**Module 3.Introduction to TCP/IP**

**1. Beginner Question**

**1. Explain Internet Protocol (IP) and IP header**

**Internet Protocol (IP):**

The Internet Protocol (IP) is the method or [protocol](https://searchnetworking.techtarget.com/definition/protocol) by which [data](https://searchdatamanagement.techtarget.com/definition/data) is sent from one computer to another on the [Internet](https://searchwindevelopment.techtarget.com/definition/Internet). Each computer (known as a [host](https://searchnetworking.techtarget.com/definition/host)) on the Internet has at least one [IP address](https://searchwindevelopment.techtarget.com/definition/IP-address) that uniquely identifies it from all other computers on the Internet.

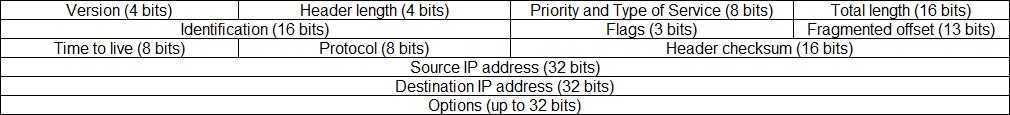
When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any [packet](https://searchnetworking.techtarget.com/definition/packet) is sent first to a [gateway](https://internetofthingsagenda.techtarget.com/definition/gateway) computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or [domain](https://whatis.techtarget.com/definition/domain). That gateway then forwards the packet directly to the computer whose address is specified. Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol ([TCP](https://searchnetworking.techtarget.com/definition/TCP)) to put them back in the right order.

IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection ([OSI](https://searchnetworking.techtarget.com/definition/OSI)) communication model, IP is in [layer 3](https://searchnetworking.techtarget.com/definition/Network-layer), the Networking Layer.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 ([IPv6](https://searchnetworking.techtarget.com/definition/IPv6-Internet-Protocol-Version-6)) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

**IP header:**

An IP header is a prefix to an IP packet that contains information about the IP version, length of the packet, source and destination IP addresses, etc. It consists of the following fields:

[](https://x9s4w2e2.stackpathcdn.com/wp-content/uploads/2016/03/ip_header.jpg)

Here is a description of each field:

* **Version** – the version of the IP protocol. For IPv4, this field has a value of 4.
* **Header length** – the length of the header in 32-bit words. The minimum value is 20 bytes, and the maximum value is 60 bytes.
* **Priority and Type of Service** – specifies how the datagram should be handled. The first 3 bits are the priority bits.
* **Total length** – the length of the entire packet (header + data). The minimum length is 20 bytes, and the maximum is 65,535 bytes.
* **Identification** – used to differentiate fragmented packets from different datagrams.
* **Flags** – used to control or identify fragments.
* **Fragmented offset** – used for fragmentation and reassembly if the packet is too large to put in a frame.
* **Time to live** – limits a datagram’s lifetime. If the packet doesn’t get to its destination before the TTL expires, it is discarded.
* **Protocol** – defines the protocol used in the data portion of the IP datagram. For example, TCP is represented by the number 6 and UDP by 17.
* **Header checksum** – used for error-checking of the header. If a packet arrives at a router and the router calculates a different checksum than the one specified in this field, the packet will be discarded.
* **Source IP address** – the IP address of the host that sent the packet.
* **Destination IP address** – the IP address of the host that should receive the packet.
* **Options** – used for network testing, debugging, security, and more. This field is usually empty.

**2. Define port number: Telnet FTP TFTP NFS SMTP POP IMAP4 TLS SIP (VoIP) RTP (VoIP) LPD X Window SNMP SSH HTTP HTTPS NTP NNTP**

|  |  |
| --- | --- |
| Protocols | Port Number |
| Telnet | 23 |
| FTP | 20,21 |
| TFTP | 69 |
| NFS | 111,**2049** |
| SMTP | 25 |
| POP | 110 |
| IMAP4 | 143 |
| TLS | **5061** |
| SIP (VoIP) | **5060 or 5061** |
| RTP (VoIP) | **1024 to 65535** |
| LPD | 515 |
| X Window | **6000** |
| SNMP | 143 |
| SSH | 1024 and 32,767 |
| HTTP | 80 |
| HTTPS | 443 |
| NTP | 123 |
| NNTP | 119 |

**3. Explain with one example of Host-to-Host layer protocols.**

**The Host-to-Host Layer Protocols**

The Host-to-Host layer’s main purpose is to shield the upper-layer applications from the complexities of the network. This layer says to the upper layer, “Just give me your data stream, with any instructions, and I’ll begin the process of getting your information ready to send.”The following sections describe the two protocols at this layer:

1. Transmission Control Protocol (TCP)
2. User Datagram Protocol (UDP)

**Transmission Control Protocol (TCP)**

The Transmission Control Protocol (TCP)takes large blocks of information from an application and breaks them into segments. It numbers and sequences each segment so that the destination’s TCP protocol can put the segments back into the order the application intended. After these segments are sent, TCP (on the transmitting host) waits for an acknowledgment of the receiving end’s TCP virtual circuit session, retransmitting those that aren’t acknowledged. Before a transmitting host starts to send segments down the model, the sender’s TCP protocol contacts the destination’s TCP protocol to establish a connection. What is created is known as a virtual circuit. This type of communication is called connection-oriented. During this initial handshake, the two TCP layers also agree on the amount of information that’s going to be sent before the recipient’s TCP sends back an acknowledgment. With everything agreed upon in advance, the path is paved for reliable communication to take place.

TCP is a full-duplex, connection-oriented, reliable, accurate protocol, and establishing all these terms and conditions, in addition to error checking, is no small task. TCP is very complicated and, not surprisingly, costly in terms of network overhead. Since today’s networks are much more reliable than those of yore, this added reliability is often unnecessary.

**2. Intermediate Question**

**1. Explain TCP/IP and the DoD Model**

**TCP/IP:**

TCP/IP (transmission control protocol/Internet protocol) is a set of rules governing communications among all computers on the Internet. More specifically, TCP/IP dictates how information should be packaged sent, and received, as well as how to get to its destination.

**How does TCP/IP work?**

As the name implies, TCP/IP is a combination of two separate protocols: [TCP](https://www.computerhope.com/jargon/t/tcp.htm) (transmission control protocol) and [IP](https://www.computerhope.com/jargon/i/ip.htm) (Internet protocol). The Internet Protocol standard dictates the logistics of packets sent out over networks; it tells packets where to go and how to get there. IP allows any computer on the Internet to forward a packet to another computer that's one or more intervals closer to the packet's recipient. You can think of it like workers in a line passing boulders from a quarry to a mining cart.

The Transmission Control Protocol is responsible for ensuring the reliable transmission of data across Internet-connected networks. TCP checks packets for errors and submits requests for re-transmissions if any are found.

Three of the most common TCP/IP protocols

* HTTP
* HTTPS
* FTP

**DoD model** is also known as the TCP/IP model due to the presence of the two most important protocols - TCP and IP. DoD model has 4 layers that resemble the 7 layers of the OSI model:-

1. **Network Access Layer** - This layer acts as an interface between the system and the network medium in use. The layer has different protocols which are used according to the physical network.
2. **Internet Layer** - The most basic protocol of the Internet, the IP protocol resides at this layer. This layer is responsible for transferring data across different physical networks.
3. **Host-to-Host Layer** - The host-to-host layer is responsible for flow control and error control, and handles process-to-process communication.
4. **Process Layer** - The top most layer of the DoD model is the process layer that interfaces directly with the end user. Protocols belonging to mail delivery, remote login, and file transfer reside at this layer.

**2. Explain with example of IP address, Subnet mask and Domain name**

**IP address**

Internet Protocol (IP) is a network layer, host-to-host delivery protocol. It means it delivers a packet from one host to the other with no knowledge about the ports within the host.

It is a connection-less protocol that makes it unreliable. Hence, it is often clubbed with TCP. TCP is a reliable protocol from the transport layer.

There are two versions of the IP address. These are [IPv4 and IPv6](https://www.csestack.org/difference-between-ipv4-and-ipv6-ip-address/).

**What is the IPv4 Address?**

An IP address uniquely identifies each host and router. This IP address is 32 bits long.One of the usual IP addresses that we see.

For example, 145.10.34.3.

This address is a 32-bit address represented within the system in binary form:  
10010001.00001010.00100010.00000011

An IP address format is usually divided into two parts:

* **Network ID:** To uniquely identify the network to which the host belongs.
* **Host ID:** To uniquely identify the host in a particular network.

**Subnet mask**

Subnet mask is a [mask](https://www.webopedia.com/TERM/M/mask.html) used to determine what [subnet](https://www.webopedia.com/TERM/S/subnet.html) an [IP address](https://www.webopedia.com/TERM/I/IP_address.html) belongs to. An IP address has two components, the network address and the [host](https://www.webopedia.com/TERM/H/host.html) address. For example, consider the IP address **150.215.017.009**. Assuming this is part of a Class B network, the first two numbers (**150.215**) represent the Class B network address, and the second two numbers (**017.009**) identify a particular host on this network.

Subnetting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. This is easier to see if we show the IP address in binary format.

**The full address is:**

10010110.11010111.00010001.00001001

**The Class B network part is:**

10010110.11010111

**The host address is:**

00010001.00001001

If this network is divided into 14 subnets, however, then the first 4 bits of the host address (0001) are reserved for identifying the subnet.

