How Computer Networks Work

Introduction

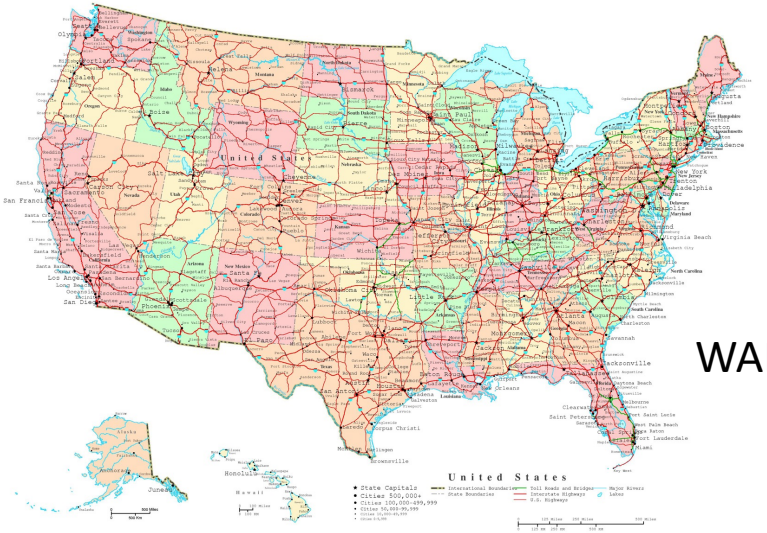
Network Classifications

- 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

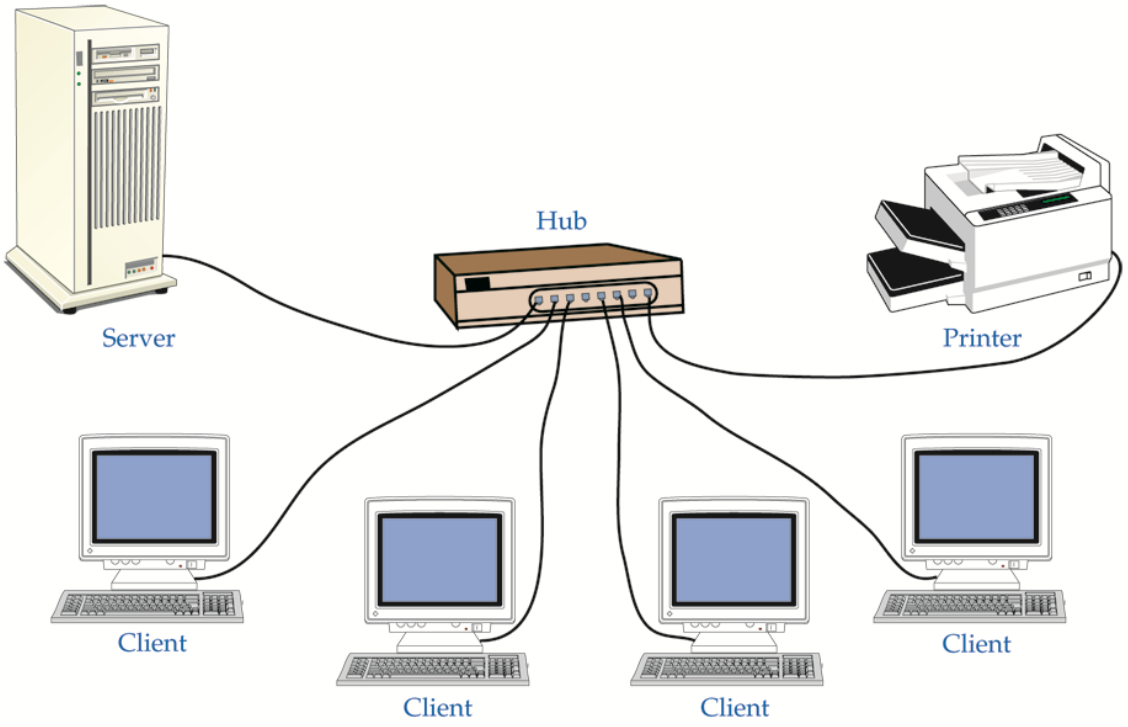
MAN



WAN

Client/Server Network

- A Server provides client services such as security, data storage, Internet access, and email



How Networks Work

How a Modem Works

56k Modem

Tone Generation

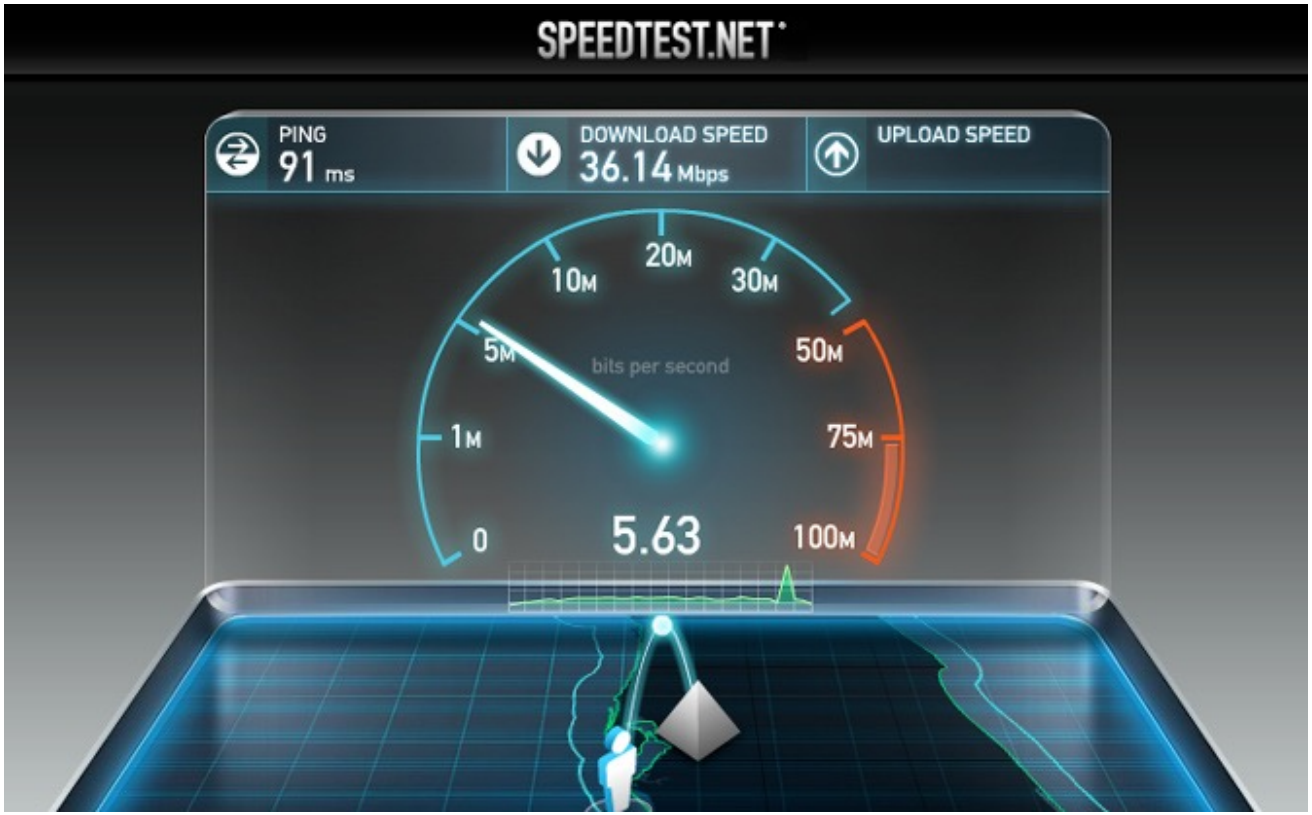
- When a terminal's modem dials a computer's modem, the terminal's modem is called the **originate** modem. It transmits a 1,070-hertz tone for a 0 and a 1,270-hertz tone for a 1.
- The computer's modem is called the **answer** modem, and it transmits a 2,025-hertz tone for a 0 and a 2,225-hertz tone for a 1.

Modem Speeds

- 300 bps (bits per second) - 1960s through 1983
- 1200 bps - Gained popularity in 1984 and 1985
- 2400 bps
- 9600 bps - First appeared in late 1990 and early 1991
- 19.2 kilobits per second (Kbps)
- 28.8 Kbps
- 33.6 Kbps
- 56 Kbps - Became the standard in 1998
- DSL, with theoretical maximum of up to 8 megabits per second (Mbps) - Gained popularity in 1999

