# Chapter 10

Introduction to IP (Internet Protocol)

OSI Model provides a guideline that companies use when designing network devices and protocols.

OSI Model has 7 layers

The OSI model does not define specific applications or protocols, it simply provides a guide or framework that is used in design.

|  |  |  |
| --- | --- | --- |
| **Layer** | **Name** | **Function** |
| 7 | Application | Determine if enough resources exist for the application |
| 6 | Presentation | Translator for Application Layer. Data Encryption, Compression, etc. |
| 5 | Session | Dialog Control (duplex), Connection Establishment, Data Transfer, Connection Release |
| 4 | Transport | End-to-end communication. Allows for multiple applications on the wire. Segments and reassembles data. Defines reliable and unreliable communication |
| 3 | Network | Path determination determines network locations and manages network addresses. |
| 2 | Data Link | Responsible for physical addresses (MAC addressing). Framing of data, converting frames to 1s and 0s. Network topology. |
| 1 | Physical | Provides physical and electrical specifications of the media. |

Layers communicate in a peer-to-peer fashion. For example: The Network layer of Host A communicates with the Network layer of Host B.

|  |  |  |
| --- | --- | --- |
| Host A |  | Host B |
| Application | < > | Application |
| Presentation | < > | Presentation |
| Session | < > | Session |
| Transport | < > | Transport |
| Network | < > | Network |
| Data-Link | < > | Data-Link |
| Physical | < > | Physical |

# DOD Reference Model

Created in the 1970s before OSI model.

The DOD model has 4 Layers v.s. the 7 layers of the OSI model

* Application
* Host-to-Host
* Internet
* Network Access

|  |  |
| --- | --- |
| **OSI** | **DOD** |
| Application  Presentation Session | Application |
| Transport | Host-to-Host |
| Network | Internet |
| Data-Link  ---------  Physical | Network access> |

|  |  |  |
| --- | --- | --- |
| **OSI** | **DOD** | **Applications** |
| Application  -----------  Presentation  Session | Application | FTP, TFTP, Telent, NFS, SMTP, DNS, SNMP,  rlogin |
| Transport | Host-to-Host | TCP, UDP |
| Network | Internet | Bootp, ICMP, ARP, RARP |
| Data-Link  ---------  Physical | Network access | Ethernet, Fast Ethernet, FDDI, Token Ring |

# TCP/IP Applications

Telnet - Terminal Emulation

* Allows a user to access a remote host as if his teminal was directly connected to the host.
* Cannot be used for file sharing, such as file transfers.
* Can be used to run applications.

Syntax: telnet < ip address> ftp - File Transfer Protocol

* Used for file transfer.
* Cannot execute programs
* Both a protocol and a program. As a program it is interactive with the user. As a protocol, other programs use ftp to transfer files.
* Reliable protocol

tftp - Trivial file transfer protocol

* Used for file transfer.
* Cannot execute programs
* Uses the UDP protocol
* This is considered an unreliable protocol.

An unreliable protocol is not necessarily bad. Unreliable, as protocols go, means that the protocol does not verify that the transmission that has taken place is good. This protocol assumes that an upper layer protocol will verify the data transfer.

# Binary To Decimal Conversion

In order to fully understand TCP/IP addressing you must understand Binary to Decimal conversion.

As we all know, computers use binary numbers for storage, communications, and other tasks, but, we use decimal numbers. So we have to know how to go between the two number systems.

For the purposes of this document, we will only do a conversion of eight bits.

For TCP/IP addressing we are concerned only with 8 bits because a TCP/IP address is composed of four groups of eight bits. The right most bit (least significant) is a 0 or 1 and converts to a 0 or 1 for decimal. Going right each bit doubles in possible value.

128 64 32 16 8 4 2 1

Using the above, we can convert from decimal to binary and back very quickly. For example, convert 195 to binary.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |

our binary number is: 11000011 Convert 10110110 to decimal.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |

128+32+16+4+2 = 182

Convert 255 to binary

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

255 is converted to 11111111 Convert 11000000 to decimal.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

128+64 = 192

# TCP/IP Addressing

A TCP/IP address is 32 bits long, divided into four octets. A dot (.) is used to separate each octet.

An octet can range from a value of 0 to 255. There are 5 classes of TCP/IP addresses.

