

CS3093D | Networks Lab
Arjun Syam
B180031CS

1.ping :

A Ping measures the time it takes for packets to be sent from the local host to a destination computer and back.

```
huraken@LAPTOP-FVLKJRU: ~                               iputils                                         PING(8) ^
```

PING(8) **iputils** **PING(8)**

NAME ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS ping [**-aAbBdDfhLnOqrRUvV46**] [**-c count**] [**-F flowlabel**] [**-i interval**] [**-I interface**] [**-l preload**] [**-m mark**]
 [**-M pmtdisc_option**] [**-N nodeinfo_option**] [**-w deadline**] [**-W timeout**] [**-p pattern**] [**-Q tos**]
 [**-s packetsize**] [**-S sndbuf**] [**-t ttl**] [**-T timestamp option**] [**hop...**] [**destination**]

DESCRIPTION ping uses the ICMP protocol's mandatory ECHO REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams ("pings") have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of "pad" bytes used to fill out the packet.

ping works with both IPv4 and IPv6. Using only one of them explicitly can be enforced by specifying -4 or -6.

ping can also send IPv6 Node Information Queries (RFC4620). Intermediate hops may not be allowed, because IPv6 source routing was deprecated (RFC5095).

OPTIONS

- 4 Use IPv4 only.
- 6 Use IPv6 only.
- a Audible ping.
- A Adaptive ping. Interpacket interval adapts to round-trip time, so that effectively not more than one (or more, if preload is set) unanswered probe is present in the network. Minimal interval is 200msec for not super-user. On networks with low rtt this mode is essentially equivalent to flood mode.
- b Allow pinging a broadcast address.
- B Do not allow ping to change source address of probes. The address is bound to one selected when ping starts.
- c count
Stop after sending count ECHO REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.
- d Set the SO_DEBUG option on the socket being used. Essentially, this socket option is not used by Linux kernel.
- D Print timestamp (unix time + microseconds as in gettimeofday) before each line.
- f Flood ping. For every ECHO_REQUEST sent a period "." is printed, while for every ECHO_REPLY received a backspace is printed. This provides a rapid display of how many packets are being dropped. If interval is not given, it sets interval to zero and outputs packets as fast as they come back or one hundred times per second, whichever is more. Only the super-user may use this option with zero interval.
- F flow_label
IPv6 only. Allocate and set 20 bit flow label (in hex) on echo request packets. If value is zero, kernel allocates random flow label.
- h Show help.
- i interval

Manual page ping(8) line 1 [press h for help or q to quit]

huraken@LAPTOP-FVLKJJR2: ~

```
PING google.com [172.217.31.206] 56(84) bytes of data.  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=1 ttl=117 time=25.5 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=2 ttl=117 time=25.9 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=3 ttl=117 time=27.6 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=4 ttl=117 time=26.7 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=5 ttl=117 time=26.8 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=6 ttl=117 time=26.3 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=7 ttl=117 time=26.8 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=8 ttl=117 time=30.9 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=9 ttl=117 time=26.2 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=10 ttl=117 time=26.6 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=12 ttl=117 time=26.8 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=13 ttl=117 time=27.7 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=15 ttl=117 time=28.1 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=16 ttl=117 time=26.3 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=17 ttl=117 time=26.4 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=18 ttl=117 time=24.6 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=19 ttl=117 time=25.7 ms  
64 bytes from maa03s28-in-f14.le100.net [172.217.31.206]: icmp_seq=20 ttl=117 time=26.5 ms
```

2. tracert/traceroute :

Computer network diagnostic commands for displaying possible routes (paths) and measuring transit delays of packets across an Internet Protocol (IP) network.

```
huraken@LAPTOP-FVLKJXR2: ~
```

Traceroute For Linux

TRACEROUTE[1]

NAME

traceroute - print the route packets trace to network host

SYNOPSIS

```
traceroute [-46dFITUnreAV] [-f first_ttl] [-g gate,...]
[-i device] [-m max_ttl] [-p port] [-s src_addr]
[-q nqueries] [-N squeries] [-t tos]
[-l flow_label] [-w waittimes] [-z sendwait] [-UL] [-O]
[-P proto] [--sport=port] [-M method] [-D mod_options]
[--mtu] [--back]
host [packet_len]
traceroute6 [options]
tcptraceroute [options]
lft [options]
```

DESCRIPTION

`traceroute` tracks the route packets taken from an IP network on their way to a given host. It utilizes the IP protocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to the host.

`traceroute6` is equivalent to `traceroute -6`

`tcptraceroute` is equivalent to `traceroute -T`

`lft`, the Layer Four Traceroute, performs a TCP traceroute, like `traceroute -T`, but attempts to provide compatibility with the original such implementation, also called "lft".

The only required parameter is the name or IP address of the destination host. The optional packet length is the total size of the probing packet (default 60 bytes for IPv4 and 80 for IPv6). The specified size can be ignored in some situations or increased up to a minimal value.

This program attempts to trace the route an IP packet would follow to some internet host by launching probe packets with a small ttl (time to live) then listening for an ICMP "time exceeded" reply from a gateway. We start our probes with a ttl of one and increase by one until we get an ICMP "port unreachable" (or TCP reset), which means we got to the "host", or hit a max (which defaults to 30 hops). Three probes (by default) are sent at each ttl setting and a line is printed showing the ttl, address of the gateway and round trip time of each probe. The address can be followed by additional information when requested. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a certain timeout, an "*" (asterisk) is printed for that probe.

