

Network Management and Administration

Code:3360703

UNIT – 5

Troubleshooting of Networking

Prepared By:

Chirag Patel

Lecturer in Computer Engineering,

K D Polytechnic, Patan

5.1 Understanding the Problem

5.1.1 Troubleshooting

- Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network.
- It is a systematic process that aims to resolve problems and restore normal network operations within the network.
- As a troubleshooter, you need to learn to quickly and confidently eliminate as many alternative causes as possible. This will allow you to focus on the things that might be the cause of the problem.
- The process of troubleshooting a computer network problem can be divided into five steps.

5.1 Understanding the Problem

5.1.1 Troubleshooting

- **Step 1: Defining the Problem**

- This task is the most critical and also time consuming.
- Troubleshooter might know how the network functions and be able to find the technical cause of the failure.
- To define the problem:
- Listen to the client or network user is your best source of information.
- Ask questions to the affected client or network user.
- Properly analyze the problem.
- Identify the general symptoms.
- Check for documented repairs and ask coworkers about attempted repairs.

5.1 Understanding the Problem

5.1.1 Troubleshooting

- **Step 2: Isolating the Cause**

- The next step is to isolate the problem. Begin by eliminating the most understandable problems and work toward the more complex and unclear.
- For example, be able to eliminate hardware as a problem, so that troubleshooter can focus on software problems.
- At every opportunity, try to narrow the number of potential problems base of knowledge so this is helpful for to create an efficient plan of action.

5.1 Understanding the Problem

5.1.1 Troubleshooting

- **Step 3: Planning the Repair**
 - Create an action plan based on the remaining potential problems.
 - Start by trying out the most obvious or easiest solution to eliminate and continue toward the more difficult and complex.
 - If the first plan is not successful (always a possibility), create a new plan based on what's discovered with the previous plan.
 - Once repairing is done, it is important to record each step of the process; document every action and its results.

5.1 Understanding the Problem

5.1.1 Troubleshooting

- **Step 4: Confirming the Results**
 - Repairing is not complete without confirmation, so ask the user to test the solution and confirm the results.
 - Make sure that the diagnosis (solution of problem) will not generate new problems and negative impact on any other aspect of the network.
- **Step 5: Documenting the Outcome**
 - Finally, document the problem and the repair.
 - Keeping a copy of the repair procedure in the technical library so it can be useful when the problem (or one like it) occurs again.

5.1.2 Segmenting the Problem

- If the initial review of network statistics and symptoms does not represent an obvious problem, dividing the network into smaller parts to isolate the cause is the next step in the troubleshooting process.
- The first question to ask is whether the problem occur from the hardware, or the software.
- If the problem appears to be hardware-based, start by looking at only one segment of the network, then looking at only one type of hardware.
- Check the hardware and network components, including:
 - NICs.
 - Cabling and connectors.
 - Clients/workstations.
 - Connectivity components such as repeaters, bridges, routers, brouters, and gateways.
 - Hubs.
 - Protocols.
 - Servers.
 - Users.
- Often, isolating or removing a portion of the network will help to get the rest of the network up and operational again.
- If removing a portion solved the problem for the rest of the network, the search for the problem can be focused on the part that was removed.

5.1.3 Isolating the Problem

- After you have gathered the information, rank the list of possible causes in order, beginning with the most likely and moving to the least likely cause of the problem.
- Then select the most likely candidate from the list of possible causes, test it and see if that is the problem.
- Start from the most obvious and work with the most difficult.
- For example, if you suspect that a faulty network interface card (NIC) in one of the computers is the cause of the trouble, replace it with a NIC that is known to be in good working order.

5.1.4 Setting Priorities

- A fundamental element in network problem solving is setting priorities
- Everyone wants his or her computer fixed first, so setting priorities is not an easy job.
- While the simplest approach is to prioritize on a "first come, first served" basis, this does not always work, as some failures are more critical to resolve than others.
- The initial step is to assess the problem's impact on the ability to maintain operations.
- To solve your problems, highest priority to lowest, might look something like this:
 - Total network failure (affect everyone)
 - Priority network failure (affect small groups of users)
 - Small network failure (affect a small, single group of users)
 - Total workstation failure (single user can't work at all)
 - Partial workstation failure (single user can't do most tasks)
 - Minor issue (single user has problems that crop up now and again)

