Chapter 2 - Part 2

The TCP/IP Protocol:
The Language of the Internet

Private IP Addresses

- RFC 1918 designates some class A, B, and C addresses as reserved
  - Designed for use in private networks
  - Internet routers will not forward packets with these destination addresses
- Class A private address range
  - 10.0.0.0 - 10.255.255.255
- Class B private address range
  - 172.16.0.0 - 172.31.255.255
- Class C private address range
  - 192.168.0.0 - 192.168.255.255

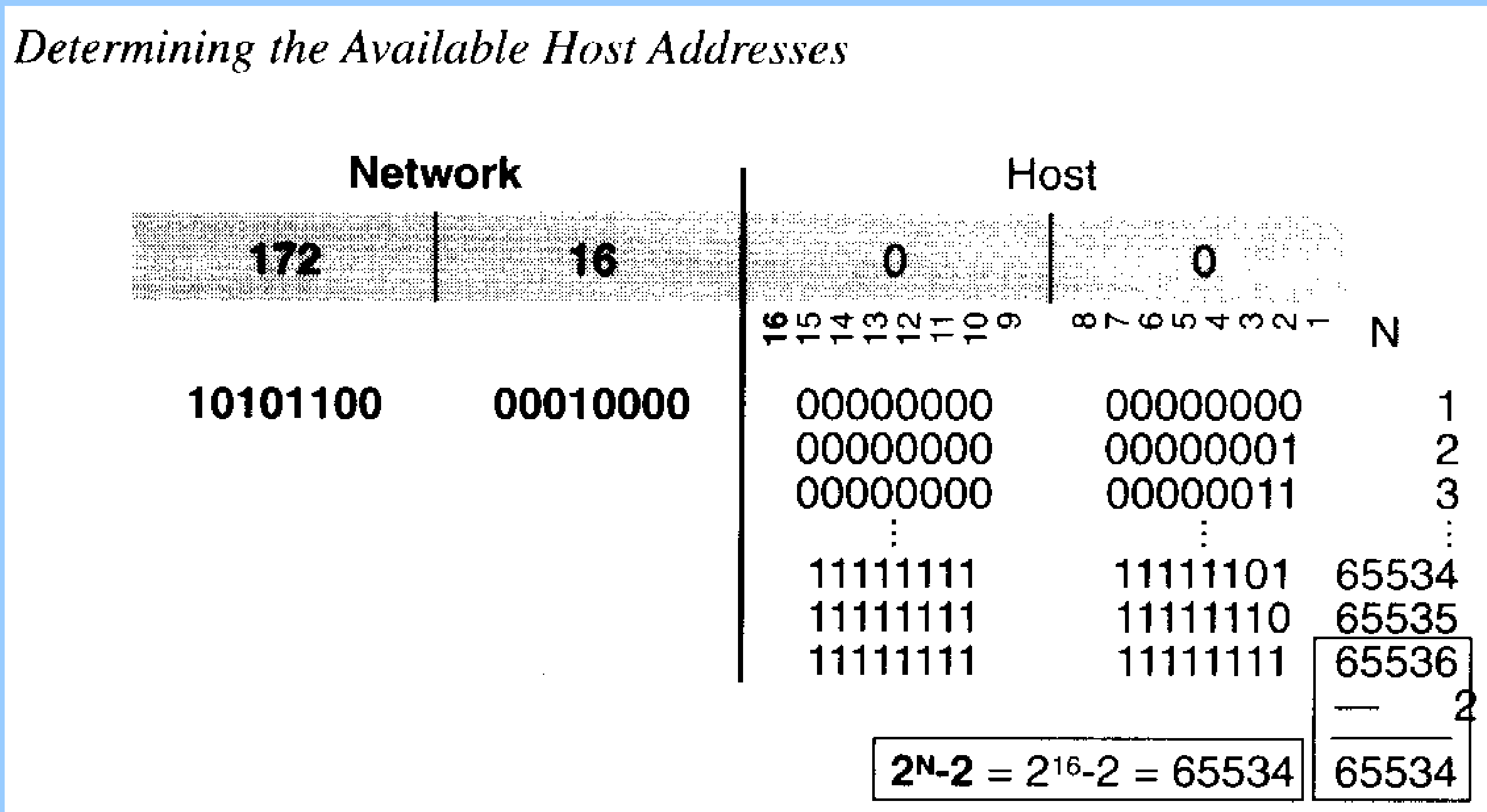
Host Addresses

- Each device or interface on a network must have a non-zero host number
- Special host addresses
  - Host address zero is given to the network wire itself
  - A host address of all 1s is the direct broadcast address
    - Packet that should be received by all hosts on the network
- Number of possible hosts on a network = 2^N-2
  - N is number of host bits
  - Example: Class B address has 16 host bits
    - Maximum number of possible hosts is $2^{16}-2 = 65,536-2 = 65,534$

