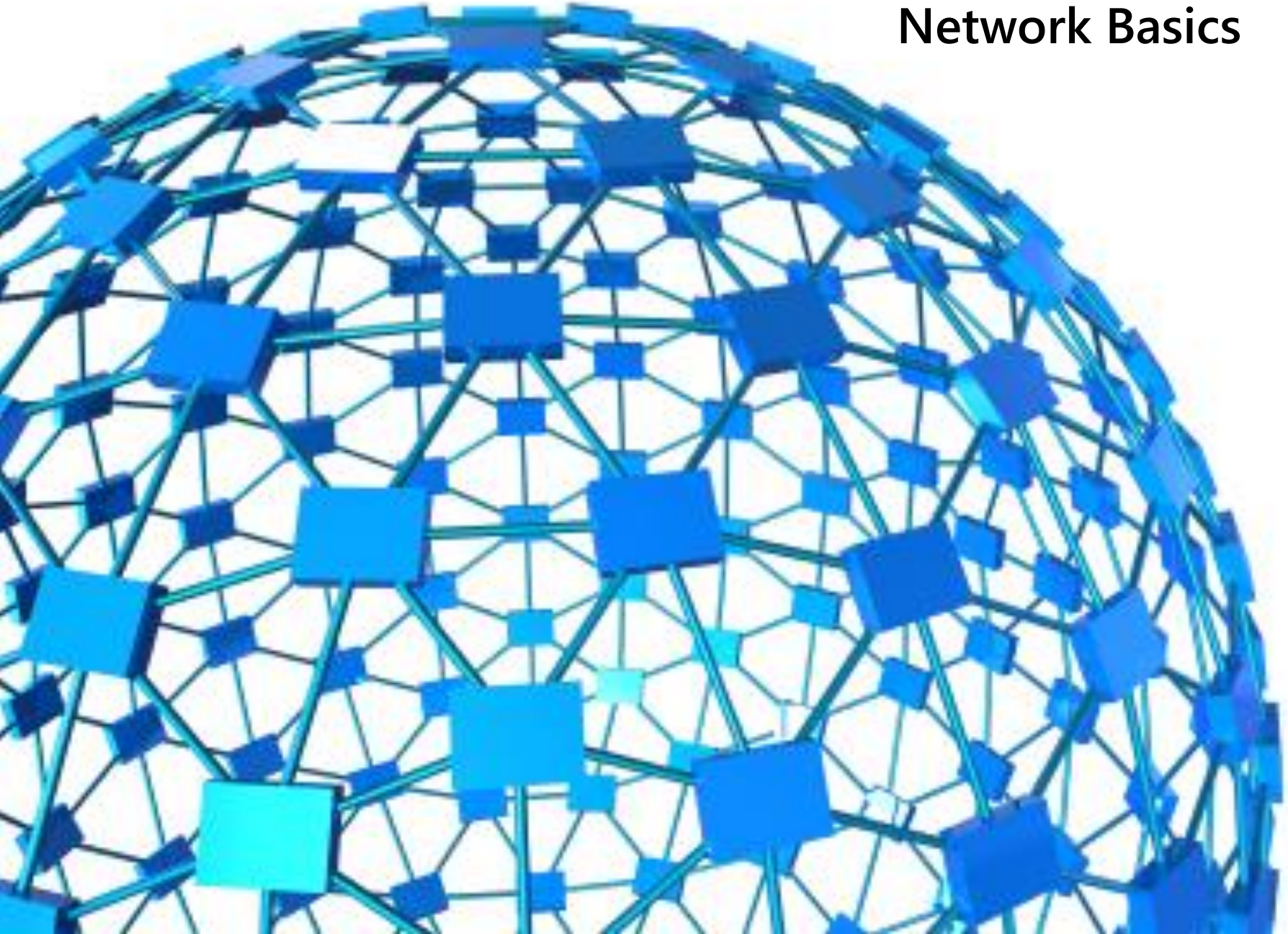
Module 1

Network Basics



Module Overview

- Intranet (Lan) / Extranet (WAN) / DMZ
- TCP/IP
- Domain Name System
- Dynamic Host Configuration Protocol

Lesson 1: Intranet (Lan) / Extranet (WAN) / DMZ

- Network Subnets
  - Classes
- Local Area Network
  - Privet Subnets
- Wide Area Network
- Demilitarized Zone

Network Subnets

Computers and devices that are participating in a network such as the Internet each have a logical address. Usually this address is unique to each device and can either be dynamically or statically configured. An address fulfills the functions of identifying the host and locating it on the network.

The most common network addressing scheme is Internet Protocol version 4 (IPv4), but its successor, IPv6 is in early deployment stages.
An IPv4 address consists of 32 bits. An IPv6 address consists of 128 bits.

In order to facilitate routing a data packet across multiple networks, the address is divided into two parts:

•Network prefix: A contiguous group of high-order bits that are common among all hosts within a network.

