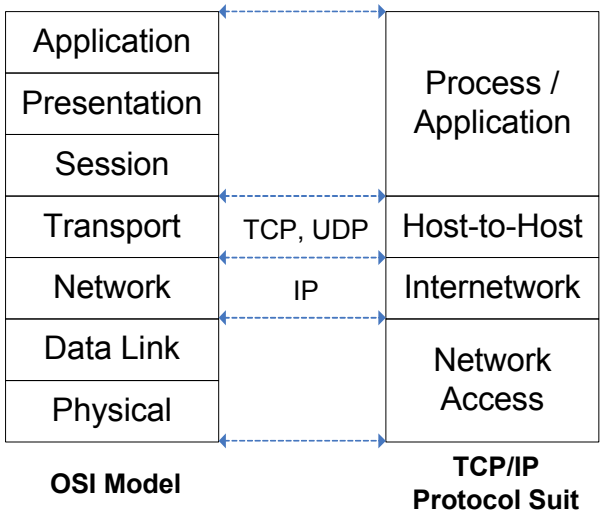
TCP/IP Concepts and Design

- The **TCP/IP** protocol suite is an example of a protocol successfully implemented using the **OSI** reference model.
- The TCP/IP suite is implemented as a set of **four** layers.
- The **bottom** layer is called the **Network Access Layer** and it represents the physical connection components such as cables, network adapter cards, and LAN access protocols such as Ethernet, Token Ring, etc.
- The next layer up is the **Internetwork Layer** which implements the functions responsible for providing a **logical address** for the **physical network interface**. In other words, this is the layer which implements the **Internet Protocol** (**IP**).
- The IP layer **maps** a **physical address** (provided by the Network Access layer) to a **logical address** using the **Address Resolution Protocol** (**ARP**), and the **Reverse Address Resolution Protocol** (**RARP**).
- The **IP** layer is also responsible for **packet routing** between hosts and networks.
- The next layer is the **Host-to-Host Layer** which implements the functions for **reliable stream** delivery of data between two hosts across a network. That is, this layer implements the **Transmission Control Protocol** (**TCP**), and the **User Datagram Protocol** (**UDP**).
- The **TCP** protocol provides **reliable**, **connection oriented**, **full-duplex stream** transfers between two hosts in a network.
- It is reliable in the sense that it uses **acknowledgments** to **retransmit** packets received with **errors**.
- The **UDP** protocol provides **unreliable**, **connectionless**, **datagram** transfers between two hosts in a network.
- It is unreliable in the sense that it does not use acknowledgments and therefore does not retransmit packets received with errors.
- The final layer is the **Process/Application Layer** which has the applications that use the Host-to-Host layer protocols. Examples are FTP, TELNET, Electronic Mail (SMTP), and Netscape.
- The relationship between the TCP/IP protocol suite and the OSI model is illustrated in the diagram shown.



The TCP/IP Protocol Suite

- **Protocols** and **applications** using the TCP/IP suite are defined in documents known as **Request For Comments** (**RFC**s) and **Standard numbers**.
- The RFCs are concerned with experimental and proposed standards. Some are just tutorials.
- The RFC that describes the list of Internet Official Protocol standards is RFC 1600.
- The table given shows some well-known standards.
- The Internet domain name for the host that provides the complete RFC archive is:

  ds.internic.net

- You can also have an RFC sent to you via e-mail:

  mailserv@ds.internic.net

Standard Name	Standard Number	RFC	TCP/IP Protocol Suite Layer
File Transfer Protocol (FTP)	9	959	Process/Application
Telnet Protocol (TELNET)	8	854, 855	Process/Application
Trivial File Transfer Protocol (TFTP)	33	1350	Process/Application
Simple Mail Transfer Protocol (SMTP)	10	821	Process/Application
Simple Network Management	15	1157	Process/Application Protocol (SNMP)
Domain Name System (DNS)	13	1034, 1035	Process/Application
Mail Routing and the DNS (DNS-MX)	14	974	Process/Application
Transmission Control Protocol (TCP)	7	793	Host-to-Host
User Datagram Protocol (UDP)	6	768	Host-to-Host
Internet Protocol (IP)	5	791	Internet
IP Subnet Extension	5	950	Internet
IP Broadcast Datagrams	5	919	Internet
IP Broadcast Datagrams with Subnets	5	922	Internet
Internet Control Message Protocol	5	792	Internet

The Internet Protocol (IP) Components

- Each of the four layers in the TCP/IP protocol suite use a specific **addressing scheme** to communicate with its peer at the remote TCP/IP host.
- The **Process/Application** layer uses **host names**. This is because users see this layer directly, and it makes it easier for users to identify hosts using names.
- The **Host-to-Host** layer uses **port numbers** as identifiers to the layer interface.
- **Port numbers** are **addresses** of **software processes** that reside on the same TCP/IP host.
- The **Internetwork** layer uses **IP addresses**. Each **network interface** on the host requires its own **IP address**.
- TCP/IP hosts that have **multiple network interfaces** (routers) are called **multihomed hosts**.

TCP/IP Protocol Suite Layer	Addressing Scheme
Process/Application	Host Name
Host-to-Host	Port number
Internetwork	IP address
Network Access	NIC Hardware address (MAC address)

Process/Application Layer Addressing

- Host names are used addresses into this layer. These **host names** are **mapped** to **IP addresses** using either DNS or a host name file.
- **Smaller networks** use static **host tables** to perform the mapping between host names and IP addresses.
- **Larger networks** use **DNS servers** (more expensive) which will require extensive configuration and maintenance.
- On **UNIX servers** the file **/etc/hosts** is used as the host name file.
- **NetWare** implements the host name files in **SYS:ETC/HOSTS**.
- **Windows NT Workstation** implements this file in **\Winnt\system32\drivers\etc\Hosts**
- An example of a **hosts** file is:

```
127.0.0.1       localhost
192.168.166.1   milliways.bcit.ca
192.168.166.2   beetelgeuse.bcit.ca
```

Host-to-Host Addressing

- This layer uses **source** and **destination port numbers** at the **Transport layer** to identify the upper layer applications from which data is receives, and to which it should be sent.
- Port numbers allow the Transport layer to **multiplex** data pertaining to more than one application and have it transmitted using the same physical connection.
- When TCP or UDP protocol modules receive a packet from the IP layer, they must distinguish between packets that need to be serviced by applications such as FTP, TELNET, SMTP, and SNMP.
- They do so by examining the **16-bit port number** fields in the packets. Thus, both **TCP** and **UDP** identify applications using **16-bit port numbers**.
- **Servers** are normally known by their "**well-known**" **port number**.
- For example, every TCP/IP implementation that provides an FTP server provides that service on TCP port 21, every TFTP is on UDP port 69, etc.
- Those services that can be provided by any implementation of TCP/IP have well-known port numbers between 1 and 1023.
- Note that a client really does not care what port number it uses on its end, all that matters is that the port number it uses be **unique** on its host.
- In a Client-Server model, a client usually exists only as long as the user is running the application using the service. Servers usually run as long as the host is up.
- **Client** port numbers are **short lived**, and so they are called **ephemeral ports**.
- Most TCP/IP implementations allocate ephemeral port numbers between 1024 and 5000.
- Port numbers above 5000 are used for those servers that are not well-known across the Internet.
- The well-known port numbers are contained in a file called **/etc/services** on **UNIX** hosts and **\Winnt\system32\drivers\etc\Services** on **Windows NT** computers.
- When two applications exchange data, they need to know the **port number** to use when **addressing** each other.
- For example, consider the Telnet application. The user specifies the host name to connect to as a command line argument.
- Telnet will establish the **login session** as follows:

    1. First, it maps the remote host name to the IP address using the hosts file.
    2. Telnet determines the port number that accurately identifies its counterpart at the remote host.

- The table below gives examples of some well-known services:

Service Name	TCP Port	UDP Port
Echo	7	7
Discard	9	9
users (Active users)	11	11
telnet	23	107 (rtelnet)
Smtp	25	
ftp	20	69 (tftp)
Nameserver (DNS)	53	53
Irc	194	194
httpd (WWW HTTP)	80	80

Ports and Sockets

- When TCP sends a request to another machine for a connection, it sends as part of the request a unique number called the socket number from the sending machine's IP address and the port number corresponding to the service requested.

- For example, if a machine with the IP address 125.66.3.20 Wants to use Telnet to communicate with another machine, it sends the IP address, port number 23 and a socket number to the destination machine.

- If the destination agrees to set up the connection, it responds with an acknowledgement that consists of a socket and port number used by Telnet on that machine (which is also 23 if the convention is followed).

- Then, both endpoints of the connection have the other's socket number and can start communicating. This connection process is illustrated in the diagram given.

- Each connection out of a TCP/IP stack is uniquely identified by unique socket and port numbers.

- After a connection between two machines has been established, the stack binds each socket to a port at both ends of the connection. The port numbers at either end will be the same (well-known service) or can be different.

- When a sending machine requests more than one connection, it uses different source port numbers. It is up to the receiving machine to reply with its assigned port numbers for each connection.

- It is possible, for example, to set up three simultaneous Telnet sessions from a single machine using three different port numbers. Each session can be to a different target, or to the same target.

- More than one machine can share a single port on a destination machine (in which case, the destination machine's socket number would be the same for each). This is called *multiplexing.*

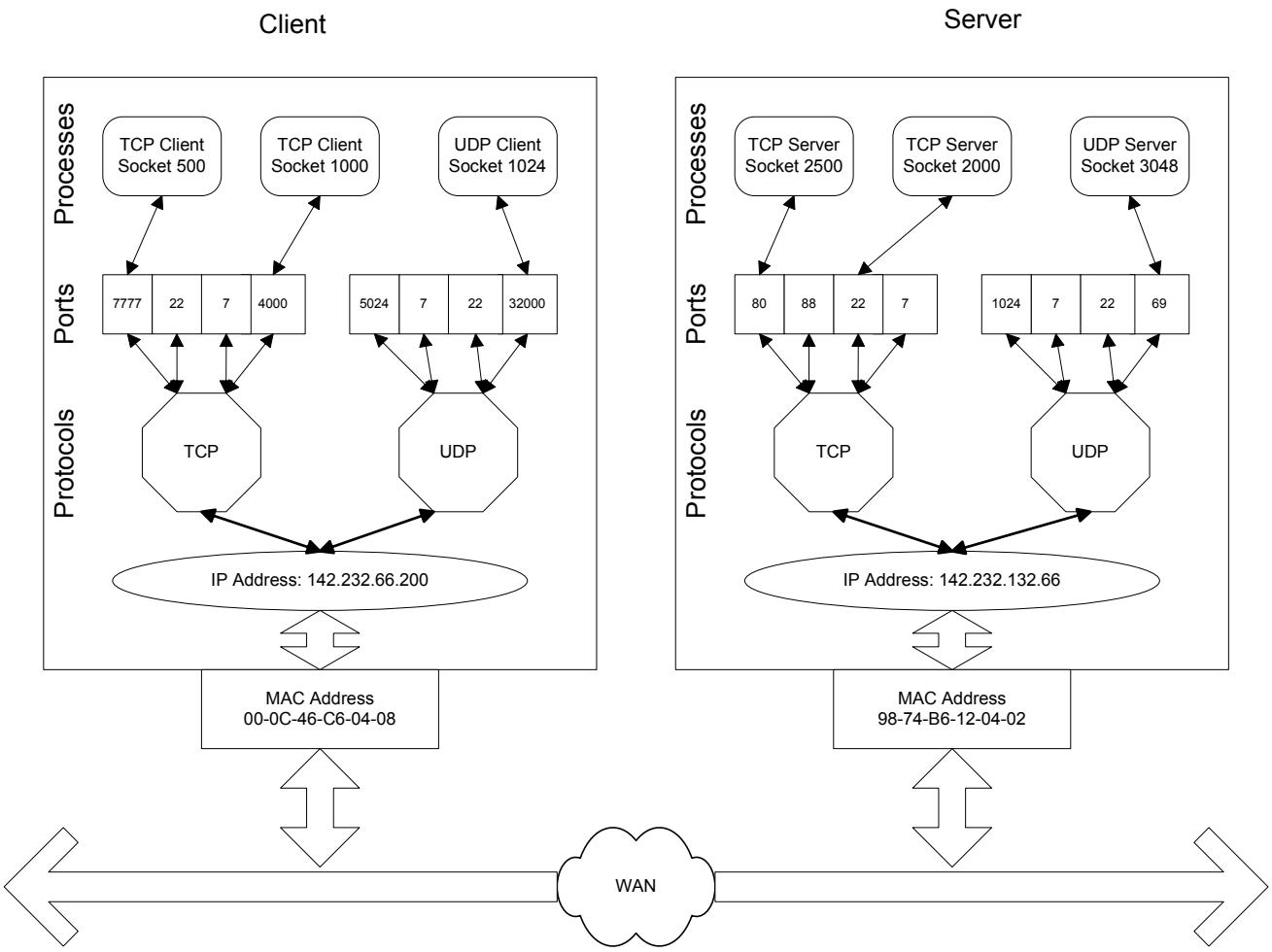
- For example, suppose three different machines establish a Telnet session with one target machine. The target can use the Telnet port for all three, which means the target's socket number is the same for all three requesting machines.