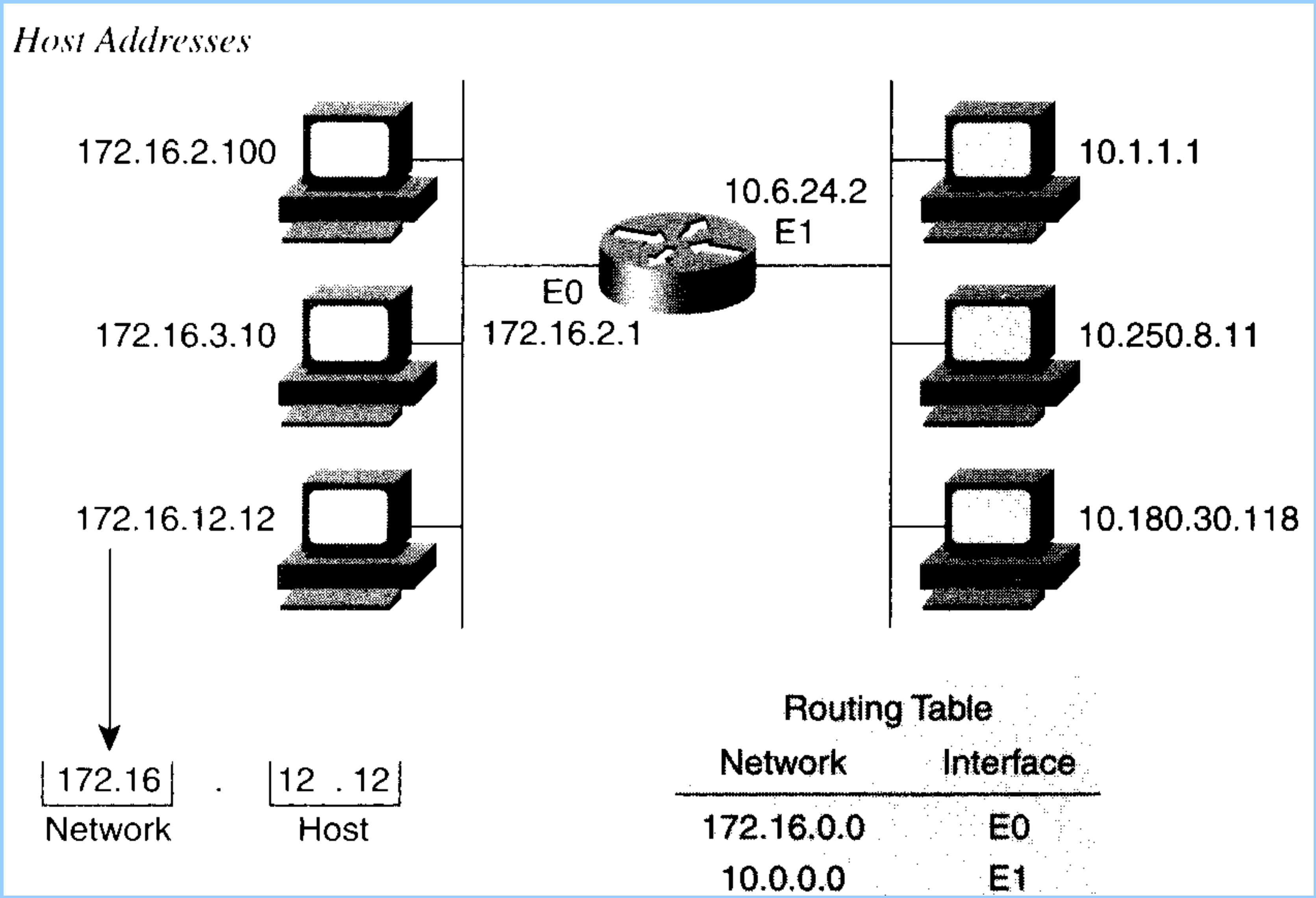
Summary of Special Addresses

Special Address	Network Number	Host Number	Source or Destination
Network address	Specific	All 0s	None
Direct broadcast address	Specific	All 1s	Destination
Flooded broadcast address	All 1s	All 1s	Destination
This host on this network	All 0s	All 0s	Source
Specific host on this network	All 0s	Specific	Destination
Loopback address	127	Any	Destination

Determining Available Host Addresses



Example of Host Addresses



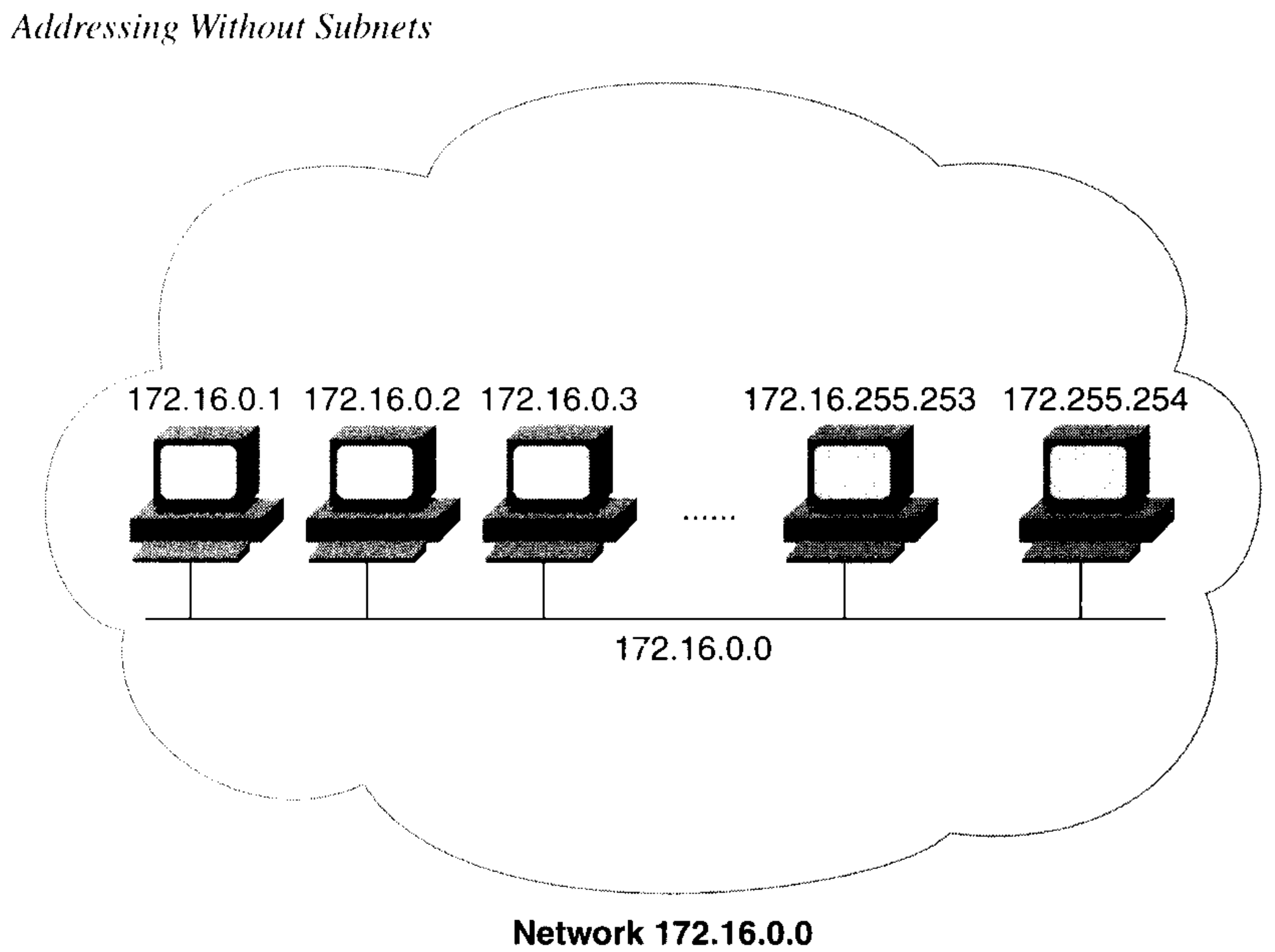
IP Addresses and Routers

- Datagrams addressed to a specific network are all treated the same regardless of the host ID
- Routers look at the network number only
- Routing table will have address entries like

Network	Interface
172.16.0.0	E0
10.0.0.0	E1

  - All packets with destination address having the first two octets as 172.16 will be sent out router interface number E0
  - Routing tables can be kept short by using network addresses

Addressing Without Subnets



Addressing Without Subnets

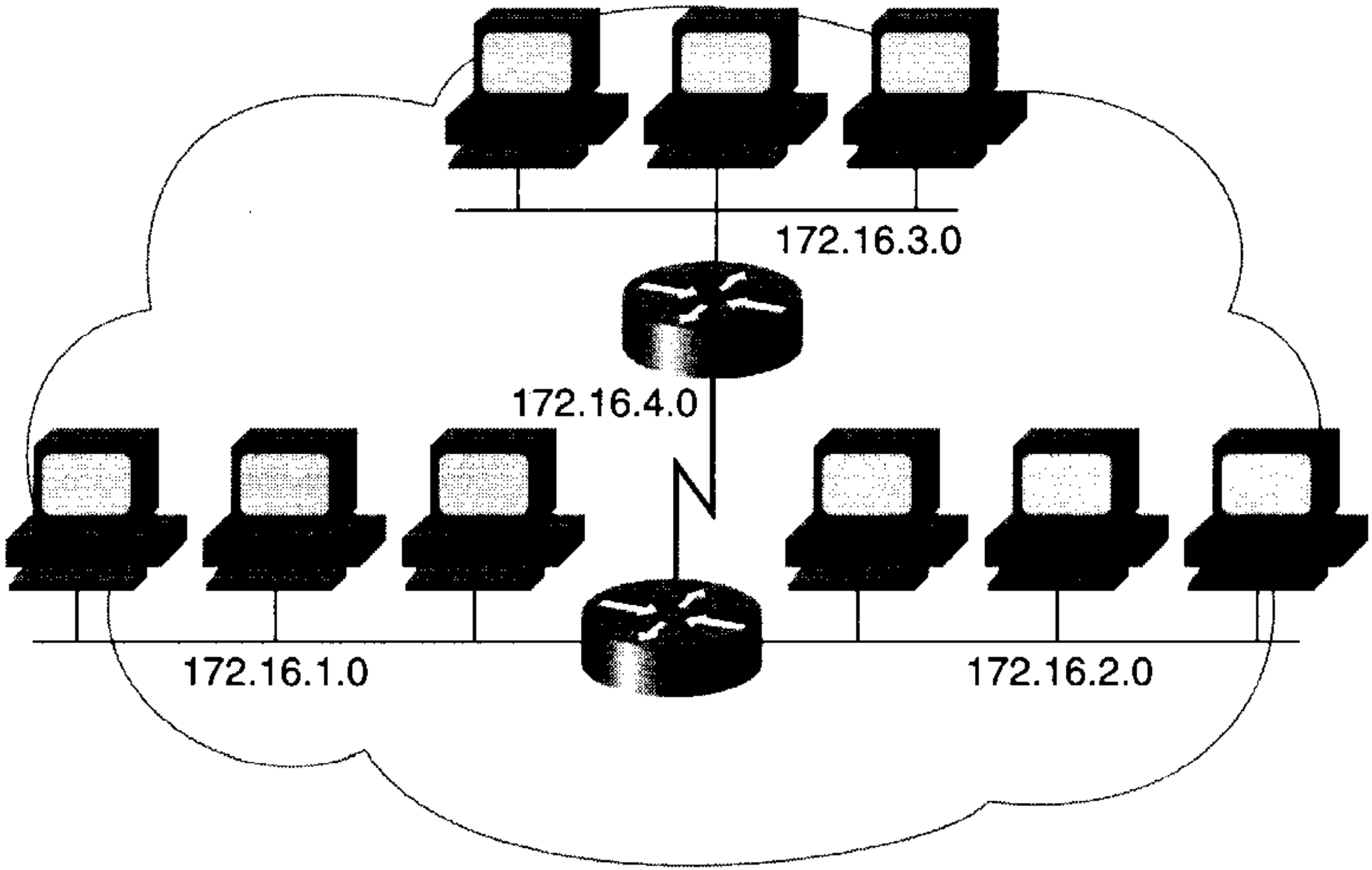
- This example is an Ethernet network having a class B network address with up to 65,634 hosts
- Ethernets can be divided into smaller collision domains by bridges and switches
  - Isolates some MAC traffic and MAC broadcasts
  - IP broadcasts are not controlled and are forwarded to all segments and hosts of bridged and switched networks
    - Such broadcasts can reduce network performance
    - Example: ARP broadcasts

Subnet Addresses

- Large networks are divided into smaller *subnets* to improve network capacity utilization
  - Network administrators determine the subnet plan
- Subnets are isolated by routers
- Broadcasts within each subnet are confined to the subnet
- Routers forward traffic between subnets
- One disadvantage of subnets is that the number of usable host addresses is reduced

Subnet Addresses

Addressing with Subnets



Network 172.16.0.0

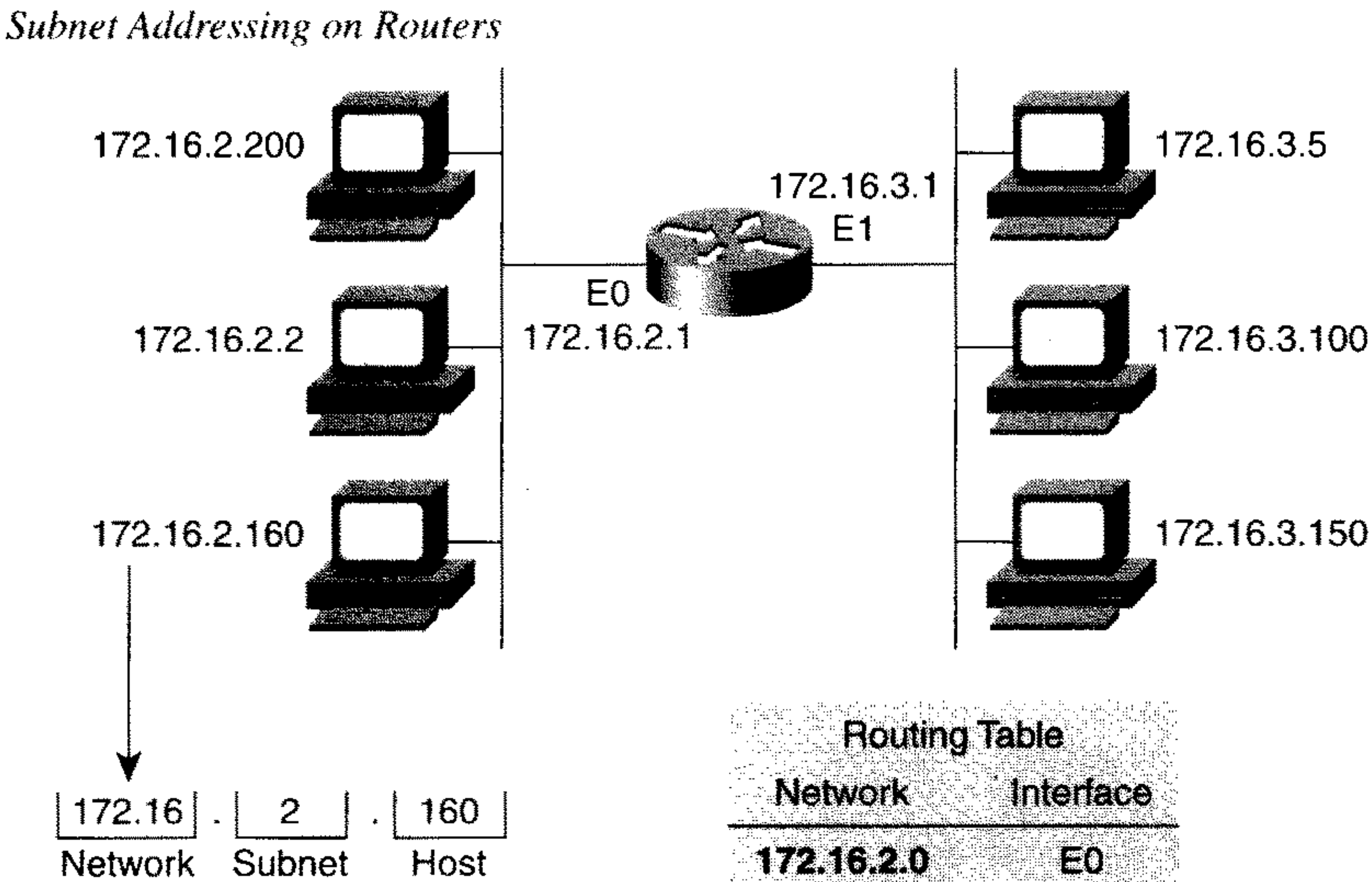
Subnet Addresses

- In this example, network 172.16.0.0 is divided into 4 subnets
  - 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0
- Third octet is being used to identify the subnet

Subnet Masks

- Network devices use the subnet mask to decide the network number, subnet number and host number
- Subnet mask structure
  - Has a contiguous number of 1s for occupying the bit positions for the network and subnet numbers
  - Followed by a contiguous number of 0s in the bit positions for the host number
  - Subnet bits are taken from the host field of the address
- *Subnetting does not affect the class of the IP address*

