Victor McGrew

BASIC IP NETWORKING

This Webinar is being recorded for distribution.
Your participation serves as consent.

EDWARDS
LEARNING CENTER

Objectives

- Discuss basic TCP/IP addressing
- Define subnet mask
- Explain components of a network
- Differentiate between network types
- Explain network wiring
- Differentiate between networking protocols
- Explain network security
- Describe network troubleshooting procedures

ConnectedSafety+

1. Cloud-based Software as a Service (SaaS) provides a secure, remote connection to EST4
2. Provides a comprehensive view of entire portfolio of connected sites
3. Real-time information and advanced analytics regarding system status
4. Recommendations to improve performance and maintain system compliance

ConnectedSafety+

ESTMobile

1. Cloud-based Software as a Service (SaaS) provides a secure, remote connection to iO panels
2. Provides insight and foresight to improve responsiveness and predict service needs
3. Access reports and on-board diagnostics from browser, smartphone or tablet
4. Sends real-time notifications and emails regarding alarms and other supervisory or fault events

ESTMobile

KESMobile

1. Live System Monitoring
2. Real-time Reports
3. Streamlined Troubleshooting
4. Complete Event History

KESMobile

NETWORKING

What is a network?

A network links similar items together using a set of rules that ensures reliable service

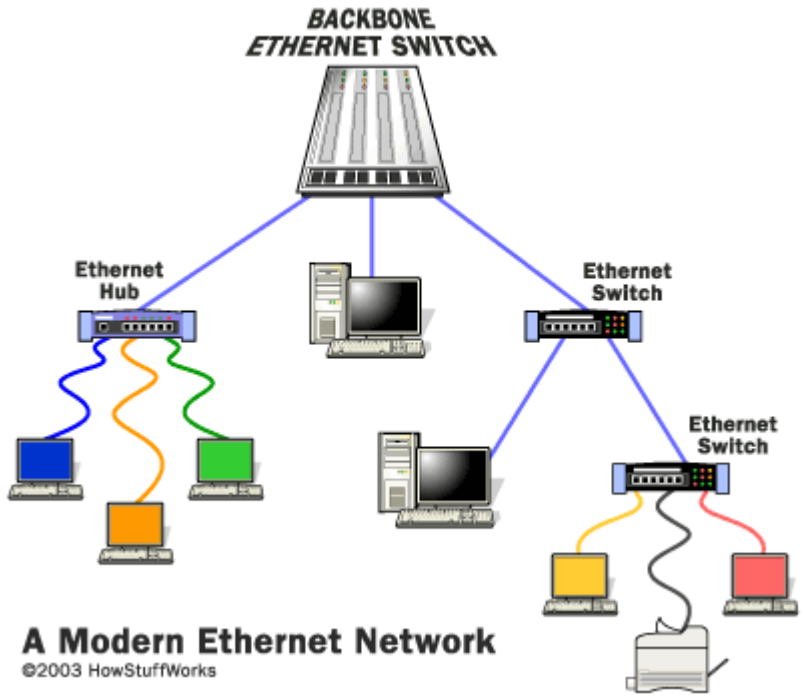
FedEx®

The Internet…

- A network of networks
- Series of private computers connected in an organization
- Each organization takes care of computers in its “sphere of influence”

Ethernet

- Ether denotes that networks are not restricted for use on only one connection type
- Ethernet can be used on many systems and function the same way
- UTP, coax, fiber optic cables, and wireless technologies can be used



NETWORK DEVICES

Why use a hub?

- PCs on a network communicate through a network interface card (NIC)
- With a hub, all PCs communicate with each other through a central location, where all the PC cables come together

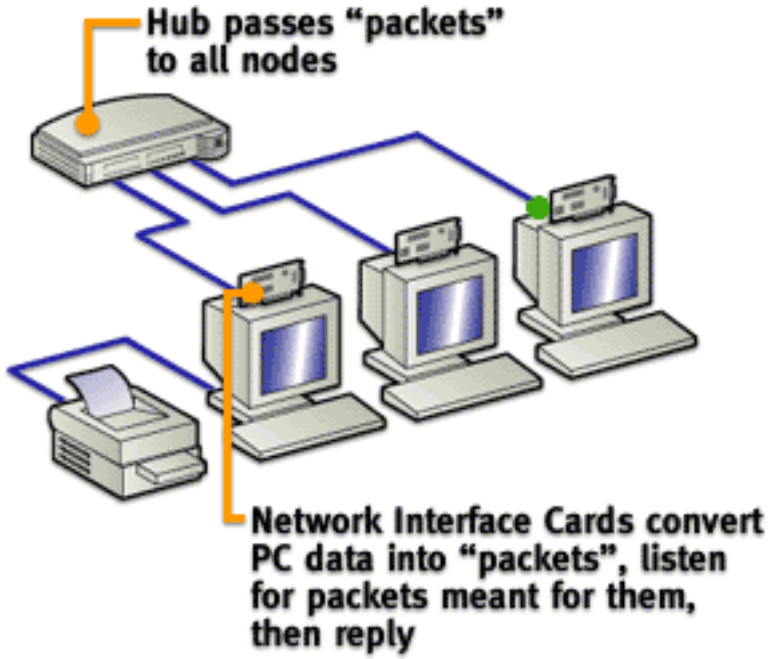
Problem?

All data is passed to all nodes

Solution:

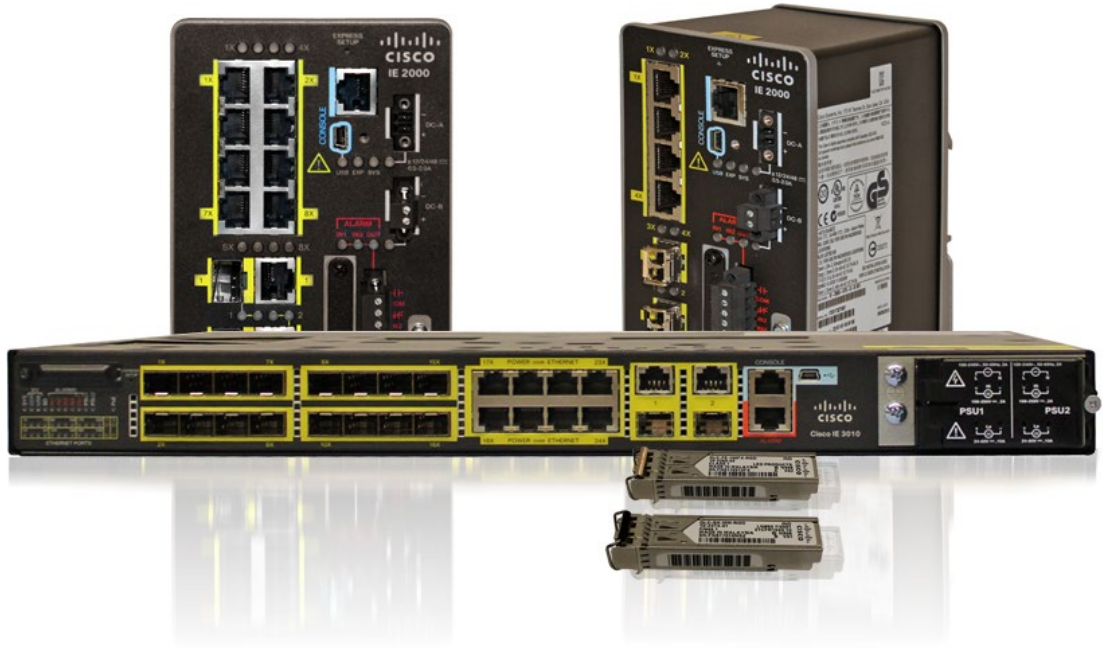
Hubs are obsolete

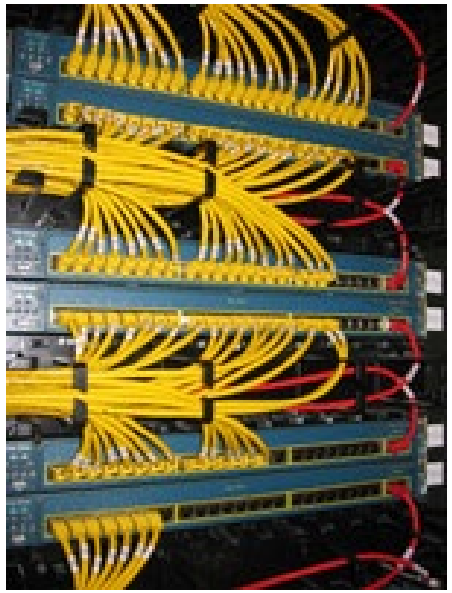
Use a network switch



Switches

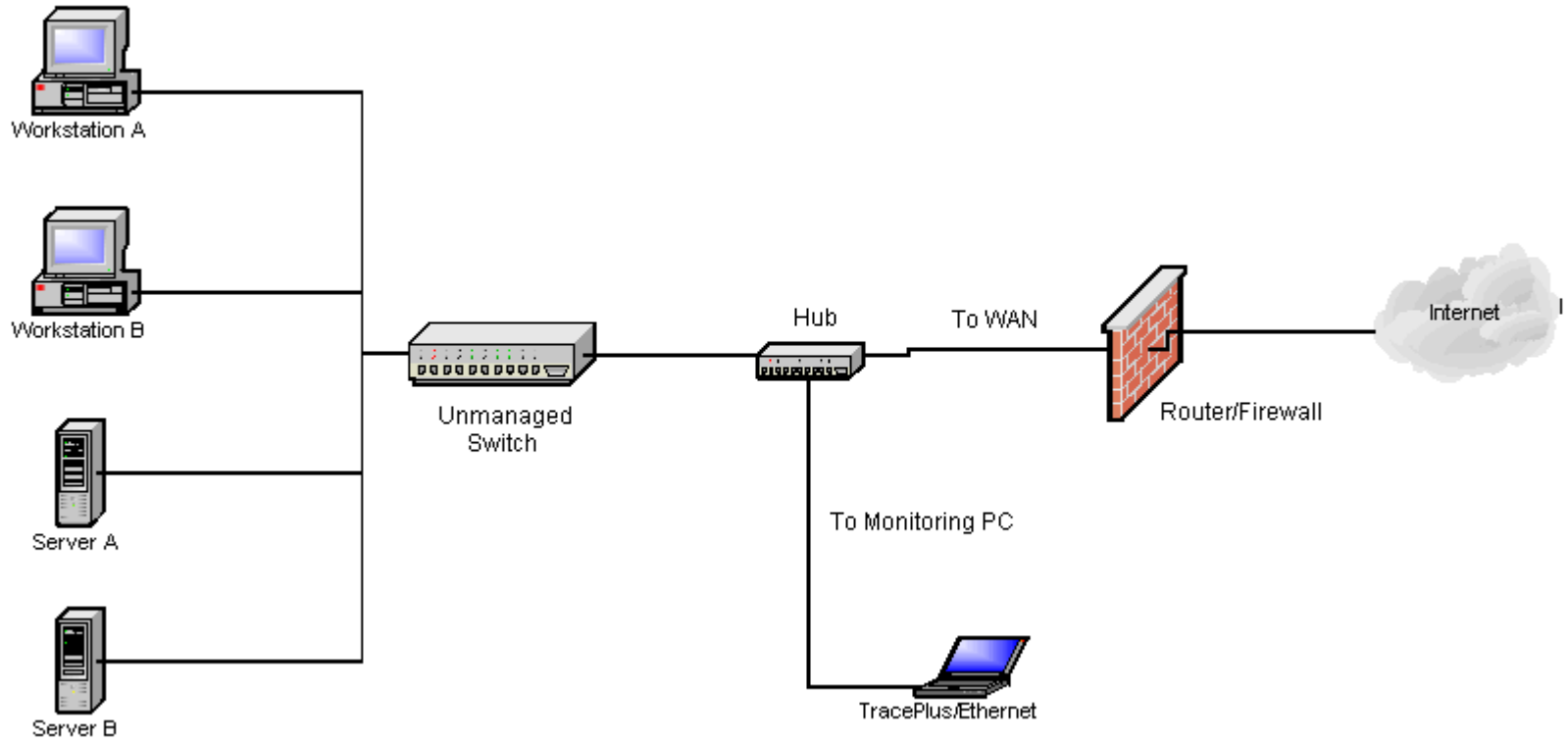
- Smarter version of a hub
- Associates each port with physical address of NIC connected to port
- Switch sends data only from NIC sending directly to NIC receiving
- Reduces transmissions and improves performance of network





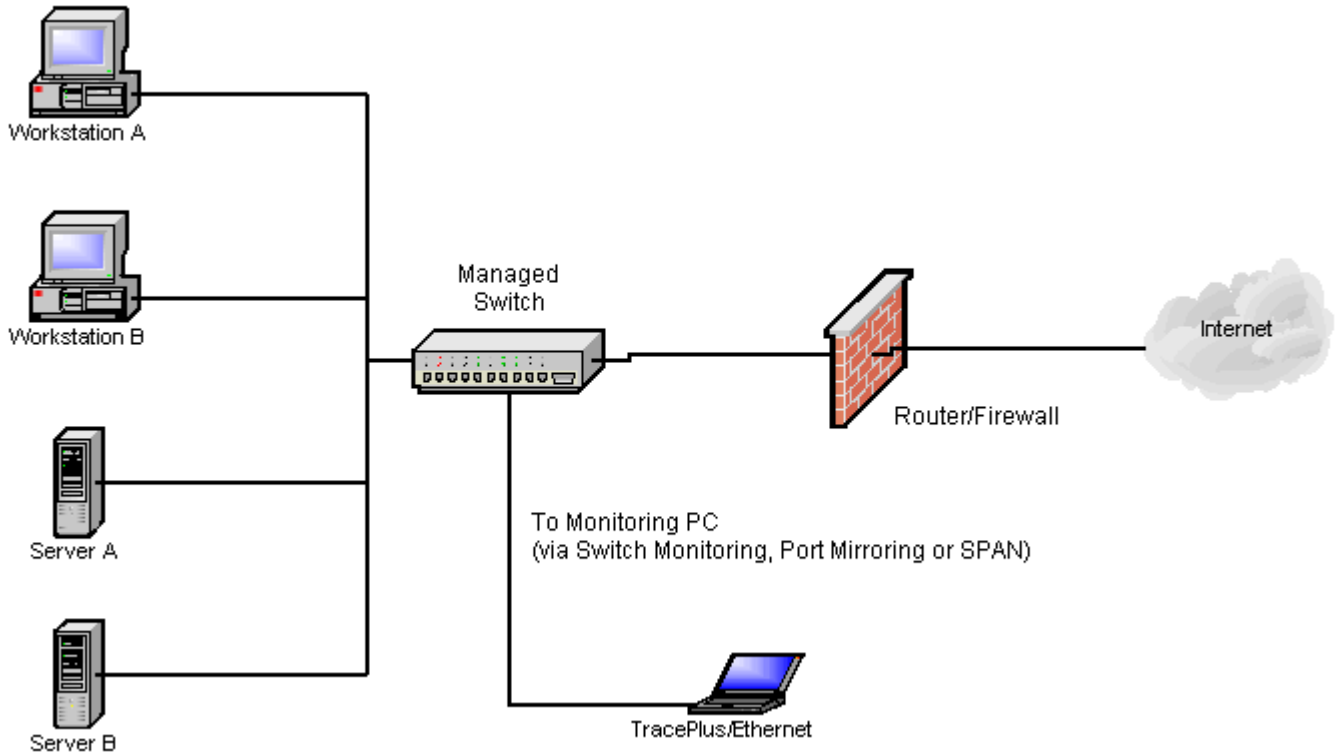
Unmanaged switches

- No configuration needed
- Build a switching table automatically
- Frames are forwarded out ports with no user intervention
- Network runs more efficiently



Managed switches

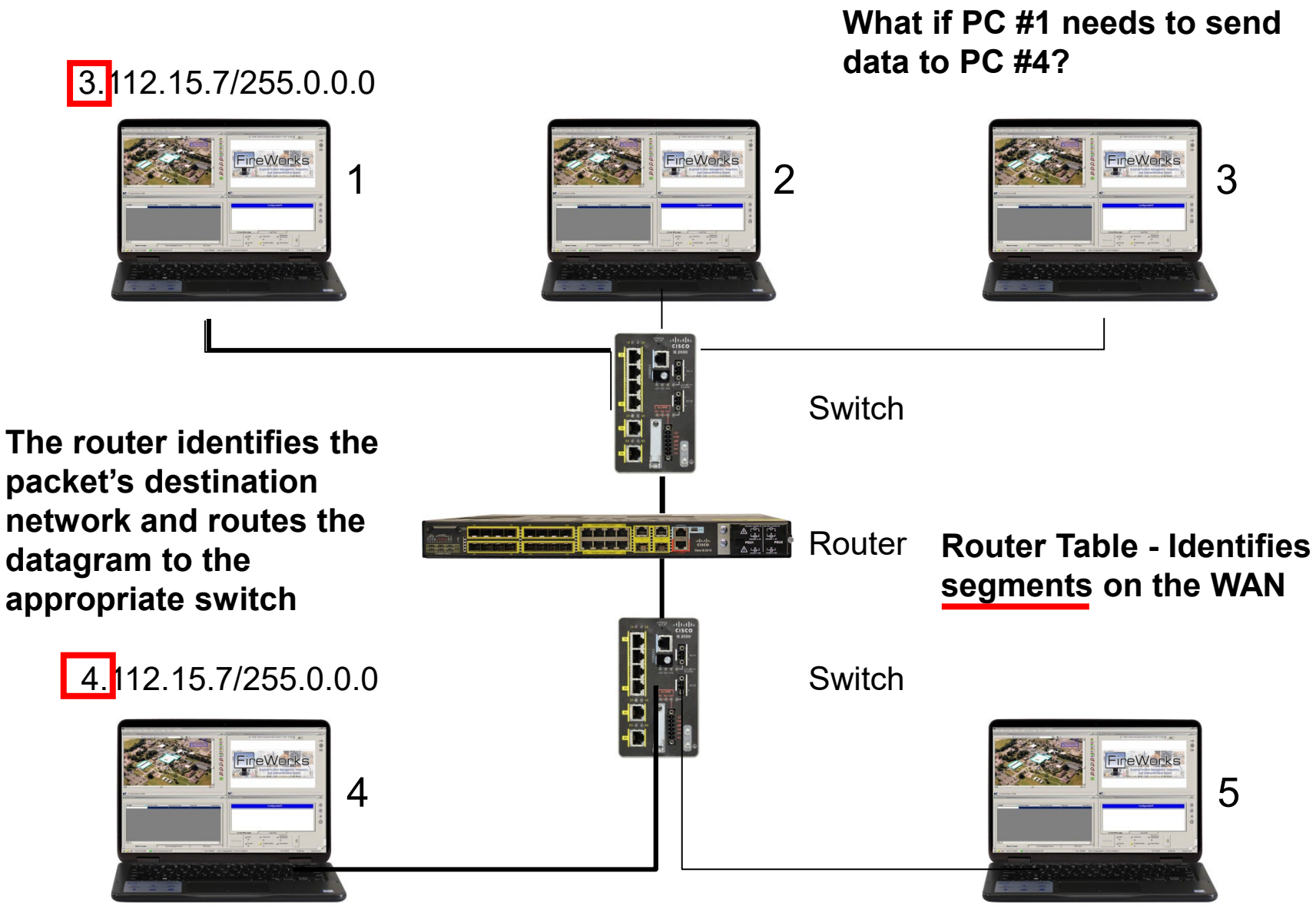
- With assigned IP address, remotely monitored and administered via web browser
- Collect and report information about network performance
- Set up broadcast domains within network
- Scalable



Routers

- Handle traffic flow for data packets that are not addressed inside the local network
- Routes packets to their destinations
- Optimized for handling packets to be transferred between networks
- Attempt to send packets from the source to the destination as fast as possible
- Provides some filtering and basic firewall services

Routers


What if PC #1 needs to send data to PC #4?
3.112.15.7/255.0.0.0
1
2
3
Switch
The router identifies the packet's destination network and routes the datagram to the appropriate switch
Router
Router Table - Identifies segments on the WAN
4.112.15.7/255.0.0.0
Switch
4
5

MEDIA TYPES

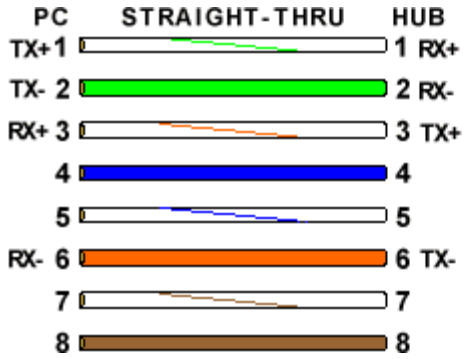
General guidelines

For wired-Ethernet, the maximum distance between nodes, hubs, switches or routers is 100 meters (325 ft.)

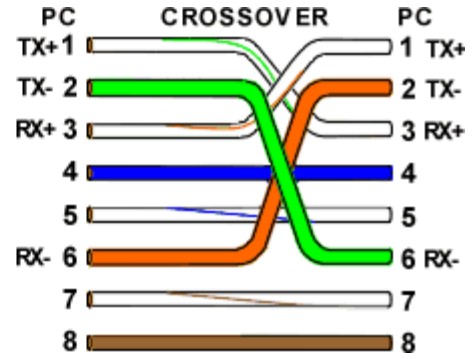
Category	Used For
6	Very fast Ethernet
5e	Fast Ethernet (and everything below) up to 1000Mbps
5	Ethernet up to 100Mbps
4	Networks other than Ethernet
3	10Mbps 10BaseT
2	Alarms and telephone voice lines
1	Unknown (not rated for anything specific)

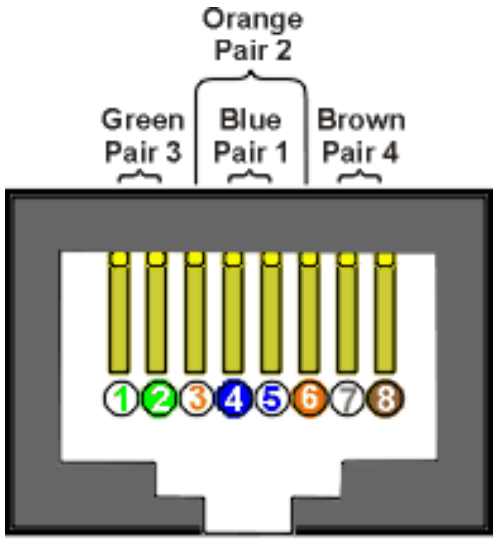
Network cables

STRAIGHT
568A 568A



CROSSOVER
568A 568B





RJ-45 JACK
EIA/TIA 568A STANDARD

10/100/1000 Physical layer standards

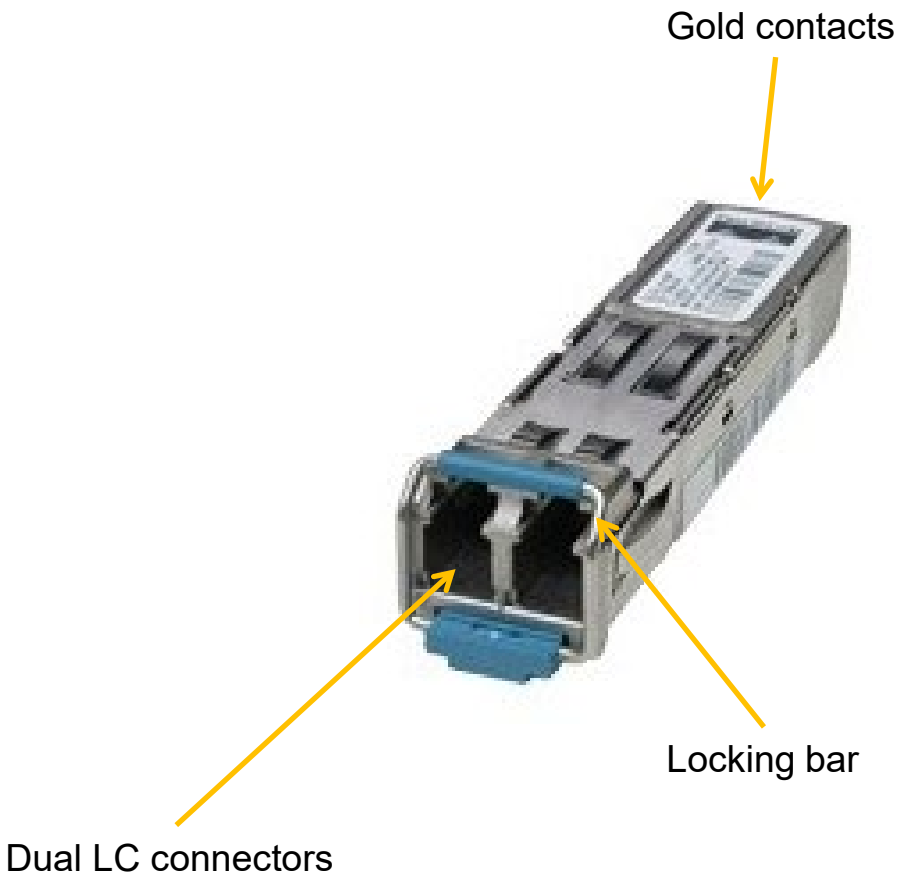
100BASE-FX 100Mbps
Multimode fiber 2km

100BASE-FX 100Mbps
Single Mode fiber 10km

Anatomy of an SFP

SFP (Small Form-Factor Pluggable) options and power levels:

- Multimode (up to 2 Km)
- Single mode (0-10, 10-70 Km)
- Dual filament
- Hot-swappable



High speed data access lines

- ISDN – Integrated Services Digital Network
- Cable Modem
- T1 & T3
- Fractional T1

NETWORK TYPES

Types of networking

- Physical networking
  - It’s the hardware!
- Logical networking
  - It’s the organization of the hardware that results from networking software

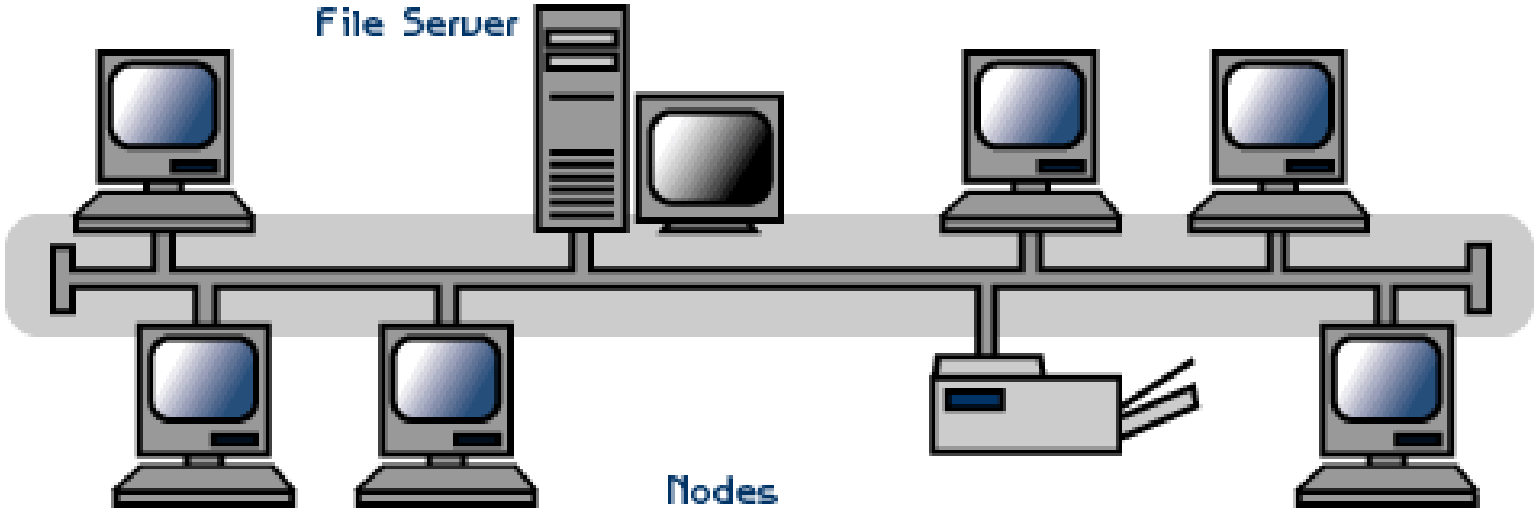
What is a physical topology?

- The arrangement of the wires in a network
- Various forms of physical topologies:
  - Bus
  - Star
  - Ring
  - Tree

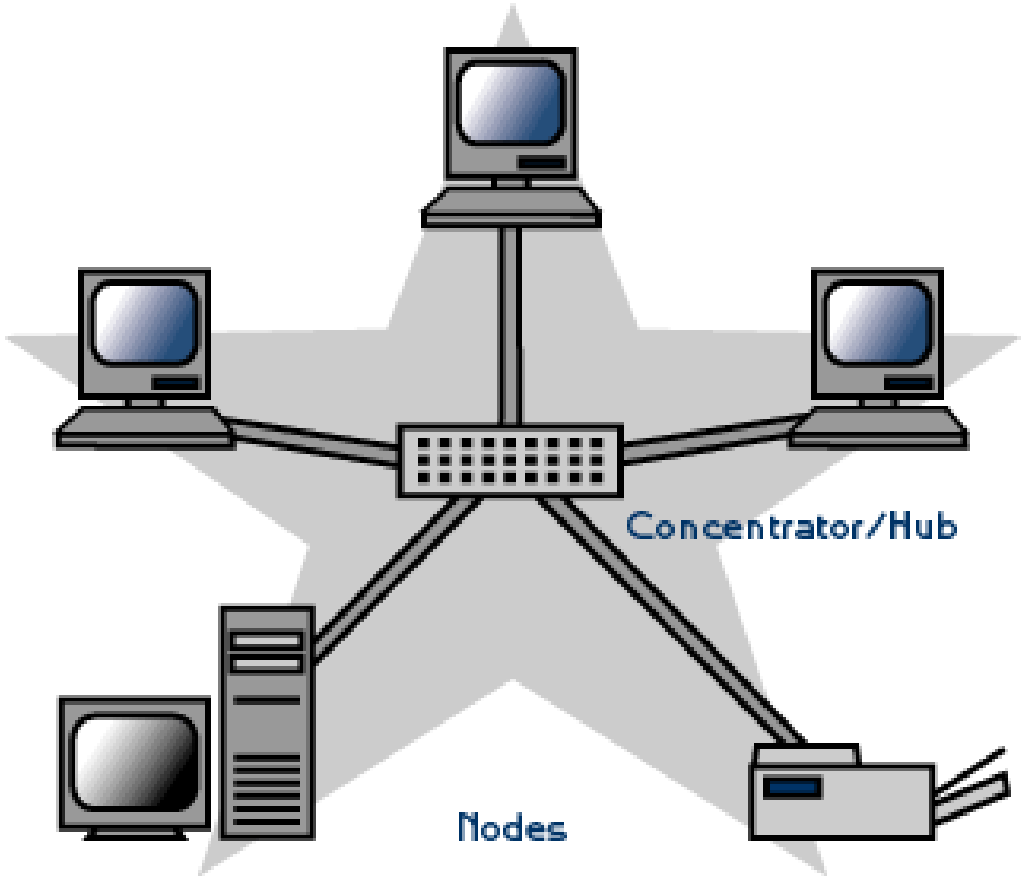
Physical devices

- Nodes – computer, printer and server
- Other devices:
  - Hubs
  - Switches
  - Routers
  - Modems

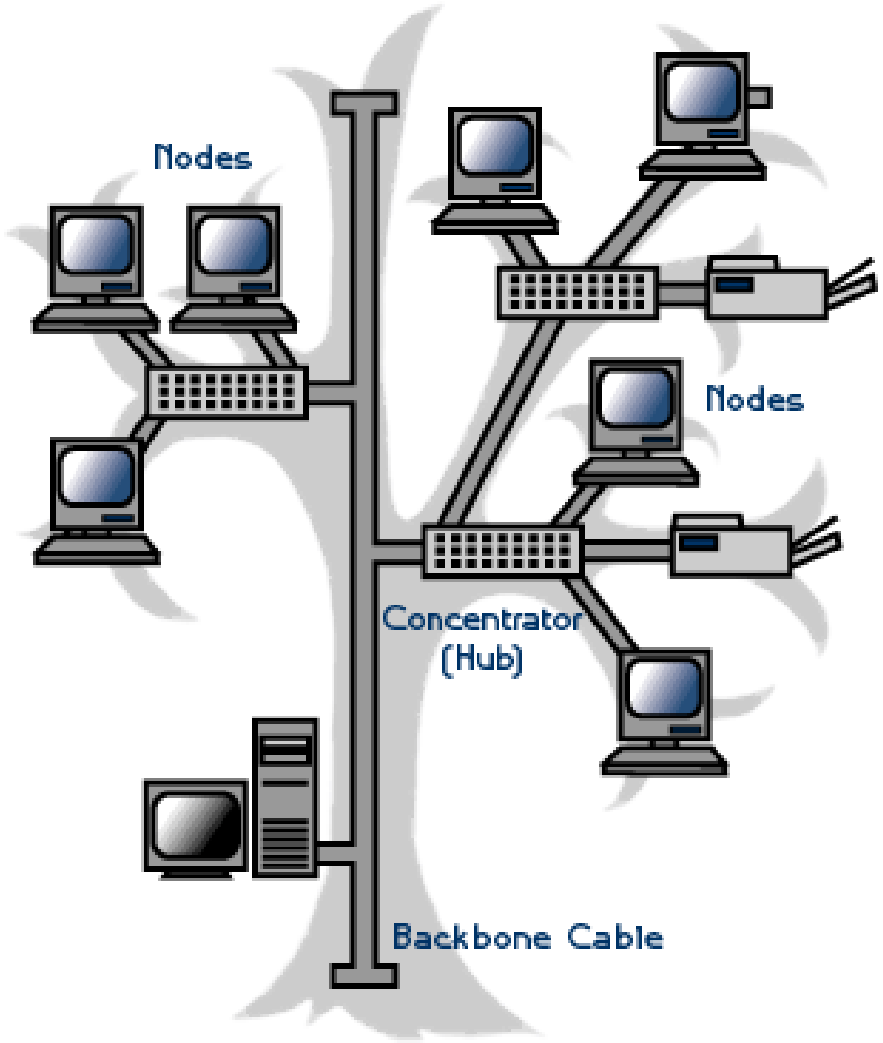
Network topologies - Bus



Network topologies - Star



Network topologies - Tree



The logical network

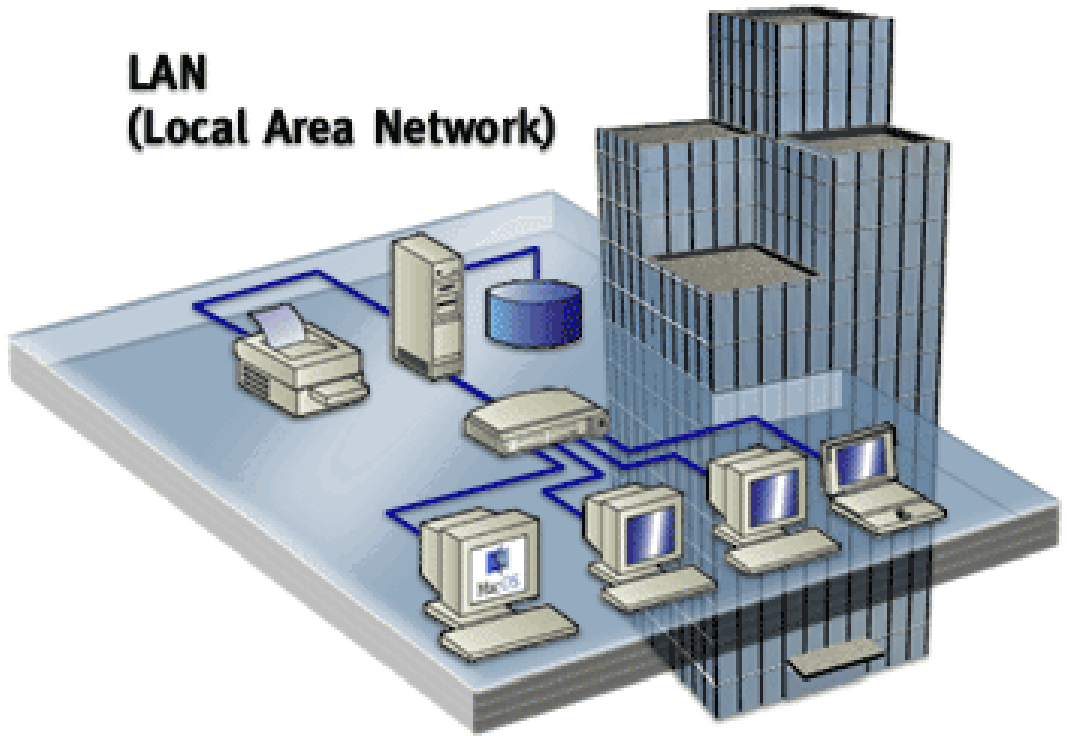
- Made up of protocols and services
- Protocols:
  - HTTP
  - FTP
  - SMTP
- Services:
  - File and pint servers
  - Active Directory

Varieties of networks

- LAN – Local Area Network
- MAN – Metropolitan Area Network
- WAN – Wide Area Network
- CAN – Campus Area Network

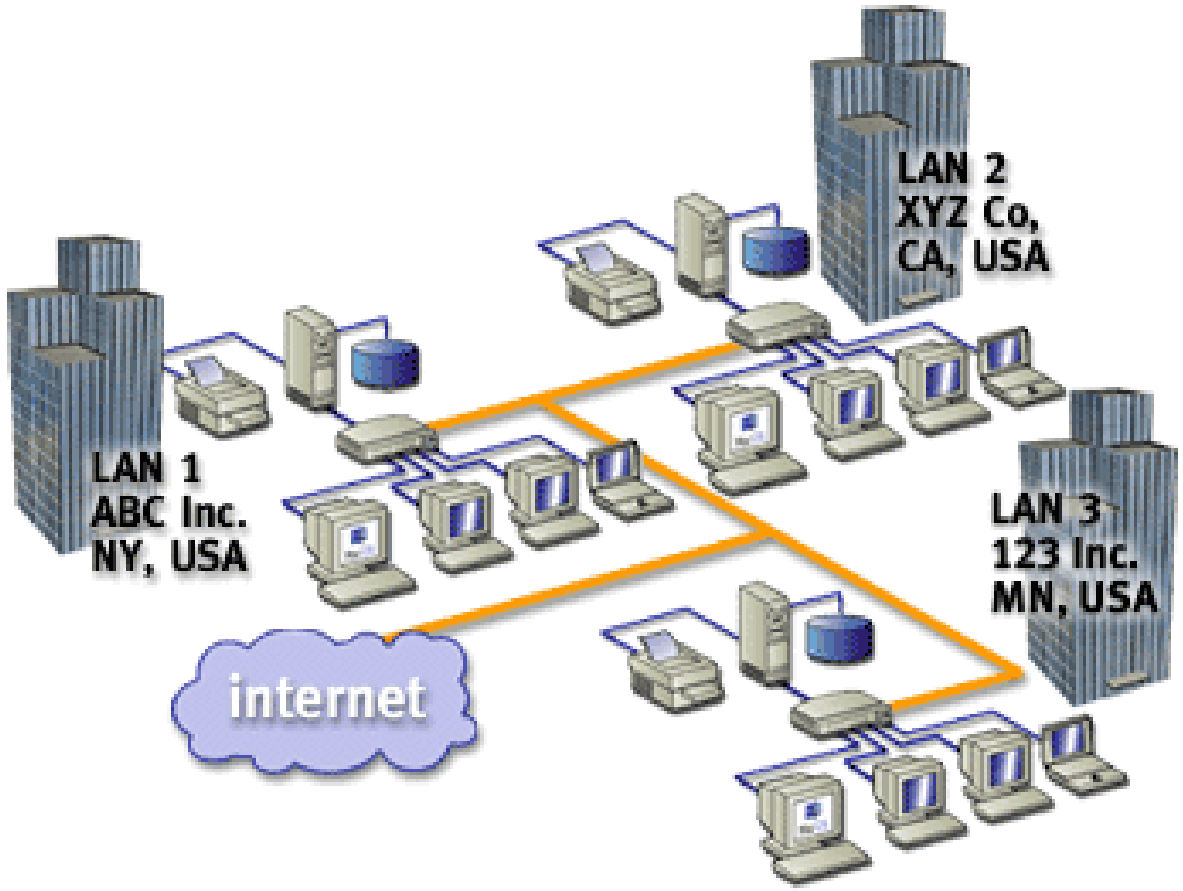
LAN

- A network confined to a relatively small area
- Limited to a small geographic area such as:
  - A single room or groups of rooms or offices
  - A single building or small localized group of buildings or a school



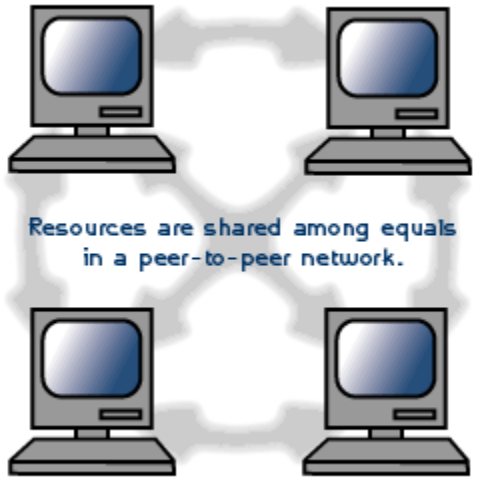
Wide Area Networks

- Networks joining together larger areas (cities, states, countries or events)
- Countries, governments, universities and individuals can be in contact with other areas within seconds

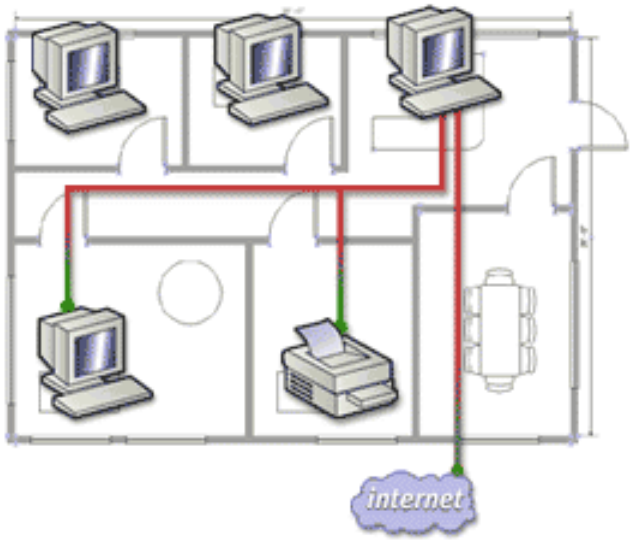


Network operating strategies

- Peer to Peer
- Client / Server

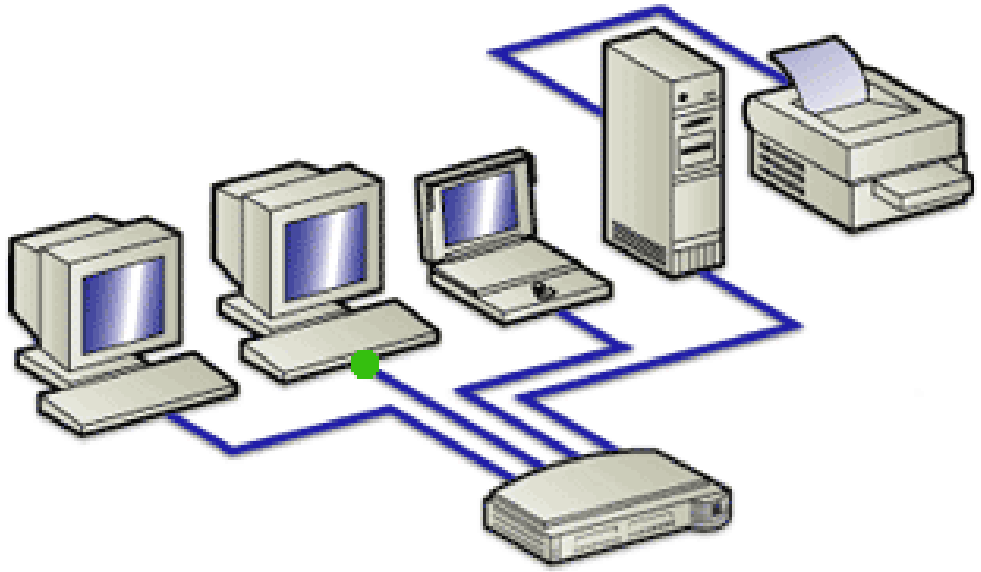


Peer-to-Peer systems



A typical computer network
(Available resources are shared by all)

Client / Server systems



A typical computer network
(Available resources controlled)

NETWORK PROTOCOLS

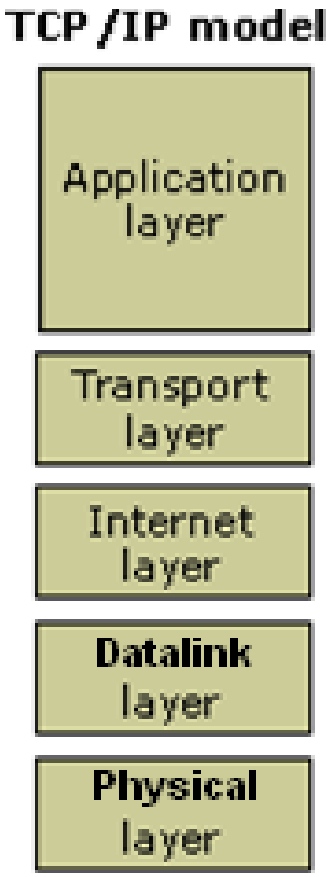
What is a Protocol?

- A set of rules for sending and receiving data across a physical network
- Handles the translation of data from applications (software) to the logical topology
- Sit on top of the logical topology
- Protocols include:
  - FTP
  - HTTP
  - SMTP
  - IP

What is TCP/IP?

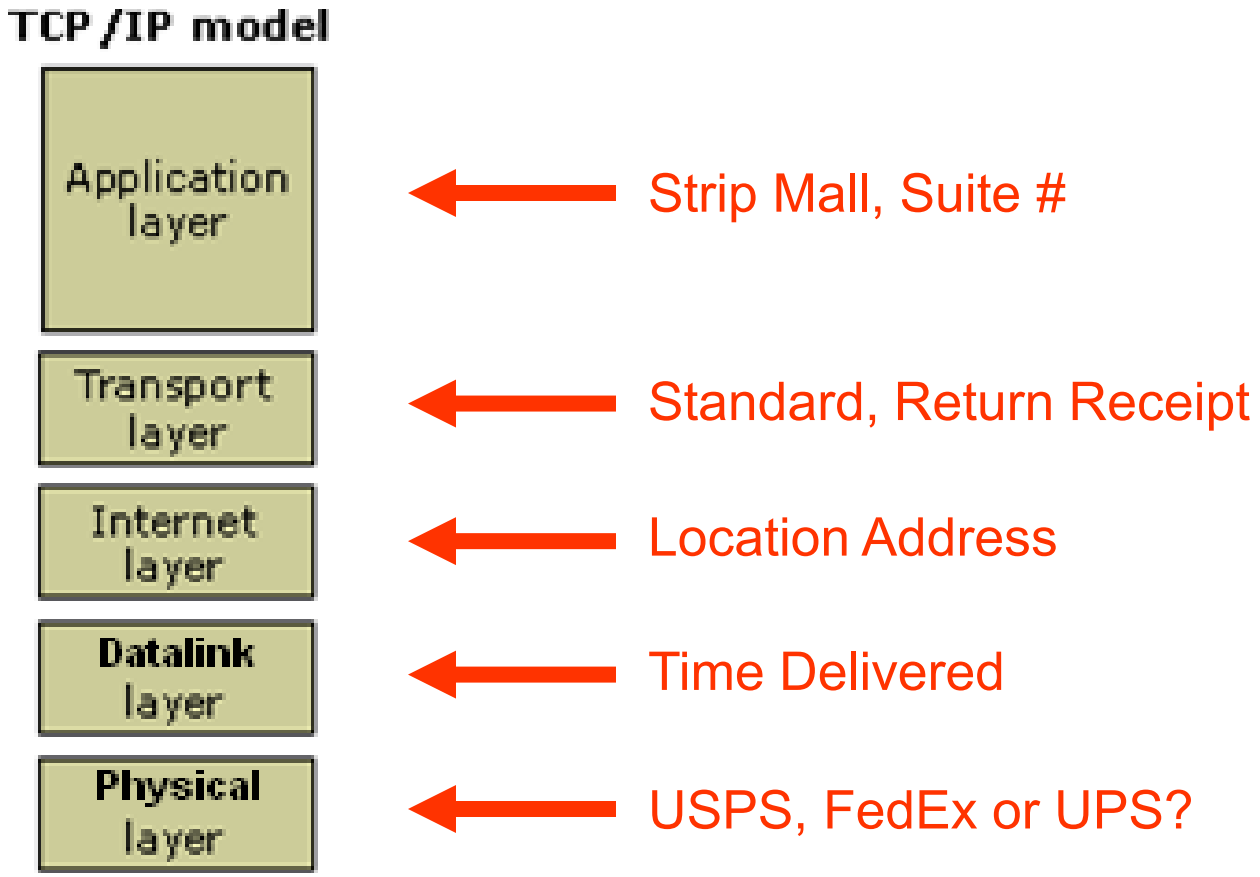
- Multifaceted protocol suite on which the Internet runs
- TCP/IP:
  - TCP – Transmission Control Protocol is the protocol that ensures reliable delivery of packets to their destinations
  - IP – Internet Protocol is the part of the suite responsible for providing addressing and routing services to packets

TCP/IP or Internet model



←	Services Layer	Who?
←	Delivery Layer	How?
←	Addressing & Security Layer	Where?
←	Link Layer	When?
←	Physical Layer	What?

TCP/IP model analogy



TCP

- Links the application layer to the network layer
- Performs packetization and reassembly
  - Breaks up a large message into smaller packets
  - Numbers the packets
  - Reassembles them in order at destination
- Ensures reliable delivery of packets
- Consumes more bandwidth than UDP

UDP

- Protocol used for connectionless routing in TCP/IP suite (no acknowledgements, no flow control)
- Uses a small packet header of 8 bytes containing 4 fields:
  - Source port
  - Destination port
  - Message length
  - Header checksum
- Used for control messages that are small, such as DNS, DHCP, RIP and SNMP
- Consumes less bandwidth than TCP

BASIC TCP/IP ADDRESSING

Physical address

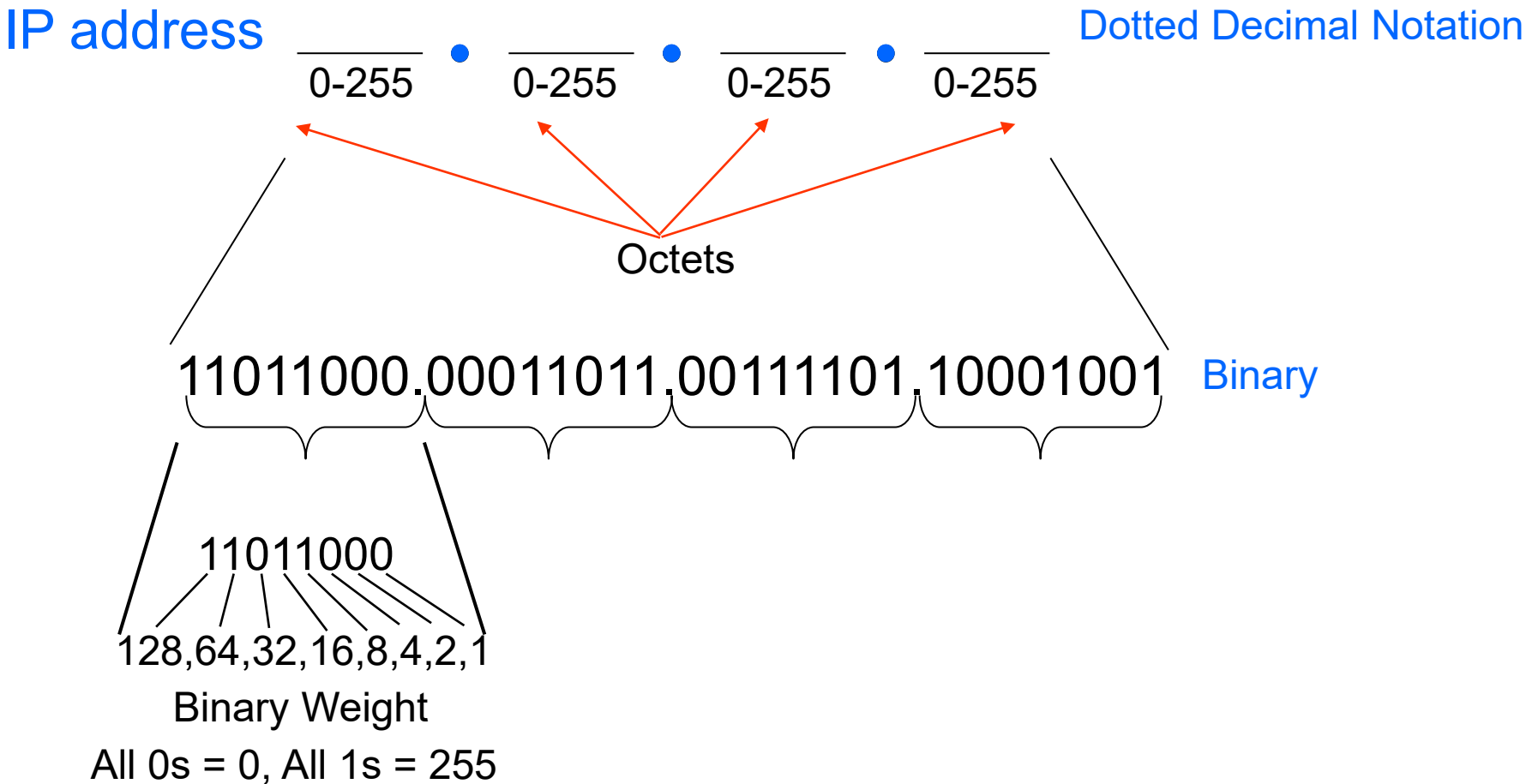
- Network Interface Card (NIC) has a unique and permanent physical address
- Every NIC on a local net listens to every transmission
- Media Access Control (MAC)
- Fixed, hard-coded number assigned at the time of manufacturing (unchangeable)
- Serial number (like RF Sensors)
  - Example: 00-08-74-4C-7F-1D

IP Address

- When connecting multiple devices, each device must have a unique identification called an IP Address
- An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network
- An IP address is represented as 4 three-digit groups of decimal values, in the range 0 to 255 (known as octets) separated by decimal points
  - Example: 140.179. 220. 200 in Dotted Decimal
- IP Addresses are referred to as Public or Private
- Public IP is assigned to customer by ISP
- Private IP is assigned by local IT admin or hardware itself
- IP runs over Ethernet and several other hardware interfaces

Network architecture

- IP version 4
- An IP address = 32 bits is made up of a group of numbers (NET ID, HOST ID) whose NET ID identifies a network and HOST ID identifies a machine on the network



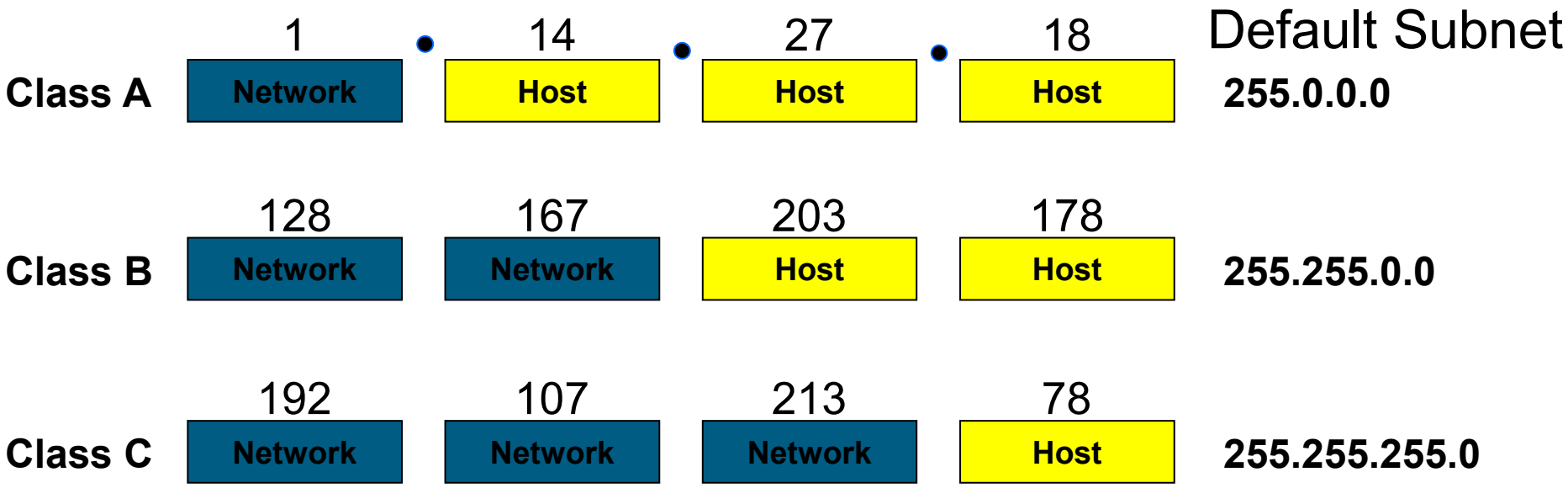
Address ranges or classes

Class	Purpose	Address Values	Networks/Class	Subnet Mask	Hosts/Net
A	Few Large Organizations	0.0.0.0 - 126.255.255.255	126	255.0.0.0	16,777,214
B	Medium-size Orgs	128.0.0.0 - 191.255.255.255	16,384	255.255.0.0	65,534
C	Relatively Small Orgs	192.0.0.0 - 223.255.255.255	2,097,152	255.255.255.0	254
D	Multicast Groups	224.0.0.0 - 239.255.255.255	N/A	N/A	N/A
E	Experimental	240.0.0.0 - 255.255.255.255	N/A	N/A	N/A

Special cases

- 127.0.0.0 – 127.255.255.255 - Loopback address
  - Most software only uses 127.0.0.1 to ping itself and to test NIC and cabling
- 169.254.0.0 – 169.254.255.255 - Auto config address
  - Reserved for Automatic Private IP Addresses and is assigned by the Windows operating system when no valid address can be found for the device
- 255.255.255.255 - Broadcast Address
  - Cannot be assigned to a host
- 0.1.1.1 - No zeros allowed in the first octet

Address ranges or classes



Static or Dynamic

- Static IPs:
  - Assigned manually
  - Remain the same
- Dynamic IPs:
  - Assigned by network equipment DHCP (Dynamic Host Configuration Protocol) server
  - Can change from time to time
  - Used to assign TCP/IP configuration parameters to nodes on a network
  - Can assign IPs, Subnet Masks, and DNS settings

Static IP Addresses

- If IP address were static, we could connect to device by putting the IP address in the URL field of our browser
- When IP address changes, customers who want to connect for remote viewing do not know the new IP address and are unable to connect

Dynamic IP Addresses

- Dynamic Host Control Protocol (DHCP) assigns IP addresses
- The customer uses DHCP for a period called a lease
- When lease expires, ISP will provide a new and different IP address

DNS – Domain Name Service

- The Domain Name Service (DNS) provides a lookup service to correlate the Domain Names to the public IP addresses
- DNS servers keep track of known Domain Names
- DNS resolvers issue host name and address conversion requests
- If DNS server cannot resolve the request, it asks a higher-level server up to the Top-Level Domains (TLDs)
- Similar to WINS and NIS
- DNS supports overall name resolution and mapping

Dynamic DNS

- DNS servers that learn a node's new IP and match it with a host or domain name
- Requires Dynamic DNS compatible router, NIC, or DHCP server that broadcasts the node's IP address to the DNS server

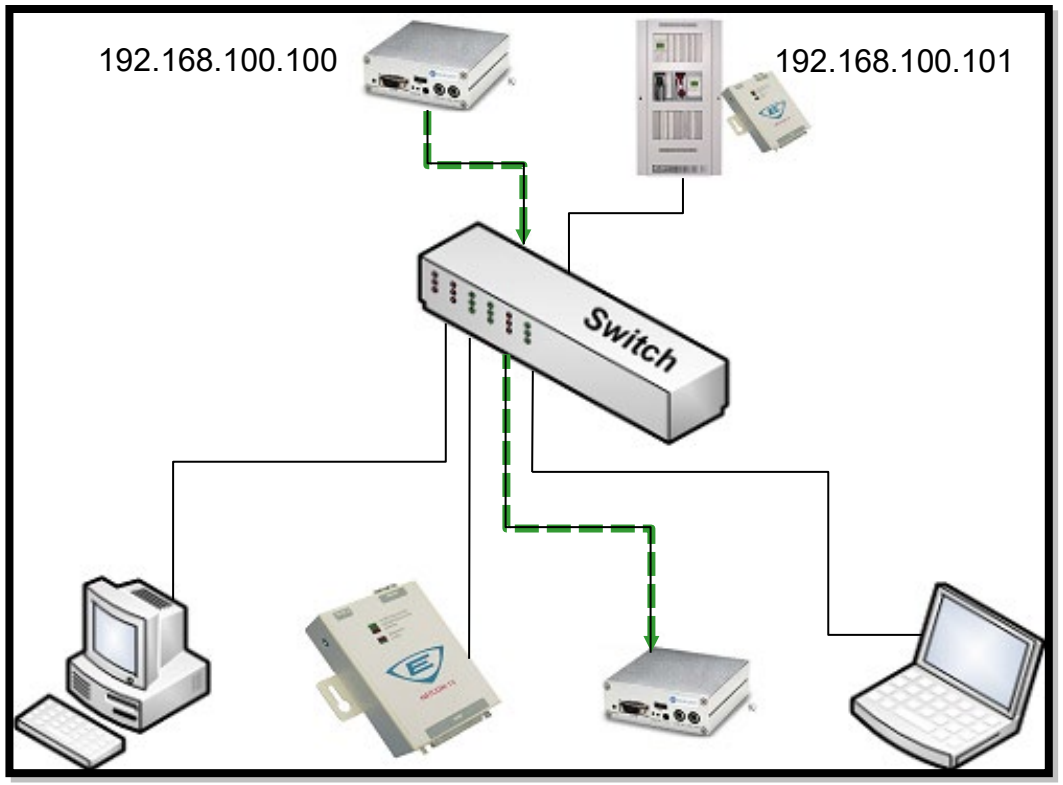
DNS to the rescue

A Dynamic DNS provider allows us to create a domain name (e.g., Fredsdeviceatmysite. com) and match it to whatever IP address the ISP server has assigned to the account where the device resides

IGMP - Internet Group Management Protocol

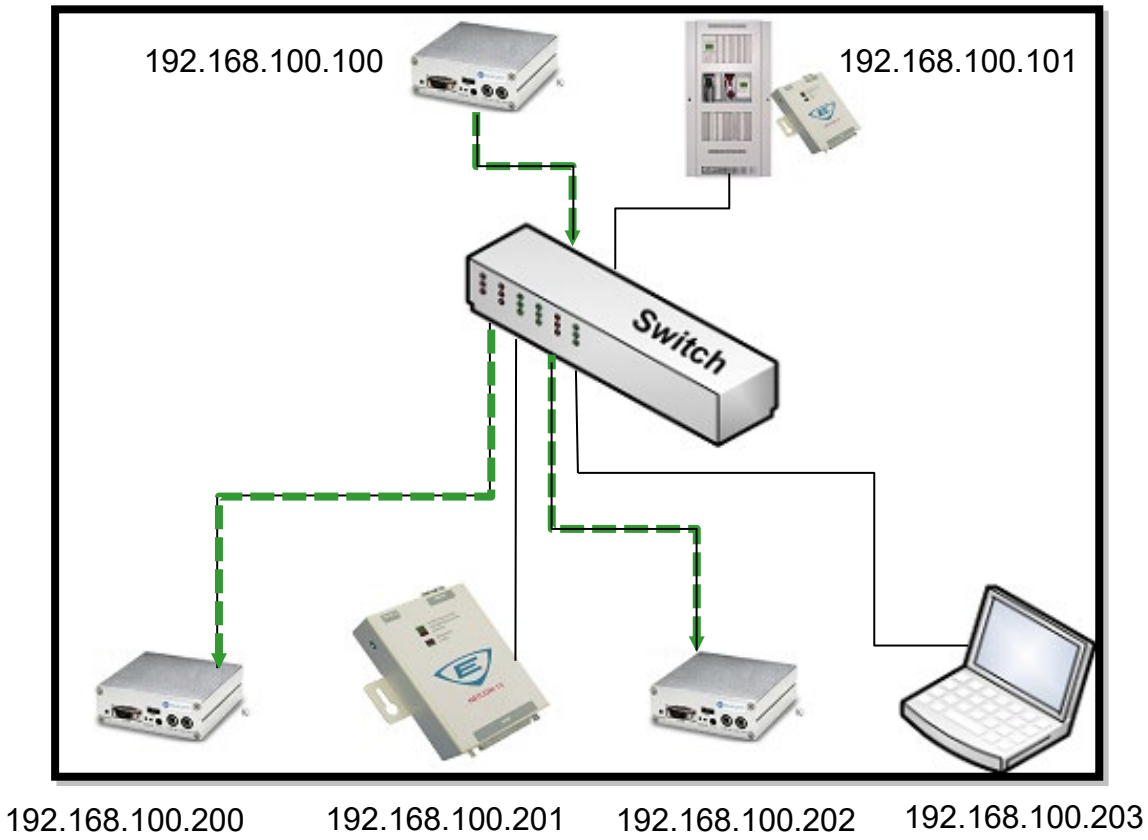
- Standard IP protocol supported by most LAN/WAN vendors in traditional LAN products, ATM, and gigabit Ethernet solutions
- Used to establish host memberships in particular multicast groups on a single network
- Allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group

Unicast: point-to-point



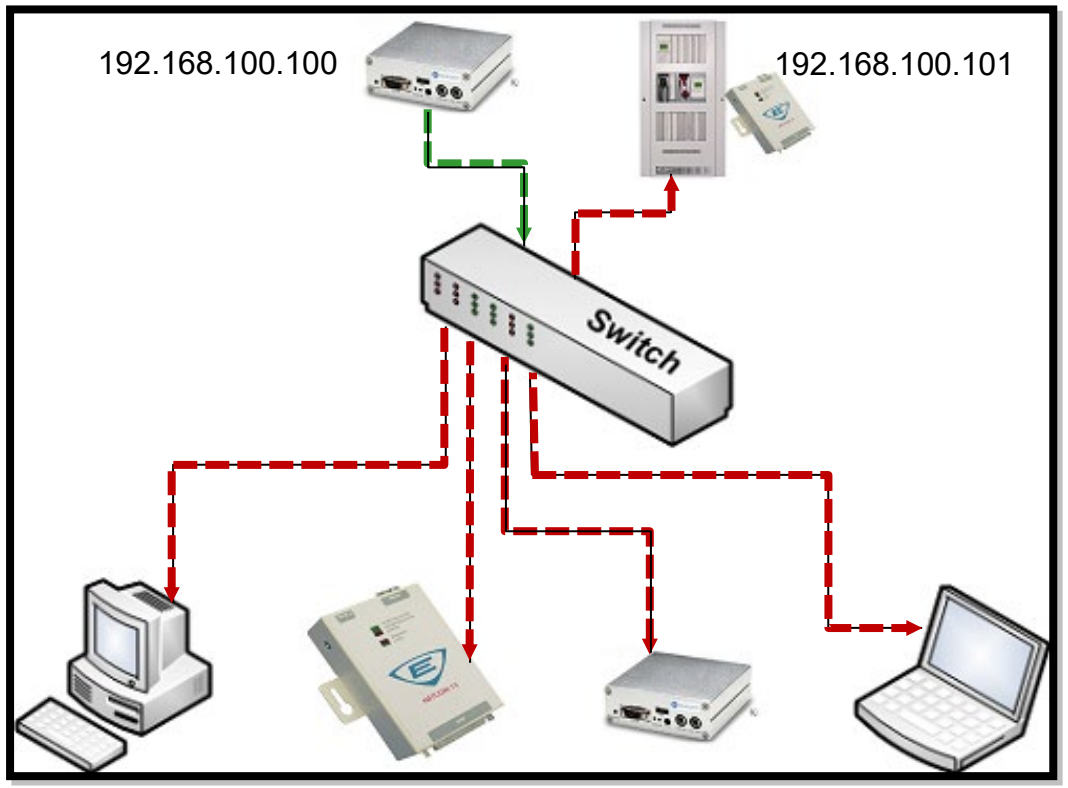
Device (192.168.100.100) sends packets to destination (192.168.100.202)

Multicast: point-to-multi-point



Device (192.168.100.100) sends packets to multi-destinations (224.16.32.10)

Broadcast: point-to-all



Device (192.168.100.100) sends packets to all destinations (255.255.255.255)

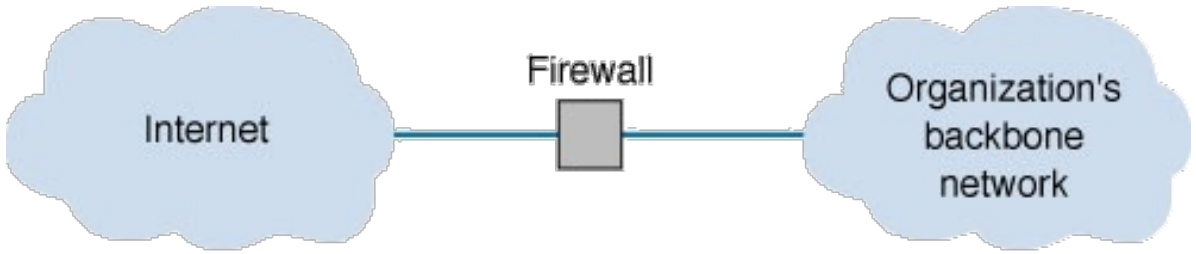
INTERNET SECURITY

Firewalls

- Firewalls prevent unwanted packets into the network
- Some PC security services disable UDP streaming
- Managed switches and routers can close unwanted ports
- Every Edwards network component utilizes different UDP and TCP ports ensure the IT department has ports open before you install

Firewalls

- Prevent intruders (by securing Internet connections)
  - From making unauthorized access and denial of service attacks to your network
- Could be a router, gateway, or special purpose computer
  - Examines packets flowing into and out of the organization's network
  - Restricts access to that network
  - Placed on every connection that network has to Internet
- Main types of firewalls:
  - Packet level firewalls (packet filters)
  - Application-level firewalls (application gateway)



Packet filters

- Examine the source and destination address of packets passing through
  - Allow only packets that have acceptable addresses to pass
  - Examine IP addresses and TCP ports
    - Firewall is unaware of applications and what the intruder is trying to do
- IP spoofing remains a problem
  - Done by changing the source address of incoming packets from their real address to an address inside the organization's network
    - Firewall will pass this packet

Ports

- Support connection to applications
- System of logical channels called ports
- Identified by a port number
- Logical pipelines that allow data to flow from the application to (and from) the protocol software
- Ports can be vulnerability of node

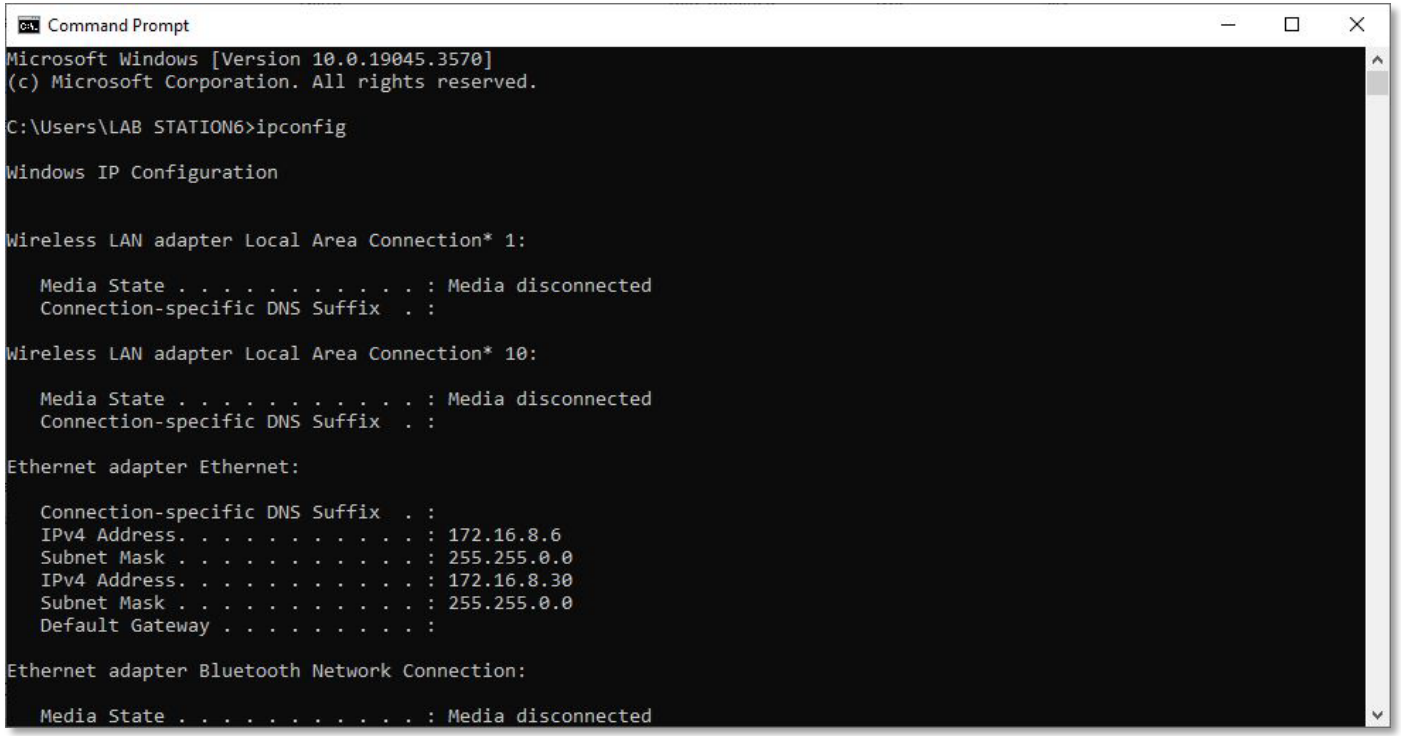
Port forwarding

- Function of a router allowing connections from the WAN side on a specific port to be forwarded to a specified LAN address
- Allows LAN Node with a private IP to receive incoming unsolicited connections
- Necessary for connection to networking equipment to not require public IP
- Be cautious of other services using same port number, e.g., Http (port 80)

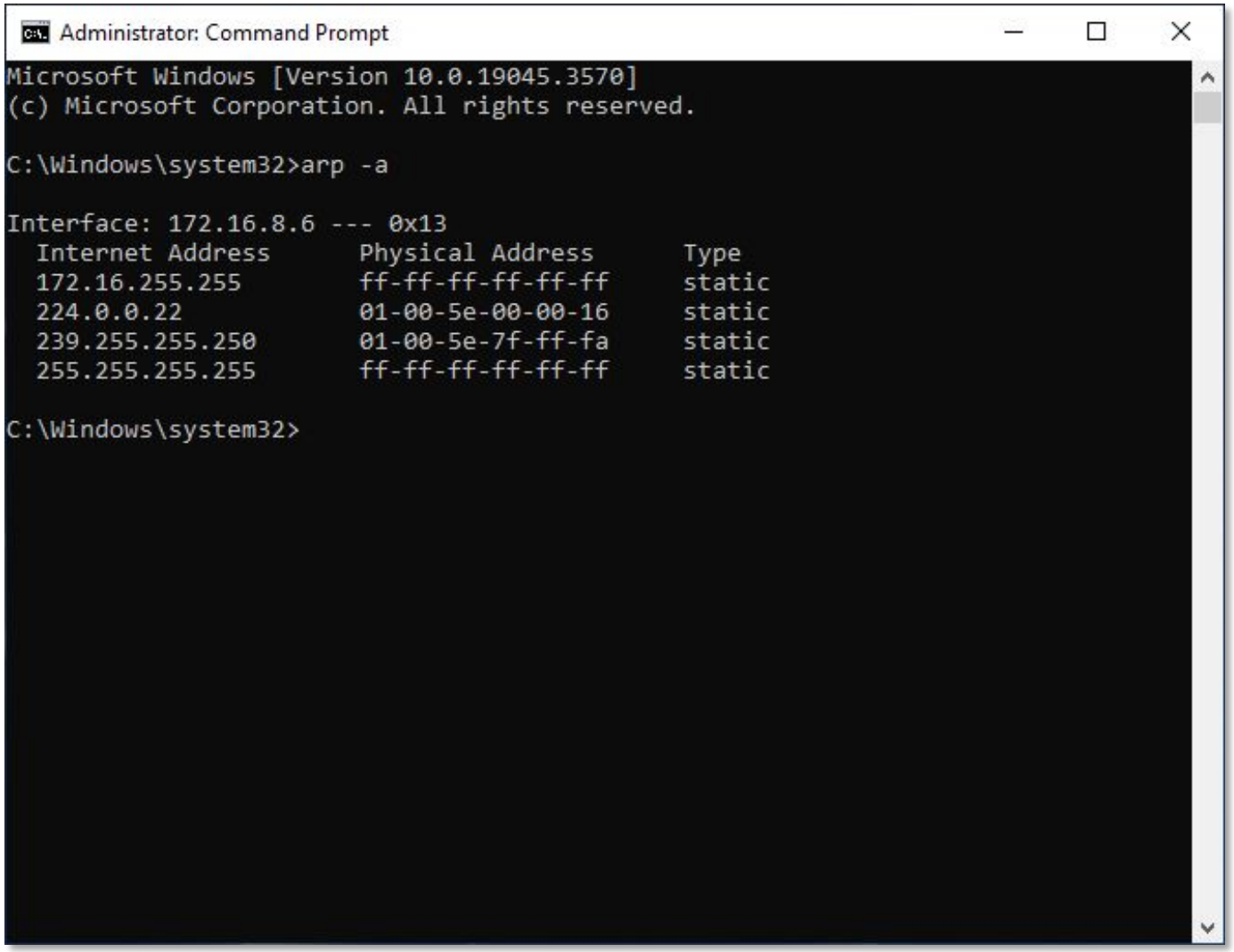
BASIC TROUBLESHOOTING TOOLS

ipconfig

- Displays the status and details of your Ethernet adaptor and node
- To obtain a list of extended ipconfig commands at the command prompt type [ipconfig ?]



