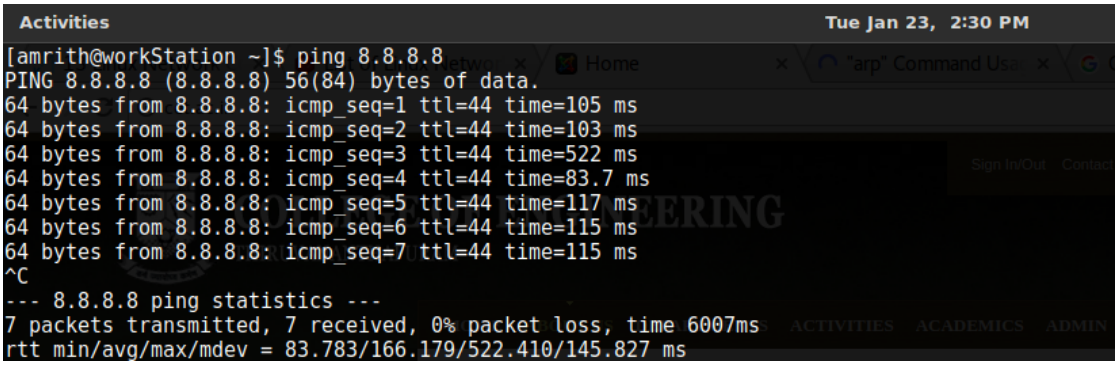
COLLEGE OF ENGINEERING TRIVANDRUM

Linux Network Commands

Amrith M
January 30, 2018

1 PING COMMAND

The ping command sends ICMP ECHO_REQUEST packets to network hosts and reports on the response from the remote server, outputting to standard output. It can be used to check if a remote host is up, or that network interfaces can be reached. It is frequently used to check whether a network connection is available between one machine and another. The ping command is useful for testing whether a remote server is available, checking your own network connection and verifying network issues.

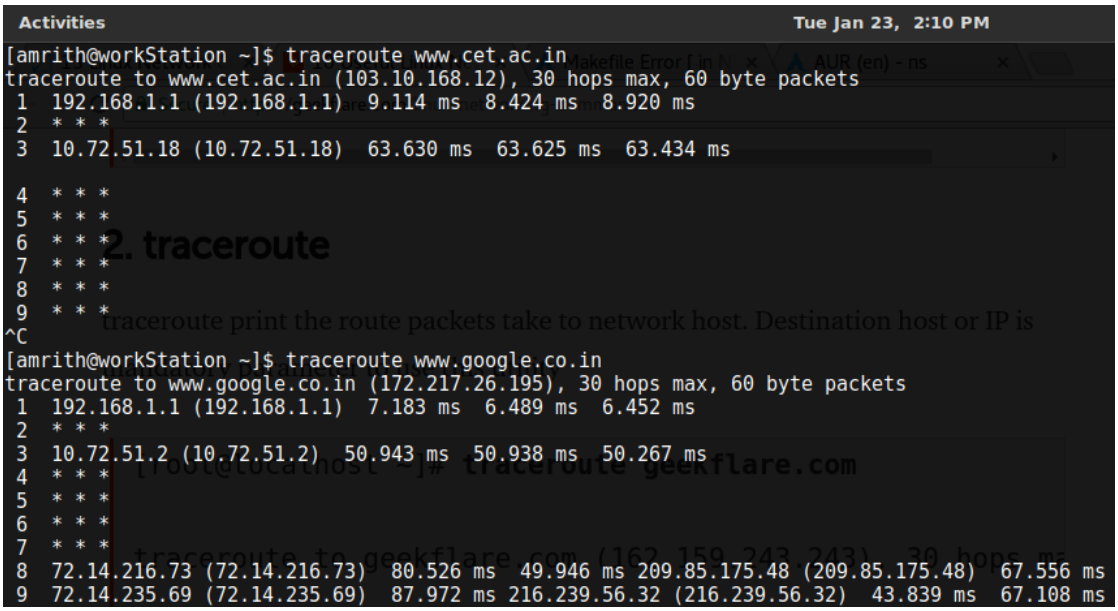


(1.1)

2 TRACEROUTE COMMAND

traceroute 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. It start its probes with a ttl of one and increases this by one

until it gets 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 5.0 seconds (default), an "*" (asterisk) is printed for that probe.



```
Activities                                                    Tue Jan 23,  2:10 PM
[amrith@workStation ~]$ traceroute www.cet.ac.in
traceroute to www.cet.ac.in (103.10.168.12), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  9.114 ms  8.424 ms  8.920 ms
 2  * * *
 3  10.72.51.18 (10.72.51.18)  63.630 ms  63.625 ms  63.434 ms

 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
^C
[amrith@workStation ~]$ traceroute www.google.co.in
traceroute to www.google.co.in (172.217.26.195), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  7.183 ms  6.489 ms  6.452 ms
 2  * * *
 3  10.72.51.2 (10.72.51.2)  50.943 ms  50.938 ms  50.267 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  72.14.216.73 (72.14.216.73)  80.526 ms  49.946 ms 209.85.175.48 (209.85.175.48)  67.556 ms
 9  72.14.235.69 (72.14.235.69)  87.972 ms 216.239.56.32 (216.239.56.32)  43.839 ms  67.108 ms
```