- However, because each requesting machine has a different IP address, the three connections are still identified by a unique pair of socket numbers.

- In the example shown, Machine 1, Machine 2, and Machine 3 all have the same destination socket number in their port tables.

- The target machine has three different socket numbers, one for each source machine. In the diagram, the three source machines use different socket numbers, although this is not necessary because their IP addresses uniquely identify their sockets.

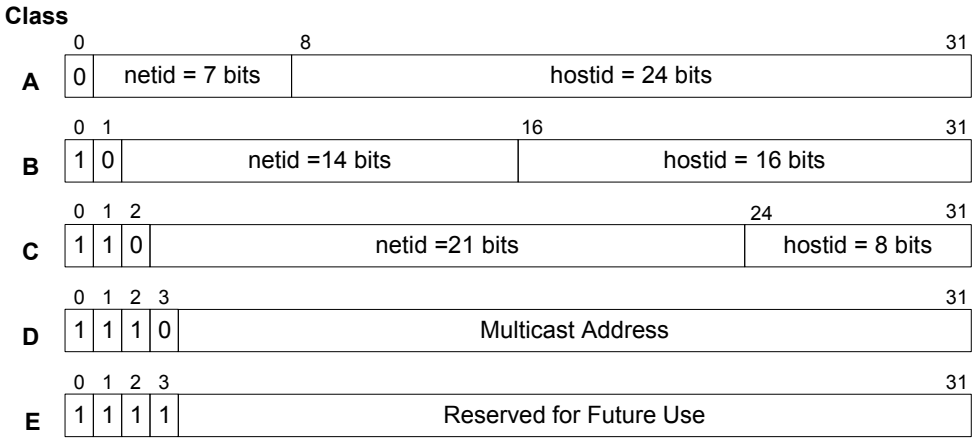
- Quite often multiple sockets are established into one port, more than one machine can share the same source and destination ports. Because the IP addresses for the machines are different, though, the sockets are still uniquely identified.



- TCP uses one of two methods to establish a connection: **active** or **passive**. An active connection is when TCP issues a request for the connection based on an instruction to establish the connection issued from a higher-level application.
- An active connection request can include some specific information about the socket number to be used, a precedence or priority level, and some security-level value.
- A passive connection is when a higher-level application requests TCP to listen for connection requests from remote systems.
- When TCP receives the connection request from the remote system, it assigns a port number and passes the number back to the application.
- There are two kinds of passive opens. A **specified passive open** creates a connection when the precedence level and security level meet particular requirements. An **unspecified passive open** opens the port to any request.
- Unspecified passive open requests are used by servers that must wait for an unknown protocol to ask for a connection.

Internetwork Layer Addressing

- Each **host** on the **Internet** is assigned a unique **32-bit integer address** called its Internet Address or its **IP address**.
- The **IP address** consists of **two parts**: a network ID (**netid**), and a host ID (**hostid**).
- **netid** identifies a **network**, and **hostid** identifies a **host** on that **network**.
- There are **five classes** of IP addresses: **A**, **B**, **C**, **D**, and **E**. The three **primary classes** A, B, and C have **assignable addresses**.



