NETWORK CONCEPTS

1.3- Purposes and Properties of IP Addresses

- Developed in the 1970s
- Created for use on the ARPANET
- Used by UNIX
- Predates the PC, the Open Systems Interconnection (OSI) model, and Ethernet
- Platform and operating system independent

- Developed using a collaborative process
- Published as Requests for Comments (RFCs) by the Internet Engineering Task Force (IETF)
- In the public domain

- Platform independence
- Quality of service
- Simultaneous development

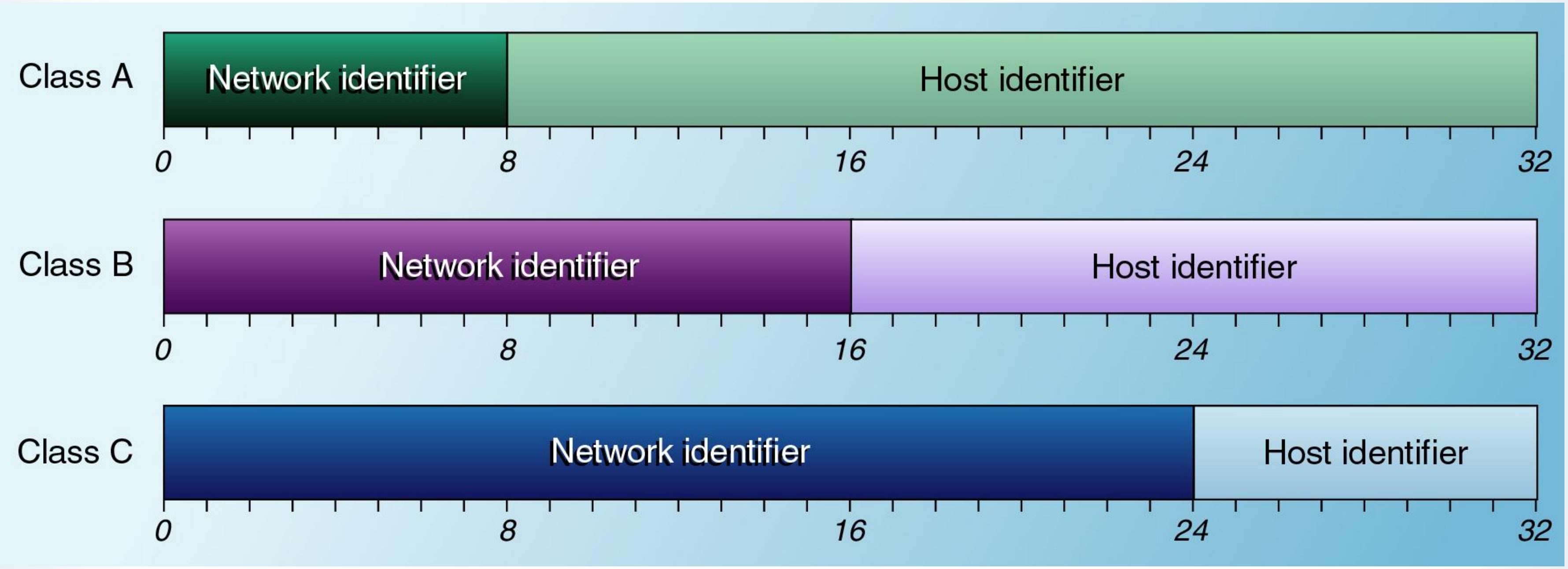
IP in Depth

- TCP/IP suite supports both simple and complex networks
  - Small LAN
  - Multiple LANs interconnected into a WAN

- TCP/IP on LAN over Ethernet
  - On small network, sending computer broadcasts using MAC address ff-ff-ff-ff-ff-ff to obtain recipient's MAC address
  - Broadcasting is disastrous to a large network

- Every network interface adapter on a network must have
  - The same network identifier as the others on the network
  - A unique host identifier
- The Internet Assigned Numbers Authority (IANA) assigns network identifiers, but you typically obtain network addresses from an Internet service provider (ISP).
- Network administrators assign host identifiers.

IP Address Classes



IP Address Class First Bit/Byte Values

Class	First Bits	First Byte Values
A	0	1–127
B	10	128–191
C	110	192–223

Class	Network ID Bits	Host ID Bits	Number of Networks	Number of Hosts
A	8	24	126	16,777,214
B	16	16	16,384	65,534
C	24	8	2,097,152	254

- All the bits in the network identifier cannot be set to zeros.
- All the bits in the network identifier cannot be set to ones.
- All the bits in the host identifier cannot be set to zeros.
- All the bits in the host identifier cannot be set to ones.

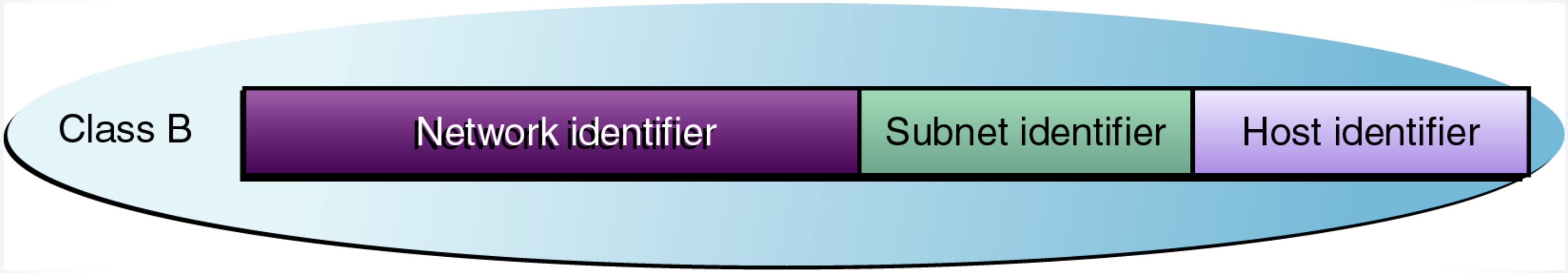
- A subnet mask is a 32-bit binary number that indicates which bits of an IP address identify the network and which bits identify the host.
- The 1 bits are the network identifier bits and the 0 bits are the host identifier bits.
- A subnet mask is typically expressed in dotted decimal notation.