Subnetting Addressing and Routers



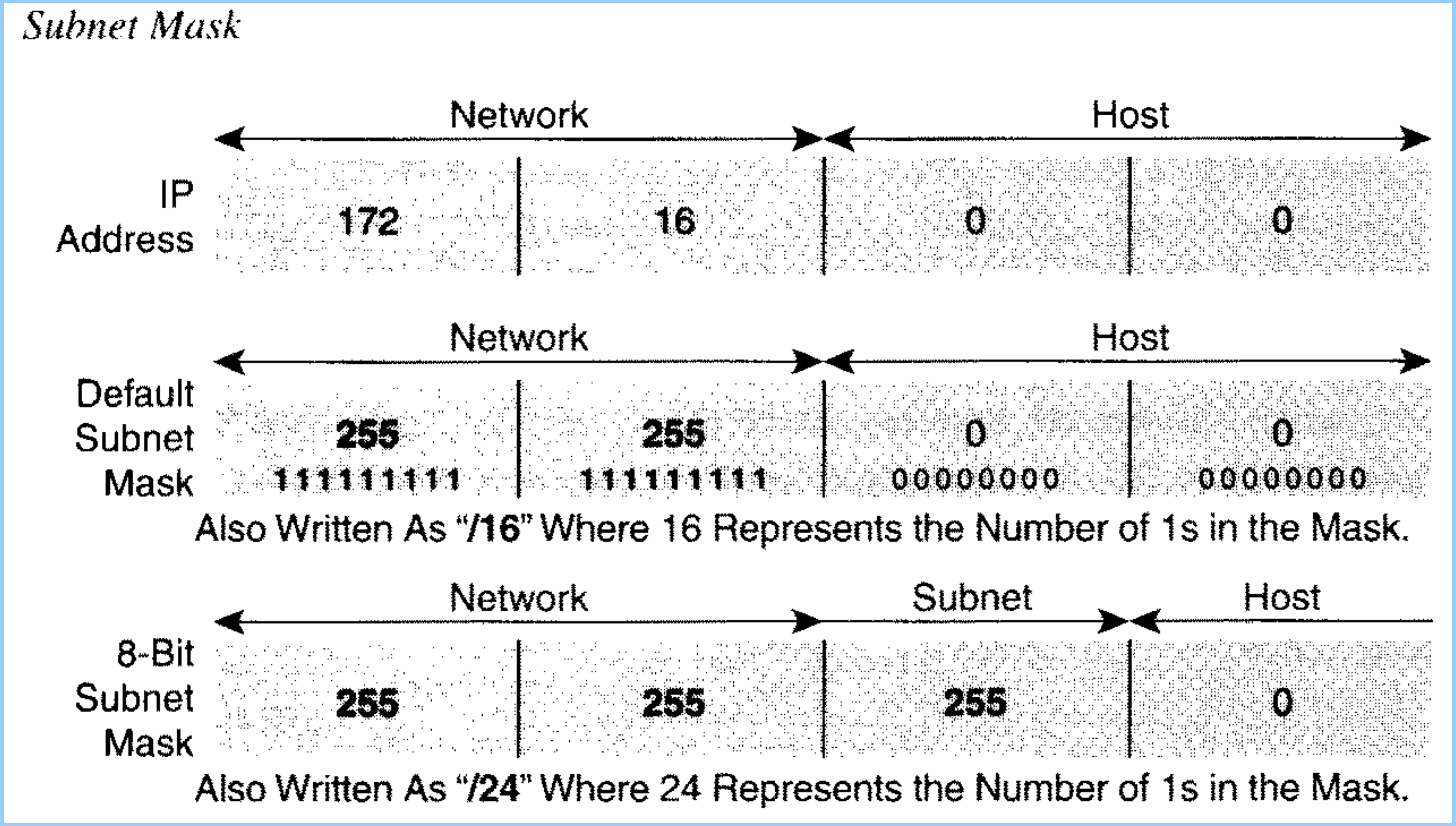
Routing Table

Network	Interface
172.16.2.0	**E0**
172.16.3.0	**E1**

Subnetting Addressing and Routers

- Routing table in this example identifies network by the subnet number

Subnet Mask Structure



Subnet Mask Structure

- Note that the “default” subnet mask has 1s for the network bits only
- Two popular ways to write IP address and subnet mask are
  - 172.16.0.0 255.255.0.0
  - 172.16.0.0/16
    - /16 implies 16 contiguous 1s starting at left of mask

Possible Subnet Masks

- Convention is to use contiguous bits for masks
  - No zeros between 1s

Subnet Mask Patterns

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

Using the Subnet Mask

- Receiving router extracts the IP address from the packet and gets subnet mask from receiving interface
- Router ANDs mask with address to extract network number
- Rest of address is host number

Using the Default Subnet Mask

Default Subnet Mask

	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

Subnet Not In Use — the Default

Extending Subnet Mask by 8 bits

Extending the Mask by 8 Bits

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.$\boxed{255}$.0	11111111	11111111	**11111111**	00000000
	10101100	00010000	**00000010**	00000000
			128 192 224 240 248 252 254 $\boxed{255}$	
Network Number	172	16	2	0

Subnet Masks Not on Octet Boundaries

Extending the Mask by 10 Bits

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000
			128 192 224 240 248 252 254 255	128 192 224 240 248 252 254 255
Network Number	172	16	2	128

Subnet Masks Not on Octet Boundaries

- In this example, how many possible subnetworks are there?
- How many possible hosts are there?

Subnet Masks Not on Octet Boundaries

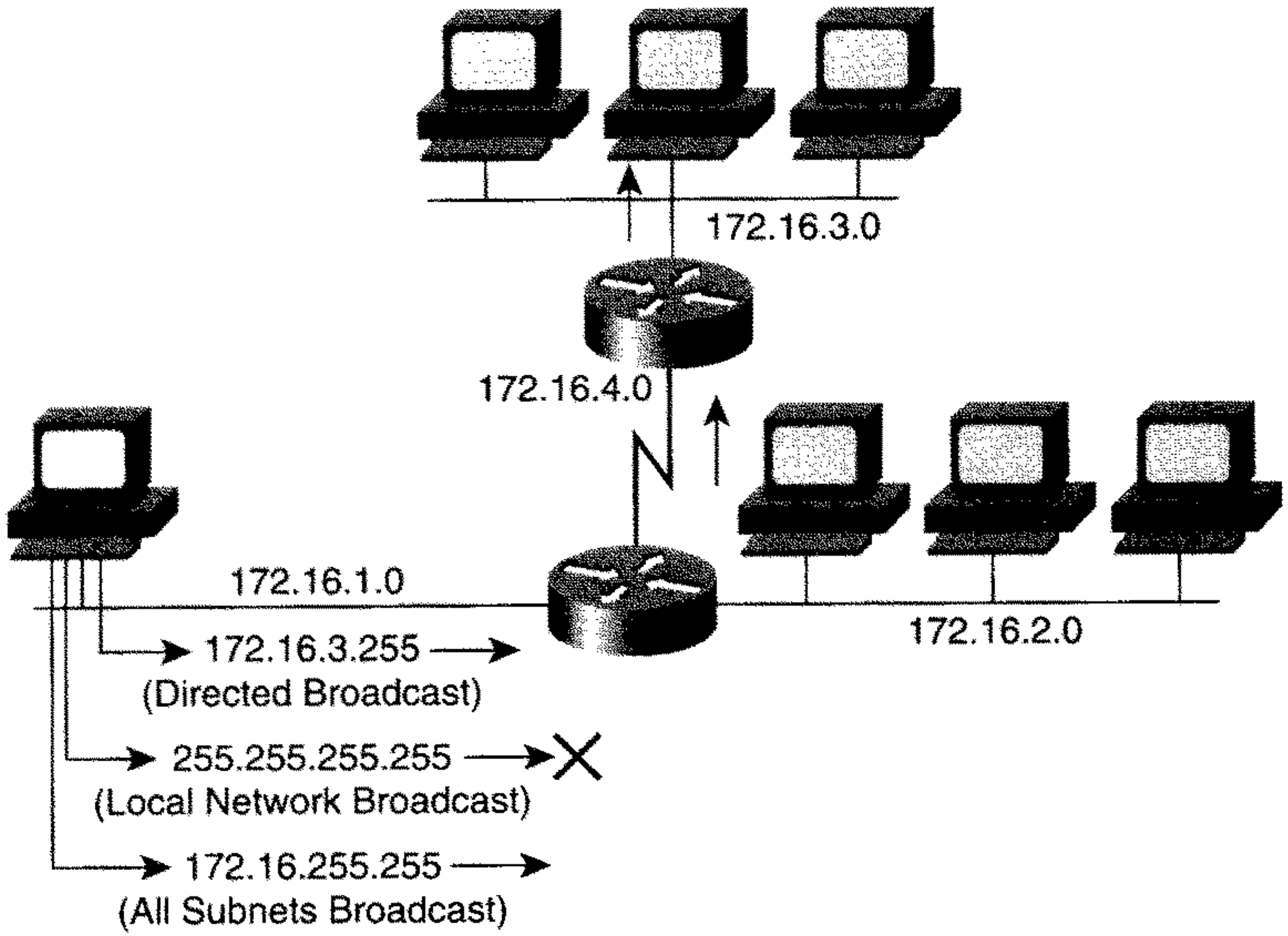
- In this example, how many possible subnetworks are there?
  - $2^{Ns}-2 = 2^{10}-2 = 1022$
  - Ns = number of subnet bits
- How many possible hosts are there?
  - $2^{Nh}-2 = 2^{6}-2 = 62$
  - Nh = number of host bits