•Host identifier: The remaining low-order bits of the address that are not designated in the network prefix. This part specifies a particular device in the local network.
The network prefix may be written in a form identical to that of the address itself. In IPv4, this is called the subnet mask of the address. For example, to specify the most-significant 18 bits of an address, i.e. in binary, 11111111.11111111.11000000.00000000, one writes this as 255.255.192.0.

An alternate form of specification of the routing prefix, is to simply count the number of bits in the routing prefix and append that number to the address with a *slash* (/) separator:

•192.168.0.0, netmask 255.255.0.0
•192.168.0.0/16

Network Subnets

Classes

Class	Leading Bits	Size of *Network Number* Bit field	Size of *Rest* Bit field	Number of Networks	Addresses per Network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Local Area Connection

A **local area network** (**LAN**) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

Switched Ethernet is the most common Data Link Layer implementation on local area networks. At the Network Layer, the Internet Protocol has become the standard. However, many different options have been used in the history of LAN development and some continue to be popular in niche applications. Smaller LANs generally consist of one or more switches linked to each other—often at least one is connected to a router, cable modem, or ADSL modem for Internet access.

Larger LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic with VLANs. Larger LANS also contain a wide variety of network devices such as switches, firewalls, routers, load balancers, and sensors.

LANs may have connections with other LANs via leased lines, leased services, or by tunneling across the Internet using virtual private network technologies. Depending on how the connections are established and secured in a LAN, and the distance involved, a LAN may also be classified as metropolitan area network (MAN) or wide area networks (WAN).

Local Area Connection – Privet Subnets

IP address range	network/mask	number of address
10.0.0.0 - 10.255.255.255	10.0.0.0/8	16,777,216 (2^{24})
172.16.0.0 - 172.31.255.255	172.16.0.0/12	1,048,576 (2^{20})
192.168.0.0 - 192.168.255.255	192.168.0.0/16	65,536 (2^{16})

1.They can run TCP/IP without any danger of address conflicts with the outside.

2.They can allocate address space from the private address space in a manner which makes sense for them (perhaps geographically, maybe ogranizationally).

3.Their internal networks are (somewhat) shielded from Internet-based attacks. An attacker has more difficulties launching an attack against IP addresses which cannot be routed.

4.Their machines with private addresses cannot directly communicate with the Internet. This necessitates the use of a proxy or masquerading mechanism, which can help perform logging and prevent unauthorized access.

5.They do not have to go through the hassle of changing IP addresses should they change ISPs, nor do they have to apply for address space when they need more.

Wide Area Connection

A **wide area network** (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). This is in contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively.

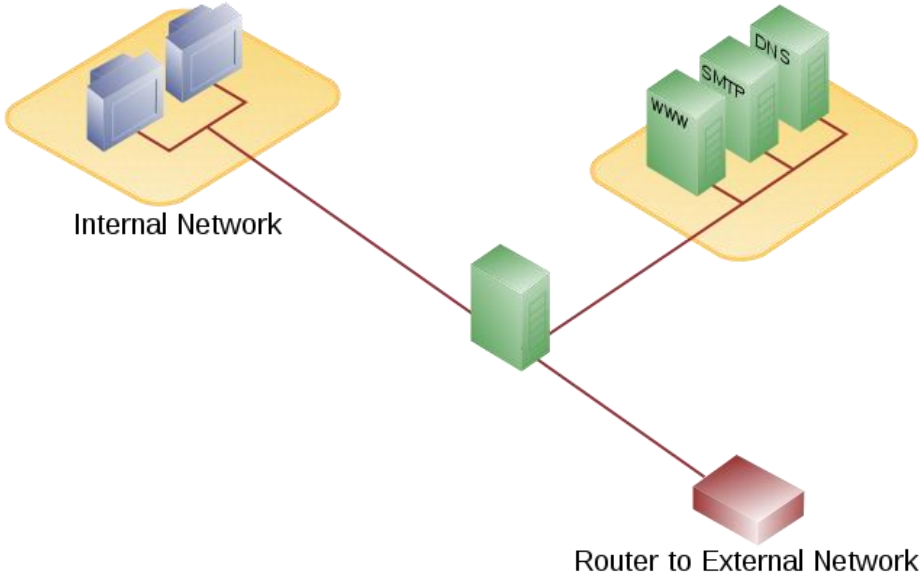
WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other.

