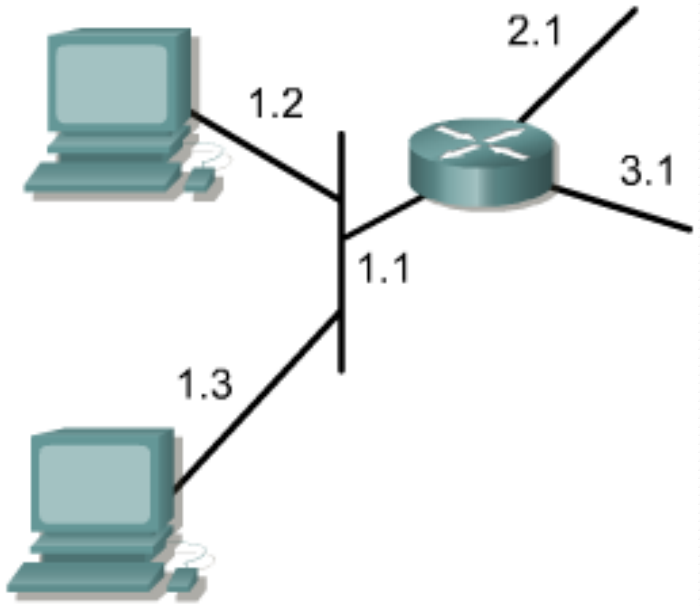
IP Addressing

Network and Host Addressing

Using the IP address of the destination network, a router can deliver a packet to the correct network.

When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the particular computer connected to that network.

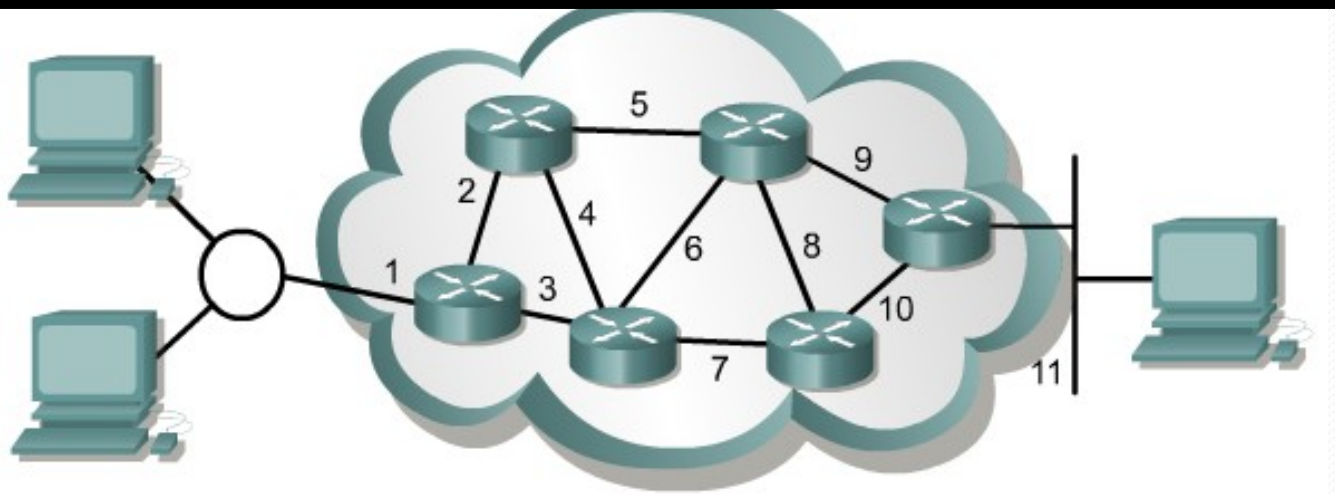
Accordingly, every IP address has two parts.



Network	Host
1	1 2 3
2	1
3	1

Network Layer Communication Path

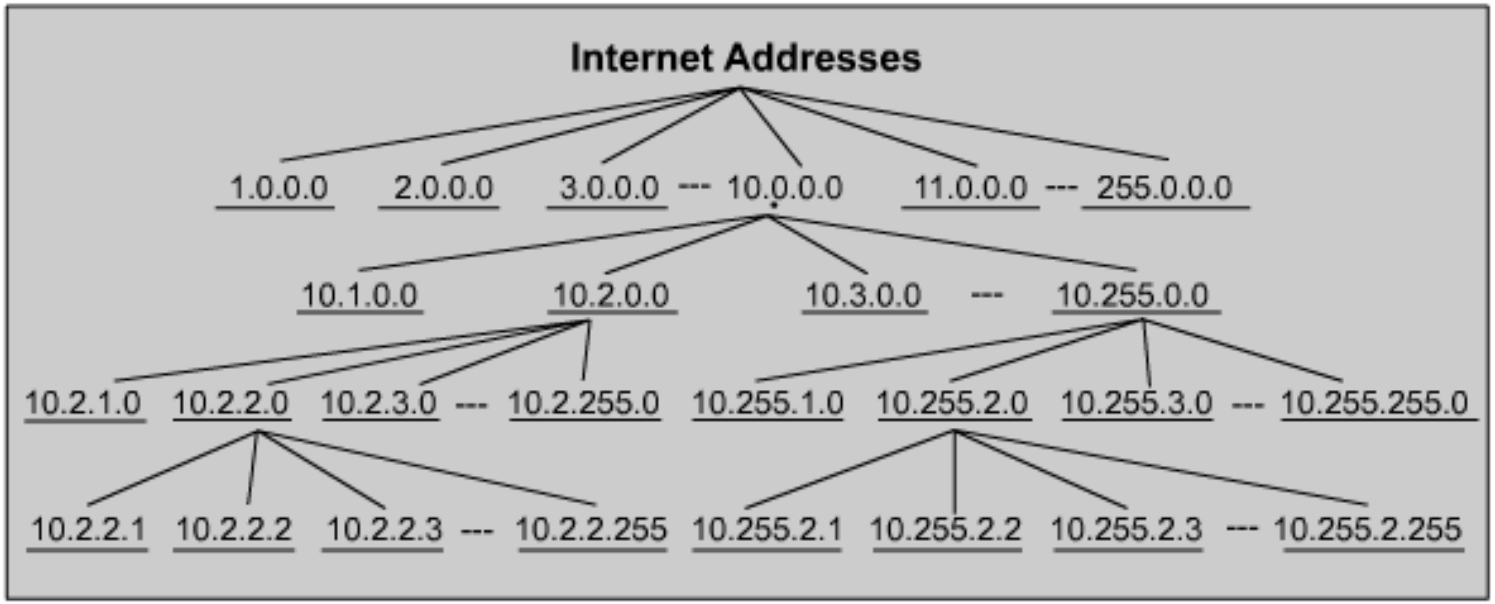
A router forwards packets from the originating network to the destination network using the IP protocol. The packets must include an identifier for both the source and destination networks.



Address represent the path of media connections

Internet Addresses

IP Addressing is a hierarchical structure.An IP address combines two identifiers into one number. This number must be a unique number, because duplicate addresses would make routing impossible.The first part identifies the system's network address.The second part, called the host part, identifies which particular machine it is on the network.



IP Address Classes

IP addresses are divided into classes to define the large, medium, and small networks.

Class A addresses are assigned to larger networks.
Class B addresses are used for medium-sized networks, &
Class C for small networks.

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

Identifying Address Classes

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

* The 127.x.x.x address range is reserved as a loopback address, used for testing and diagnostic purposes.

Address Class Prefixes

To accommodate different size networks and aid in classifying these networks, IP addresses are divided into groups called classes.This is **classful addressing**.

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

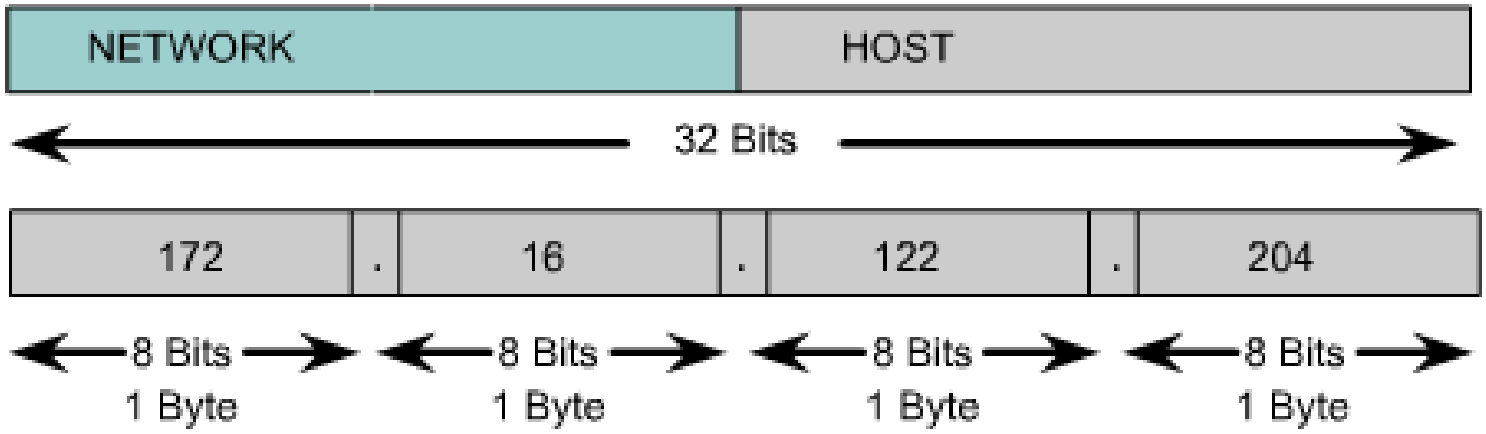
Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Class D addresses are used for multicast groups. There is no need to allocate octets or bits to separate network and host addresses. Class E addresses are reserved for research use only.