Subnet Masks for IP Address Classes

Class	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

- Borrow bits from the host identifier and use them as a subnet identifier.
- Increment the subnet and host identifiers separately.
- Convert the binary values to decimals.

Subnetting a Class B Address



Private Network Addresses

Class	Network Addresses
A	10.0.0.0 through 10.255.255.255
B	172.16.0.0 through 172.31.255.255
C	192.168.0.0 through 192.168.255.255

- Expands IP address space from 32 to 128 bits
- Designed to prevent the depletion of IP addresses
- Uses XX:XX:XX:XX:XX:XX:XX:XX notation

- TCP/IP protocols
  - The TCP/IP protocols were developed to support systems that use any computing platform or operating system.
  - The TCP/IP protocol stack consists of four layers: link, internet, transport, and application.
  - IP uses the ARP protocol to resolve IP addresses into the hardware addresses needed for data-link layer protocol communications.
  - The ICMP protocol performs numerous functions at the internet layer, including reporting errors and querying systems for information.
  - Application layer protocols enable specific programs and services running on TCP/IP computers to exchange messages.

- IP addressing
  - IP addresses are 32 bits long and consist of a network identifier and a host identifier, expressed as four decimal numbers separated by periods.
  - Every network interface adapter on a TCP/IP network must have a unique IP address.
  - The IANA assigns IP network addresses in three classes, and network administrators assign the host addresses to each individual system.
  - The subnet mask specifies which bits of an IP address identify the network and which bits identify the host.
  - Modifying the subnet mask for an address in a particular class lets you "borrow" some of the host bits to create a subnet identifier.

- 32-bit value that contains a network identifier and a host identifier
- Expressed in dotted decimal notation
- Assigned to network interface adapters, not computers

- TCP is the acronym for Transmission Control Protocol.
- TCP is
  - Connection oriented
  - Reliable
- It is used to carry large amounts of data.
- It provides services that Internet Protocol (IP) lacks.
- TCP is defined in Request for Comments (RFC) 793.

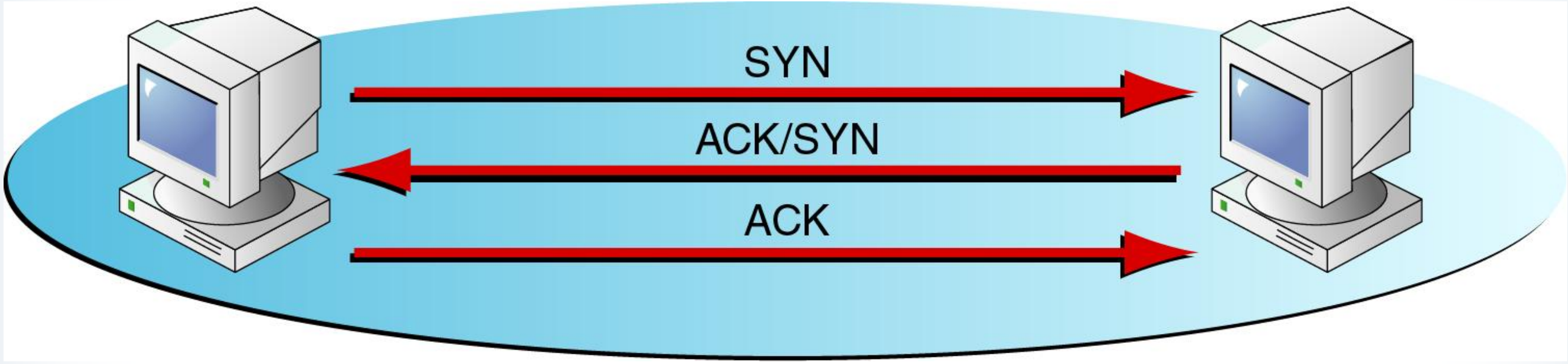
- Guaranteed delivery
- Packet acknowledgment
- Flow control
- Error detection
- Error correction

- TCP splits application layer messages into datagram-sized segments and encapsulates each segment with its own header.
- The collection of segments is called a sequence.
- The destination system reassembles the segments into the original sequence.
- The segmentation process is completely separate from the network layer fragmentation process.

- A port number refers to a specific application or process running on a computer.
- A socket is a combination of a port number and an IP address.
- The Internet Assigned Numbers Authority (IANA) assigns well-known port numbers to common Internet applications.
- The most commonly used port numbers are listed in the Services file on computers running TCP/IP.

- Verify that both computers are operating and ready to receive data
- Exchange initial sequence numbers (ISNs)
- Exchange maximum segment sizes (MSSs)
- Exchange port numbers

Three-Way Handshake Messages



- Information needed to transmit data:
  - Port number
  - Sequence number
  - MSS

- TCP implements packet acknowledgment by using the Sequence Number and Acknowledgment Number fields.
- The Sequence Number field specifies the number of bytes transmitted.
- The Acknowledgment Number field specifies the number of bytes received.

- TCP systems do not have to individually acknowledge every packet they receive.
- The frequency of acknowledgment is left up to the individual TCP implementation.