Check your Speed

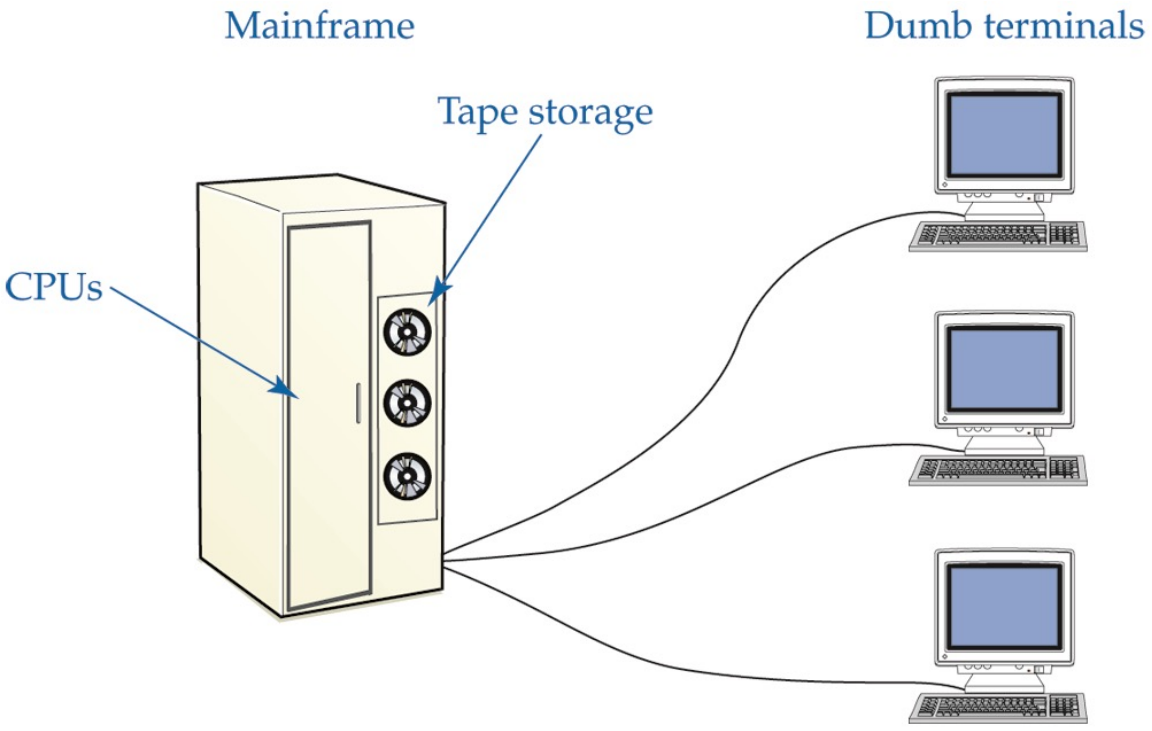
- http://www.speedtest.net



How Networks Work

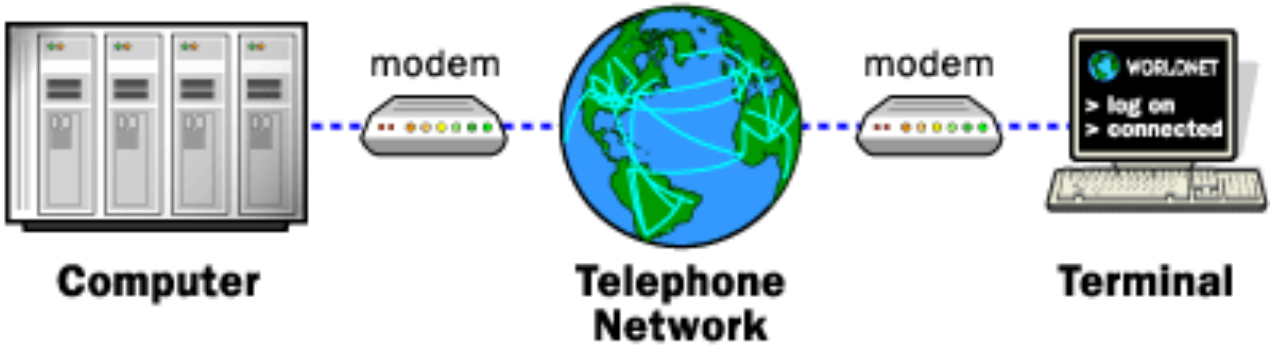
How Terminals Work

Terminal / Mainframe



Terminal PC

- Terminals "Dial in" to a large, central computer

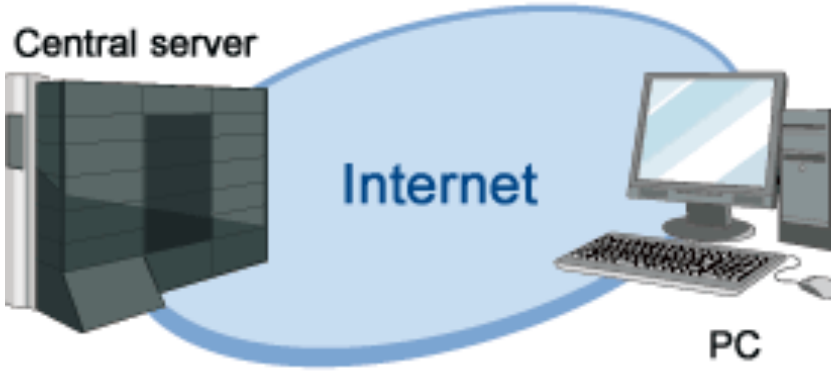


How Networks Work

The PC as a Terminal

ASP Model

Infrastructure as a Service

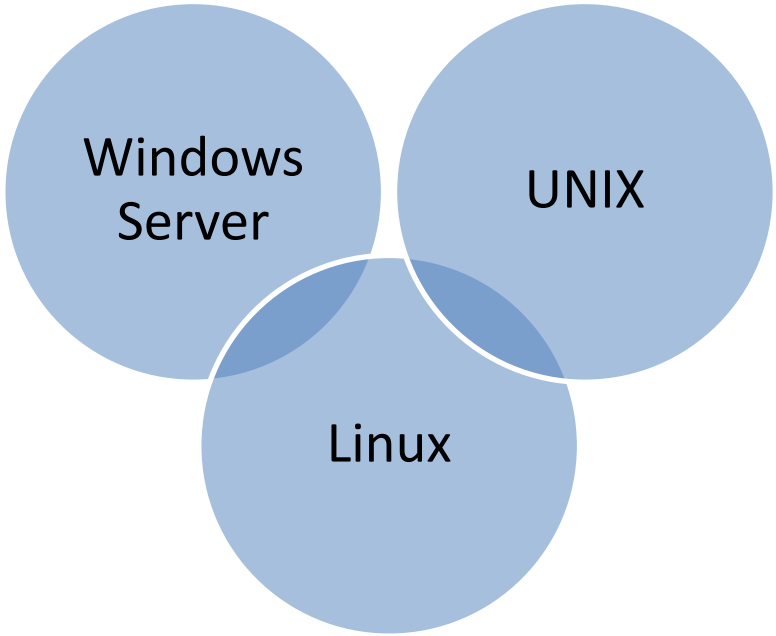


How Networks Work

How Networking Operating Systems Work

Network Operating System (NOS)

- Provides communication between different operating systems



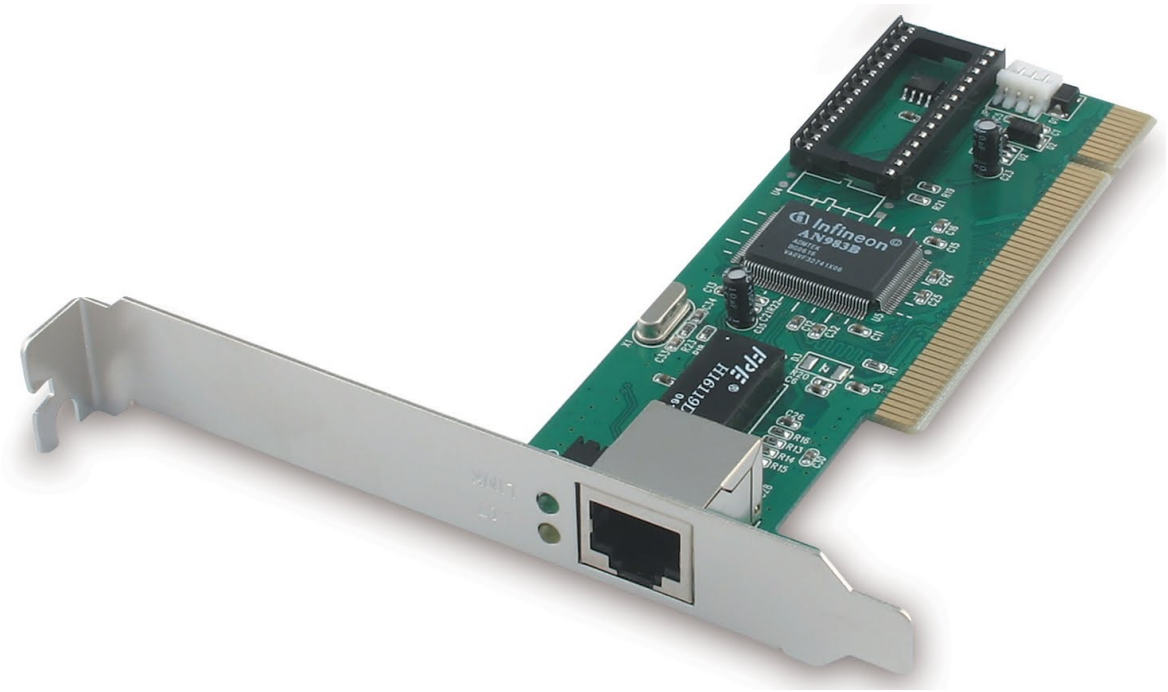
Common Operating System Traits

Common Features of a Network Operating System	Examples
Internet communications	TCP/IP protocol
Resource sharing	Printer, scanner, storage devices, files
Security	Logon/authentication and resource, file and directory permissions
Services	Web, e-mail, FTP
Storage and file management	File management utilities, backup utilities, encryption
Troubleshooting utilities	Network and server diagnostics
User interface	GUI and command line

How Networks Work

How Network Interface Cards Work

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

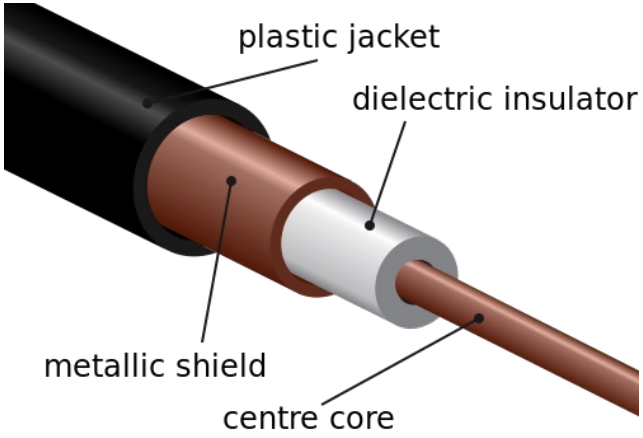
How Networks Work

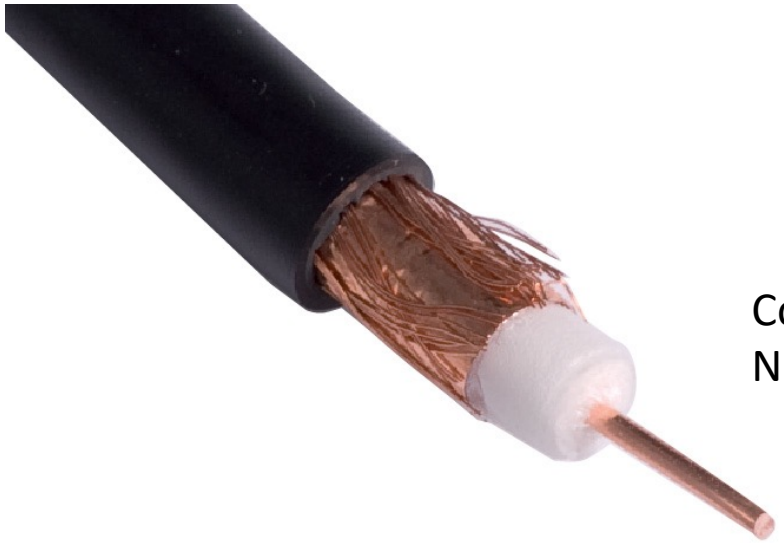
How Network Cables Work

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

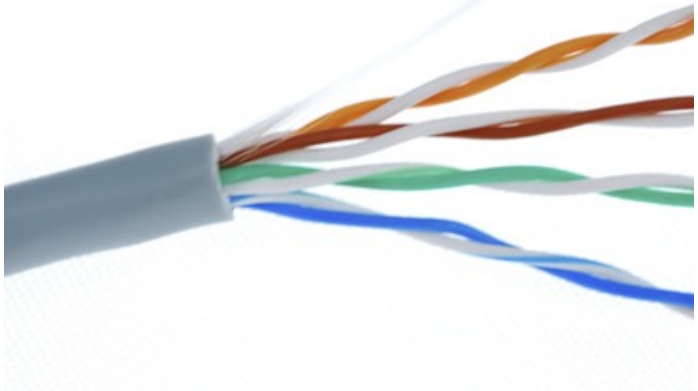
Coaxial Cable





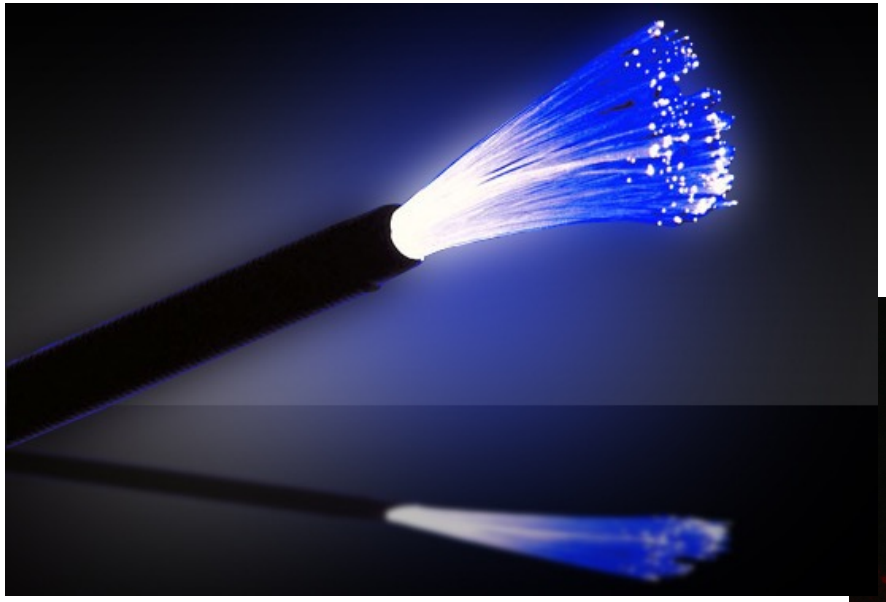
Common Types: RG – 59, RG – 6
Number of Shields can be Single, Double, etc.

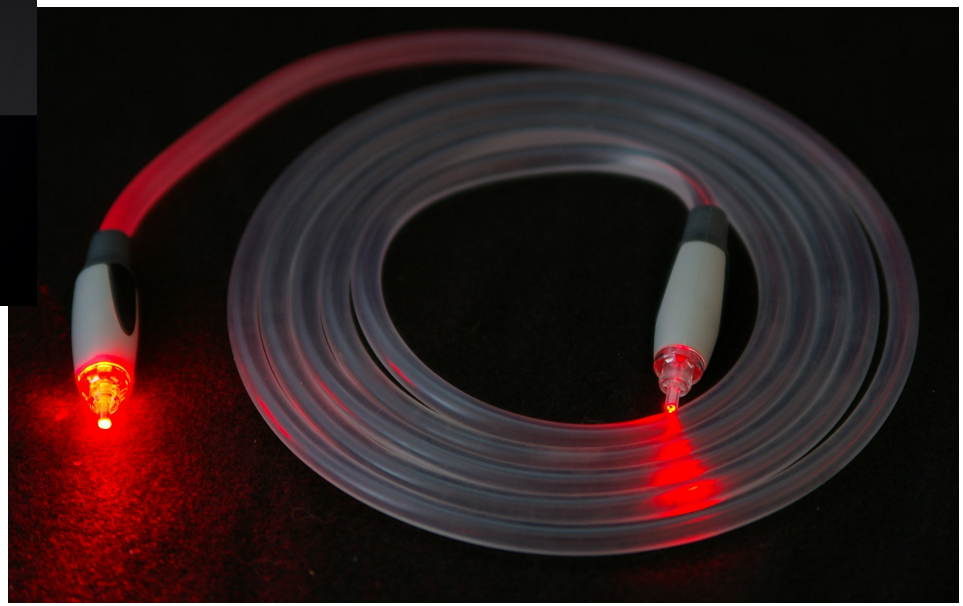
Network Cable



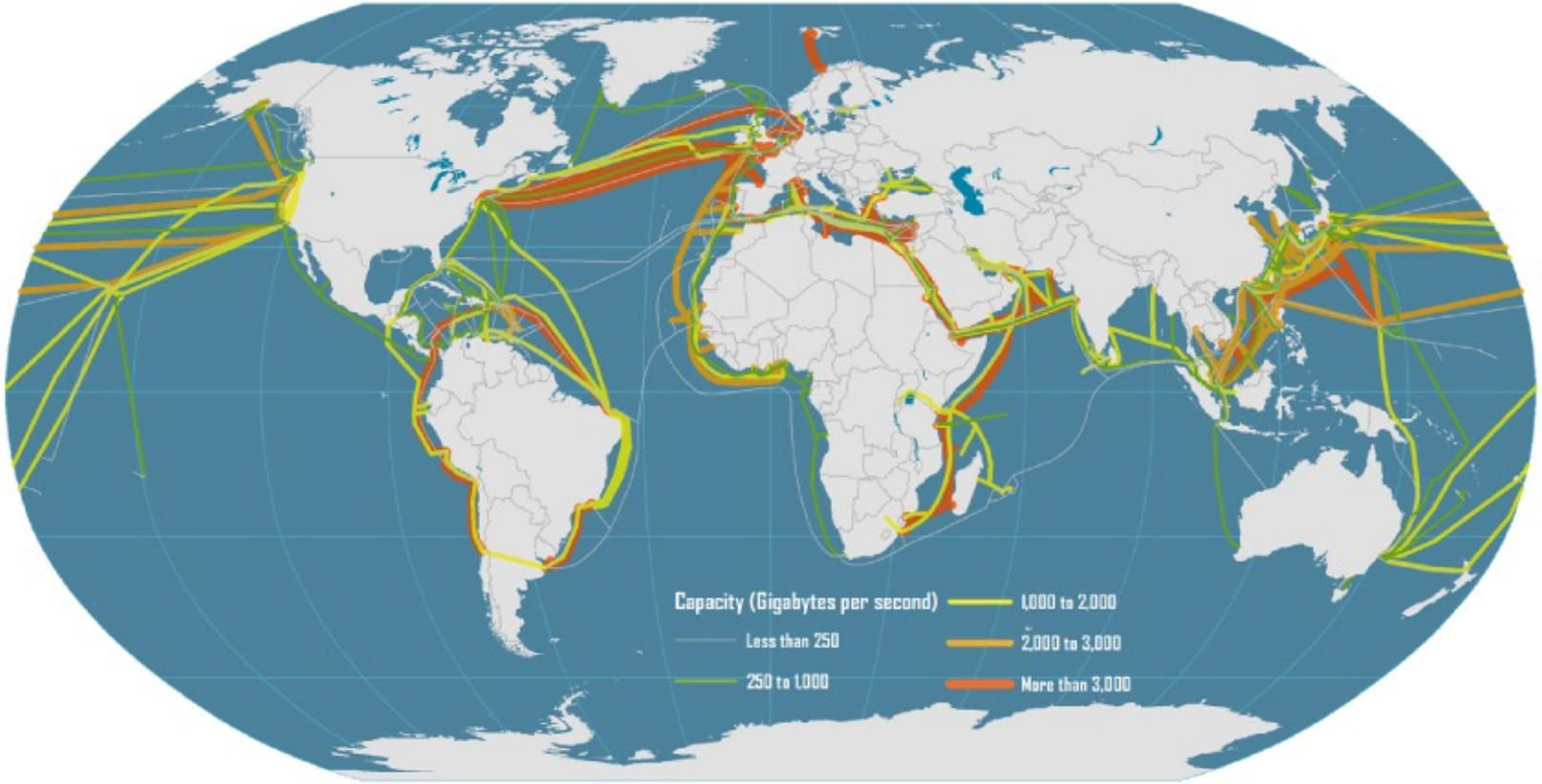
Category 5e (Cat 5e) standardized cable for Ethernet

Fiber Optic





Transcontinental "Submarine" Network Cables



How Networks Work

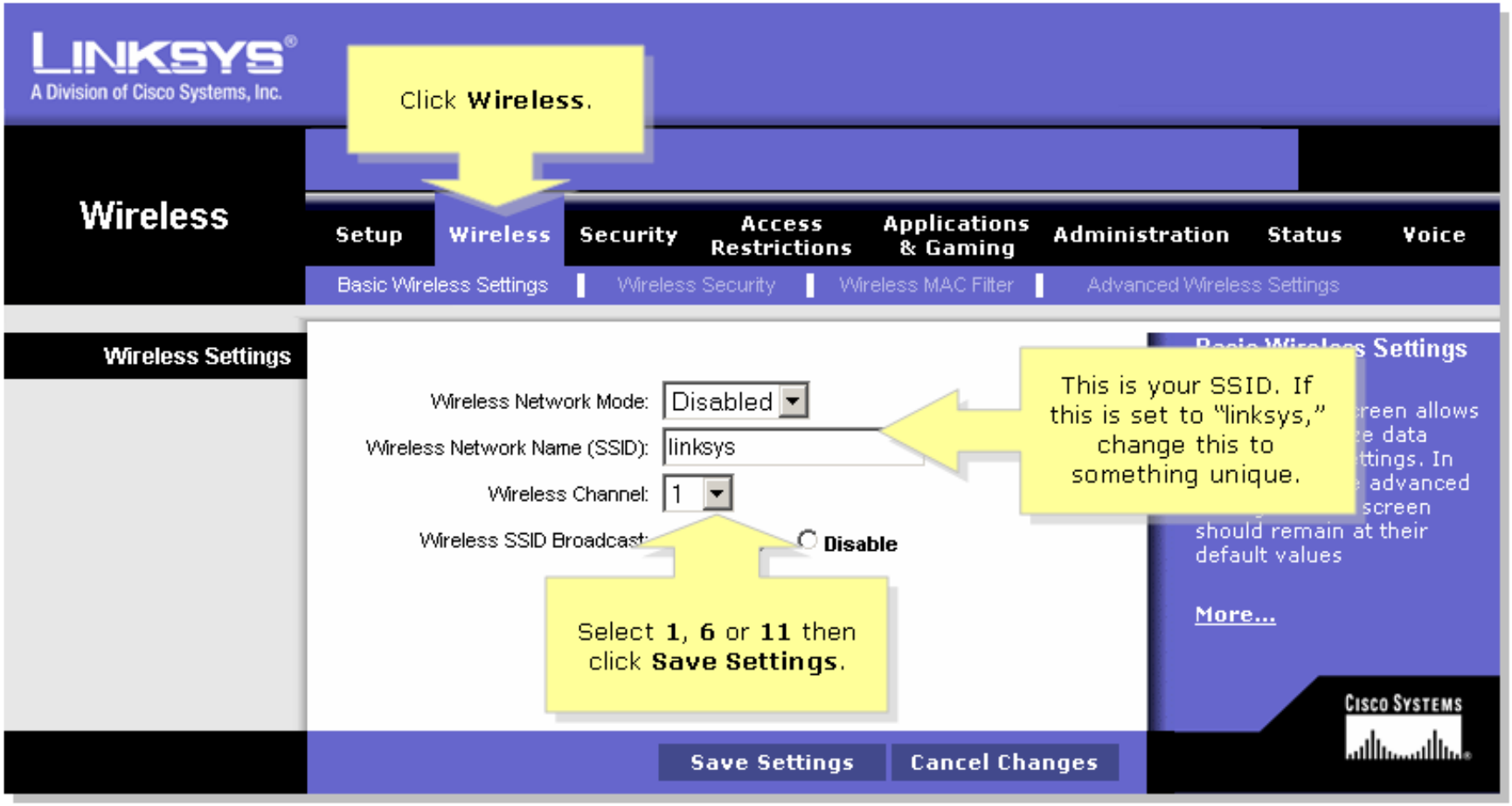
How Wireless Networks Work

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

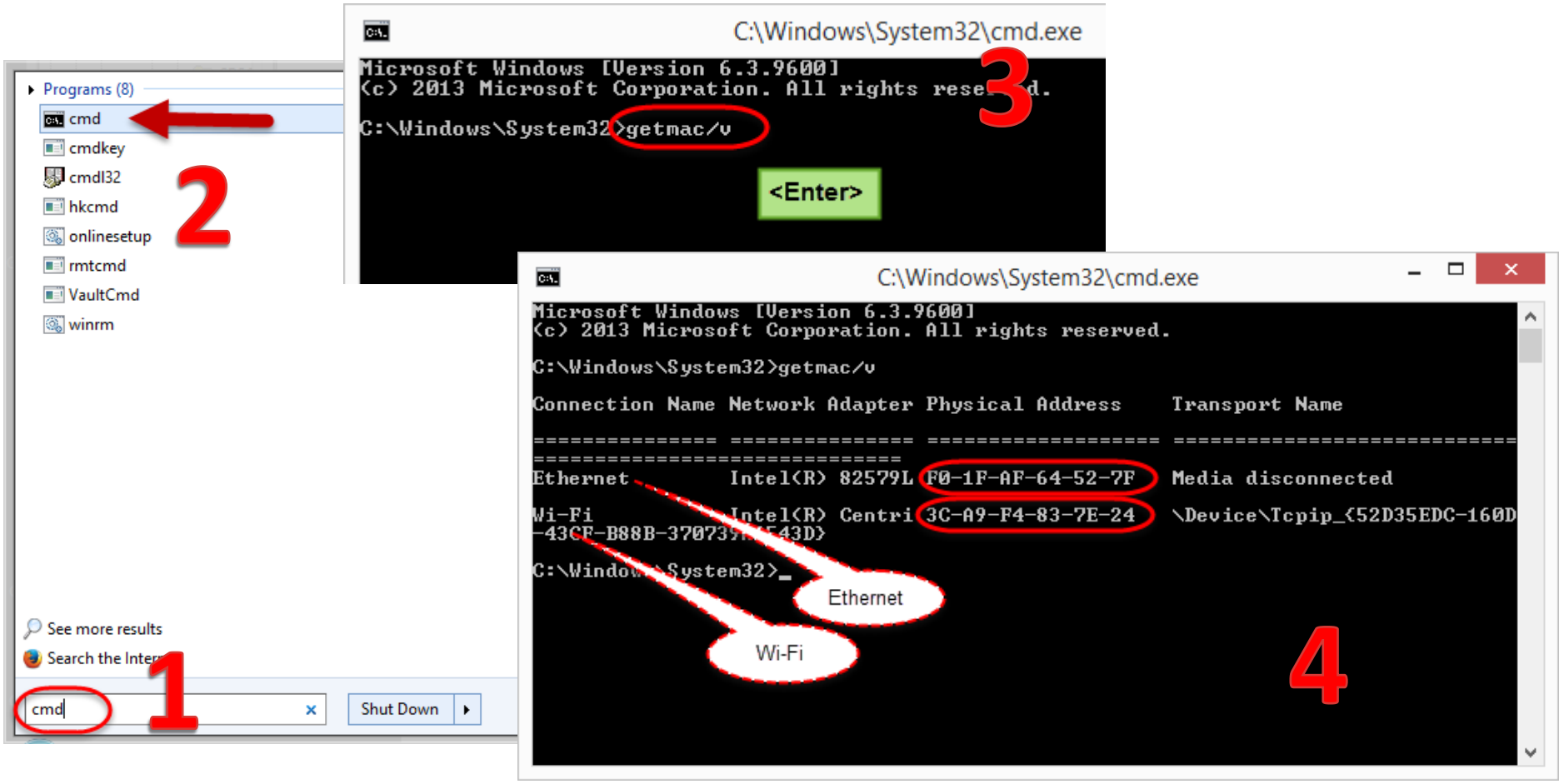
SSID


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.
screen allows
e data
ttings. In
advanced
screen
should remain at their default values
More...
Cisco Systems
Save Settings
Cancel Changes

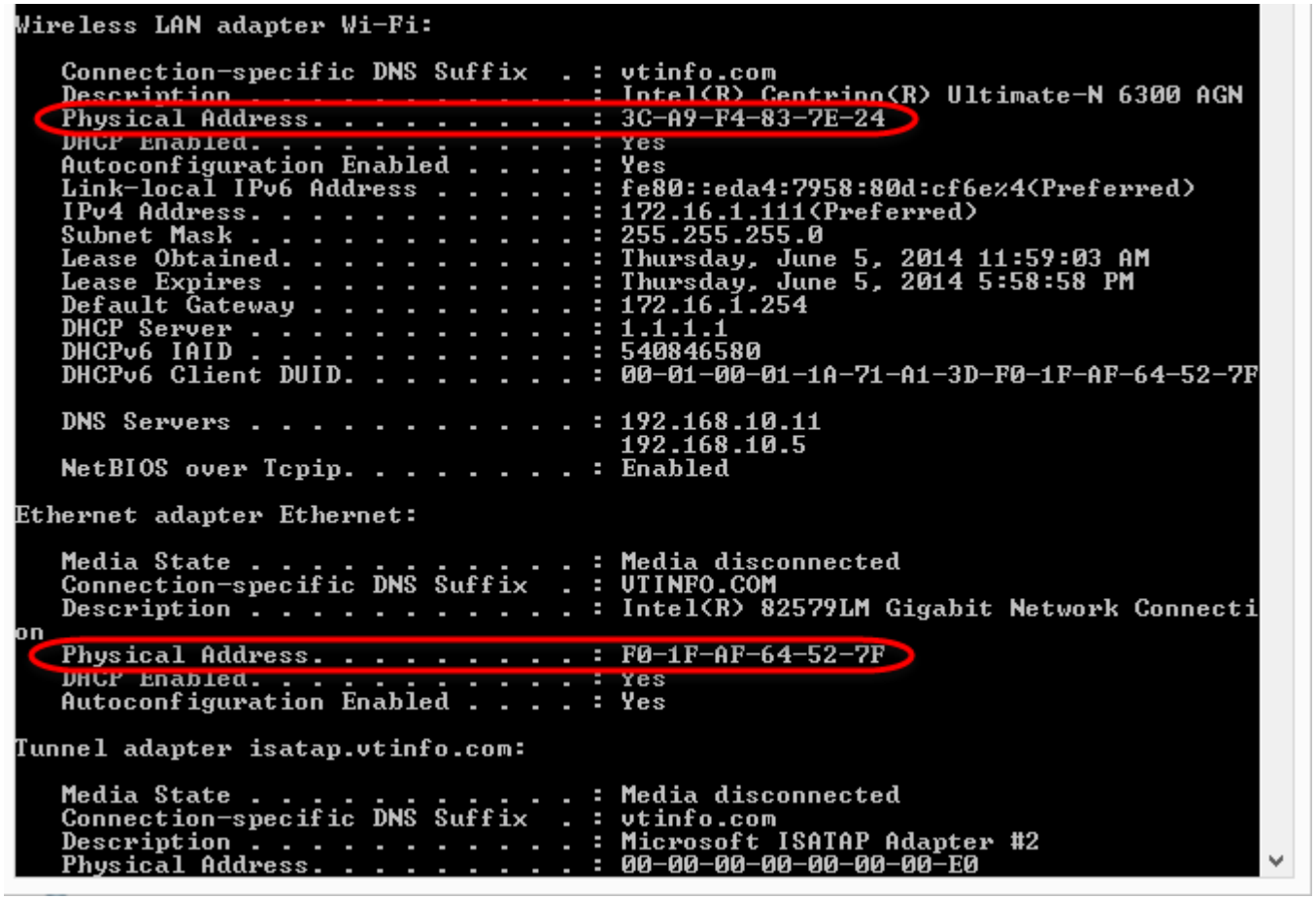
Media Access Control (MAC) Filtering

- To configure MAC filtering, administrator creates an Access Control List (ACL)
- ACL is located on Wireless Access Point (WAP)
- ACL contains list of MAC addresses belonging to authorized wireless network devices

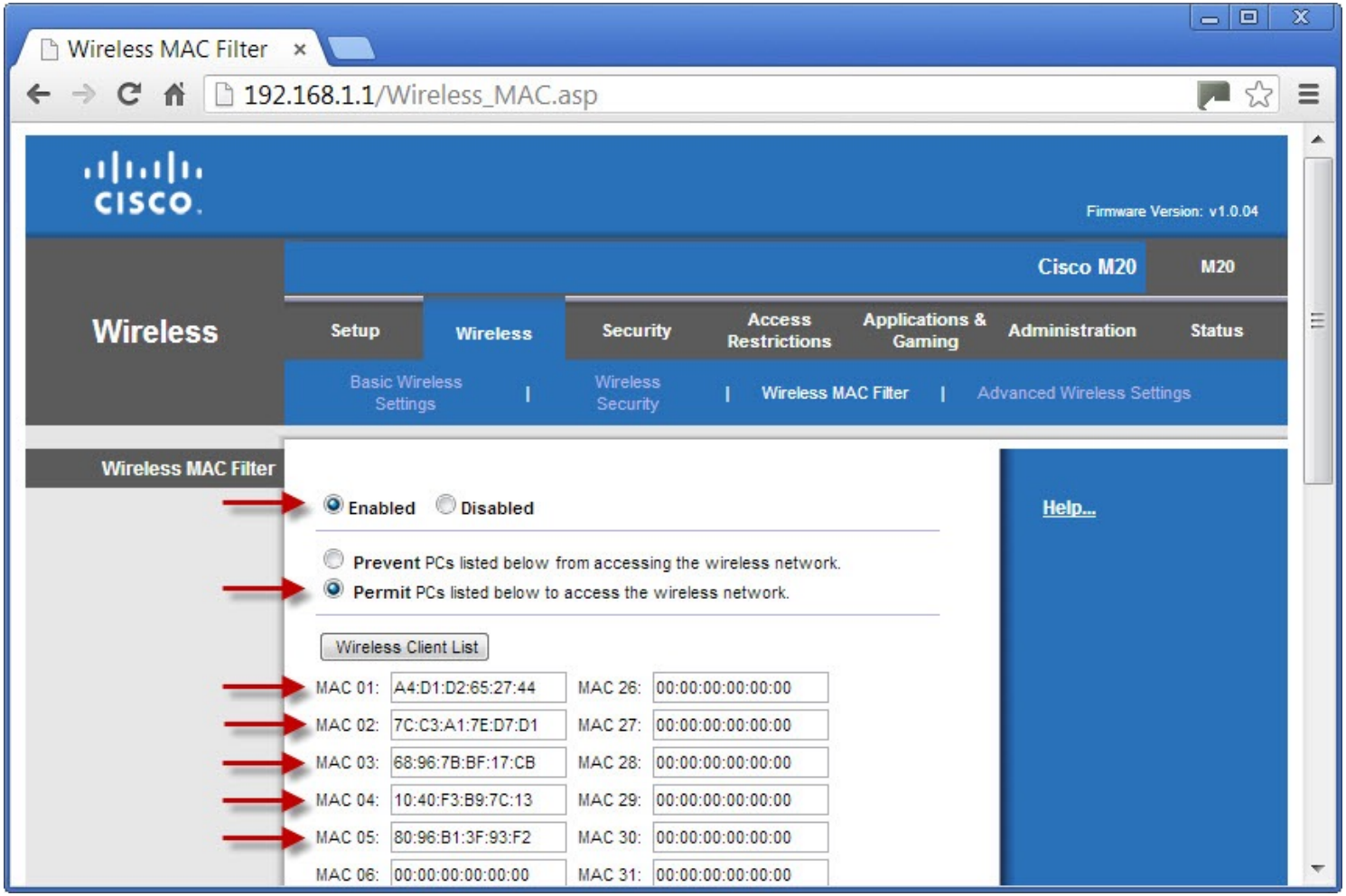
Find your MAC Address



Also: ipconfig /all



CISCO Router MAC Filter Setup



Wired Equivalent Privacy (WEP)

- First attempt use encryption to secure the data transferred across a wireless network
- Algorithm not complex and can be easily cracked
- A VPN can add to the security set in place by WEP

Wi-Fi Protected Access (WPA)

- Developed by the Wi-Fi organization to overcome the vulnerabilities of WEP
- Compatible with 802.11 devices
- Wi-Fi Protected Access 2 (WPA2) is an enhanced version of WPA
- WPA2 is compatible with the 802.11i standard

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

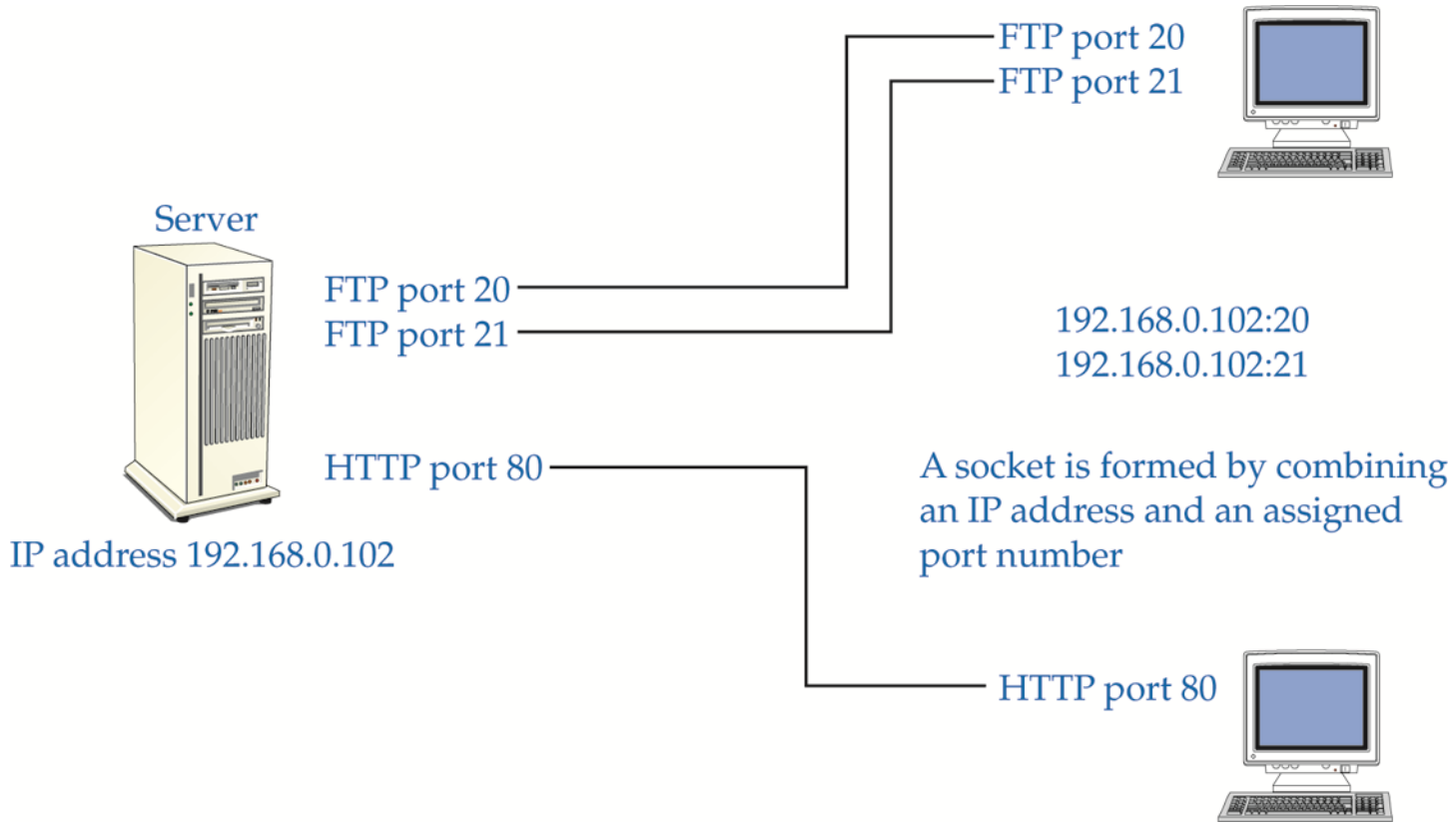
- TCP/IP (Transmission Control Protocol/Internet Protocol)—Provides Internet communication
- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)—Used to transfer files from one host to another

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

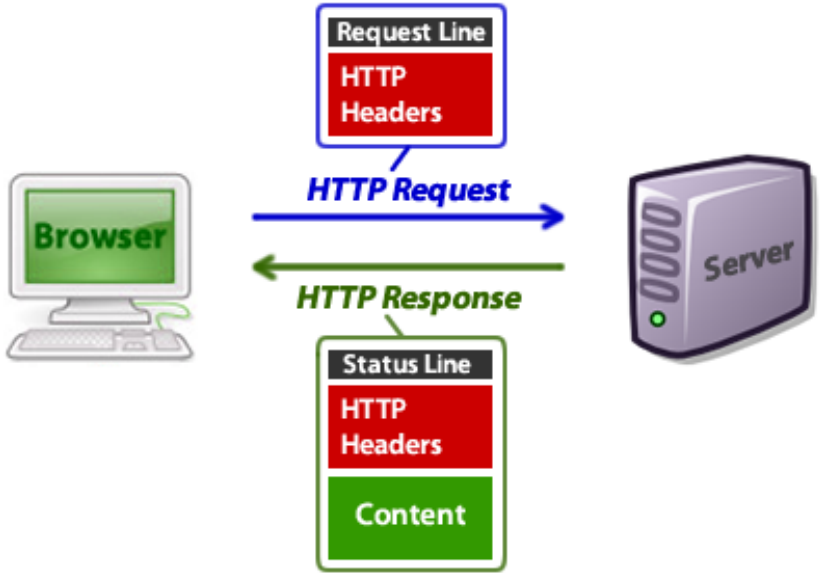
- A port number combined with an IP address (socket) is used to create a virtual connection



Common Port Numbers

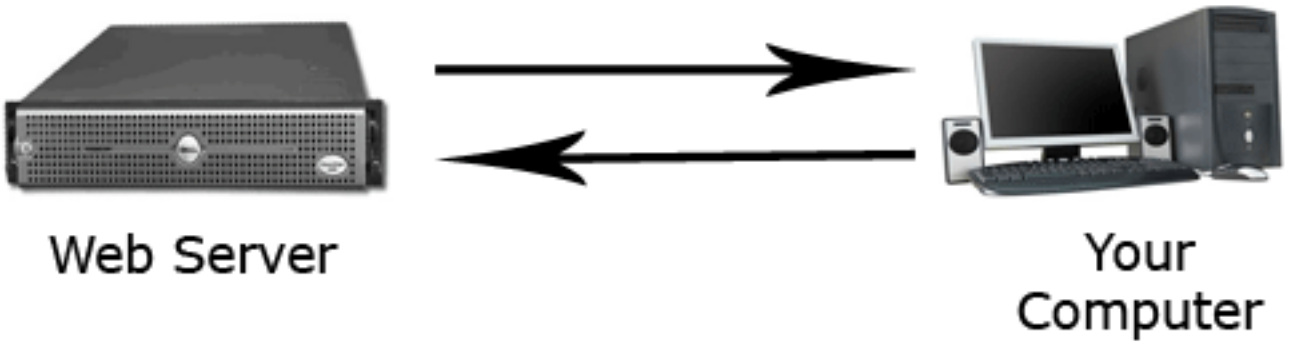
Service or Protocol	Port Number
FTP	20, 21
SSH	22
Telnet	23
SMTP	25
DNS	53
TFTP	69
HTTP	80
POP3	110
NNTP	119
NTP	123
IMAP4	143
HTTPS	443

Hypertext Transfer Protocol (HTTP)

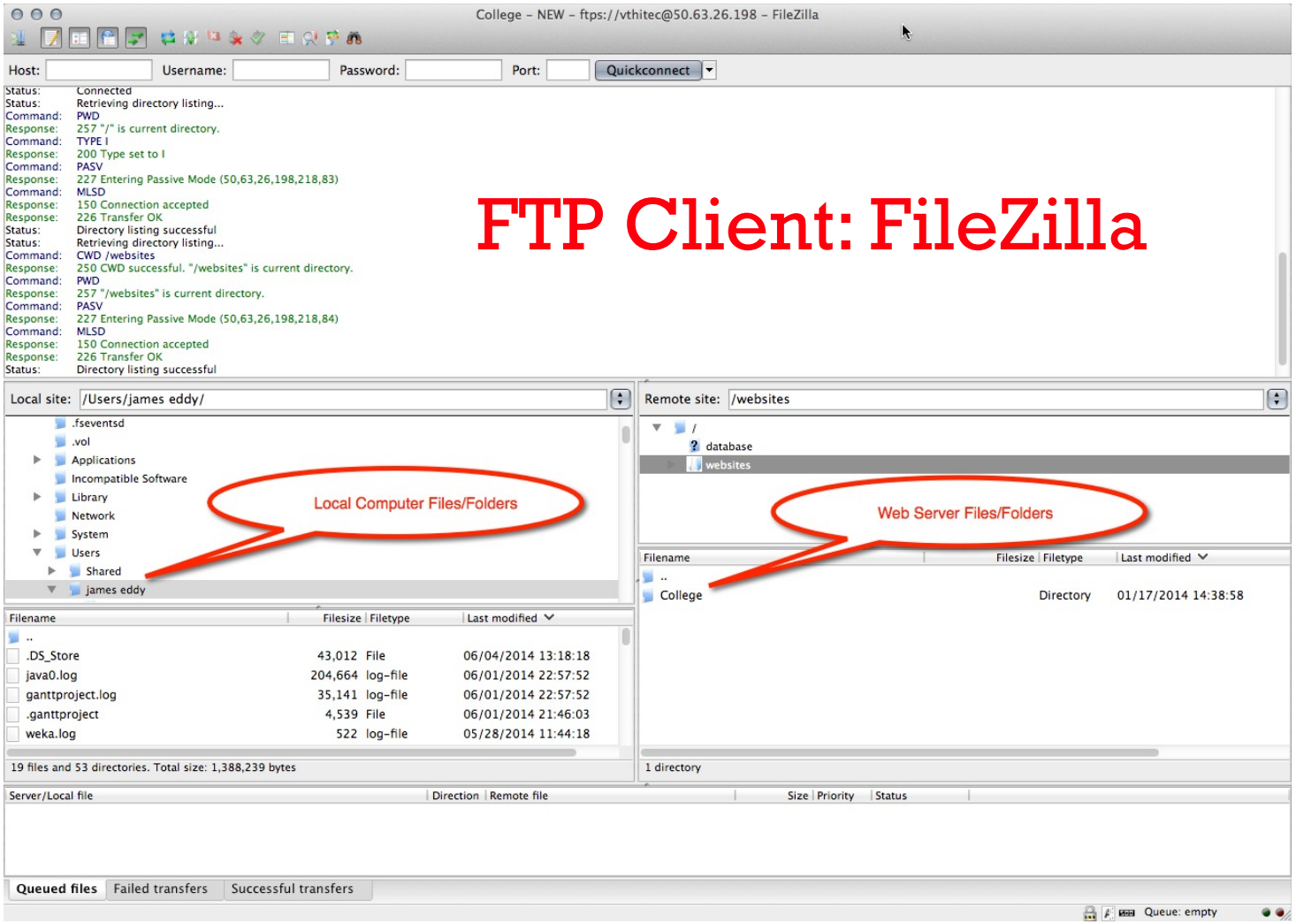


FTP

- File Transfer Protocol (FTP)



Transferring Files

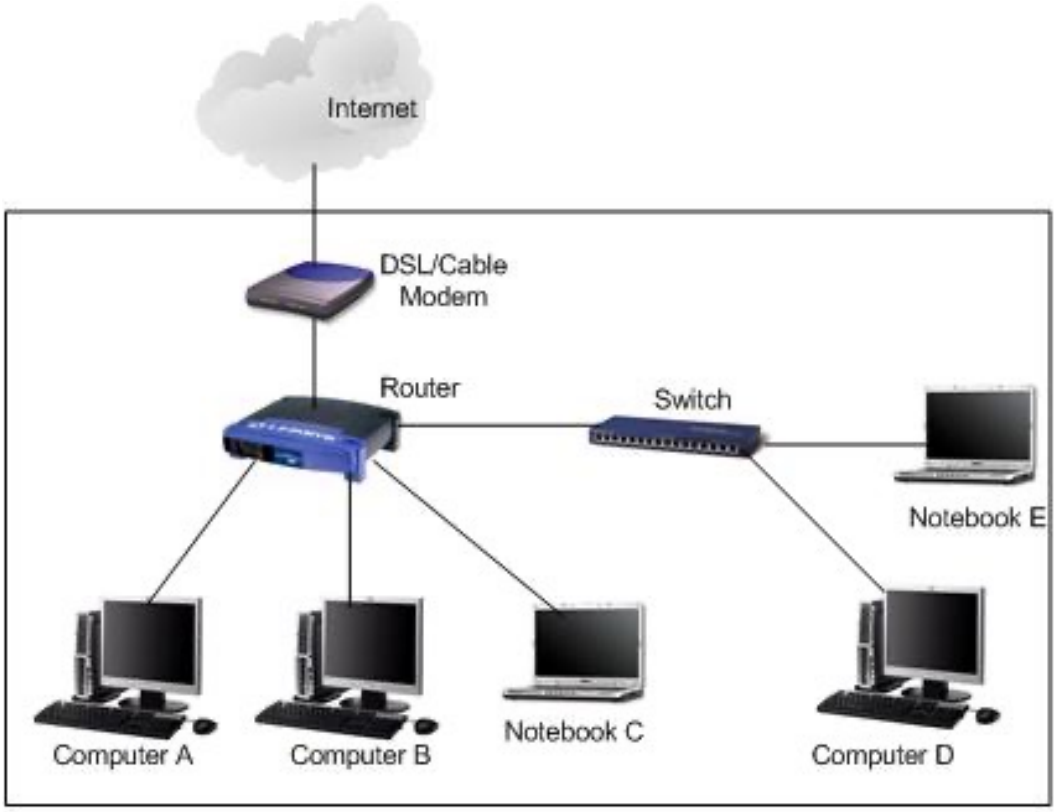


FTP Client: FileZilla

How Networks Work

How Bridges, Routers, and Switches Work

Basic Network Setup



Bridge

- Forward data depending on the destination address in the data packet.
- Address is the MAC address.
- Used to connect two LANs.
- Bridge is software based

Switch

- Similar to Bridges, but have multiple ports
- Switch makes decision in hardware (internal main processer)
- Designed to connect devices

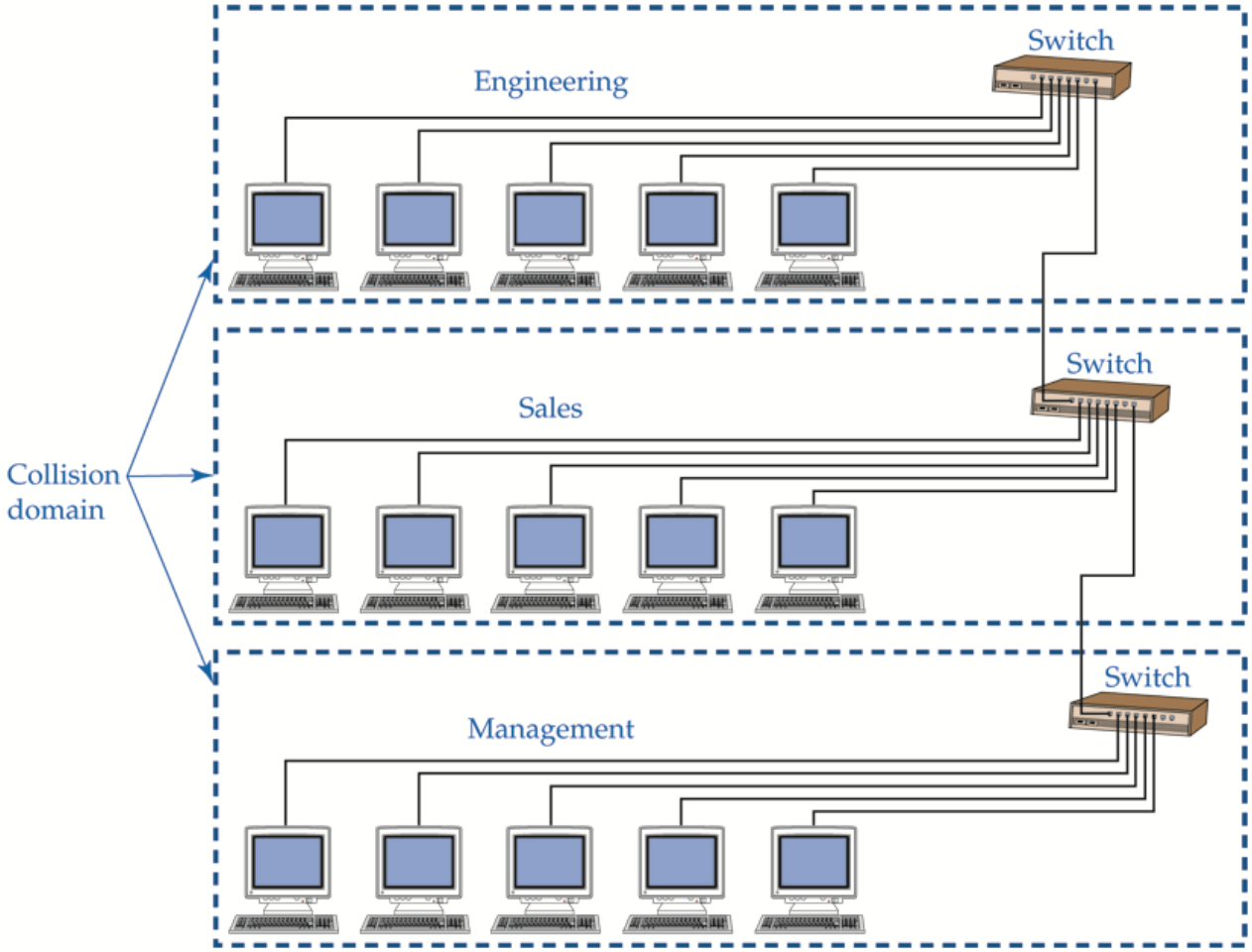
Switch

- 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.

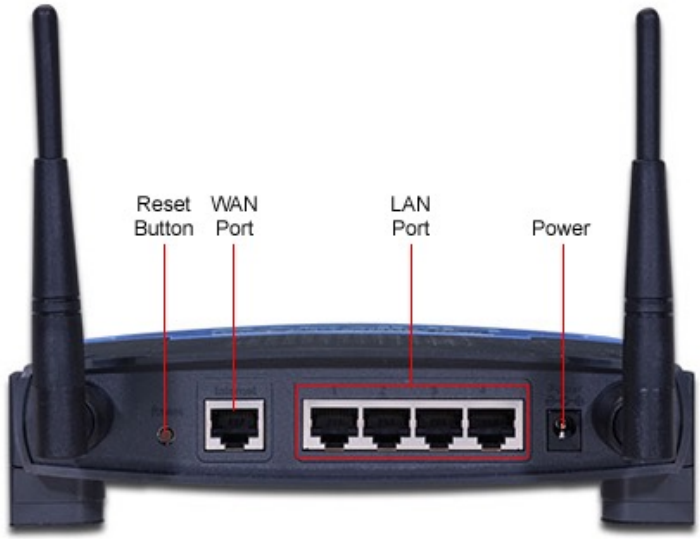
Network Segmenting Devices

- 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



Wireless Router



Linksys WRT54GL Wireless-G Broadband Router

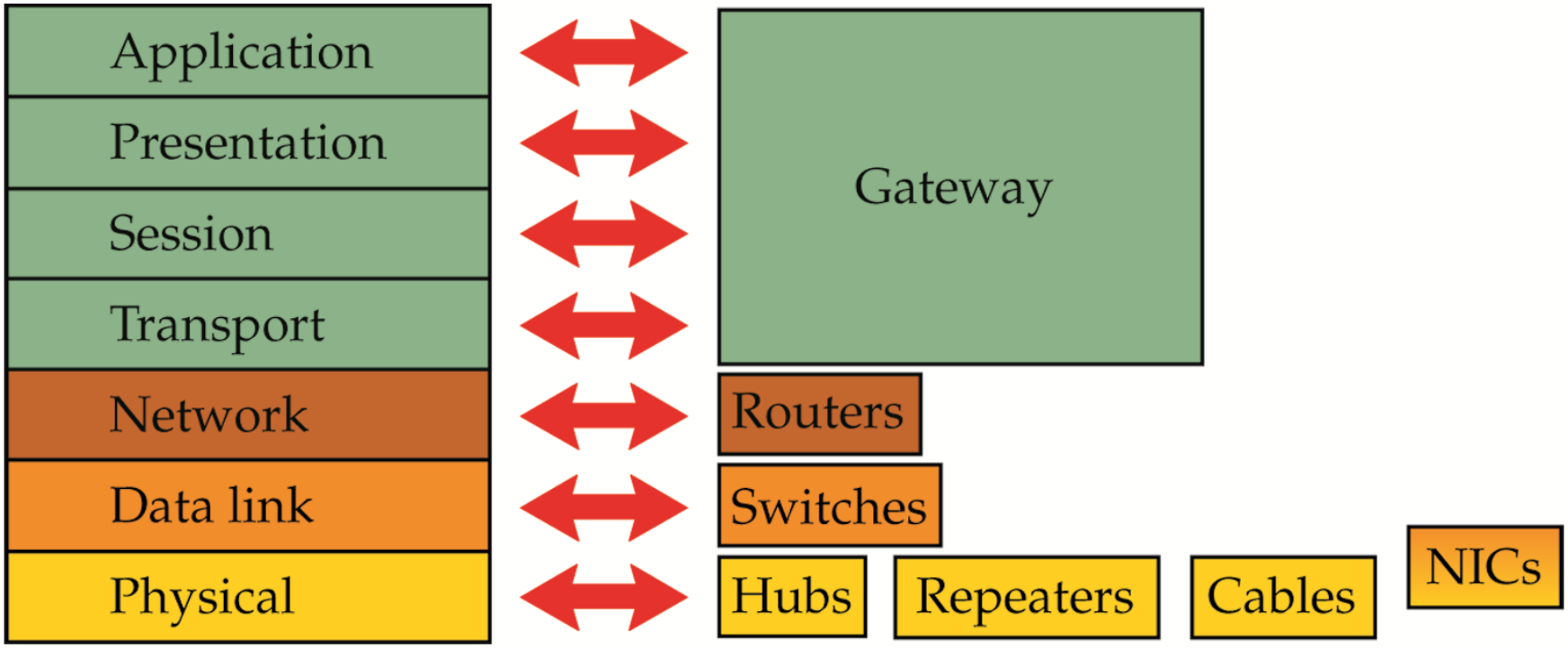
How Networks Work

How Internet Connections Work

Open Systems Interconnection (OSI) Model

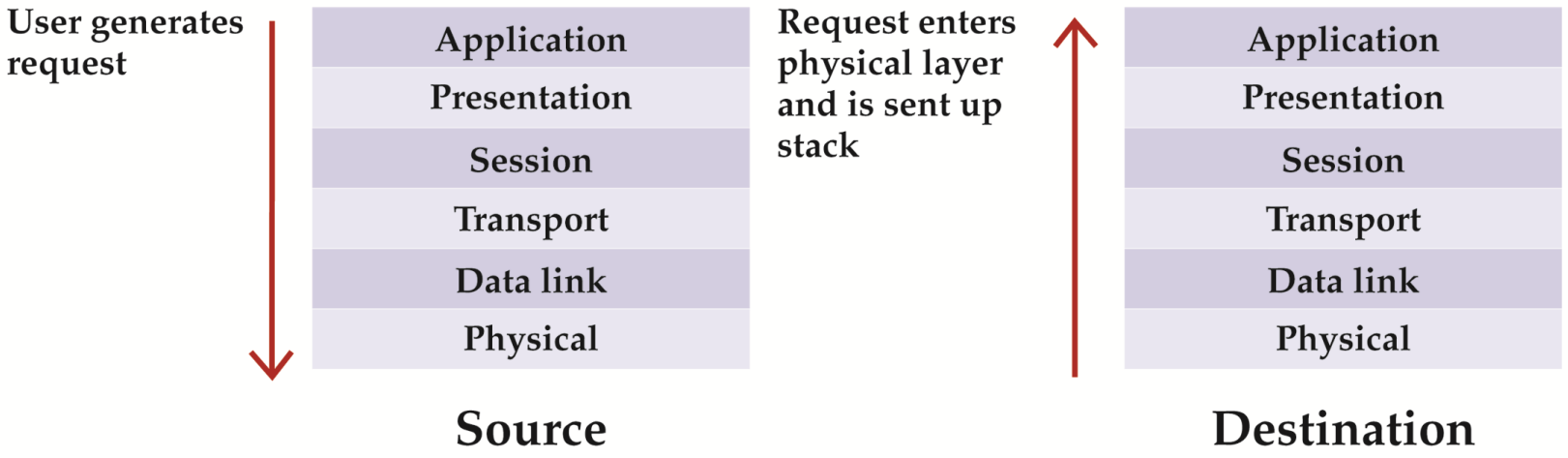
Layer	Function
Application	Interfaces to the network system.
Presentation	Packages data into a universally agreed on form, such as ASCII, BCD, BMP, JPG, and WAV.
Session	Establishes and coordinates communication between two points.
Transport	Ensures accurate delivery.
Network	Encapsulates packets for 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

