IP (Internet Protocol)

The primary network communications protocol used on networks today is the IP (Internet Protocol). IP relays or transfers network packets, also known as datagrams, to destinations on local networks or across the public Internet. It defines the structures which encapsulate information as well as the legal addressing methods used to identify the source and destination network hosts or computing devices. When first introduced in 1974, IP was the datagram service included with the TCP (Transmission Control Program) protocol providing a connectionless service coupled with the connection-based TCP protocol. As a result, the standard is commonly referred to as TCP/IPvice solely IP.

What is the Purpose of the Internet Protocol?

IP is primarily responsible for providing legitimate network addresses and the encapsulation and routing of data packets across one or many IP-based networks. The primary functions of the protocol are providing identification of computer hosts and a straight-forward location service. The primary version of the protocol in use on the Internet today is IPv4, Internet Protocol Version 4. The succeeding protocol to IPv4 is IPv6 (Internet Protocol Version 6) that is slowly being adopted by industry after testing over Internet 2.

How Are IP Datagrams Constructed?

Every IP network packet or datagram has two sections: 1 – A datagram header, and 2 – The datagram payload. The header under the Internet Protocol construct includes the source address, destination, and meta-data that is required to properly route and deliver the information. The network “payload” is the information included in the datagram for transport. The concept of including or nesting data within the datagram including a packet header is referred to as encapsulation.

How Does IP Addressing and Routing Work?

IP addressing assigns addresses (IP addresses) to computer hosts and sub-networks of IP host addresses. All network hosts are capable of performing IP-based routing; however, network routers handle the majority of routing between individual networks (or between major network nodes on private networks). In order to tell if a datagram needs to be delivered locally or sent to another network, routers rely on the subnet of the address to determine the next destination for the information.

In legacy IPv4 addresses, the IP address is comprised of numbers separated by the "." symbol. The numbers must be between 0 and 255. For example, 202.11.71.68. These numbers are not assigned arbitrarily. Every local network based on Internet Protocol, will be assigned a sufficient block of addresses to support the size of the network. These addresses are then split into a network and host ID section. For example, the IP address of 202.11.71.XX signifies the network identification, while the final two digits signify the host which is connected to the network.

When new networks are first configured, the administrator is required to apply for a block of IP addresses to identify the network. Once obtained, these are allocated to the computers that connect to the network. The IP addresses can be split in a number of ways to provide both network and host ID's through the use of a subnet mask. The subnet uses a series of ones and zeros that indicate the bit in the IP address to use as the network ID. For example, a subnet mask of 255.0.0.0 (11111111.0.0.0) will indicate that the first eight bits of the address are the network

An IP address can be split in different ways to give a network ID and a host ID and this is usually indicated by a subnet mask. This is a pattern of ones and zeros that indicates which bit in the IP address is to be regarded as part of the network ID. For example a subnet mask of 11111111.0.0.0 or 255.0.0.0 in decimal means that the first eight bits of the IP address are the network ID and the rest identify particular machines on that network. By making use of the subnet mask, routers can determine if datagrams should be routed to the internal network or passed on to external routers for further routing.

Internet Protocol and Reliability

IP (Internet Protocol) makes an assumption that the supporting network infrastructure is unreliable at any single location on the local network or greater Internet. To remove the need for a central monitoring node, the rules or information required to forward and receive network traffic is contained at the ending nodes of the data path (end-end principle). The network routers that are located in between the two nodes use the rule sets to send data packets to the closest network gateway which most closely matches the routing prefix for the desired destination. As a result, network traffic that uses IP is considered a “Best Effort” delivery means and is characterized as being unreliable. For those who like more technical descriptions, IP is considered to be “connection-less.”

Due to the nature of IP, there are a number of errors that can exist on an IP-based network such as packet loss, data corruption, out-of-order packet delivery, and packet duplication. Due to the dynamic nature of packet routing in the IP scheme, some datagrams can take a longer path to arrive at the destination host than those sent afterwards. The IPv4 standard only provides error checking in the packet-header. If the checksum in the header is incorrect, the node will discard the packet without notifying the sending or receiving node. Higher-level (or layer) protocols are relied upon to correct or mitigate these issues in IPv4-based network. For example, caching information is used to ensure that datagrams are arranged in the correct order before providing the data to the desired program located at the application-layer on the computer host receiving the data transmission.

IP Header Format

```
IP Header Format

-----------------



0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|Version| IHL |Type of Service| Total Length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Identification |Flags| Fragment Offset |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Time to Live | Protocol | Header Checksum |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Source Address |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Destination Address |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Options | Padding |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Version: Version of the IP address being used by the network packet. Two available options are: IPv4 or IPv6.
Length: Length of the IP header of the datagram.
TOS: Used for quality of service in some networks (TOS= Type of Service). Allows network routers to prioritize delivery of predefined network packets.
Size of Datagram: Includes the length of the packet header and size of the datagram. Normally measured in bytes.
Identification: An exclusive value assigned to the packet.
Flags: Identifies if the packet should be fragmented or not. The default value is not to perform fragmentation.
Fragmentation Offset: Larger than the MTU. Represents a byte count that provides for segmentation and reassembly of large IP packets.
Time to Live: The total number of hops that the IP packet can be routed over. The value is decremented with each network hop made by the network packet.
Protocol: Represents the network protocol used by the packet. Examples include: Telnet = 23; FTP = 21; TCP=6; UDP= 17.
Header Checksum: Used to detect processing errors and to maintain data integrity in the datagram.
Source Address: IP address of the original sender that transmitted the IP packet.
Destination Address: IP address of the last destination of the packet (i.e. the intended recipient of the packet).
Options: The field is optional and has been used for testing and security purposes by some academics/vendors. When used, the IP header length will increase in size.
Data: The payload or information sent over the network.

What are the Types of IP Addresses?

The three primary types of IP addresses are Broadcast, Multicast, and Unicast. Each of the address types is designed for a specific purpose for use on an IP-based network.

Broadcast – Broadcast IP addresses send network information to all network hosts located on the identified subnet instead of an individual computer. The Broadcast address is further defined by RFC 919 and is used for mass communication to multiple computer hosts. The address is determined through using the bit complement of the subnet mask and then using an OR operation on the IP address.
Multicast – The Multicast IP address is used to send network data to one or many computer hosts that are part of multicast groups. The defined address ranges for multicast range from 224.0.0.0 to 239.255.255.255 and are popular for broadcast of multimedia, modeling and simulation, and network gaming.
Unicast – Unicast IP addresses are used to send data to specific network or computer devices on the destination network.
Other types of IP addresses include private (local IP addresses which cannot be routed over the public Internet) and public (unique IP addresses governed by the Internet Assigned Network Authority (IANA)).

What is the Difference in a Public and Private IP Address?

A public IP address is one that is (or can be) connected to the open Internet. The resulting addresses are then assigned to various international agencies such as the Asia-Pacific Network Information Center (APNIC) and ARIN (American Registry for Internet Numbers) to make allocations of IP address blocks to ISPs (Internet Service Providers) from the IANA. The ISPs then assign smaller address blocks to smaller organizations and ISPs for further assignment and use. In order to extend the finite IPv4 address space, ISPs will dynamically assign IP addresses to computers when they connect to the Internet through their service. Conversely, a static IP address can be assigned to organizations or end-users that require a dedicated address over a persistent timeframe.
If an IP address is not registered through the IANA, it is not visible on the public Internet. Once an address is assigned, the network administrator has to handle the

mechanics of assigning computer network host IDs to the network devices. To avoid depleting the pool of available IP addresses on a local network and increase security, most organizations leverage private IP addresses on the internal network.

The IANA has three blocks of IP addresses assigned for private address use detailed in RFC 1918:
10.0.0.0 to 10.25.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255
These address ranges are not visible on the public Internet and are commonly used on networks that support TCP/IP for both services and local computer hosts. Devices assigned as private IP address are still able to access services and websites on the public Internet using one of several methods which include leveraging a proxy or Network Address Translation (NAT) server.

How Are IP Addresses Assigned?

Networks that support TCP/IP can make address assignments via one of two methods: static or dynamic assignment. A static IP address assignment means that a given computer host or device will always have the same IP address whenever connecting to the local network. If the address is changed every time the device connects to the network it is dynamic. In a static configuration, the network administrator is required to manually make IP address assignments and is difficult to scale for large networks. If dynamic assignment is used, the network admin setups up the DHCP (Dynamic Host Configuration Protocol) to automatically assign the addresses on the network. Typically, static address assignments will be used for servers on an enterprise network while DHCP will be used to support client computing devices. DHCP was created and deployed in order to extend the useful life of the finite IPv4 32 bit address space (approximately 4,294,967,296 unique addresses). The IPv6 protocol uses a 128 bit wide address space and supports a much larger pool of IP addresses.

How Does Dynamic IP Address Assignment Work?

Most computer networks will configure one or many computers as a DHCP server. Network clients are then configured by administrator(s) to request an IP address assignment when connecting to the network from the DHCP server. All assignments made by the server are from the predetermined IP address range and are dynamic in nature (i.e. the same computer host will not necessarily receive the same IP address on subsequent connections to the network). Some of the methods used to manage the client IP address assignment include: Gateway addresses, DNS and WINS servers, Static IP Addresses, and TCP/IP configuration parameters. The static IP address assignment is used in DHCP for the DHCP server and for other important network nodes to include DNS servers and domain controllers. Automatic private IPaddressing (APIPA) can be used as an alternative to DHCP servers on smaller networks. This method is commonly used when a computer host is commonly used on more than one small network.

What is IPv6?

Internet Protocol version 6 is the most current version of IP (Internet Protocol) and was developed by the IETF (Internet Engineering Task Force). Although it has been in use for more than a decade, the majority of local and public Internet use continues to leverage IPv4 at the time of this writing. The protocol was created to address a number of the shortcomings inherent in IPv4 to include the finite address space. By using a 128 bit address space, IPv6 supports a much larger address space to the point that they are unlikely to run out if Internet and network use continues as we know it today. IPv6 addresses are displayed using eight groupings of four hexadecimal digits that are separated by colons. For example:

3ffe:1900:4545:3:200:f8ff:fe21:67cf

In the IPv6 construct, leading zeros can be omitted in each field (for example :0003 can be expressed as :3). Additionally, two colons in a row, ::, can be used to replace multiple zero fields.

Although adoption of IPv6 has seen acceleration over the past several years, both industry and consumers continue to slowly adopt the technology. The primary barrier to adoption continues to be cost of new equipment (at both the ISP and end-user level) and the fact that IPv4 continues to function satisfactorily.

Source: http://www.tech-faq.com/ip.html