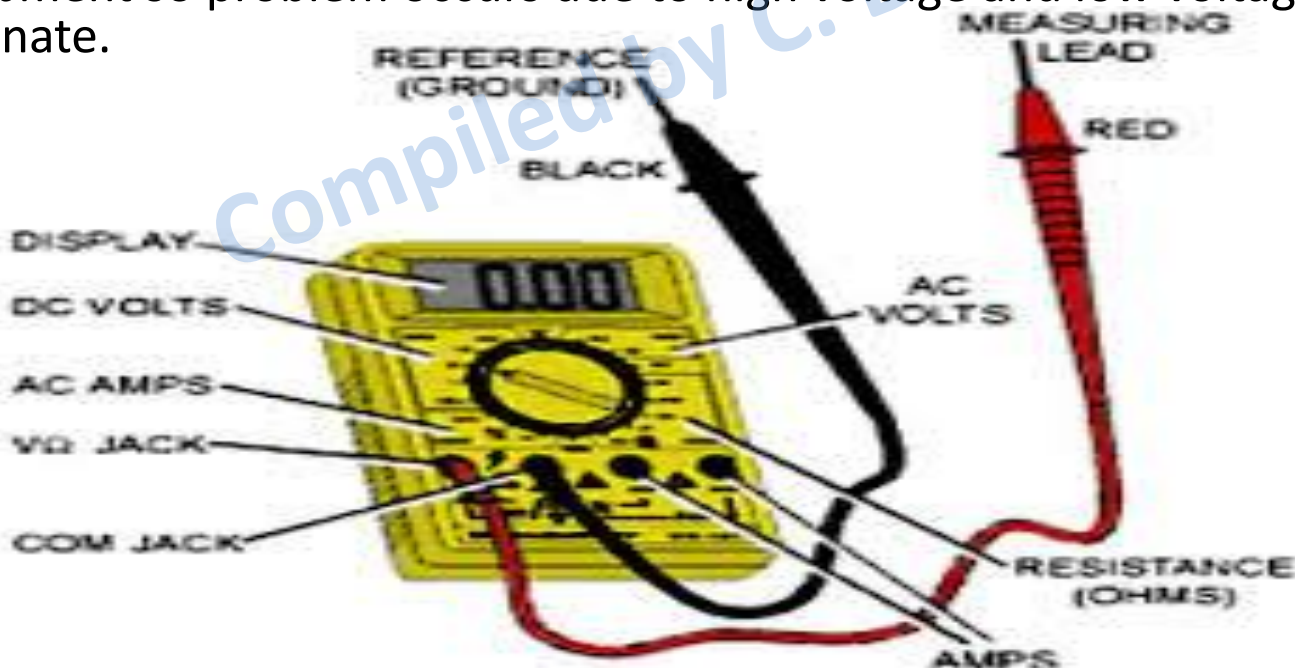
5.2 Troubleshooting Tools

5.2.1 Hardware Tools

- Troubleshooting network problems are often accomplished with the help of hardware and software.
- To troubleshoot effectively, you need to know how these tools can be used to solve network problems.
- Hardware tools were once very expensive and difficult devices to use. They are now less expensive and easier to operate.
- They are helpful to identify performance trends and problems. This section describes the most common of these tools.

1. Digital Voltmeters

- The digital voltmeter (volt-ohm meter) is the primary all-purpose electronic measuring tool.
- Voltmeters can determine if:
 - The cable is continuous (has no breaks).
 - The cable can carry network traffic.
 - Two parts of the same cable are exposed and touching (thereby causing shorts).
 - An exposed part of the cable is touching another conductor, such as a metal surface.
- The network administrator has to confirm source voltage for the network equipment so problem occurs due to high voltage and low voltage eliminate.



2. Time-Domain Reflectometers (TDRs)

- A time-domain Reflectometer (TDR) is an electronic instrument that uses time-domain Reflectometry to characterize and locate faults in metallic cables (for example, twisted pair wire or coaxial cable)
- Time-domain Reflectometer sends sonar like electrical signal into a cable and can determine the location of a break in the cable. The pulse is reflected back to the TDR and the TDR can tell where the break is by timing the time it takes for the pulse to return.
- Network performance suffers when the cable is not intact. If the TDR locates a problem, the problem is analyzed and the results are displayed.
- TDR can determine:
 - Speed and condition of cable.
 - Cable impedance characteristics.
 - Estimated cable length.
 - Splice and connector location.
 - Damage in cable.
 - Used heavily during the installation of a new network, TDRs are also invaluable in troubleshooting and maintaining existing networks.



3. Advanced Cable Testers

- Advanced cable testers work in the physical layer, data-link layer, network layer, and even the transport layer of the OSI reference model.
- Advanced cable testers doesn't only measure where a break is located in a cable, but can also gather other information, including a cable's impedance, resistance, and attenuation characteristics?
- Also measure message frame counts, collisions, congestion errors, and beaconing information or broadcast storms.



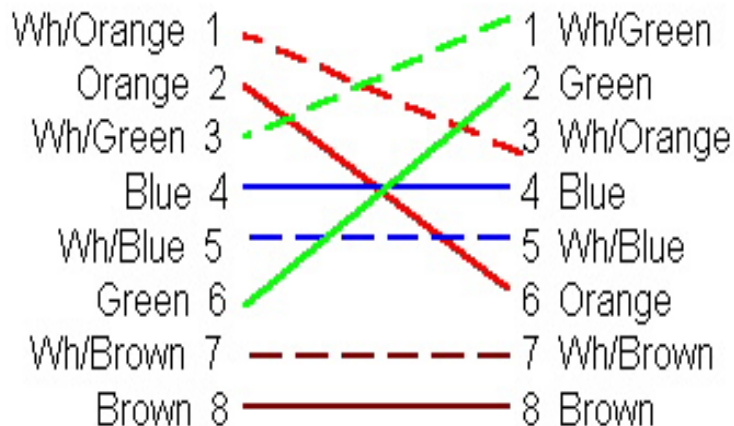
4. Oscilloscopes

- Oscilloscopes are advanced pieces of electronic equipment that measure signal voltage per unit of time and display the result on a monitor.
- When used with TDRs, an oscilloscope can display:
 - Shorts.
 - Sharp bends or crimps in the cable.
 - Opens (breaks in the cable).
 - Attenuation problem (loss of signal power).