Broadcasts

- Three kinds
  - Flooding
    - IP address 255.255.255.255
    - Local only, router does not propagate
  - Directed broadcasts
    - 1s in host portion
    - Router will forward to network
    - Example: network 172.16, subnet 3
      - 172.16.3.255
  - All subnets broadcast
    - 1s in subnet portion and host portion of address
    - Example: network 172.16, all subnets
      - 172.16.255.255

Broadcasts

Broadcast Addresses



Identifying IP Addresses

Step 1	Write the 32-bit address in binary notation.
Step 2	Write the 32-bit subnet mask in binary just below it.
Step 3	Draw a vertical line just after the last contiguous subnet mask 1 bit.
Step 4	In a row just below, place all 0s for the remaining free spaces (to the right of the line). This will be the subnet.
Step 5	In the next row, to the right of the line, place all 1s until you reach the 32-bit boundary. This will be the broadcast address.
Step 6	On the right side of the line in the next row, place all 0s in the remaining free spaces until you reach the last free space. Place a 1 in that free space. This will be your first usable address.
Step 7	On the right side of the line in the next row, place all 1's in the remaining free spaces until you reach the last free space. Place a 0 in that free space. This will be your last usable address.
Step 8	Copy down all the bits you wrote in Step 1 for the bit fields to the left of the line for all four lines.
Step 9	Convert the bottom four rows back to dotted-decimal.

Identifying IP Addresses

Calculating Address Space

	172	16	2	160	
				3	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
9	8				
172.16.2.128	10101100	00010000	00000010	10000000	Subnet 4
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast
					5
172.16.2.129	10101100	00010000	00000010	11000001	First 6
172.16.2.190	10101100	00010000	00000010	10111110	Last 7

Identifying IP Addresses

- This method allows you to find the subnet, and the broadcast, first, and last addresses on the subnet

Subnet Example

Subnet Example

IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	**11111111**	00000000
Subnet:	10101100	00010000	**00000010**	00000000
Broadcast:	10101100	00010000	00000010	11111111

Subnet Address = 172.16.2.0
Host Addresses = 172.16.2.1–172.16.2.254
Broadcast Address = 172.16.2.255
Eight Bits Of Subnetting

Class B Subnets

Class B Subnet Table

Number of Bits	Subnet Mask	Number of Subnets	Number of Hosts
2	255.255.192.0	2	16,382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16,382	2

Routing Table

- Routers and workstations maintain routing tables so they know where to send IP packets
- Given a destination IP address for the packet to be sent, the device looks in its routing table to find which interface the packet must be sent out

Workstation Routing Table

MS-DOS Prompt

```
C:\WINDOWS>netstat -r

Route Table

Active Routes:

  Network Address          Netmask  Gateway Address        Interface  Metric
          0.0.0.0          0.0.0.0     168.28.186.1    168.28.186.54       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
     168.28.186.0  255.255.255.192    168.28.186.54    168.28.186.54       1
    168.28.186.54  255.255.255.255        127.0.0.1        127.0.0.1       1
   168.28.255.255  255.255.255.255    168.28.186.54    168.28.186.54       1
        224.0.0.0        224.0.0.0    168.28.186.54    168.28.186.54       1
  255.255.255.255  255.255.255.255    168.28.186.54    168.28.186.54       1

Active Connections

  Proto  Local Address          Foreign Address          State
  TCP    Tigger:1146            unknown.Level3.net:80    CLOSE_WAIT

C:\WINDOWS>
```

Interpreting the Table

- Network address
  - Destination address
  - Four types
    - Host address
      - Route to a single, specific destination IP address
    - Subnet address
      - Route to a subnet
    - Network address
      - Route to an entire network
    - Default gateway
      - Route used when there is no other match

Interpreting the Table

- Netmask
  - Defines the portion of the network address that must match in order for that route to be used
- Gateway address
  - Where the packet must be sent
  - Can be the local network card address or the address of the gateway (router) on the local subnet
- Interface
  - Address of the network card through which the packet should be sent

Interpreting the Table

- Metric
  - Number of hops to the destination
    - Anything on the local subnet is one hop
    - Each router crossed adds one to the metric

Address Resolution Protocol (ARP)

- When a host wants to send an IP packet, it must be encapsulated in a frame that includes the destination MAC address
  - The host does not usually know the destination address
- ARP is used to find a physical (MAC) address when the IP address is known
- Defined in RFC 826

Basic ARP Operation

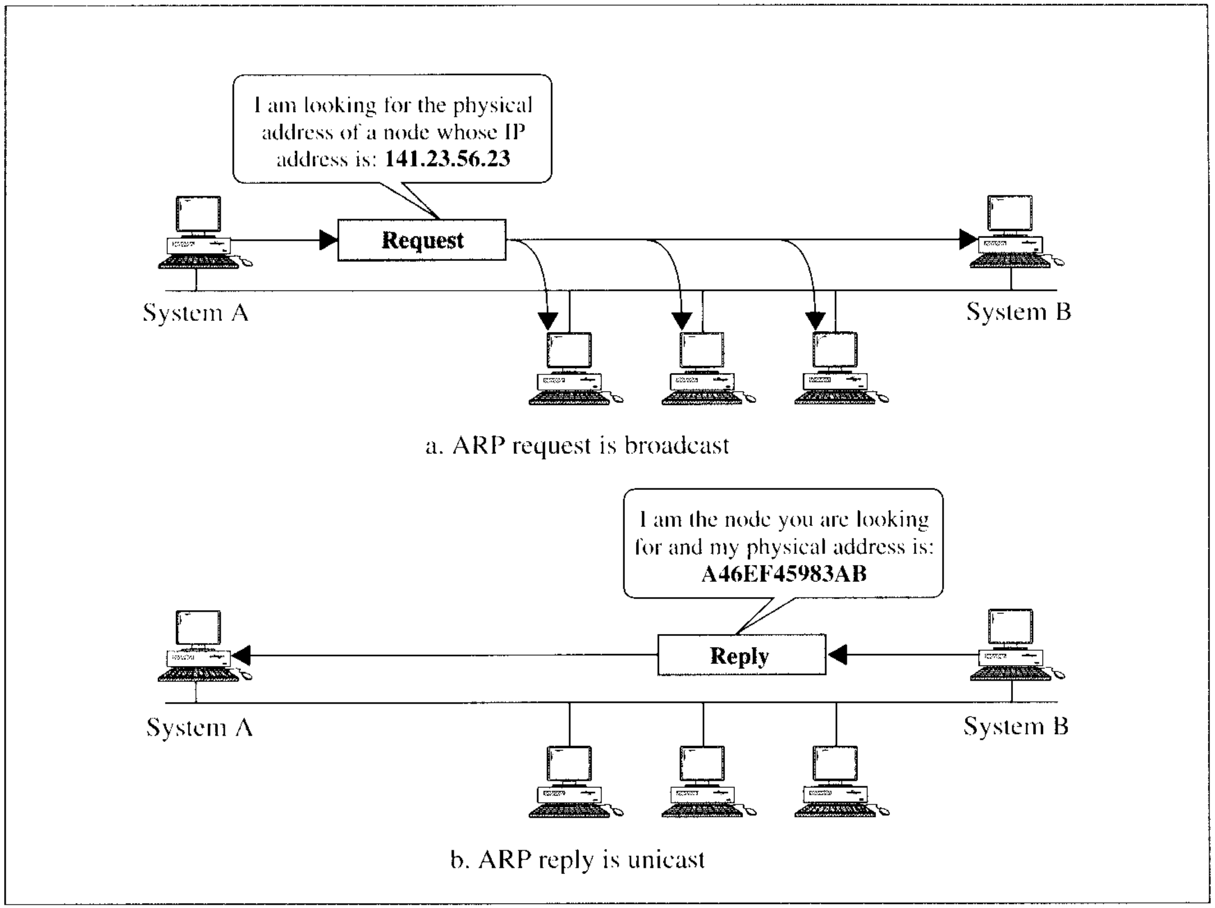
- To find the MAC address,
  1. The sending host *broadcasts* an ARP request to all entities on its network
  2. The entity with the IP address matching the one in the request sends an ARP Reply directly to the requesting host (unicast)
     - The reply contains the relying host's MAC address in its source address field
     - The original sending host now knows the MAC address of the entity it wants to send the packet to

Basic ARP Operation

3. If there is no reply to the request, the sending host sends the data packet to the default gateway router
   - It may have to send an ARP request to get the router's MAC address
   - The packet sent to the router has as its destination IP address that of the desired destination entity but the destination MAC address is now the router
   - The router must now determine the next place to send the packet
     - If the destination network is directly attached to the router, it will send an ARP request to that network to get the final destination MAC address
     - If the network is not directly attached, the packet is sent to the next-hop router

ARP Operation

Figure 8.2 *ARP operation*



- B. Forouzan, TCP/IP Protocol Suite, New York, McGraw-Hill, 2000

Domain Name Service (DNS)

- Users find it easier to remember names rather than addresses
  - Example:
    - www.spsu.edu identifies the SPSU web server
    - Your browser still needs an IP address to communicate with it, even for the first time
    - Your computer sends a request to a domain name server to translate the name into an IP address

Domain Name Service (DNS)

- For some instances a fixed lookup table residing on your computer is sufficient
  - Example:
    - The name localhost is stored in a table and has corresponding address 127.0.0.1
- The purpose of DNS is to resolve symbolic names into IP addresses

DNS Components

- Three elements
  - Domain name space
  - Name servers
  - Resolvers

Computer Names

- Names have alphanumeric segments separated by periods
- Number of segments is variable
- Names are hierarchical
  - Most significant part is on right
  - This is the *Top Level Domain* (TLD)

Domain Names

- ***The domain part of the name is all segments but the left-most***
- **TLD of the name is determined by DNS**
  - ***com*** **is commercial organization**
  - ***edu*** **is educational institution**
  - ***gov*** **is government**
  - ***mil*** **is military**
- **Leftmost part is the computer name**

Uniqueness of Name

- Organizations apply for names in a top-level domain:
  - spsu.edu
  - yahoo.com
  - slb.com
- Organizations determine their own internal structure
  - anadrill.slb.com
- All names are unique

Geographic TLDs

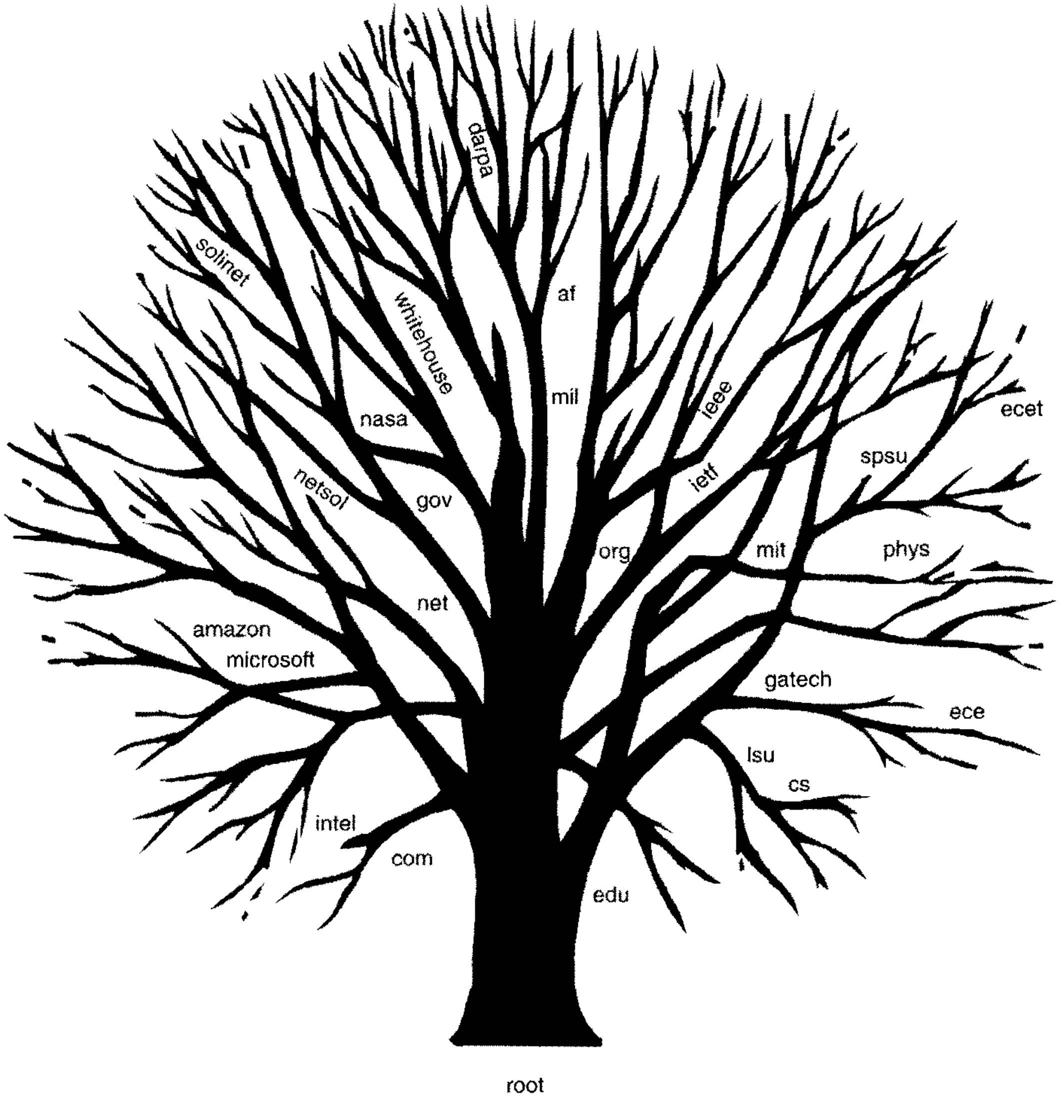
- Geographic registration is also used
- Often seen in addresses for foreign countries
  - ac.uk used in United Kingdom
  - ac stands for academic

DNS Structure

- Hierarchical tree structure
  - Base is root
  - Immediately above root are Top Level Domains
  - Above TLDs are subdomains
  - Eventually, leaves of tree represent hosts

DNS Structure

FIGURE 2.9
Domain name space (partial view).