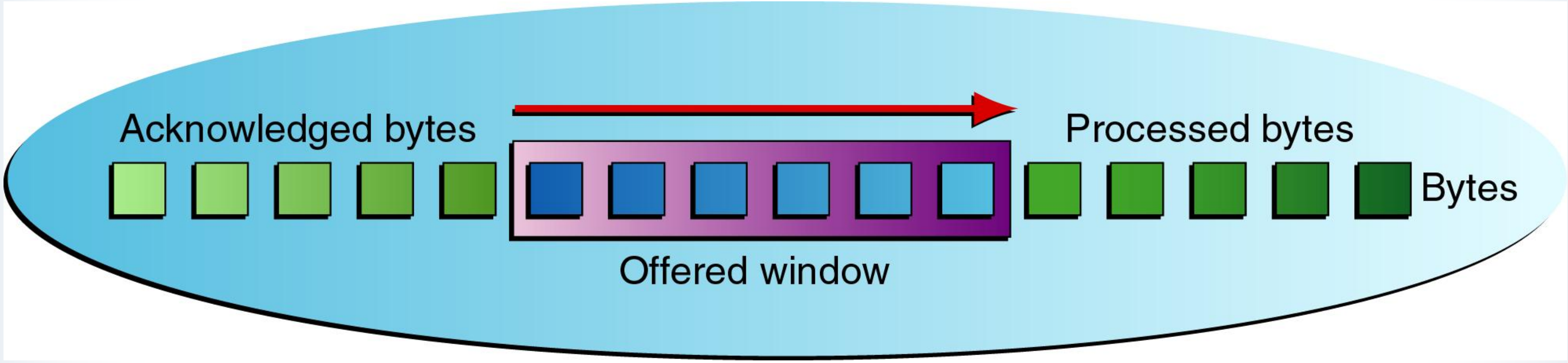
Positive and Negative Acknowledgments

- With positive acknowledgment with retransmission, TCP systems acknowledge only the number of bytes they have received correctly.
- With negative acknowledgment, the computer specifies the information that it has not received correctly.
  - All data beginning with the failed segment is retransmitted.
- Messages that are not acknowledged are retransmitted.

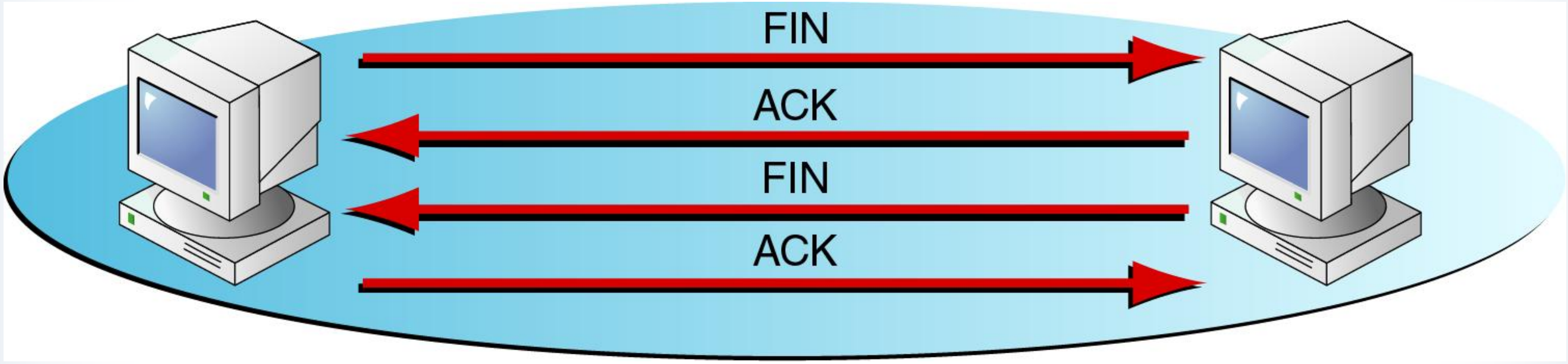
- TCP provides the only end-to-end error detection for the application layer data.
- TCP computes a checksum based on
  - The TCP header
  - The application layer information in the TCP Data field
  - A pseudo-header created from some of the fields in the IP header

- Flow control allows a receiving system to control the transmission rate of the sending system.
- Each computer has a buffer for storing incoming packets.
- When a computer transmits too quickly, the buffer on the receiving system can fill up, causing packets to be dropped.
- TCP uses the Window field in its acknowledgment messages to implement flow control.
  - The Window value indicates how much buffer space the receiving system has available.
  - The sending system is permitted to transmit only the number of bytes specified in the Window field.

