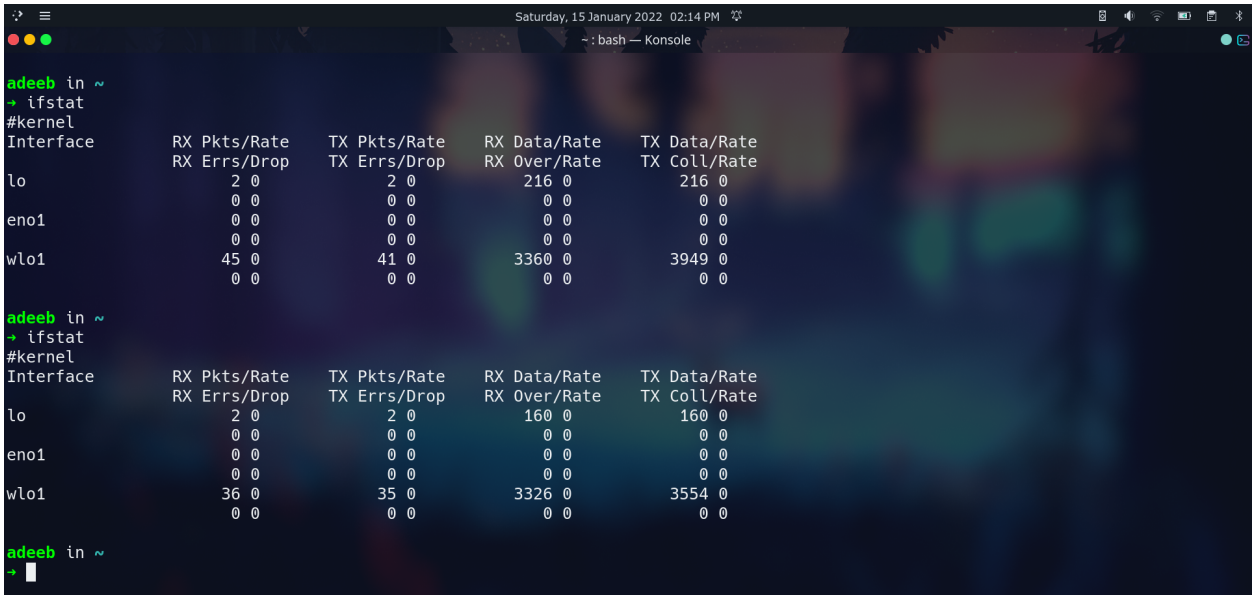
11. ifstat

About

Ifstat prints out network interface statistics. The utility keeps records of the previous data displayed in history files and by default only shows the difference between the last and the current call.

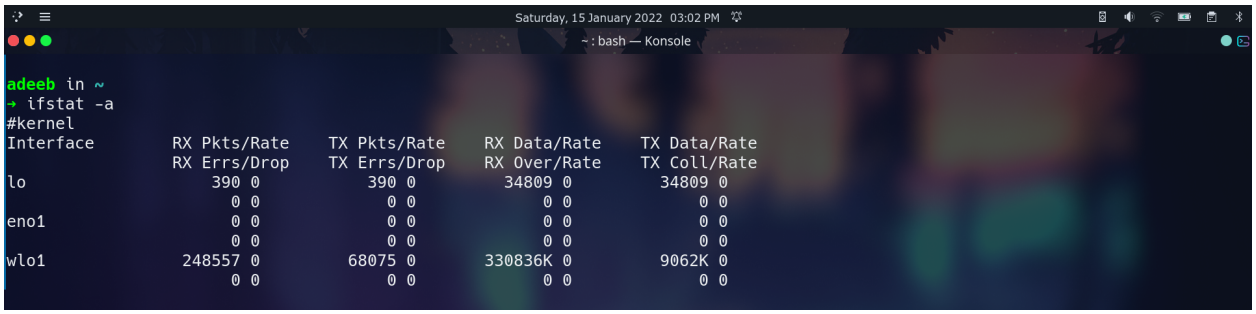
Command Execution

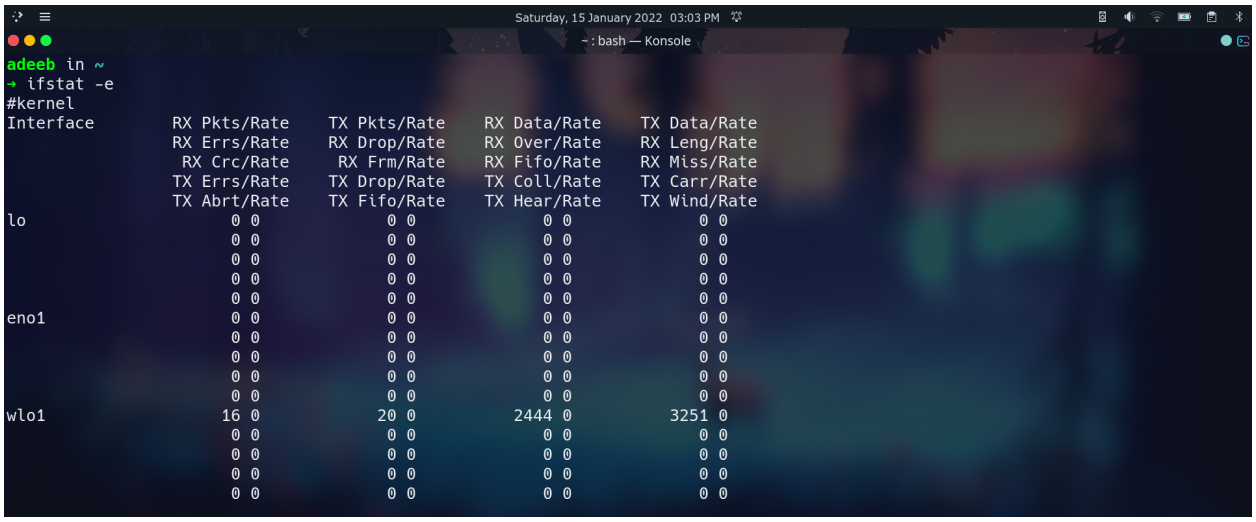
1. Ifstat - - Prints network interface statistics considering history
2. ifstat -a - - Ignores history
3. ifstat -e - - Shows errors
4. ifstat -r - - Resets history

