Malineni Anusha, Student ID: 1623382

Assignment-1

Network Architecture – 1, Fall 2016

1. Suppose two hosts, A and B are separated by 40,000 kilometers and are connected by a direct link of R=1 Mbps. Suppose the propagation speed over the link is $2*10^8$ meters/sec. Consider sending a file of 4,000,000 bits from Host A to Host B.

a. Suppose the file is sent continuously as one big message. How long does it take to send the file, assuming it is sent continuously?

Solution:

Given,
Distance between A and B (D) = 40,000km

R = 1 Mbps = 10^6 bits

S = $2*10^8$ meters/sec

L = $4*10^6$ bits

So, considering the formula for time taken

Time Taken = propagation delay+ queuing delay + processing delay + transmission delay

Since it is a direct link, processing delay and queuing delay will be 0

Transmission Delay = L/R

= $4*10^6/ 10^6$

= 4 seconds

Propagation delay = D/S

= $40000 * 10^3 / 2 * 10^8$

= 0.2 seconds

Time taken (T) = 4 + 0.2 = 4.2 seconds

b. Suppose now the file is broken up into 500 packets with each packet containing 2,000 bits. Suppose that each packet is acknowledged by the receiver and the transmission time of an acknowledgement packet is negligible.

Finally, assume that the sender cannot send a packet until the preceding one is acknowledged. How long does it take to send the file?

Solution:
Given,
L = 4000
Number of packets = 1000
D = 40,000km
R = 1 Mbps = 10^6 bits
S = $2*10^8$ meters/sec

Given that transmission time of an acknowledgement packet is negligible.

Total time taken by each packet = Propagation delay (sender) + Transmission delay (sender) + Propagation delay (receiver) + Transmission delay (receiver)

But Transmission delay (receiver) = 0 (Given)

Propagation Delay (sender) = D/S

= $40000 * 10^3 / 2 * 10^8$

= 0.2 seconds

Transmission delay (sender) = L/R

= $4000 / 10^6$

= 0.004 seconds

Propagation delay (receiver) = D/S

= $40000 * 10^3 / 2 * 10^8$

= 0.2 seconds

Time Taken for each packet= 0.2 + 0.004 + 0.2 = 0.404 seconds

Time Taken for 1000 packets to be sent = 1000*0.404 = 404 seconds

c. Calculate the bandwidth-delay product, $R*t_{prop}$. What does it mean? (Provide an interpretation of the bandwidth-delay product.)

Solution:
Bandwidth-delay product = $R*t_{prop}$
= $10^6 * 0.2$

$= 2*10^5$ bits.

d.If there are two routers between Host A and B (rather than a direct link), and all three links have 1 Mbps links, how long does it take to send the file? (use the assumptions in 1.b)

Solution:

Given two routers R1 and R2 between A and B,

So, there will be total 3 links (A to R1, R1 to R2, R2 to B).

Total transmission delay will be 3*(L/R)

Given that transmission time of an acknowledgement packet is negligible.

Total time taken by each packet = Propagation delay (sender) + Transmission delay (sender) + Propagation delay (receiver) + Transmission delay (receiver)

But Transmission delay (receiver) = 0 (Given)

Propagation delay (Sender) = D/S

$= 40000 * 10^3/2 * 10^8$

$= 0.2$ seconds

Transmission delay (Sender) = 3(L/R)

$= 3*(4000)/10^6$

$= 0.012$ seconds.

Propagation delay (Receiver) = D/S

$= 40{,}000* 10^3/2* 10^8$

$= 0.2$ seconds.

Total time taken by each packet = 0.2 + 0.012 + 0.2

= 0.412 seconds.

Now, total time taken for 1000 packets = 1000* 0.412

= 412 seconds.

So, total time taken to send all the packets from A to B is = 412 seconds.

2. Read articles on two Internet pioneers from http://www.ibiblio.org/pioneers/index.html, and write 1~2 paragraph(s) of your personal perspective (why you chose the person, what part of the story strikes/interests you, or what you learned from the story, etc.) on each person's story (thus 2~4 paragraphs total).

Answer:

Vannevar Bush:

Bush was born on March 11, 1890, in Chelsea, Massachusetts. Though he was not involved in the creation or development of internet, he is known as Godfather of our wired age with reference to his article “As we may think”. In this article, Bush described a theoretical machine "memex," which was to intensify human memory by allowing the user to store and retrieve the documents which are linked by associations, and also this associative linking was very similar to that of hypertext known today. Through this machine, Bush hoped to transform an information explosion into a knowledge explosion.

Bush’s solution to the problem of information consultation is a device called the memex which is essentially a desk with two screens on it, switches and leavers, and magnetic tape for recording and storing data. Technical specifics aside, the brilliance of the memex and how it tackles the problem of information access is by way of associative indexing. Basically, Bush conceived of a machine that worked in much the same way the world wide web does by way of associations and hypertextuality. By creating “trails” of associated information, one could create and share collections of connected data which would not only be more intuitive, but would rapidly increase the speed and depth of research and information sharing.

Paul Baran:

Paul Baran was born on April 29, 1926 in Poland who was a pioneer in the development of computer networks. He gave two main ideas that became very important in the development of the ARPANET. The first idea was about the idea of building a distributed network and the second idea was a technique for data transmission that was later called as packet switching.

The main idea of packet switching is to divide the big message in to message blocks rather than sending the complete message at a time. These message blocks are called as packets. Baran also extended his work in packet switching to wireless-spectrum theory, developing what he called "kindergarten rules" for the use of wireless spectrum. In addition to his innovation in networking products, he is also credited with inventing the first doorway gun detector.

3. Discuss on computer virus, worm, spyware, malware, Trojan horse, and botnet (1~5 sentences each).

Answer:

Computer Virus:

Computer virus is a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. All computer viruses are man-made. A computer virus is a program that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. Virus performs harmful activities like stealing hard disk space, corrupting data etc. However, we can install any antivirus like Avg, Mcafee etc., to get rid of computer virus.

Worm:

A computer worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worm is a malware programs that spreads on itself and is not made by humans. It spreads to other computers with the help of computer networks, relying on security failures on the target computer to access it. Worm only cause some damage to the computer like reducing the bandwidth of the network but does not infect the computer by changing the files whereas virus affects the computer files.

Spyware:

The definition of spy explains as a person who secretly collects information on the activities, movements, and plans of an enemy or competitor and reports them. In the similar way, spyware is a software that helps in collecting information about a person or organization without their knowledge and may send such personal information to other entity. Spyware can collect almost any

kind of data such as user login details, credit card details etc. A spyware infestation can create harmful things such as significant unwanted disk usage, network traffic and CPU activity.

Malware:

Malware, short for malicious software. It is a software used to disrupt or damage the computer operation or system without the user's consent, collect sensitive and private information, or gain access to private systems. Malware is sometimes called as computer contaminant. It is also used as the general term covering all the different types of threats to computer safety such as viruses, spyware, worms, trojans, rootkits etc.

Trojan horse:

Trojan horse or Trojan is a software which misrepresents itself to the user as useful, routine, or interesting in order to force the user to install it but instead introduces viruses onto computer. Trojans cannot self-replicate. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth.

Botnet:

A Botnet also referred as a zombie army is a collection of number of computer systems connected through internet that are been set up to forward transmissions to other computers on the Internet while the owners are unaware of it. They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Botnet is a combination of a 'robot' and a 'network'.

Laboratory Homework

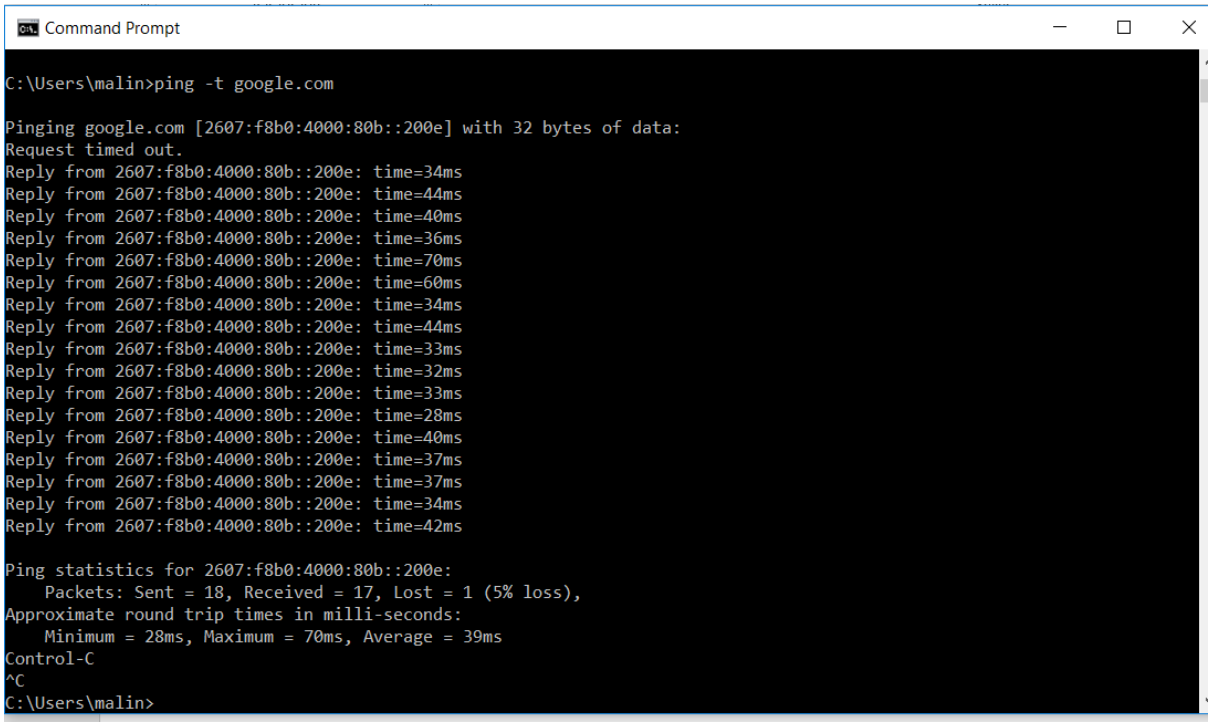
4. Explore 'ping' and 'traceroute' (or 'tracert' on Windows) which are basic tools used to measure network performance and retrieve network status. Run 'ping' and 'traceroute' with at least three different hosts and options. Record the commands and their output.

Answer:

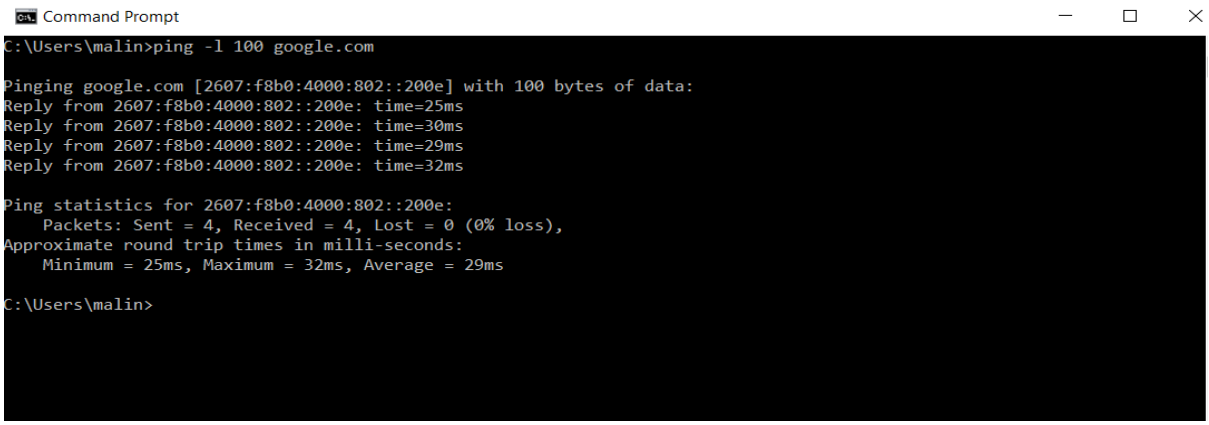
Ping: This is a tool or a networking utility program to test if the particular host is reachable. The term 'ping' can refer to the time it takes for a data packet to

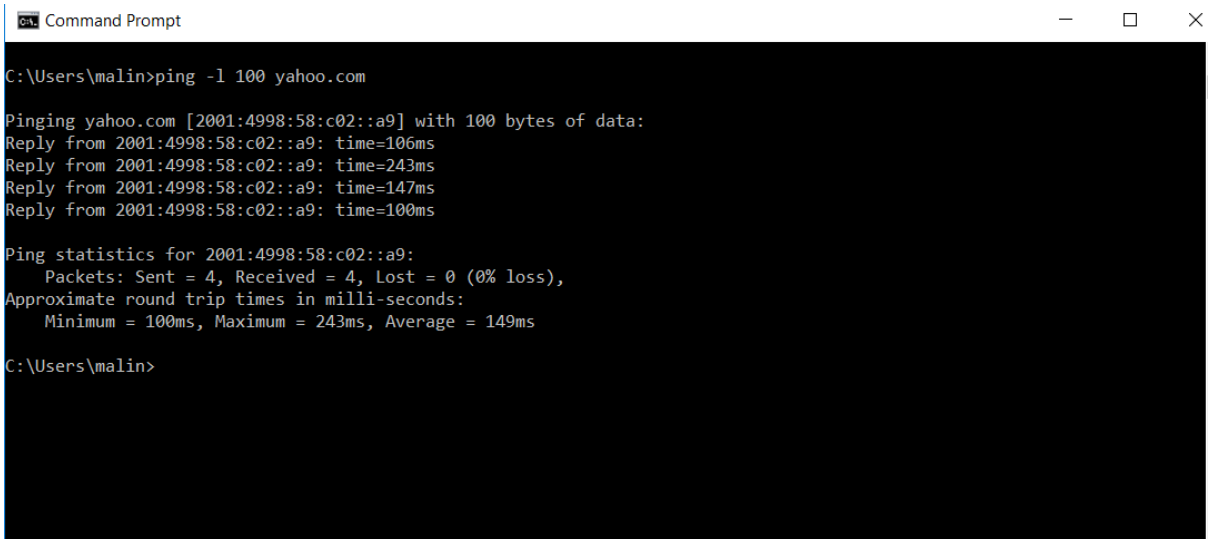
travel round-trip. It is a diagnostic that checks if the computer is connected to a server. In a network computer, a ping test is a way of sending messages from a computer to another.

Ping –t: this will ping the target until we stop with control c

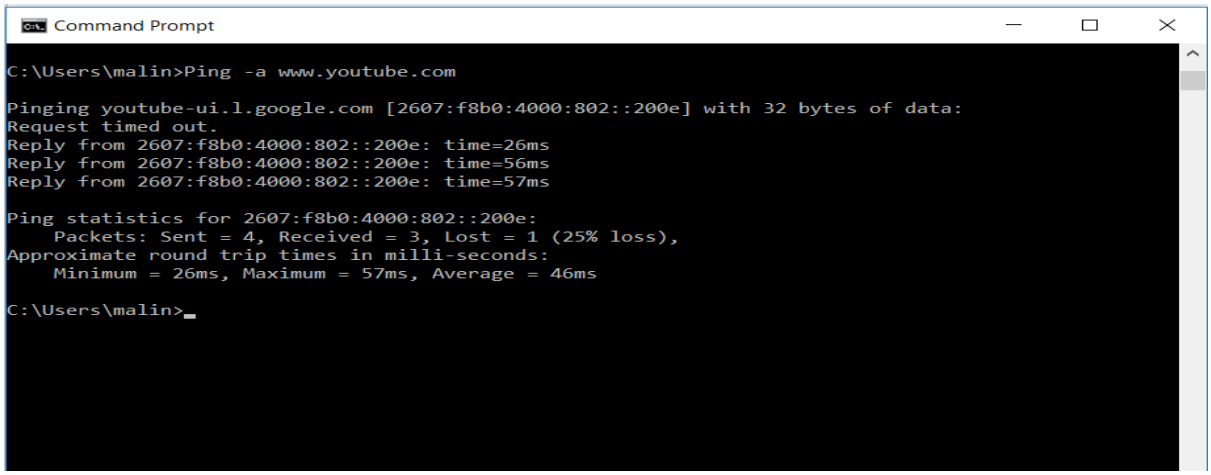


Ping **-l** *size:* this option is used to set the size, in bytes, of the echo request packet from 32 to 65,527.



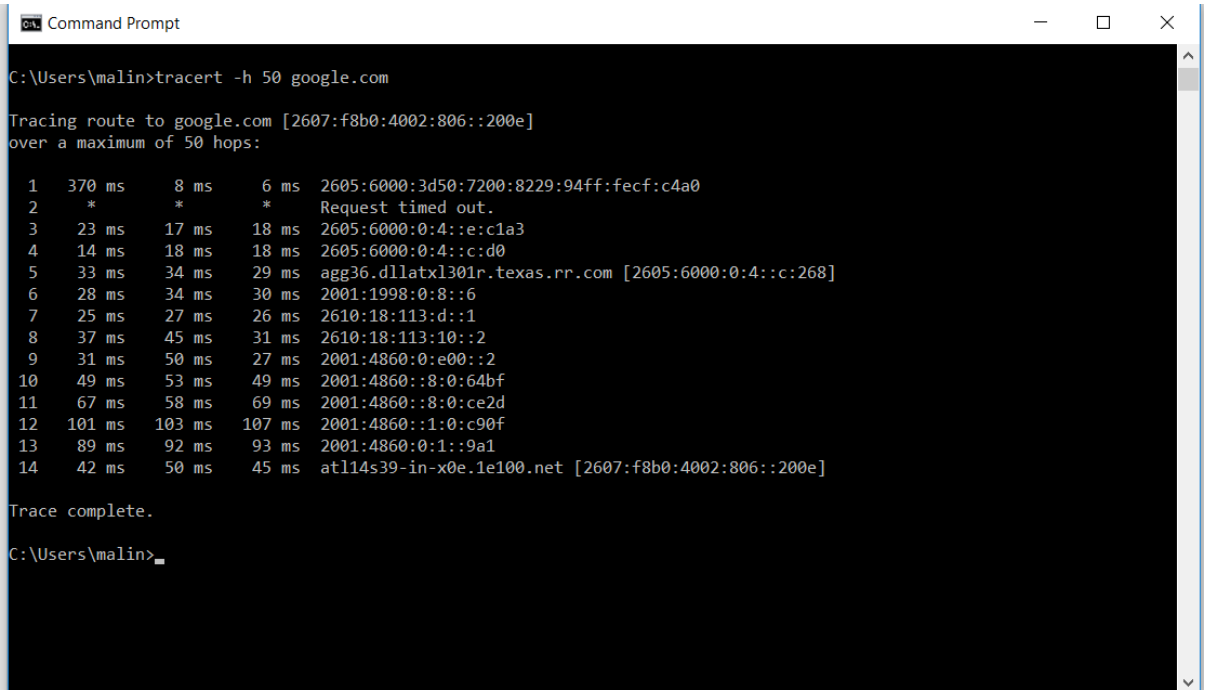


Ping –a: this ping option will resolve the host name

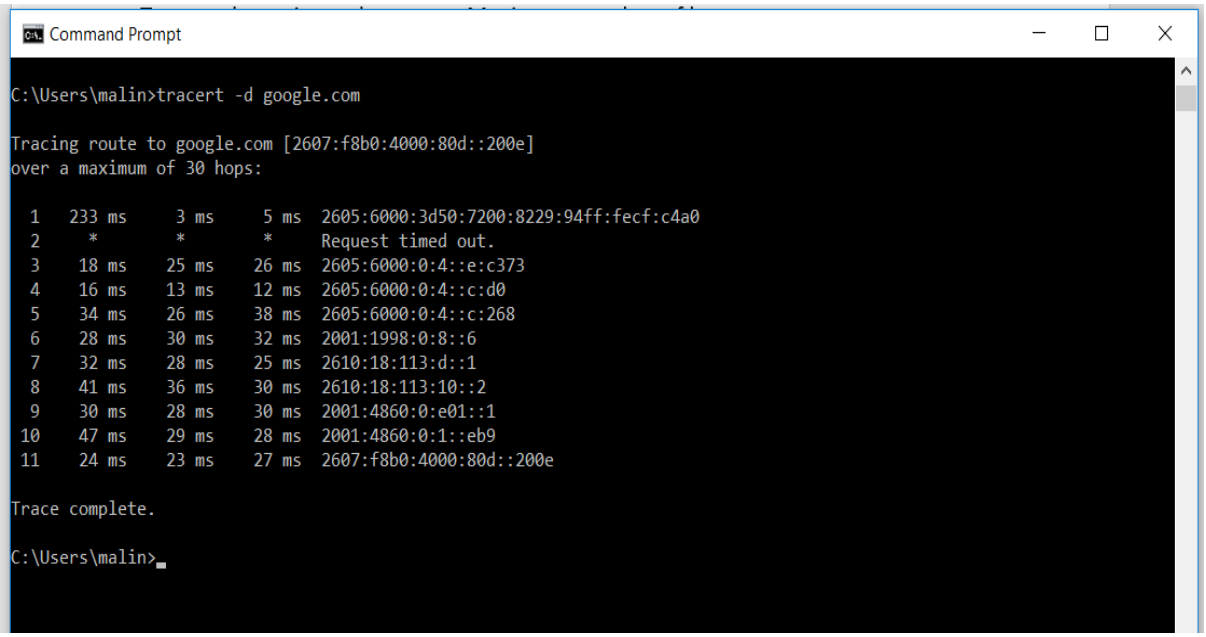


Tracert: This is a utility that records the route through the Internet between the requested computer and a specified destination computer.