Network and Host Division

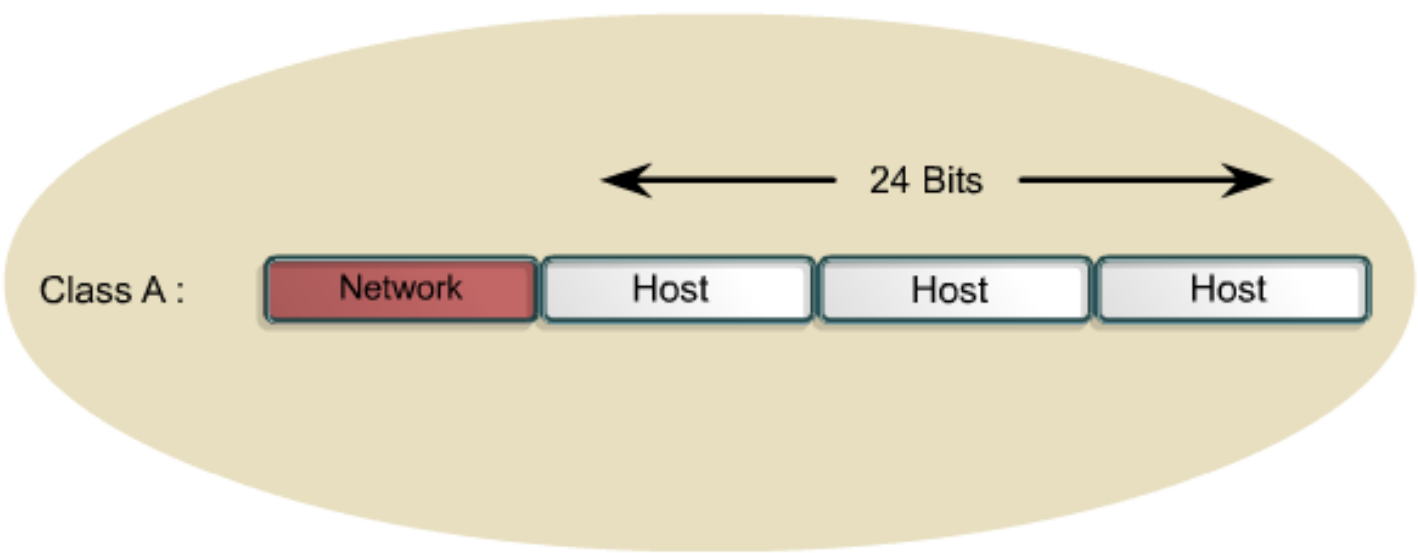
Each complete 32-bit IP address is broken down into a network part and a host part. A bit or bit sequence at the start of each address determines the class of the address. There are 5 IP address classes.



An IP address will always be divided into a network and host portion. In a classful addressing scheme, these divisions take place at the octet boundaries.

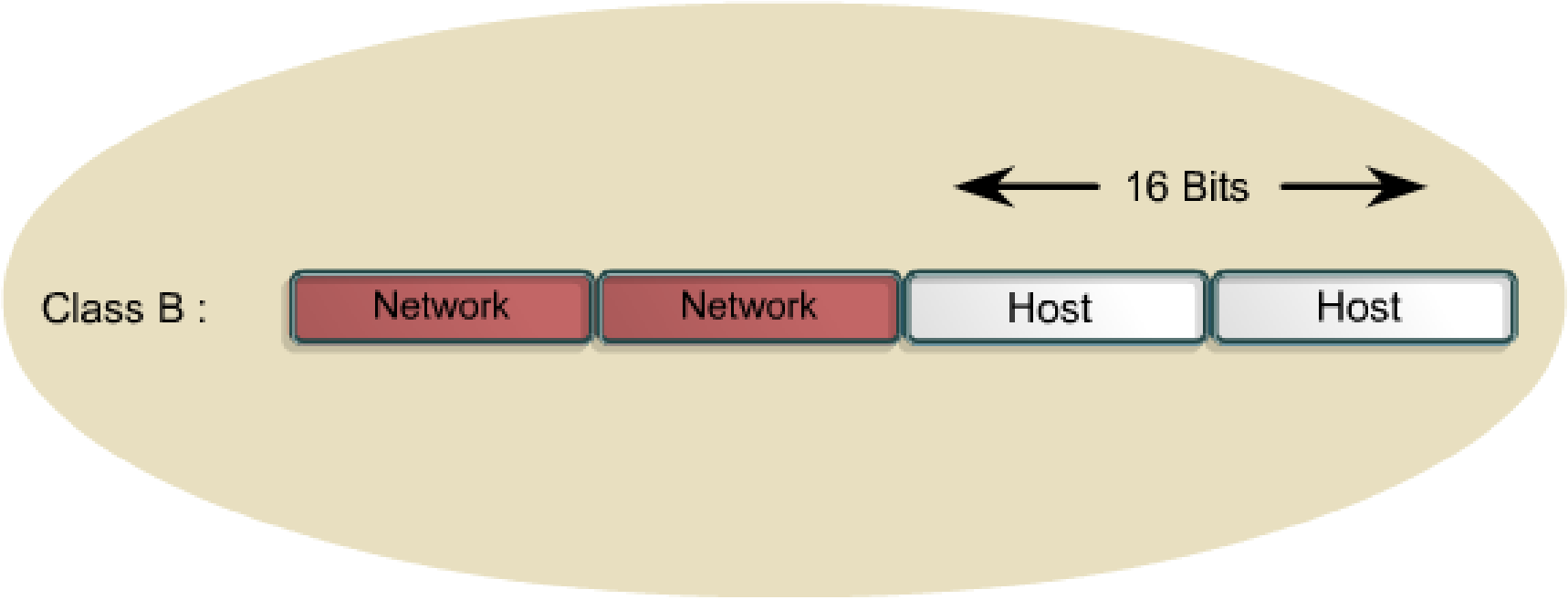
Class A Addresses

The Class A address was designed to support extremely large networks, with more than 16 million host addresses available. Class A IP addresses use only the first octet to indicate the network address. The remaining three octets provide for host addresses.



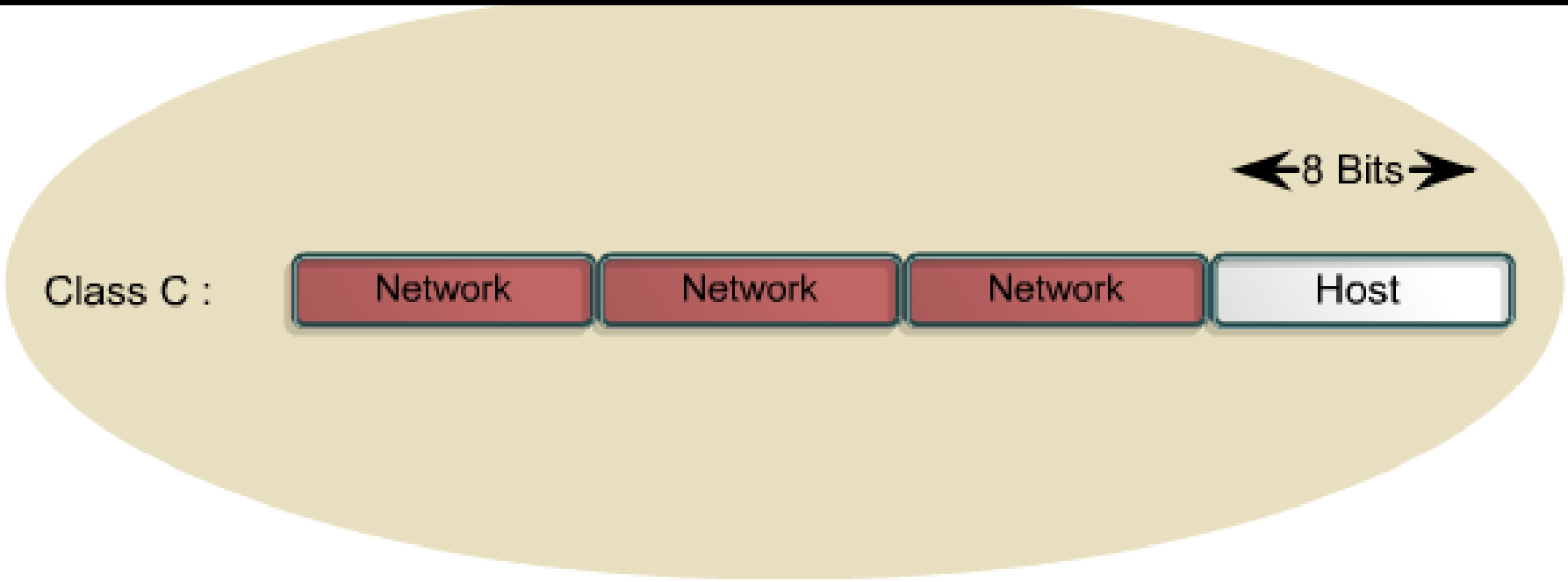
Class B Addresses

The Class B address was designed to support the needs of moderate to large-sized networks.A Class B IP address uses the first two of the four octets to indicate the network address. The other two octets specify host addresses.



