

Network Tools

Note: For help refer “man” pages in Linux [*man command-name*].

ifconfig

Ifconfig is used to assign an address to a network interface and to configure network interface parameters. If no arguments are given, ifconfig displays the status of the currently active interfaces. Ifconfig is usually used at boot time to define the network address of each interface present on a machine. It may also be used at a later time to refine an interface's address or other operating parameters.

- a) Run “/sbin/ifconfig -a” on a Linux workstation and find the following:
 - i) IP address, its Class
 - ii) Is this a local or global address?
 - iii) Is subnetting used? What is the host number, the network number, and, if applicable, the subnet number?
 - iv) Hardware address
 - v) Default Gateway and DNS Servers
 - vi) What are the options to set the IP address, netmask and to bring up an interface?
 - vii) Can you determine the broadcast address? If so, what is it?
 - viii) What is the IP address of the primary DNS server?
 - ix) What is the host name and network name for the computer?
 - x) What is the default gateway for the computer?
 - xi) What type of data-link network is being used and, if applicable, what is the data-link address?

Can you determine if DHCP is used? If so, what are the DNS parameters?

Note: Use man ifconfig for help

ping

The ping utility is one of the more useful utilities for testing a network. Ping is a program for testing whether a remote host is up or not. Some versions of ping also measure how fast the connection is. The ping utility works by sending a short message of type echo-request to a host using a network protocol called ICMP, the Internet Control Message Protocol. A host that supports ICMP (and most do) and receives an echo-request message simply replies by sending a short ICMP message of type echo-response back to the originating host.

- a) Try pinging local host, a host in the Karunya network and one of your favourite websites. What can you tell from the outputs and what you cannot tell?
- b) Try the flag -R. What extra information do you get?
- c) Try the flag -A. What does it do?
- d) Use the -t flag to set the time to live. What's the smallest value for which you receive response packets? In what sense does this number measure a

"distance"?

- e) Compare output from the ping program for a computer that's turned off with the output of a non-existent address (like 10.0.0.50). Do they differ?
 - f) Two numbers are reserved in the final octet of the dotted decimal notation, that is, there are two numbers never used for host IP addresses in the final digit z of an IP address of the form w.x.y.z. What are these numbers? What happens if you ping one of these numbers on your local subnet?
 - g) For the following hosts, send 20 packets, each with a length of 56 data bytes. Indicate what percent of the packets resulted in a successful response. For the packets from which you received a response, write down the minimum, average, and maximum round trip times in milliseconds. Note that ping reports these times to you if you tell it how many packets to send on the command line.
 - www.karunya.ac.in, www.stanford.edu, www.kyoto-u.ac.jp, www.cca.vu.nl.
 - i) Compare the round trip times. How strong is the relationship between round trip time and geographical distance?
 - ii) You may find that the packet responses are 64 bytes instead of 56 bytes. Look at RFC 792 to find out the reason.
 - iii) For 56-byte packets, what can you say about the differences in the minimum round-trip times? What reason can you give to explain why these differences occur?
 - iv) For same hosts listed above, send 20 packets that have lengths of 512 data bytes and 1024 data bytes. Write down the minimum, average, and maximum round trip times in milliseconds.
 - v) When comparing 56-byte packets, 512-byte packets, and 1024-byte packets, what can you say about the difference in minimum round-trip times to the same host?
- h) For a range of packet sizes, plot the round trip time versus the packet size. Fit a line to this curve and compute its slope and intercept. The slope of the line is the marginal additional time per additional byte, which is the inverse of bandwidth. Compute the inverse of the slope and compare it to the bandwidth you expected to get from the network.

arp

The arp program is used to display and modify the Internet to Ethernet address translation tables. The host may be specified by name or by number, using Internet dot notation.

a) Each Ethernet device uses a 48-bit address. Each address can be divided into two parts, a 24-bit Organization Unique Identifier (OUI) and a 24-bit assigned address. Each Ethernet manufacturer is assigned a different OUI by the IEEE. It uses these as the first 24 bits of the address of every interface it manufactures. You can look up an OUI at the site <http://standards.ieee.org/regauth/oui/index.shtml>. Find the manufacturer of your ethernet card.

