GOVERNMENT POLYTECHNIC AHMEDABAD
PROGRAM: DIPLOMA IN COMPUTER ENGG

NETWORK MANAGEMENT AND ADMINISTRATION (3360703)

UNIT-5
TROUBLE SHOOTING OF NETWORKING

Process of trouble shooting a computer network problem divided in to five steps:

- Step:1
  - Defining the problem
  - Without complete understanding of entire problem, you can spend great of time working on symptoms, without gettting to the cause.
  - The only tool required for this phase are a pad of paper,a pen,and good listening skill.
  - Listening to the client or network user is best source of information.

Cont…..

- you might know how the network functions before and after problems started.
- recall the events that led up to the failure.
- To identify the problem.

  list the sequence of events as they occurred before failure.

Isolating the cause

- There are several useful methods for isolating a problem:
- Retrace your steps—Try to return to a state that existed before the problem appeared. When the network is in a known state, take small steps forward, watching carefully for the recurrence of symptoms.
- Divide the problem into its smallest unit—Cut the problem in half and test each half. If only one half continues to have the problem, cut it in half again or compare it to the valid half to see how it is different. You might find the solution in the difference.
- Identify which functions are working correctly—Do not waste time investigating functions that are not broken.
- Keep careful records of changes and effects—Ask questions and document changes as you work on a system.

Cont……

- Notice how various symptoms might be related—If you are finding unexpected or unwanted results in more than one area, try to discover what those areas have in common and what variables would affect them. You probably will find the source for the problem in the common areas.
- Imagine what type of errors or failures could lead to the particular symptom—Test for the errors or failures to see if they are actually occurring.
- Do not try to solve multiple unrelated problems simultaneously—If multiple symptoms occur that do not appear to be related, select one symptom or set of symptoms and focus on it. However, do not completely ignore the other symptoms, because you might discover that they are related after all.

PLANNING THE REPAIR

- Create a planned approach to problem based on your knowledge at this point.
- Start by trying out the most obvious or easiest solution to eliminate problem and continue toward more difficult and complex.
- It is important to record each step of the process , document every action and its result.

Cont…..

- After you have created your plan , it is important to follow it throw as design.
- Jumping ahead and randomly trying thing out of the order can often lead to problems.
- If the first plan is not successful, create a new plan based on what you discovered with the previous plan.
- Be sure to refer, to reexamine and reassess any assumptions you might have made in the previous plan.
- After you have located the problems, either repair the defect or replace the defective component.
- If the problem is software based, be sure to record the before and after changes.

Confirming the result

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

Documenting the outcome

- Keeping a copy of the repair procedure in your technical library can be useful when the problems occurs again.

Segmenting(divide in the separate part) the problem

- The first question is 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.

Cont…..

- Check Hardware and network component:
  - NICs
  - Cabling and connectors
  - Client/workstations
  - Connectivity components such as repeaters, bridges, router and gateways.
  - Network switches or hubs
  - Protocols
  - Servers
  - users

Cont….

- 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.
- Most protocols use what's known as “retry logic” in which the software attempts an automatic recovery from a problem.
- Failing hardware device, such as hardware drive, will use retry logic by repeatedly interrupting the CPU for more processing time to complete their task.
- When you are accessing hardware performance problem, use the information obtained from the hardware baselines to compare against current symptoms and performance.

Isolating the problem

- Gather information of cause
- Rank the list of cause
- Start from the most likely and move to the least likely problem.
- Start from the most obvious and work to the most difficult.

Setting priorities

- Set priorities of problems.
- Not first come first serve give priority to more critical problems.
- For example:
  - Monitor getting fuzzy would have lower priority than the inability to access the payroll file server prior to check run.

Troubleshooting Tools:

- There are two types of tools for troubleshooting network

➔ Hardware Tools

-Digital voltmeter

-Time-Domain Reflectometer

-Advance Cable Tester

-Osciloscope

-Crossover Cables

-Hardware Loopback

-Tone Generator and Tone Locator

Troubleshooting Tools:

➔ Software Tools

-Protocol Analyzer

Digital Voltmeter

- Digital Voltmeter measures and displays the voltage applied at one of its analog inputs.
- The measured voltage is displayed in millivolts on the PC screen. The range of the input voltage must be 0 to + 3.3 V. Higher voltages can be measured by using resistive voltage divider circuits at the input of the voltmeter.
- The aim of Digital Voltmeter is to show how an analog input port of the Nucleo-F411RE development board can be programmed to measure analog voltages.


DW-6160
AC
100.2
W
Leakage
0.00
mA
WATT / Leakage METER RS-232
TRUE RMS
AUTO RANGE
REC
HOLD
MAX / MIN
Watt
Leakage
DCV
VA
OFF
COM
VΩ

Cable Tester

- In todays most recent networks, it is not at all enough to say that the cable is working properly or not and it is proper setup.
- In case, if you install the CAT 6 type cable, then it has to provide bandwidth of 1000Mbps for the data. The only path that it can do this if all the patch panels, connector, wall jacks, and so forth are the things which should be installed properly. By using the device, it is possible to test all the network segments to compare the result and identify the fault. This testing device is known as a certifier.
- The cable certifier is one among the type of tester which makes to certify cabling by checking it for performance and speed to check that this implementation can live up to a rating. Most tests and stress the system depend upon the error and noise testing. It is required to know whether the Gigabit cable which is running is providing necessary speed to the network. There are many different varieties of certifiers available and which is for fiber, copper and for wireless networks too. Some of the devices can combine few aspects of all 3 types of networks.

Atcom
Tools

PRO-basic
LAN Cable Tester

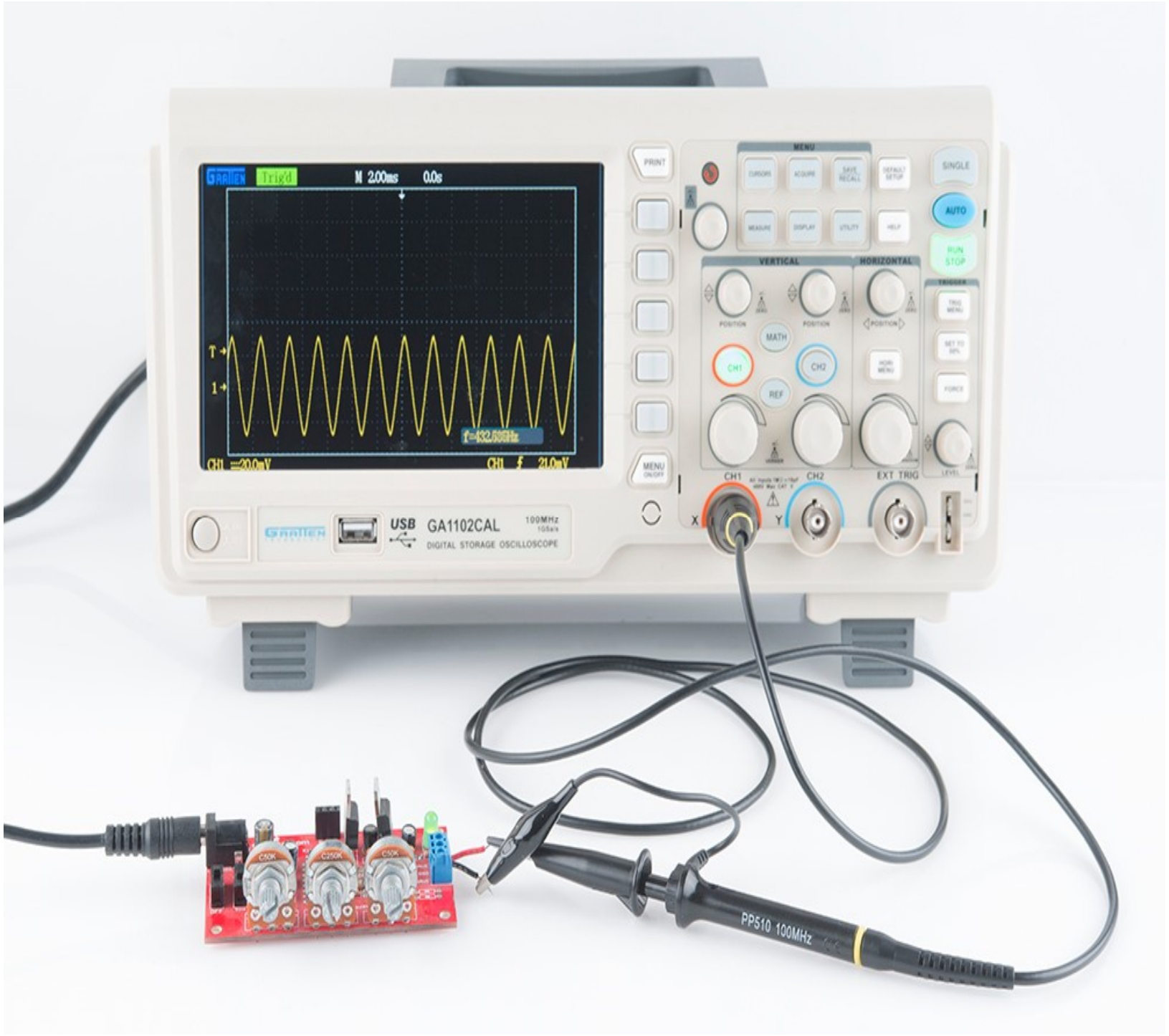
Time Domain Reflectometer

- This TDR is referred as time domain reflectometer.
- This device is used to send the signals via the particular medium to test the cable continuity.
- The high quality TDR will identify many different types of cabling issues such as damaged conductors, severed sheath, loose connectors, shorts, faulty crimps and much more. However, the network administrator need not to use this tool every day, it provides significant assistance in most of the troubleshooting process.
- This time domain reflectometer assistance ensures that the data sent through the network will not interrupt by the poor cabling which may cause issues in the data delivery.
- This tool will work at the physical layer of OSI model, allowing the signal via length of the cable searching for cable faults.

Oscilloscope

- 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 (breaks in the cable).
  - ➔Attenuation (loss of signal power).

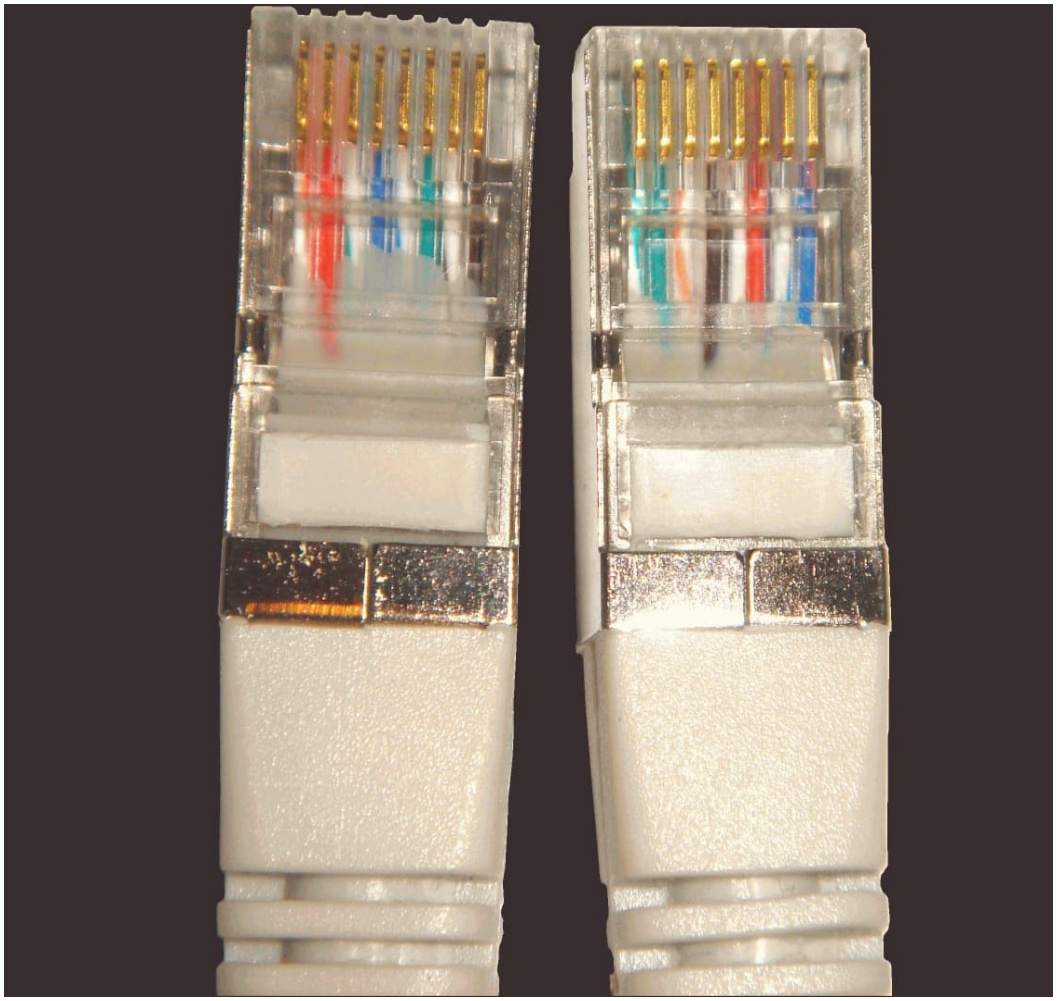

Trigd
M 2.00ms
0.0s
f=432.50Hz
CH1 20.0mV
CH1 f 21.0mV
PRINT
MENU
SINGLE
AUTO
RUN STOP
VERTICAL
HORIZONTAL
TRIGGER
POSITION
MATH
CH1
CH2
REF
EXT TRIG
LEVEL
USB
GA1102CAL
100MHz
DIGITAL STORAGE OSCILLOSCOPE
PP510 100MHz

Crossover Cables

- Crossover cables are used to connect two computers directly 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. Two computers can be directly connected, bypassing the network and test the communication capabilities of one computer, rather than the whole network

- The crossover cable is typically used to connect two hubs or switches. It can also be used to test communications between cable is used only in Ethernet UTP installation workstations directly, bypassing the hub. The cable is used only in Ethernet UTP installation

- The standard Ethernet UTP crossover cable used in both situations has its transmit and receive wire pairs crossed so that the transmit set on one side is connected to the receive set on the other.

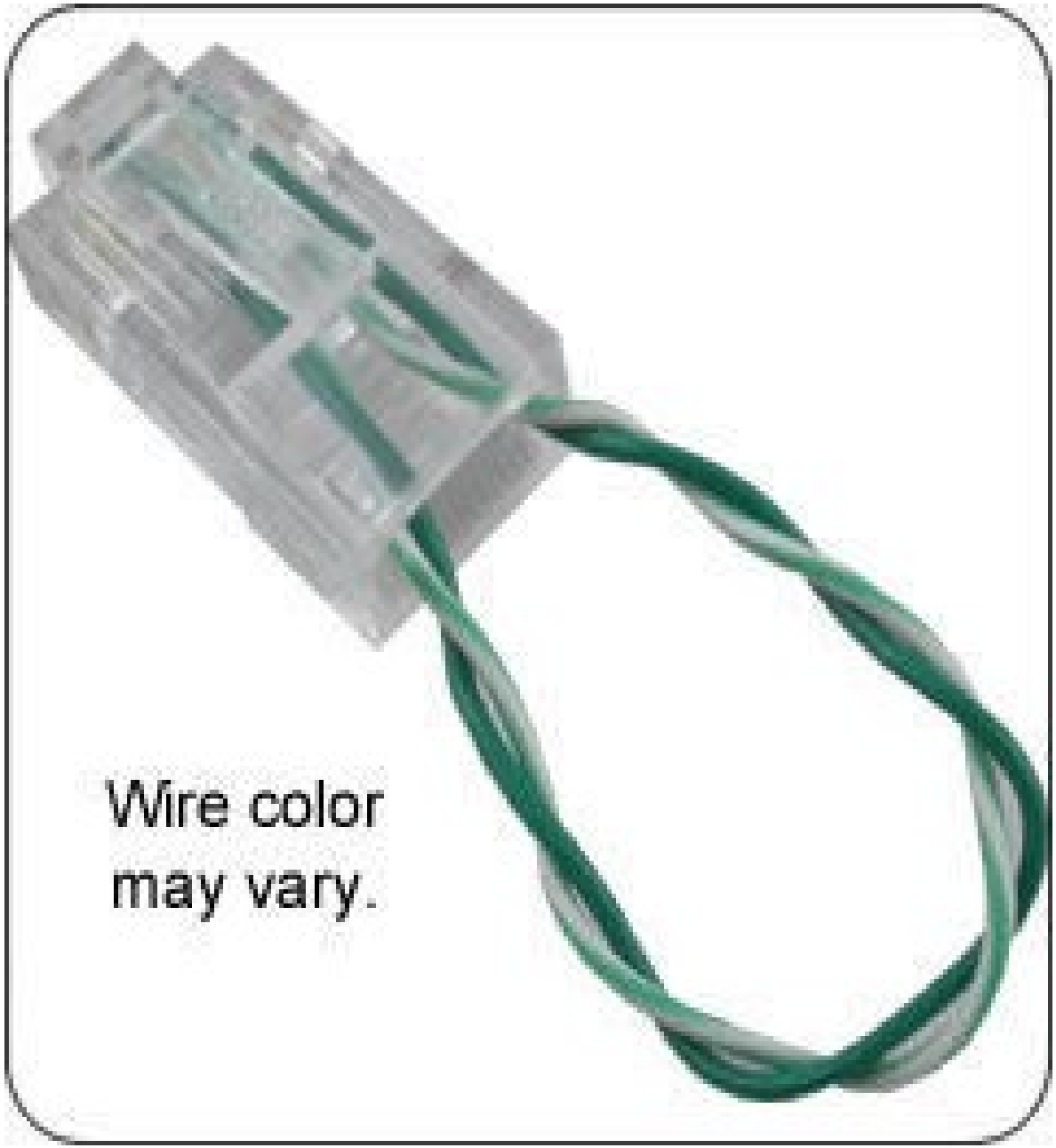


Hardware Loopback

- 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, then returned as received data. If the transmitted data does not return, the hardware loopback detects a hardware malfunction.

- A hardware loopback is a special connector for the Ethernet 10Base-T NICs. It is used by the NIC's software diagnostics to test transmission and reception capabilities,

- The NIC manufacturers provide diagnostic routines that could be used to troubleshoot NICs for proper functioning. Such diagnostic routes normally use hardware loopback through which an NIC transmits, and receives the same data for further diagnosis.


Wire color
may vary.

Tone Generator and Tone Locator

- Tone generators are standard tools for wiring technician in all fields. A tone 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.

- 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."

- The combination of tone generator and tone locator is used in telephone systems to locate cables. The tone generator is a small electronic device that sends an electrical signal down one set of UTP wires
- Then move the locator over multiple sets of cables until a tone is heard.


TENMA
Amplifier Probe
CE

Software Tools:

- **Protocol analyzer**
  - The protocol analyzer is the tool which is used to analyze the network protocols including UDP, TCP, FTP and HTTP.
  - This protocol analyzer can also act as a software as well as hardware based.
  - Additionally, this tool is also used to identify malicious and wanted networks traffic, identify and clear the computer networking problem, alert the user when protocols unused and its related issues. Similar to packet sniffers, this tool capture communication stream in between the system. Additionally, unlike packet sniffers, this tool captures more network traffic and it decodes and read the traffics. This decoding will allow the administrators to check network communications in English. Through this, the administrator will get great ideas about the traffic, which is running on the network.
  - This protocol analyzer also refers to an IP load tester, telecom network protocol analyzer, a bus analyzer and a network packet analyzer.