* Class A
* Class B
* Class C
* Class D
* Class E

The type of address that is used is determined by the first five bits of the first octet.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Class A | 0 | \* | \* | \* | \* \* \* \* |
| Class B | 1 | 0 | \* | \* | \* \* \* \* |
| Class C | 1 | 1 | 0 | \* | \* \* \* \* |
| Class D | 1 | 1 | 1 | 0 | \* \* \* \* |
| Class E | 1 | 1 | 1 | 1 | \* \* \* \* |

The breakdown of the addresses are: Class A

* 1 to 126
* 16,777,214 host addresses Class B
* 128 to 191
* 65,534 host addresses Class C
* 192 to 223
* 254 host addresses Class D
* 224 to 239 Class E
* 240 to 255

Class A, Class B, and Class C addresses are used for hosts on a network. *Class D is reserved for multicast, and Class E is reserved for research.*

Along with the class of address numbers the octets are also broken down into network and host portions. The network number is given by the network administrator. The host portion can be assigned by a DHCP server or entered by a technician or administrator.

The network and host portion breakdown is:

Class A: N.H.H.H Class B: N.N.H.H

Class C: N.N.N.H

N is the network. H is the host.

The Internet Assigned Numbers Authority (IANA) is responsible for allocation of all registered TCP/IP addresses. (องค์การจัดการ IP)

RFC (3330) Special-Use IPv4 Addresses

|  |  |  |
| --- | --- | --- |
| Reserved address blocks | | |
| [**CIDR**](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) **address block** | **Description** | **Reference** |
| 0.0.0.0/8 | Current network (only valid as source address) | [RFC 1700](http://tools.ietf.org/html/rfc1700) |
| 10.0.0.0/8 | [Private network](http://en.wikipedia.org/wiki/Private_network) | [RFC 1918](http://tools.ietf.org/html/rfc1918) |
| 14.0.0.0/8 | Public data networks (per 2008-02-10, available  for use) | [RFC 1700](http://tools.ietf.org/html/rfc1700) |
| 127.0.0.0/8 | [Loopback](http://en.wikipedia.org/wiki/Localhost) | [RFC 3330](http://tools.ietf.org/html/rfc3330) |
| 128.0.0.0/16 | Reserved (IANA) | [RFC 3330](http://tools.ietf.org/html/rfc3330) |
| 169.254.0.0/16 | [Link-Local](http://en.wikipedia.org/wiki/Zeroconf) | [RFC 3927](http://tools.ietf.org/html/rfc3927) |
| 172.16.0.0/12 | [Private network](http://en.wikipedia.org/wiki/Private_network) | [RFC 1918](http://tools.ietf.org/html/rfc1918) |
| 191.255.0.0/16 | Reserved (IANA) | [RFC 3330](http://tools.ietf.org/html/rfc3330) |
| 192.0.0.0/24 | Reserved (IANA) | [RFC 3330](http://tools.ietf.org/html/rfc3330) |
| 192.0.2.0/24 | Documentation and example code | [RFC 3330](http://tools.ietf.org/html/rfc3330) |
| 192.88.99.0/24 | [IPv6](http://en.wikipedia.org/wiki/IPv6) to IPv4 relay | [RFC 3068](http://tools.ietf.org/html/rfc3068) |
| 192.168.0.0/16 | [Private network](http://en.wikipedia.org/wiki/Private_network) | [RFC 1918](http://tools.ietf.org/html/rfc1918) |
| 198.18.0.0/15 | Network benchmark tests | [RFC 2544](http://tools.ietf.org/html/rfc2544) |
| 223.255.255.0/24 | Reserved (IANA) | [RFC 3330](http://tools.ietf.org/html/rfc3330) |
| 224.0.0.0/4 | [Multicasts](http://en.wikipedia.org/wiki/Multicast) (former Class D network) | [RFC 3171](http://tools.ietf.org/html/rfc3171) |
| 240.0.0.0/4 | Reserved (former Class E network) | [RFC 1700](http://tools.ietf.org/html/rfc1700) |
| 255.255.255.255 | Broadcast |  |

***The following are the four ranges reserved for private networks:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Address range** | **Number of addresses** | [***Classful***](http://en.wikipedia.org/wiki/Classful_network)  **description** | **Largest** [**CIDR**](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) **block** |
| 24-bit  block | 10.0.0.0–  10.255.255.255 | 16,777,216 | Single Class A | 10.0.0.0/8 |
| 20-bit  block | 172.16.0.0–  172.31.255.255 | 1,048,576 | 16 contiguous  Class Bs | 172.16.0.0/12 |
| 16-bit  block | 169.254.0.0–  169.254.255.255 | 65,536 | 256 contiguous  Class Cs | 169.254.0.0/16 |
| 16-bit  block | 192.168.0.0–  192.168.255.255 | 65,536 | 256 contiguous  Class Cs | 192.168.0.0/16 |