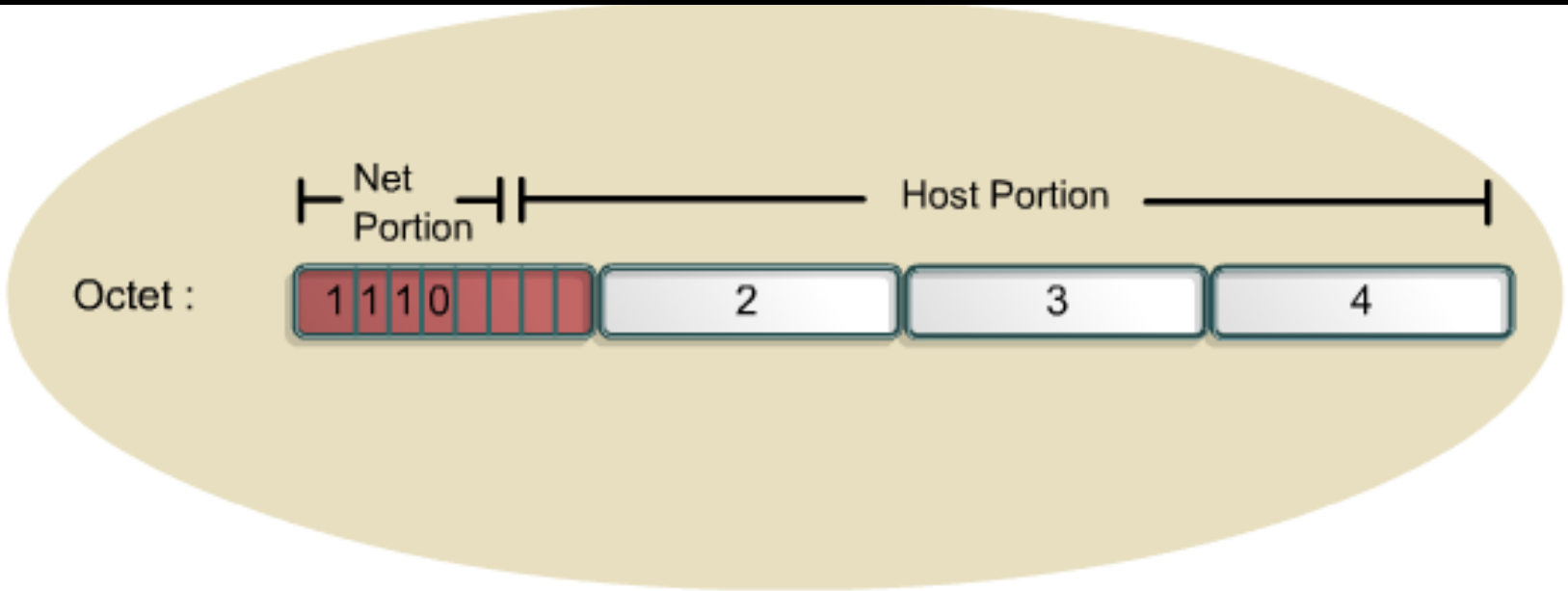
Class C Addresses

The Class C address space is the most commonly used of the original address classes.This address space was intended to support small networks with a maximum of 254 hosts.



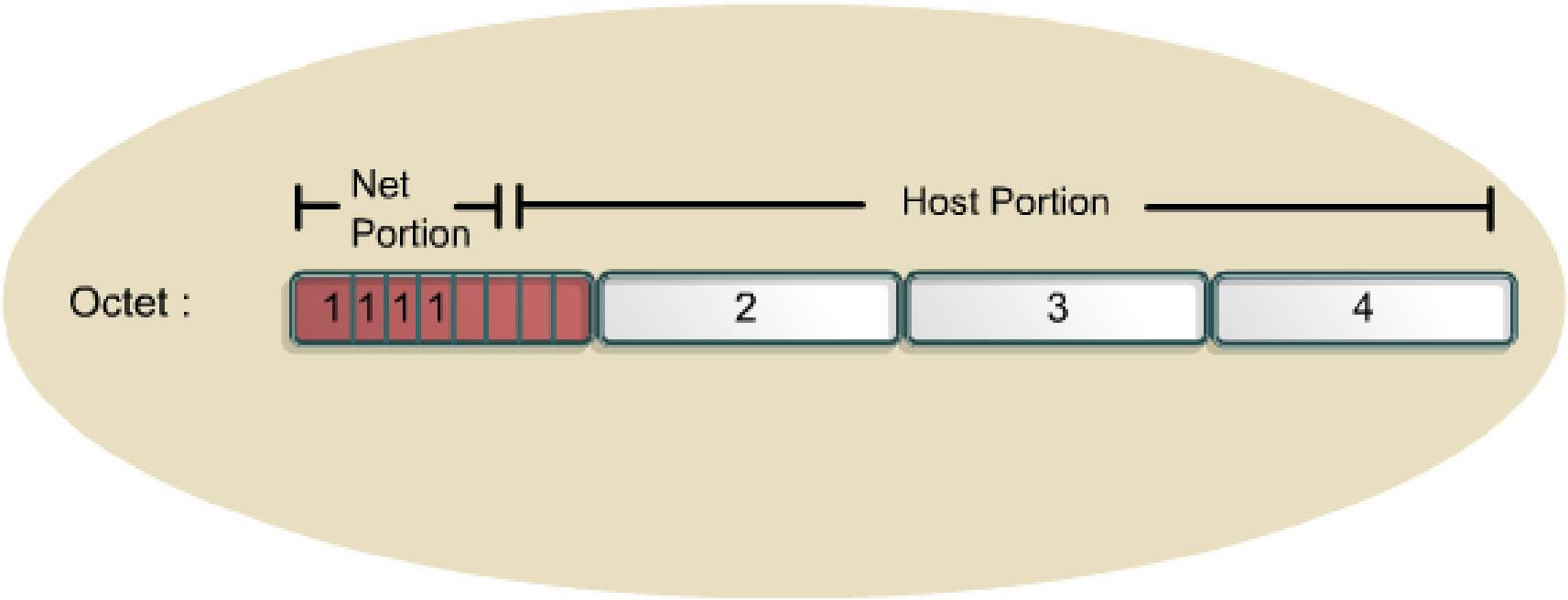
Class D Addresses

The Class D address class was created to enable multicasting in an IP address. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of data to multiple recipients.



Class E Addresses

A Class E address has been defined. However, the Internet Engineering Task Force (IETF) reserves these addresses for its own research. Therefore, no Class E addresses have been released for use in the Internet.



IP Address Ranges

The graphic below shows the IP address range of the first octet both in decimal and binary for each IP address class.

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

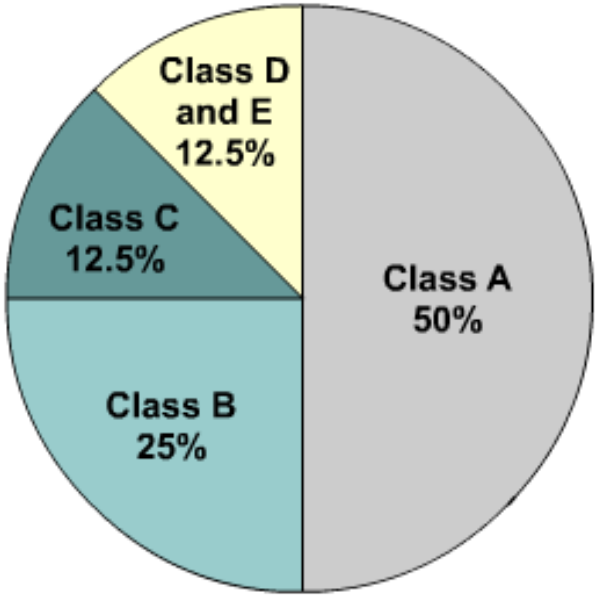
Determine the class based on the decimal value of the first octet

* 127 (011111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.

IPv4

As early as 1992, the Internet Engineering Task Force (IETF) identified two specific concerns: Exhaustion of the remaining, unassigned IPv4 network addresses and the increase in the size of Internet routing tables.