The Five IP Address Classes

Class A

- The first **octet** (eight bits) defines the **netid**. However, the leftmost bit must be zero to define the class as A. The remaining seven bits define different networks.
- Theoretically we have $2^7 = 128$ networks. However, there are actually 126 networks in class A because two of the addresses are reserved for special purposes.
- In a class A network, 24 bits are used to define the **hostid**. Theoretically we can have up to $2^{24} = 16{,}777{,}216$ hosts. However, two special addresses (hostid all 0's and hostid all 1's) are used for special address.
- Class A addresses are suitable for a small number of networks with a very large number of hosts. The original **ARPANET** is an example of such a network.

Class B

- Two octets define the **netid** and two octets define the **hostid**. The two leftmost bits are 10 to define the class as B. The next 14 bits define different networks.
- We can have 2^{14} = 16,384 class B networks. 16 bits are used to define the hostid. Theoretically we can have up to 2^{16} = 65,536 hosts).
- However, two of these addresses (hostid all O's and hostid all 1's) are used for special addresses. This means that a class B network can have up to 65,534 hosts.
- Class B addresses are used to provide a larger number of medium-size networks, suitable for medium to large organizations.

Class C

- Three octets define the netid and one octet defines the hostid. The three leftmost bits are 1 10 to define the class as C. The next 21 bits define different networks. We can have 2^{21} = 2,097,152 networks.
- Eight bits are used to define the hostid. This means each network can theoretically have up to 28 = 256 hosts. However, again two addresses (hostid all 0's and hostid all 1's) are reserved for special addresses.
- Class C addresses are used to provide for a very large number of small-size networks, suitable for small organizations which have no more than 254 hosts in a network.

Class D & E

- **Class D** is reserved for **multicasting** and is used by certain protocols (UDP) to transmit datagrams to a group of hosts.
- **Class E** is reserved for future use.
- Given an **IP address**, the **primary address class** can be determined using the **three high-order bits** of the address.

- The different classes define IP addresses which address the needs of different network sizes as shown in the table below.

Address Class	Number of Networks	Number of Hosts
A	2^{7} - = 126	2^{24} – 2 = 16,777,214
B	2^{14} = 16,384	2^{16} – 2 = 65,534
C	2^{21} = 2,097,152	2^{8} – 2 = 254

Special Addresses

- Some parts of the address space in class A, B, and C are used for special addresses as shown in the table below.

Special address	Netid	Hostid	Source or Destination
Network address	specific	All 0's	None
Direct broadcast address	specific	All 1's	Destination
Limited broadcast address	All 1's	All 1's	Destination
This host on this network	All 0's	All 0's	Source
Specific host on this network	All 0's	specific	Destination
Loopback address	127	Any	Destination

Network Address

- In classes A, B, and C, an address with a hostid of all zeros is not assigned to any host; it is reserved to define the network address itself. In other words, the network itself is considered an entity with an IP address in which the hostid part is set to zero.

- Note that this address cannot be used to define a source or destination address in an IP packet. Note also that this special address reduces the number of available hostids for each netid in

Direct Broadcast Address

- In classes A, B, and C, if the hostid is all I s, the address is called a **direct broadcast address.** It is used by a router to send a packet to all hosts in a specific network.

- All hosts will accept a packet having this type of destination address. Note that this address can be used only as a destination address in an IP packet.

Limited Broadcast Address

- In classes A, B, and C, an address with all 1 s for the netid and hostid (32 bits) is used to define a broadcast address in the current network.

- A host which wants to send a message to every other host can use this address as a destination address in an IP packet. However, a router will block a packet having this type of address to confine the broadcasting to the local network. Note that this address belongs to class E.

This Host on This Network

- If an IP address is composed of all zeros, it means **this host on this network**. This is used by a host at bootstrap time when it does not know its IP address.

- The host sends an IP packet to a bootstrap server using this address as the source address and a limited broadcast address as the destination address to find its own address.

- Note that this address can be used only as a source address. Note also that this address is always a class A address regardless of the network.

Specific Host on This Network

- An IP address with a netid of all zeros means a specific host on this network. It is used by a host to send a message to another host on the same network.

- Because the packet is blocked by the router, it is a way of confining the packet to the local network. Note that it can be used only for a destination address.

Loopback Address

- The IP address with the first byte equal to 127 is used for the **loopback address,** which is an address used to test the software on a machine.