5. Crossover Cables

- Crossover cables are used to connect two computers directly with a single patch cable. The send and receive wires are reversed at one end, the send wire from one computer is connected to the receive port on the other computer.
- Crossover cables are useful in troubleshooting network connection problems.
- By using a crossover cable easily check the problem lies with network cable, and not with the workstation's software or hardware.
- Two computers can be directly connected, bypassing the network and making it possible to isolate and test the communication capabilities of one computer, rather than the whole network.



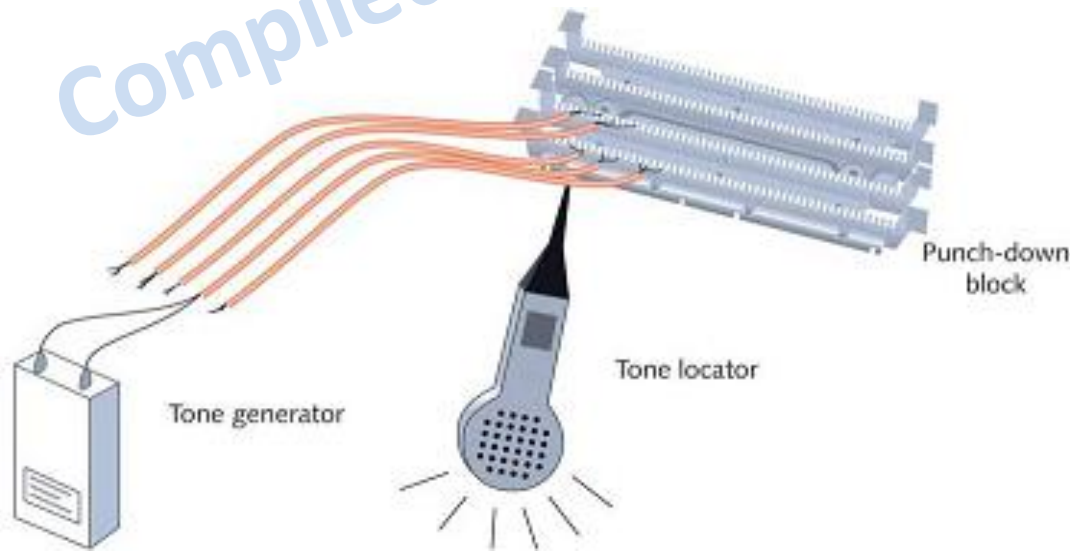
6. Hardware Loopback

- A hardware loopback device is a serial port connector that enables you to test the communication capabilities of a computer's serial port without having to connect to another computer or peripheral device.
- Instead, using the loopback, data is transmitted to a line, and then returned as received data.
- If the transmitted data do not return, the hardware loopback detects a hardware malfunction.



7. Tone Generator and Tone Locator

- A tone generator is used to apply an alternating or a continuous tone signal to a cable or a conductor.
- The tone generator is attached to one end of the cable.
- A matching tone locator is used to detect the correct cable at the other end.
- These tools are also able to test for wiring continuity and line polarity.
- They can be used to trace twisted-pair wiring, single conductors, and coaxial cables, among others.
- This pair of equipment is sometimes referred to as "fox and hound."



5.2.2 Software Tools

- Software tools are needed to monitor trends and identify network performance problems.
- These tools have fallen into two main categories:
 - Performance monitoring Tools
 - Protocol Analyzers

Performance monitoring Tools

- Performance monitoring Tools are software tools that track all or a selected part of network traffic.
- They examine data packets and gather information about packet types, errors, and packet traffic to and from each computer.
- They are very useful for establishing part of the network baseline.
- After the baseline has been established, you will be able to troubleshoot traffic problems and monitor network usage to determine when it is time to upgrade.
- Netware comes with the MONITOR.NLM utility and windows 2000 comes with performance monitor.

Protocol Analyzers

- Protocol analyzers, also called "network analyzers," perform real-time network traffic analysis using packet capture, decoding, and transmission data.
- Protocol analyzers have built-in TDR to help determine the network's status
- The protocol analyzer can provide insights and detect network problems including:
 - Faulty network components.
 - Configuration or connection errors.
 - LAN bottlenecks.
 - Traffic fluctuations.
 - Protocol problems.
 - Applications that might conflict.
 - Unusual server traffic.
 - Identify the most active computers.
 - Identify computers that are sending error-filled packets.
 - View and filter certain types of packets. This is helpful for routing traffic.
- Two common examples of Protocol analyzers are sniffer, a network general product and Novell's LANalyzer.

