UNIT-V

TROUBLE SHOOTING OF NETWORKING

5.1 Understanding the Problem

5.5.1

- Troubleshooting is perhaps the most difficult task that computer professionals face. Added to the need to get to the bottom of a problem afflicting the network is the pressure to do so as quickly as possible.
- Computers never seem to fail at a convenient time. Failures occur in the middle of a job or when there are deadlines, and pressures to fix the problem immediately are intense.
- Troubleshooting is more of an art from than an exact science.

Step 1 : Defining the Problem

- The first phase is the most critical, yet most often ignored. Without a complete understanding of the entire problem, you can spend a great deal of time working on the symptoms, without getting to the cause. The only tools required for this phase are a pad of paper, a pen (or pencil), and good listening skills.
- Listening to the client or network user is your best source of information.

Step 2 : Isolating the Cause

- The nest step is to isolate the problem. Being by eliminating the most obvious problems and work toward the more complex and obscure.
- Your purpose is to narrow your search down to one or two general categories.
- Be sure to observe the failure yourself. If possible, have someone demonstrate the failure to you.
- If it is operator-induced problem, it is important to observe how it is created, as well as the results.

Step 3 : Planning the Repair

- After you have lessened, your search down to a few categories, the final process of elimination begins.
- Create a planned approach to isolating the problem based on your knowledge at this point.
- Start by trying out the most obvious or easiest solution to eliminate and continue toward the more difficult and complex.
- It is important to record each step of the process; document every action and its results.

Step 4 : Confirming the Results

- No repair is complete without confirmation that the job has been successfully concluded.
- You need to make sure that the problem no longer exists.
- Ask the user to test the solution and confirm the results.
- You should also make sure that the fix did not generate new peroblems.
- Be sure to confirm not only the problem you fixed, but also that what you have done has not had a negative impact on any other aspect of the network.

Step 5 : Documenting the Outcome

- Finally, document the problem and the repair.
- Recording what you've learned will provide you with invaluable information.
- There is no substitute for experience in troubleshooting, and each new problem presents you with an opportunity to expand that experience.
- Keeping a copy of the repair procedure in your technical library can be useful when the problem (or one like it) occurs again.

5.1.2 Segmenting the Problem

- If the initial of network statistics does not expose 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 stems 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.

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 sec if that is the problem.
- Start from the most obvious and work to the most difficult.
- For example, if you suspect that a faulty network interface card (NIC) that is known to be in good working order.

5.1.4 Setting priorities

- A fundamental element in network problem is setting priorities.
- Everyone want 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.

5.2 TROUBLESHOOTING TOOLS

- If problems are not easily solve then use various tools for solve it, Troubleshooting tools are a necessity for every network administrator.
- When getting started in the networking field, it is important to collect a number of tools that can be used Troubleshoot a variety of different network conditions. While it is true that the use of specific tools can be subjective and at the discretion of the engineer,

5.2.1 Hardware Tools

- Hardware tools were once very expensive and difficult devices to use. They are now less expensive and easier to operate. They are now less expensive and easier to operate. They are helpful to identify performance trends and problems.
- The level of troubleshooting most often performed on PC hardware is exchanging field replaceable units (FRUs).
- However, a few hardware diagnostic tools can be very helpful in isolating defective hardware components. These tools include

Digital Voltmeters

- The digital voltmeter (volt-ohm meter) is the primary all-purpose electronic measuring tool.
- It is considered standard equipment for any computer or electronic technician and can reveal for more than just the amount of voltage passing through resistance.
- Voltmeter can determine in following case define as under :
  - The cable is continuous(has no breaks).
  - The cable can carry network traffic.
  - Two parts of the same cable are exposed and touching.
  - An exposed part of the same cable is touching another conductor, such as a metal surface.
- one of the network administrator's most important function is to confirm source voltage for the network equipment.

Digital Voltmeters

TIME-DOMAIN REFLECTOMETERS(TDRS)

- Time-domain reflectometers (TDRs), As shown in Figure.
- This equipment , send sonar-like piles along cables to locate breaks, shorts, or imperfections.
- Network performance suffers when the cable is not intact.
- If the TDR locates a problem is analyzed and the results are displayed. A TDR can locate a break within a few feet of the actual separation in the cable.