- When this address is used, a packet never leaves the machine; it simply returns to the protocol software. It can be used to test the IP software.

- For example, an application such as "ping" can send a packet with a loopback address as the destination address to see if the IP software is capable of receiving and processing a packet.

Dotted Decimal Notation

- The **32-bit IP address** is conveniently represented as a set of **four decimal integers** separated by **periods**, where each **integer** gives the value of **one octet** of the IP address.

- Thus, a 32-bit IP address can be shown in binary form as well as using the dotted decimal notation as shown:

IP Address (binary form): 10000000 11101000 01000010 00000001

IP Address (DDD): 128.232.66.1

- The table below summarizes the range of IP addresses for each class:

Class	Most Significant Bits	Lowest IP Address	Highest IP Address
A	1	0.1.0.0	127.0.0.0
B	10	128.0.0.0	191.255.0.0
C	110	192.0.1.0	223.255.255.0
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

- As mentioned earlier, interconnected networks must have unique netids. If a network is to be connected to other networks such as the Internet, you must apply to a central authority to obtain a unique netid.

- The **Internet Assigned Number Authority** (**IANA**) has ultimate control over numbers assigned and sets the various policies.

- However, when an organization joins the Internet, it can obtain network addresses from the **Internet Network Information Center** (**INTERNIC**).

- The central authority is only needed to assign the network portion of the address. Once the network prefix is obtained, an organization can choose to assign a unique suffix to each host within the network however it chooses.

- The INTERNIC assigns a class C number to a network with a small number of attached host computers and reserves class B numbers for organizations that have a large number of attached hosts.

- An organization with a gigantic number of attached hosts (65535) can obtain a class A address.

Subnet Masks

- As it turns out, the original IP addressing scheme has one major weakness and that is simply: **growth**.
- The original designers (mainframe world) did not foresee the tens of thousands of small networks of PCs that would appear a decade after the conception of TCP/IP.
- This growth is most apparent in the Internet where the size doubles every nine months or so.
- This explosion of small networks impacts the overall Internet design in three ways:

    1. Enormous administrative overhead in managing network addresses.
    2. Routers require very large routing tables.
    3. The address space will eventually be exhausted.

- The third problem is crucial because the original address scheme could not accommodate the number of networks currently on the Internet.
- This is especially true of class B prefixes since they are insufficient to cover all the medium-size networks on the Internet.
- The main issue then is, how can we minimize the number of assigned network addresses, especially class B, without completely re-designing the original scheme?
- The answer lies in **sharing one network address** among **multiple physical networks**. In particular we will examine a technique called **subnetting** (aka **subnet addressing** and **subnet routing**).
- The **subnetting** scheme uses some of the **bits** in the **hostid field** for distinguishing between two or more networks and leave the rest for host number assignments.
- The resulting networks are called **subnets**. This standard is documented in **RFC 950**.
- Consider a **single site** which has a **single class B IP network address** assigned to it, but has **two** or more **physical networks**.
- Now all we have to do is to have the local **routers** know that there are multiple physical networks and how to route data among them.
- Essentially, the **32-bit IP address** now has an **Internet portion** and a **local portion**.
- The **Internet portion** identifies a **site**, possibly with more than one physical network, and the **local portion** identifies a **physical network** and a **host** at that **site**.
- The diagram shown illustrates this technique. In this example, the site is using the **single** class B IP address **128.232.0.0** for **two networks**.
- Except for this site's router, all routers in the Internet route as if it were a single physical network.

- Once the packet reaches the router, it will be sent to the destination workstation on the correct physical network.

- In this example, this site has chosen to use the **third octet** of the address to **distinguish** between the **two networks**.

- The network manager in this case will assign workstations on one physical network addresses of the form: 128.232.66.X, and 128.232.132.X to workstations on the second physical network. X represents the unique integer used to identify a specific workstation.

- The **router** will examine the **third octet** of the **IP address**, and will route datagrams with value 66 to the network labeled 128.232.66.0 and those with value 132 to the network labeled 128.232.132.0.

- The key here is that the router must be made to understand that the **hostid** field of the IP address is to be processed in a special way.

- Part of the **hostid** is used for the **subnet number** and the remaining part of the **host number**. This information is represented to the router in the form of a **subnet mask**.