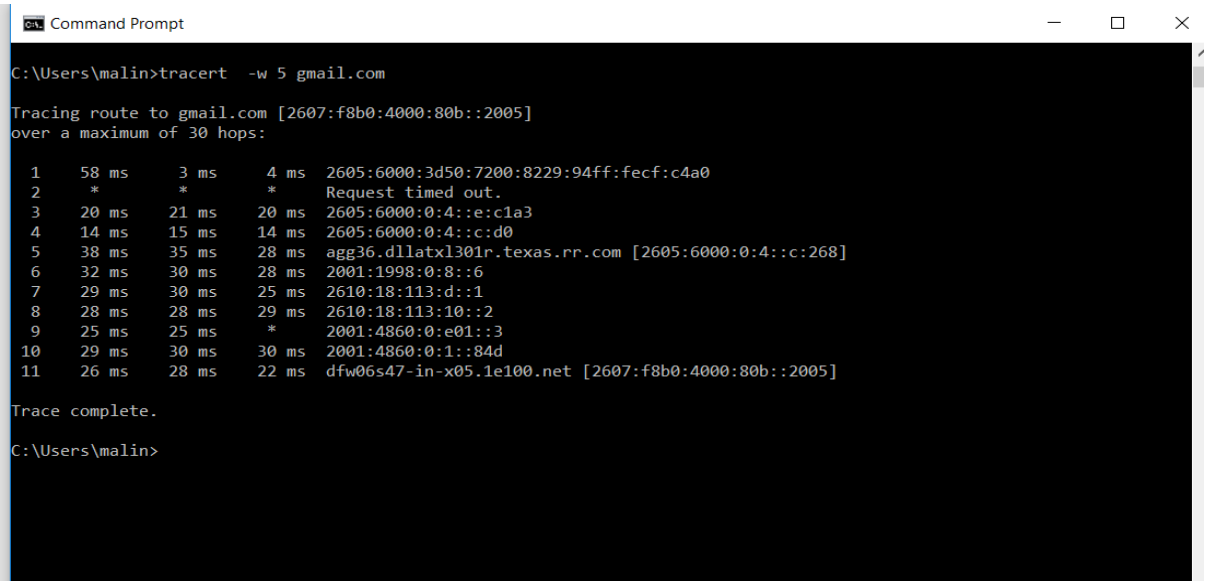
Tracert –h maximum hops: Maximum number of hops to search for target



Tracert –d: do not resolve addresses to host name



Tracert –w timeout: wait timeout milliseconds for each reply



5. Explore ‘nslookup’ which is a program to query Internet domain name servers. Particularly,

a. find out the ip address(es) of www.yahoo.com

b. find out the name servers and their IP addresses of yahoo.com domain.

c. find out the email servers and their IP addresses of yahoo.com domain.

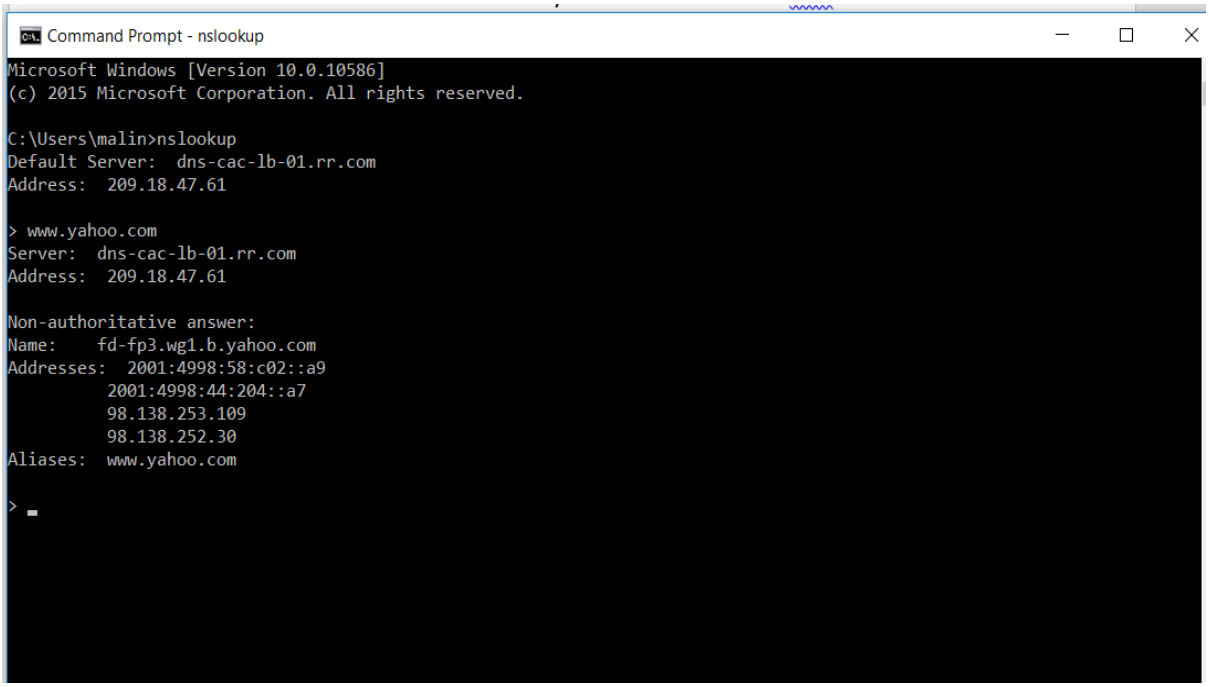
d. Try two other options (same server, different command parameters).