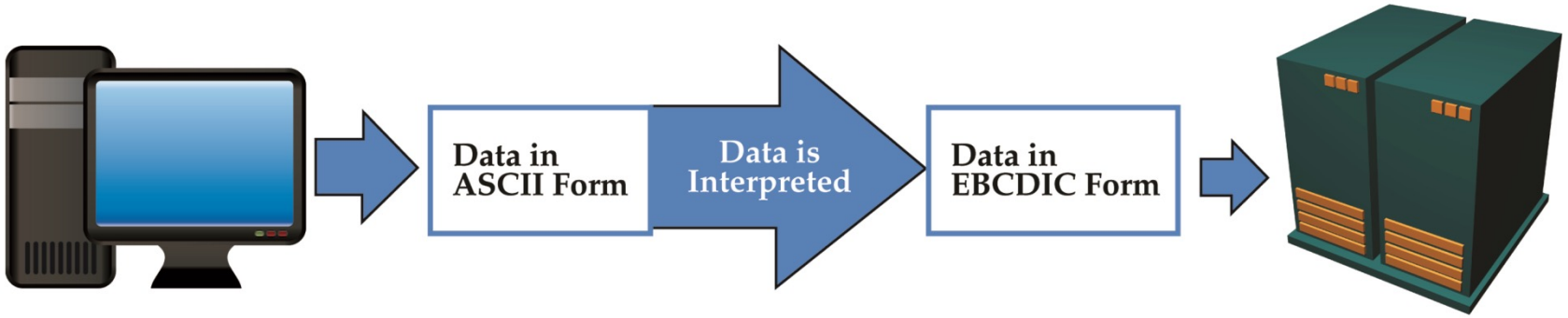
Application Layer

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



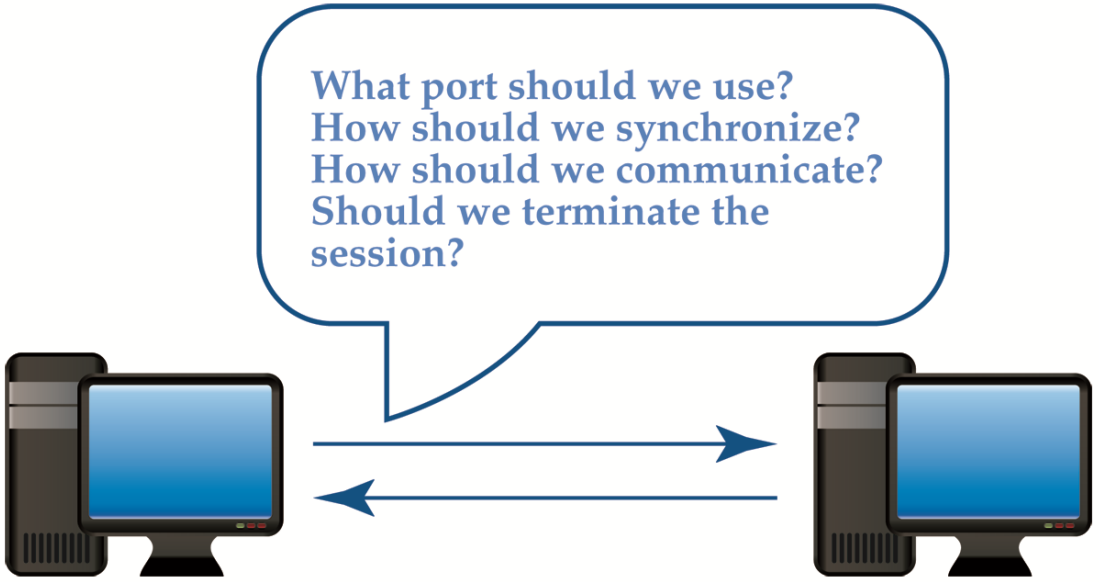
Presentation Layer

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



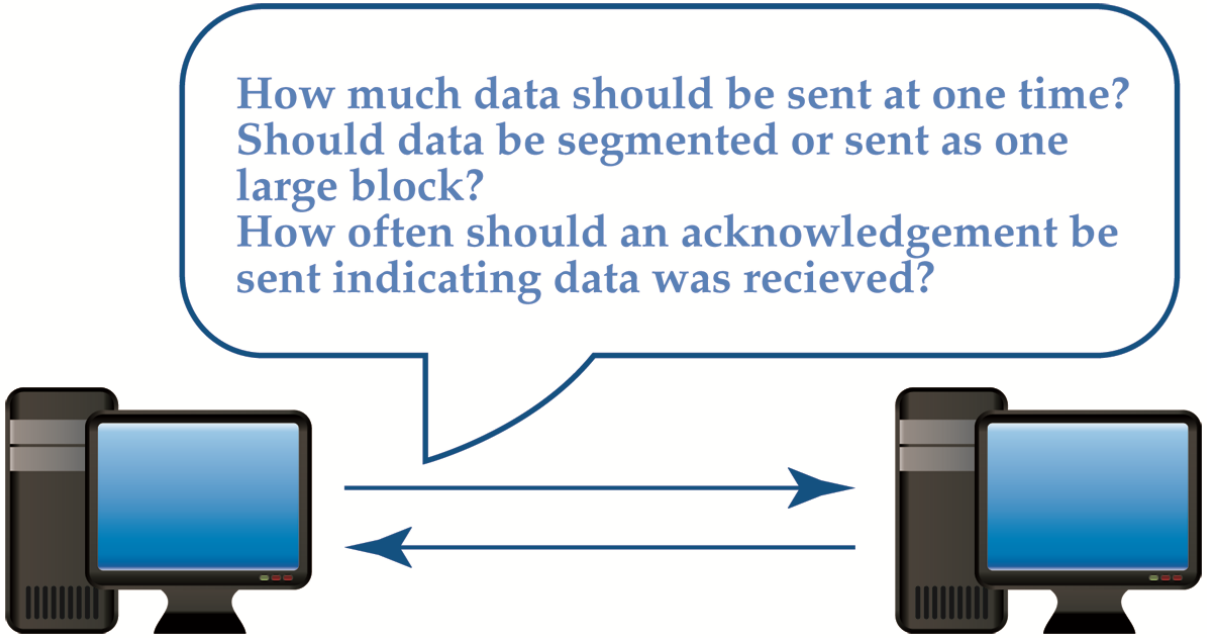
Session Layer

- 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



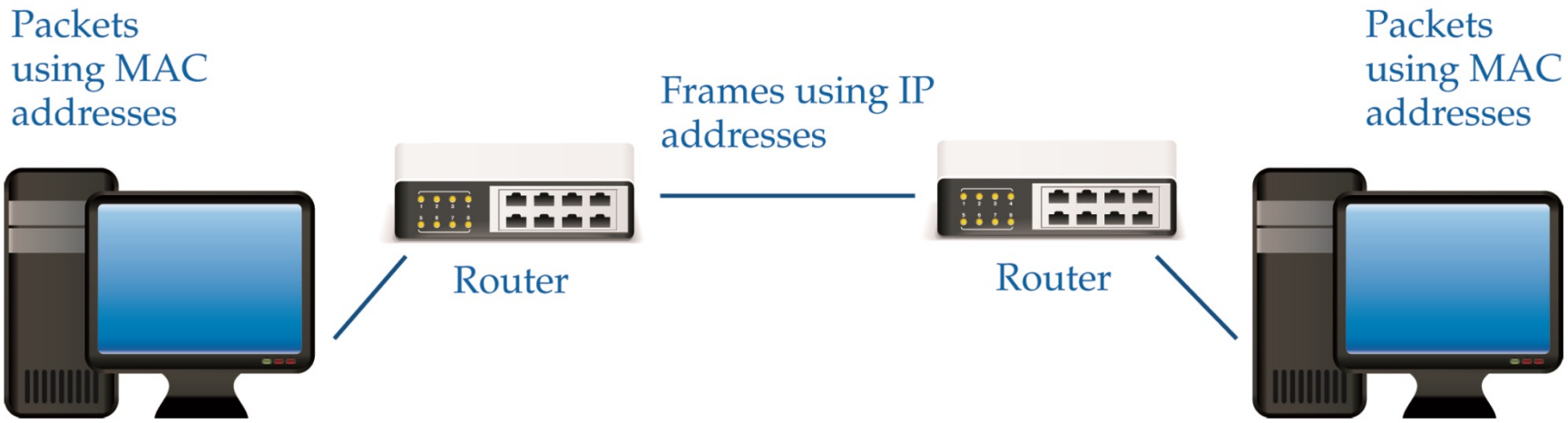
Transport Layer

- Responsible for flow of data to and from destination computer



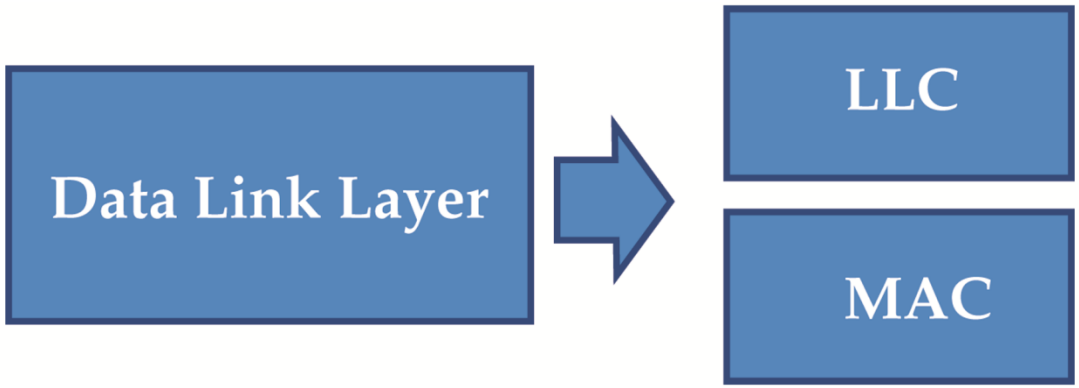
Network Layer

- 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



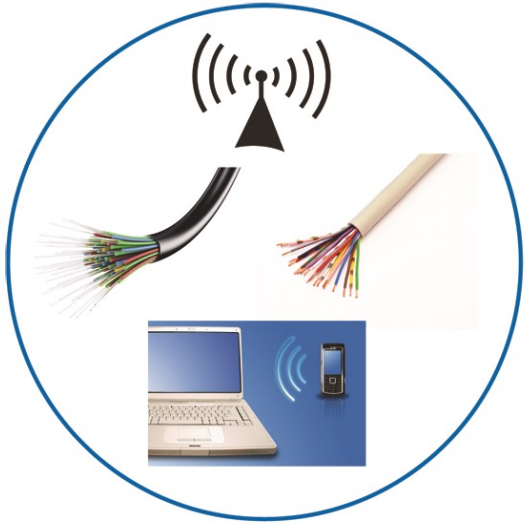
Data Link Layer

- 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

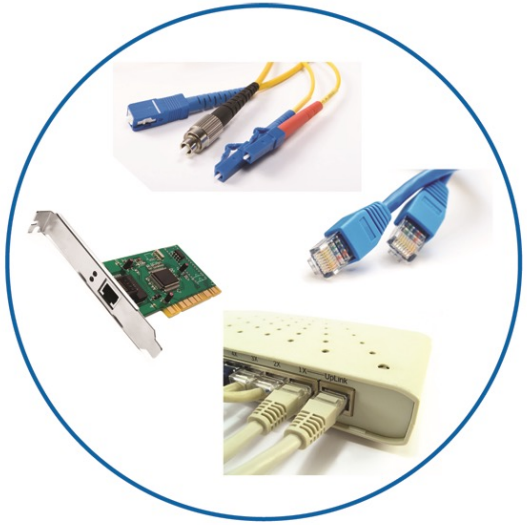


Physical Layer

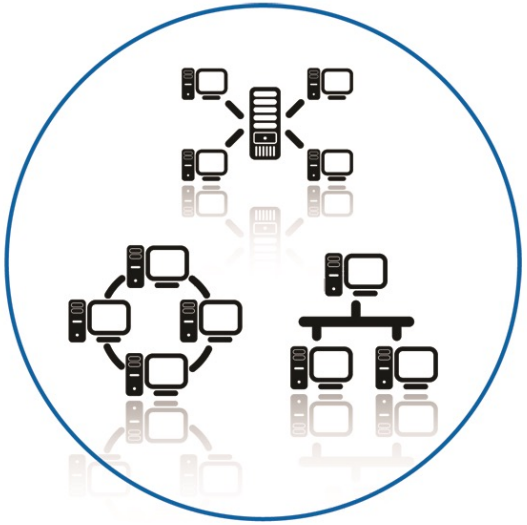
- Concerned with media, hardware, and network topology



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

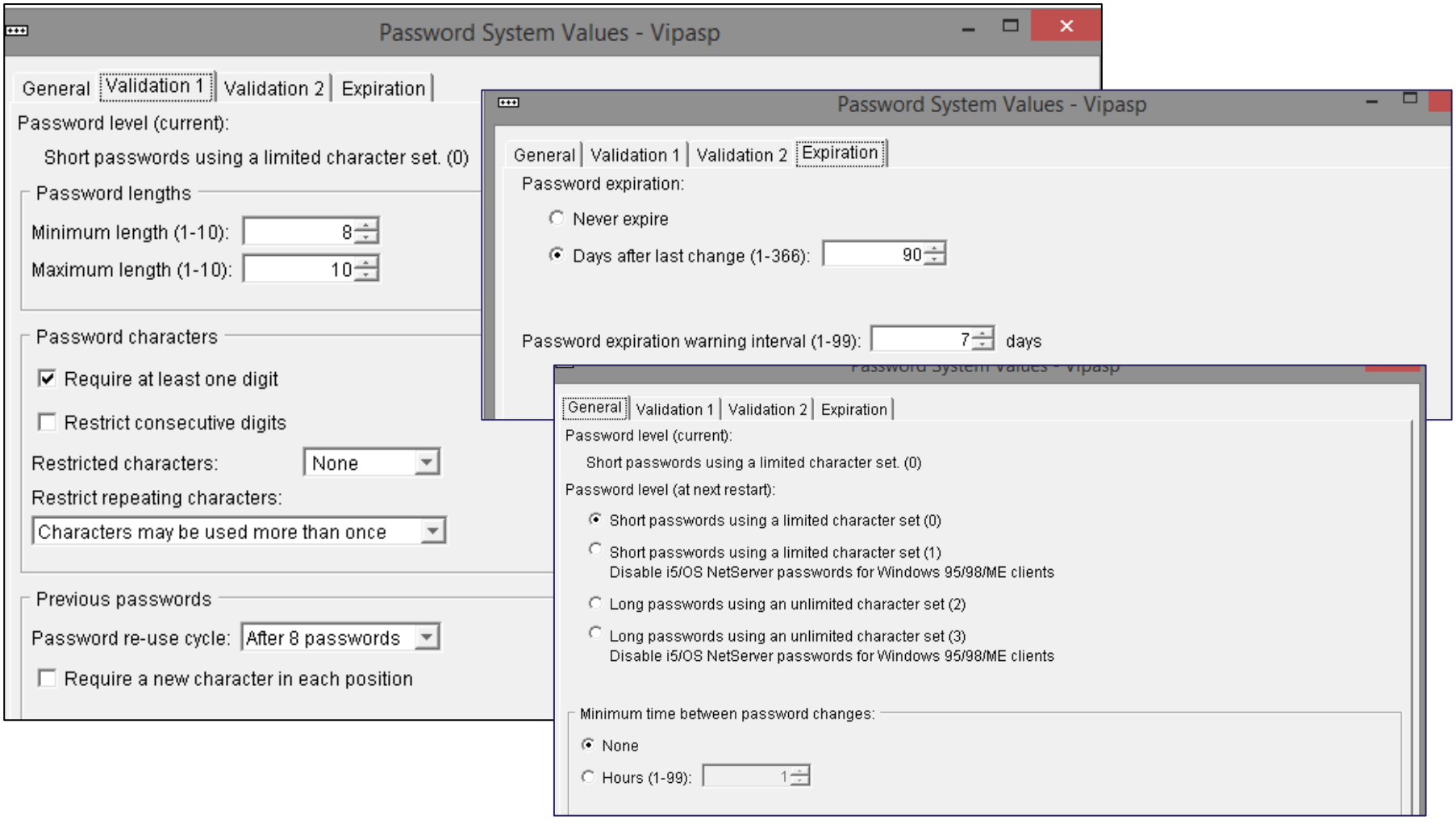
Network Security

- Network security comprises authentication and encryption
- Authentication is typically accomplished through a user name and password
- Other forms of authentication are digital certificates, smart cards, and biometrics

Administrator Account

- User provides password for default administrator account
- Default administrator account name should be changed to better secure network
- Ability to delete or rename the administrator account varies according to operating system

Setting Password Criteria (admin)



User Account Passwords

- To make passwords more secure administrators should:
  - Set defaults for password histories, age, and length
  - Educate users about poor and secure passwords

Poor Passwords

- Poor passwords contain:
  - Words that are found in a dictionary
  - Names familiar to the password owner
  - Keyboard patterns
  - Social security numbers
- Secure passwords are less vulnerable to hashing techniques

Denial of Service (Dos)

- One of the most common attacks on a server
- Can overload a server to the point that it crashes or is not able to complete a legitimate user request

Trojan Horse

- Example: Free download that contains malicious code
- That code could contain virus, worm, or backdoor
- Example: Can imitate legitimate logon screen
- When user logs on, name and password are sent to unauthorized user

E-mail Attachments

- Source of most commonly encountered viruses
- Malicious code can be programmed into attachment
- When recipient opens attachment, malicious program is activated

Social Engineering

- Relies on the gullibility of a network user and his or her respect for authority

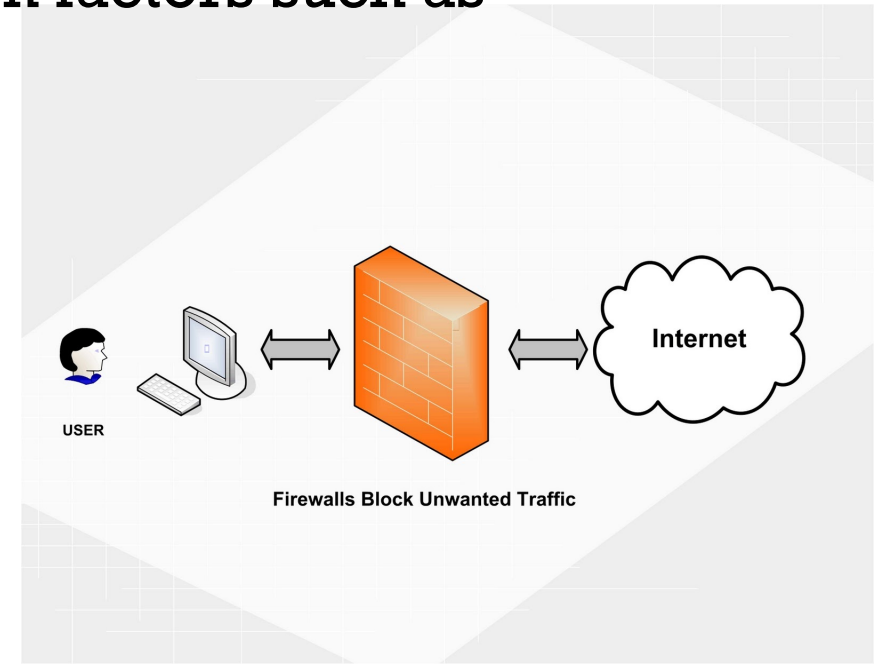
Phishing

- E-mail can appear as if it's from a legitimate company, such as a credit card company
- E-mail requests user's personal information, such as social security number or bank account PIN
- Phony web sites that look authentic, but have slightly different domain names

Legitimate Site	Bogus Site	Look at the following in the bogus Web site:
www.paypal.com	www.paypa1.com	The number *1* used in place of the letter *l*.
www.firstfederal.com	www.firstfedera1.com	The letter *l* again.
www.payonline.com	www.pay0nline.com	The number *0* for the letter *O*.

Firewall

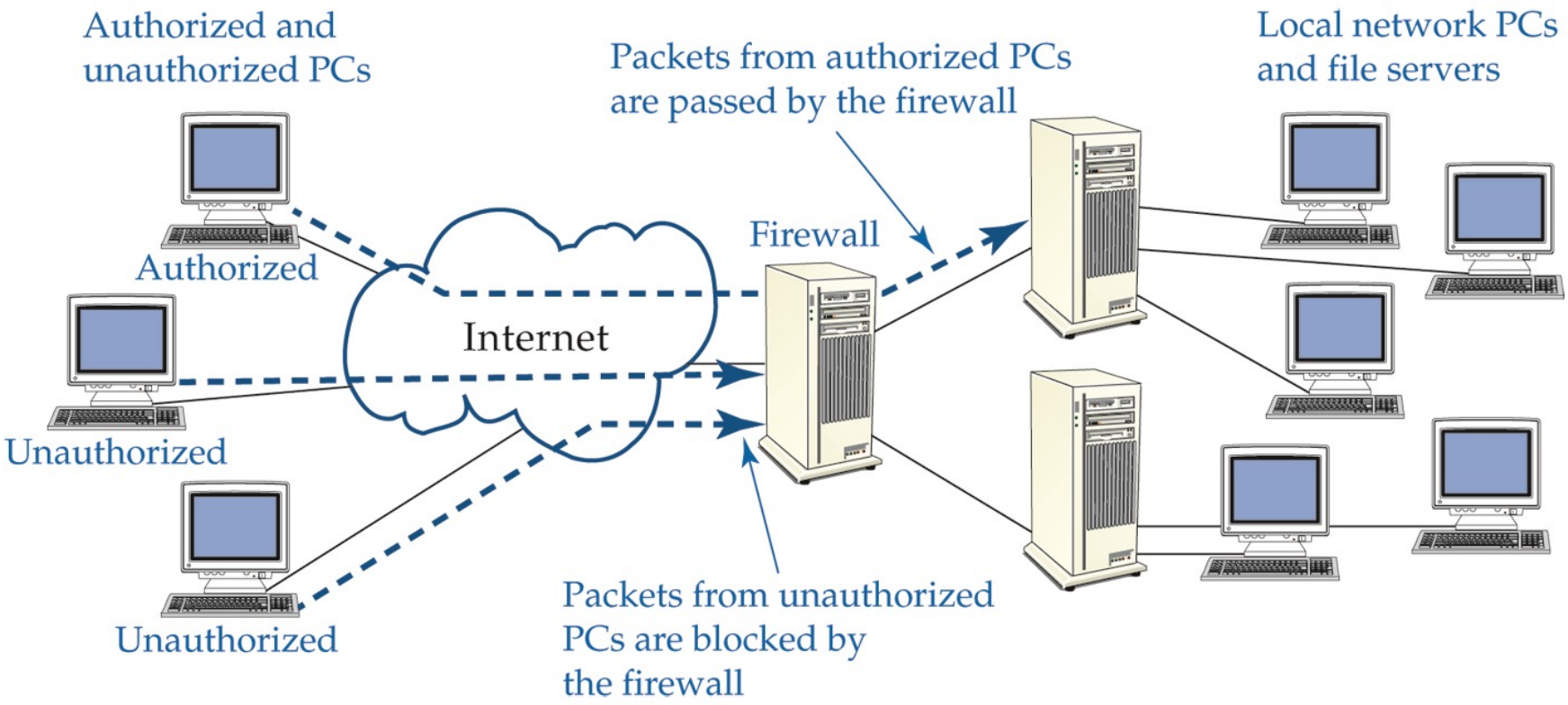
- Can consist of hardware, software, or a combination
- Servers, routers, and PCs may be used
- Designed to filter inbound and outbound flow of network packets based on factors such as
  - IP address
  - Port number
  - Software application
  - Packet contents
  - Protocol



What is a Firewall?