After the trip time, some additional annotation can be printed: !H, !N, or !P (host, network or protocol unreachable), !S (source route failed), !F (fragmentation needed), !X (communication administratively prohibited), !V (host precedence violation), !C (precedence cutoff in effect), or !<num> (ICMP unreachable code <num>). If almost all the probes result in some kind of unreachable, traceroute will give up and exit.

We don't want the destination host to process the UDP probe packets, so the destination port is set to an unlikely value (you can change it with the -p flag). There is no such a problem for ICMP or TCP tracerouting (for TCP we use half-open technique, which prevents our probes to be seen by applications on the destination host).

In the modern network environment the traditional traceroute methods can not be always applicable, because of widespread use of firewalls. Such firewalls filter the "unlikely" UDP ports, or even ICMP echoes. To solve this, some additional tracerouting methods are implemented (including tcp), see LIST OF AVAILABLE METHODS below. Such methods try to use particular protocol and source/destination port, in order to bypass firewalls (to be seen by firewalls just as a start of allowed type of a network session).

OPTIONS

```
--help Print help info and exit.
-4, -6 Explicitly force IPv4 or IPv6 tracerouting. By default, the program will try to resolve the name given, and choose the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, traceroute will use IPv4.
-I, --icmp
    Use ICMP ECHO for probes
```

Manual page traceroute(1) line 1 (press h for help or q to quit)

```
Windows PowerShell
PS C:\Users\HURAKEN> tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d           Do not resolve addresses to hostnames.
    -h maximum_hops Maximum number of hops to search for target.
    -j host-list  Loose source route along host-list (IPv4-only).
    -w timeout   Wait timeout milliseconds for each reply.
    -R           Trace round-trip path (IPv6-only).
    -S srcaddr   Source address to use (IPv6-only).
    -4           Force using IPv4.
    -6           Force using IPv6.

PS C:\Users\HURAKEN> tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

 1     1 ms      1 ms      1 ms  192.168.1.1
 2    12 ms      7 ms      3 ms  100.82.192.1
 3     3 ms      3 ms      3 ms  118.151.164.202.asianet.co.in [202.164.151.118]
 4     3 ms      3 ms      3 ms  41.151.164.202.asianet.co.in [202.164.151.41]
 5     3 ms      *         4 ms  5-1-1-1.datagroup.ua [5.1.1.1]
 6    27 ms      26 ms     26 ms  94.151.164.202.asianet.co.in [202.164.151.94]
 7    27 ms      25 ms     25 ms  77.252.88.202.asianet.co.in [202.88.252.77]
 8    25 ms      25 ms     25 ms  74.125.252.219
 9    34 ms      26 ms     32 ms  142.250.233.143
10    27 ms      28 ms     26 ms  dns.google [8.8.8.8]

Trace complete.
PS C:\Users\HURAKEN>
```

3.Ifconfig :