ARP -A

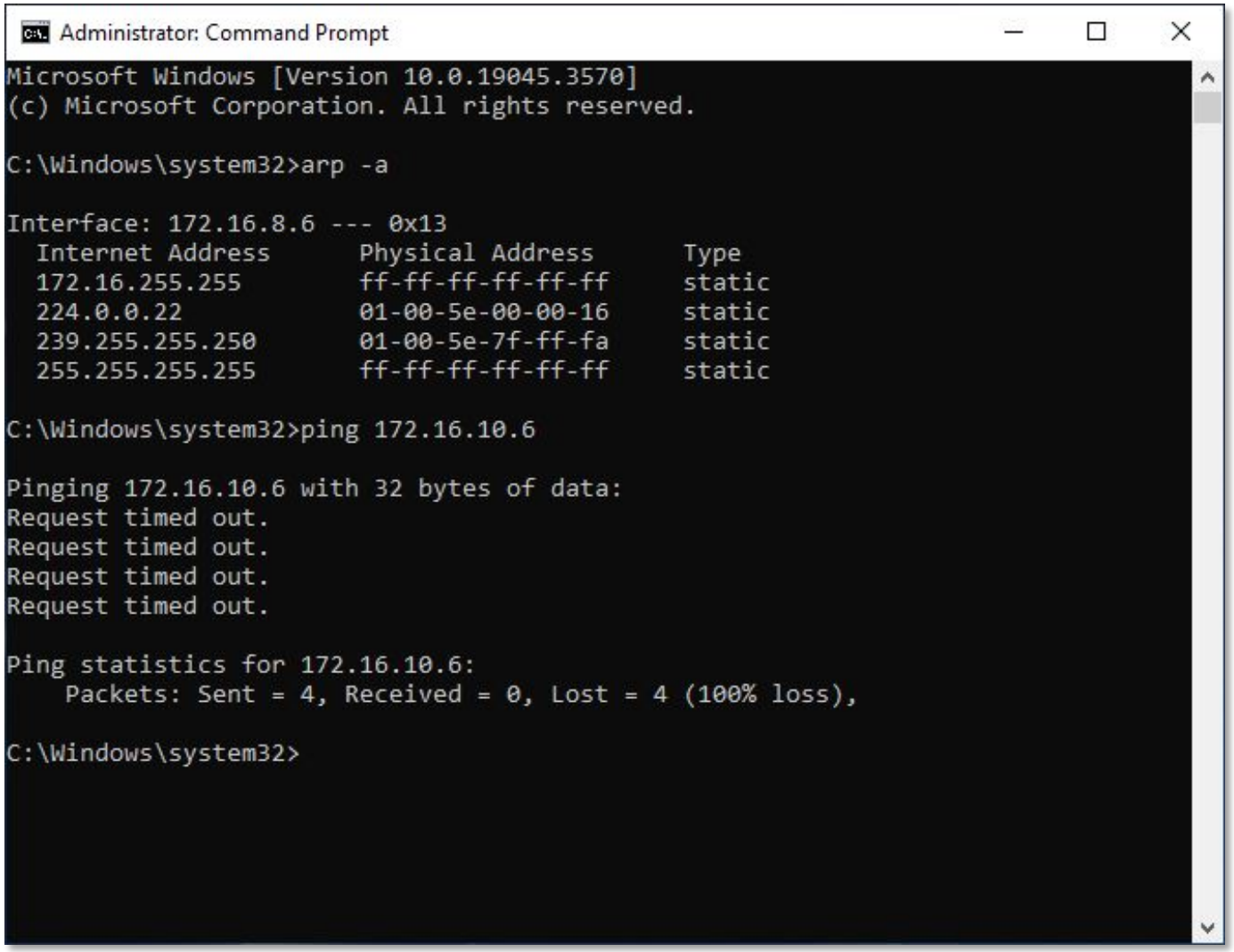

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>arp -a
Interface: 172.16.8.6 --- 0x13
Internet Address Physical Address Type
172.16.255.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Windows\system32>

Pinging (Packet InterNet Groper)

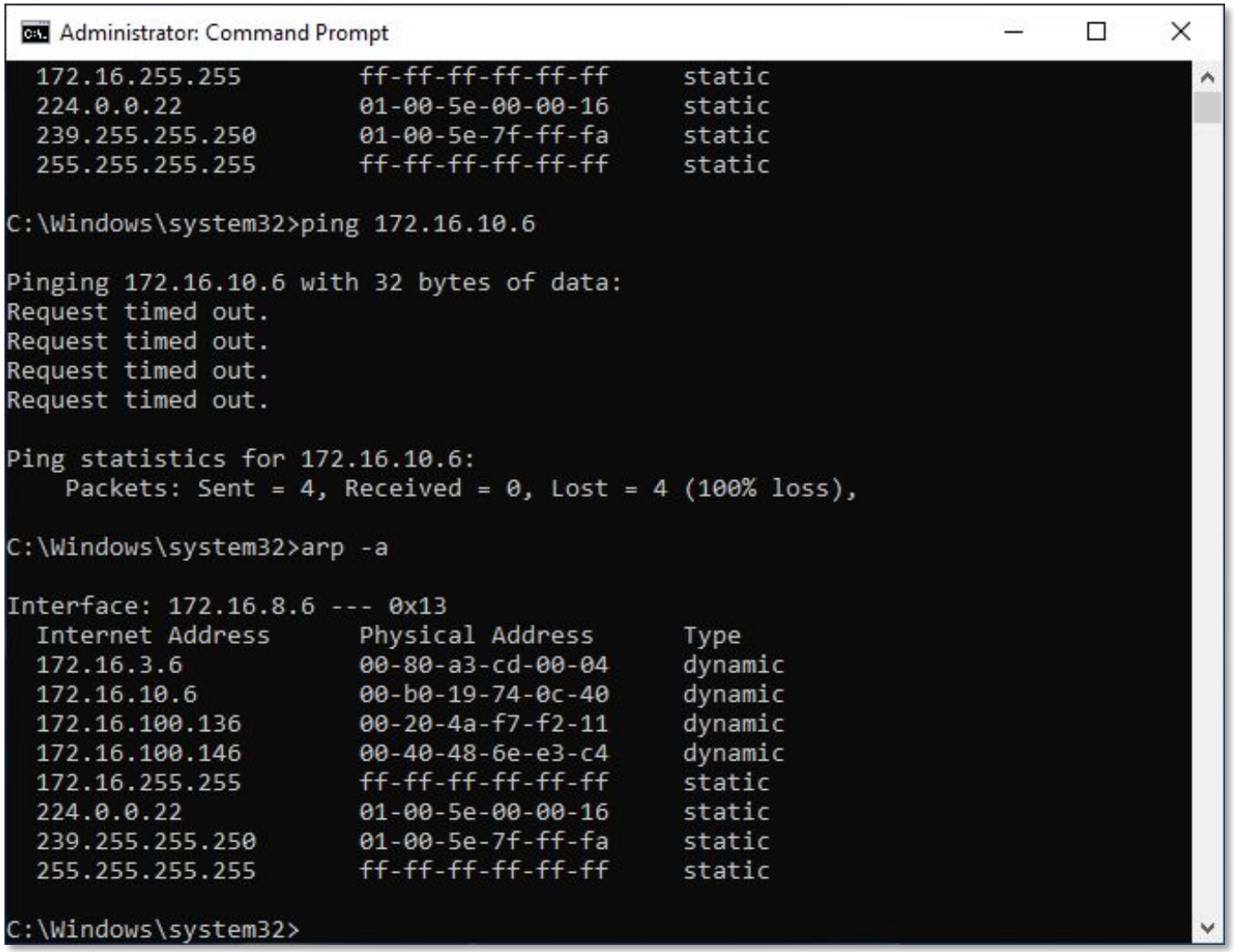
Some of the extended ping command set include:

- ping 172.16.10.6 – will ping an IP address
- ping domainname – will ping a domain by name
  – Example “ping google.com”
- To obtain a list of the ping commands, type [ping/?]

Ping 4-FWALx

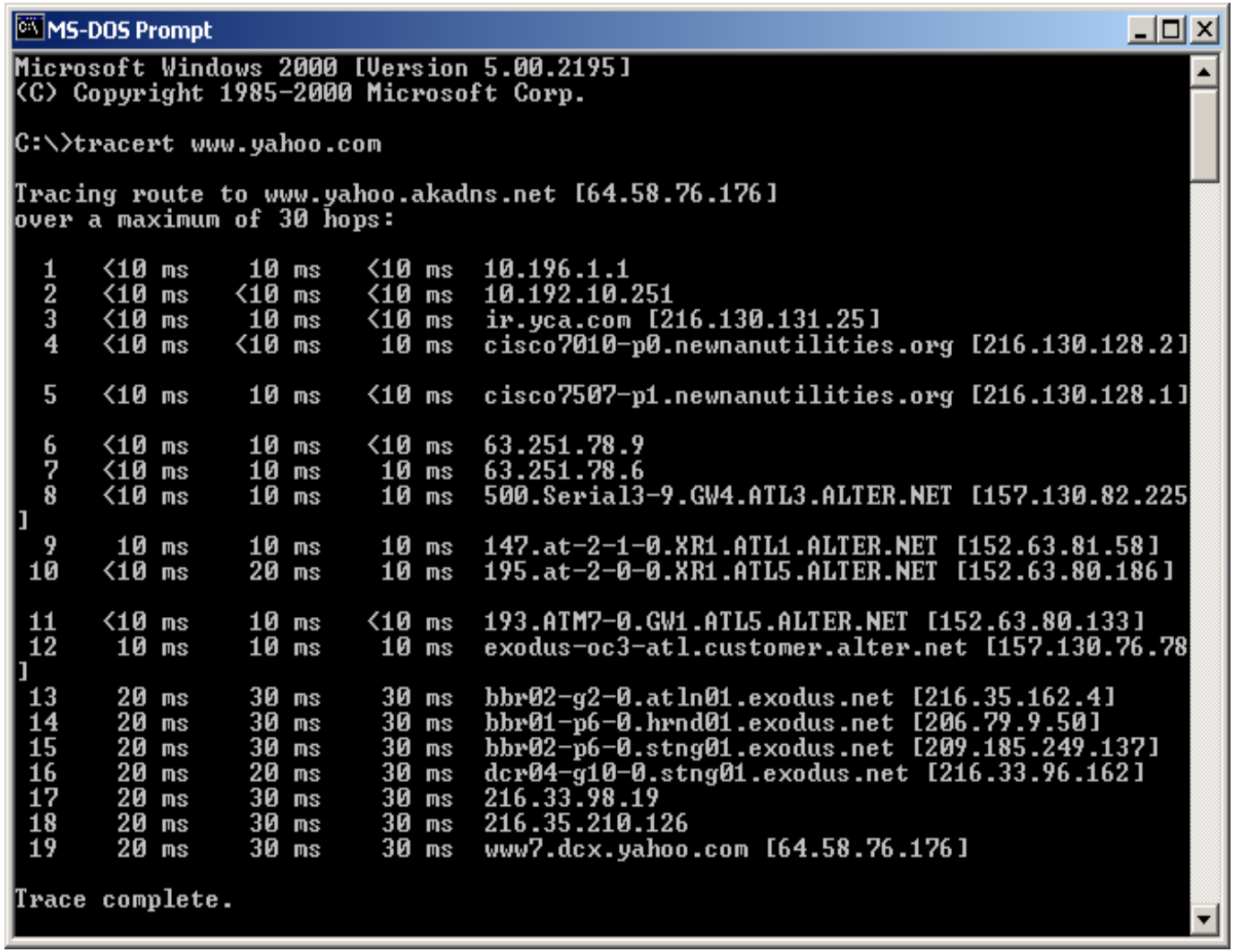

Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>arp -a
Interface: 172.16.8.6 --- 0x13
Internet Address Physical Address Type
172.16.255.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Windows\system32>ping 172.16.10.6
Pinging 172.16.10.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.10.6:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\system32>

ARP -A


Administrator: Command Prompt
172.16.255.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Windows\system32>ping 172.16.10.6
Pinging 172.16.10.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.10.6:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\system32>arp -a
Interface: 172.16.8.6 --- 0x13
Internet Address Physical Address Type
172.16.3.6 00-80-a3-cd-00-04 dynamic
172.16.10.6 00-b0-19-74-0c-40 dynamic
172.16.100.136 00-20-4a-f7-f2-11 dynamic
172.16.100.146 00-40-48-6e-e3-c4 dynamic
172.16.255.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Windows\system32>

Tracert.www.yahoo.com

tracert *hostname or address* traces the route that a packet takes from the current workstation



EDWARDS LEARNING CENTER