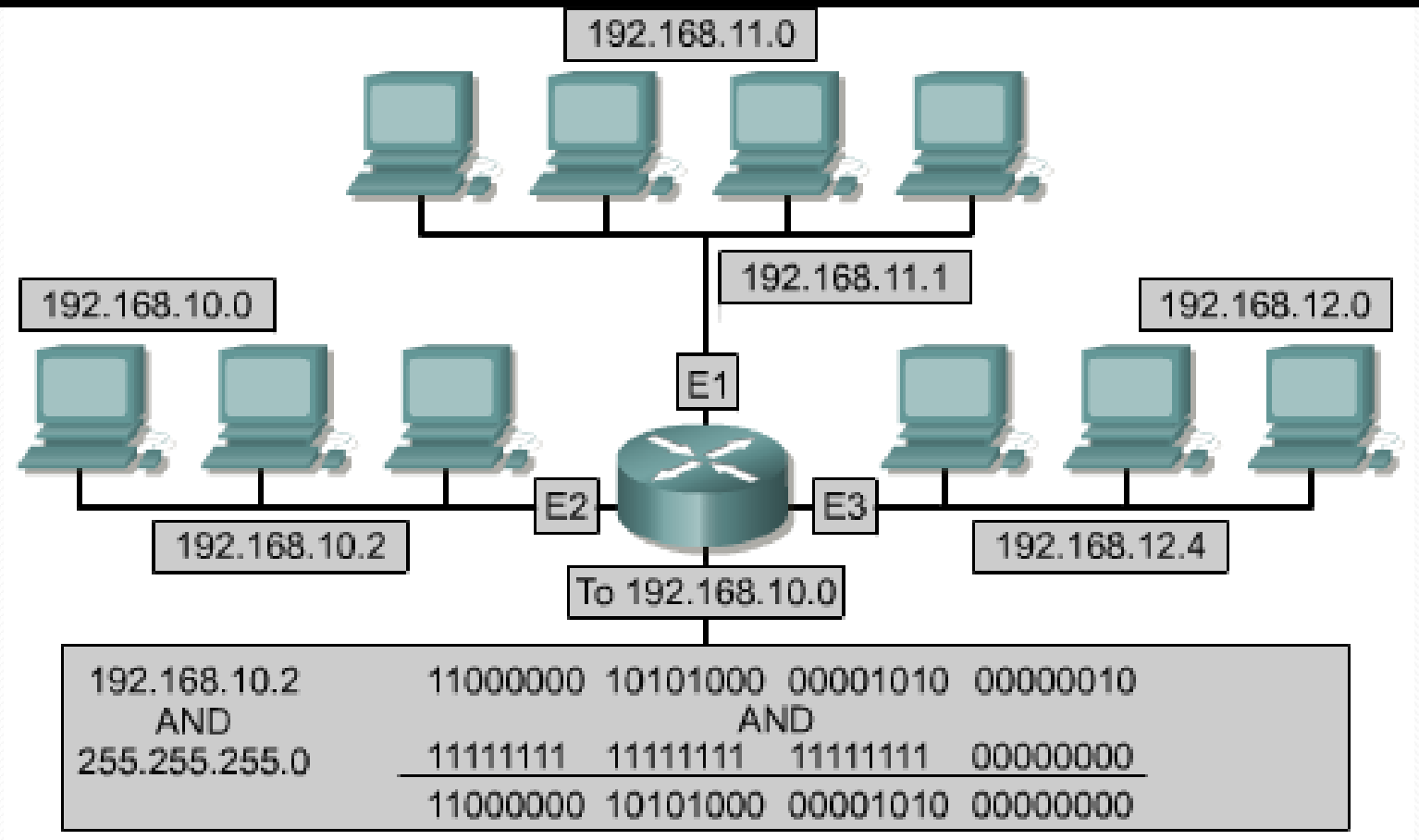
Over the past two decades, numerous extensions to IPv4 have been developed. Two of the more important of these are subnet masks and classless interdomain routing (CIDR).



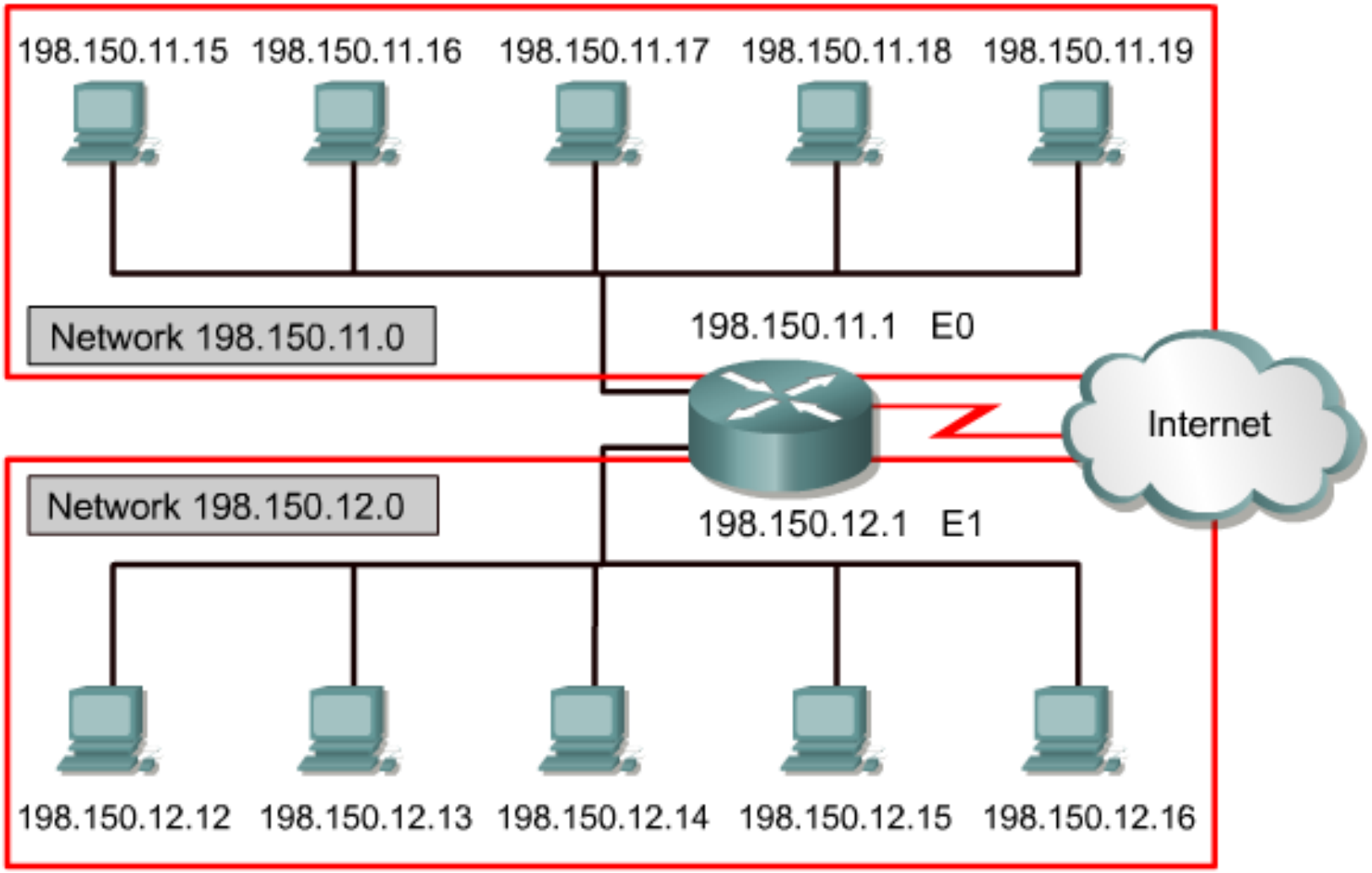
With Class A and B addresses virtually exhausted, Class C addresses (12.5 percent of the total space) are left to assign to new networks.

Finding the Network Address with ANDing

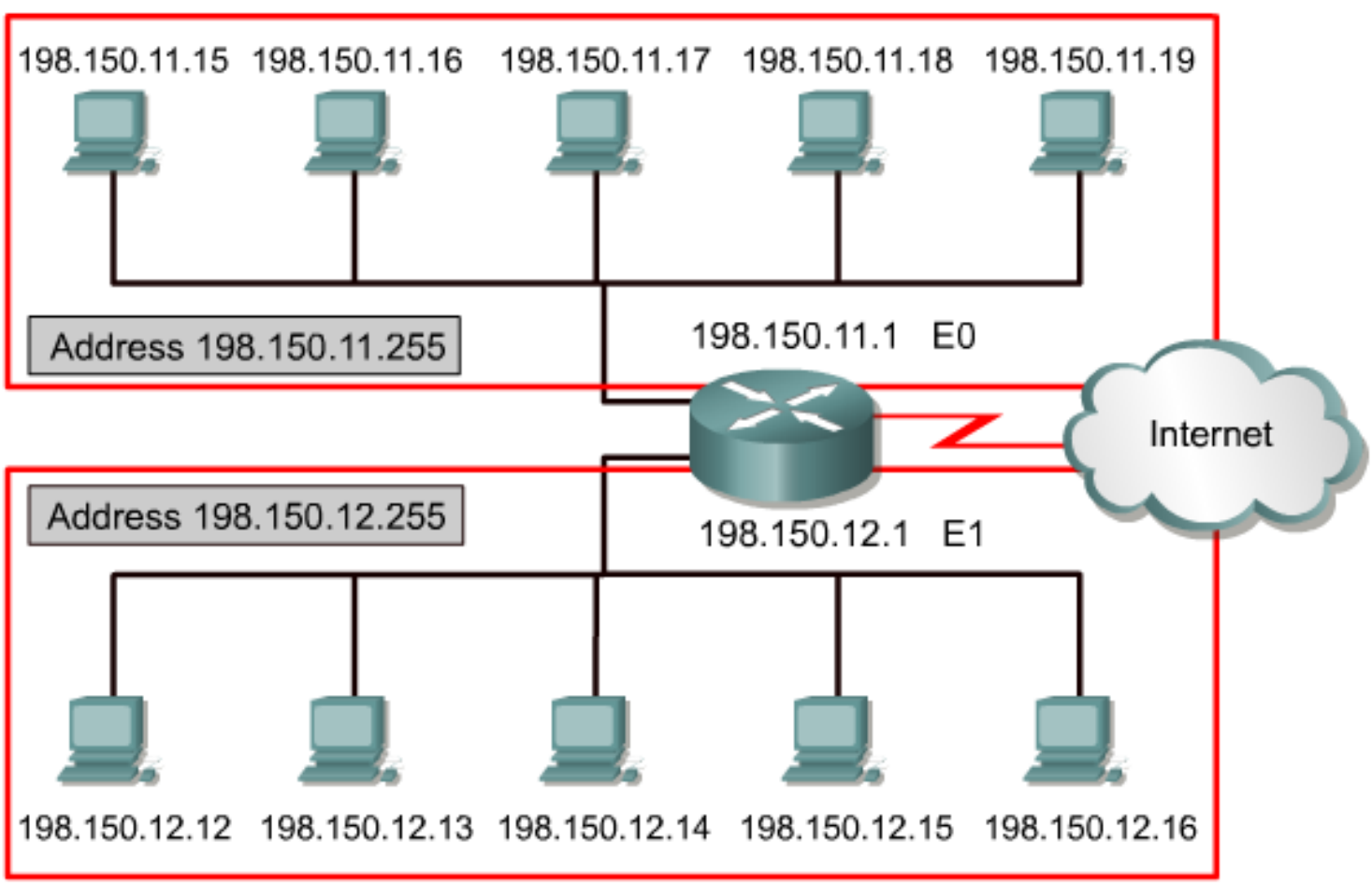
By ANDing the Host address of **192.168.10.2** with **255.255.255.0** (its network mask) we obtain the network address of **192.168.10.0**



Network Address



Broadcast Address



Network/Broadcast Addresses at the Binary Level

An IP address that has binary 0s in all host bit positions is reserved for the network address, which identifies the network. An IP address that has binary 1s in all host bit positions is reserved for the broadcast address, which is used to send data to all hosts on the network. Here are some examples:

Class	**Network Address**	**Broadcast Address**
A	100.0.0.0	100.255.255.255
B	150.75.0.0	150.75.255.255
C	200.100.50.0	200.100.50.255

Public IP Addresses

Unique addresses are required for each device on a network.