Network General Sniffer,

Novell's LANalyzer

- **Network General Sniffer**
- Sniffer, which is part of a family of analyzers from Network General.
- It can decode and interpret frames from 14 protocols, including AppleTalk, Windows NT, NetWare, SNA, TCP/IP, VINES, and X.25.
- Sniffer measures network traffic in kilobytes per second, frames per second, or as a percentage of available bandwidth.
- It will gather LAN traffic statistics, detect faults such as beaconing, and present this information in a profile of the LAN.
- A Sniffer can also identify bottlenecks by capturing frames between computers and displaying the results.
- **Novell's LANalyzer**
- The LANalyzer software performs much the same function as Sniffer but is available only on a NetWare LAN.

5.2.3 Monitoring and Troubleshooting Tools

- Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via message or other alarms) in case of outages.
- Small peer-to-peer networks consisting of 10 or fewer computers can be monitored visually by one support person.
- However, a large network or WAN might need a dedicated staff and sophisticated equipment to perform proper network monitoring.
- The administrator will need to manage and keep track of every aspect of the network's performance.

Performance Monitors

- Most current network operating systems include a monitoring utility that will help a network administrator keep track of a network's server performance.
- These monitors can view operations in both real time and recorded time for:
 - Processors.
 - Hard disks.
 - Memory.
 - Network utilization.
 - The network as a whole.
- These monitors can:
 - Record the performance data.
 - Send an alert to the network manager.
 - Start another program that can adjust the system back into acceptable ranges.
- When monitoring a network, it is important to establish a baseline.
- The baseline information can help you identify and monitor dramatic and subtle changes in your network's performance.

Network Monitors

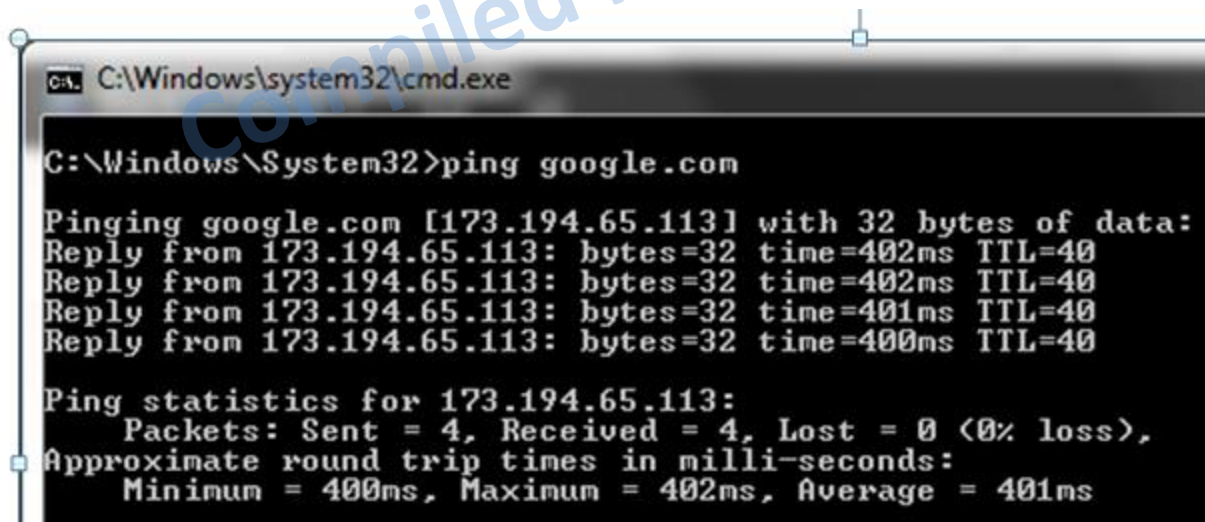
- Some servers include network monitoring software.
- Windows NT Server, for example, includes a diagnostic tool called Network Monitor.
- This tool gives the administrator the ability to capture and analyze network data streams to and from the server.
- This data is used to troubleshoot potential network problems.
- The packets of data in the data stream consist of the following information:
 - The source address of the computer that sent the message.
 - The destination address of the computer that received the frame.
 - Headers from each protocol used to send the frame.
 - The data or a portion of the information being sent.

Simple Network Management Protocol (SNMP)

- The network management software follows standards created by network equipment vendors.
- One of these standards is the simple network management protocol (SNMP).
- In an SNMP environment, programs called "agents" are loaded onto each managed device.
- The agents monitor network traffic in order to gather statistical data. This data is stored in a management information base (MIB).
- SNMP components (device) include:
 - Hubs.
 - Servers.
 - NICs.
 - Routers and bridges.
 - Other specialized network equipment.
- To collect the information in a usable form, a management program console regularly polls these agents and downloads the information from their MIBs.
- After the raw information has been collected, the management program can perform two more tasks:
 - Present the information in the form of graphs, maps, and charts
 - Send the information to designated database programs to be analyzed
 - If any of the data falls above or below thresholds set by the manager, the management program can notify the administrator by means of alerts on the computer.