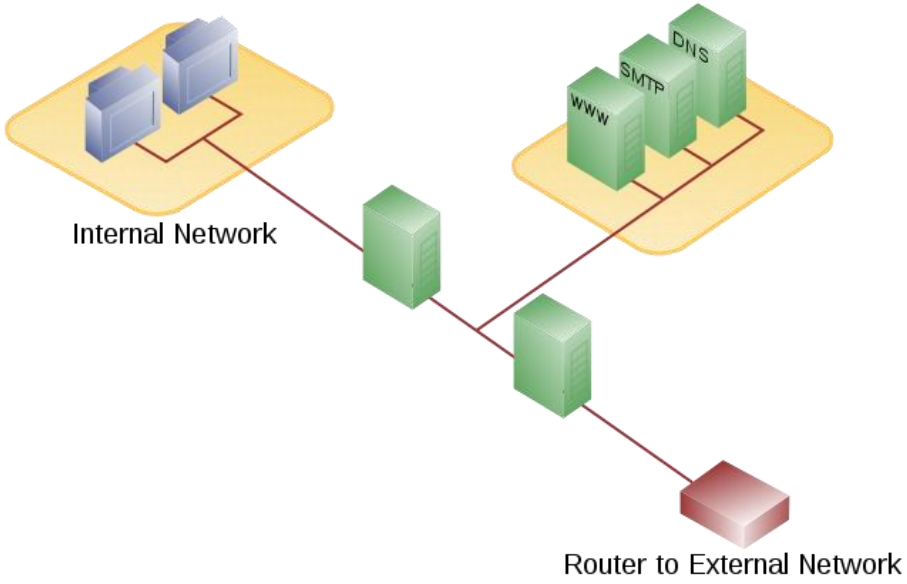
Demilitarized Zone

In computer security, a DMZ, or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network.

The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

Generally, any service that is being provided to users from an external network could be placed in the DMZ. The most common of these services are web servers, mail servers, ftp servers, VoIP servers and DNS servers. In some situations, additional steps need to be taken to be able to provide secure services.





Lesson 2: TCP/IP

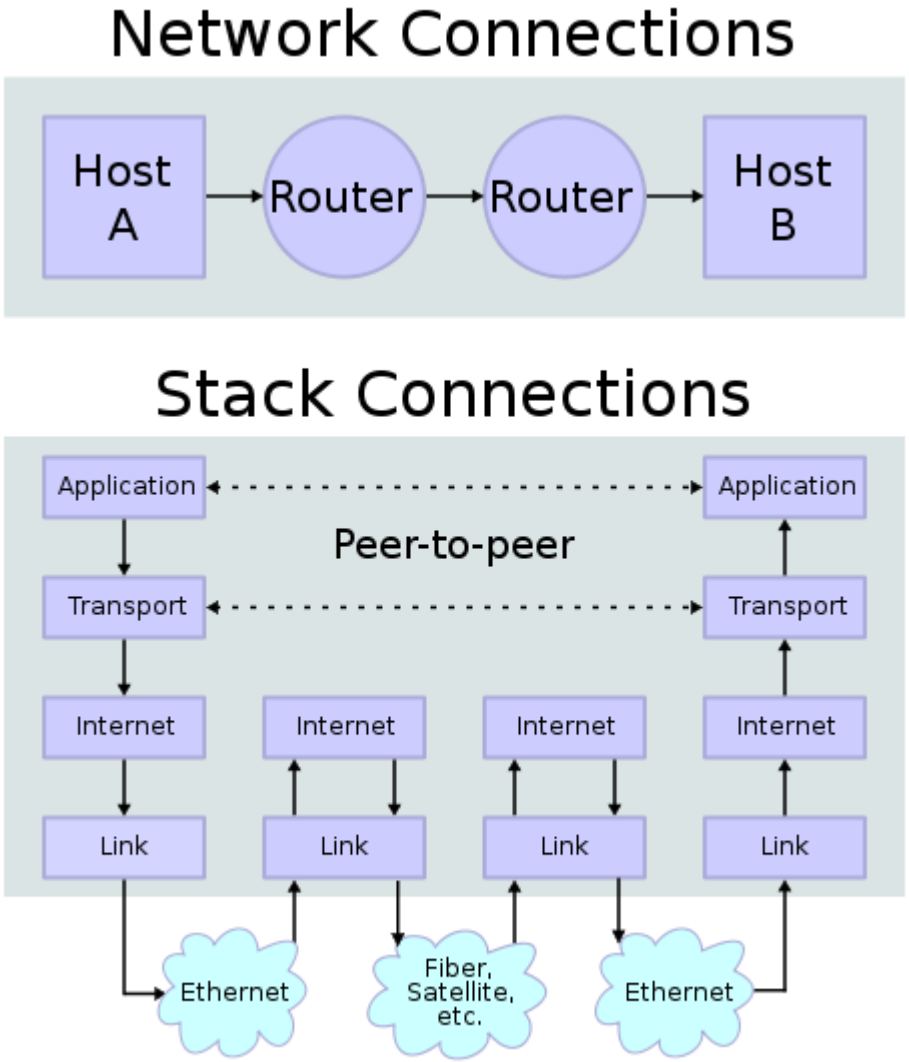
- What is the TCP/IP protocol ?
- The TCP/IP Layer Model
- The TCP/IP Frame
- Most Common Ports

What is the TCP/IP protocol ?

Transmission Control Protocol (TCP) and Internet Protocol (IP)

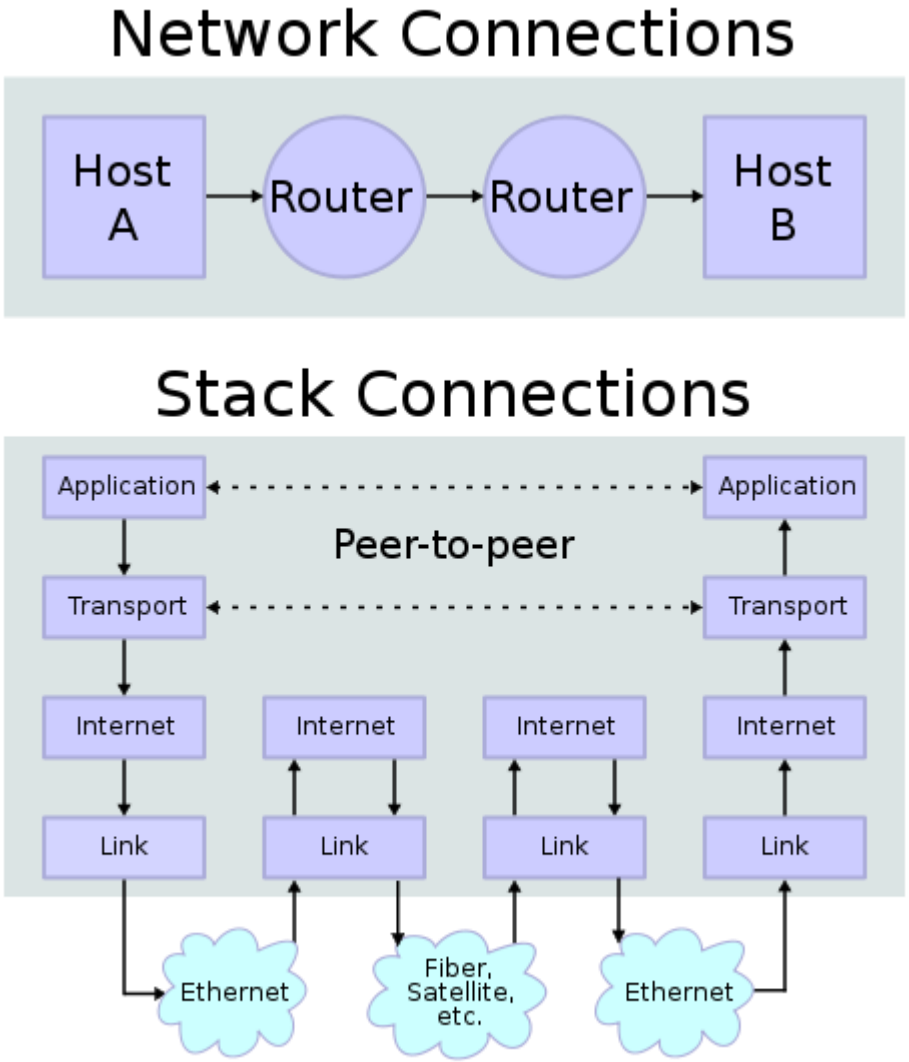
- TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the IP details.
- IP works by exchanging pieces of information called packets. A packet is a sequence of bytes and consists of a *header* followed by a *body*. The header describes the packet's destination and, optionally, the routers to use for forwarding until it arrives at its final destination. The body contains the data which IP is transmitting.

The TCP/IP Layer Model



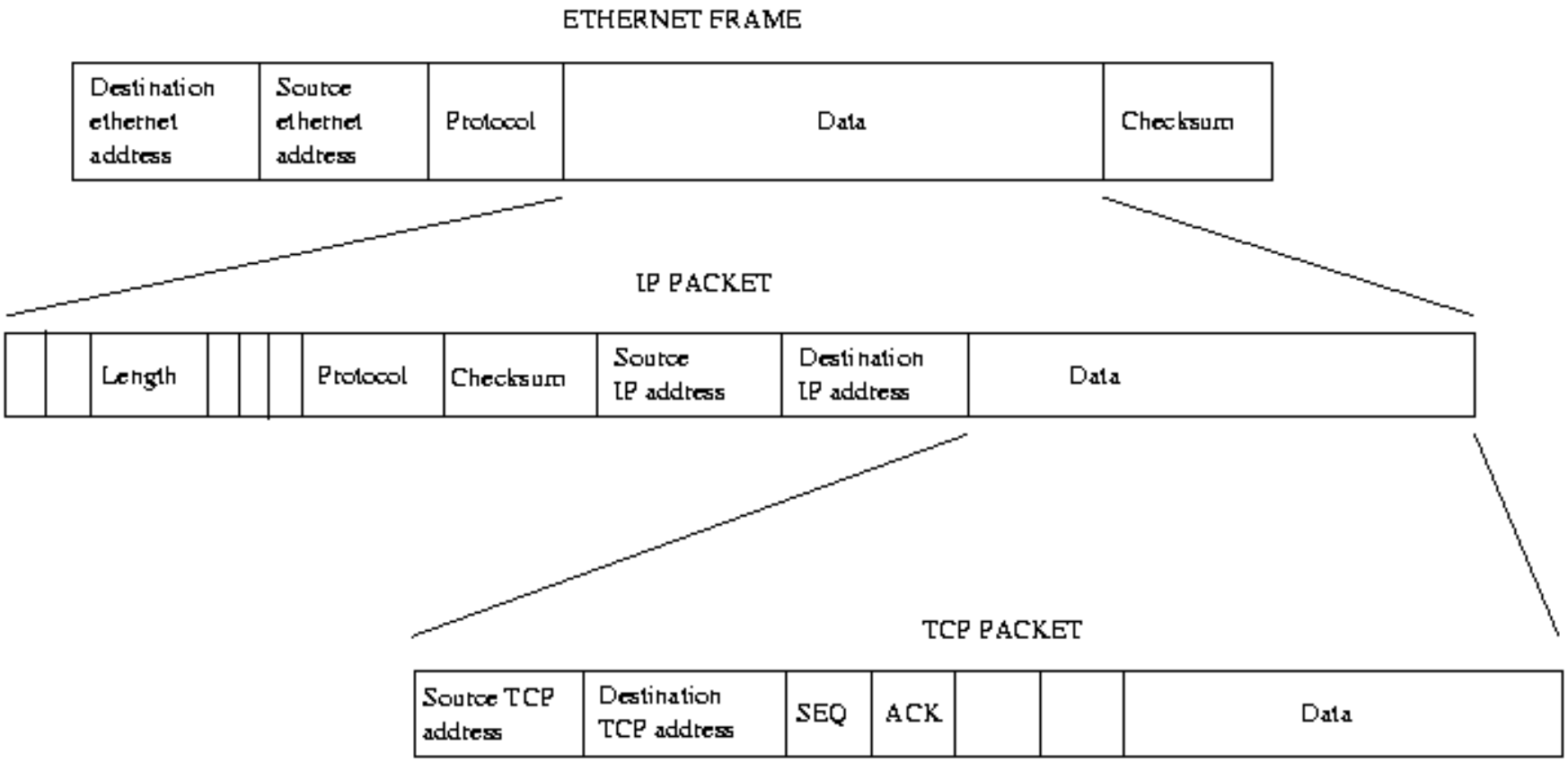
- **Application Layer**
- **Transport Layer**
- **Internet Layer**
- **Link Layer**

The TCP/IP Layer Model



- **Application Layer**
- **Transport Layer**
- **Internet Layer**
- **Link Layer**

The TCP/IP Frame



Most Common Ports

- **20/TCP** FTP – data
- **21/TCP** FTP – control (command)
- **22/TCP,UDP** Secure Shell (SSH)—used for secure logins, file transfers (scp, sftp) and port forwarding
- **25/TCP,UDP** Simple Mail Transfer Protocol (SMTP)—used for e-mail routing between mail servers
- **53/TCP,UDP** Domain Name System
- **67/UDP** Bootstrap Protocol (BOOTP) Server; also used by Dynamic Host Configuration Protocol (DHCP)
- **68/UDP** Bootstrap Protocol (BOOTP) Client; also used by Dynamic Host Configuration Protocol (DHCP)
- **80/TCP,UDP** Hypertext Transfer Protocol (HTTP)
- **443/TCP,UDP** Hypertext Transfer Protocol over TLS/SSL (HTTPS)
- **3389/TCP** Microsoft Terminal Server (RDP) officially registered as Windows Based Terminal (WBT)

Lesson 3: Domain Name System

- What is the DNS ?
- How DNS works ?
- DNS Record Types
- DNS Server Zones
- DNS Queries

What is the DNS ?

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.

It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.example.com translates to 208.77.188.166.