To configure kernel-resident network interface

```
huraken@LAPTOP-FVLKJUR2: ~ IFCONFIG[8] Linux System Administrator's Manual IFCONFIG[8]
NAME
    ifconfig - configure a network interface
SYNOPSIS
    ifconfig [-v] [-a] [-s] [interface]
    ifconfig [-v] interface [aftype] options | address ...
DESCRIPTION
    Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up
    interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is
    needed.

    If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single
    interface argument is given, it displays the status of the given interface only; if a single -a argument is
    given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an in-
    terface.

Address Families
    If the first argument after the interface name is recognized as the name of a supported address family,
    that address family is used for decoding and displaying all protocol addresses. Currently supported ad-
    dress families include inet (TCP/IP, default), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase
    2), ipx (Novell IPX) and netrom (AMPR Packet radio). All numbers supplied as parts in IPv4 dotted decimal
    notation may be decimal, octal, or hexadecimal, as specified in the ISO C standard (that is, a leading '0x'
    or '0X' implies hexadecimal; otherwise, a leading '0' implies octal; otherwise, the number is interpreted as
    decimal). Use of hexadecimal and octal numbers is not RFC-compliant and therefore its use is discouraged.

OPTIONS
    -a    display all interfaces which are currently available, even if down
    -s    display a short list (like netstat -i)
    -v    be more verbose for some error conditions

interface
    The name of the interface. This is usually a driver name followed by a unit number, for example
    eth0 for the first Ethernet interface. If your kernel supports alias interfaces, you can specify
    them with syntax like eth0:0 for the first alias of eth0. You can use them to assign more addresses.
    To delete an alias interface use ifconfig eth0:0 down. Note: for every scope (i.e. same net with
    address/netmask combination) all aliases are deleted, if you delete the first (primary).

    up    This flag causes the interface to be activated. It is implicitly specified if an address is as-
        signed to the interface; you can suppress this behavior when using an alias interface by appending
        an - to the alias (e.g. eth0:0-). It is also suppressed when using the IPv4 0.0.0.0 address as the
        kernel will use this to implicitly delete alias interfaces.

    down  This flag causes the driver for this interface to be shut down.

    [-]arp Enable or disable the use of the ARP protocol on this interface.

    [-]promisc
        Enable or disable the promiscuous mode of the interface. If selected, all packets on the network
        will be received by the interface.

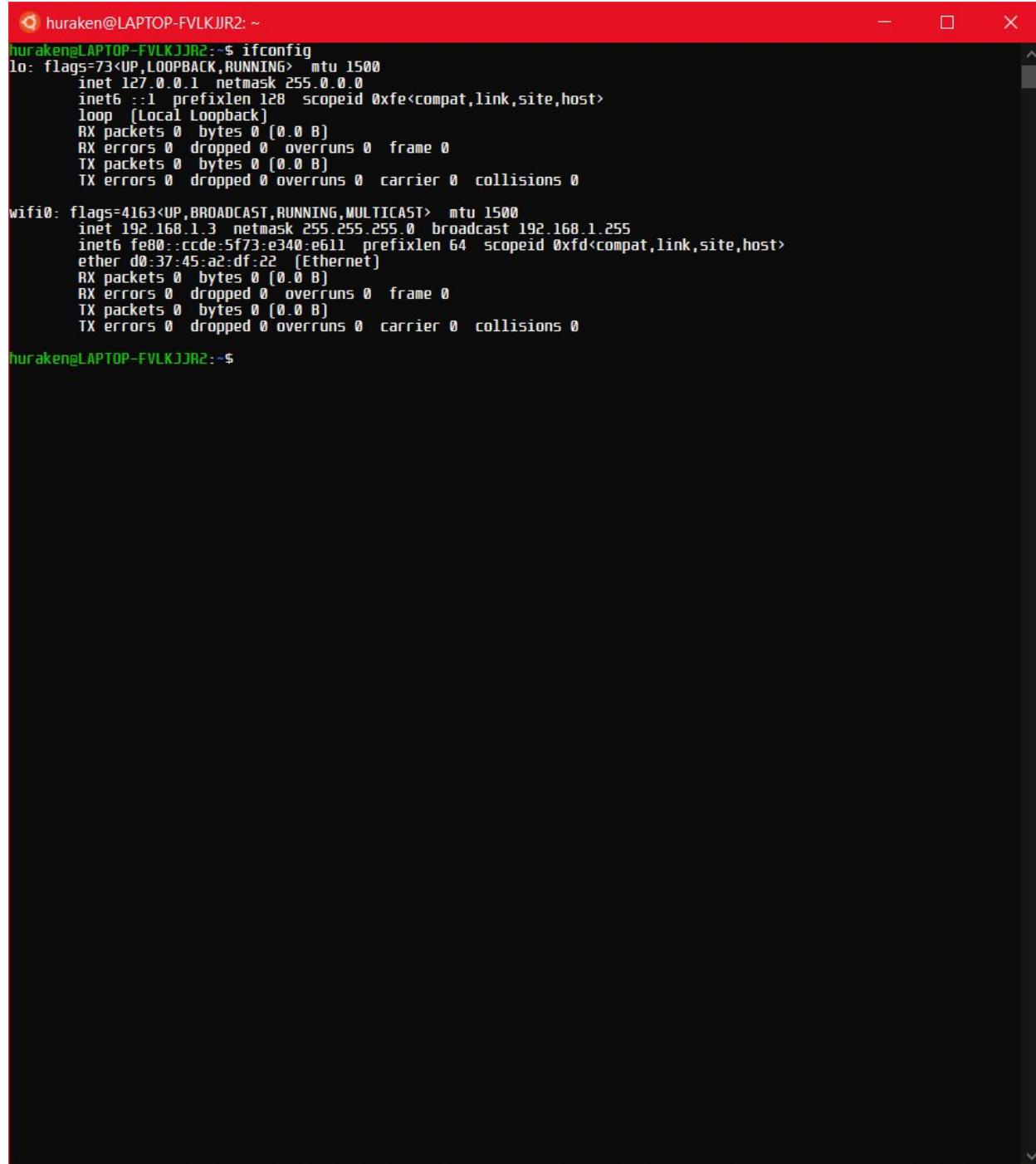
    [-]allmulti
        Enable or disable all-multicast mode. If selected, all multicast packets on the network will be re-
        ceived by the interface.

    mtu N  This parameter sets the Maximum Transfer Unit (MTU) of an interface.

    dstaddr addr
        Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete;
        use the pointopoint keyword instead.

    netmask addr
        Set the IP network mask for this interface. This value defaults to the usual class A, B or C net-
```

^ ⌂ ENG 21:17



```
huraken@LAPTOP-FVLKJJR2:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 1500
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0xfe<compat,link,site,host>
            loop (Local Loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.3 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::ccde:5f73:e340:e611 prefixlen 64 scopeid 0xfd<compat,link,site,host>
            ether d0:37:45:a2:df:22 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

huraken@LAPTOP-FVLKJJR2:~$
```

4. Dig :

Used to display the DNS lookups and displays the answers from the name server that was queried

```
huraken@LAPTOP-FVLKJUR2: ~
```

DIG[1] BIND9 DIG[1]

NAME
dig - DNS lookup utility

SYNOPSIS
dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-v]
[-x addr] [-y fhmac[:name:key]] [(-4) | (-6)] [name] [type] [class] [queryopt...]
dig [-h]
dig [global-queryopt...] [query...]

DESCRIPTION
dig is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.

Although dig is normally used with command-line arguments, it also has a batch mode of operation for reading lookup requests from a file. A brief summary of its command-line arguments and options is printed when the -h option is given. Unlike earlier versions, the BIND 9 implementation of dig allows multiple lookups to be issued from the command line.

Unless it is told to query a specific name server, dig will try each of the servers listed in /etc/resolv.conf. If no usable server addresses are found, dig will send the query to the local host.

When no command line arguments or options are given, dig will perform an NS query for "." (the root).

It is possible to set per-user defaults for dig via \${HOME}/.digrc. This file is read and any options in it are applied before the command line arguments. The -r option disables this feature, for scripts that need predictable behaviour.

The IN and CH class names overlap with the IN and CH top level domain names. Either use the -t and -c options to specify the type and class, use the -q to specify the domain name, or use "IN." and "CH." when looking up these top level domains.

SIMPLE USAGE
A typical invocation of dig looks like:

```
dig @server name type
```

where:

server
is the name or IP address of the name server to query. This can be an IPv4 address in dotted-decimal notation or an IPv6 address in colon-delimited notation. When the supplied server argument is a hostname, dig resolves that name before querying that name server.

If no server argument is provided, dig consults /etc/resolv.conf; if an address is found there, it queries the name server at that address. If either of the -4 or -6 options are in use, then only addresses for the corresponding transport will be tried. If no usable addresses are found, dig will send the query to the local host. The reply from the name server that responds is displayed.

name
is the name of the resource record that is to be looked up.

type
indicates what type of query is required - ANY, A, MX, SIG, etc. type can be any valid query type. If no type argument is supplied, dig will perform a lookup for an A record.

OPTIONS

-4	Use IPv4 only.
-6	Use IPv6 only.

^ ⌂ 🔋 ENG 21:20

```
huraken@LAPTOP-FVLKJJR2:~$ man dig
huraken@LAPTOP-FVLKJJR2:~$ dig google.com
; <>> DiG 9.16.1-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 597
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;
;; QUESTION SECTION:
;google.com.           IN      A
;
;; ANSWER SECTION:
google.com.        264     IN      A      172.217.31.206
;
;; Query time: 5 msec
;; SERVER: 192.168.1.1#53[192.168.1.1]
;; WHEN: Sun Jan 24 21:23:24 IST 2021
;; MSG SIZE  rcvd: 44
huraken@LAPTOP-FVLKJJR2:~$
```

5. Whois

Cmd : whois 8.8.8.8

To get info regarding a specific IP address

```
Select huraken@LAPTOP-FVLKJUR2: ~
Ref: https://rdap.arin.net/registry/entity/LPL-141

OrgAbuseHandle: LAC56-ARIN
OrgAbuseName: L3 Abuse Contact
OrgAbusePhone: +1-877-453-8353
OrgAbuseEmail: abuse@level3.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/LAC56-ARIN

OrgTechHandle: IPADD5-ARIN
OrgTechName: ipaddressing
OrgTechPhone: +1-877-453-8353
OrgTechEmail: ipaddressing@level3.com
OrgTechRef: https://rdap.arin.net/registry/entity/IPADD5-ARIN

# end

# start

NetRange: 8.8.8.0 - 8.8.8.255
CIDR: 8.8.8.0/24
NetName: LVLT-60GL-8-8-8
NetHandle: NET-8-8-8-0-1
Parent: LVLT-ORG-8-8 (NET-8-0-0-0-1)
NetType: Reallocated
OriginAS:
Organization: Google LLC (GOGL)
RegDate: 2014-03-14
Updated: 2014-03-14
Ref: https://rdap.arin.net/registry/ip/8.8.8.0

OrgName: Google LLC
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2019-10-31
Comment: Please note that the recommended way to file abuse complaints are located in the following links.
Comment: To report abuse and illegal activity: https://www.google.com/contact/
Comment: For legal requests: http://support.google.com/legal
Comment: Regards,
Comment: The Google Team
Ref: https://rdap.arin.net/registry/entity/GOGL

OrgTechHandle: Z639-ARIN
OrgTechName: Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef: https://rdap.arin.net/registry/entity/Z639-ARIN

OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: network-abuse@google.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE5250-ARIN

# end
```