Time domain reflectometer

Advance Cable Taster

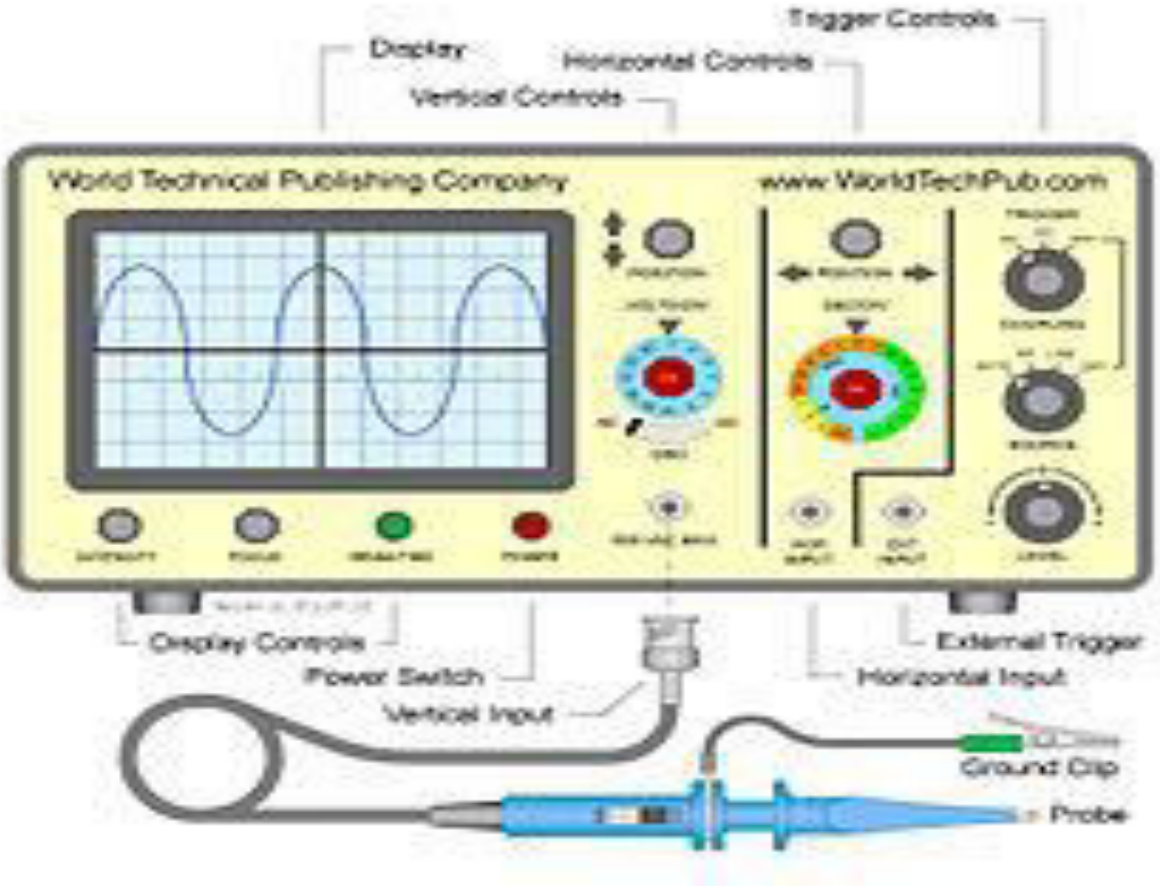
- Advanced cable testers work beyond the physical layer of the OSI reference model in the data-link layer, network layer, and even the transport layer. They can also display information about the condition of the physical cable.
- Ethernet cable can exhibit a variety of problems including : opens, shorts, reversed pairs, split pairs, mis-wires, and shield failures.
- The testing of Ethernet cable is generally conducted in two phases. The open phase test checks to verify all intended connections are good. The short test phase then determines that there are no unintended connections.

Cable tester

OSCILLOSCOPES

- Oscilloscopes are electronic instruments that measure the amount of 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 (beaks in the cable).
  - Attenuation (loss of signal power).