- The **subnet mask** is used by **routers** and **hosts** on a subnet to **interpret** the **hostid** field in such a way such that they can determine the **number of bits** being used for **subnetting**.

- The subnet mask **divides** the **hostid** field into the **subnet number** and the **host number**.

- The mask itself is a set of 32 bits, each bit set according to the rules established in RFC 950.

- Bits in the mask are set to **1** if the network treats the corresponding bit in the IP address as part of the **network address**, and **0** if it treats the bit as part of the **host address**.

- Consider the following subnet mask:

  11111111 11111111 11111111 00000000

- The above mask specifies that the first three octets are used to identify the network and the fourth octet is used to identify a host on the network.

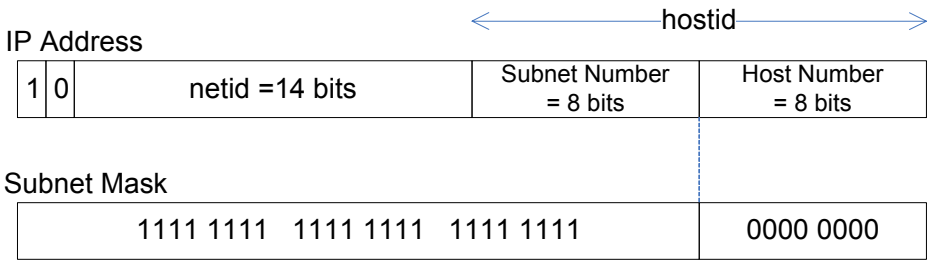
- In dotted notation the above mask is represented as **255.255.255.0**.

- The router uses the **subnet mask** to **extract** bits of the **destination address** for comparison with entries in a **routing table**.

- It does so by performing a **bit-wise Boolean AND** of the **32-bit IP address** and the **subnet mask** field from an entry, and then checks to see if the result equals the value in the network address field of that entry.

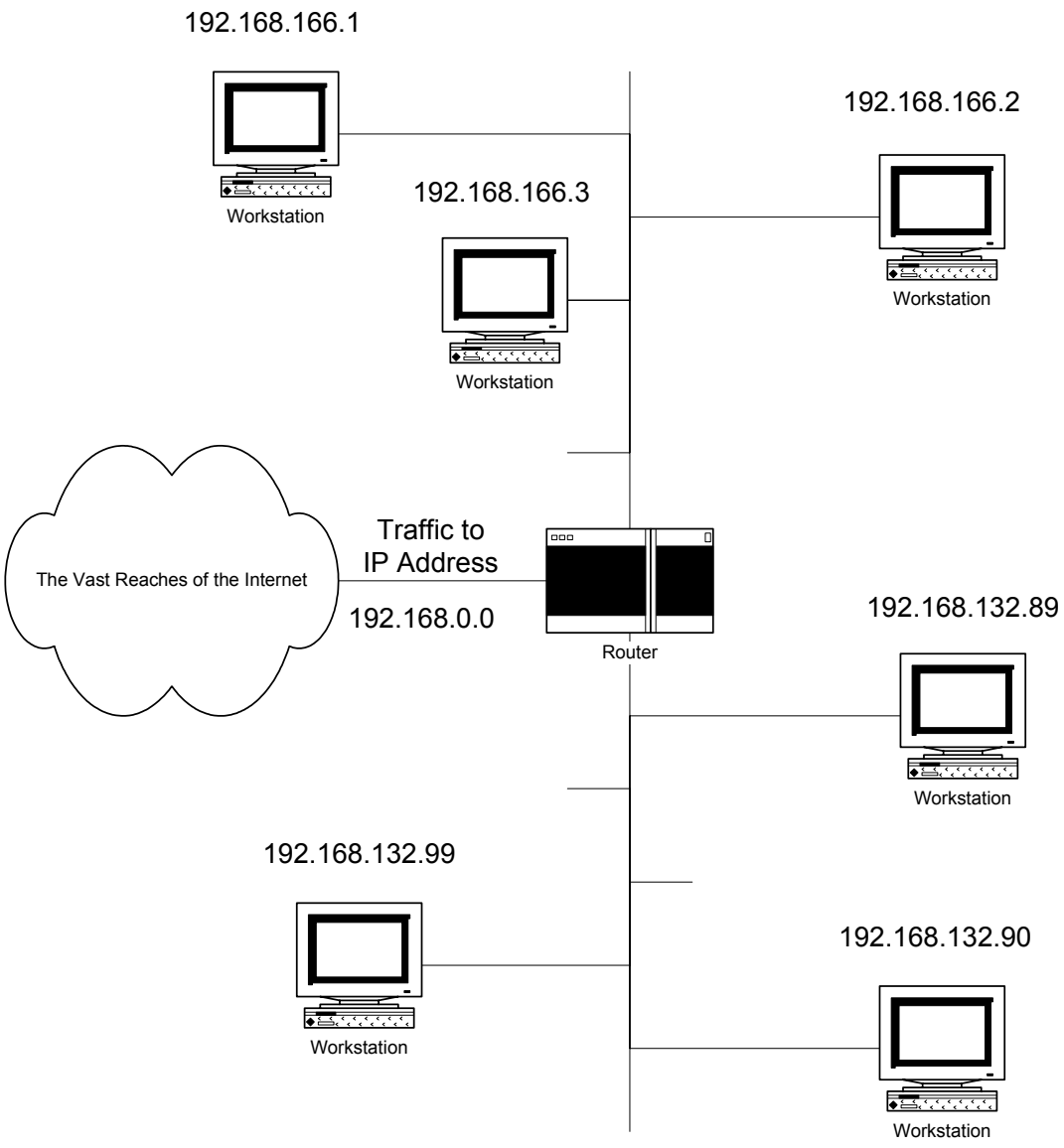
- If so, the router sends the datagram to the address specified for a machine on the subnet.