The subnet mask is the network address plus the bits reserved for identifying the subnetwork -- by convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address. In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a [*mask*](https://www.webopedia.com/TERM/M/mask.html) because it can be used to identify the subnet to which an IP address belongs by performing a [bitwise](https://www.webopedia.com/TERM/B/bitwise_operator.html) [AND operation](https://www.webopedia.com/TERM/A/AND_operator.html) on the mask and the IP address. The result is the subnetwork address:

|  |  |  |
| --- | --- | --- |
| Subnet Mask | 255.255.240.000 | 11111111.11111111.11110000.00000000 |
| IP Address | 150.215.017.009 | 10010110.11010111.00010001.00001001 |
| Subnet Address | 150.215.016.000 | 10010110.11010111.00010000.00000000 |

The subnet address, therefore, is 150.215.016.000.

**Domain name:**

Domain names are used to identify one or more [IP addresses](https://www.webopedia.com/TERM/I/IP_address.html). For example, the domain name microsoft.com represents about a dozen IP addresses. Domain names are used in [URLs](https://www.webopedia.com/TERM/U/URL.html) to identify particular [Web pages](https://www.webopedia.com/TERM/W/web_page.html). For example, in the URL http://www.pcwebopedia.com/index.html, the domain name is pcwebopedia.com.

Every domain name has a suffix that indicates which [top level domain (TLD)](https://www.webopedia.com/TERM/T/TLD.html) it belongs to. There are only a limited number of such domains. For example:

 **gov** - Government agencies

 **edu** - Educational institutions

 **org** - Organizations (nonprofit)

 **mil** - Military

 **com** - commercial business

 **net** - Network organizations

 **ca** - Canada

 **th** - Thailand

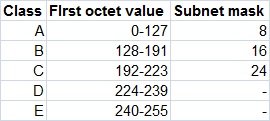
Because the Internet is based on IP addresses, not domain names, every [Web server](https://www.webopedia.com/TERM/W/Web_server.html) requires a [Domain Name System (DNS)](https://www.webopedia.com/TERM/D/DNS.html) server to translate domain names into IP addresses.

**3. Define the ClassA,B,C,D IP address range.**

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class E for experimental purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for the small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts.

Classes of IP addresses are:

[](https://study-ccna.com/wp-content/images/classes_of_ip_addresses.jpg)

For the IP addresses from Class A, the first 8 bits (the first decimal number) represent the network part, while the remaining 24 bits represent the host part. For Class B, the first 16 bits (the first two numbers) represent the network part, while the remaining 16 bits represent the host part. For Class C, the first 24 bits represent the network part, while the remaining 8 bits represent the host part.

**3. Advance question**

**1. Explain Application Layer Protocols**

Application Layer:-The application layer is present at the top of the OSI model. It is the layer through which users interact. It provides services to the user.

Application Layer protocol:-

1. TELNET: Telnet stands for the **TEL**ecomunications **NET**work. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

2. FTP: FTP stands for file transfer protocol. It is the protocol that actually lets us transfer files.It can facilitate this between any two machines using it. But FTP is not just a protocol but it is also a program.FTP promotes sharing of files via remote computers with reliable and efficient data transfer. Port number for FTP is 20 for data and 21 for control.

3. TFTP: The Trivial File Transfer Protocol (TFTP) is the stripped-down, stock version of FTP, but it’s the protocol of choice if you know exactly what you want and where to find it. It’s a technology for transferring files between network devices and is a simplified version of FTP

4. NFS: It stands for network file system. It allows remote hosts to mount file systems over a network and interact with those file systems as though they are mounted locally. This enables system administrators to consolidate resources onto centralized servers on the network.

5. SMTP: It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP protocol. Using a process called “store and forward,” SMTP moves your email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. Port number for SMTP is 25.

6. LPD: It stands for Line Printer Daemon. It is designed for printer sharing. It is the part that receives and processes the request. A “daemon” is a server or agent.

7. X window: It defines a protocol for the writing of graphical user interface–based client/server applications. The idea is to allow a program, called a client, to run on one computer. It is primarily used in networks of interconnected mainframes.

8. SNMP: It stands for Simple Network Management Protocol. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring  
them to disclose certain information. It is a way that servers can share information about their current state, and also a channel through which an administrate can modify pre-defined values. Port number of SNMP is 161(TCP) and 162(UDP).

9. DNS: It stands for Domain Name Service. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name [www.abc.com](http://www.abc.com) might translate to 198.105.232.4.  
Port number for DNS is 53.

#### 10. DHCP: It stands for Dynamic Host Configuration Protocol (DHCP).It gives IP addresses to hosts. There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. Port number for DHCP is 67, 68.