Originally, an organization known as the Internet Network Information Center (InterNIC) handled this procedure.

InterNIC no longer exists and has been succeeded by the Internet Assigned Numbers Authority (IANA).

No two machines that connect to a public network can have the same IP address because public IP addresses are global and standardized.

All machines connected to the Internet agree to conform to the system.

Public IP addresses must be obtained from an Internet service provider (ISP) or a registry at some expense.

Private IP Addresses

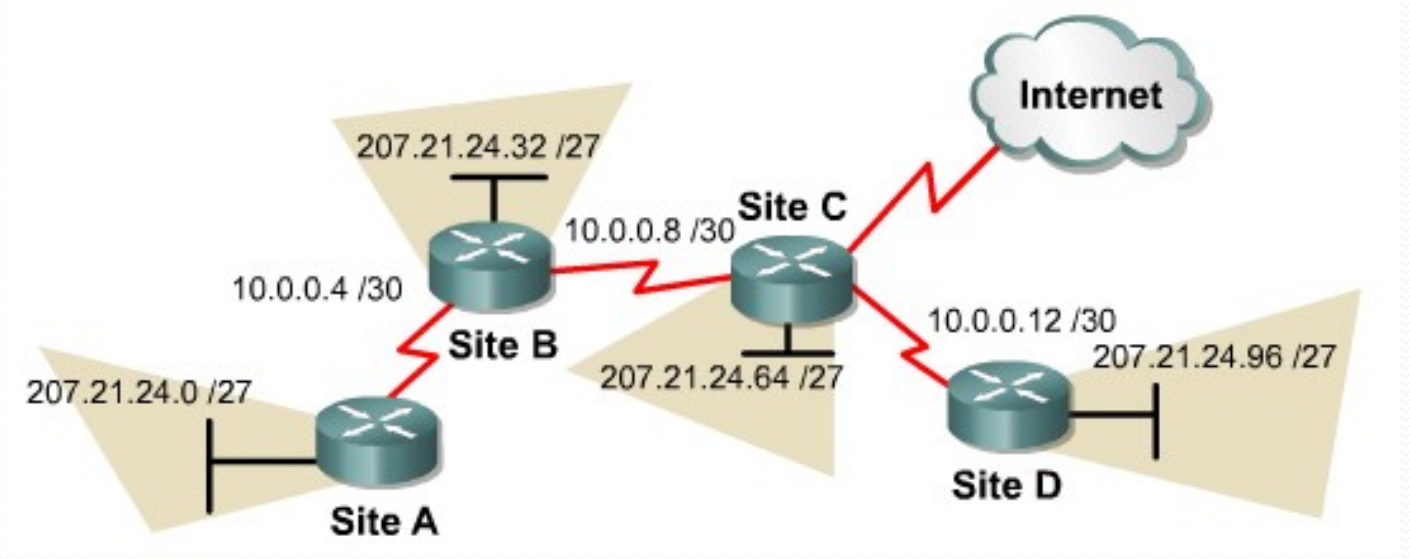
Private IP addresses are another solution to the problem of the impending exhaustion of public IP addresses.As mentioned, public networks require hosts to have unique IP addresses.

However, private networks that are not connected to the Internet may use any host addresses, as long as each host within the private network is unique.

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Mixing Public and Private IP Addresses

Private IP addresses can be intermixed, as shown in the graphic, with public IP addresses.This will conserve the number of addresses used for internal connections. Connecting a network using private addresses to the Internet requires translation of the private addresses to public addresses. This translation process is referred to as Network Address Translation (NAT).



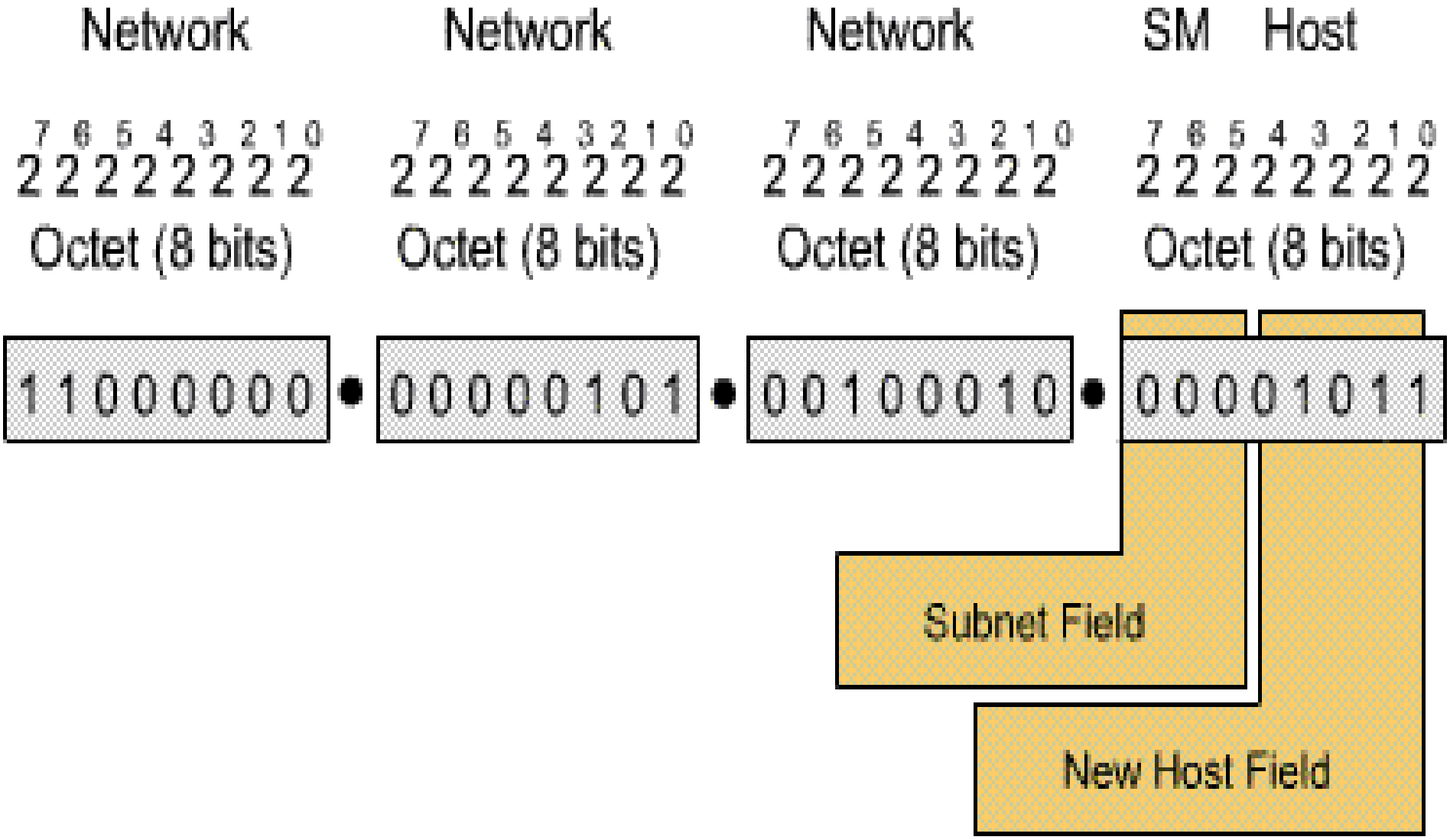
Introduction to Subnetting

Subnetting a network means to use the subnet mask to divide the network and break a large network up into smaller, more efficient and manageable segments, or subnets.

With subnetting, the network is not limited to the default Class A, B, or C network masks and there is more flexibility in the network design.

Subnet addresses include the network portion, plus a subnet field and a host field.The ability to decide how to divide the original host portion into the new subnet and host fields provides addressing flexibility for the network administrator.

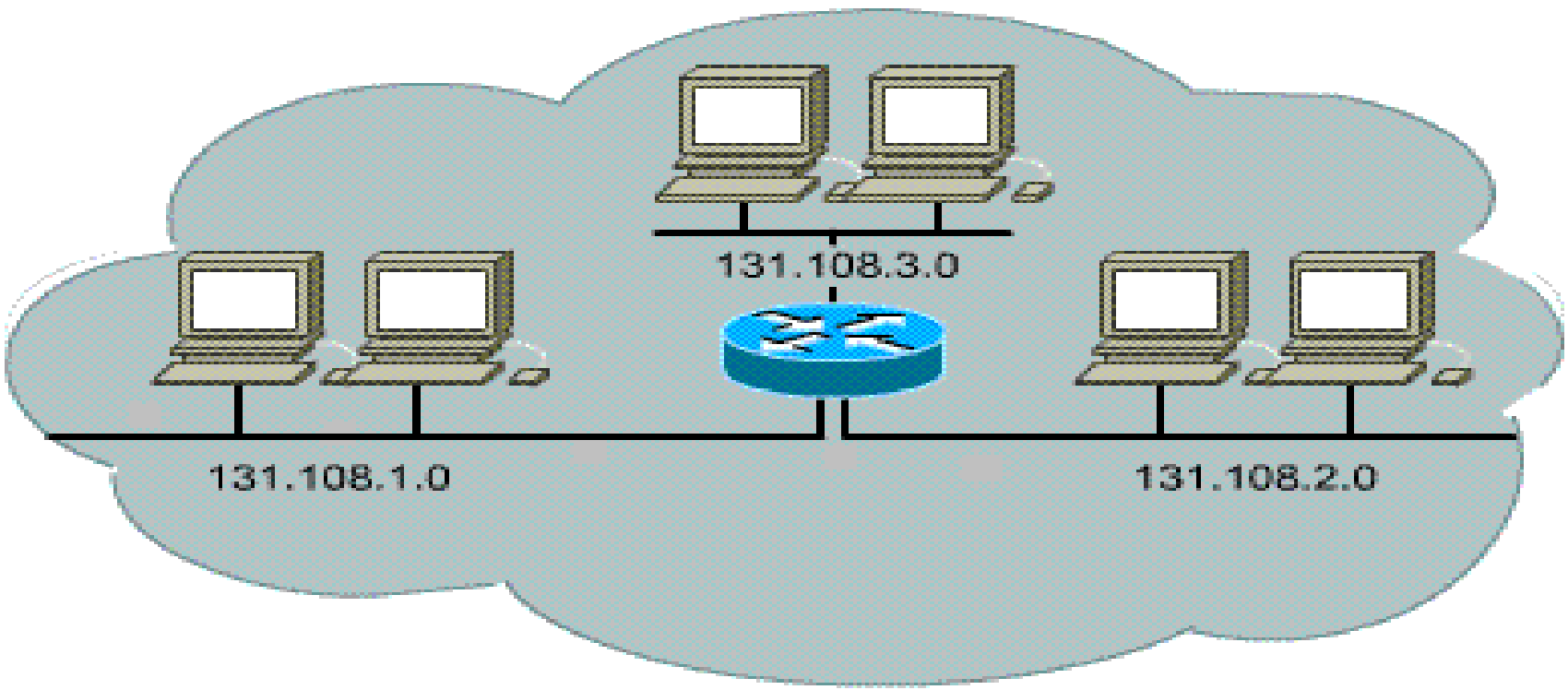
The 32-Bit Binary IP Address



Numbers That Show Up In Subnet Masks (Memorize Them!)

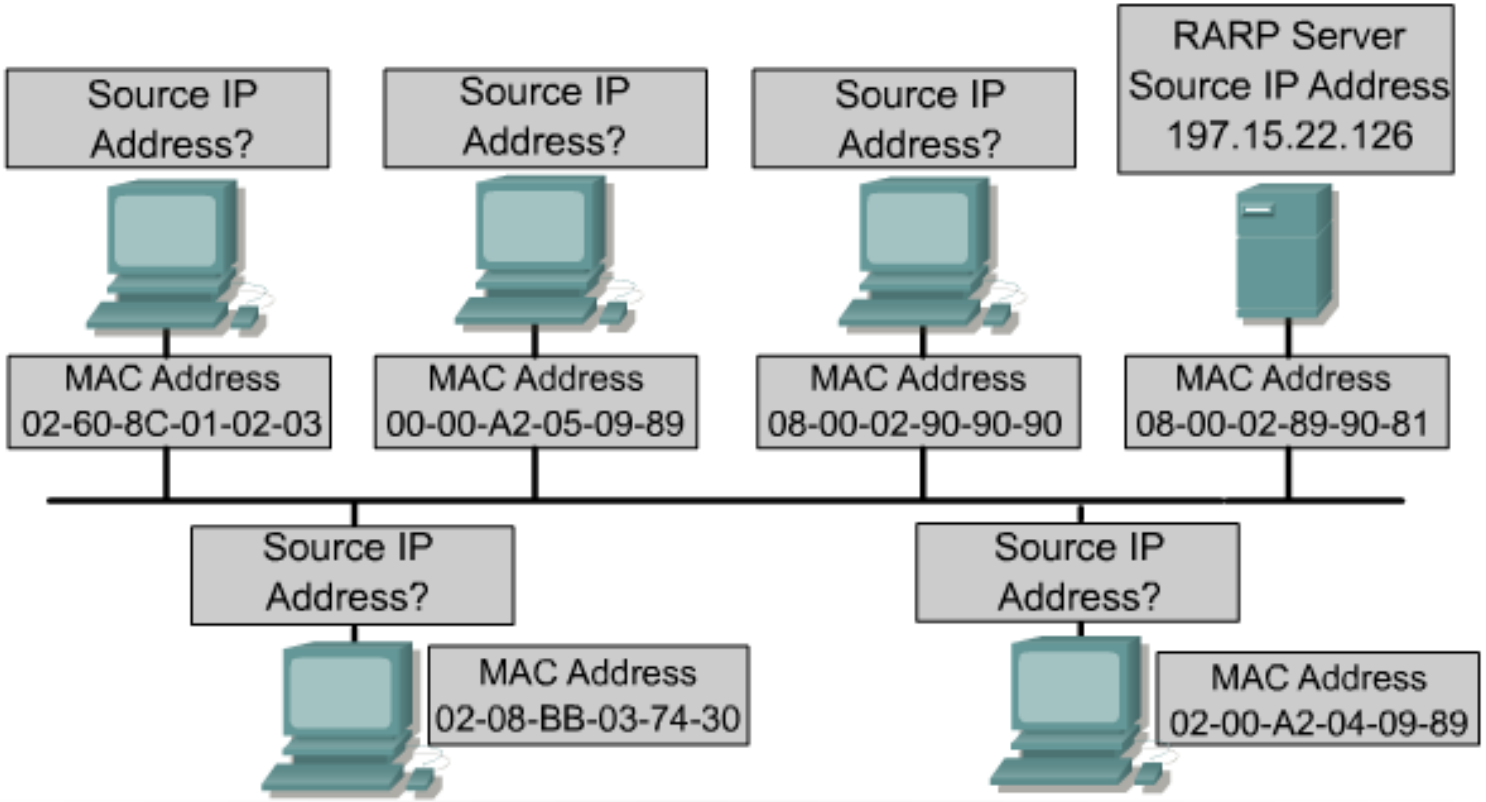
128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255

Addressing with Subnetworks



Internally, networks may be divided into smaller networks called sub-networks, or simply sub-nets. By providing a third level of addressing, sub-nets provide extra flexibility for the network administrator. For example, a class "B" network provided by the InterNIC, can be broken up into many sub-networks. In this example,131.108.1.0, 131.108.2.0, and 131.108.3.0 are all sub-nets within the network 131.108.0.0.

Obtaining an Internet Address



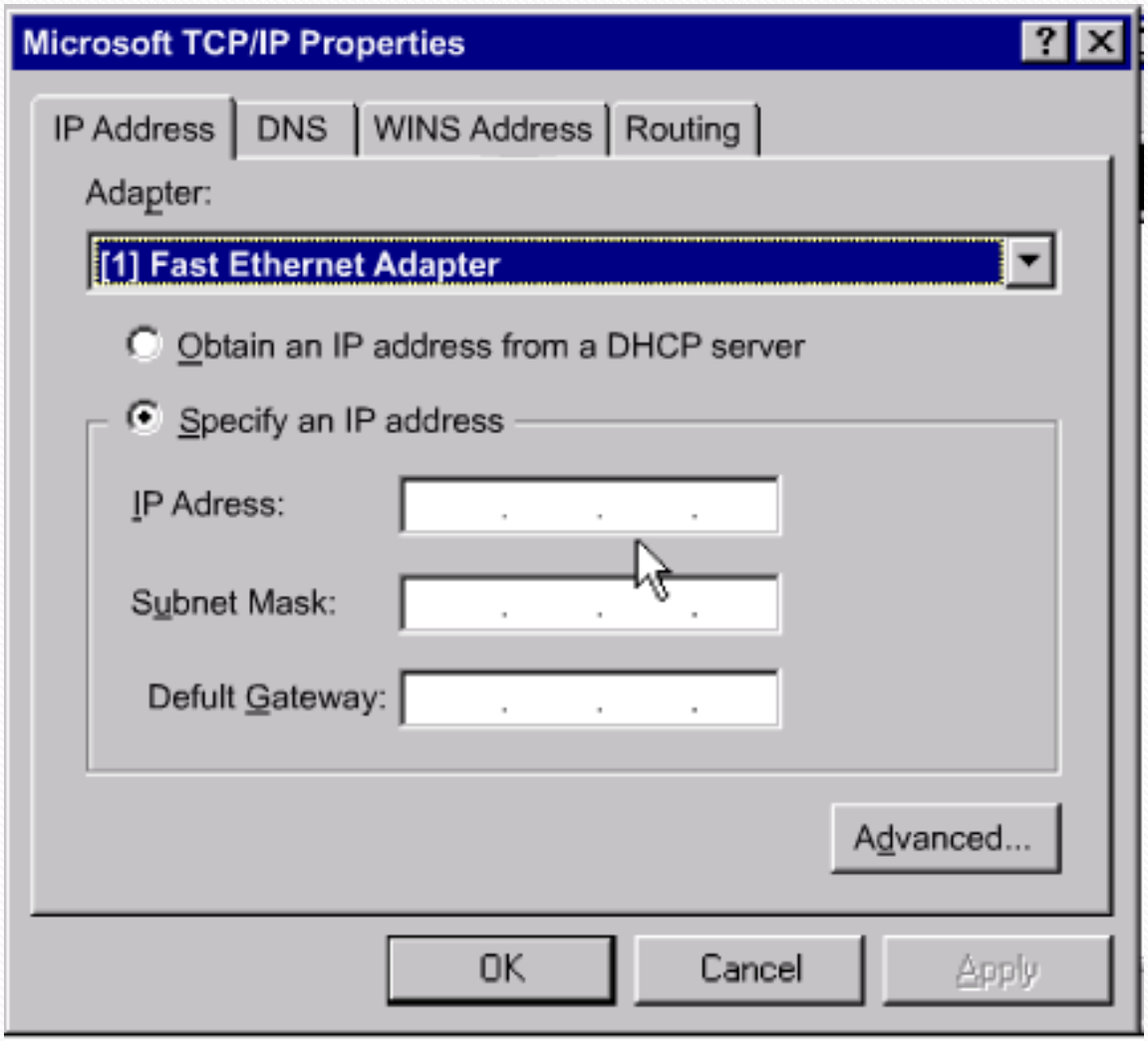
The hosts have a physical address by having a network interface card that allows connection to the physical medium. IP addresses have to be assigned to the host in some method. The two methods of IP address assignment are static or dynamic.

Static Assignment of an IP Address

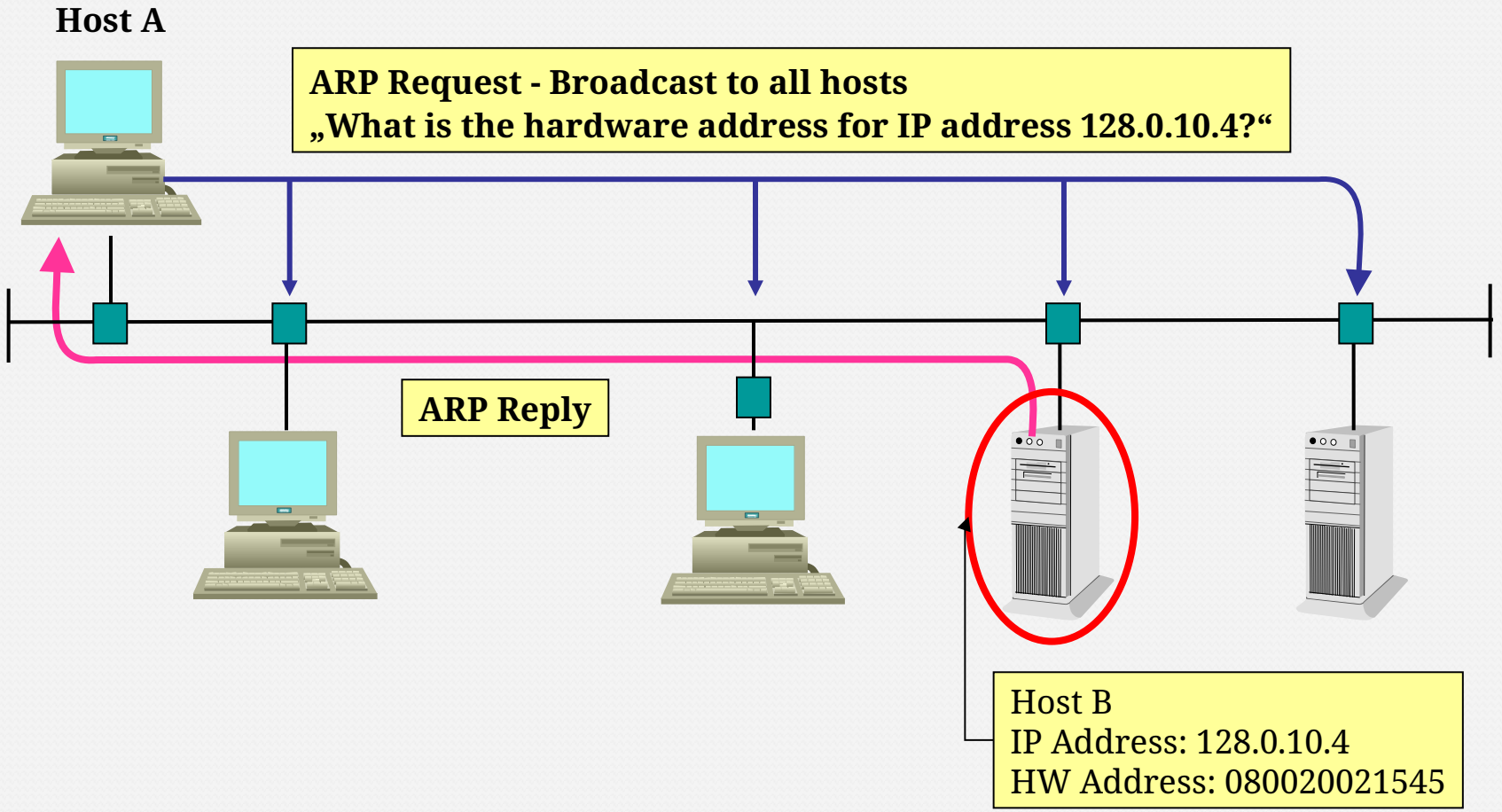
Static assignment works best on small networks.

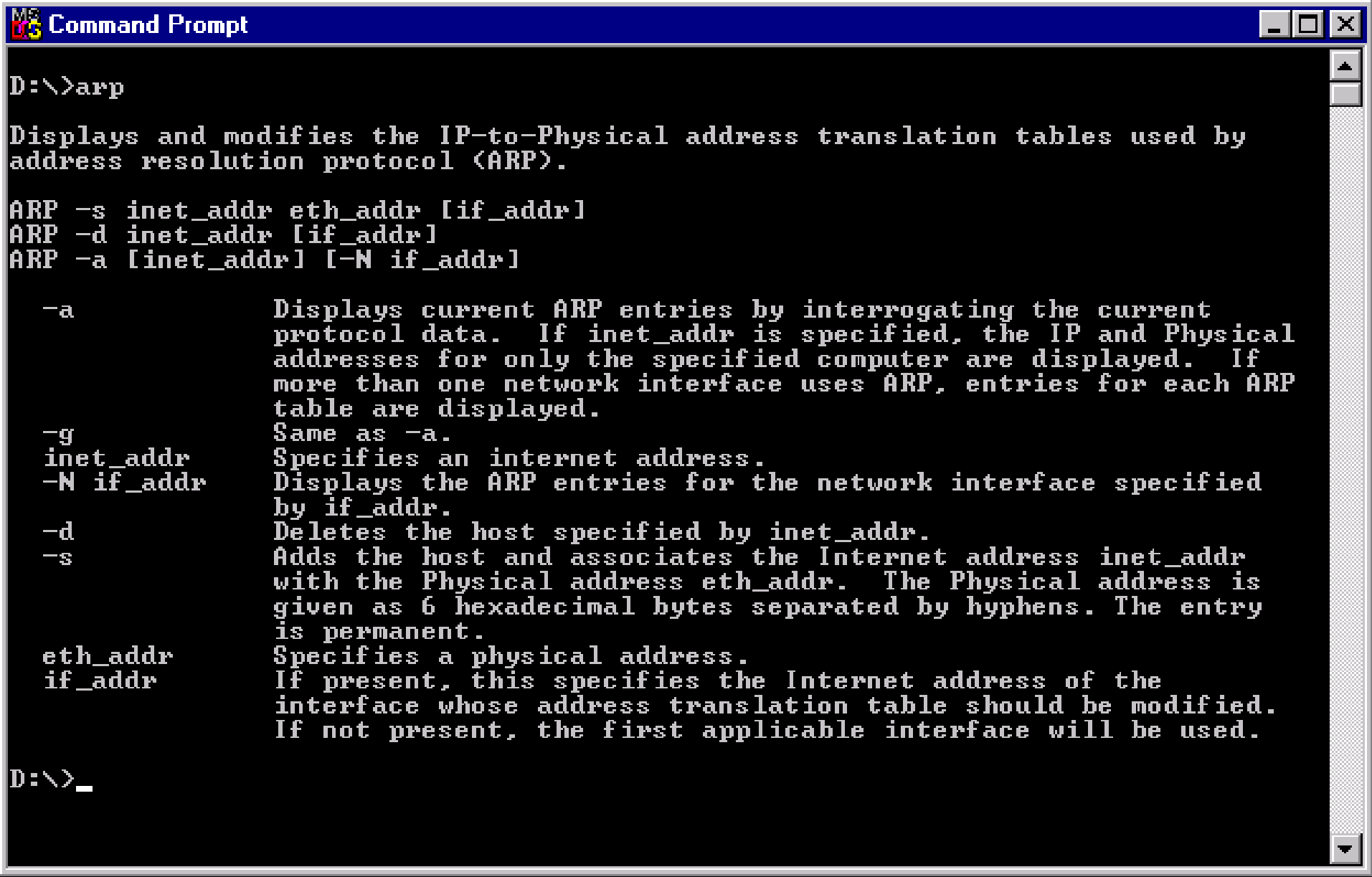
The administrator manually assigns and tracks IP addresses for each computer, printer, or server on the intranet.

Network printers, application servers, and routers should be assigned static IP addresses.