PING Command

- Ping (packet InterNet Groper) command can be used to verify connectivity between computers in a network.
- The ping command tells the minimum, maximum and average time taken by ping packet to reach the specified destination and how long it will take to receive a reply.
- Ping command creates an echo request to a host on a TCP/IP based network.
- It communicates by using ICMP (Internet Control Messaging Protocol) protocol.
- When using ping command, systems send ICMP packet and waits for a response from a remote host.



```
C:\Windows\system32\cmd.exe

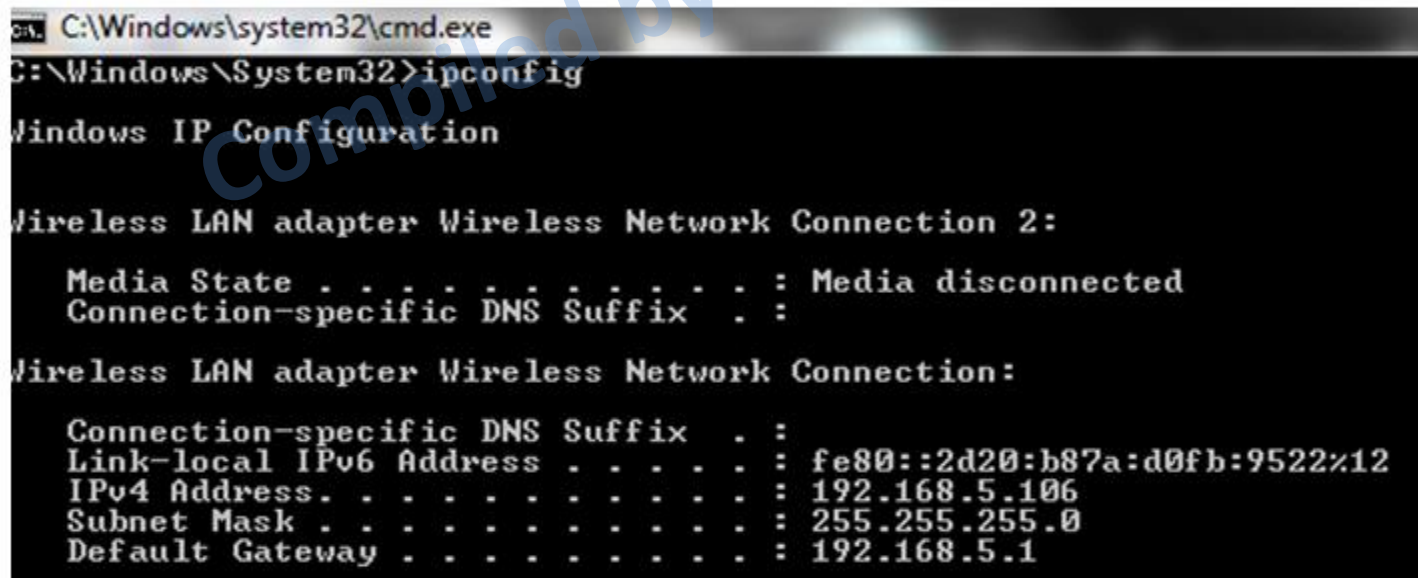
C:\Windows\System32>ping google.com

Pinging google.com [173.194.65.113] with 32 bytes of data:
Reply from 173.194.65.113: bytes=32 time=402ms TTL=40
Reply from 173.194.65.113: bytes=32 time=402ms TTL=40
Reply from 173.194.65.113: bytes=32 time=401ms TTL=40
Reply from 173.194.65.113: bytes=32 time=400ms TTL=40

Ping statistics for 173.194.65.113:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 400ms, Maximum = 402ms, Average = 401ms
```

IPCONFIG Command

- IPCONFIG is a MS-DOS command which can be used to display the network settings currently assigned and given by a network administrator.
- Use ipconfig command to view host computer configuration information including IP address, subnet mask and default gateway. You can use the ipconfig command with all options to view detailed configuration information for all interfaces.



```
C:\Windows\system32\cmd.exe
C:\Windows\System32>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

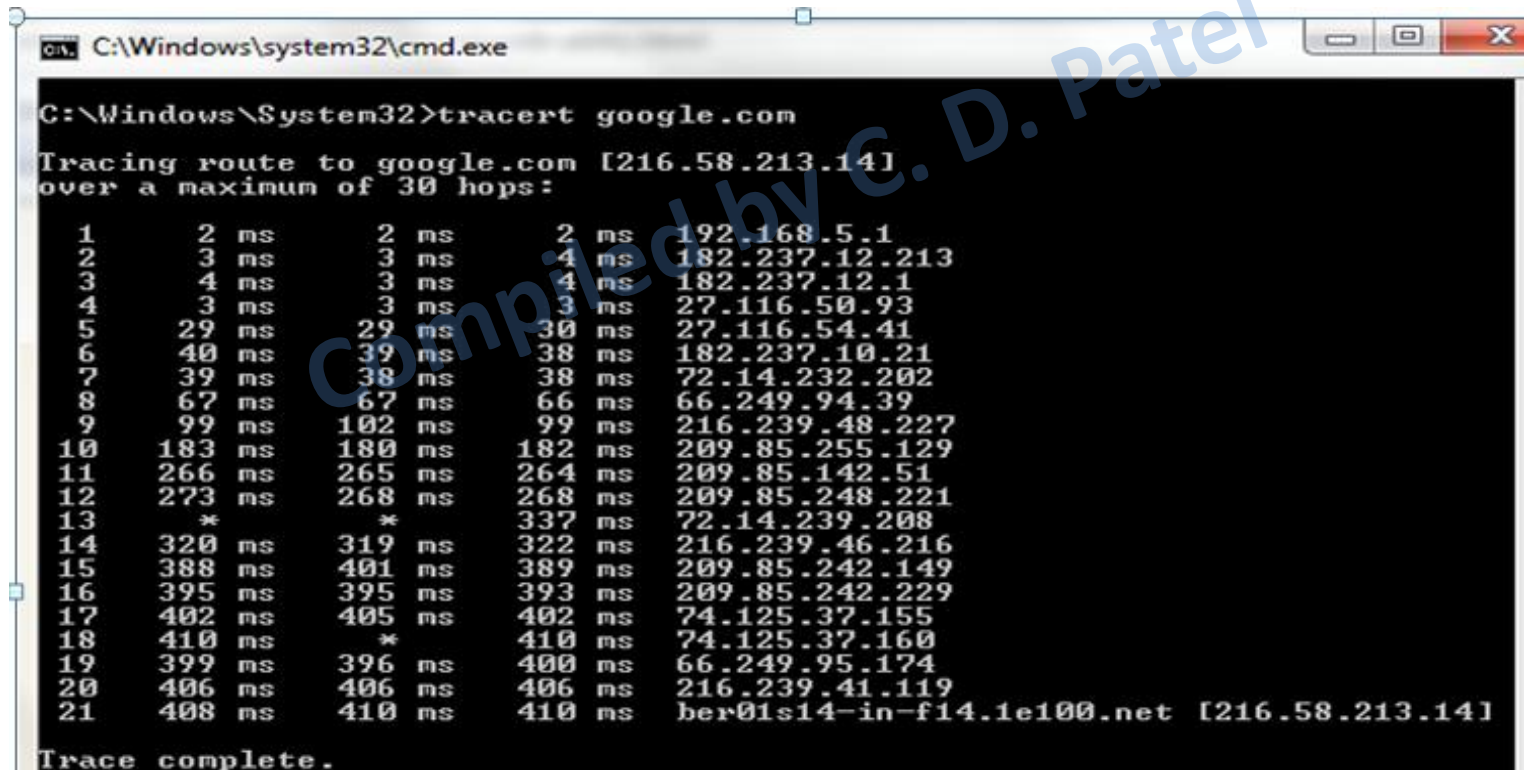
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2d20:b87a:d0fb:9522%12
    IPv4 Address. . . . . : 192.168.5.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.5.1
```

TRACERT Command

- TRACERT is short for trace route which displays the path that data takes to reach the destination.
- The tracert command is used to see the network packet sent and received and the number of hops required for that packet to reach its destination.
- The tracert command displays a series of routers used for delivering packets from computer to the destination and time taken on each hop.
- You can see that there will be a maximum of 30 hops displayed.



```
C:\Windows\system32\cmd.exe

C:\Windows\System32>tracert google.com

Tracing route to google.com [216.58.213.14]
over a maximum of 30 hops:

  1      2 ms      2 ms      2 ms      192.168.5.1
  2      3 ms      3 ms      4 ms      182.237.12.213
  3      4 ms      3 ms      4 ms      182.237.12.1
  4      3 ms      3 ms      3 ms      27.116.50.93
  5     29 ms     29 ms     30 ms      27.116.54.41
  6     40 ms     39 ms     38 ms      182.237.10.21
  7     39 ms     38 ms     38 ms      72.14.232.202
  8     67 ms     67 ms     66 ms      66.249.94.39
  9     99 ms    102 ms     99 ms      216.239.48.227
 10    183 ms    180 ms    182 ms      209.85.255.129
 11    266 ms    265 ms    264 ms      209.85.142.51
 12    273 ms    268 ms    268 ms      209.85.248.221
 13      *        *      337 ms      72.14.239.208
 14   320 ms    319 ms    322 ms      216.239.46.216
 15   388 ms    401 ms    389 ms      209.85.242.149
 16   395 ms    395 ms    393 ms      209.85.242.229
 17   402 ms    405 ms    402 ms      74.125.37.155
 18   410 ms      *      410 ms      74.125.37.160
 19   399 ms    396 ms    400 ms      66.249.95.174
 20   406 ms    406 ms    406 ms      216.239.41.119
 21   408 ms    410 ms    410 ms      ber01s14-in-f14.1e100.net [216.58.213.14]

Trace complete.
```

NETSTAT Command

- Netstat (network statistics) is a command-line tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface and network protocol statistics.
- The netstat command is used to view the active TCP and UDP port activity for either servers or workstations.

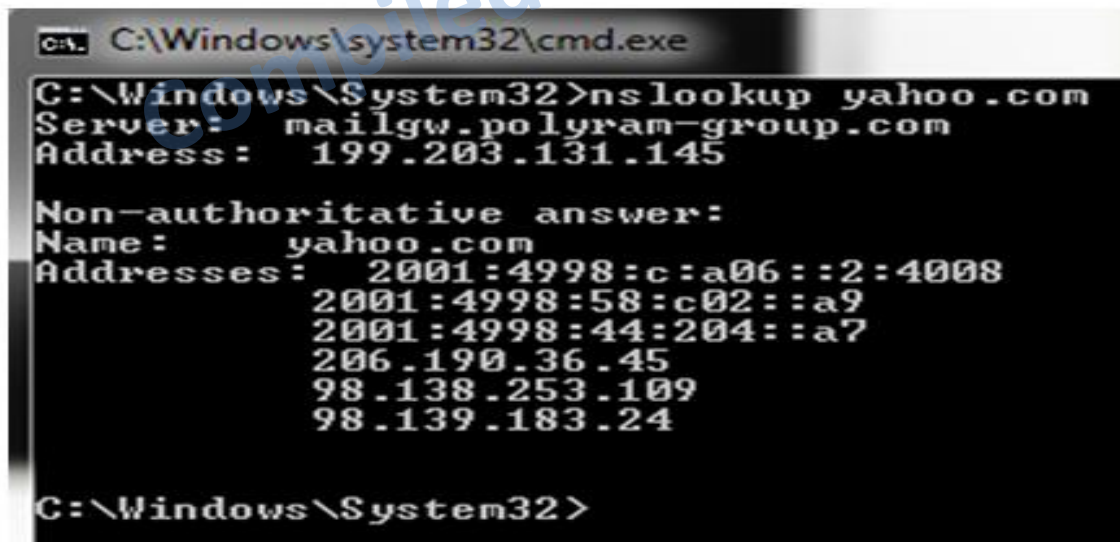
```
C:\Windows\System32>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.5.106:49944	stackoverflow:https	ESTABLISHED
TCP	192.168.5.106:50056	a95-101-72-192:http	ESTABLISHED
TCP	192.168.5.106:50057	a95-101-72-192:http	ESTABLISHED
TCP	192.168.5.106:50332	yv-in-f91:https	ESTABLISHED
TCP	192.168.5.106:50333	yv-in-f91:https	TIME_WAIT
TCP	192.168.5.106:50334	ea-in-f100:https	ESTABLISHED
TCP	192.168.5.106:50338	wb-in-f95:http	ESTABLISHED
TCP	192.168.5.106:50339	ea-in-f191:https	ESTABLISHED
TCP	192.168.5.106:50340	fr:https	ESTABLISHED
TCP	192.168.5.106:50341	fr:https	ESTABLISHED
TCP	192.168.5.106:50343	82-166-201-176:http	ESTABLISHED

NSLOOKUP (Name Server Lookup) Command

- NSLOOKUP is enables to look up an IP address of a domain to host on a network.
- Using NSLOOKUP:
 - Identify domain's name server.
 - IP address of specific host.
 - Look up the fully-qualified domain name for an IP address.
 - Look up mail server for a specific domain or host .
 - If you enter a domain name then you will get IP address to which it corresponds and if you enter an IP number then you get the domain name to which it corresponds.



```
C:\Windows\system32\cmd.exe
C:\Windows\System32>nslookup yahoo.com
Server:  mailgw.polyram-group.com
Address:  199.203.131.145

Non-authoritative answer:
Name:     yahoo.com
Addresses: 2001:4998:c:a06::2:4008
           2001:4998:58:c02::a9
           2001:4998:44:204::a7
           206.190.36.45
           98.138.253.109
           98.139.183.24

C:\Windows\System32>
```


Route

- Route is a command used to view and manipulate the TCP/IP routing table in both UNIX-like and Microsoft Windows operating systems.
- This command displays the current status of the routing table on the host.
- Example:-
c:\windows\System32> route print

```
C:\Windows\system32\cmd.exe
C:\Windows\System32>route print

=====
Interface List
13...0c 60 76 35 fb 00 .....Microsoft Virtual WiFi Miniport Adapter
12...0c 60 76 35 fb 00 .....Dell Wireless 1397 WLAN Mini-Card
11...00 25 64 55 c9 53 .....Marvell Yukon 88E8040 PCI-E Fast Ethernet Controll
er
15...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
16...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
1.....Software Loopback Interface 1
19...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
20...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #4
14...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
18...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #6
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.5.1      192.168.5.106    25
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
192.168.5.0                255.255.255.0    On-link          192.168.5.106    281
192.168.5.106              255.255.255.255  On-link          192.168.5.106    281
192.168.5.255              255.255.255.255  On-link          192.168.5.106    281
192.168.6.0                255.255.255.0    On-link          192.168.6.1      276
192.168.6.1                255.255.255.255  On-link          192.168.6.1      276
192.168.6.255              255.255.255.255  On-link          192.168.6.1      276
192.168.11.0               255.255.255.0    On-link          192.168.11.1     276
192.168.11.1               255.255.255.255  On-link          192.168.11.1     276
192.168.11.255             255.255.255.255  On-link          192.168.11.1     276
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.6.1      276
224.0.0.0                  240.0.0.0        On-link          192.168.11.1     276
224.0.0.0                  240.0.0.0        On-link          192.168.5.106    281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.6.1      276
255.255.255.255            255.255.255.255  On-link          192.168.11.1     276
255.255.255.255            255.255.255.255  On-link          192.168.5.106    281
=====

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128 On-link
15 276 fe80::/64 On-link
16 276 fe80::/64 On-link
12 281 fe80::/64 On-link
12 281 fe80::2d20:b87a:d0fb:9522/128 On-link
16 276 fe80::4cc0:481b:ff1b:f94b/128 On-link
```

5.3 Internal Security

- Internal security is the process of securing your network from internal threats, which are generally much more common than external threats.
- Examples of internal threats include the following:
- Internal users inappropriately accessing information such as payroll records, accounting records, or business development information.
- Internal users accessing other users' files to which they should not have access.
- Internal users impersonating other users and causing mischief, such as sending e-mail under another person's name.
- Internal users accessing systems to carry out criminal activities, such as embezzling funds.
- Internal users compromising the security of the network, such as by accidentally (or deliberately) introducing viruses to the network.
- Internal users "sniffing" packets on the network to discover user accounts and passwords.

5.3.1 Account Security

- Account security refers to the process of managing the user accounts enabled on the network.
- Following are a number of general steps you should take to manage general account security:
 - You should remove guest account and also avoid creating accounts that are obviously for testing purposes, such as Test, Generic, and so forth.
 - Most network operating systems start up with a default name for the administrative account. You should immediately rename this account to avoid direct attacks against it.
 - You should know the steps required to remove access to network resources quickly from any user account and be sure that all network resources might be contain their own security systems.
 - You have to work closely with human resources (HR) department. So you have an idea about any terminations immediately so you can take proper steps.

5.3.1 Account Security

- I&A is done by assigning user IDs and names to each user on the system.
- Biometrics uses unique human characteristics such as fingerprints, hand geometry, retina scans, facial geometry, and voiceprints for authentication.
- Passwords are the most common type of authentication mechanism used.
- Passwords should be at least eight characters in length and contain a mixture of uppercase and lowercase letters, numbers, and special characters.
- You to establish limits on when and where a user can log in to the network.
- You can establish times of day that a user is allowed to log in, and you can also restrict a user account to particular network computers.

5.3.2 File and Directory Permissions

- Another type of internal security that you need to maintain for information on your network involves the users' access to files and directories.
- Network operating systems allow considerable flexibility in setting permissions on files and directories.
- Examples of generic directory roles include the following:
 - Create only This type of role enables users to add a new file to a directory, but restricts them from seeing, editing, or deleting existing files, including any they've created.
 - Read only This role enables users to see the files in a directory and even to pull up the files for viewing on their computer.
 - Change this role lets users do whatever they like with the files in a directory, except give other users access to the directory.
 - Full control usually reserved for the "owner" of a directory, this role enables the owners to do whatever they like with the files in a directory and to grant other users access to the directory.

5.3.3 Practices and User Education

- To establish good practices, you need to document security-related procedures, and then set up some sort of process to make sure that the employees follow the procedures regularly.
- You can easily enforce some procedures through settings on the network operating system, but you must handle others through education.
- Set up guidelines for the users include choosing secure passwords, not giving their passwords to anyone else, not leaving their computers unattended for long periods of time while they are logged in to the network, not installing software from outside the company, and so forth.
- When new employees join the company and are oriented on using the network, make sure that you discuss security issues with them.
- Periodically audit users' security actions. If the users have full-control access to directories, examine how they've assigned permissions to other users.
- Make sure that you review the security logs of the network operating system you use. Investigate and follow up on any problems reported.

ASSIGNMENT

1. What is the role of Hardware tools. List and explain any one Hardware tool.
2. What is the role of software tools. List and explain any one software tool.
3. Explain Account Security in details.
4. List and explain different types of File and Directory permission.
5. What is the role of performance monitoring tools. List and explain any one performance monitoring tools.
6. How to troubleshoot network fault(Troubleshooting Steps).
7. Write a short note on network monitoring tools.
8. List Common Networking Problems. Explain any one Problem.
9. Explain Segmenting the Problem.
10. Explain major threats to the security of data on a network