King Fahd University of Petroleum & Minerals

Electrical Engineering Department

EE 400, Experiment # 1

Internetworking Basics, Devices and Models. Configuration of TCP/IP Parameters and Troubleshooting Network Connectivity using DOS Networking Utilities.

Objectives:

1. Internetworking Basics and Devices
2. Internetworking Models; OSI Model
3. Network Cables; Categories and Types.
4. TCP/IP Model
5. DHCP Protocol.
6. Static Configuration of TCP/IP Parameters.
7. Dynamic Configuration of TCP/IP Parameters
8. Use *ipconfig* utility to view configured TCP/IP parameters.
9. Use *ping* utility to test TCP/IP communications.
10. Use *arp* command

INTERNETWORKING BASICS AND DEVICES

Network Interface Card:

Network interface cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable.

Many NIC adapters comply with Plug-n-Play specifications. On these systems, NICs are automatically configured without user intervention, while on non-Plug-n-Play systems, configuration is done manually through a setup program and/or DIP switches.

Cards are available to support almost all networking standards, including the latest Fast Ethernet environment. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Full duplex networking is another option, where a dedicated connection to a switch allows a NIC to operate at twice the speed.

Repeater :

A repeater is a device used to extend the network length and topology beyond what can be achieved by a single cable segment. It is used to re-time and amplify the individual signals and has no concept of packets.

Repeaters, also called hubs or concentrators, are bit level devices. What this means that they do not examine the data packets that travel through them. They have no knowledge of addresses associated with the source or the destination. The basic operation of a repeater is to repeat traffic. Any data arriving on one port will be amplified and repeated out all ports (except the port on which it was received).

Repeaters were originally designed with only two ports and were used to increase the size of coax cable-based networks. This way, different lengths of coax cable coulds be attached to the repeater to extend the size of the network. This would allow the network to reach all areas of large or tall buildings. Data would be repeated from one cable segment to the other.

When the coax cabling was replaced by concentrators or hubs, the concentrators were, in fact, just repeaters with many more ports. Now, data reeived on one port would be replicated anywhere from twice to hundreds of times and transmitted to attached stations. The repeater also had the ability to track how much traffic was crossing through it.

Repeaters may also be linked together for even greater distances, but it is recommended that the data should not need to cross more than four repeaters. This is because each time the data gets repeated it may be slightly distorted. If there are too many distortions, original signal may be unreadable.

A very important fact to note about hubs is that they only allow users to shared Ethernet. A network of hubs/repeaters is termed a "shared Ethernet," meaning that all members of the network are contending for transmission of data onto a single network (collision domain). This means that individual members of a shared network will only get a percentage of the available network bandwidth

Repeaters support all standard LAN protocols and cabling types, and a repeater can translate between different cabling. Today, repeaters are being replaced called a bridge.

Bridge and Layer-2 Switch:

A bridge operates at layer 2 of the OSI model and offers several functions, including expansion of networks beyond normal physical limitation, overcoming station count limitations, packet storage and forwarding, and keeping local traffic local by building an address table (SAT) of where devices are located within the network.

Bridges offer several advantages over repeaters, including:

- **Expansion of network** - because of regeneration issues, packets can only be repeated a limited number of times. Bridges eliminate the problem by copying and recreating new packets before forwarding them.
- **Overcoming station count limitations** - each type of LAN (Ethernet, token ring, FDDI) has a maximum number of users allowed on one segment. Bridges allows for the creation of multiple bridging segments.
- **Packet storage and forwarding** – bridges receive the packet, examine it, and then determine where it needs to go. If there is other traffic on the destination port, the bridge buffers (stores) the packet until the port is able to accept more traffic.

- **Keeping local traffic local** – the bridge's ability to read packets and identity addresses enables it to determine where a destination is located. This eliminates sending packets to segments that do not contain the destination.
- **Translating between different speeds** – bridges are required to interface between networks of different speeds (e.g., Ethernet's 10, 100, and 1000 Mbps)

- **Translating traffic between LAN protocols** – bridges, acting as interpreters, have the ability to translate packets between other LAN protocols such as Ethernet, token ring, FDDI, and ATM.

Bridges fit into the network in a similar fashion as repeaters and they support all the capabilities of repeaters (amplifications of signals, etc.). However, bridges have increased intelligence and can perform additional functions.

The repeater repeats all traffic that goes through it, so if I had a 24-port repeater and a packet came in one port, it would be repeated out 23 other ports. This is because the repeater does not know where to send it. A bridge, though, is aware of the individual packets and the addressing that is used. A bridge that receives that same packet examines it and resends it only to the port that has the destination address attached to it. Obviously, this is a better way to handle traffic.

Besides having the ability to examine packets and forward based on addresses, bridges have the ability to learn where the different addresses are located on the network. This means the bridge will learn which PC is located on which port, and it also keep track of this address if the PC is moved. Bridges can also be used to separate repeated networks. Bridges support all protocol and media types, and even have the ability to translate one LAN protocol to another.

Routers:

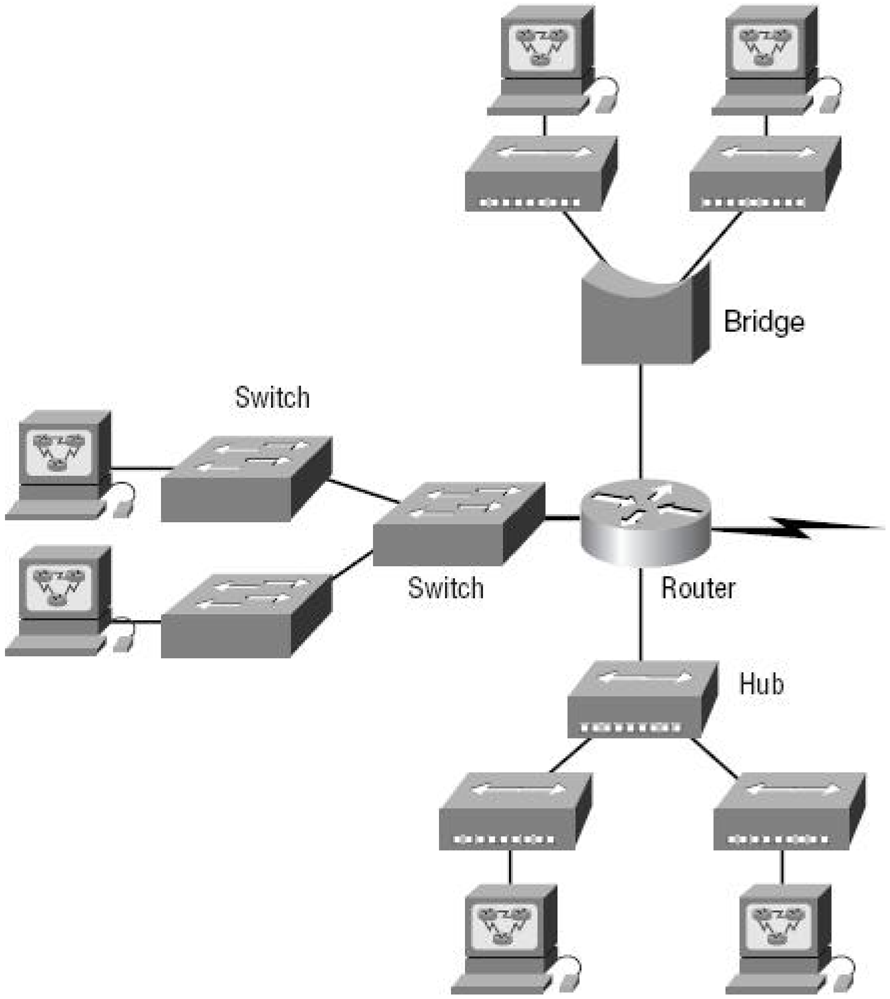
Routers perform their function at layer 3 of the OSI Model and are used to forward messages across an extended network based on network layer addresses (logical addressing), not MAC layer addresses. They route messages from end-station to end station, allowing multiple paths between them. Routeres can also be used to provide better traffic isolation and security by using access lists that control who can communicate through the router. Routers are used to forward traffic on the internet.

Routers offers several advantages over repeaters and bridges. These include:

- **Isolation of broadcast traffi**c **–** routers prevent the flow of broadcast traffic from one LAN to another.
- **Path selection** – routers can use the best path that physically exists between source and destination. Some routers allows for load balancing over redundant paths.
- **Flexibility –** routers can support any desired protocol or network topology.
- the total size of the network interconnected with routers is, for all practical purposes, unlimited (e.g., the Internet)
- Routers supports layer 1,2,and 3 functionality.

Note : Routers are more intelligent than bridges, but they are not plug-and-play routers must be configured by a human.

Routers are designed to separate different parts of the network into what are called sub-nets, which are subdivisions of the the total network. This division of the network is done to support the different requirements of the organization, and it allows a network manager to separate and control traffic in the different sub-nets. Routers are often used to separate the network for the purpose of security. Doing this allows a network manager to keep some traffic inside a sub-net and allows other traffic to cross sub-net boundaries. An example of using routers and sub-nets would be a large company that has divided their network up based on departments. Sales might be one sub-net, marketing on another sub-net, and engineering on another sub-net. All these sub-nets would form the complete network, and within each sub-net is a collection of users connected to bridges or repeaters.
Routers support all the capabilities of bridges and repeaters along with network layer (layer3) protocols.



Layer-3 Switches:

Networks started as a collection of computers connected by a single cable.

The next evolution of networks was the introduction of the repeater. The repeater allowed the larger networks (Distance and size) and eliminated the cable as a single point of failure. The problem was that traffic was flooded everywhere.

The next evolution was the bridge. Originally, bridges were designed to separate networks into different sections, and this cut down on the amount of flooded traffic. Bridges could then used to interconnect groups of users connected to repeaters.

Next came the router. With the routers, logical groupings could be defined, traffic could be better controlled. Now you had networks with users connected to repeaters, the repeater connected to bridges and the bridges connected to routers, with each network network device doing its own thing.

A switch operates at layer 1, layer 2, and layer 3 (sometimes layer 4) and allows users to use a single device to support multiple capabilities. Now, using one device, some traffic can be repeated, some bridged, and some routed, all based on where the traffic needs to go. This is called switching. Switches combine the intelligence of repeaters, bridges, and routers into one networking device. Some of the advantages to using single box for all three functions are listed as follows:

- Save time – one device to manage
- Single device required for spare
- Reconfigure instead of move/replace
- Single version of software need for upgrading network.

Switches look like repeaters or bridges and allow direct connection to the PCs or to other switches, bridges, or routers, These devices are designed with much more intelligence built in, and the network manager can configure any port, or groups of ports , to act as repeaters, bridges, or routers. the idea here is that you do not need to purchase and manage three different types of devices in your network – you can purchase one type of device and configure it the way you need it.

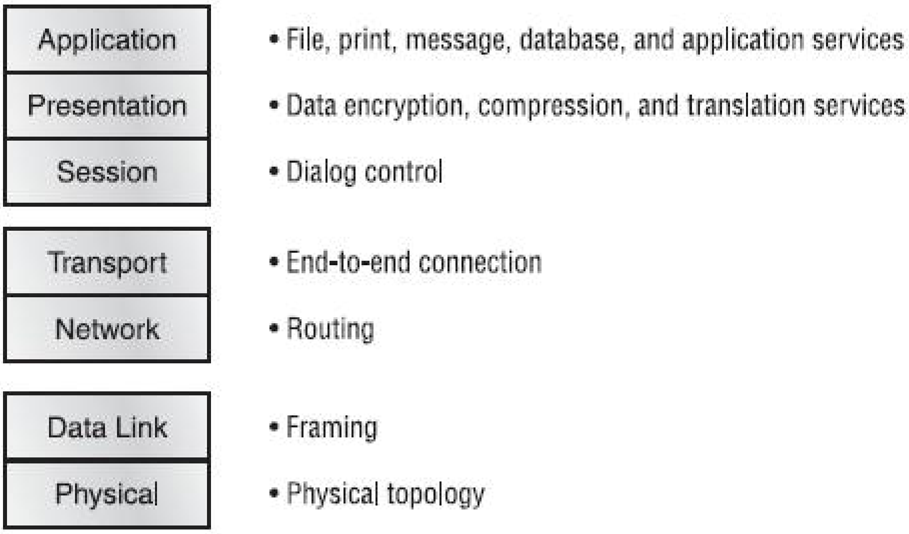
OSI REFERENCE MODEL

One of the greatest functions of the OSI (Open Systems Interconnection) specifications is to assist in data transfer between disparate hosts – meaning, for example, that they enable us to transfer data between a Unix host and a PC or a Mac.

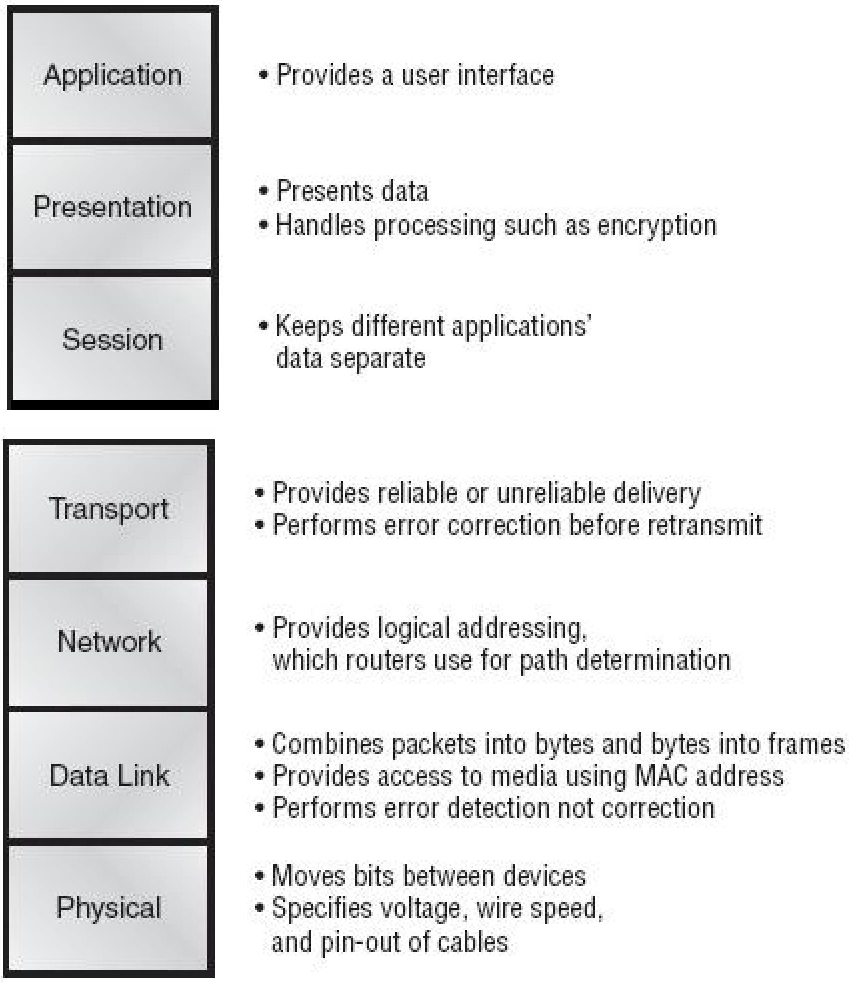
The OSI is not a physical model, though. Rather, it is a set of guidelines that application developers can use to create and implement applications that run on a network. It also provides a framework for creating and implementing networking standards, devices, and internetworking schemes.

The OSI reference model has seven layers:

- Application layer (layer 7)
- Presentation layer (layer 6)
- Session layer (layer 5)
- Transport layer (layer 4)
- Network layer (layer 3)
- Data Link layer (layer 2)
- Physical layer (layer 1)



The OSI has seven different layers, divided into two groups. The top three layers define how the applications within the end stations will communicate with each other and with users. The bottom four layers define how data is transmitted end-to-end.


Application
• Provides a user interface
Presentation
• Presents data
• Handles processing such as encryption
Session
• Keeps different applications' data separate
Transport
• Provides reliable or unreliable delivery
• Performs error correction before retransmit
Network
• Provides logical addressing, which routers use for path determination
Data Link
• Combines packets into bytes and bytes into frames
• Provides access to media using MAC address
• Performs error detection not correction
Physical
• Moves bits between devices
• Specifies voltage, wire speed, and pin-out of cables

NETWORK CABLES

Cable Categories:

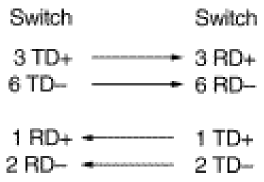
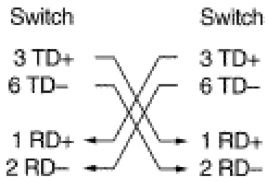
Cable categories represent the amount of twist per unit length in the cable that results in better shielding effect in the cable thus increasing the capability of the cable to carry high speed data.

- *Category 1*: suitable for voice only (1950s)
- *Category 2*: suitable for voice and low data rates (less than 4 Mbps). (1960s)
- *Category 3:* suited for voice and data rates up to 10 Mbps. Uses 4 twisted-pairs. Standard for most telephone installations. (1991)
- *Category 4:* consists of 4 twisted-pairs. Suitable for data rates up to 16 Mbps. Support fast Token Ring networks. (1993)
- *Category 5:* consists of 4 twisted-pairs. Suitable for data rates up to 100 Mbps. Supports 100Base-TX. (1994)
- *Category 6:* consists of 4 twisted-pairs. Suitable for data rates up to 1 Gbps. Supports 1000Base-TX. (1994)

Straight-Through and Crossover Cable Pin outs:

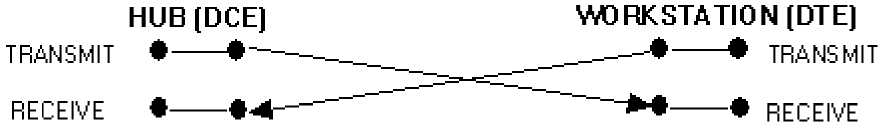
Cables ending in RJ45's may be wired up in two ways: **straight through** and **crossover**. A straight through cable connects pins N at both ends, whereas a crossover cable has the various pairs crossed over. Whether a straight through or crossover cable is required will depend on the types of network equipment and how they are interlinked.

The schematics of crossover and straight-through cables are shown in below.

Straight-Through Cable Schematic	**Crossover Cable Schematic**
 Switch Switch 3 TD+ 3 RD+ 6 TD– 6 RD– 1 RD+ 1 TD+ 2 RD– 2 TD–	 Switch Switch 3 TD+ 3 TD+ 6 TD– 6 TD– 1 RD+ 1 RD+ 2 RD– 2 RD–

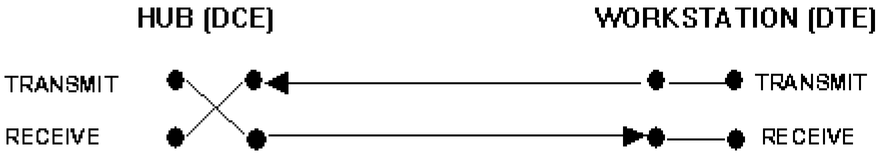
MDI / MDI-X ports:

Consider the connection between a hub (DCE) and a workstation (DTE), shown in the figure below



The connection between a DCE and a DTE using a crossover cable.

There must be a point of crossover between the DCE and DTE for data to be successfully exchanged. Above figure shows a cable with the transmit and receive pairs crossed over. On a hub most of the ports will connect to DTE's (workstations, PCs etc.) and at some point a signals crossover must be affected. Equipment manufacturers are aware of this situation so the industry accepted standard is that all ports on hubs and switches which do not have a media conversion capability have crossovers already built in. In such cases (the vast majority) only a straight-through cable is required to connect to a DTE. Figure below shows the DCE (hub) with a built in crossover port. Visually it is not easy to distinguish between straight-through and crossover cables so it is preferable to avoid having both types of cable in an installation. Using hubs and switches with crossover ports built in is a way of eliminating the need for crossover cables altogether. Ports on such equipment are often marked **MDI-X (Media Dependant Interface-Internally Crossed over).** Uplink ports (e.g. 100BaseT) will not usually have built-in crossover and may be marked **MDI (Media Dependant Interface).**



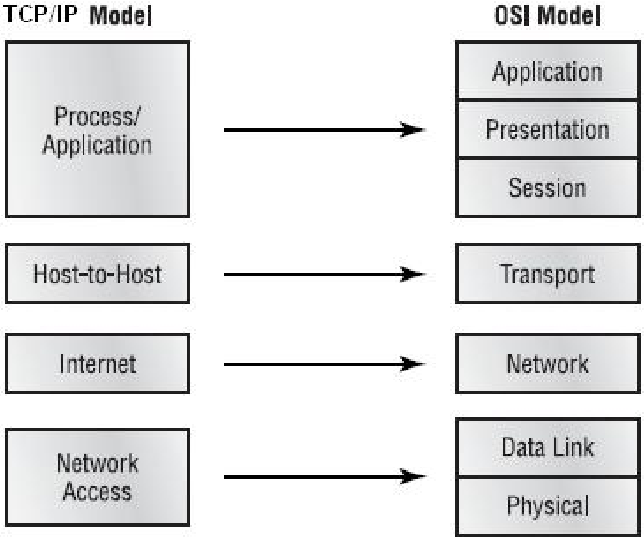
The connection between a DCE and DTE using a straight through cable because the port of the DCE is already crossed over internally. Many hubs and switches feature ports which are switchable between crossover for DTE connection and straight-through for cascading or up linking, all others being MDI-X only, or unmarked.

TCP/IP MODEL

The TCP/IP model is basically a condensed version of the OSI model – it is composed of four, instead of seven, layers:

- Process/Application layer
- Host-to-Host layer
- Internet layer
- Network Access layer

Figure below shows a comparison of the TCP/IP model and the OSI reference model. As you can see, the two are similar in concept, but each has a different number of layers with different names.



DHCP (Dynamic Host Configuration Protocol)

Dynamic Host Configuration Protocol (DHCP) gives IP addresses to hosts. It allows easier administration and works well in small-to-even-very-large network environments. All types of hardware can be used as a DHCP server, including a Cisco router.

There is a lot of information a DHCP server can provide to a host when the host is requesting an IP address from the DHCP server. Here is a list of the information a DHCP server can provide:

- IP address
- Subnet mask
- Domain name
- Default gateway (routers)
- DNS
- WINS information

A DHCP server can give us even more information than this, but the items in that list are the most common. A client that sends out a DHCP Discover message in order to receive an IP address sends out a broadcast at both layer 2 and layer 3. The layer 2 broadcast is all “Fs” in hex, which looks like this: FF:FF:FF:FF:FF:FF. The layer 3 broadcast is 255.255.255.255, which means all networks and all hosts.

Domain Name Service (DNS)

The Domain Name System protocol provides a mapping between cryptic IP address and, easier to remember, host names. Host names are used because they are easier for humans to remember. For example, telnet mail.kfupm.edu.sa is easy to remember than telnet 196.15.32.8

The Internet Domain Name System (DNS) is an attempt to decentralize administration of the mapping of host names to host addresses by the use of name-servers, each of which controls part of name space. This becomes necessary partly because the static host table formerly used for that purpose most of the hosts in the Internet are on networks local to particular organizations. It is desirable to allow the local administration to control that mapping. The DNS also implements a hierarchical naming scheme and provides protocols for communication with the name-servers. A set of top-level domains is administered by the Internet and is defined in the basic DNS specifications.

Top Level Domains:

The top level domains can be categorized as Organizational and Geographic:

com	Commercial
edu	Educational
gov	Governmental
mil	Military
net	Administrative organizations for network such as CSNET, BITNET etc.
org	Other Organizations
XX	two letter country code, e.g., sa for Saudi Arabia.

Network Identification Settings

1. Right click on **My Computer** icon on desktop, click on **Properties**, Click on **Network Identification** tag, click on **Properties**.
2. Type computer name **ee400pcX** (where **X** is the number of computer written on your computer).
3. In peer-to-peer networking, the computer is standalone or a part of any Workgroup. Check *Workgroup* and type **ee400** in workgroup.
4. Click **OK**, and click **OK** again and restart your computer for new settings to take effect.

Static Configuration of TCP/IP Parameters

1. In *Local Area Connection Properties* window, select *Internet Protocol (TCP/IP)* then click **Properties**.
2. *Use the following IP address* then you would have to enter the static IP address with proper subnet mask and gateway address. (The static IP address is **10.59.2.X**, where X is your computer number, subnet mask is **255.255.240.0** and default gateway is **10.59.0.64**).
3. Check *Use the following DNS server addresses,* Enter **10.140.3.165** in the *preferred DNS server* (Primary DNS server) and enter **10.140.1.160** in the *Alternate DNS server* (Secondary DNS server).
4. Click on **Advanced**, in *IP settings* tab you will see the computer IP address and gateway address, if there is no gateway address present, then click **Add**, enter the *default gateway address* and click **Add** again.
5. Click **DNS** tab, you will see the DNS server addresses.
6. Click **WINS** tab, if there is no WINS addresses, click on **Add**, and enter **196.15.32.158**, click **Add**.
7. Now click **OK**, click **OK** again on TCP/IP properties window.
8. Click close on Local Area Connection Properties window.

Using ipconfig

1. Start *command prompt*, click on **Start**, click **RUN**, and type **cmd** and press enter, you will enter in the DOS command prompt.
2. To verify the TCP/IP parameters, type **ipconfig** and press enter, you will see the IP address of your computer, subnet mask, and default gateway.
3. For a detailed configurations, type **ipconfig /all** and press enter, now you will see the host name of your computer, IP address of your computer, subnet mask, default gateway, MAC/Physical address, DNS servers, WINS server IP addresses etc.

Dynamic Configuration of TCP/IP Parameters

1. In *Local Area Connection Properties* window, select *Internet Protocol (TCP/IP)* then click **Properties**.
2. Now Select *Obtain an IP Address automatically.* Then select *Obtain DNS server address automatically*.
3. Now click **OK**, click **OK** again on TCP/IP properties window.
4. Click close on Local Area Connection Properties window.
5. Now verify the TCP/IP parameters, use **ipconfig** and **ipconfig/all**, you will see the IP address of your computer, subnet mask, and default gateway and all other details.

Using ping (Packet Internet Groper)

1. Start *command prompt*, click on **Start**, click **RUN**, and type **cmd** and press enter, you will enter in the DOS command prompt.
2. Type **ping 127.0.0.1** and then press enter. This internal loop-back test should give you four replies if TCP/IP is bound to the Network Adaptor.
3. Now we will test the TCP/IP connectivity, **ping 10.59.0.64** (which is the EE-400 lab Gateway). Four replies messages from Gateway should appear if the configurations are OK.
4. Try **ping** other computers in the lab.

ARP Cache

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP) network layer protocol to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the OSI link layer, and is used when IP is used over Ethernet

1. Log on as a Local **Administrator**.
2. First ping some computers, then.
3. Start the command prompt, type **arp –a** and then press **Enter** to view the ARP cache.
4. **Ping** the IP address of any computer in the lab. This will add an entry to the arp cache.
5. View the new entry in arp cache.
6. To remove the any entry in the ARP cache, type **arp –d** <IP_address>. (where the IP_address is the one to be removed from the ARP cache).