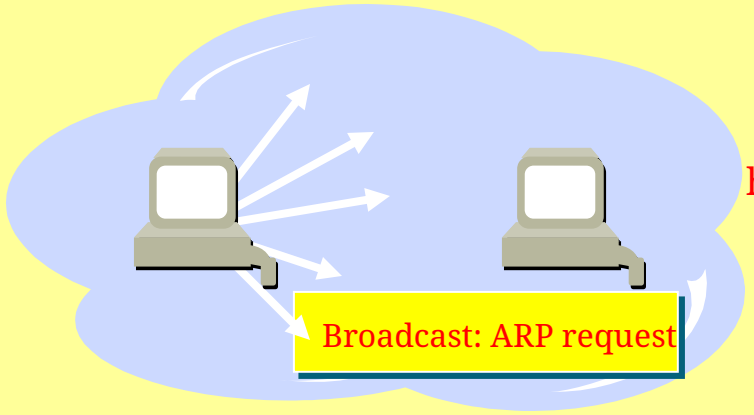


ARP (Address Resolution Protocol)



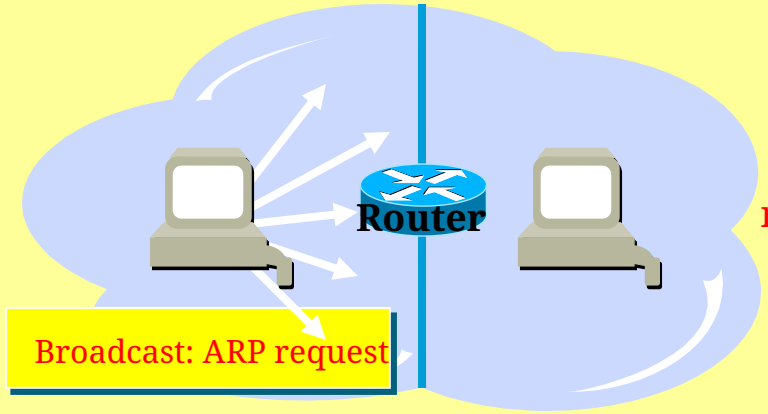

Command Prompt
D:\>arp
Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
-g Same as -a.
inet_addr Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified by if_addr.
-d Deletes the host specified by inet_addr.
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.
D:\>

1 Network = 1 Broadcast Domain

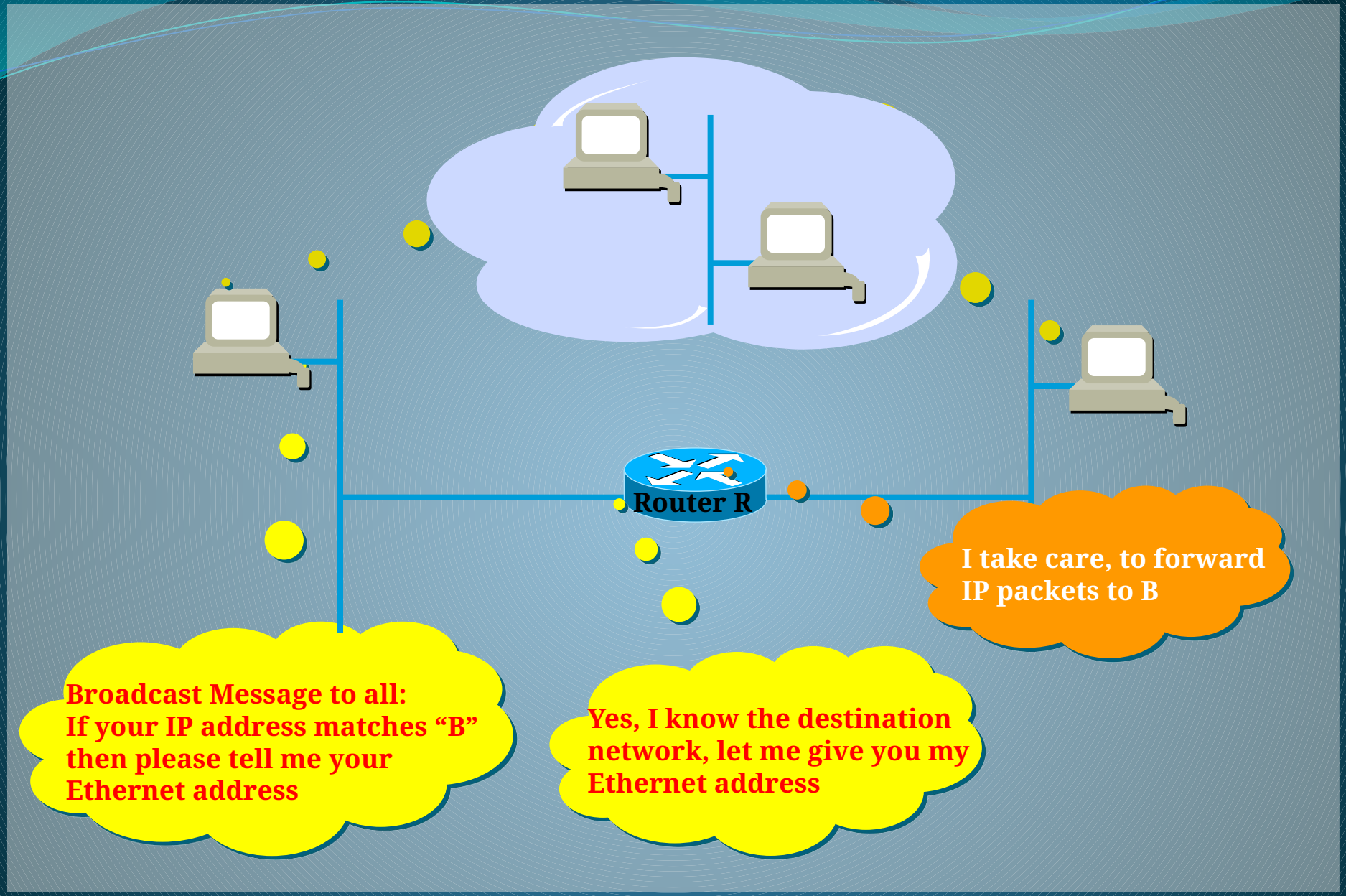


host B would reply

2 Networks = 2 Broadcast Domains



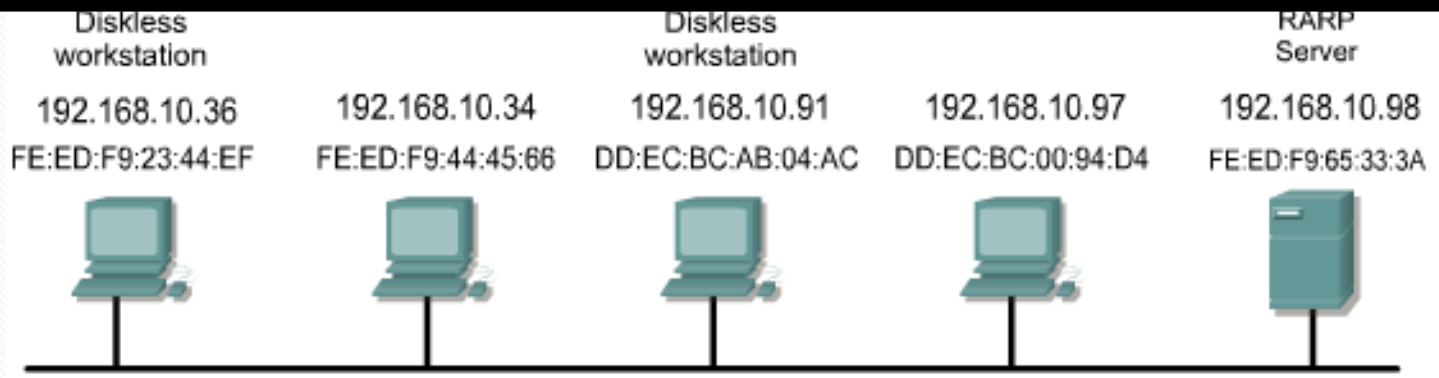
no one would reply


Router R
I take care, to forward IP packets to B
Broadcast Message to all: If your IP address matches “B” then please tell me your Ethernet address
Yes, I know the destination network, let me give you my Ethernet address

RARP

Reverse Address Resolution Protocol (RARP) associates a known MAC addresses with an IP addresses.

A network device, such as a diskless workstation, might know its MAC address but not its IP address. RARP allows the device to make a request to learn its IP address.
Devices using RARP require that a RARP server be present on the network to answer RARP requests.



Computer FE:ED:F9:23:44:EF stores the IP address received in the RARP reply for later use.

BootP

The bootstrap protocol (BOOTP) operates in a client-server environment and only requires a single packet exchange to obtain IP information.

However, unlike RARP, BOOTP packets can include the IP address, as well as the address of a router, the address of a server, and vendor-specific information.

One problem with BOOTP, however, is that it was not designed to provide dynamic address assignment. With BOOTP, a network administrator creates a configuration file that specifies the parameters for each device.The administrator must add hosts and maintain the BOOTP database.

Even though the addresses are dynamically assigned, there is still a one to one relationship between the number of IP addresses and the number of hosts.

This means that for every host on the network there must be a BOOTP profile with an IP address assignment in it. No two profiles can have the same IP address.

DHCP

Dynamic host configuration protocol (DHCP) is the successor to BOOTP.

Unlike BOOTP, DHCP allows a host to obtain an IP address dynamically without the network administrator having to set up an individual profile for each device.

All that is required when using DHCP is a defined range of IP addresses on a DHCP server.As hosts come online, they contact the DHCP server and request an address.

The DHCP server chooses an address and leases it to that host.

With DHCP, the entire network configuration of a computer can be obtained in one message.

This includes all of the data supplied by the BOOTP message, plus a leased IP address and a subnet mask.

The major advantage that DHCP has over BOOTP is that it allows users to be mobile.