Sliding Window Technique



Terminating the Connection

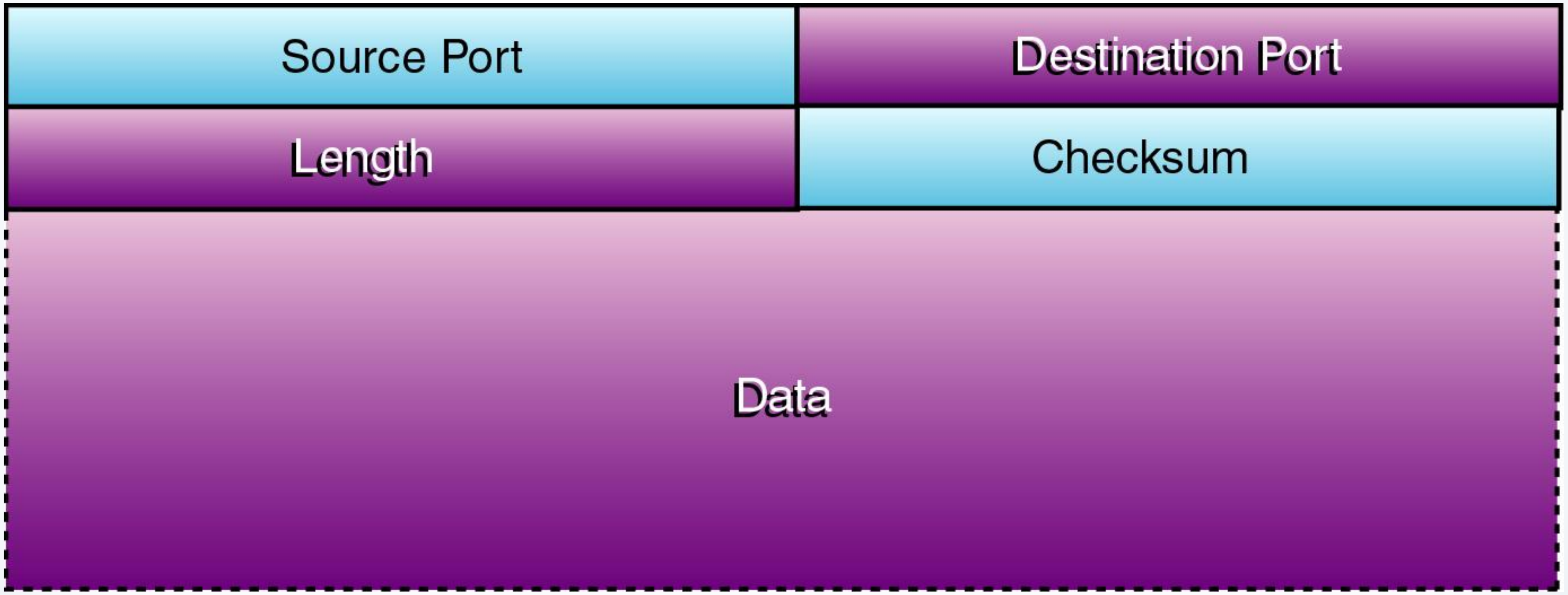


HYBRID TECHNOLOGY TRAINING
PRINCE GEORGE'S COMMUNITY COLLEGE

- UDP is the acronym for User Datagram Protocol.
- UDP is defined in RFC 768.
- It is a connectionless protocol.
- It is used primarily for brief request/reply transactions.

The UDP Message Format

HYBRID TECHNOLOGY TRAINING
PRINCE GEORGE'S COMMUNITY COLLEGE



Uniqueness

- Every MAC address must be unique
- Every IP address must be unique

Utilities for displaying IP and MAC addresses

- Every OS has a command-line utility
    - Windows has IPCONFIG
    - UNIX/Linux/Mac use IFCONFIG

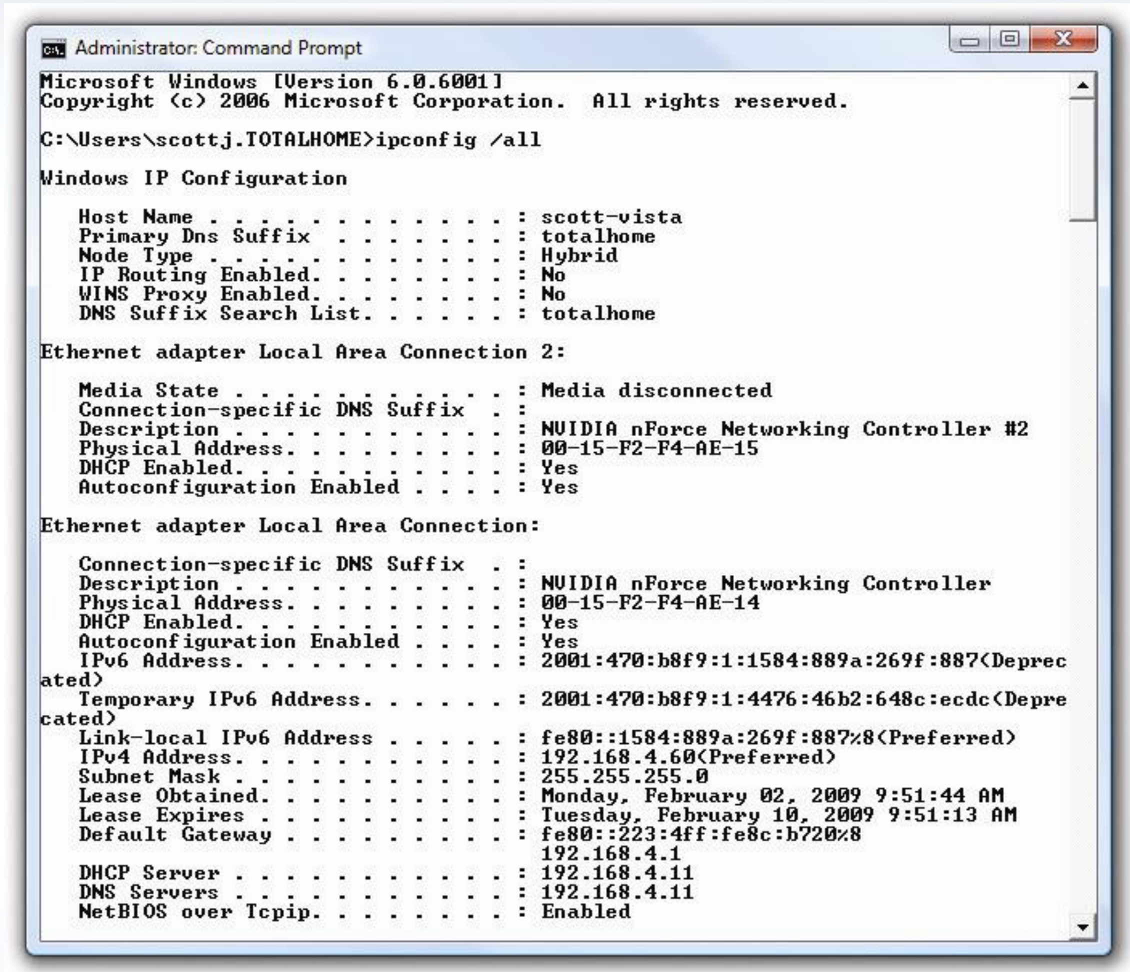


Figure 7.8 ipconfig /all

vmuser@vmuser-desktop: ~

File Edit View Terminal Tabs Help

```
vmuser@vmuser-desktop:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:62:be:d4
          inet addr:192.168.4.43  Bcast:192.168.4.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe62:bed4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26569 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11412 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29675139 (29.6 MB)  TX bytes:973598 (973.5 KB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2066 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2066 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:103300 (103.3 KB)  TX bytes:103300 (103.3 KB)

vmuser@vmuser-desktop:~$
```

Figure 7.9 IFCONFIG in Linux

Network IDs

- IP must give each LAN its own identifier
  - All computers on same LAN must have same network ID
  - Each computer on same LAN must have a unique host ID
  - Example: 192.168.5.*x* represents addresses in Figure 7.10

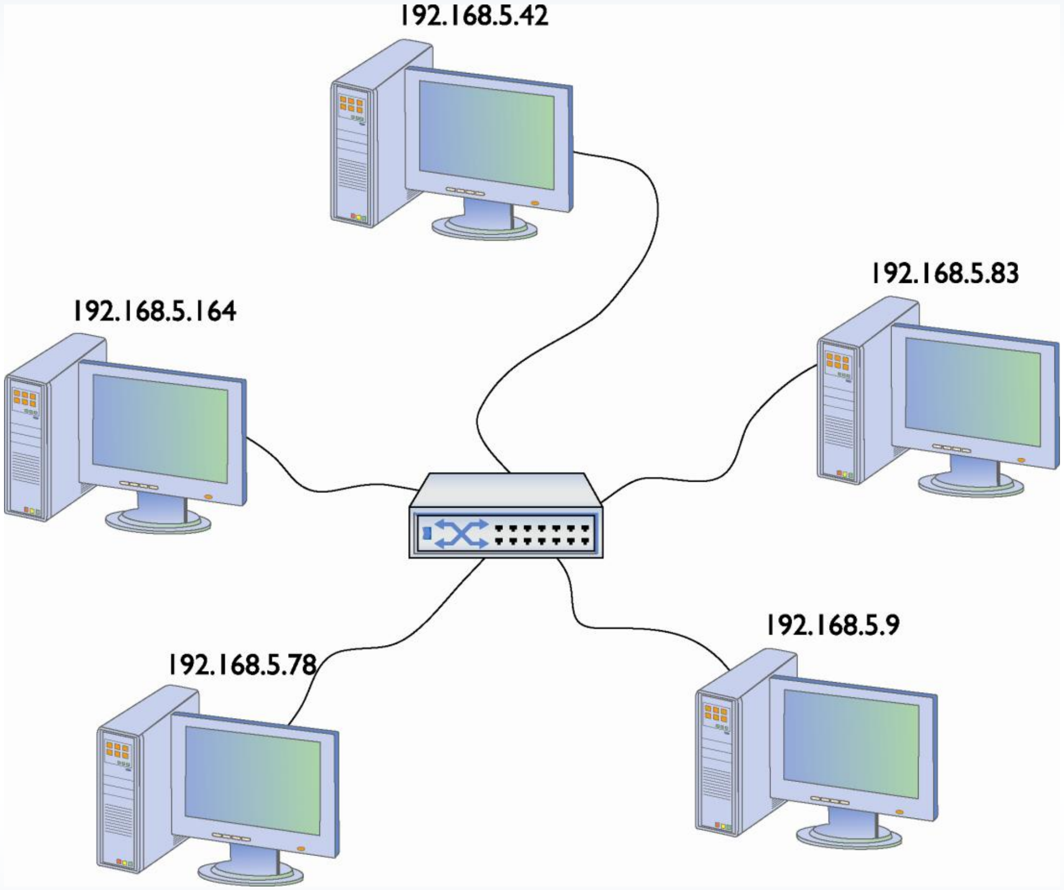


Figure 7.10 IP addresses for a LAN

Interconnecting

- Router uses a built-in router table
  - Uses this to determine where to send packets
  - How router uses routing table:

Everything for 192.168.5.0 goes out 192.168.5.1	**Everything else goes out 14.23.54.223**