Who Runs Top-Level Domain Servers?

- The Internet Corporation for Assigned Names and Numbers (ICANN) delegates responsibility for handling root domains
  - “ICANN has been recognized by the U.S. and other governments as the global consensus entity to coordinate the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system” – *ICANN Fact Sheet* (www.icann.org)
  - Example: Network Solutions (now Verisign) handles .com assignments
    - Soon to change, ICANN enabling competition

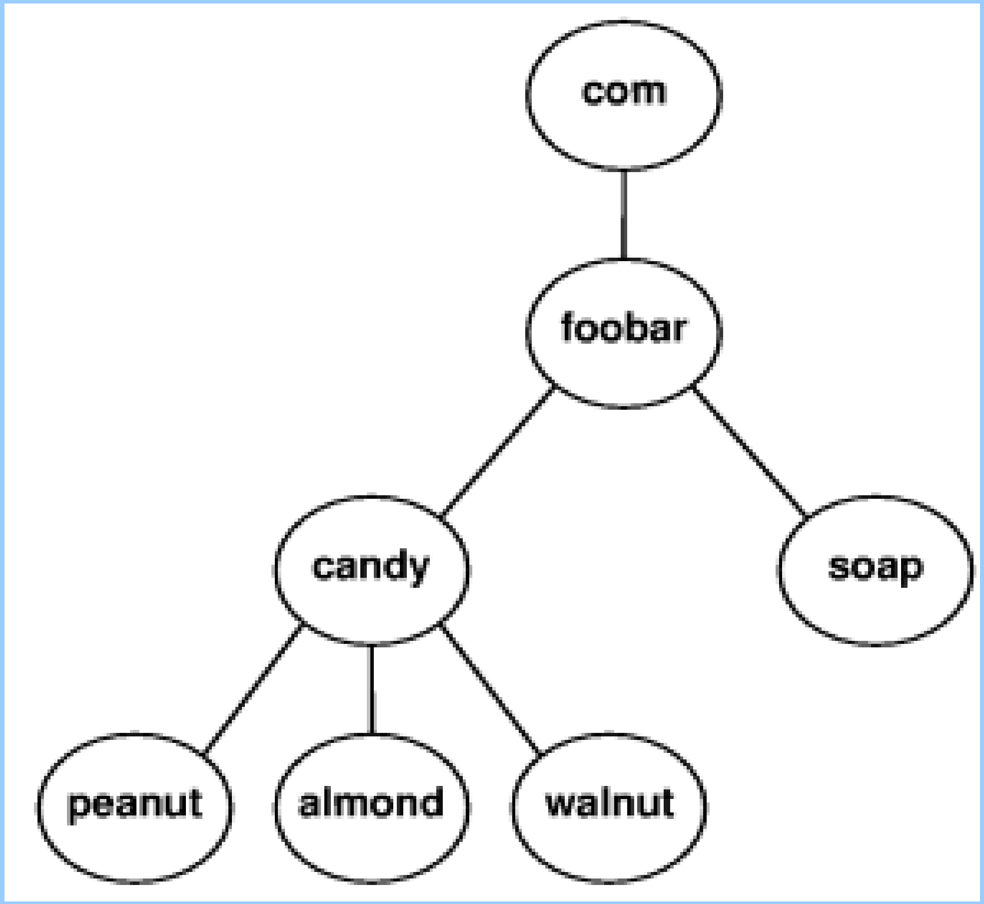
Who Runs Top-Level Domain Servers?

- TLD name servers know the IP addresses of DNS servers for every second-level domain
- An organization supplies the name of its second-level DNS server when registering for a second-level domain
  - Example: SPSU is a second-level domain and the .edu top level DNS server knows its IP address
  - Once you have a registered 2nd-level domain name, you are responsible for handling your subdomain naming structure

Domain Name & Tree Structure

- A domain name of an institution is formed by following a path starting at the institution's subdomain and ending at the root
  - Example:
    - Start at SPSU's ECET department
    - Next subdomain is SPSU
    - TLD is edu
    - Resulting domain name is ecet.spsu.edu
- Add host name to domain and you get the *Fully Qualified Domain Name* (FQDN)
  - The ECET department's web server computer name is www, so we have the FQDN www.ecet.spsu.edu

Example Domain Structure in an Organization



- D. Comer, Computer Networks and Internets With Internet Applications, 3ed., Upper Saddle River, NJ, Prentice-Hall, 2001

Name Servers

- DNS name servers store information describing the domain name space
- Servers have authority over regions of the domain name space called *zones*
- Zones may include a branch and all of its subordinate branches

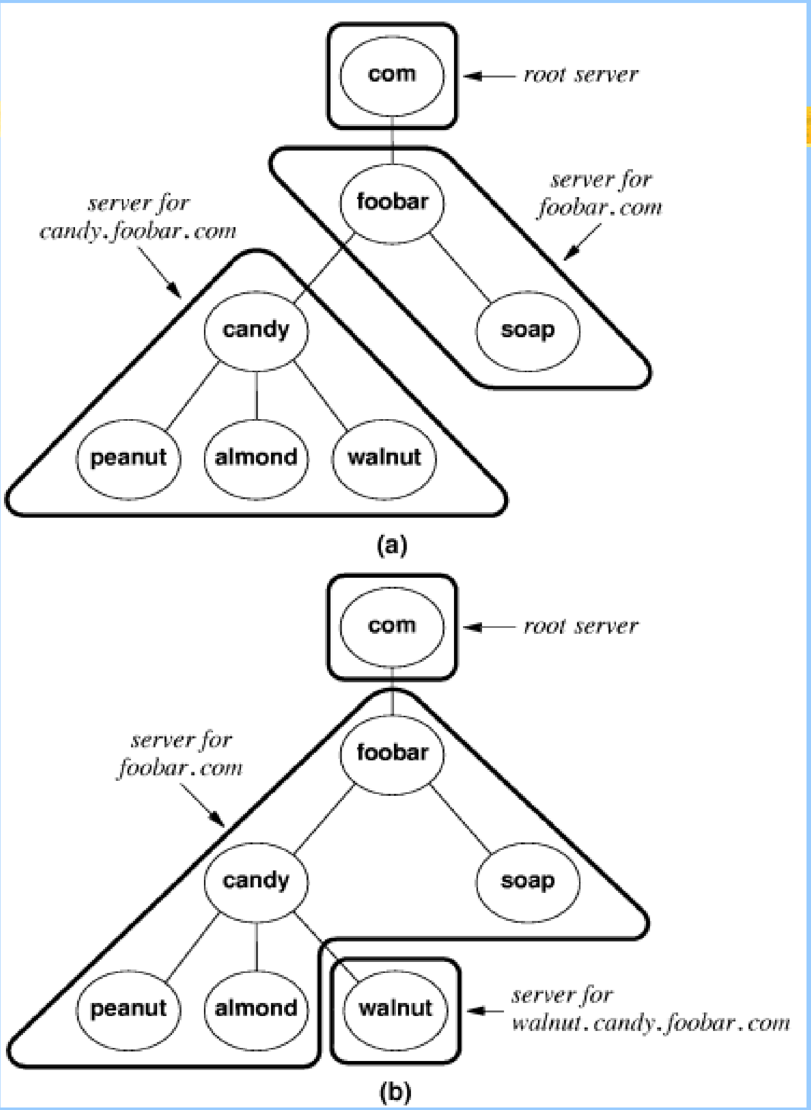
DNS Client-Server Model

- Most organizations have a domain name server
  - DNS server has a database of names
  - Server has links to higher-level servers
- An application (client) requests address translation from DNS server
  - Sends DNS request message
- Server either responds with IP address or sends request to next higher server