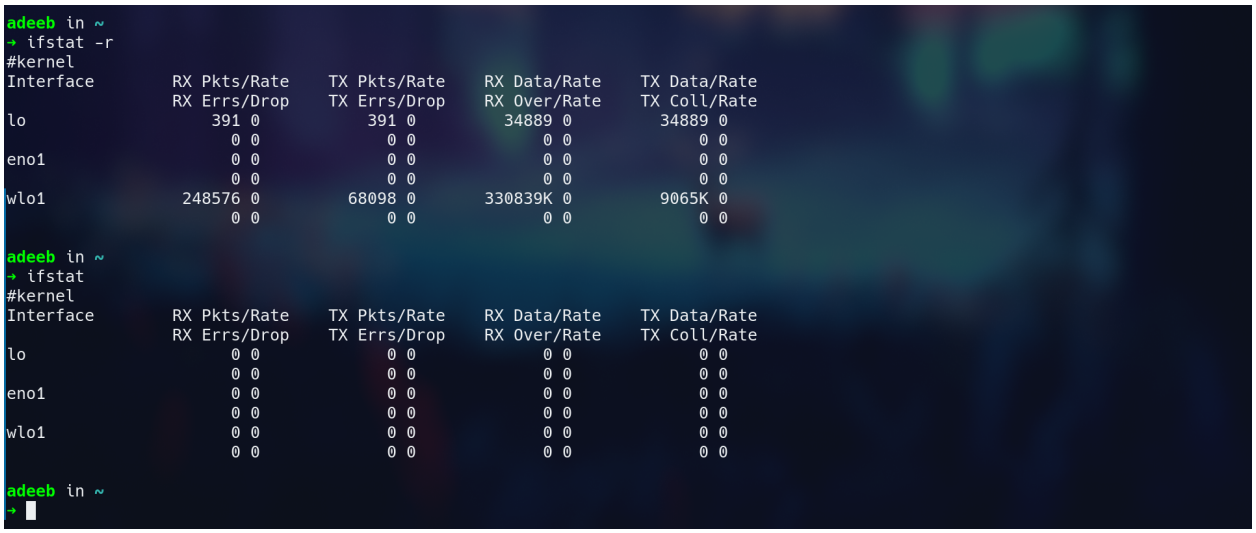


Packets *received* and rate in the RX column, as well as any errors or drops on those packets.

In the TX column, we have packets *transmitted* and rate, as well as errors and drops.


Saturday, 15 January 2022 03:02 PM
~ : bash — Konsole
adeeb in ~
→ ifstat -a
#kernel
Interface RX Pkts/Rate TX Pkts/Rate RX Data/Rate TX Data/Rate
RX Errs/Drop TX Errs/Drop RX Over/Rate TX Coll/Rate
lo 390 0 390 0 34809 0 34809 0
0 0 0 0 0 0 0 0
eno1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
wlo1 248557 0 68075 0 330836K 0 9062K 0
0 0 0 0 0 0 0 0


Saturday, 15 January 2022 03:03 PM
~ : bash — Konsole
adeeb in ~
→ ifstat -e
#kernel
Interface RX Pkts/Rate TX Pkts/Rate RX Data/Rate TX Data/Rate
RX Errs/Rate RX Drop/Rate RX Over/Rate RX Leng/Rate
RX Crc/Rate RX Frm/Rate RX Fifo/Rate RX Miss/Rate
TX Errs/Rate TX Drop/Rate TX Coll/Rate TX Carr/Rate
TX Abrt/Rate TX Fifo/Rate TX Hear/Rate TX Wind/Rate
lo 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
eno1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
wlo1 16 0 20 0 2444 0 3251 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0


adeeb in ~
→ ifstat -r
#kernel
Interface RX Pkts/Rate TX Pkts/Rate RX Data/Rate TX Data/Rate
RX Errs/Drop TX Errs/Drop RX Over/Rate TX Coll/Rate
lo 391 0 391 0 34889 0 34889 0
0 0 0 0 0 0 0 0
eno1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
wlo1 248576 0 68098 0 330839K 0 9065K 0
0 0 0 0 0 0 0 0
adeeb in ~
→ ifstat
#kernel
Interface RX Pkts/Rate TX Pkts/Rate RX Data/Rate TX Data/Rate
RX Errs/Drop TX Errs/Drop RX Over/Rate TX Coll/Rate
lo 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
eno1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
wlo1 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
adeeb in ~
→

12. wget

About

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. With Wget, you can download files using HTTP, HTTPS, and FTP protocols.

Command Execution

1. *wget google.com*
2. *wget google.com -c* - - resume a partially downloaded file