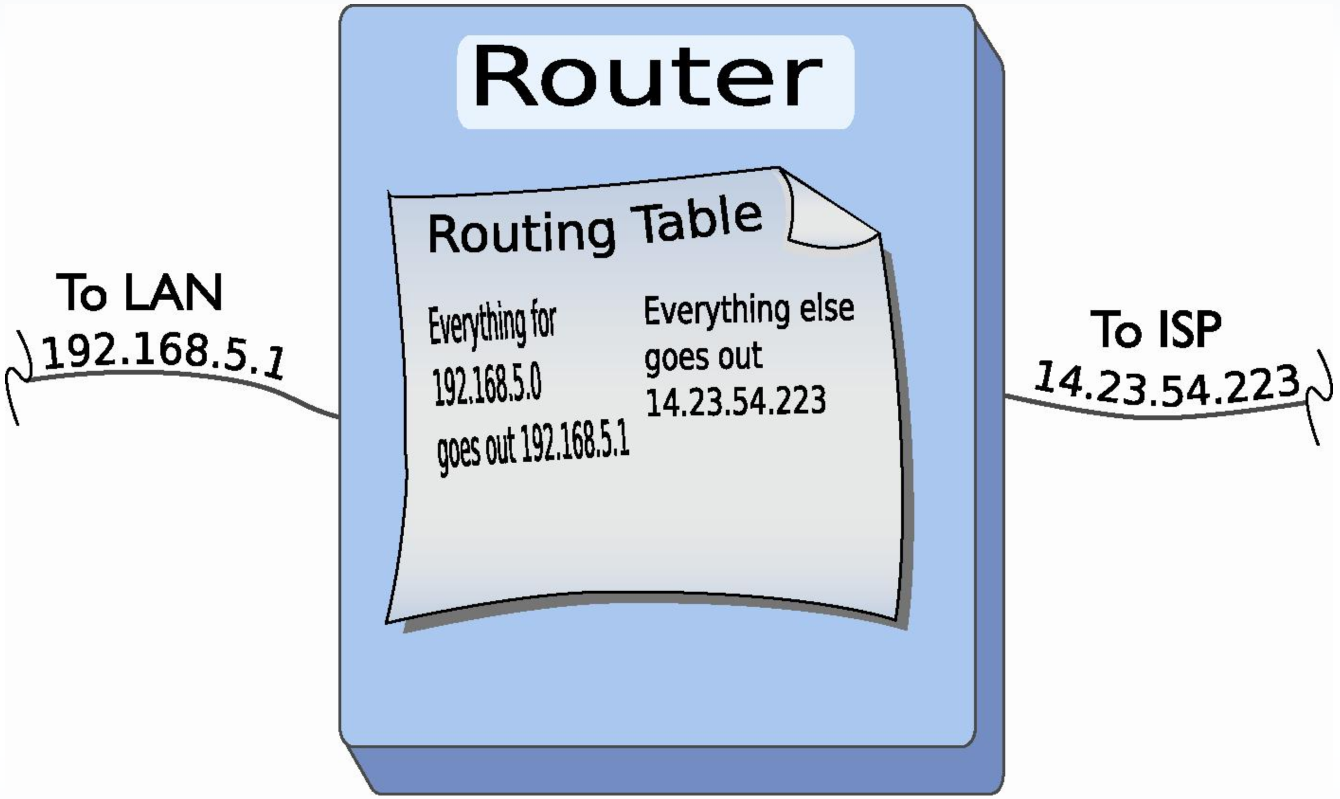


Figure 7.12 Router diagram

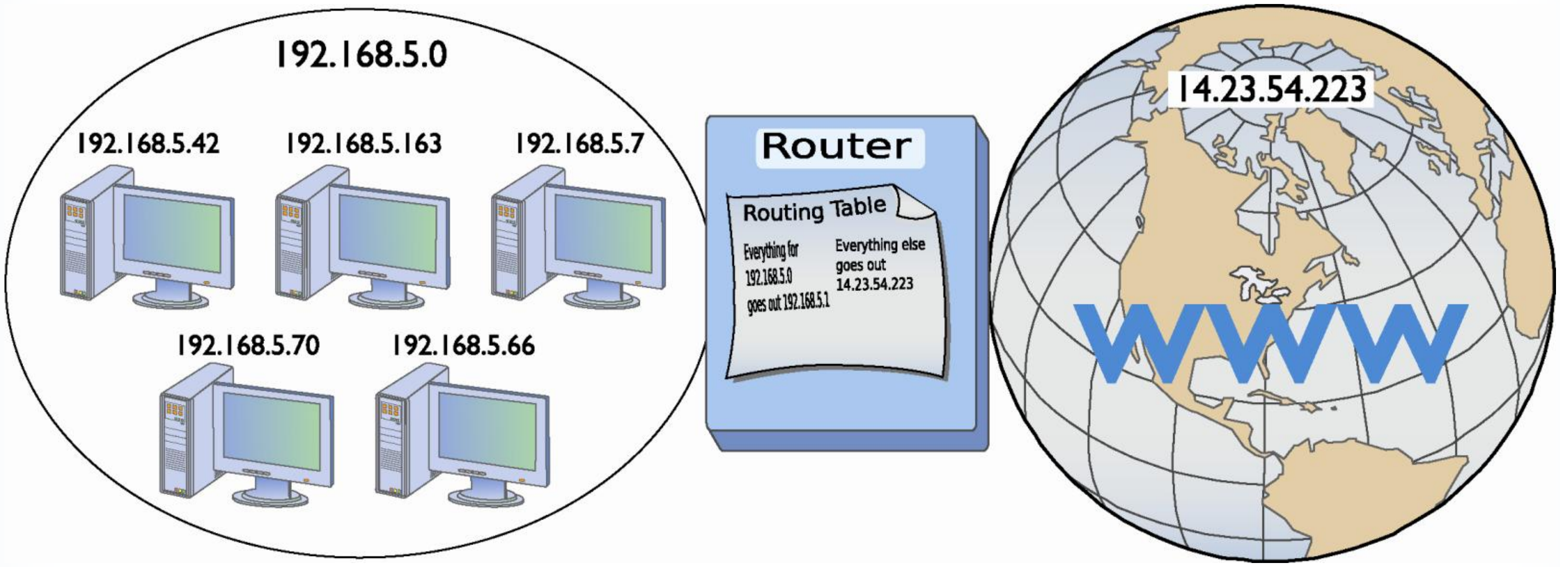


Figure 7.13 LAN, router, and the Internet

Public Vs Private IP Addresses

- A public IP address is an address that is accessible over the internet
- Public addresses are usually assigned by international naming groups since they must be unique
- A private IP address is an address assigned to a device on a local area network (LAN)
- Private address are only accessible within the Local Area Network (LAN)

Subnet Mask (cont.)

- Line up an IP address with a corresponding subnet mask in binary
    - Portion of IP address that aligns with the ones of the subnet mask is the network ID of the IP address.
    - Portion of IP address that aligns with the zeroes of the subnet mask is the network ID of the IP address

	Dotted Decimal	Binary
IP address	192.168.5.23	11000000.10101000.00000101.00010111
Subnet mask	255.255.255.0	11111111.11111111.11111111.00000000
Network ID	192.168.5.0	11000000.10101000.00000101.*x*
Host ID	*x.x.x.23*	x.x.x.00010111

Subnet Mask (cont.)

- Sending computer compares the destination IP address to its own IP address using the subnet mask
- If the destination IP address matches the computer IP wherever there's a '1' in the subnet mask, sending computer knows the address is local
- If the destination IP address does not match the sending computer's IP wherever there's a '1' in the subnet mask, sending computer knows the address is remote

Computer A's IP:	110000001010100000000101 00010111
Subnet mask	111111111111111111111111 00000000
Computer B's IP:	110000001010100000000101 00101100

These all match! It's a local call.

Figure 7.16 Comparing addresses

Subnet Mask (cont.)