## Localhost

In addition to private networking, the address range 127.0.0.0–127.255.255.255 (or *127.0.0.0/8* in [CIDR](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) notation) is reserved for [localhost](http://en.wikipedia.org/wiki/Localhost) communication. Any address within this range should never appear on an actual network and any packet sent to this address does not leave the source computer, and will appear as an incoming packet on that computer (known as [loopback](http://en.wikipedia.org/wiki/Loopback))

## Addresses ending in 0 or 255

It is a common misconception that addresses ending in 255 or 0 can never be assigned to hosts, but this is only true of networks with subnet masks of at least 24 bits — Class C networks *in the old classful addressing scheme*, or in CIDR, networks with masks of */24* to */32* (or 255.255.255.0–255.255.255.255).

In classful addressing (now obsolete with the advent of [CIDR](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing)), there are only three possible subnet masks: Class A, 255.0.0.0 or /8; Class B, 255.255.0.0 or /16; and Class C, 255.255.255.0 or /24. For example, in the subnet 192.168.5.0/255.255.255.0 (or 192.168.5.0/24) the identifier 192.168.5.0 refers to the entire subnet, so it cannot also refer to an individual device in that subnet.

A [broadcast address](http://en.wikipedia.org/wiki/Broadcast_address) is an address that allows information to be sent to all machines on a given subnet rather than a specific machine. Generally, the broadcast address is found by taking the bit complement of the subnet mask and then OR-ing it bitwise with the network identifier. More simply, the broadcast address is the last address in the range belonging to the subnet. In our example, the broadcast address would be 192.168.5.255, so to avoid confusion this address also cannot be assigned to a host. On a Class-A, -B, or -C subnet, the broadcast address would always end in 255.

However, this does not mean that every addresses ending in 255 cannot be used as a host address. For example, in the case of a Class B subnet 192.168.0.0/255.255.0.0 (or 192.168.0.0/16), equivalent to the address range 192.168.0.0–192.168.255.255, the broadcast address is 192.168.255.255. However, one can assign 192.168.1.255, 192.168.2.255, etc. (though this can cause confusion). Also, 192.168.0.0 is the network identifier and so cannot be assigned, but 192.168.1.0, 192.168.2.0, etc. can be assigned (though this can also cause confusion).

With the advent of CIDR, broadcast addresses do not necessarily end with 255.

In general, the first and last addresses in a subnet are used as the network identifier and broadcast address, respectively. All other addresses in the subnet can be assigned to hosts on that subnet.

# Subnets and Subnet Masking

Along with the address portion in a TCP/IP address a subnet mask is assigned the default subnet mask for Class A, B, and C addresses are:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Like the TCP/IP address a subnet mask consists of four octets separated by periods. A subnet mask is used to separate network bits from host bits.

A subnet is used for the following reasons:

* Conserve valuable IP addresses
* Allow the creation of multiple networks given a limited number of IP addresses.
* Reduces network congestion by limiting the broadcast domain of the network.
* Isolate network problems.

One of the most common reasons for using subnets is the conservation of IP addresses. For example, a company may install a T-1 line between two sites. The only devices that are on this line are the two routers. Without a subnet the company would have to use a full Class C TCP/IP address. Using a Class C address with a subnet mask of 252, the company saves about 130 addresses.

Subnet addresses are simply a series of 1s added the default address (0s cannot be mixed in with the 1s in a subnet mask). This position in the mask creates additional subnets, and reduces the number of hosts (see the table)

|  |  |  |  |
| --- | --- | --- | --- |
| **Class C Subnet Reference Chart** | | | |
| **Bits** | **Subnet Mask** | **No. of Subnets** | **No. of Hosts** |
| 1i | 255.255.255.128 | 0/2 | 126 |
| 2 | 255.255.255.192 | 2/4 | 62 |
| 3 | 255.255.255.224 | 6/8 | 30 |
| 4 | 255.255.255.240 | 14/16 | 14 |
| 5 | 255.255.255.248 | 30/32 | 6 |

To see how a subnet mask works, look at the following example.