**2. Explain IGMP,LPR,DNS,APIPA**

**IGMP:**

Internet Group Management Protocol is a group management [protocol](https://ecomputernotes.com/computernetworkingnotes/computer-network/protocol) that mainly manages the group membership in a multicast network.

In a multicast network, multicast routers are used to route packets to all the computers that are having membership of a particular group.

The multicast routers use the [information](https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) from IGMP to determine which hosts are having membership of which group.

A multicast router generally receives thousands of multicast packets that have to be transmitted to various groups. If a router has no knowledge about the group membership, it will broadcast packet to every host and this will increase the load on the network.

In order to save the network from such a problem, a list of groups IS maintained when members of the group are present in the network.

Thus, IGMP helps the multicast router to create and update this list.

**DNS:**

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

**APIPA:**

**APIPA** is short for **A**utomatic **P**rivate **IP** **A**ddressing, a feature of Windows operating systems, meant for non-routed small business environments, usually less than 25 clients.

With APIPA, [DHCP](https://www.webopedia.com/TERM/D/DHCP_Server_Settings.html) clients can automatically self-configure an [IP address](https://www.webopedia.com/TERM/I/IP_address.html) and [subnet mask](https://www.webopedia.com/TERM/S/subnet_mask.html) when a DHCP server isn't available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask.

The APIPA service also checks regularly for the presence of a DHCP server. If it detects a DHCP server on the network, APIPA stops, and the DHCP server replaces the APIPA networking addresses with dynamically assigned addresses.

**3. Explain Default gateway (routers), DNS server address, WINS server address**

**Default gateway:**

A default gateway serves as an access point or IP router that a networked computer users to send information to a computer in another network or the internet. Default simply means that this gateway is used by default, unless an application specifies another gateway. The default server does not even need to be a router; it may be a computer with two network adapters, where one is connected to the local subnet and the other is connected to an outside network.

A default gateway allows computers on a network to communicate with computers on another network. Without it, the network is isolated from the outside. Basically, computers send data that is bound for other networks (one that does not belong to its local IP range) through the default gateway.

Network administrators configure the computer’s routing capability with an IP range's starting address as the default gateway and point all clients to that IP address.

**DNS server address:**

A [DNS](https://www.lifewire.com/what-is-dns-domain-name-system-2625855) server is a computer server that contains a database of [public IP addresses](https://www.lifewire.com/what-is-a-public-ip-address-2625974) and their associated [hostnames](https://www.lifewire.com/what-is-a-hostname-2625906), and in most cases serves to resolve, or translate, those names to [IP addresses](https://www.lifewire.com/what-is-an-ip-address-2625920) as requested. DNS servers run special software and communicate with each other using special protocols.

## The Purpose of DNS Servers:

It's easier to remember a domain or hostname like lifewire.com than it is to remember the site's IP address numbers 151.101.2.114. So when you access a website, like Lifewire, all you have to type is the [URL](https://www.lifewire.com/what-is-a-url-2626035) https://www.lifewire.com.

However, computers and network devices don't work well with domain names when trying to locate each other on the internet. It's far more efficient and precise to use an IP address, which is the numerical representation of what server in the network (internet) the website resides on.

**WINS server address:**

Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses.

If you do not already have WINS deployed on your network, do not deploy WINS - instead, deploy Domain Name System (DNS). DNS also provides computer name registration and resolution services, and includes many additional benefits over WINS, such as integration with Active Directory Domain Services.

**4. Explain the process of a client/server relationship using a DHCP connection**

DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network. A DHCP server provides this information to a DHCP client through the exchange of a series of messages, known as the DHCP conversation or the DHCP transaction.

### DHCP discovery:

The client computer broadcasts messages on the physical subnet to discover available DHCP servers. This client-computer creates a User Datagram Protocol (UDP) packet with the default broadcast destination of 255.255.255.255 or the specific subnet broadcast address if any configured.

### DHCP offer:

When a DHCP server receives an IP lease request from a client, it reserves an IP address for the client and extends an IP lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

### DHCP request:

In most companies, two DHCP servers provide fault tolerance of IP addressing if one server fails or must be taken offline for maintenance. So client could receive DHCP offers from multiple servers, but it will accept only one DHCP offer. In response to the offer Client requests the server. The client replies DHCP Request, unicast to the server, requesting the offered address. Based on the Transaction ID field in the request, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses. In some cases DHCP request message is broadcast, instead of being unicast to a particular DHCP server, because the DHCP client has still not received an IP address. Also, this way one message can let all other DHCP servers know that another server will be supplying the IP address without missing any of the servers with a series of unicast messages.

### DHCP acknowledgement:

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed.