

Practical no. 1

Identifying various Hardware components of a network.

Computer network components are the major parts which are needed to install the software. Some important network components are NIC, switch, cable, hub, router and modem.

Following are major components required to install a network:

NIC:

NIC stands for network interface card. It is a hardware component used to connect a computer with another computer onto a network.

There are two types of NIC:

- i- wired NIC
- ii- wireless NIC



Modem



NIC



Repeater



Hub



Switch



Router



Bridge



Gateway

Wired NIC:

The wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

Wireless NIC:

The wireless NIC contains antenna to obtain connection over wireless network.

HUB:

A HUB is a hardware device that divides network connection among multiple devices. The process used by HUB consumes more bandwidth and limits the amount of communication.

Switch:

A switch is a hardware device that connects multiple devices on a computer network. A switch contains more

advanced features than HUB.

Router:

A router is a hardware device which is used to connect LAN with internet connection. A router works in network layer. It forwards packet based on information.

Modem:

A modem is hardware device that allows computer to connect internet over existing telephone line. It stands for Modulator/Demodulator. It converts digital data into analog signal over telephone lines.

Cables and Connectors:

Cable is transmission media used for transmitting a signal.

There are three types of cables:

- i- Twisted pair cable
- ii- Fibre-optic cable
- iii- Coaxial cable

Practical no. 2

Studing Network Card

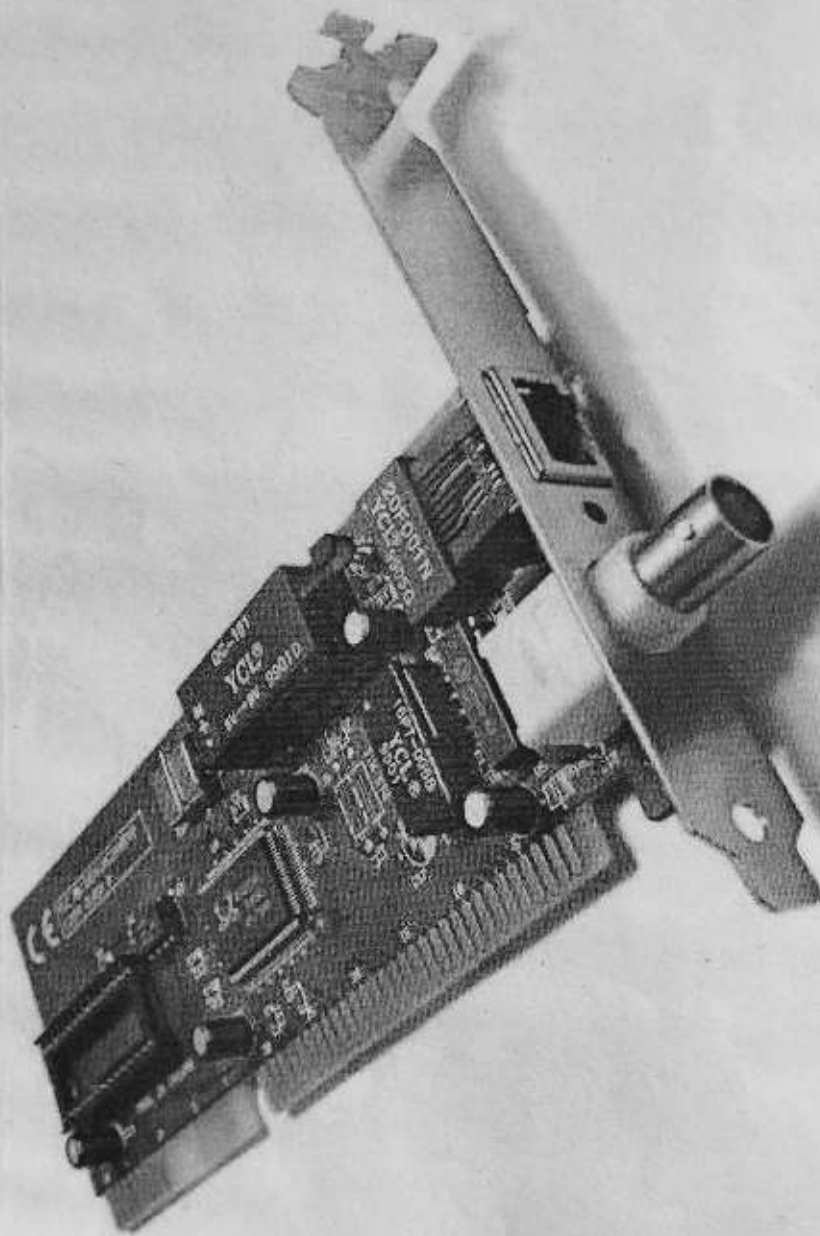
NICs - sometimes called network cards - are the mechanisms by which computers connect to a network. NIC's come in all shapes and sizes, and they come in prices to suit all budgets.

Network compatibility:

Perhaps this is a little obvious, but sometimes people order the wrong type of NIC for network. Given the prevalence of Ethernet networks, you are likely to have to specify network compatibility only when buying NIC for another networking system.

Port compatibility:

Generally a NIC has only one port, for twisted - pair cabling. If we want some



other connectivity, you need to be sure to specify your card accordingly.

Hardware compatibility:

Before installing a network card into a system, you must verify compatibility between network card and operating system. If you are using good-quality network cards from recognized manufacturers, such verification should be little more than a formality.

Types of network interfaces:

Network interfaces come as add-in expansion cards or as PCMCIA card and network. A network interface typically has at least two LEDs that indicate certain conditions:

Link light:

This LED indicates whether a network connections exists between card and network.

Activity light:

This LED indicates network activity. Under normal conditions, the light should flicker sporadically and often.

Speed light:

This LED indicates that interface is connected at a certain speed. This feature is normally found on Ethernet NICs that operates at 10Mbps/100Mbps.

Installing network cards:

At some point in your networking career, it is likely that you will have to install a NIC into a system. For that reason, an understanding of procedures related to NIC are installed.

Built-in network interfaces:

A built-in network interfaces is a double-edged sword. The upsides are that it does not occupy an expansion slot and the hard compatibility.

Practical no. 3

Coaxial Cable

Coaxial cable is commonly used by cable operators, telephone companies, and internet providers around the world to convey data, video and voice communication to customers.

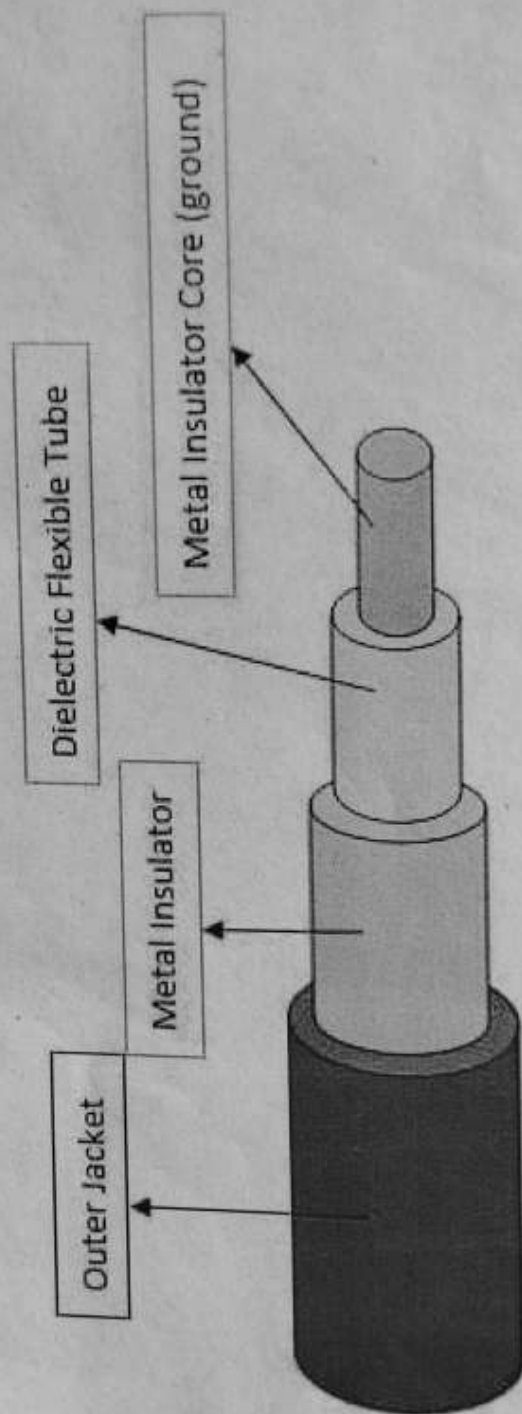
The three most common cable sizes are RG-6, RG-11 and RG-59:

- RG stands for "radio guide." The number of various versions of RG cable refer to diameter. They are also called RF cables.

- Most non-industrial coax is now known as RG-6, but installers may use a thicker cable, like RG-11.

- RG cables used in homes should be 75 ohm impedance.

There are several types of



F-type Connectors for RG-6 cables:

- Compression connector
- Screw-on connectors
- Crimp-style connector

What are coaxial cable?

It is a type of cable that has an inner conductor. Many cables have an insulating outer jacket.

i- Centre conductor: copper-clad steel.

ii- Centre conductor bond- clean stripping polymer is utilized to block moisture migration.

iii- Dielectric: polyethylene providing mechanically stable, closed cell foam with high VP.

iv- First outer conductor: shield with an aluminium polymer aluminium tape securely bonded to dielectric core.

v- Integral messenger: a galvanized, carbon steel wire support member attached to cable by a separable web.

Practical no. 4

Twisted Pair Cable

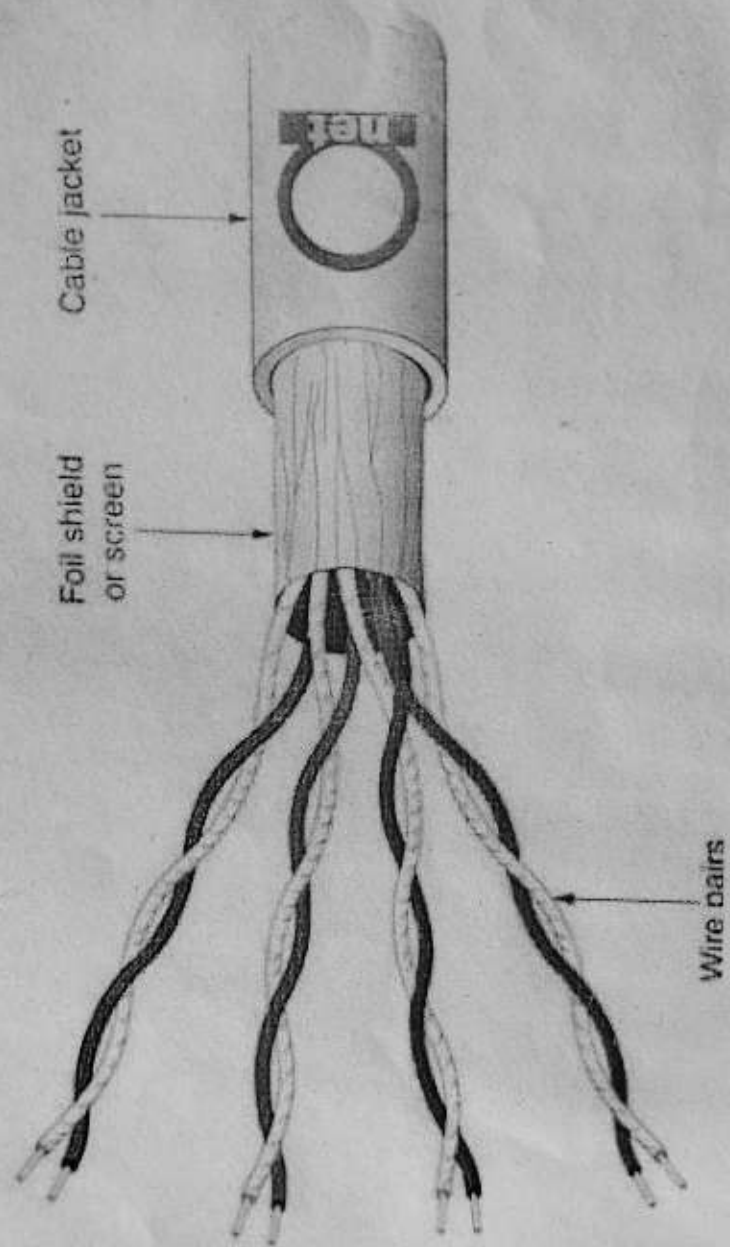
Twisted pair is the ordinary copper wire which connects home and many business computers to telephone company.

Twisted pair cable is good for transferring balanced differential signals.

How to make network cable?

To create network cable, you will first need equipment listed below:

- Cat₅, Cat_{5e}, Cat₆ or Cat₇ cable
- RJ-45 connectors
- Crimping tool
- Wire stripper or knife



Once you have necessary equipment needed to create a network cable, you need to determine type of network cable you want to create. There are two major network cables:

i- Striaight through cable (T568A)

Computer to HUB, switch, router
or wall.

ii- Crossover cable (T568A & T568B)

a. Computer to computer with no switch or hub.

b. Network device to network device.

For example, router to router.

Practical no. 5

Using a cable tester.

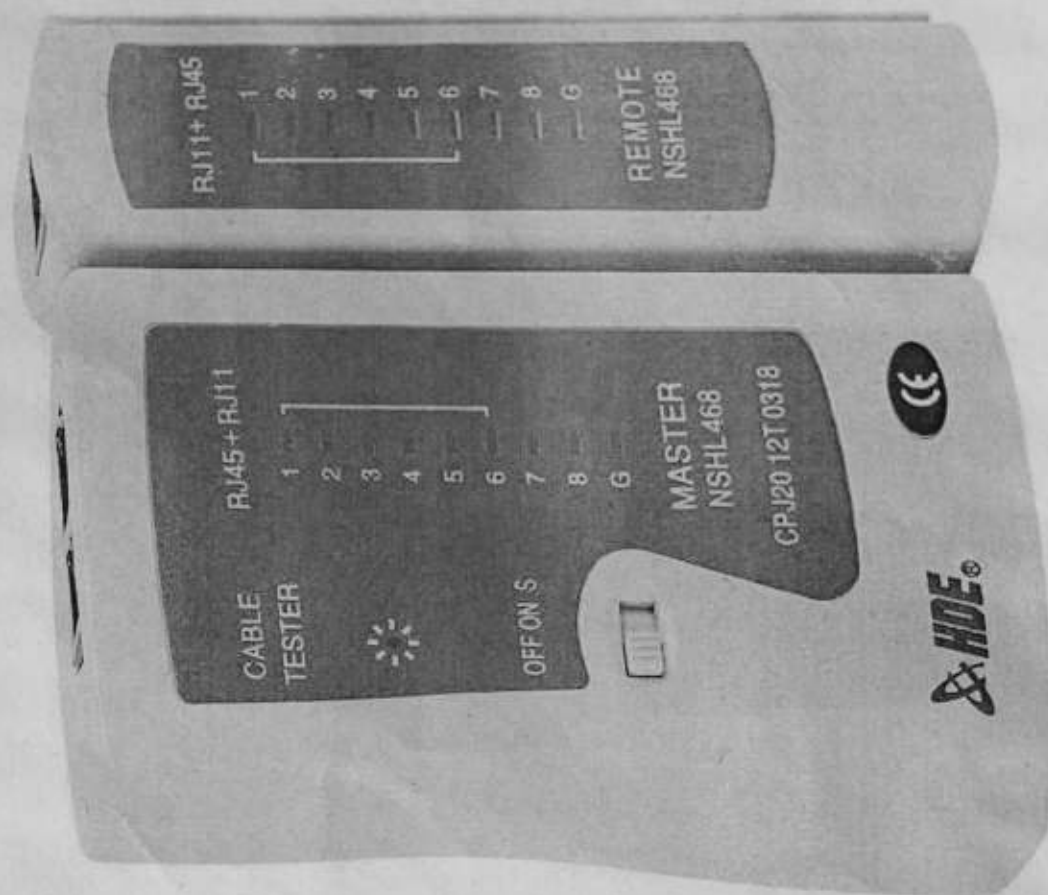
What is cable tester?

A cable tester is a hand held electronic device. It is used to verify electrical connections in a cable network.

Signal strength, particularly in computer networks, is crucial for data transmission.

When to use a cable tester?

Once you are ready to check if a cable is set up properly to achieve strong connection between source and destination. That type is, typically after installation/set up is complete. It is good practice to test system once all components are connected in order to assure the job has been done properly.



If the test shows connectivity troubleshoots, you can address issue(s) and retest.

Possible issues:

- Connection between server and the computer(s) is weak.
- Outside interference causing data loss or decreased signal strength
- Faulty cable

How to use cable tester:

- 1- Select the cable to be tested and make sure it is not plugged to any electrical power.
- 2- Visually inspect the cable for damage.
- 3- Plug it into appropriate port on cable tester, connect other end to remote.
- 4- Switch tester on to test your cable. The tester will show results.

Practical no. 6

Configuring MAC address on Windows/Linux OS.

A device's MAC address is assigned by the manufacturer, but it's not too hard to change - or "spoof" - those addresses when you need to. Here's how to do it, and why you might want to.

What MAC address are used for?

At a lowest networking level, network interfaces attached to network use MAC addresses to communicate with each other. When a browser on your computer needs to grab a web page from a server on internet, for example, that request passes down through several layers of TCP/IP.

Change a MAC address in Windows:

First, open the Device manager.

On windows 8 and 10, press Windows + X, and click "Device Manager" on Power user menu. On windows 7, press window key, type "Device Manager" to search for it, then click "Device Manager" entry.

In device manager, under "Network adapters" section, right click network interface you want to modify, then select "Properties". Now, on the "Advanced" tab and select "Network address" entry in "property" list.

Enable value option and type your desired MAC address. Click "OK" when you're done.

In Modern Linux distributions like Ubuntu, you'd click the network icon on top panel, click "Edit

Connections", select the network connection you want to modify, and then click "Edit".

On the Ethernet tab, you'd enter a new MAC address in "Cloned MAC address" field, then save your changes.

Practical no. 7

Configuring IP address on Windows.

Sometimes, it's better to assign a PC its own IP address rather than letting your router assign one automatically. Right now, the IP addresses for your PCs and other devices are automatically assigned by your router using a protocol known as Dynamic Host Configuration Protocol (DHCP).

Set a static IP address in window 7, 8 and 10.

To change a computer's IP address in Windows, you'll need to open "Network connections" window. Hit Windows + R, type "ncpa.cpl" into Run box, and then hit Enter.

In "Network Connection" window, right-click the adapter for which you want

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

192 . 168 . 1 . 2

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

. . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

8 . 8 . 8 . 8

Alternate DNS server:

8 . 8 . 4 . 4

☒ Validate settings upon exit

Advanced...

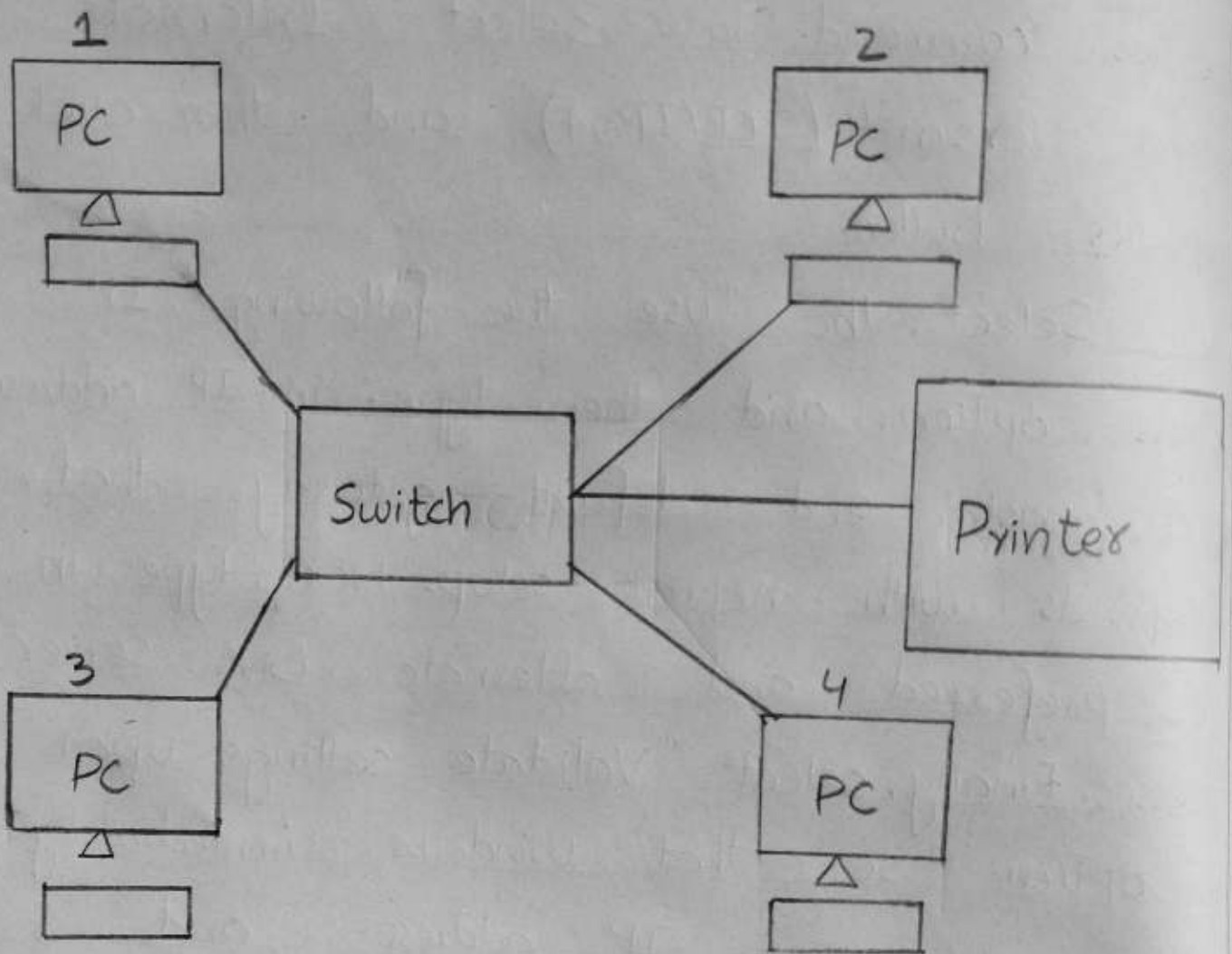
OK

Cancel

to set a static IP address, then select "properties" command. Now select "Internet Protocol Version 4 (TCP/IPv4)" and then click "Properties" button.

Select the "use the following IP address" option, and then type in IP address, subnet mask and default gateway that corresponds with network setup. Next, type in your preferred and alternate DNS server addresses. Finally, select "Validate settings upon exit" option so that windows immediately checks your new IP address and corresponding information to ensure that it works. When you're ready, click "OK" button.

And then close out of network adapter's properties window.



Practical no. 8

Designing a Local Area Network.

Part 1: Determining your network Needs:

- 1- Count the number of computers you need to handle.
- 2- Decide if you want to create a wireless network.
- 3- Determine if you want all network devices to have internet access.
- 4- Measure the distances for all hardwired devices.
- 5- Consider your future need.