- b) How do you show the full ARP table for your machine?
- c) If you try and use the arp command to add or delete an entry to the ARP

table what happens?

Why do you suppose this the case? How can you affect (add, delete, or change) entries in the ARP table?

d) You still have the ability to modify the ARP table, just not directly. Use the ping command to ping one of the other computers on the network that is not currently in your ARP table. Use this mechanism to add at least two new hosts to the ARP table. Why might the first ping take longer than the rest?

e) Delete all entries in your ARP table. Use the ping command to ping a device outside of your network where the ping must be forwarded by the default gateway. You can use a URL instead of an actual IP address. Explain why the ARP request was for the default gateway and not the IP address of the ping. How did the host decide this?

f) How long do entries stay cached in the ARP table? Describe a trial-and-error method to discover the timeout value. Is this dependent on the operating system?

g) What is the command to create a static ARP entry? Create a static ARP entry to another device on the local network. Show the commands and the outputs.

h) Do routers have ARP tables? Do routers need to do ARP requests or ARP replies? Explain.

i) Explain why two hosts connected to the same switch or hub must have IP addresses that belong to the same subnet in order to communicate without using a router.

traceroute

Traceroute is a program which finds out the route to another host. It can also help spot traffic bottlenecks and fast routes.

a) Try traceroutes to several different interfaces or workstation in our LAN.

b) Try a traceroute to an Internet website like www1.yahoo.com. How many routers/gateways are there between your system and that server? Which router in our LAN is our "gateway" router, based on your traceroute? By looking at the names of the intermediate routers, can you tell where the packets went, geographically?

c) Sometimes, a router or workstation doesn't respond (a "*" in the traceroute). Any thoughts on why this is the case?

d) Looking glasses are web sites that allow you to run simple network analysis programs like ping and traceroute from their sites.

The site <http://www.traceroute.org/> maintains a list of such sites. Visit one of these sites and do a trace to Karunya network. Try to find a site that is reasonably close. But don't abuse these sites. Be sure to record the source address for the site you use.

e) For this exercise, you need to use the traceroute server at <http://www.getnet.com/cgi-bin/trace>. Enter the name or IP address of our gateway machine where it says "Enter search keywords:" and press return. The traceroute server will execute traceroute on the machine running the webserver. Now run traceroute trojan.neta.com on your machine. Can you figure out a way to tell the path which people from outside take to get to Karunya network?

f) We want to traceroute to a non-existent machine outside of Karunya. The first problem is how do we know that a particular machine does not exist? If we just pick an IP address and ping it, why is that not sufficient?

g) Describe what is strange about the observed output when executing the command `traceroute 18.31.0.200`, and why traceroute gives you such an output. The man page has useful hints to help you understand the output better.

nslookup

Nslookup is a tool which can be used many purposes: to find out whether a given domain exists, what are the name servers of a domain, what are its e-mail servers, etc.

a) You can lookup domain registration information by going to the appropriate registrar. For the edu domain, go to <http://whois.educause.net>. Enter the domain for karunya.edu. You should be able to identify the administrative contacts for the domain and the name server for the domain. What else can you discover?

b) What is the IP address of Karunya Mail Server and Karunya Web Server?

c) From which machine is this information coming from? Why is it coming from this machine?

d) What are the authoritative name servers of karunya.ac.in and karunya.edu domains?

e) Find the IP addresses of Web Server, Mail Server and DNS Server of yahoo.com and yahoo.co.in domains.

f) How many of the different kinds of records (SOA, NS, CNAME, A, MX, etc) are there in the cis.ksu.edu domain?