6. Route : to manipulate IP routing tables

```
● huraken@LAPTOP-FVLKJXR2: ~                                         -   □   X
ROUTE[8]                                     Linux System Administrator's Manual          ROUTE[8] ^

NAME      route - show / manipulate the IP routing table
SYNOPSIS  route [-CFvnNee] [-A family |-4|-6]
           route  [-v] [-A family |-4|-6] add [-net|-host] target [netmask Nm] [gw Gw] [metric N] [mss M] [window W]
           route  [-v] [-A family |-4|-6] del [-net|-host] target [gw Gw] [netmask Nm] [metric M] [[dev] If]
           route  [-V] [--version] [-h] [-help]

DESCRIPTION
Route manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig(8) program.

When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

OPTIONS
-A family
    use the specified address family (eg `inet'). Use route --help for a full list. You can use -6 as an alias for --inet6 and -4 as an alias for -A inet
-F     operate on the kernel's FIB (Forwarding Information Base) routing table. This is the default.
-C     operate on the kernel's routing cache.
-v     select verbose operation.
-n     show numerical addresses instead of trying to determine symbolic host names. This is useful if you are trying to determine why the route to your nameserver has vanished.
-e     use netstat(8)-format for displaying the routing table. -ee will generate a very long line with all parameters from the routing table.
del   delete a route.
add   add a new route.

target the destination network or host. You can provide an addresses or symbolic network or host name. Optionally you can use /prefixlen notation instead of using the netmask option.

-net   the target is a network.
-host  the target is a host.

netmask Nm
    when adding a network route, the netmask to be used.

gw Gw route packets via a gateway.
NOTE: The specified gateway must be reachable first. This usually means that you have to set up a static route to the gateway beforehand. If you specify the address of one of your local interfaces, it will be used to decide about the interface to which the packets should be routed to. This is a BSDism compatibility hack.

metric M
    set the metric field in the routing table (used by routing daemons) to M. If this option is not specified the metric for inet6 (IPv6) address family defaults to '1', for inet (IPv4) it defaults to '0'. You should always specify an explicit metric value to not rely on those defaults - they also differ from iproute2.

mss M sets MTU (Maximum Transmission Unit) of the route to M bytes. Note that the current implementation of the route command does not allow the option to set the Maximum Segment Size (MSS).

Manual page route(8) line 1 (press h for help or q to quit)
```

```
huraken@LAPTOP-FVLKJJR2: ~
huraken@LAPTOP-FVLKJJR2:~$ route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
127.0.0.0       0.0.0.0        255.0.0.0      U     256    0      0 lo
127.0.0.1       0.0.0.0        255.255.255.255 U     256    0      0 lo
127.255.255.255 0.0.0.0       255.255.255.255 U     256    0      0 lo
224.0.0.0       0.0.0.0        240.0.0.0      U     256    0      0 lo
255.255.255.255 0.0.0.0       255.255.255.255 U     256    0      0 lo
0.0.0.0         192.168.1.1   255.255.255.255 U     0      0      0 wifi0
192.168.1.0     0.0.0.0        255.255.255.0   U     256    0      0 wifi0
192.168.1.3     0.0.0.0        255.255.255.255 U     256    0      0 wifi0
192.168.1.255   0.0.0.0        255.255.255.255 U     256    0      0 wifi0
224.0.0.0       0.0.0.0        240.0.0.0      U     256    0      0 wifi0
255.255.255.255 0.0.0.0       255.255.255.255 U     256    0      0 wifi0
huraken@LAPTOP-FVLKJJR2:~$
```

7. **Tcpdump** : displays the contents of the packets on a network interface

uraken@LAPTOP-FVLKJJR2: ~

TCPDUMP(8) System Manager's Manual TCPDUMP(8)

NAME

tcpdump - dump traffic on a network

SYNOPSIS

```
tcpdump [ -AbdDefhHIJKLnNOpqStuUvxX# ] [ -B buffer size ]
        [ -c count ]
        [ -C file size ] [ -G rotate seconds ] [ -F file ]
        [ -i interface ] [ -j tstamp type ] [ -m module ] [ -M secret ]
        [ --number ] [ -O in|out|inout ]
        [ -r file ] [ -v file ] [ -s snaplen ] [ -T type ] [ -w file ]
        [ -W filecount ]
        [ -E spineipaddr algo:secret.... ]
        [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
        [ --time-stamp-precision=tstamp precision ]
        [ --immediate-mode ] [ --version ]
        [ expression ]
```

DESCRIPTION

Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match expression will be processed by **tcpdump**.

Tcpdump will, if not run with the -c flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing your interrupt character, typically control-C) or a SIGTERM signal (typically generated with the kill(1) command); if run with the -c flag, it will capture packets until it is interrupted by a SIGINT or SIGTERM signal or the specified number of packets have been processed.

When **tcpdump** finishes capturing packets, it will report counts of:

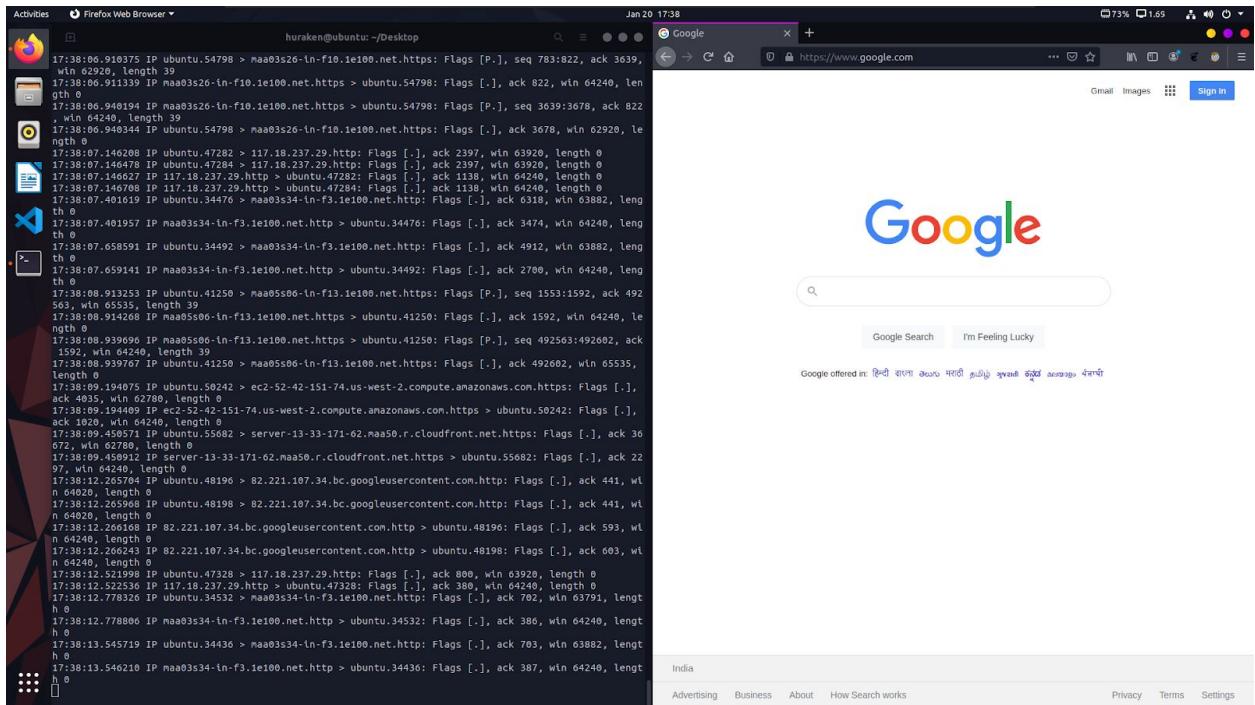
- packets ``captured'' (this is the number of packets that **tcpdump** has received and processed);
- packets ``received by filter'' (the meaning of this depends on the OS on which you're running **tcpdump**, and possibly on the way the OS was configured - if a filter was specified on the command line, on some OSes it counts packets regardless of whether they were matched by the filter expression and, even if they were matched by the filter expression, regardless of whether **tcpdump** has read and processed them yet, on other OSes it counts only packets that were matched by the filter expression regardless of whether **tcpdump** has read and processed them yet, and on other OSes it counts only packets that were matched by the filter expression and were processed by **tcpdump**);
- packets ``dropped by kernel'' (this is the number of packets that were dropped, due to a lack of buffer space, by the packet capture mechanism in the OS on which **tcpdump** is running, if the OS reports that information to applications; if not, it will be reported as 0).

On platforms that support the SIGINFO signal, such as most BSDs (including Mac OS X) and Digital/Tru64 UNIX, it will report those counts when it receives a SIGINFO signal (generated, for example, by typing your ``status'' character, typically control-T, although on some platforms, such as Mac OS X, the ``status'' character is not set by default, so you must set it with stty(1) in order to use it) and will continue capturing packets. On platforms that do not support the SIGINFO signal, the same can be achieved by using the SIGUSR1 signal.

Reading packets from a network interface may require that you have special privileges; see the pcap (3PCAP) man page for details. Reading a saved packet file doesn't require special privileges.

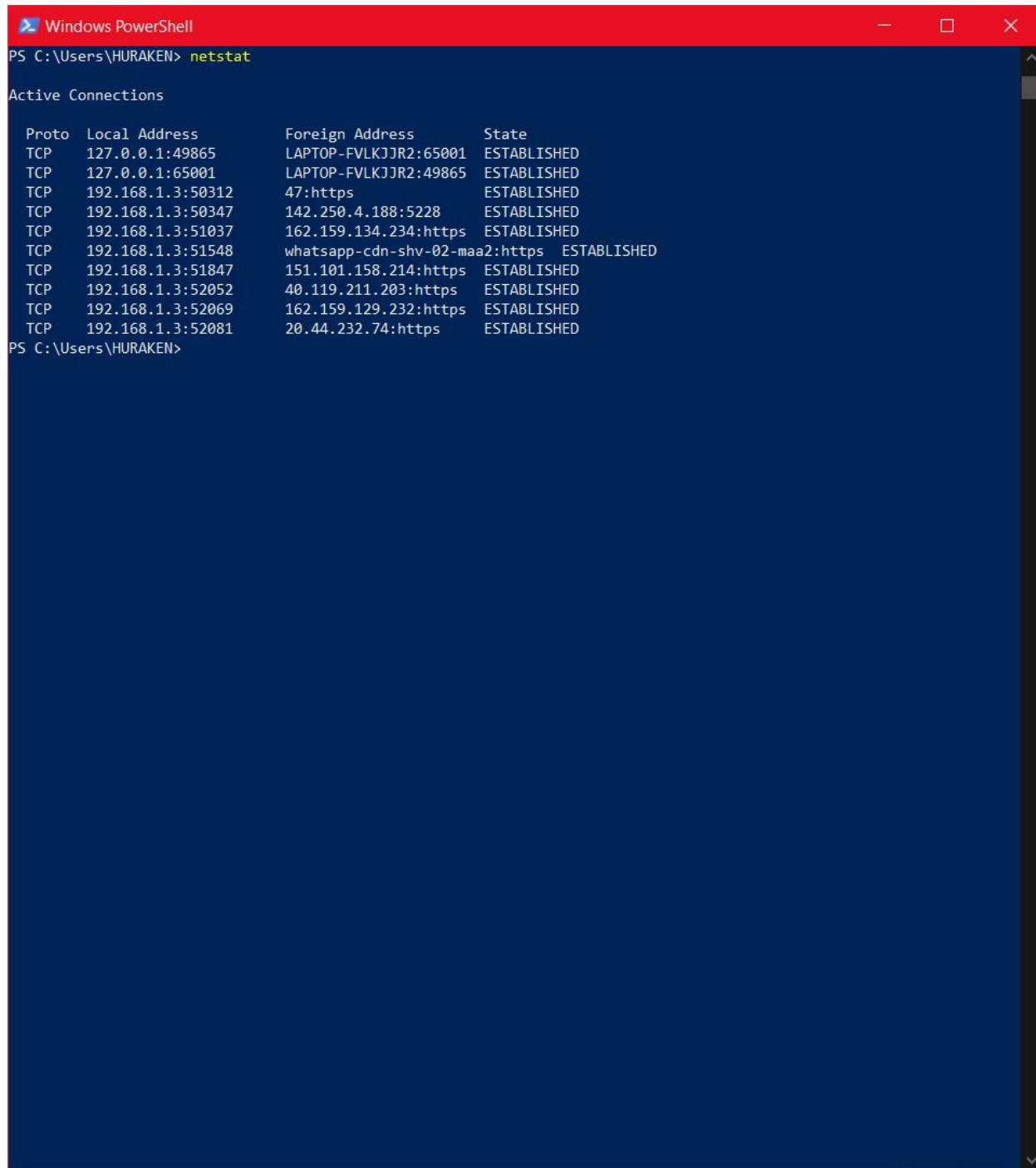
OPTIONS

- A Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.
- b Print the AS number in BGP packets in ASDOT notation rather than ASPLAIN notation.
- B buffer size
--buffer-size=buffer size
Set the operating system capture buffer size to buffer size, in units of KiB (1024 bytes).



8. Netstat

The network statistics (**netstat**) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.



A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the output of the "netstat" command. The output displays "Active Connections" with columns for Proto, Local Address, Foreign Address, and State. Most connections are in the ESTABLISHED state, with one notable connection to "whatsapp-cdn-shv-02-maa2:https".

```
PS C:\Users\HURAKEN> netstat

Active Connections

Proto  Local Address          Foreign Address        State
TCP    127.0.0.1:49865        LAPTOP-FVLKJJR2:65001  ESTABLISHED
TCP    127.0.0.1:65001        LAPTOP-FVLKJJR2:49865  ESTABLISHED
TCP    192.168.1.3:50312      47:https               ESTABLISHED
TCP    192.168.1.3:50347      142.250.4.188:5228  ESTABLISHED
TCP    192.168.1.3:51037      162.159.134.234:https  ESTABLISHED
TCP    192.168.1.3:51548      whatsapp-cdn-shv-02-maa2:https  ESTABLISHED
TCP    192.168.1.3:51847      151.101.158.214:https  ESTABLISHED
TCP    192.168.1.3:52052      40.119.211.203:https  ESTABLISHED
TCP    192.168.1.3:52069      162.159.129.232:https  ESTABLISHED
TCP    192.168.1.3:52081      20.44.232.74:https   ESTABLISHED

PS C:\Users\HURAKEN>
```

9.Dstat :

To view all your system resources instantly

```
Select huraken@LAPTOP-FVLKJJR2: ~
DSTAT(1)                               DSTAT(1)

NAME      dstat - versatile tool for generating system resource statistics
SYNOPSIS  dstat [-afv] [options..] [delay [count]]
DESCRIPTION
Dstat is a versatile replacement for vmstat, iostat and ifstat. Dstat overcomes some of the limitations and adds some extra features.

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).

Dstat also cleverly gives you the most detailed information in columns and clearly indicates in what magnitude and unit the output is displayed. Less confusion, less mistakes, more efficient.

Dstat is unique in letting you aggregate block device throughput for a certain diskset or network bandwidth for a group of interfaces, ie. you can see the throughput for all the block devices that make up a single filesystem or storage system.

Dstat allows its data to be directly written to a CSV file to be imported and used by OpenOffice, Gnumeric or Excel to create graphs.

Note
Users of Sleuthkit might find Sleuthkit's dstat being renamed to datastat to avoid a name conflict. See Debian bug #283709 for more information.

OPTIONS
-c, --cpu
    enable cpu stats (system, user, idle, wait), for more CPU related stats also see --cpu-adv and --cpu-use

-C 0,3,total
    include cpu0, cpu3 and total (when using -c/--cpu); use all to show all CPUs

-d, --disk
    enable disk stats (read, write), for more disk related stats look into the other --disk plugins

-D total,hda
    include total and hda (when using -d/--disk)

-g, --page
    enable page stats (page in, page out)

-i, --int
    enable interrupt stats

-I 5,10
    include interrupt 5 and 10 (when using -i/--int)

-l, --load
    enable load average stats (1 min, 5 mins, 15mins)

-m, --mem
    enable memory stats (used, buffers, cache, free); for more memory related stats also try --mem-adv and --swap

-n, --net
    enable network stats (receive, send)

-N eth1,total
    include eth1 and total (when using -n/--net)

-p, --proc
    enable process stats (runnable, uninterruptible, new)

Manual page dstat(1) line 1 (press h for help or q to quit)
```

```
huraken@LAPTOP-FVLKJJR2:~$ dstat
You did not select any stats, using -cdnqy by default.
Module dstat_disk24_old failed to load. (No suitable block devices found to monitor)
--total-cpu-usage-- --net/total-- --paging-- --system--
usr sys idl wai stl recv send in out int csw
14 6 80 0 0 0 0 0 0 0 119 66
1 1 98 0 0 0 0 0 0 0 0 0
1 2 97 0 0 0 0 0 0 0 0 0
1 1 99 0 0 0 0 0 0 0 0 0
0 0 100 0 0 0 0 0 0 0 0 0
0 1 99 0 0 0 0 0 0 0 0 0
0 1 99 0 0 0 0 0 0 0 0 0
1 1 98 0 0 0 0 0 0 0 0 0
0 1 99 0 0 0 0 0 0 0 0 0
0 0 99 0 0 0 0 0 0 0 0 0
1 2 97 0 0 0 0 0 0 0 0 0
1 1 98 0 0 0 0 0 0 0 0 0
0 2 97 0 0 0 0 0 0 0 0 0
1 2 97 0 0 0 0 0 0 0 0 0
2 4 93 0 0 0 0 0 0 0 0 0
0 2 98 0 0 0 0 0 0 0 0 0
```