- The diagram shown illustrates the application of a subnet mask to a class B IP address.



Class B Subnetting

- **Eight bits** of the **hostid** field are being used for the **subnet number** and the remaining **eight bits** are used for identifying a **host** on that **subnet**.
- Note that if a **subnet mask** value of **255.255.0.0** is used for a **class B** address, the indication is that **no subnetting** is being used.
- This is simply because a **class B** address has a **netid** field of **16 bits**. This accounts for the first two octets (255.255.) in the mask. The remaining two octets (0.0) must therefore correspond to the **hostid**.
- Thus, if the **IP address** is **128.232.66.1** and the subnet mask is **255.255.0.0**, a **bit-wise AND** will produce the **network number** which is **128.232.0.0**.
- Conversely, a subnet mask value of **255.255.0.0** for a **class A** address indicates that **subnetting** is being used.
- A **class A** address has an **8-bit netid**. The **netid** is accounted for by the **first octet** (255) in the mask. The **remaining 255** must correspond to the **subnet number**, which is 8-bits long.



A Class B site with two physical networks using subnet addressing to connect to the Internet.

Multihomed Devices

- An Internet address defines the node's connection to its network. It follows, therefore, that any device connected to more than one network must have more than one Internet address.

- A computer that is connected to different networks is called a **multihomed** computer and will have more than one address, each possibly belonging to a different class.

- A router must be connected to more than one network, otherwise it cannot route. Therefore a router definitely has more than one IP address, one for each interface.

Private Networks

- If an organization does not need access to the Internet but wants the TCP/IP protocol on its network, there are three choices for its addressing needs:
    - It can apply for a unique address and use it without being connected to the Internet.
    - It can use any class A, B, or C address without registering with the Internet authorities. Because the network is isolated, the address does not have to be unique.
    - To overcome the problems associated with the first and second strategies, the Internet authorities have reserved three blocks of addresses, shown below.

Class	Range	Subnet Mask
A	10.0.0.0 ==> 10.255.255.255	255.0.0.0
B	172.16.0.0==> 172.31.255.255	255.255.0.0
C	192.168.0.0==> 192.168.255.255	255.255.255.0

- Private IP addresses are sometimes referred to as Non-Routable IP. This is because the addresses are not routed to the Internet by an Internet Service Provider.

- Network administrators often use private IP addresses when setting up firewall security systems. The systems inside some firewalls are not directly accessible from the Internet and only communicate by proxy, they can use private IP addresses.

- This is partly a security measure since the addresses will not be routed across the Internet, and partly a measure to conserve IP addresses.