g) nslookup can be used as both an interactive or command-line tool. If you enter nslookup without an argument, you will enter interactive mode. You can type a "?" for a brief list of commands options. I want to find the IP address of where my email to wards@hotmail.com goes. What you really need to do is find the "mail exchanger" for hotmail.com. There is an option in nslookup that tells you what the mail exchanger is for hotmail.com. Figure out the exact syntax of the format of this command, and execute it. Now what is the IP address of where my email to hotmail goes?

h) DNS can also be used for reverse name lookup, i.e., converting an IP address into a host name. This can be important if you want to know who is visiting your site. For example, due to laws limiting the export of encryption software, you may want to check the address of a system trying to download such software from your server. Try looking up 205.153.63.30 using nslookup.

dig

Dig (Domain Information Groper) is used to send domain name query packets to name servers to gather information from the Domain Name System servers about the mapping of host names to IP addresses or vice versa. See man pages for dig, resolver, resolv.conf, named, host and nslookup for more information on name resolution.

a) For this problem, you will go through the steps of resolving a particular hostname, by iterating through a series of servers, just like a regular server

might. Assuming it knows nothing else about a name, a DNS resolver will ask a known root server (rendezvous point).

The root servers on the Internet are in the domain root-servers.net, some of which are included in the list from the response above. Use dig to ask one of these servers the address of redlab.lcs.mit.edu without recursion. What command do you use to do this? It is unlikely that these servers actually know the answer so they will refer you to host (or list of hosts) that might know more. Go through the hierarchy without recursion and following the referrals manually until you have found the address of the machine. What is the address? Display the output of the final command. How many iterations did it take? What commands did you use for each one?

b) Ask your default server for information, without recursion, about the host www.dmoz.org.

i) What command did you use? Does it have the answer in its cache? How do you know? How long did this query take? If this information was cached, please find some other host name that is not cached and do this section with that other host.

ii) Now, ask your default this same query but use recursion. It should return an answer for you. How long did this take?

iii) Finally, ask your default server again without recursion. How long does this request take? Has the cache served its purpose?

iv) Watch the TTL decrement on the cache by repeating the previous step. If you wait long enough, you can watch it return to the original state and then you can repeat this cycle. A good host to play with for this might be ad.doubleclick.net.

If you look at this, do you notice anything else interesting about the responses that you get back?

whois

whois program uses information from InterNIC database which registers domain names for the Internet.

a) List some websites which provide whois service?

b) Using one of those website find the information about karunya.ac.in domain. Find the IP addresses reserved for it, DNS servers, Contact information etc.

c) What happens when I send email to president@whitehouse.gov. Run the following two commands:

```
whois -h whois.arin.net 198.137.241.40
```

```
whois -h whois.arin.net whitehouse.gov
```

Where did I get the IP address: 198.137.241.40? What can you say about the reason that each commands returns a different set of information?

d) What machine has IP address 198.182.196.56? What machines act as the DNS nameserver for the domain that 198.182.196.56 is in?

e) Find out who owns the website of President of India and www.gmail.com.

netstat

Netstat displays the contents of various network-related data structures in various formats, depending on the specified options. netstat displays a list of active sockets for each protocol. Netstat interval displays running statistics of packet traffic on configured network interfaces; the interval indicates the number of seconds in which to gather statistics between displays. The -r option displays the current kernel routing table.

a) By using netstat figure out the number of interfaces on your machine. In the output you'll find an interface named lo0. Can you say any function of this interface?

b) What parameters for netstat should you use to show all the TCP connections established?

c) What does netstat -r show? What are each of the fields in this output?

d) Try using netstat in your machine while you are logged in the Linux Server (192.168.2.1).

Execute the command in the Linux Server and identify the connection between your machine and the Server from both the outputs.

route

a) What does route command show?

b) Print the routing table of your machine using route command. Identify the network address, broadcast address, loopback address and the gateways to route the packets with those addresses.

netsh

Find out the use of netsh command

ip

Find out the use of ip command