10. Ifstat: to show interface activity

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal Jan 24 09:05 huraken@ubuntu: ~/Desktop

IFSTAT(1) System Utilities IFSTAT(1)

```
NAME
    ifstat - Report Interface STATistics

SYNOPSIS
    ifstat [-a] [-l] [-z] [-n] [-v] [-h] [-t] [-i if0,if1,...] [-d drv[:opt]] [-s [comm@[#]host[/nn]] [-T] [-A] [-w] [-W] [-S] [-b] [-q] [delay[/delay] [count]]

DESCRIPTION
    Ifstat is a little tool to report interface activity, just like iostat/vmstat do for other system statistics.

OPTIONS
    ifstat accepts the following options:

    -l Enables monitoring of loopback interfaces for which statistics are available. By default, ifstat monitors all non-loopback interfaces that are up.
    -a Enables monitoring of all interfaces found for which statistics are available.
    -z Hides interface which counters are null, eg interfaces that are up but not used.
    -i Specifies the list of interfaces to monitor, separated by commas (if an interface name has a comma, it can be escaped with '\'). Multiple instances of the options are added together.
    -s Equivalent to -d snmp:[comm@[#]host[/nn]] to poll a remote host through SNMP. See below for details.
    -h Displays a short help message.
    -n Turns off displaying the header periodically.
    -t Adds a timestamp at the beginning of each line.
    -T Reports total bandwidth for all monitored interfaces.

    -A Disables use of interface indexes: by default, when polling mechanism is index based (snmp, ifmib), ifstat remembers indexes of monitored interfaces to poll only them. However, if interfaces indexes change often (new interfaces added, etc), you might lose some stats, hence this flag. Note that if you ask ifstat to monitor a non existent interface, it will poll all interfaces until it finds the requested one (regardless of this flag) so you can poll for an interface that goes up and down.

    -w Uses fixed width columns, instead of enlarging them if needed for interfaces names to fit.
    -W Wrap lines that are larger than the terminal width (implies -w). Wrapped lines are prefixed with a cycling letter to ease reading.
    -S Keep stats updated on the same line if possible (no scrolling nor wrapping).
    -b Reports bandwidth in kbytes/sec instead of kbytes/sec.
    -q Quiet mode, warnings are not printed.
    -v Displays version and the compiled-in drivers.

    Manual page ifstat(1) line 1 (press h for help or q to quit)
```

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal Jan 24 09:04 huraken@ubuntu: ~/Desktop

IFSTAT(1) System Utilities IFSTAT(1)

```
huraken@ubuntu:~/Desktop$ ifstat
    ens33
    KB/s in KB/s out
    0.12   0.31
    0.18   0.43
    0.15   0.23
    0.00   0.00
    0.00   0.00
    0.39   0.29
    0.27   0.18
    0.35   0.45
    0.06   0.06
    0.00   0.00
    0.00   0.00
```

11. Wget used to retrieve files using HTTP, HTTPS, FTP, FTPS

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal Jan 24 09:06 huraken@ubuntu: ~/Desktop

huraken@ubuntu: ~/Desktop

huraken Wget

huraken@ubuntu: ~/Desktop

huraken WGET(1)

NAME

Wget - The non-interactive network downloader.

SYNOPSIS

wget [option]... [URL]...

DESCRIPTION

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.

Wget can follow links in HTML, XHTML, and CSS pages, to create local versions of remote web sites, fully recreating the directory structure of the original site. This is sometimes referred to as "recursive downloading." While doing that, Wget respects the Robot Exclusion Standard ([/robots.txt](#)). Wget can be instructed to convert the `l`inks in downloaded files to point at the local files, for offline viewing.

Wget has been designed for robustness over slow or unstable network connections; if a download fails due to a network problem, it will keep retrying until the whole file has been retrieved. If the server supports regetting, it will instruct the server to continue the download from where it left off.

OPTIONS

Option Syntax

Since Wget uses GNU getopt to process command-line arguments, every option has a long form along with the short one. Long options are more convenient to remember, but take time to type. You may freely mix different option styles, or specify options after the command-line arguments. Thus you may write:

```
 wget -r --tries=10 http://fly.srk.fer.hr/ -o log
```

The space between the option accepting an argument and the argument may be omitted. Instead of `-o log` you can write `-olog`.

You may put several options that do not require arguments together, like:

```
 wget -drc <URL>
```

This is completely equivalent to:

```
 wget -d -r -c <URL>
```

Since the options can be specified after the arguments, you may terminate them with `--`. So the following will try to download URL `-x`, reporting failure to `log`:

```
 wget -o log -- -x
```

The options that accept comma-separated lists all respect the convention that specifying an empty list clears its value. This can be useful to clear the `.wgetrc` settings. For instance, if your `.wgetrc` sets "exclude_directories" to `/cgi-bin`, the following example will first reset it, and then set it to exclude `/nobody` and `/somebody`. You can also clear the lists in `.wgetrc`.

```
 wget -X " -X /nobody,-/somebody
```

Most options that do not accept arguments are boolean options, so named because their state can be captured with a yes-or-no ("boolean") variable. For example, `--follow-ftp` tells Wget to

Manual page `wget(1)` line 1 (press h for help or q to quit)