How Computer Networks Work

Introduction

Networks

- Dictionary: *Network (n) - a system of interconnected computer systems, terminals, and other equipment allowing information to be exchanged*
- Can be as simple as two computers in one room or as large as thousands of computers all over the world

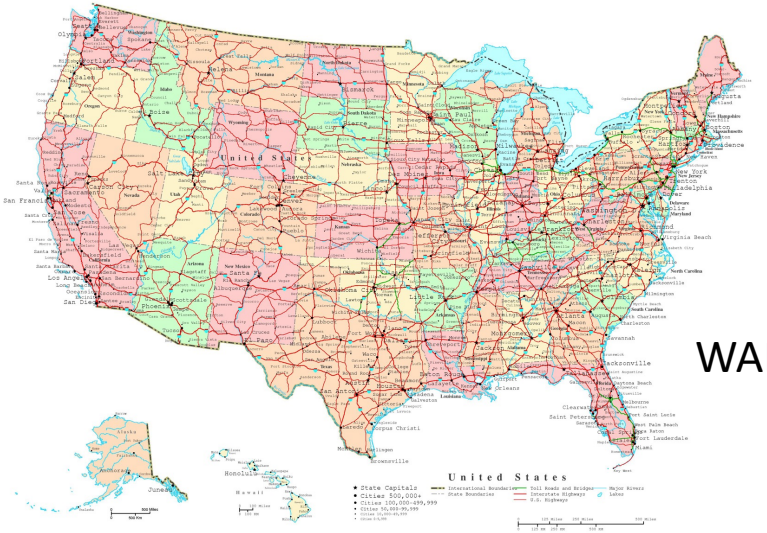
Network Classifications

- Local area network (LAN)—Example: Computers in an office
- Metropolitan area network (MAN)—Example: University or city
- Wide area network (WAN)—Example: Company with offices around the world

Network Classification

LAN

MAN

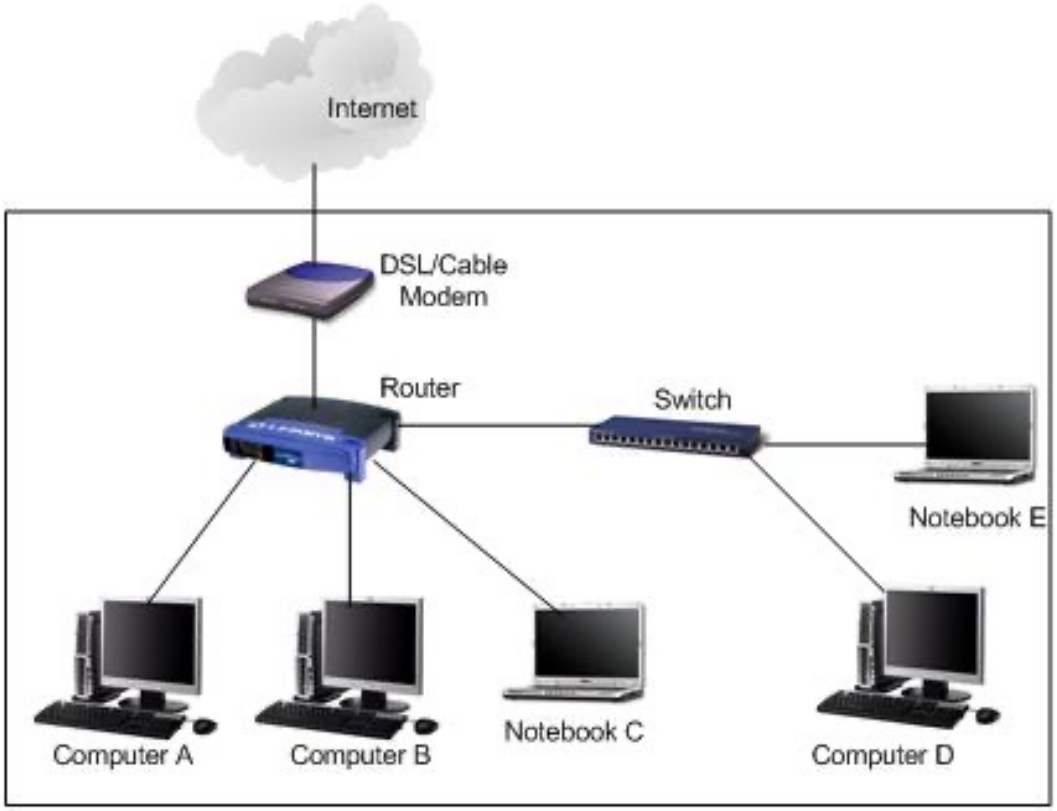


WAN

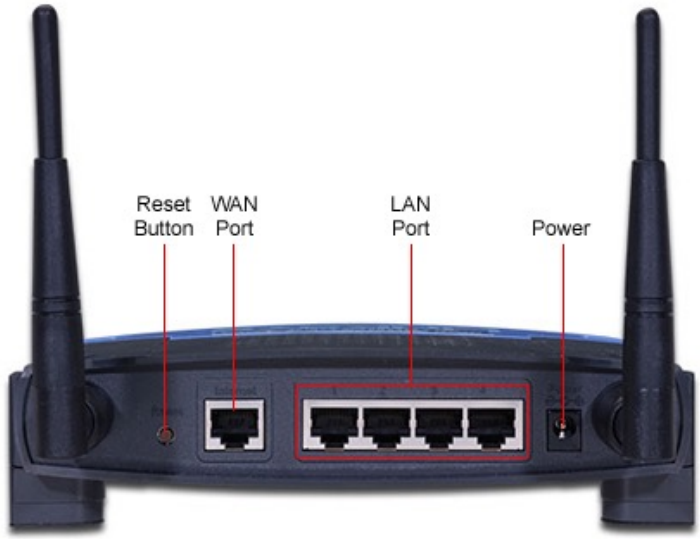
How Networks Work

How Routers and Switches Work

Basic Network Setup



Wireless Router



Linksys WRT54GL Wireless Broadband Router

Switch

- Multiple ports
- Switch makes decision in hardware (internal main processer)
- Designed to connect additional wired devices over Ethernet