Record the commands and their output.

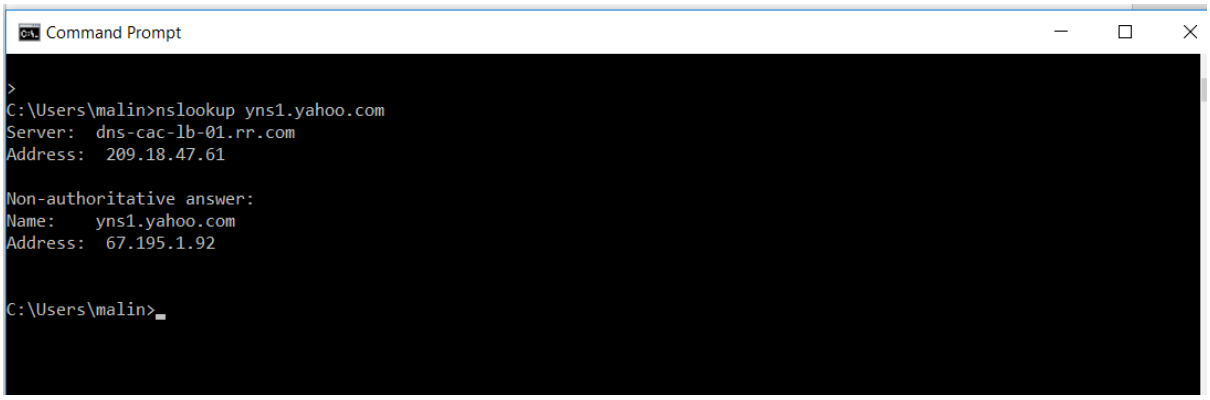
Solution:

nslookup is a network program which is used to obtain information about Internet servers. As the name suggests it gives name server information for each domain. It will also do reverse name lookup and find the host name for an IP address we specify.

