CS315 : Computer Networks Lab

Assignment 1

Sourabh Bhosale (200010004)

January 3, 2023

1 Task 1: Background

Trying out the following commands and writing the understanding of the output:

- ping www.google.com :

  It will measure the round-trip time (duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point) for messages sent from the originating host to a destination computer that are echoed back to the source. The terminal output includes a summary table that lists the corresponding response time, the packet size as well as the TTL per response packet.

- traceroute www.google.com :

  The command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.

- arp

  ARP stands for Address Resolution Protocol. arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. The primary function of this protocol is to resolve the IP address of a system to its mac address.

- ifconfig

  ifconfig(interface configuration) command is used to configure the network interfaces. With this command you can view IP Address and Hardware / MAC address assign to interface. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.

- hostname

  Main purpose of this command is to set or display the name of the current host system.

- /etc/hostname

  This file stores your system's host name, your system's fully qualified domain name.

- /etc/hosts

  The /etc/hosts file contains the Internet Protocol (IP) host names and addresses for the local host and other hosts in the Internet network. This file is used to resolve a name into an address (that is, to translate a host name into its Internet address). This file needs to always contain an entry for an IP address, if the machine is connected to the network.

- /etc/resolv.conf

  It is used to configure dns name servers. The file /etc/resolv. conf file contains information that is read by the resolver routines the first time they are invoked by a process. It lists nameservers that are used by your host for DNS resolution. If you are using DHCP, this file is automatically populated with DNS record issued by DHCP server.

- /etc/protocols

  Protocols definitions file. The /etc/protocols file contains information regarding the known protocol. For each protocol, a single line should be present with the following information:

  official_protocol_name protocol_number aliases

- /etc/services

  /etc/services file contains a definition of the networks, services and the associated port for each protocol that are available on this system

2 Task 2: Warm-up Questions

(i) What is your machine's hostname and IP address? How did you get this information.

Hostname : sysad-OptiPlex-7050-1
IP address : 10.250.65.132
By running the following commands, I got the information:

1. `$ hostname`
2. `$ ifconfig or $ hostname -I`

(ii) What is the next hop router's IP address and MAC address? How did you get this information?

Hop router's IP address: 10.196.3.250
MAC address : 02:04:96:9a:82:e8
By running the following commands, I got the information: `$ traceroute and $ arp`

(iii) What is the local DNS server's IP address? How did you get this information?

Local DNS server's IP address : nameserver 127.0.0.53
By running the following commands, I got the information: `$ cat /etc/resolv.conf`

(iv) What do the numbers in the file /etc/protocols represent?

Numbers in the file /etc/protocols are the protocol numbers. The protocol number is a single byte in the third word of the datagram header. The value identifies the protocol in the layer above IP to which the data should be passed.

(v) What is the port number associated with applications: ssh, ftp, nfs, smtp (email)? How did you get this information?

Port numbers associated with applications ssh, ftp, nfs, smtp (email) are:
ssh : 22 , ftp : 20, 21 , nfs : 2049, smtp : 25
By running the following commands, I got the information: $ cat /etc/services

(vi) How many of these questions can you answer for the phone running on android/ios?

First three questions can be answered on the phone running on android/ios, but the iv and v requires accessing the files which are present in the phone but are not accessible easily. We will need external third party application to get the information regarding iv and v in phone.

3 Task 3. Questions

(i)The Unix utility Ping can be used to find the RTT to various Internet hosts. Read the man page for ping, and use it to find the RTT to the following websites : www.amazon.in and www.iitb.ac.in

RTT to the www.amazon.in :
rtt min/avg/max/mdev = 35.140/35.450/35.705.0.201 ms

(a) Explain the results that you obtain; For example, the success and failure of the Ping.

The ping for amazon.in succeeds but for iitb.ac.in it fails. If you ping a destination by IP address, and the ping succeeds, you know you have basic connectivity. If you ping the same destination by hostname, and it fails, you know name resolution is not working. This is because ping could not resolve the given hostname to an IP address in the second test. Also, the case maybe that iitb.ac.in may have blocked the ping requests.

(b) What are the reasons for the values of RTTs that you see?

RTT is a measure of how long it took to receive a response. Measured in milliseconds (ms), the process starts when a browser sends a request to a server and is completed when a response from the server is received. RTT is a key performance metric of web applications. RTT values present here fluctuate due to traffic and other factors.

Read the man page for the Unix utility Traceroute and use it for the website www.amazon.in

(a) Explain what you see. Whenever successful, draw a network map from your machine to the destination, which includes the hop addresses obtained from Traceroute.

The command is used to reach the amazon.in host from the local machine and it also prints detail about all the hops that it visits in between.

```
traceroute to www-amazon-in.customer.fastly.net (162.219.225.220), 64 hops max
 1   172.27.240.1  0.602ms  0.309ms  0.334ms
 2   10.196.3.250  2.937ms  3.469ms  4.589ms
 3   10.250.209.251  3.064ms  9.984ms  3.075ms
 4   14.139.150.65  4.265ms  2.998ms  4.615ms
 5   *  *  *
 6   *  *  *
 7   10.255.221.33  21.200ms  22.937ms  25.785ms
 8   115.247.100.29  35.954ms  36.486ms  35.934ms
 9   *  *  *
10   *  *  *
11   162.219.225.220  43.717ms  42.034ms  44.464ms
```

Figure 1: `Network Map`

(b) How can you change the maximum hop number?

From man 1 traceroute:

`-m or -max-hop=num`

Specifies the maximum number of hops (max time-to-live value). The default is 30.

(c) What do the three timestamps signify in the result of Traceroute?

RTT Columns - The next three columns display the round trip time (RTT) for your packet to reach that point and return to your computer. This is listed in milliseconds.

(d) What is the use of TTL (Time To Live) field in ICMP packets?

TTL means "time to live". It is a value on an ICMP packet that prevents that packet from propagating back and forth between hosts ad infinitum. Each router that touches the packet decrements the TTL. If the TTL ever reaches zero, the packet is discarded.