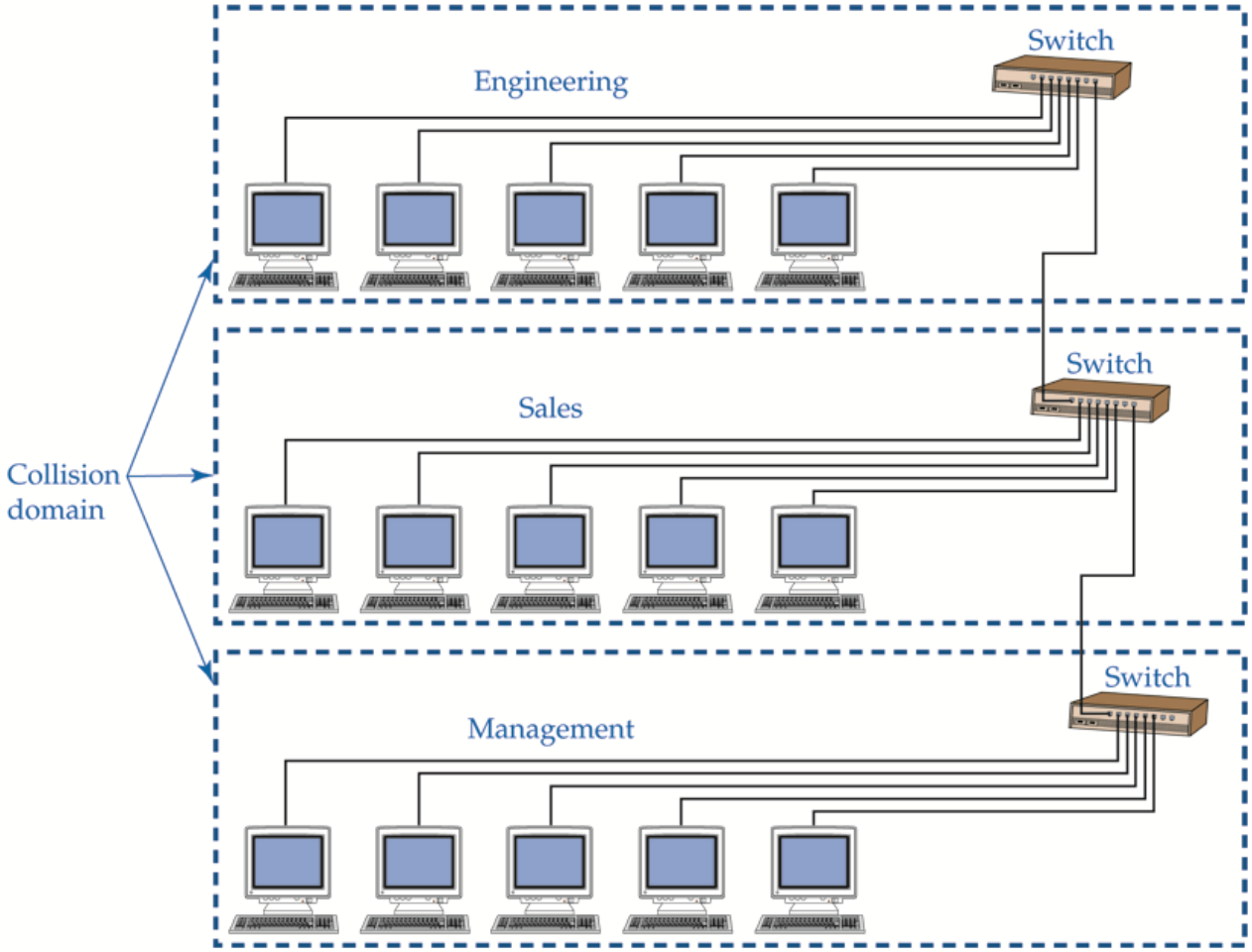
Switch

- A switch is used in a wired network to connect Ethernet cables from a number of devices together. The switch allows each device to talk to the others. Switches aren't used in networks with only wireless connections, since network devices such as routers and adapters communicate directly with one another, with nothing in between.
- Although you can use the ports on the back of a router or modem to connect a few Ethernet devices together, depending on the model, switches have a number of advantages:
  - Switches allow dozens of devices to connect.
  - Switches keep traffic between two devices from getting in the way of your other devices using the same network.
  - Switches allow control of who has access to various parts of the network.
  - Switches allow you to monitor usage.
  - Switches allow communication (within your network) that's even faster than the Internet.
  - High-end switches have pluggable modules to tailor them to network needs.

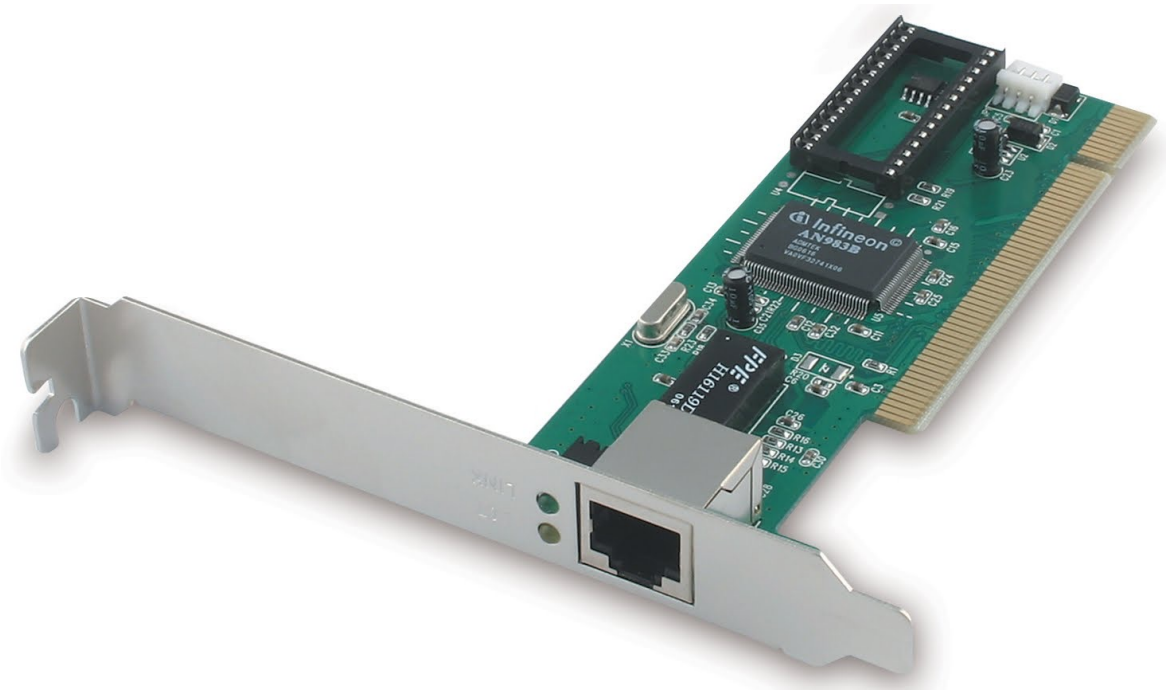
Network Segmenting Devices

- Physical devices can also be used to segment a network
- Bridge and switch segment a network at the data link layer
- A router segments the network at the network layer

Segmenting with Switches or Routers



Network Interface Card (NIC)



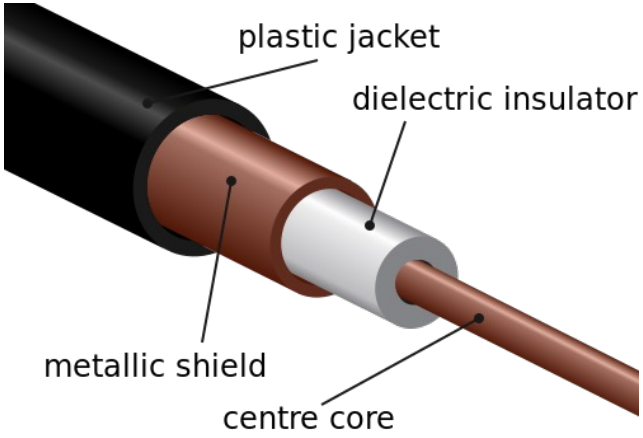
Network Interface Card (NIC)

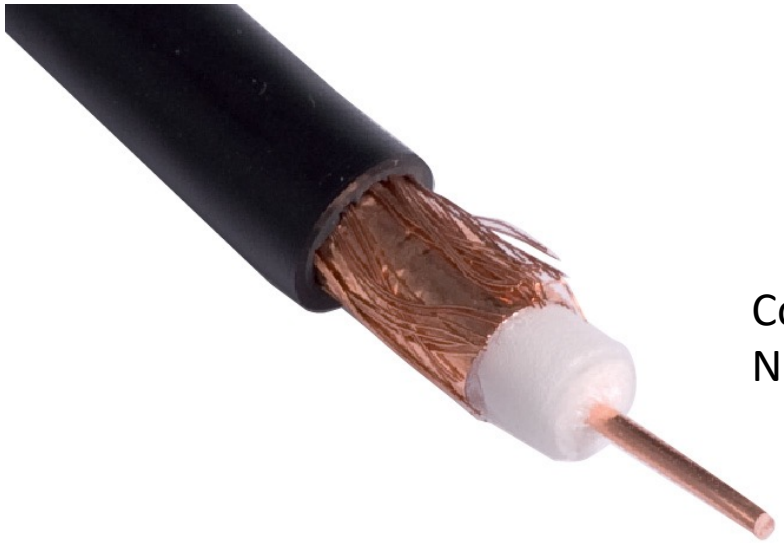
- Must match physical communication requirements of the network
- Requires driver to communicate with other computer hardware
- Contains unique identifiers:
  - Physical: MAC (media access control) address
  - Logical identification: Computer name

Media Types

- Copper core cable—Most common media; plastic or synthetic insulation
- Network Cables—Cat5/5e, Cat6 Twisted pair
- Fiber-optic cable—Has glass or plastic core
- Radio waves—Carries signals in wireless networks
- Infrared light—Beam used to transport digital signal

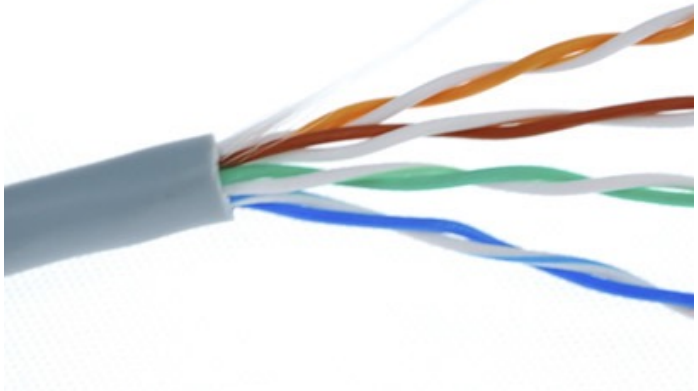
Coaxial Cable





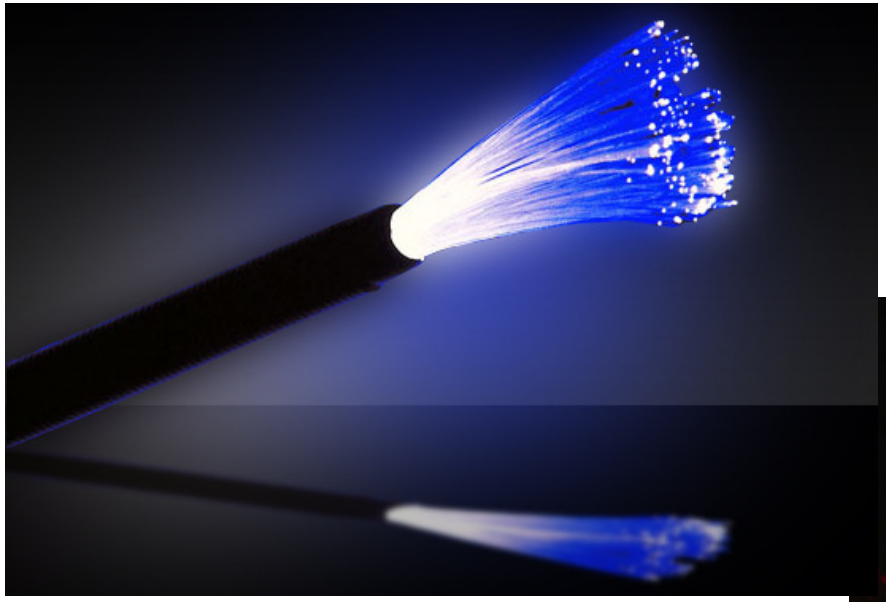
Common Types: RG – 59, RG – 6
Number of Shields can be Single, Double, etc.