- When the destination address is local, the sending computer sends out an Address Resolution Protocol (ARP) broadcast to determine the destination computer's MAC address
- The ARP packet contains the sending computer's IP address as well as the destination address
- Destination computer responds to the ARP request by sending an ARP response containing its MAC address
- Sending computer can now send data packets to destination

Subnet Mask (cont.)

- When the sending computer discovers that the destination address does not have the same network ID as itself, then it must send the packet beyond the local network
- The packet must be sent to the default gateway
- Sending computer must ARP for the MAC address of the default gateway

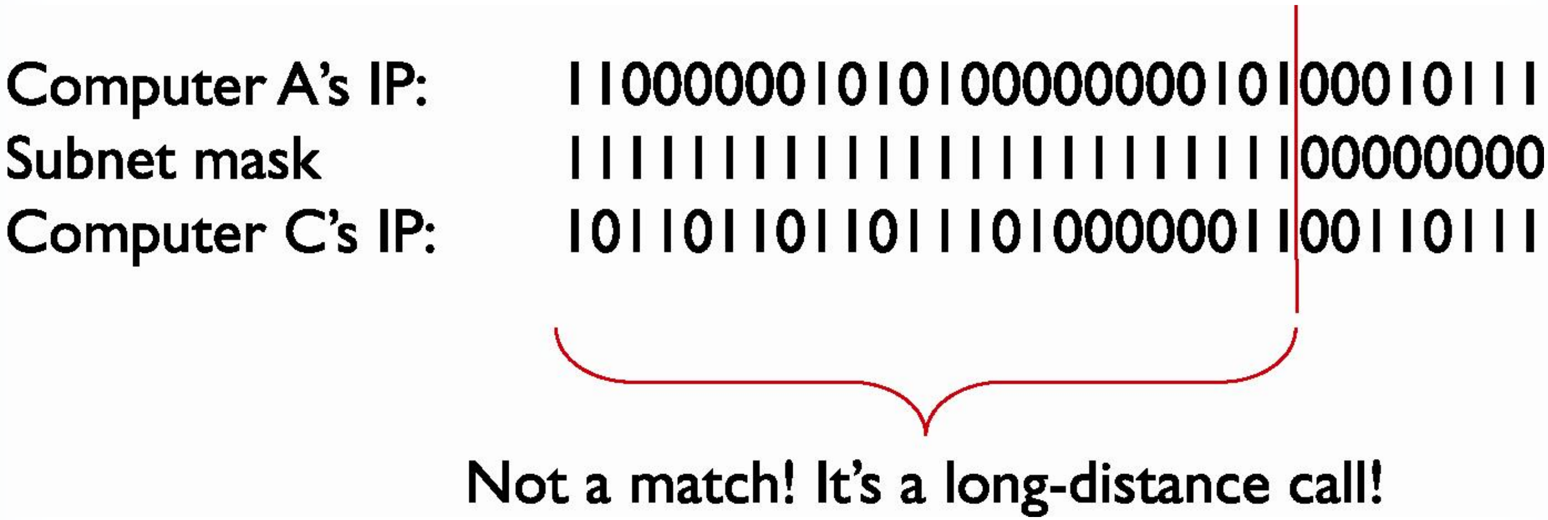


Figure 7.20 Comparing addresses again

– Subnet Mask (cont.)

- **Some valid subnet masks**

```
11111111111111111111111100000000 = 255.255.255.0
11111111111111110000000000000000 = 255.255.0.0
11111111000000000000000000000000 = 255.0.0.0
```

- **Shorthand for subnet mask**

```
11111111111111111111111100000000 = /24 (24 ones)
11111111111111110000000000000000 = /16 (16 ones)
11111111000000000000000000000000 = /8 (8 ones)
```

– **Subnet Mask (cont.)**

- **An IP address followed by the / and a number describes the IP and the address in one statement**

```
201.23.45.123/24 = IP address plus subnet mask
IP address = 201.23.45.123
Subnet mask = 255.255.255.0


184.222.4.36/16 = IP address plus subnet mask
IP address = 184.222.4.36
Subnet mask = 255.255.0.0
```

Subnet Mask (cont.)

- Network administrators must enter correct IP address and subnet mask when configuring a network card
- The networking software does the rest
- If you want a computer to work in a routed network, you must configure the computer correctly with an IP address, subnet mask, and default gateway

Class IDs

- No two devices on the Internet can share the same IP address
- Internet Assigned Number Authority (IANA) tracks and disperses IP addresses in chunks called class licenses
  - Oversees several Regional Internet Registries (RIRs)
  - RIRs in turn pass out IP addresses to large ISPs
  - ISPs pass out IP addresses to most end users

	First Decimal Value (range)	Addresses	Hosts per Network ID
Class A	1 – 126	1.0.0.0 – 126.255.255.255	16,277,214
Class B	128 – 191	128.0.0.0 – 191.255.255.255	65,534
Class C	192 – 223	192.0.0.0 – 223.255.255.255	254
Class D	224 – 239	224.0.0.0 – 239.255.255.255	Multicast
Class E	240 – 255	240.0.0.0 – 255.255.255.255	Reserved

IP Address Classes

Class IDs – More about Class D and E

- Three ways to send a packet
  - Broadcast to every computer on the LAN
  - Unicast from one computer to another computer
  - Multicast from one computer to a group
    - Uncommon between computers
    - Often used by routers

Class IDs – The state of IP address

- IP class licenses were allocated too generously at first
- Unallocated IP addresses became scarce
- IP class licenses concept did not scale well
  - If you needed 2000 IP addresses you had to take a single Class B or eight Class C licenses
- Solution
  - New method for generating blocks of IP addresses
  - Classless Inter-Domain Routing (CIDR)