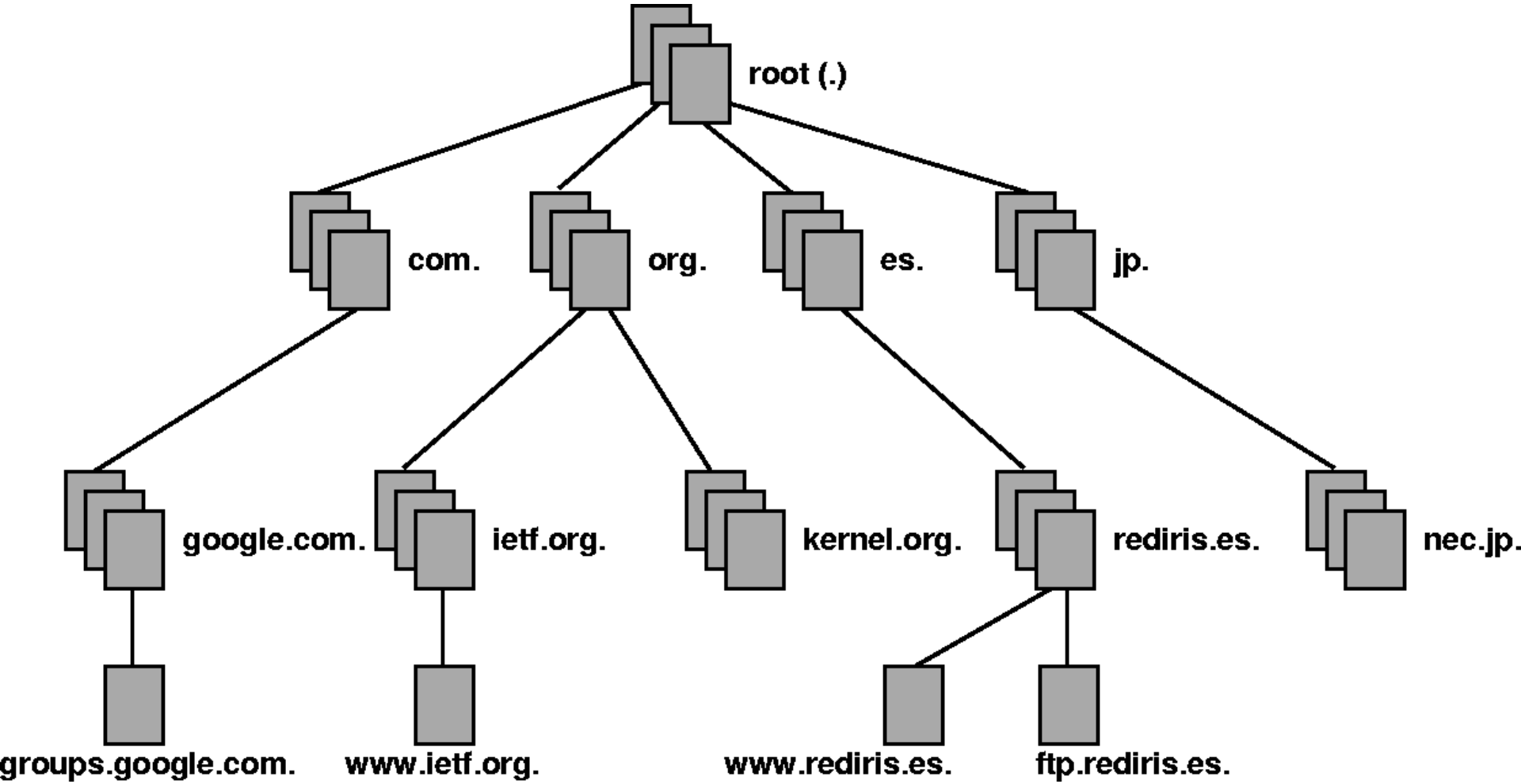
How DNS works ?

DNS Domain Names

The Domain Name System is implemented as a hierarchical and distributed database containing various types of data, including host names and domain names. The names in a DNS database form a hierarchical tree structure called the domain namespace. Domain names consist of individual labels separated by dots, for example: mydomain.microsoft.com.

A Fully Qualified Domain Name (FQDN) uniquely identifies the hosts position within the DNS hierarchical tree by specifying a list of names separated by dots in the path from the referenced host to the root. The next figure shows an example of a DNS tree with a host called mydomain within the microsoft.com. domain. The FQDN for the host would be mydomain.microsoft.com.

How DNS works ?



DNS Record Types

Description	Type	Data
Start of Authority	SOA	Owner Name Primary Name Server DNS Name, Serial Number Refresh Interval Retry Interval Expire Time Minimum TTL
Host	A	Owner Name (Host DNS Name) Host IP Address
Name Server	NS	Owner Name Name Server DNS Name
Mail Exchanger	MX	Owner Name Mail Exchange Server DNS Name, Preference Number
Canonical Name (an alias)	CNAME	Owner Name (Alias Name) Host DNS Name

DNS Server Zones

The three zones used by DNS servers

- Primary
- Secondary
- Stub

Primary is a zone to which all updates for the records that belong to that zone are made. A secondary zone is a read-only copy of the primary zone. A stub zone is a read-only copy of the primary zone that contains only the resource records that identify the DNS servers that are authoritative for a DNS domain name. Any changes made to the primary zone file are replicated to the secondary zone file. DNS servers hosting a primary, secondary or stub zone are said to be authoritative for the DNS names in the zone.

As mentioned above, a DNS server can host multiple zones. A DNS server can therefore host both a primary zone (which has the writeable copy of a zone file) and a separate secondary zone (which obtains a read-only copy of a zone file). A DNS server hosting a primary zone is said to be the primary DNS server for that zone, and a DNS server hosting a secondary zone is said to be the secondary DNS server for that zone.