IP host address: 201.164.204.114 (11001001.10100100.11001100.1110010)

Subnet mask: 255.255.255.240 (11111111.11111111.11111111.11110000)

The actual subnet address is calculated by using the logical AND on both the host address and the mask for the length of the subnet mask. The host address is taken from the resulting bits in the host portion. This gives the following result:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 10100100. | 11001100. | 0111 | 0010 |
| 11111111. | 11111111. | 11111111. | 1111 | 0000 |
| 11001001. | 10100100. | 11001100. | 0111 | 0010 |
| 201 | 164 | 204 | 7 | 2 |

Please remember that a host cannot contain all 1s or all 0s. A host address with all 1s is the subnet broadcast address and the host address with all 0s is the actual network number. Also, a subnet with all 0s and all 1s is illegal. Using the above example. The address 201.164.204.112 is the network (or wire) address and the address 201.164.204.127 is the subnet broadcast address.

Continuing with the example involving a T-1 line, if the company has the address 199.168.142.0 and would like to subnet the address to support only two devices, therefore, saving address in this space, the subnet mask of 252 should be used. If the company takes the first subnet address space in this network for this use, it gets the following:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11000111. | 10101000. | 10001110. | 000001 | 00 |
| 11111111. | 11111111. | 11111111. | 111111 | 00 |
| 11000111. | 10101000. | 10001110. | 000001 | 00 |
| 199 | 168 | 142 | 1 | 0 |

The address 199.168.142.4 is the first network number that our company can use. Its two host addresses (one for each router ) are:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11000111. | 10101000. | 10001110. | 000001 | 01 |
| 11111111. | 11111111. | 11111111. | 111111 | 00 |
| 11000111. | 10101000. | 10001110. | 000001 | 01 |
| 199 | 168 | 142 | 1 | 1 |

First host address: 199.168.142.5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11000111. | 10101000. | 10001110. | 000001 | 10 |
| 11111111. | 11111111. | 11111111. | 111111 | 00 |
| 11000111. | 10101000. | 10001110. | 000001 | 10 |
| 199 | 168 | 142 | 1 | 2 |

Last host address: 199.168.142.6

The two host addresses for this subnet are 199.168.142.5 and 199.168.142.6. The broadcast address is 199.168.142.7.

Another example would be for a company that has two remote sites with only 20 devices installed at each site. This growth for these sites is very limited and will not exceed a total of 25 devices each. First, from the Class C subnet reference chart, a subnet mask of 255.255.255.224 is needed. This subnet mask will support 30 hosts and 6 subnets, which meets the needs of these offices. Using the Class C address of 201.241.144.0 and the subnet mask of 255.255.255.224 calculate the first and second subnets that can be used.

Then list the hosts and broadcast addresses of each subnet. Office number 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 11110001. | 10010000. | 001\* | 00000 |
| 11111111. | 11111111. | 11111111. | 111 | 00000 |
| 11001001. | 11110001. | 10010000. | 001 | 00000 |
| 201 | 241 | 144 | 1 | 0 |

Subnet number one is 201.241.144.32

\* subnet 001 is chosen because a subnet cannot contain all 0s or all 1s.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 11110001. | 10010000. | 001\* | 00001 |
| 11111111. | 11111111. | 11111111. | 111 | 00000 |
| 11001001. | 11110001. | 10010000. | 001 | 00001 |
| 201 | 241 | 144 | 1 | 1 |

First host of subnet one is 201.241.144.33

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 11110001. | 10010000. | 001\* | 11110 |
| 11111111. | 11111111. | 11111111. | 111 | 00000 |
| 11001001. | 11110001. | 10010000. | 001 | 11110 |
| 201 | 241 | 144 | 1 | 30 |

Last host of subnet one is 201.241.144.62 Broadcast address of subnet one is 201.241.144.63

Office number 2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 11110001. | 10010000. | 010 | 00000 |
| 11111111. | 11111111. | 11111111. | 111 | 00000 |
| 11001001. | 11110001. | 10010000. | 010 | 00000 |
| 201 | 241 | 144 | 2 | 0 |

Subnet number two is 201.241.144.64

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 11110001. | 10010000. | 010 | 00001 |
| 11111111. | 11111111. | 11111111. | 111 | 00000 |
| 11001001. | 11110001. | 10010000. | 010 | 00001 |
| 201 | 241 | 144 | 2 | 1 |

First host of subnet two is 201.241.144.65

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Network |  | Subnet | Host |
| 11001001. | 11110001. | 10010000. | 010 | 11110 |
| 11111111. | 11111111. | 11111111. | 111 | 00000 |
| 11001001. | 11110001. | 10010000. | 010 | 11110 |
| 201 | 241 | 144 | 1 | 30 |

Last host of subnet two is 201.241.144.94

The broadcast address of subnet two is 201.241.144.95.