(2.1)

3 NSLOOKUP COMMAND

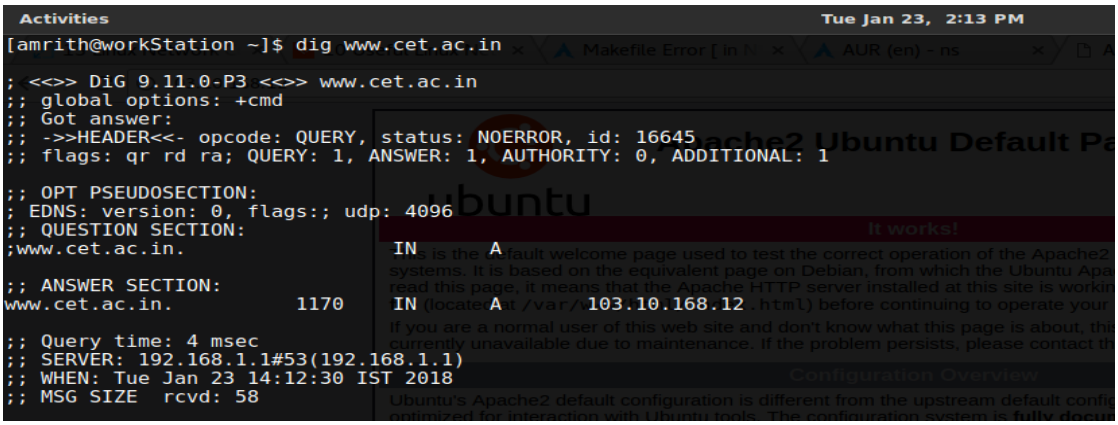
nslookup is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record.It is also used to troubleshoot DNS related problems. This article provides few examples on using the nslookup command.You can see that we have received a "Non-authoritative answer" to our query. An answer is "authoritative" only if our DNS has the complete zone file information for the domain in question. More often, our DNS will have a cache of information representing the last authoritative answer it received when it made a similar query; this information is passed on to you, but the server qualifies it as "non-authoritative": the information was recently

received from an authoritative source, but the DNS server is not itself that authority.

(3.1)

4 DIG COMMAND

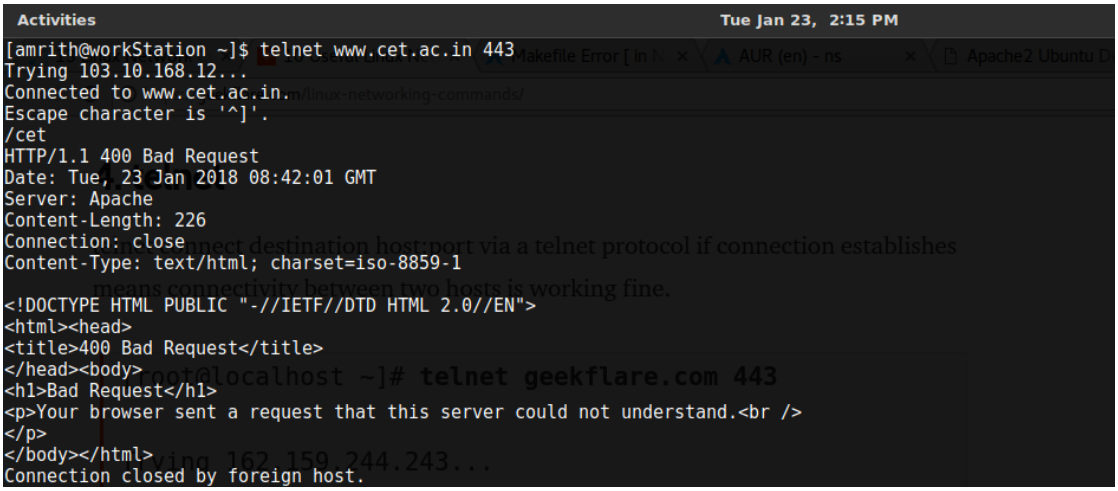
Dig stands for (Domain Information Groper) is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite. dig command replaces older tool such as nslookup and the host. dig tool is available in major Linux distributions.



(4.1)

5 TELNET COMMAND

The telnet command is used to communicate with another host using the TELNET protocol. Iftelnet is invoked without the host argument, it enters command mode, indicated by its prompt (telnet>) In this mode, it accepts and executes the commands listed below.If it is invoked with arguments, it performs an open command with those arguments.



```
Activities                                                    Tue Jan 23,  2:15 PM
[amrith@workStation ~]$ telnet www.cet.ac.in 443
Trying 103.10.168.12...
Connected to www.cet.ac.in.
Escape character is '^]'.
/cet
HTTP/1.1 400 Bad Request
Date: Tue, 23 Jan 2018 08:42:01 GMT
Server: Apache
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
</body></html>
Connection closed by foreign host.
```

(5.1)

6 IFCONFIG COMMAND

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 interface.

```
Activities                                                    Tue Jan 23,  2:06 PM
[amrith@workStation ~]$ ifconfig -a
enp7s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether fc:3f:db:d8:b7:db  txqueuelen 1000  (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

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 352  bytes 27552 (26.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 352  bytes 27552 (26.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp13s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.147  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2405:204:d202:cf6e:8fcb:78:b98a:18ab  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::de8a:2d2c:c1a4:1a53  prefixlen 64  scopeid 0x20<link>
        ether 30:f7:72:2a:1c:41  txqueuelen 1000  (Ethernet)
        RX packets 10732  bytes 6385957 (6.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10655  bytes 1867173 (1.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

(6.1)

7 ROUTE COMMAND

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 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.

```
[amrith@workStation ~]$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    600    0        0 wlp13s0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp13s0
```

(7.1)

8 WHOIS COMMAND

whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information. Most modern versions of whois try to guess the right server to ask for the specified

object. If no guess can be made, whois will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

```
Activities                                                    Tue Jan 23,  3:32 PM
[amrith@workStation ~]$ whois 2405:204:d202:cf6e:8fcb:78:b98a:18ab
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '2405:200::/29'

% Abuse contact for '2405:200::/29' is 'ip.abuse@ril.com'

inet6num:       2405:200::/29
netname:        RELIANCEJIO-IN
descr:          Reliance Jio Infocomm Limited
country:        IN
org:            ORG-RJIL1-AP
admin-c:        RJIL1-AP
tech-c:         RJIL1-AP
mnt-by:         APNIC-HM
mnt-lower:      MAINT-IN-RELIANCEJIO
mnt-routes:     MAINT-IN-RELIANCEJIO
mnt-irt:        IRT-RELIANCEJIO-IN
status:         ALLOCATED PORTABLE
remarks:        ----------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        ----------------------------------------------------
last-modified:  2017-09-26T23:29:11Z
source:         APNIC

irt:            IRT-RELIANCEJIO-IN
address:        Reliance JIO INFOCOMM LTD GHANSOLI INDIA
e-mail:         ip.abuse@ril.com
abuse-mailbox:  ip.abuse@ril.com
admin-c:        IBSP1-AP
```

(8.1)

9 ARP COMMAND

Arp manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one or display the current content.ARP stands for Address Resolution Protocol, which is used to find the media access control address of a network neighbour for a given IPv4 Address.

```
[amrith@workStation ~]$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   bc:8a:e8:15:b5:83   C                     wlp13s0
```

(9.1)

10 TCPDUMP COMMAND

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.

```
Activities   Chromium ▾                                   Tue Jan 23,  2:49 PM
[amrith@workStation ~]$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp13s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:48:39.264089 IP6 2405:204:d202:cf6e:8fcb:78:b98a:18ab.36148 > 2404:6800:4003:c03::bc.hpvroom: Flags [P.], seq
 3314713249:3314713282, ack 2883798453, win 349, options [nop,nop,TS val 1179478428 ecr 4206859646], length 33
14:48:39.268314 IP 192.168.1.147.50103 > 192.168.1.1.domain: 9334+ PTR? c.b.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.c.0.
3.0.0.4.0.0.8.6.4.0.4.2.ip6.arpa. (90)
14:48:39.357614 IP 192.168.1.1.domain > 192.168.1.147.50103: 9334 NXDomain 0/1/0 (150)
14:48:39.359949 IP 192.168.1.147.48455 > 192.168.1.1.domain: 35972+ PTR? b.a.8.1.a.8.9.b.8.7.0.0.b.c.f.8.e.6.f.c
.2.0.2.d.4.0.2.0.5.0.4.2.ip6.arpa. (90)
14:48:39.364389 IP 192.168.1.1.domain > 192.168.1.147.48455: 35972 NXDomain 0/0/0 (90)
14:48:39.366778 IP 192.168.1.147.47041 > 192.168.1.1.domain: 13319+ PTR? 1.1.168.192.in-addr.arpa. (42)
14:48:39.371035 IP 192.168.1.1.domain > 192.168.1.147.47041: 13319 NXDomain 0/0/0 (42)
14:48:39.372453 IP 192.168.1.147.33390 > 192.168.1.1.domain: 3677+ PTR? 147.1.168.192.in-addr.arpa. (44)
14:48:39.397328 IP6 2404:6800:4003:c03::bc.hpvroom > 2405:204:d202:cf6e:8fcb:78:b98a:18ab.36148: Flags [P.], seq
 1:34, ack 33, win 182, options [nop,nop,TS val 4206884048 ecr 1179478428], length 33
14:48:39.397365 IP6 2405:204:d202:cf6e:8fcb:78:b98a:18ab.36148 > 2404:6800:4003:c03::bc.hpvroom: Flags [.], ack
34, win 349, options [nop,nop,TS val 1179478468 ecr 4206884048], length 0
^C
10 packets captured
11 packets received by filter
1 packet dropped by kernel
```

(10.1)