CIDR and Subnetting

CIDR and Subnetting Overview

- Classless Inter-Domain Routing (CIDR) based on subnetting
- Subnetting chops up a single class of IP addresses into multiple smaller groups
- CIDR and subnetting are virtually the same thing
- Subnetting done by an organization on a block of addresses to create multiple subnetworks
- CIDR done by an ISP on a block of addresses to create multiple subnets to pass out to customers

Subnetting

- Enables separation of networks for security
- Enables bandwidth control

Suffix	Hosts	32 - Borrowed = CIDR	2^Borrowed = Hosts	Binary => dec = Suffix
.255	1	/32	0	...11111111
.254	2	/31	1	...11111110
.252	4	/30	2	...11111100
.248	8	/29	3	...11111000
.240	16	/28	4	...11110000
.224	32	/27	5	...11100000
.192	64	/26	6	...11000000
.128	128	/25	7	...10000000
Classful / Classless				

Calculating Hosts

- Hosts on a /24 network
- 192.168.4.1 to 192.168.4.254 = 254 hosts
- Calculate in binary
  - In a /24 network 8 binary digits are used for the host ID
  - 00000001 to 11111110 = 254 hosts
  - $2^{(\text{number of zeroes in the subnet mask})} - 2$
  - $2^8 - 2 = 254$ total hosts
- Memorize the formula

Calculating Hosts (cont.)

- Hosts on a /16 network
  - In a /16 network 16 zeroes are part of the host ID
  - 0000000000000001 to 1111111111111110 = 65,534 hosts
  - $2^{(\text{number of zeroes in the subnet mask})} – 2$
  - $2^{16} – 2 = 65{,}534$ total hosts

Calculating Hosts (cont.)

- Hosts on a /26 network
  - In a /26 network 6 zeroes are part of the host ID
  - 000001 to 111110 = 62 hosts
  - $2^{(\text{number of zeroes in the subnet mask})} - 2$
  - $2^6 - 2 = 62$ total hosts

Exercise: Your First Subnet

- Convert the 192.168.4/24 net ID into three network IDs
- Write out the subnet mask in binary
- Place a line at the end of the ones

Subnet mask 111111111111111111111111 00000000

Figure 7.23 Step 1 in subnetting

Your First Subnet (cont.)

- Draw a second line one digit to the right

- Three areas (a Mike Trick, not official terms)
  - Subnet mask (SM)
  - Network ID extension (NE)
  - Hosts (H)

- This is now a /25 subnet mask

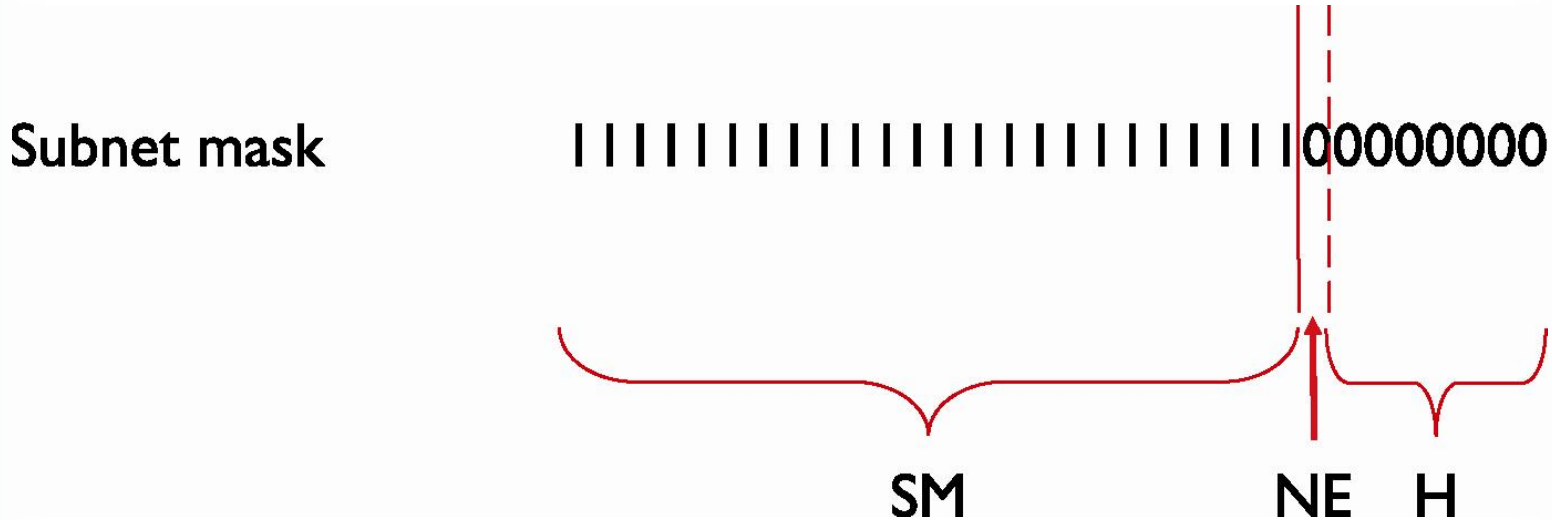


Figure 7.24 Organizing the subnet mask

Your First Subnet (cont.)

- A subnet mask is *always* 32 binary digits long
- A string of ones followed by a string of zeroes

  1111111111111111111111111 0000000

- Put periods between every eight digits

  11111111.11111111.11111111.10000000

- Then convert to dotted decimal
- The resulting subnet mask:

  255.255.255.128

Manual Dotted Decimal to Binary Conversion

- Start with bit values beginning with 128
- Place decimal value above the first value on the left which it exceeds and subtract and place a one to represent this binary value

```
221
128      64      32      16       8      4      2      1
 93
  1
```

Manual Dotted Decimal to Binary Conversion

- Place the remainder above the next bit value that it exceeds (Place a zero in positions that are skipped)

221	93		29	13	5		1
128	64	32	16	8	4	2	1
93	29		13	5	1		0
1	1	0	1	1	1	0	1

- Decimal 221 = binary 11011101