Private Address Spaces

With the explosion of the internet, address space became a very scarce resource. To combat the problem a new TCP/IP addressing scheme was proposed. This new addressing scheme is called IP version 6. However, it could be many years before this new addressing scheme would be ratified and implemented. To help fix the problem in the short term a series of addresses were designated as private address space. These addresses are not routed on the internet. These can only be routed on a companies internal network. A special computer (usually a firewall) can run either the Network Address Translation Protocol or Port Address Translation Protocol. These two protocols will translate from the private addresses to public addresses.

The following addresses are considered private address space: Class A: 10.0.0.0 to 10.255.255.255

Class B: 172.16.0.0 to 172.32.255.255

Class C: 192.168.0.0 to 192.168.255.255.

A firewall running Network Address Translation performs a one-to-one translation of a private address to a public address. Port Address Translation converts all outgoing requests to a single IP address. It differentiates between each session by assigning a different port to each individual session.

For more information on Private Address Space see RFC 1918 IP addresses for inside and perimeter addresses.

TCP/IP addresses reserved for 'private' networks are:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

and as of July 2001

169.254.0.0 to 169.254.255.255 [rfc](http://search.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-04.txt)

These are invalid addresses on the internet. Routers don't route them.

**Lab:**

**Exercises1:**

Assign IP Class C 192.168.16.0 to students to subnet IP addresses to suit the following departments:

1. Lab computer, 24 devices
2. Computer Master's Room. 16 devices
3. Chemistry Department laboratories, 40 devices

Answer the following questions

1. What number is the subnet mask of Class C?

/24

2. What is the Network portion of Class C?

3

3. What is the Host portion of Class C?

1

4. How much to do with all the Subnets?

3

5. How many bits will you need to borrow from a Host portion?

3

6. What is the new netmask (answered as base 2)?

11111111.11111111.11111111.11000000

7. What much is the new netmask (answered in base 10)?

/26

8. How many subnet numbers can be changed ?

2 (26 and 27)

9. How much usable host Ips does each subnet have?

30 & 62

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet | IP address | Network address | Broadcast address |
| /26 | 192.168.16.0 | 192.168.16.0 | 192.168.16.63 |
| /26 | 192.168.16.64 | 192.168.16.64 | 192.168.16.127 |
| /26 | 192.168.16.128 | 192.168.16.128 | 192.168.16.191 |
| /26 | 192.168.16.192 | 192.168.16.192 | 192.168.16.255 |

**Exercises 2:**

Assign IP Class B 172.168.16.0 to students to subnet IP addresses to suit the following departments:

3 subnets for computer-labs each with 100 devices.

40 subnets for master student rooms, 16 devices each room

37 subnets for professor's rooms, 12 devices/room

Answer the following questions

1. What number is the subnet mask of Class B?

/16

2. What is the Network portion of Class B?

2

3. What is the Host portion of Class B?

2

4. How much to do with all the Subnets?

80

5. How many bits will you need to borrow from a Host portion?

9

6. What is the new netmask (answered as base 2)?

11111111.11111111.11111111.10000000

7. What much is the new netmask (answered in base 10)?

255.255.255.128

8. How many subnet numbers can be changed?

3 (25, 27 and 28)

9. How much usable host Ips does each subnet have?

126, 30, 14

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet | IP address | Network address | Broadcast address |
| /25 | 172.168.0.0 | 172.168.0.0 | 172.168.0.127 |
| /25 | 172.168.0.128 | 172.168.0.128 | 172.168.0.255 |
| /25 | 172.168.1.0 | 172.168.1.0 | 172.168.1.127 |
| /27 | 172.168.1.128 | 172.168.1.128 | 172.168.1.159 |

.

.

|  |  |  |  |
| --- | --- | --- | --- |
| /28 | 172.168.6.128 | 172.168.6.128 | 172.168.6.143 |
| /28 | 172.168.6.144 | 172.168.6.144 | 172.168.6.159 |

.

.

|  |  |  |  |
| --- | --- | --- | --- |
| /28 | 172.168.8.192 | 172.168.8.192 | 172.168.8.207 |