Part 2: Setting UP Basic LAN:

- 1- Gather your network hardware.
- 2- Setup your router.
- 3- Connect your modem to router.
- 4- Connect your switch to your router.
- 5- Connect your computers to open LAN ports.
- 6- Setup one PC as a DHCP server if you're just using a switch.
- 7- Verify network connection on each computer.
- 8- Setup file and printer sharing.

Practical no. 9

Troubleshooting network connectivity.

Always start troubleshooting using these simple network troubleshooting steps to help diagnose and refine issue.

1. Check the hardware:

When you're beginning the troubleshooting process, check all your hardware to make sure it is connected properly, turned on and working.

2. Use ipconfig:

Open the command prompt and type "ipconfig" into terminal.

3. Use ping and tracert:

If your router is working fine, and you have an IP address

starting with 169, the problems most likely located between your router and internet.

At this point, it's time to use ping tool.

You can Ping Google DNS servers by opening command prompt and typing "ping 8.8.8.8", you can also add "-t" at the end (ping 8.8.8.8-t).

4- Perform a DNS check:

Use the command "nslookup" to determine whether there's a problem with server you're trying to connect to.

5- Contact the ISP:

If all the above turn up no problems, try contacting your internet service provider to see if they're having issues.

6- Check on virus and malware protection:

Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.

7- Review database logs:

Review all your database logs to make sure databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

Practical no. 10

Installing and Configuring a Network Printer.

A network printer is a printer that is connected to a computer network and can be accessed from many different computers.

Installation:

Connect your network to your printer. The process for this varies from printer to printer.

- If your printer is wi-fi capable, you can generally connect it to network using built-in menu display.

- Make sure your wi-fi printer is close enough to router to get solid signal.

Connectivity:

- Click start menu and select control panel. windows 8 users can press \square win and type "control panel."
- Select "devices and Printers" or "View devices and printers".
- Click Add a printer at top of window.
- Select "Add a network, wireless or Bluetooth printer".
 - Select your network printer from list and click next.
 - Install necessary drivers if prompted. windows should be able to find and install correct drivers for most printers.

Printing:

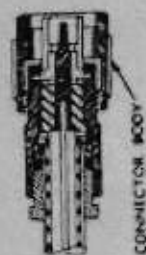
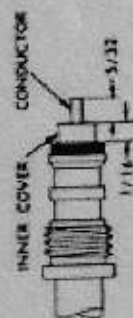
Print to the network printer.

- make sure that printer is turned on and that you are connected to the same internet.

PROCEDURE

1. CUT CABLE TO PROPER LENGTH AND REMOVE $5/16$ INCH OF OUTER COVER.
2. COME OUT SHIELDING.
3. SLIDE LOCK NUT, GASKET, AND BRAID CLAMP ON CABLE.
4. FOLD SHIELDING OVER BRAID CLAMP AND TRIM EXCESS.
5. CUT INNER COVER TO $1/16$ INCH AND CONDUCTOR TO $5/32$ INCH AS SHOWN.
6. TIN CONDUCTOR AND REMOVE EXCESS SOLDER.
7. SOLDER CONTACT TO CONDUCTOR.
8. INSERT CONTACT INTO CONNECTOR BODY, SLID GASKET FORWARD AND TIGHTEN LOCK NUT SECURELY.

ILLUSTRATION



Practical no. 11

Terminating the coaxial cable.

Procedure:

Ensure dielectric is securely seated into the compression connector.

The dielectric should not pass through the hole at the end of compression connector.

The center conductor should extend slightly past the end of compression connector.

Practical no. 12

Using Network Monitors.

The network monitoring systems are used by the technicians to ensure availability and overall performance of system and network services. They allow admins to monitor right to use, routers, slow mechanisms, firewalls, core switches, client machine, and server performance, among other network data.

What does a network monitor do?

Network monitoring is the use of system that constantly monitors a computer network for slow and failing components and that notifies the network administrator (via email, SMS or

other alarms) in case of outages or other trouble.

Four categories of network monitoring:

1. Availability monitoring
2. Configuring monitoring
3. Performance monitoring
4. Cloud infrastructure monitoring