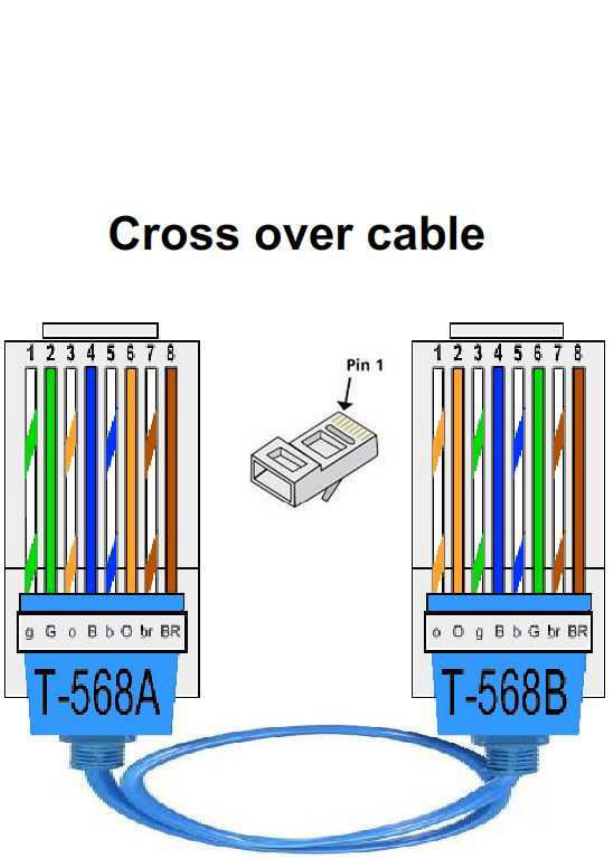
Oscilloscopes



Crossover Cables

- Crossover cables are used to connect two computers with a single patch cable. Because the send and receive wires are reversed on 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.

Crossover cable



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 devices.
- Instead, using the loopback, data is transmitted to a line, then returned as received data. If the transmitted data does not return, the hardware loopback detects a hardware malfunction.

Tone Generator and Tone Locator

- Tone generators are standard tools for wiring technicians in all fields.
- A tone generator is used to apply an alternating or continuous tone signal to a cable or a conductor.
- The tone generator is attached to one end of the cable in question. A matching tone locator is used to detect the correct cable at the other end of the run.

5.2.2 Software Tools

- Software tools are network to monitor trends and identify network performance problems. This section described some of the more useful of these tools.
- Network troubleshooting tools are a necessity for every network administrator. When getting started in the networking field, it is important to amass a number of tools that can be used to troubleshooting a variety of different network conditions.

Protocol Analyzers

- Protocol analyzers, also called ”network analyzers,” perform real-time network traffic analysis using packet capture, decoding, and transmission data.
- Network administrators who work with large networks rely heavily on the protocol analyzer. These are the tools used most often to monitor network interactivity.
- Protocol analyzers look inside the packet to identify a problem. They can also generate statistics based on network traffic to help create a picture of the network, including the:
  - Cabling.
  - Software.
  - File servers.
  - Workstations.
  - Network interface cards.
- Protocol analyzers have built-in TDRs, discussed in the previous Topic.

Network General Sniffer

- Sniffer, which is a part of a family of analyzers from Network General, can decode and interpret frames from 14 protocols including AppletTalk, Windows NT, NetWare, SNA, TCP/IP, VINES, and X.25.
- Sniffer measure 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.

5.2.3 Monitoring and Troubleshooting tools

- After a network has been installed and is operational, administrator needs to make sure it performs effectively. To do this, the administrator will need to mange and keep track of every aspect of the network's performance.
- The scope of a network management program depends on:
  - The size of the network.
  - The size and capabilities of the network support staff.
  - The organization's network operating budget.
  - The organization's exceptions of the network .

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.

Performance Monitors

- Most current network operating system include monitoring utility that will help network administrator keep track of network's server performance.
- These monitors can view operating system in both real time and recorded time for
  - Processors.
  - Hard disks.
  - Memory.
  - Network utilization.
  - The network as 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.

Network Monitors

- Network monitoring systems are used to ensure availability and overall performance computers (hosts) and network services.
- A network monitoring system is capable of detecting and reporting failures of devices or connection.
- These includes data transmission rate(throughput),error rates , downtime/uptime, usetime percentages and response time to user and automated input and requests.

Simple Network Management Protocol(SNMP)

- Network management software follows standards created by network equipment vendors.
- In an SNMP environment, illustrated in figure, 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).

PING

- To verify and test the connectivity of internet or packets
- **C:\Users\Extra>ping 160.160.18.54**
- Pinging 16.160.18.54 with 32 bytes of data
- Reply from 160.160.18.54 : bytes=32 time <1ms

TRACERT/TRACERIUTE

- Typicaly, once the ping utility has been used to determine basic connectivity.
- Figure below shows an example of the tracert utility begin used to find the path from a host inside an office to www.gobgle.com.
- C:\user\extra>tracert 160.160.18.54

IPCONFIG/IFCONFIG

- Display the current TCP/IP configuration and display the information on server.
- Windows IP configuration

NSLOOKUP

- Display the rewords of domain name server.
- C:\users\extra>nslookup
  - Default server : unknown
  - Address : 160.160.1.1

  >exit

NETSTAT

- Display the tcp/ip protocols session connection and open port connection information
- C:\users\extra>netstat
- Active connections

Route

- The last of the tools covered in this article is the route utility
- This utility is used to display the current status of the routing table on a host.

Internal Security

- Internal security and causing mischief is the process of securing your network from internal threats, which are generally much more common then external threats.
- Example of Internal threats are:
  - Internal users inappropriately accessing information, to which they should not have access, such as payroll records, accounting records or business development information.
  - Internal users accessing other user's files.
  - Internal users compromising the security of the network, such as virus attack.
  - "Sniffing" packets on the network to discover passwords or user accounts. Etc...

Account security

- Account security refers to the process of managing the users accounts enabled on the network.
- User account security requires following factors to be considered:
  1. Changes to user account and resources permissions.
  2. Failed attempts by users to log on.
  3. Changes to system files.
- Managing the user accounts on the server:
  1. Add user account
  2. Remove user account
  3. View user account
  4. Activate or Deactivate a user account

- Add a user account:
  - Create user account with name and password.
  - Grant privileges to user.
  - Permit to access shared resources.
  - Assign user to groups.
  - Steps,
    - Open windows server dashboard
    - Click users
    - Click Add a user account.
    - Follow the instruction to complete the wizard.
- Remove a user account:
  - When you select Remove a user account from server, a wizard deletes selected account.
  - Steps,
    - Open windows server dashboard
    - Click users
    - In the list of user accounts select the account which you want to remove.
    - Click Remove user account.
    - On the Do you want to keep the files? Wizard, you can choose to delete user's files. Click Next.
    - Click Delete Account.

- View a user account:
  - Open the windows server dashboard.
  - Click users.
  - Dashboard displays a current list of user accounts.
  - Steps,
    - Select user which your want to view, Click View the account properties.
    - Click a page to display properties for that account
    - To save any changes that you make to user , click Apply.
- Activate a user account:
  - Open the windows server dashboard.
  - Click users.
  - In the list view, select user accounts to activate.
  - Steps,
    - Click Activate the user account.
    - Click a Yes to confirm your action.

- Deactivate a user account:
  - Open the windows server dashboard.
  - Click users.
  - In the list view, select user accounts to deactivate.
  - Steps,
    - Click Deactivate the user account.
    - Click a Yes to confirm your action.

File and directory permissions

- The second type of internal security that you need to maintain information on your network involves the users access to files and directories.
- Manage users account because you usually have at least 20 directories and several hundred files for every user, you have on the network.
- Level of access to shared folders
  - You have 3 access settings for shared folders on server:
    1. Read/Write: Allows user account permission to create, change and delete any files in the shared folders.
    2. Read only: Allows user account permission to only read the files.
    3. No access: Do not allows access of any files in the shared folder to user.

Practices and user education

- The third important type of internal security concerns with the most insecure part of any network are the **people.**
- You need to establish good security practices and habits to help protect the network.
- It is better to keep the overall network security design as simple as possible.
- Following are some tips to make this easier:
  - Spell out for user what is expected of them in terms of security.
  - Provide a document the that describes security what they need to do to maintain.
  - When new employees join, make sure that you discuss security issues with them.
  - Periodically audit user's security actions.
  - Maintain the security logs of the network.