a) IP address of yahoo.com

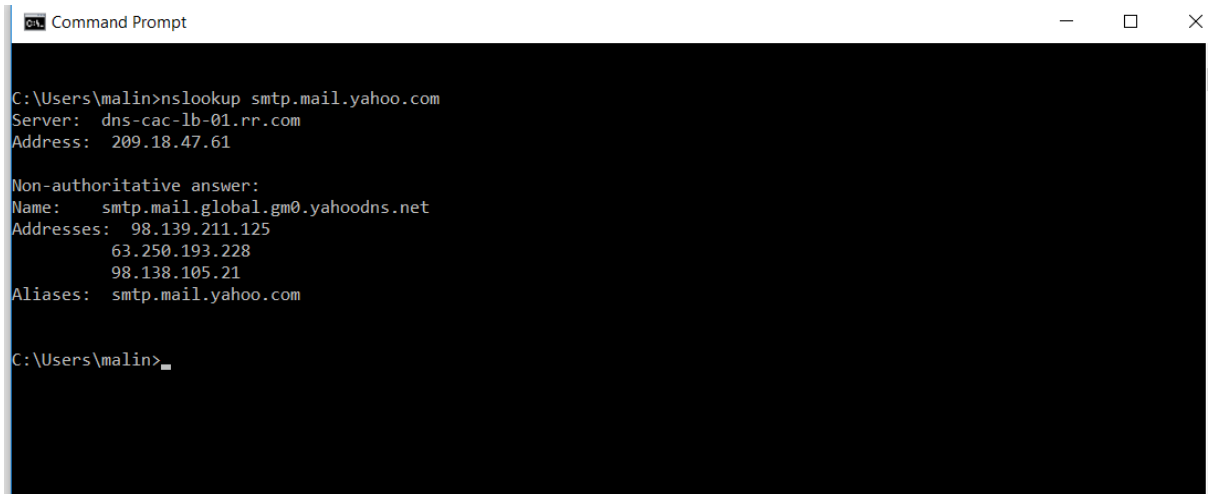


b) Name server of yahoo



c) Incoming email server

d) Outgoing email server



6. Explore IETF web page (www.ietf.org) and find out how many RFCs are there currently? Then, list at least 5 working groups. Among those working groups, choose one of them and summarize its activities in one page, i.e., objective of the charter, documents/issues published or discussed in the working group.

Solution: IETF stands for Internet Engineering Task Force. The goal of IETF is to provide high quality internet. The IETF's standards development work is organised into several areas which are sub divided into 1 or more Area Directors which together comprise the IESG (Internet Engineering Steering Group). The IESG is responsible for the internet standard process and also for technical management of IETF activities. Each area is further subdivided into several working groups(WG). Each WG again has one or more chairs and a written charter that defines what the work is and before when it should be done. The main purpose of the working group is to address a specific problem or produce guidelines.

There are total 7748 RFCs in total at present.

The IETF divides its work into a number of areas, each comprised of working groups that relate to that area's focus. Some of them are:

1) Transport Area (tsv)
2) Internet Area (int)
3) General Area (gen)
4) Operations and Management Area (ops)

5) Security Area (sec)
6) Routing Area (rtg)
7) Applications and Real-Time Area (art)

As already discussed each Area has Working Groups(WGs)

WGs are mainly classified into Active working groups and Concluded Working groups.

Some of the Working groups under TSV are

1. tcpinc : TCP Increased Security
2. tcpm : TCP Maintenance and Minor Extensions
3. tram : TURN Revised and Modernized
4. tsvwg : Transport Area Working Group
5. ippm : IP Performance Metrics
6. mptcp : Multipath TCP
7. nfsv4 : Network File System Version 4
8. rmcat : RTP Media Congestion Avoidance Techniques
9. taps : Transport Services

Multipath TCP:

The Multipath TCP (MPTCP) working group develops mechanisms that add the capability of simultaneously using multiple paths to a regular TCP session.

Key goals for MPTCP are:

- to be deployable and usable without significant changes to existing Internet infrastructure.
- to be usable by unmodified applications.
- to be stable and congestion-safe over the wide range of existing Internet paths, including NAT interactions.

MPTCP assumes that both peers are modified and that one or both peers have multiple addresses, which often results in different network paths that are at least partially divergent.

In its initial charter the WG produced experimental or informational documents that defined:

a. An architectural framework for congestion-dependent multipath transport protocols. It describes the motivations and the general approach that should be followed to enable congestion-dependent multipath transport.

b. A security threat analysis for multipath TCP.

c. A coupled multipath-aware congestion control algorithm. This algorithm is the multipath equivalent of SACK/NewReno congestion control.

d. Extensions to current TCP to support multi-addressed multipath TCP. This covers all on-the-wire changes required to create a two-ended MPTCP solution using multiple IP addresses at one or both ends. It includes a basic security solution.

e. Application Interface Considerations. It summarises the impact that MPTCP may have on applications, such as changes in performance. Also, it describes an optional, basic application interface for MPTCP-aware applications that provides access to multipath address information and a level of control equivalent to regular TCP.

The primary goal of the working group is to create a bis version of the protocol document on the Standards track.

Documents:

Multipath TCP (MPTCP) Application Interface Considerations:

- This document summarizes the impact that MPTCP may have on applications, such as changes in performance.
- Furthermore, it discusses compatibility issues of MPTCP in combination with non-MPTCP-aware applications.
- Finally, the document describes a basic application interface that is a simple extension of TCP's interface for MPTCP-aware applications.

Malineni Anusha, Student ID: 1623382

Architectural Guidelines for Multipath TCP Development:

- This document outlines architectural guidelines for the development of a Multipath Transport Protocol, with references to how these architectural components come together in the development of a Multipath TCP (MPTCP).

- This document lists certain high-level design decisions that provide foundations for the design of the MPTCP protocol, based upon these architectural requirements.