DNS Server Hierarchy

- Name servers do not store all of the existing names in their data base
  - They depend on higher-level and lower-level servers who may have the desired name/address listing in their data base
- A *root server* is responsible for TLDs
  - Knows how to reach servers that handle requests for lower-level addresses (slb.com, spsu.edu)
- Next lower level DNS server knows how to find servers below it
- Company can use one or more DNS servers
  - Multiple servers can balance load

Example: An Organization's DNS Zone Hierarchy



- D. Comer, Computer Networks and Internets With Internet Applications, 3ed., Upper Saddle River, NJ, Prentice-Hall, 2001

Example: An Organization's DNS Zone Hierarchy

- In previous figures, the .com root server must know the address of the foobar.com DNS server
  - In the top figure, the foobar.com server must know the address of the candy.foobar.com server
  - In the lower figure, the foobar.com server must know the address of the walnut.candy.foobar.com server
- All DNS servers in foobar.com must know the address of a root server

Resolving Names

- Name resolution means that a name is resolved to an address
- Resolver software runs on the client computer and interfaces between the user application and the DNS server
  - Resolver knows address of its local DNS server
  - Sends *DNS request, or query* to server
  - Can cache addresses received from name servers

Resolving Names

- Server sends *DNS reply or answer*
  - If server does not have address, it sends request to next higher server
- Each DNS server knows address of a root server

DNS Request/Reply Sequence

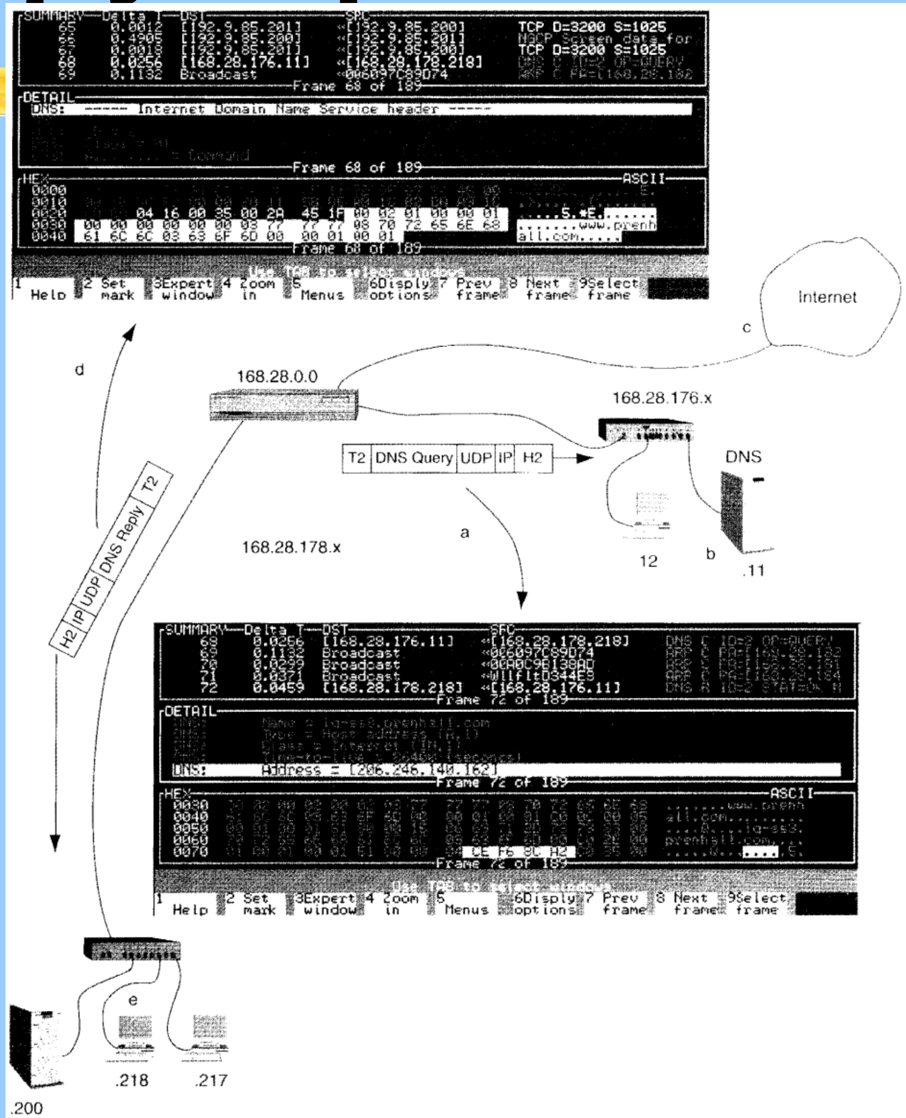


FIGURE 2.10
The DNS protocol.

◆ **In figure, screen captures are reversed**

Dynamic Host Control Protocol (DHCP)

- Client-server based system for assigning IP address information t hosts
- Greatly simplifies IP address management in organizations
- Three modes of operation
  - Manual entry
    - Administrator associates a given host to a given IP address on DHCP server
  - Dynamic
    - “Lease” address configuration for a period of time
  - Automatic
    - “Lease” address configuration indefinitely

DHCP Address Leases

- In dynamic and automatic modes, DHCP servers have a range of addresses that it can supply to hosts
  - When a host boots, it requests IP address information from the DHCP server
  - The server assigns an address from its range
    - In dynamic mode, the host loses its configuration after a fixed time period and must request another configuration when it needs it
      - It also loses it when it is shut down
    - In automatic mode, the host does not lose its configuration until it shuts down

Diagnostic Tools

- Ping
  - used to transmit an ICMP echo request to a remote host and wait for a reply
  - Used to see that a remote host is running and its TCP/IP protocol is properly configured

Diagnostic Tools

- Traceroute
  - Used to trace the path to a destination host
  - Implemented by sending UDP IP packets with increasing time-to-live TTL values, starting at 1, until destination is reached
    - Each intermediate router must decrement TTL by 1
    - If TTL reaches 0, that router must send an ICMP response back to the sender
  - Resulting display shows round-trip time to each intermediate node
  - Each UDP packet is send 3 times with same TTL, resulting in three different responses from each node

Diagnostic Tools

- **Netstat**
  - **Displays network and interface statistics for local host**

SLIP and PPP

- Serial Line IP (SLIP)
  - A data link protocol created to transport IP over a serial line
    - Used in dial-up circuits
  - Not very robust
  - Replaced by PPP
- Point-to-Point Protocol (PPP)
  - Transports multi-protocol packets over various types of point-to-point links