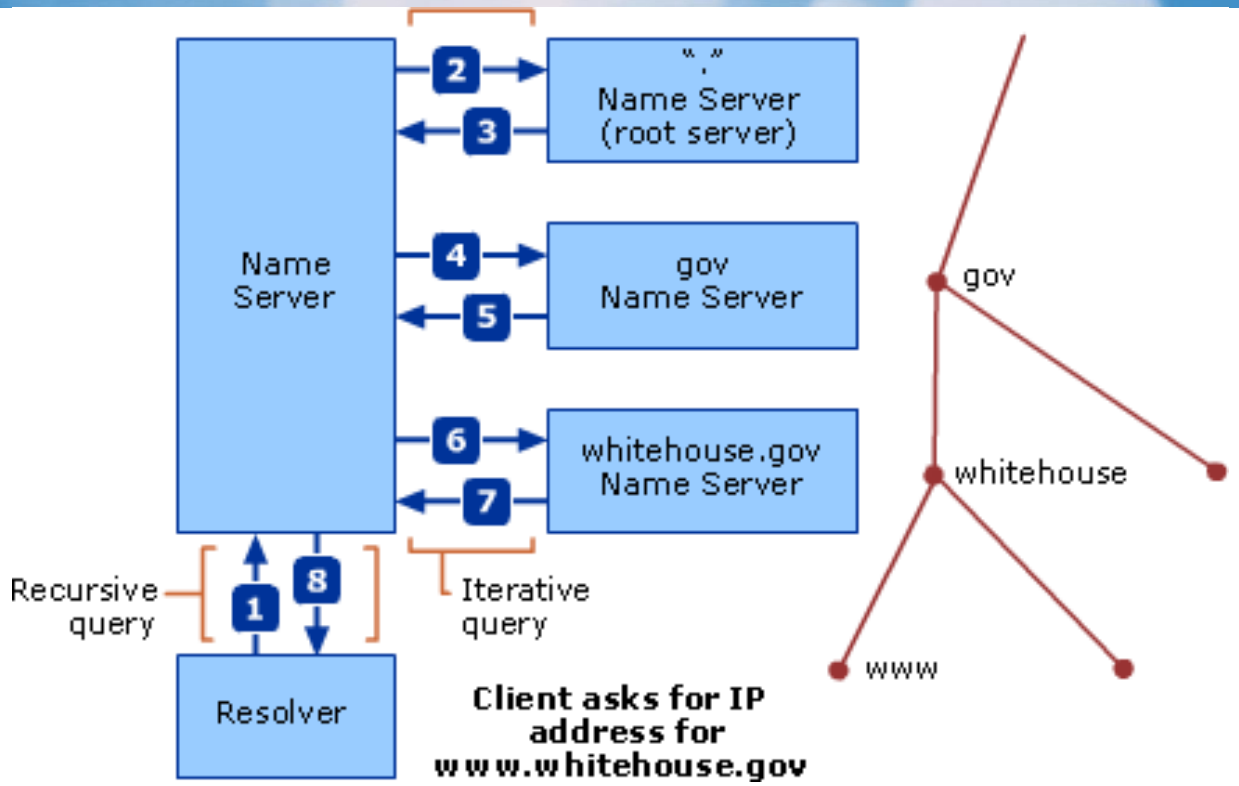
DNS Server Zones

Zone Transfer

The process of replicating a zone file to multiple DNS servers is called zone transfer.Zone transfer is achieved by copying the zone file from one DNS server to a second DNS server. Zone transfers can be made from both primary and secondary DNS servers.

A master DNS server is the source of the zone information during a transfer. The master DNS server can be a primary or secondary DNS server. If the master DNS server is a primary DNS server, then the zone transfer comes directly from the DNS server hosting the primary zone. If the master server is a secondary DNS server, then the zone file received from the master DNS server by means of a zone transfer is a copy of the read-only secondary zone file.

DNS Queries



DNS queries can be sent from a DNS client to a DNS server, or between two DNS servers.

There are two types of DNS queries that may be sent to a DNS server:

•Recursive

•Iterative

Lesson 4: Dynamic Host Configuration Protocol

- What is DHCP ?
- Why use DHCP ?
- DHCP Terms and Definitions
- How DHCP works ?

What is DHCP ?

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

The benefits of DHCP

Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

Reduced network administration. DHCP includes the following features to reduce network administration:

- Centralized and automated TCP/IP configuration.
- The ability to define TCP/IP configurations from a central location.
- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.
- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
- The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Why use DHCP ?

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another.
DHCP enables this entire process to be automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

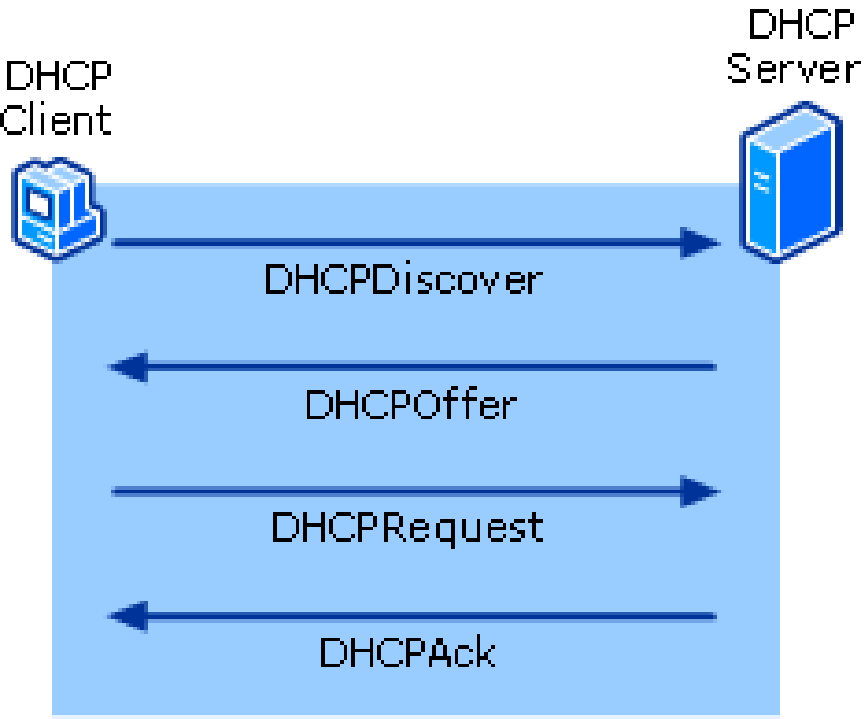
The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.
- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.
- A DHCP-enabled client, upon accepting a lease offer, receives:
  A valid IP address for the subnet to which it is connecting.
  Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients. Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name. For a full list of DHCP options, see "DHCP Tools and Settings."

DHCP Terms and Definitions

Term	Definition
Scope	A range of IP addresses that are available to be leased to DHCP clients by the DHCP Server service.
Lease	The length of time for which a DHCP client can use a DHCP-assigned IP address configuration.
Reservation	A specific IP address within a scope permanently set aside for leased use by a specific DHCP client. Client reservations are made in the DHCP database using the DHCP snap-in and are based on a unique client device identifier for each reserved entry.
Exclusion/exclusion range	One or more IP addresses within a DHCP scope that are not allocated by the DHCP Server service. Exclusions ensure that the specified IP addresses will not be offered to clients by the DHCP server as part of the general address pool.
DHCP relay agent	Either a host or an IP router that listens for DHCP client messages being broadcast on a subnet and then forwards those DHCP messages directly to a configured DHCP server. The DHCP server sends DHCP response messages directly back to the DHCP relay agent, which then forwards them to the DHCP client. The DHCP administrator uses DHCP relay agents to centralize DHCP servers, avoiding the need for a DHCP server on each subnet. Also referred to as a *BOOTP relay agent*.
Automatic Private IP Addressing (APIPA)	A TCP/IP feature in Windows XP and Windows Server 2003 that automatically configures a unique IP address from the range 169.254.0.1 through 169.254.255.254 with a subnet mask of 255.255.0.0 when the TCP/IP protocol is configured for automatic addressing, the **Automatic private IP address** alternate configuration setting is selected, and a DHCP server is not available. The APIPA range of IP addresses is reserved by the Internet Assigned Numbers Authority (IANA) for use on a single subnet, and IP addresses within this range are not used on the Internet.

How DHCP works ?



1.The DHCP client requests an IP address by broadcasting a DHCPDiscover message to the local subnet.

2.The client is offered an address when a DHCP server responds with a DHCPOffer message containing an IP address. If no DHCP server responds to the client request, the client sends DHCPDiscover messages at intervals of 0, 4, 8, 16, and 32 seconds. If there is no response from a DHCP server after one minute, the client can proceed in one of two ways:

- The client self-configures an IP address for its interface (APIPA).
- If the client does not support alternate configuration, such as APIPA, or if IP auto-configuration has been disabled, the client network initialization fails.

In both cases, the client begins a new cycle of DHCPDiscover messages in the background every five minutes, until it receives a DHCPOffer message from a DHCP server.

3.The client indicates acceptance of the offer by selecting the offered address and broadcasting a DHCPRequest message in response.

4.The client is assigned the address and the DHCP server broadcasts a DHCPAck message in response, finalizing the terms of the lease.

When the client receives acknowledgment, it configures its TCP/IP properties by using the DHCP option information in the reply, and completes its initialization of TCP/IP.

How DHCP works ?

- **Renewing a Lease**

The DHCP client first attempts to renew its lease when 50 percent of the original lease time, known as *T1*, has passed. At this point the DHCP client sends a unicast DHCPRequest message to the DHCP server that originally granted its lease. If the server is available, and the lease is still available, the server responds with a unicast DHCPAck message and the lease is renewed.

If the original DHCP server is available, but the client's current lease is no longer available, the DHCP server responds with a DHCPNack message, and the client immediately starts the process to obtain a new lease. This can happen if the client has changed subnets or if the DHCP server cannot fulfill the lease request for some other reason.

If there is no response from the DHCP server, the client waits until 87.5 percent of the lease time has passed (known as *T2*). At T2, the client enters the rebinding state, and broadcasts a DHCPRequest message to attempt to renew the lease from any available DHCP server. If no DHCP server is available by the time the lease expires, the client immediately unbinds itself from the existing lease and starts the process to obtain a new lease, beginning with a DHCPDiscover message.

How DHCP works ?