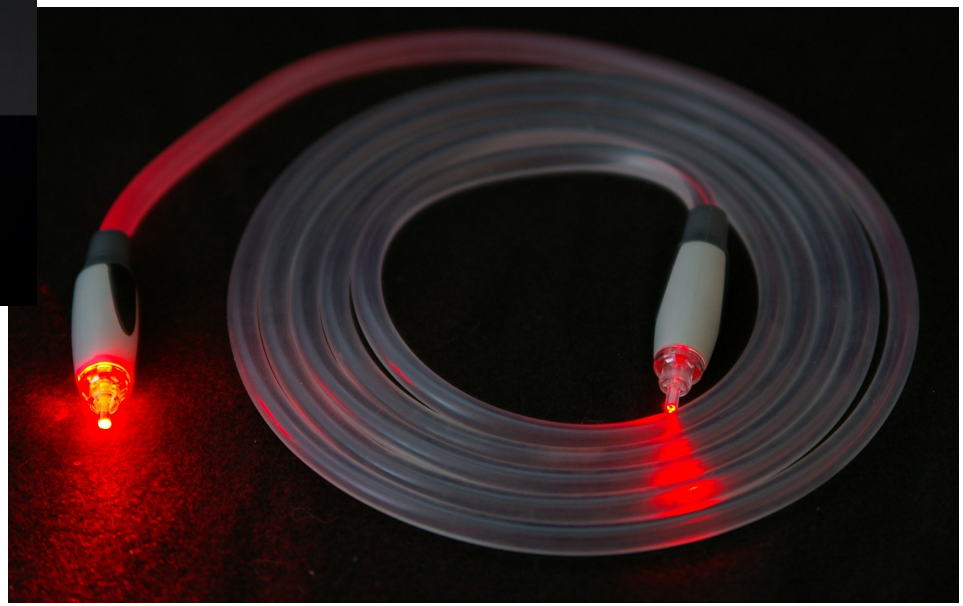
Network Cable



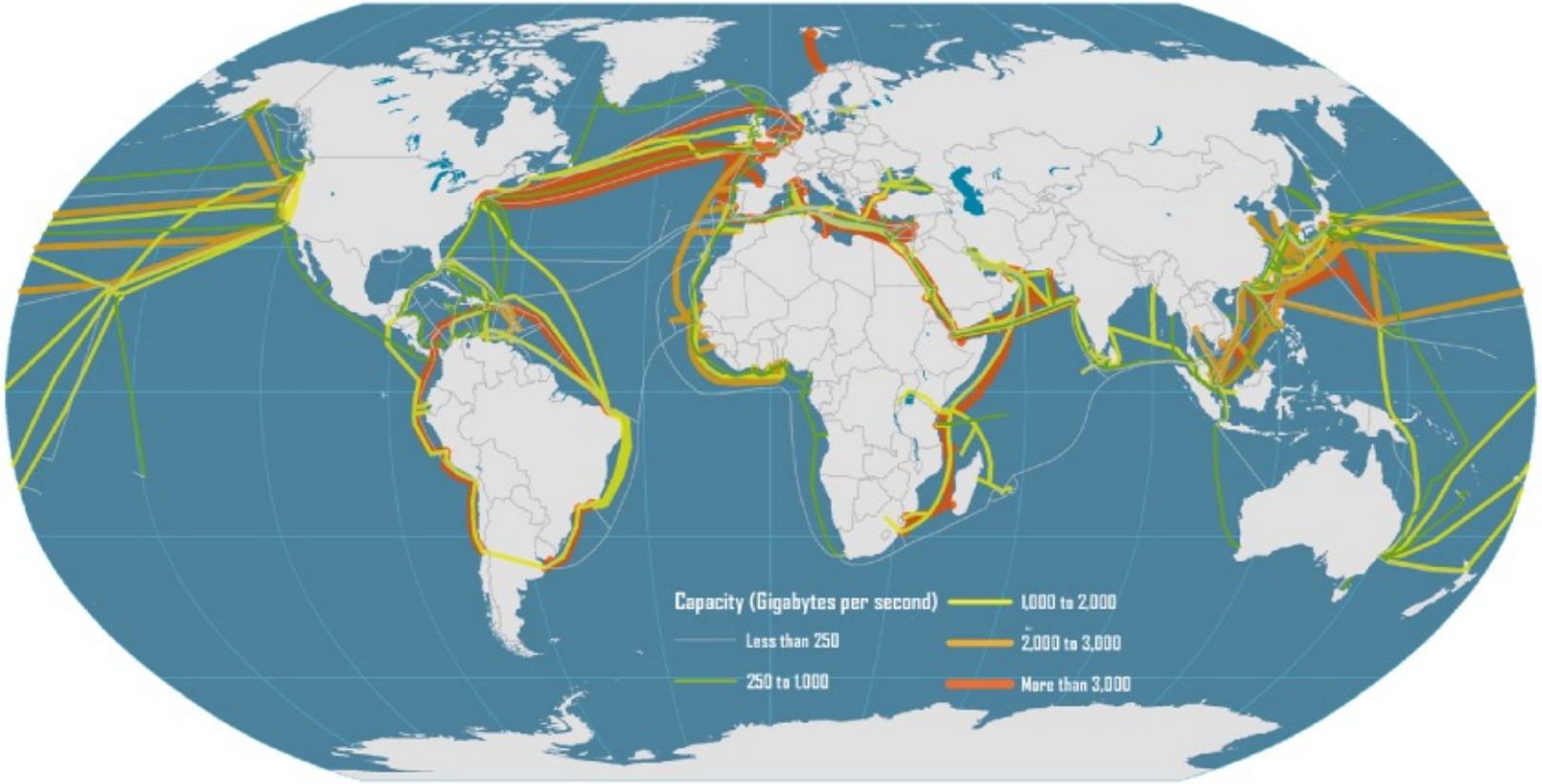
Category 5e (Cat 5e) standardized cable for Ethernet

Fiber Optic





Transcontinental "Submarine" Network Cables



How Networks Work

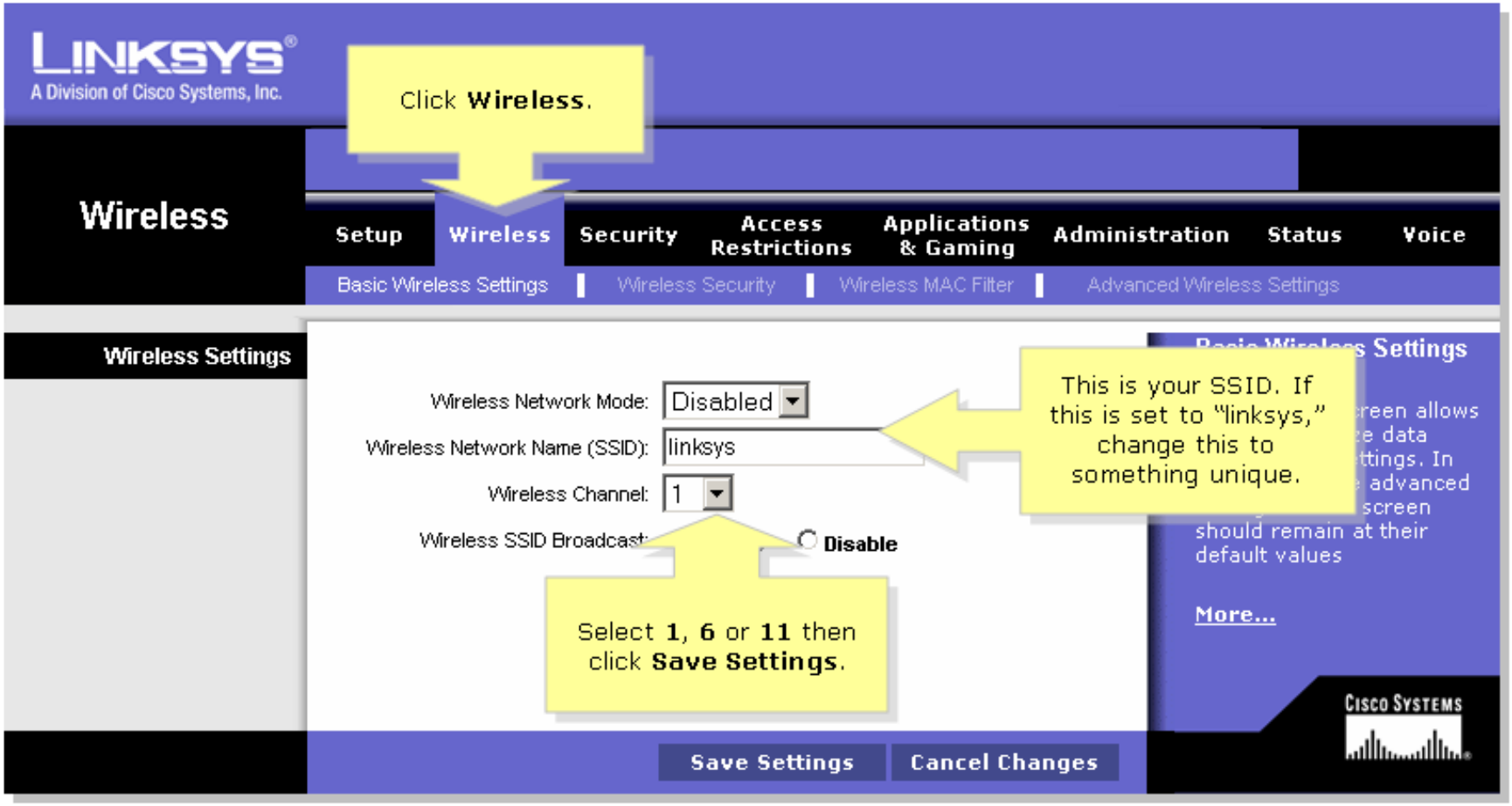
How Wireless Networks Work

Typical Home Network

Service Set Identifier (SSID)

- Identifies wireless network
- Similar to workgroup name
- All wireless network devices are configured with a default SSID (i.e., Linksys)
- To secure the wireless network, the default SSID should be changed

SSID


LINKSYS
A Division of Cisco Systems, Inc.
Click Wireless.
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Voice
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Wireless Settings
Wireless Network Mode:
Disabled
Wireless Network Name (SSID):
linksys
Wireless Channel:
1
Wireless SSID Broadcast:
Disable
This is your SSID. If this is set to "linksys," change this to something unique.
Select 1, 6 or 11 then click Save Settings.
should remain at their default values
More...
Cisco Systems
Save Settings
Cancel Changes

How Networks Work

How TCP/IP Works

Protocol

- Set of rules governing communication between devices on a network
- Determines:
  - How devices identify each other
  - Method of data exchange
  - Size of each packet
  - Timing for packet transmission
  - Signal to be used to end a session

Protocols

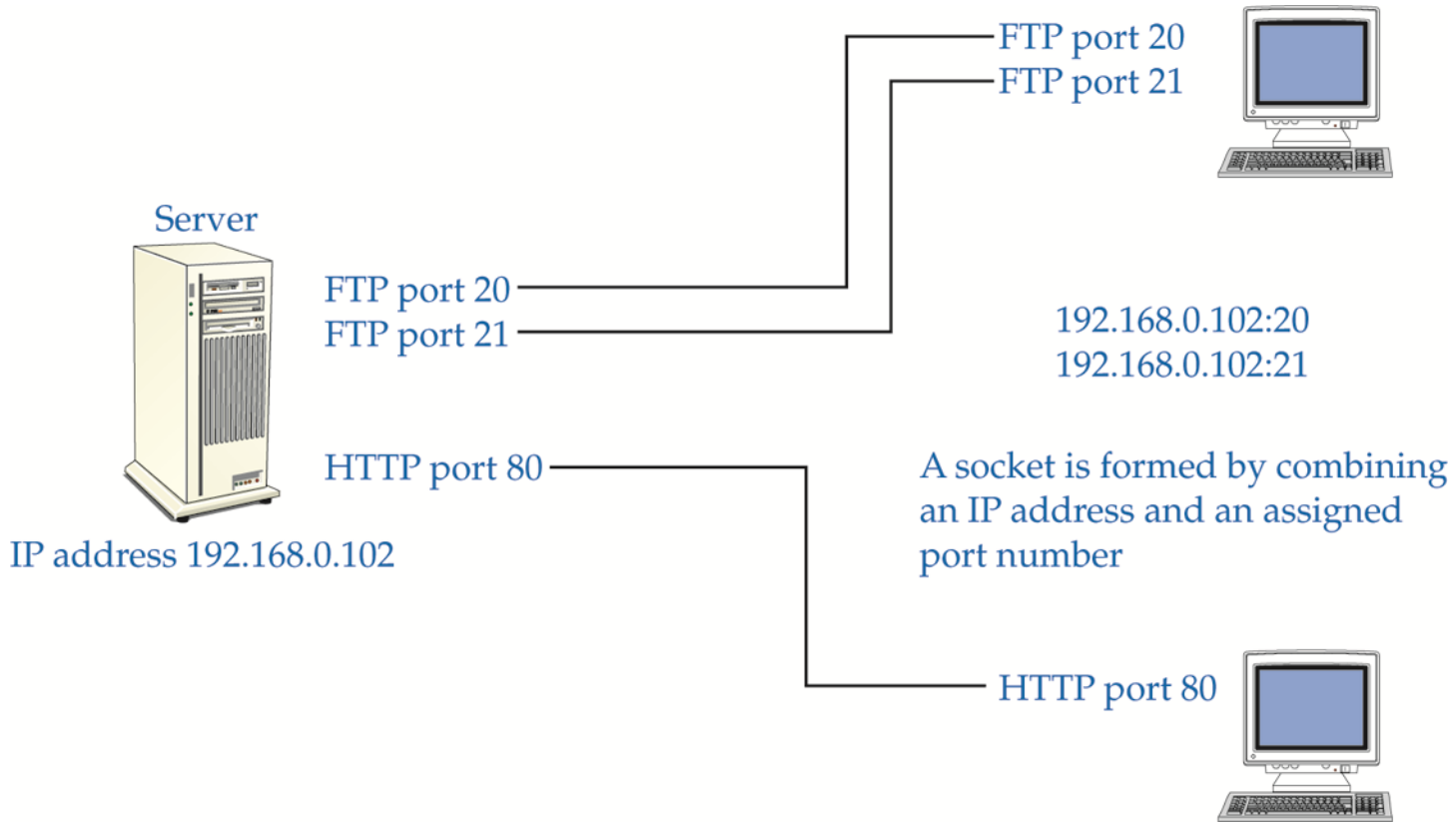
- TCP/IP (Transmission Control Protocol/Internet Protocol)—Provides Internet communication
- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)—Used to transfer files from one host to another

TCP/IP

- Suite of protocols that supports communication between network devices on a LAN and the Internet
- All major operating systems
  - Use the TCP/IP protocol suite and IPv4 and IPv6 format
  - Each OS uses its own proprietary protocols to maintain backward compatibility with legacy OSs, and for file sharing and printer access

TCP/IP Ports and Socket

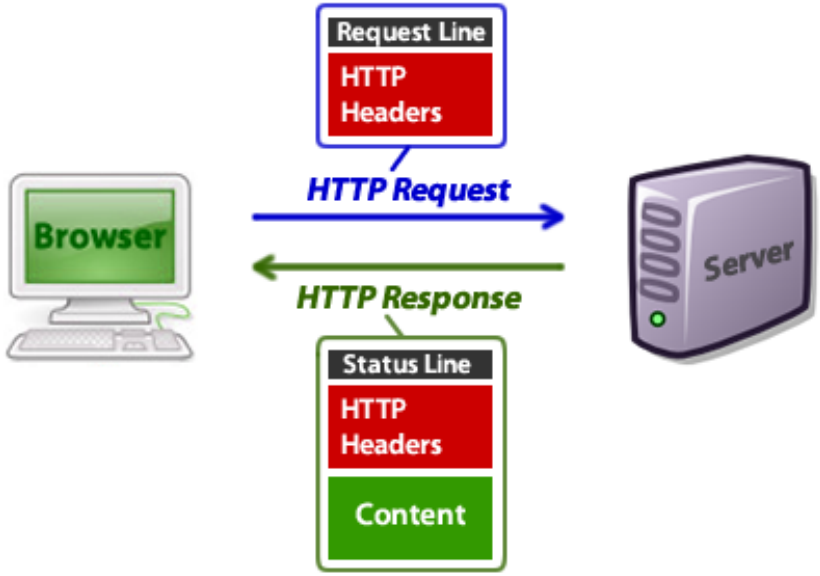
- A port number combined with an IP address (socket) is used to create a virtual connection



Common Port Numbers

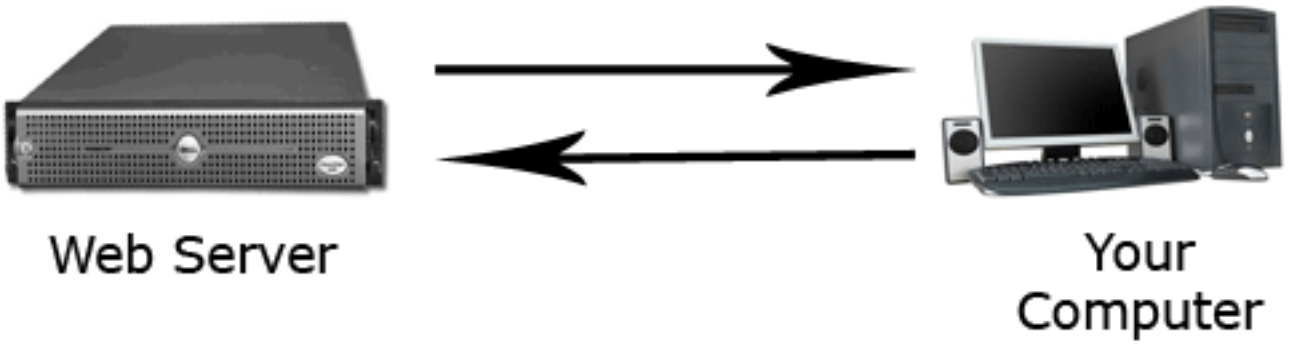
Service or Protocol	Port Number
FTP	20, 21
SSH	22
Telnet	23
SMTP	25
DNS	53
TFTP	69
HTTP	80
POP3	110
NNTP	119
NTP	123
IMAP4	143
HTTPS	443

Hypertext Transfer Protocol (HTTP)

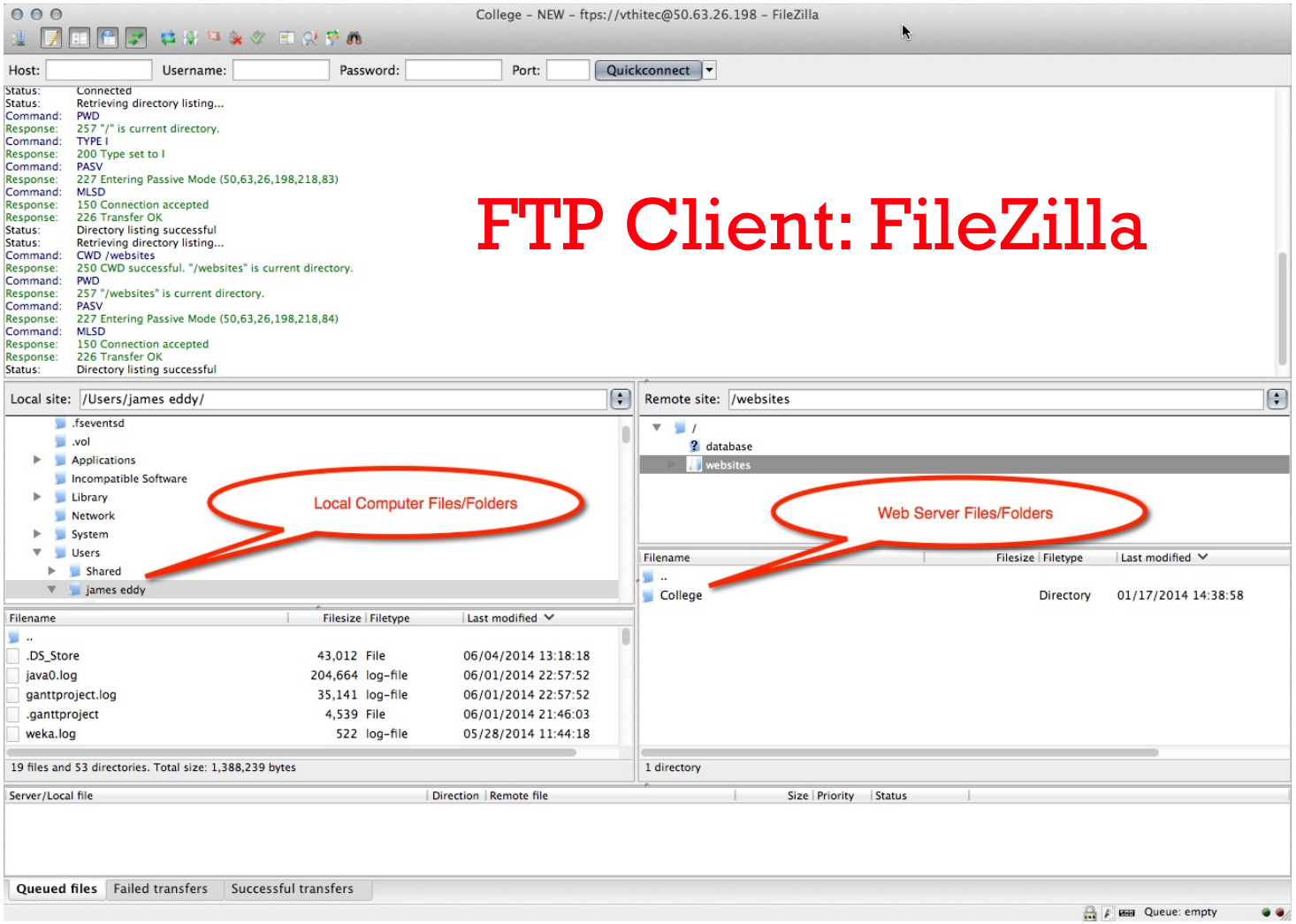


FTP

- File Transfer Protocol (FTP)



Transferring Files



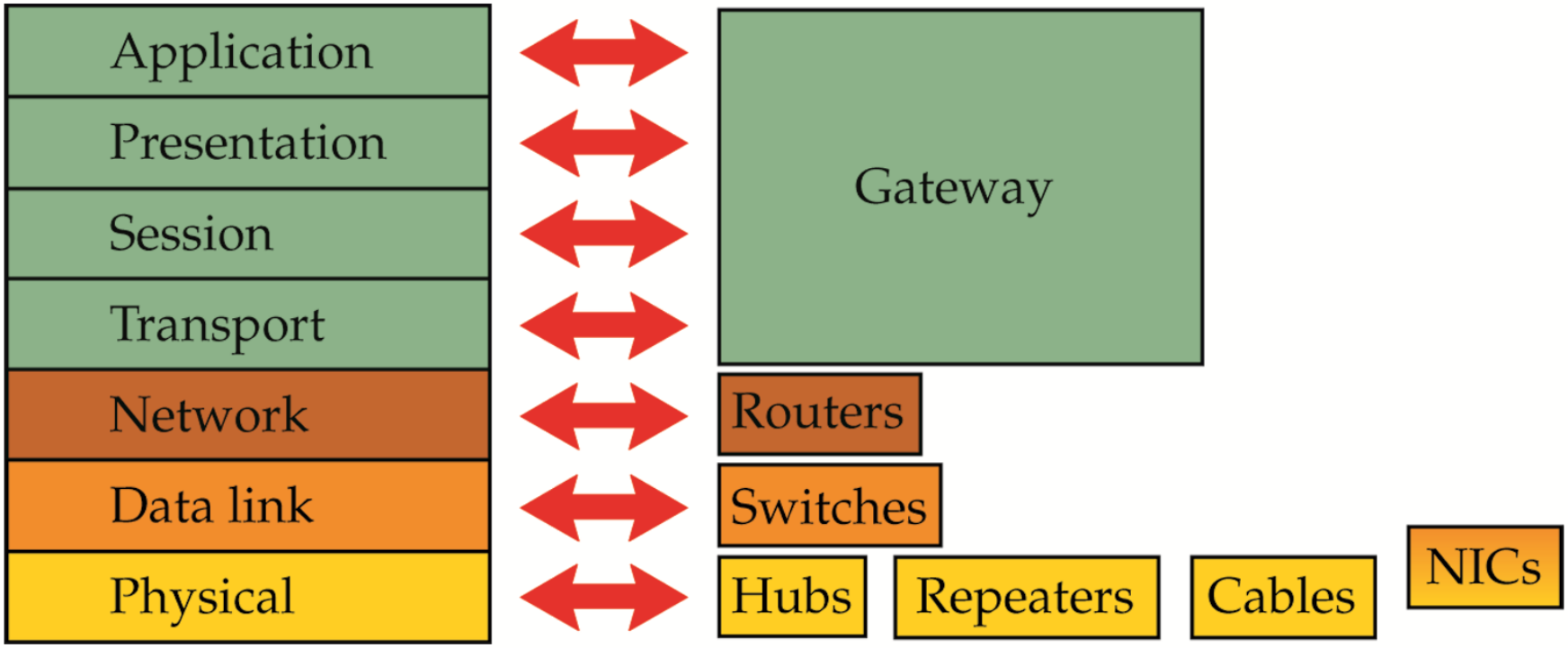
How Networks Work

How Internet Connections Work

Open Systems Interconnection (OSI) Model

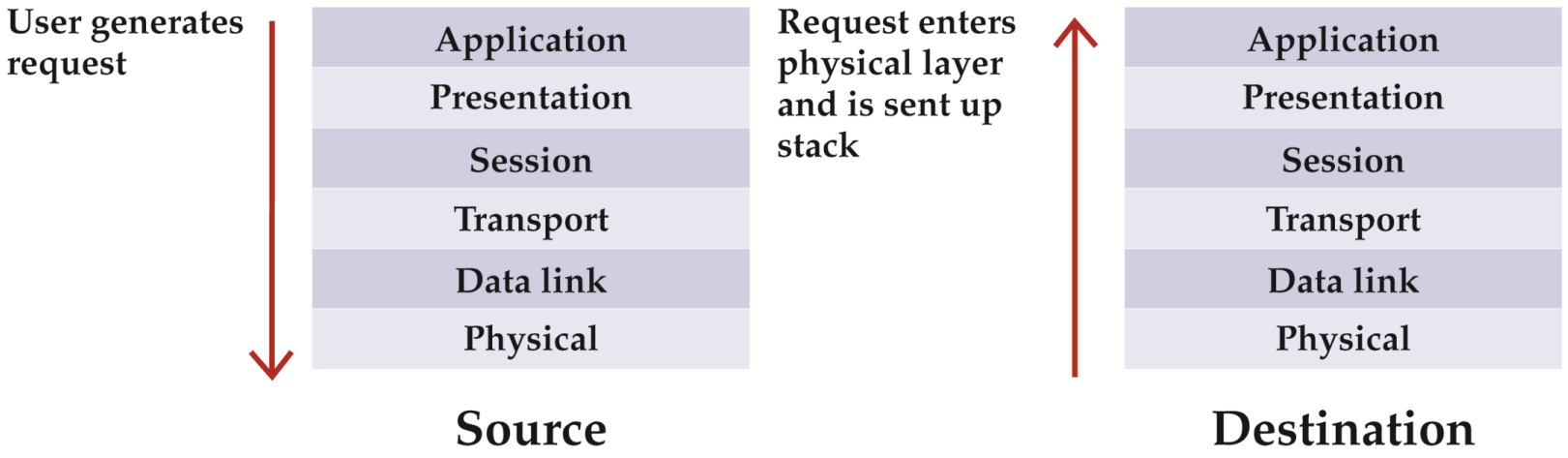
Layer	Function
Application	Interfaces to the network system.
Presentation	Packages data into a universally agreed on form, such as ASCII, BCD, BMP, JPG, and WAV.
Session	Establishes and coordinates communication between two points.
Transport	Ensures accurate delivery.
Network	Encapsulates packets for routing.
Data link	Converts frames or packets into electronic signals and places them on the network media.
Physical	The network media.

OSI Model


Application
Presentation
Session
Transport
Network
Data link
Physical
Gateway
Routers
Switches
Hubs
Repeaters
Cables
NICs

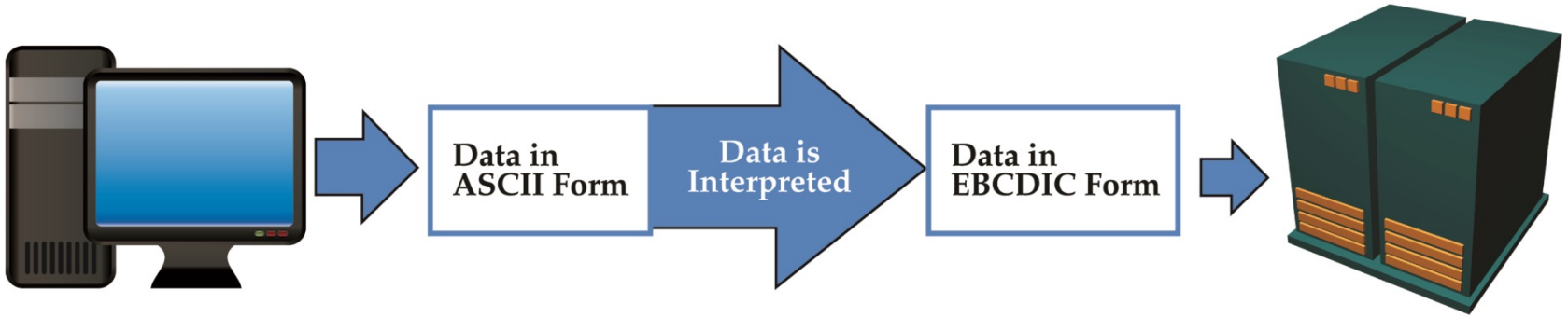
Application Layer

- Where the user interfaces with network operating system
- Start and final destination of data communication



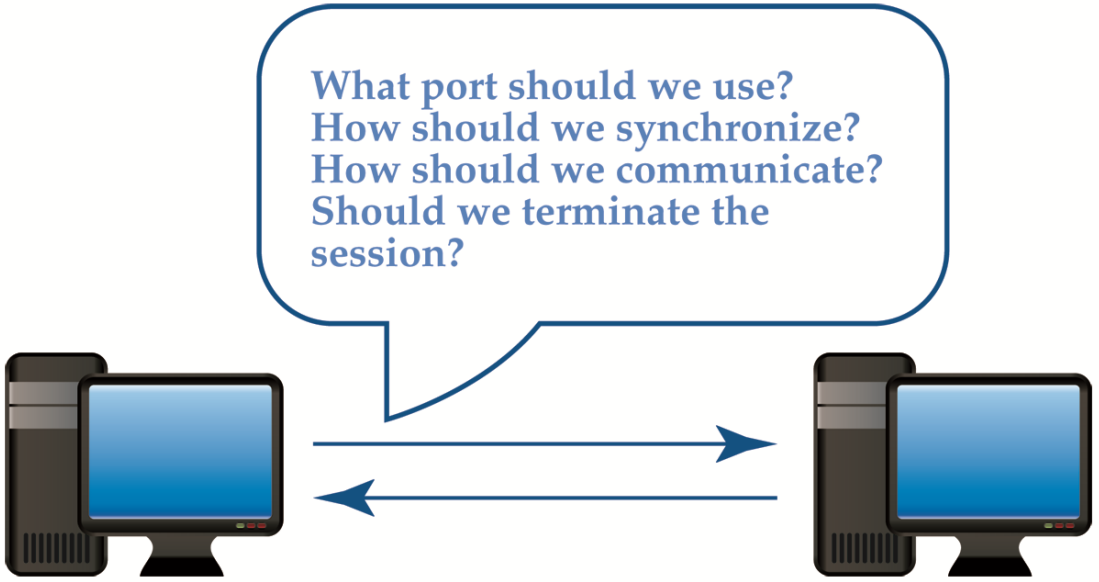
Presentation Layer

- Raw data is packaged into a universally agreed on form
- Data byte order is also agreed on
- Data encryption occurs



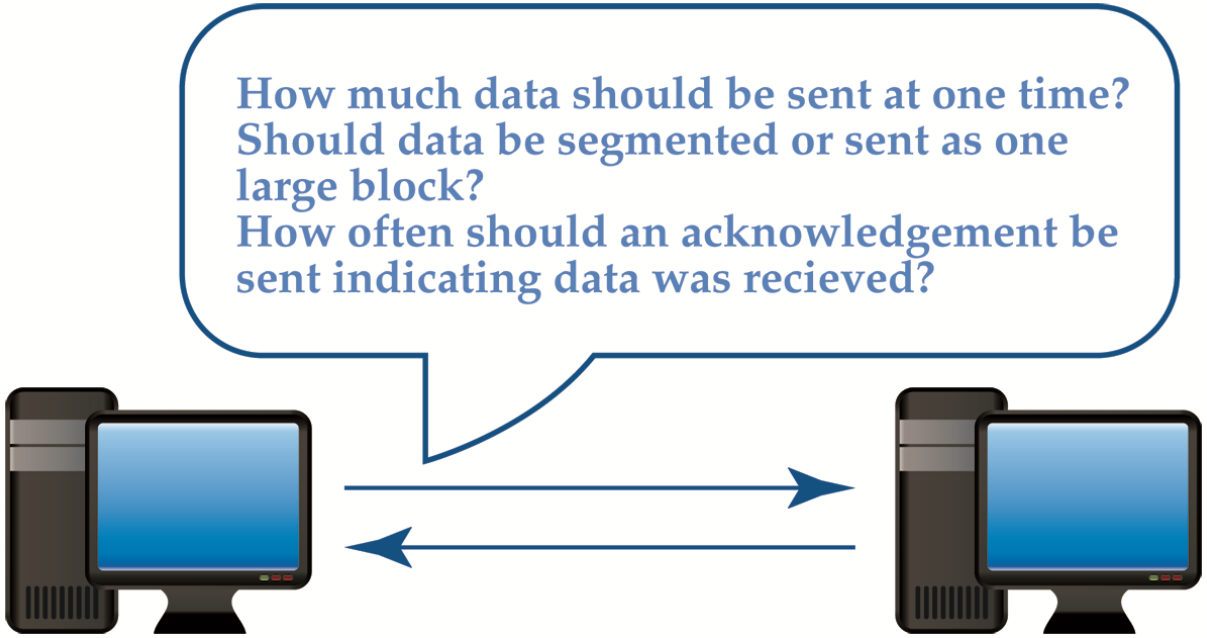
Session Layer

- Establishes a dialog between source and destination
- Negotiates decisions about how data flow is controlled and how session ends
- Decides on whether confirmation of arrival is needed



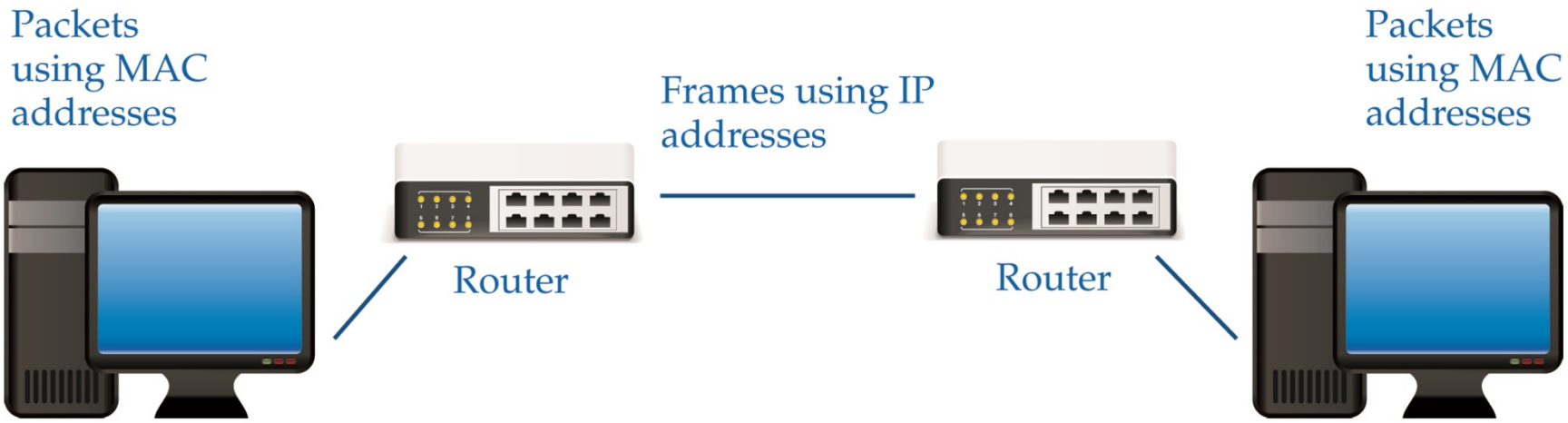
Transport Layer

- Responsible for flow of data to and from destination computer



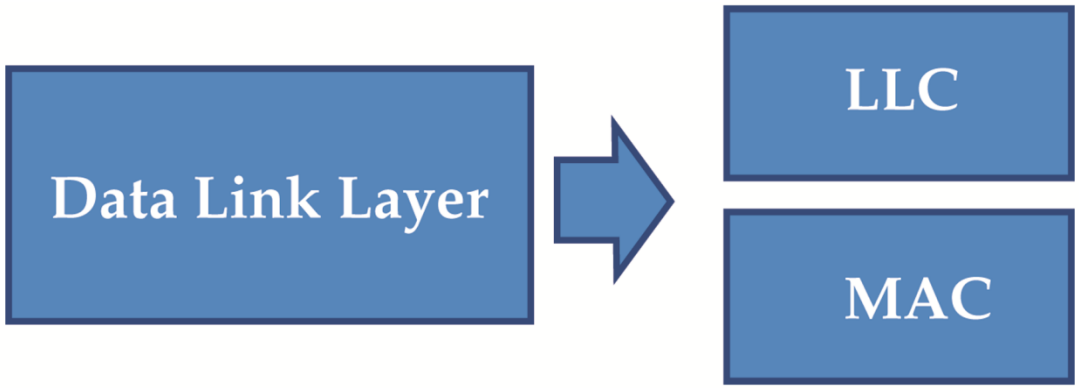
Network Layer

- Provides the means of routing data packets across a WAN or MAN
- Uses TCP/IP protocol standards
- Encapsulates packets with source and destination IP addresses
- Responsible for virtual networks



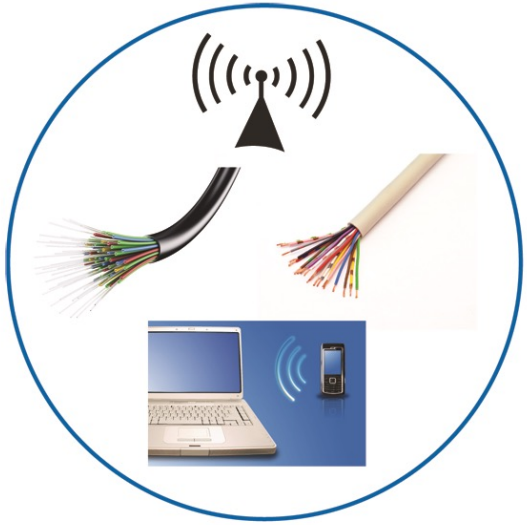
Data Link Layer

- Converts data package into electrical pulses and places pulses on network media
- Subdivided into logical link control (LLC) and MAC sublayer
- Parity and Cyclic Redundancy Checks (CRC) performed

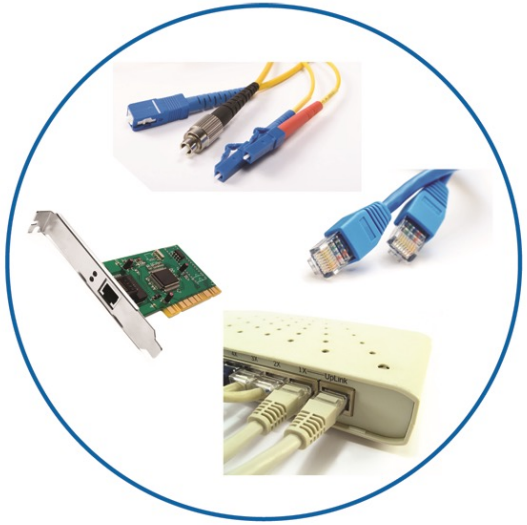


Physical Layer

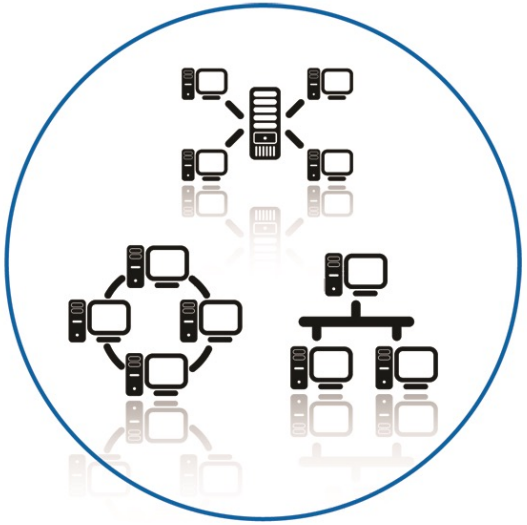
- Concerned with media, hardware, and network topology



Media



Media



Media

OSI Model and Network Devices

Layer 3 Device	• Makes decisions about where a packet is sent based on the Internet Protocol
Layer 2 Device	• Makes decisions about where a packet is sent based on a MAC address or logical name
Layer 1 Device	• Makes no decisions about where a packet is sent

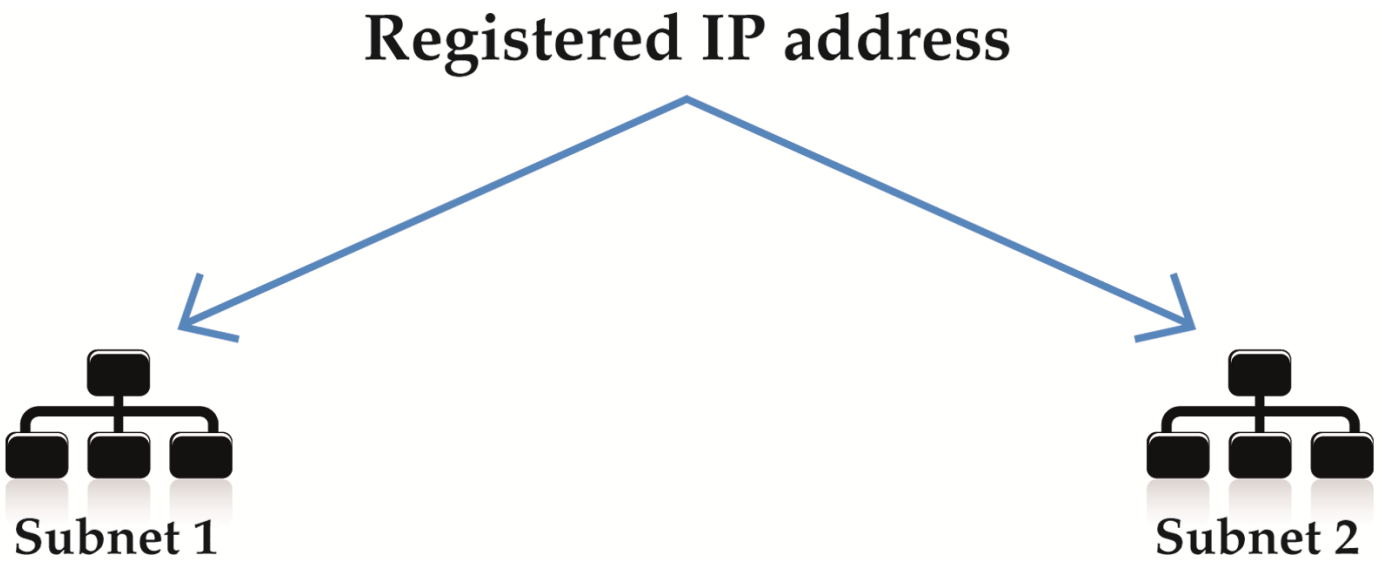
How Networks Work

How Network Security Works

How Networks Work

Subnetting

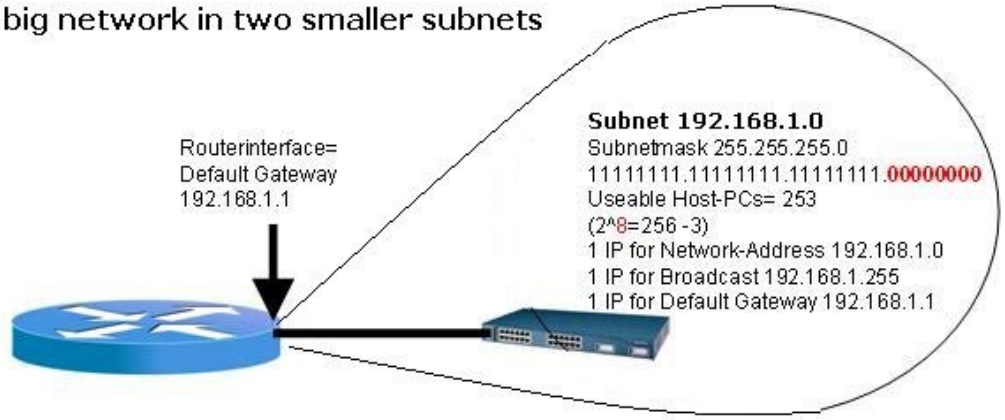
Purpose of Subnetting



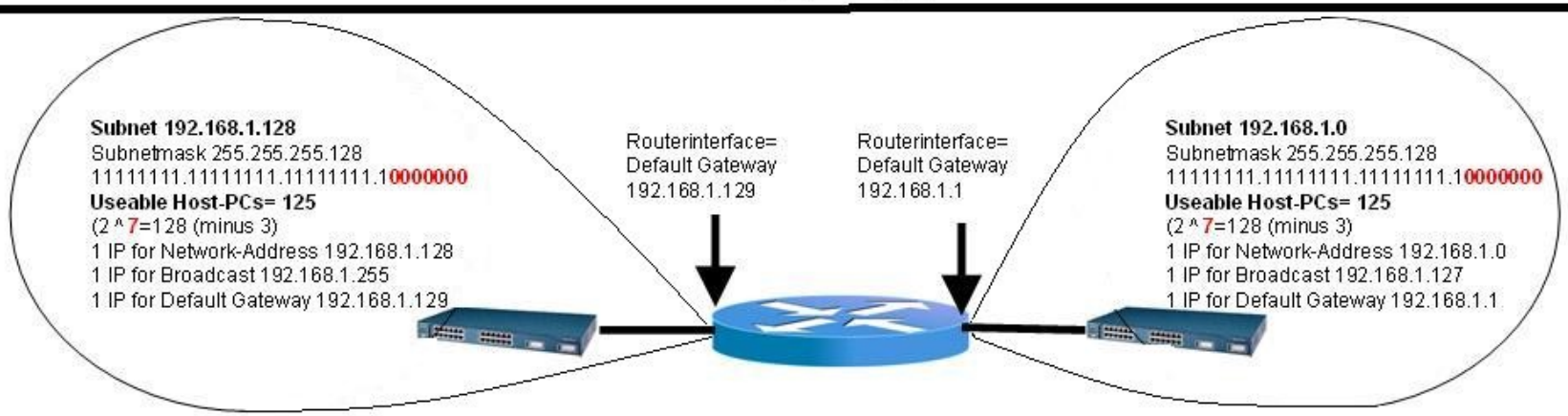
Advantages / Disadvantages

Advantages	Disadvantages
Creates a more secure network by placing hosts on separate networks	Can be difficult to manage
Reduces amount of collision on the network	Can be confusing because some equipment use subnets based on all one and all zero bit patterns

EXAMPLE:
Dividing a big network in two smaller subnets



We have ONE network 192.168.1.0.
It has 253 useable IP-Addresses for Host-PCs.
We want to divide it in two smaller pieces (subnets).



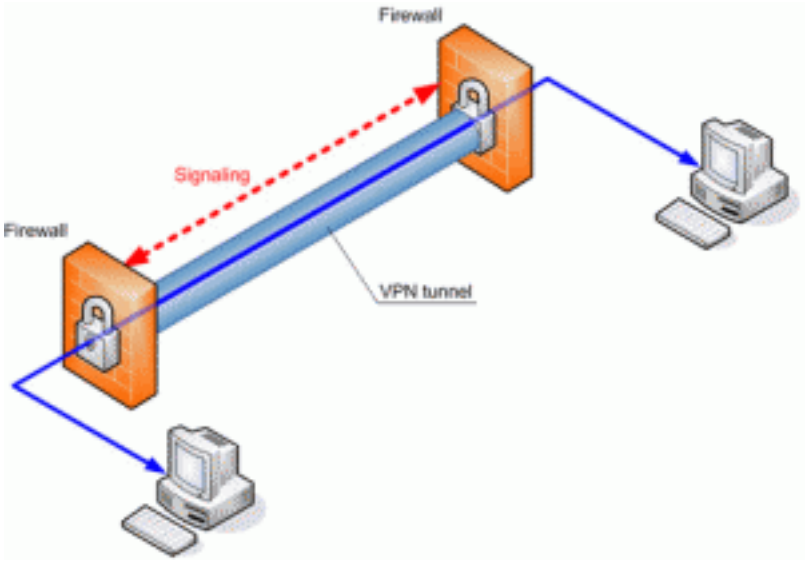
Now we have TWO subnets,
192.168.1.0 and 192.168.1.128.
Each has 125 useable IP-Addresses for Host-PCs.

How Networks Work

VPN

Virtual Private Network (VPN)

- Creates a private connection over the Internet or Intranet
- VPN software and firewalls provide security
- Four most common protocols used in a VPN are PPTP, L2F, L2TP, and IPSec



TCP/IP Troubleshooting Utilities

TCP/IP Utility	Function	When to Use
netstat	Displays current TCP/IP and port statistics	To determine network problems, monitor connections, and check for open ports
nbtstat	Displays NetBIOS over TCP statistics	To see a list of computers currently connected to the network
ping	Sends a packet from one host to another and then echoes a return reply	To quickly check the state of network media between two hosts
tracert or **traceroute**	Sends a packet from one host to another and gathers statistics and information along the way	To troubleshoot the path to a distant destination
arp	Maps the host MAC address to the host IP address	To verify IP address and MAC address assignments
nslookup	Resolves domain names to IP addresses	To find information about domain names and IP addresses

Pros and Cons

Advantages	Disadvantages
Share software, data, equipment, and communications quickly, easily, and inexpensively	Losing access to files Need additional personnel
Secure data	Vulnerability to hackers, viruses, and disgruntled workers