- A layer of security between your home network and the Internet. Since a router or modem is the main connection from a home network to the Internet, a firewall is often packaged with those devices.
- Firewalls are a combination of hardware and software. The hardware part gives firewalls excellent performance, while the software part allows firewalls to be tailored to your specific needs.

Firewall Example



What is a Firewall?

- Some applications outside a network require manually changing your firewall to allow them access. Examples of these applications include online games, VPN, and Voice-Over-IP.
- A firewall does not secure against every kind of data and attack. (still need to run a virus-checker on all your computers.)
- Other products such as Windows and macOS create software firewalls. These can cause network problems, because they are trying to apply different security to your network, which other firewalls will not accept. May need to disable conflicting firewalls.
- Firewall features vary by model - newer and more expensive products have more advanced features. Firewall features are described in a product's datasheet, and their configuration information is found in the manuals.
- The term firewall is often used to describe the part of a network that is protected by a firewall, as in the phrase behind the firewall. Parts of a network that are outside the firewall are more vulnerable to attack.

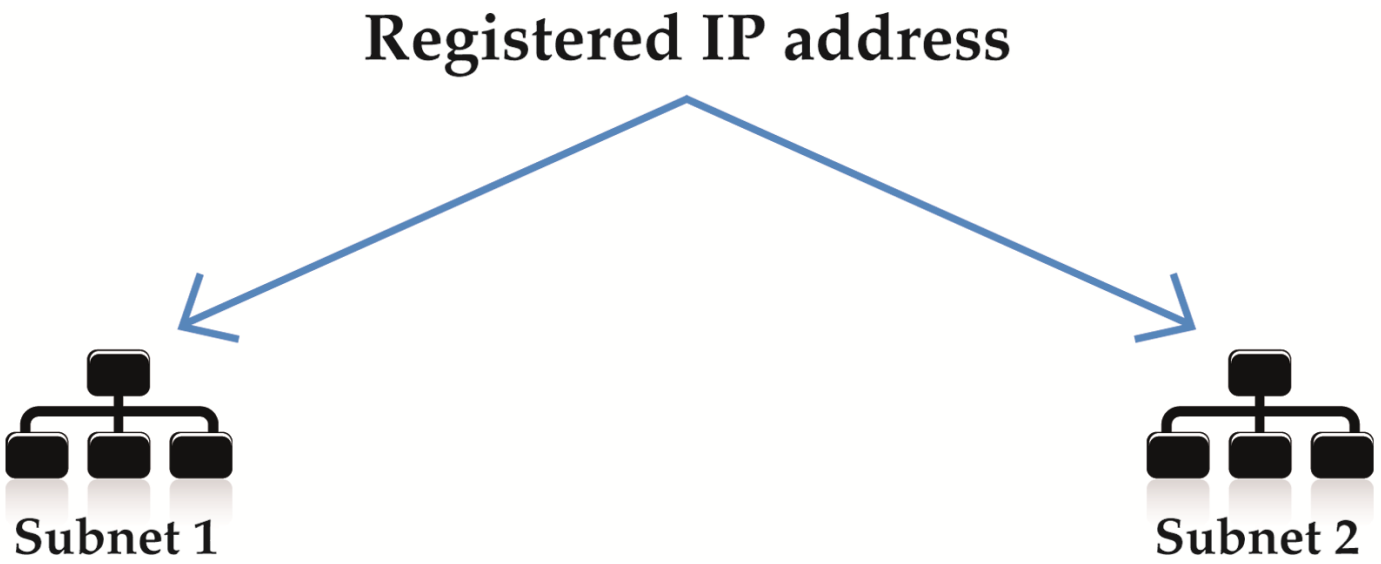
Network Address Translation (NAT)

- Allows unregistered private network addresses to communicate with legally registered IP addresses
- Advantages
  - Hides internal IP addresses, thus providing security
  - Eliminates need for multiple registered IP addresses
  - Allows multiple ISDN (Integrated Services for Digital Network) connections to be combined into one Internet connection

How Networks Work

Subnetting

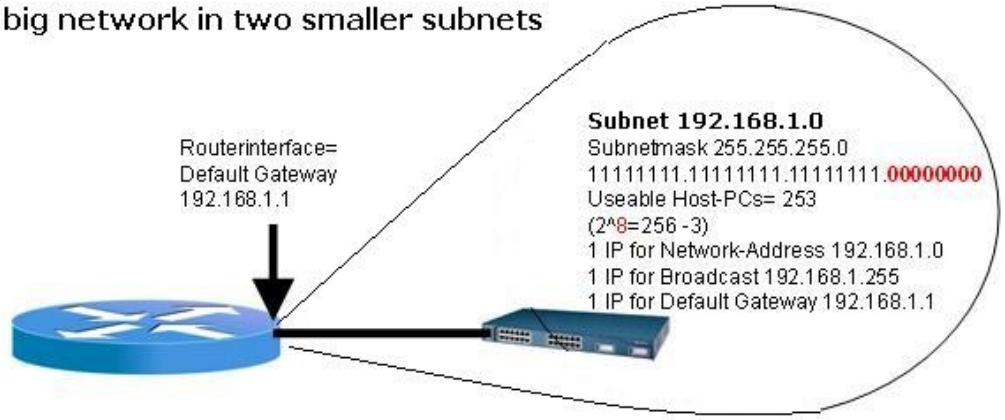
Purpose of Subnetting



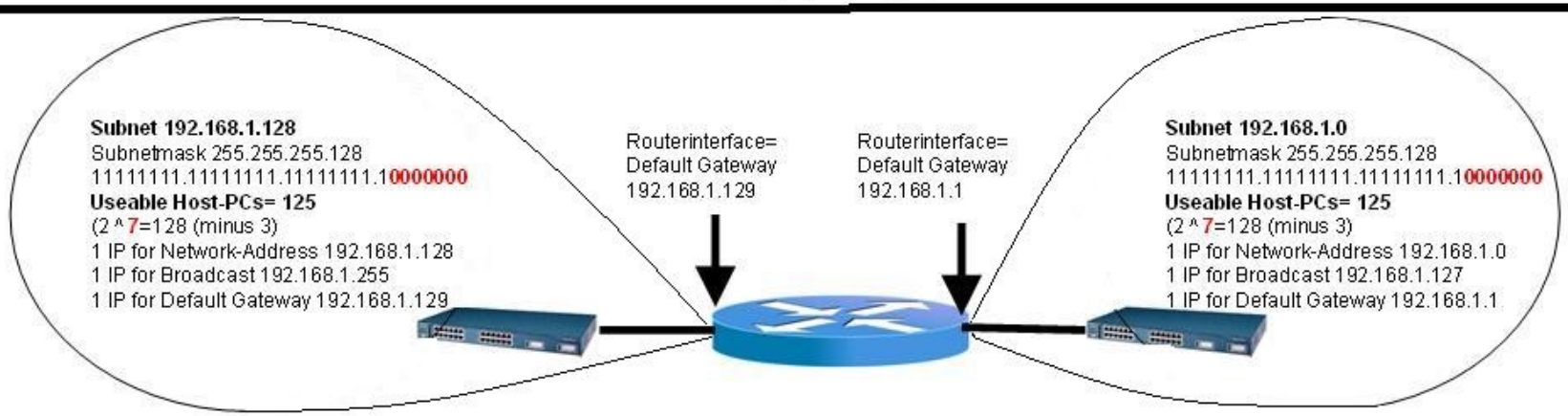
Advantages / Disadvantages

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).



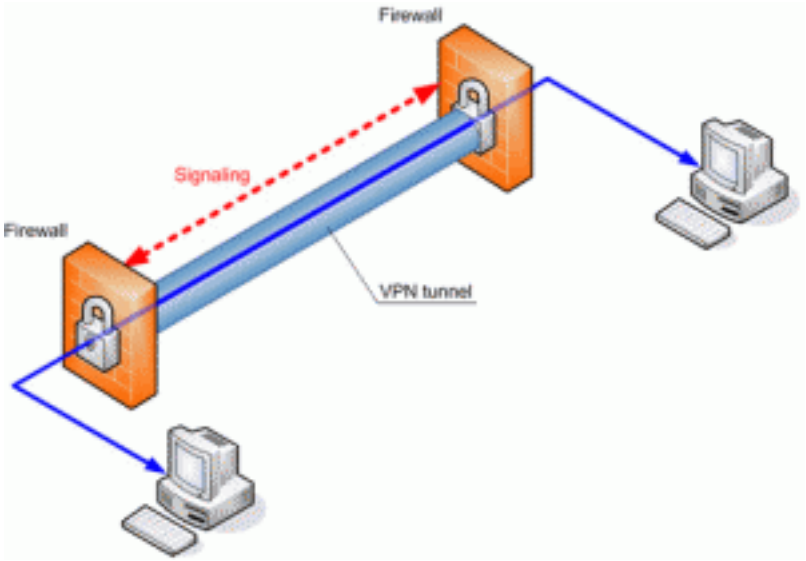
Now we have TWO subnets,
192.168.1.0 and 192.168.1.128.
Each has 125 useable IP-Addresses for Host-PCs.

How Networks Work

VPN

Virtual Private Network (VPN)

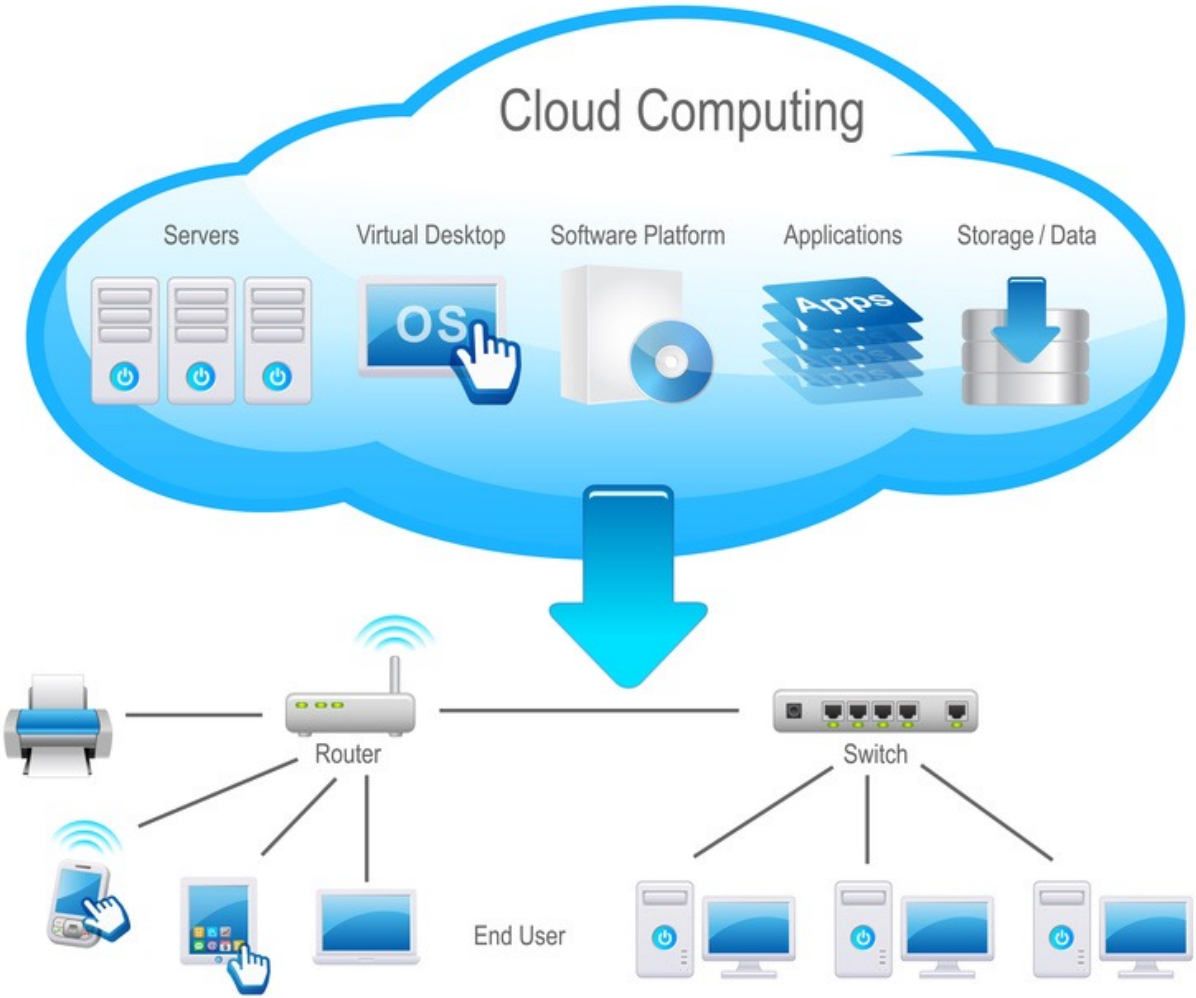
- Creates a private connection over the Internet or Intranet
- VPN software and firewalls provide security
- Four most common protocols used in a VPN are PPTP, L2F, L2TP, and IPSec



How Networks Work

Cloud Computing

Cloud Computing



How Networks Work

Network Troubleshooting

Troubleshooting Methodology

Given a scenario, implement the following network troubleshooting methodology:

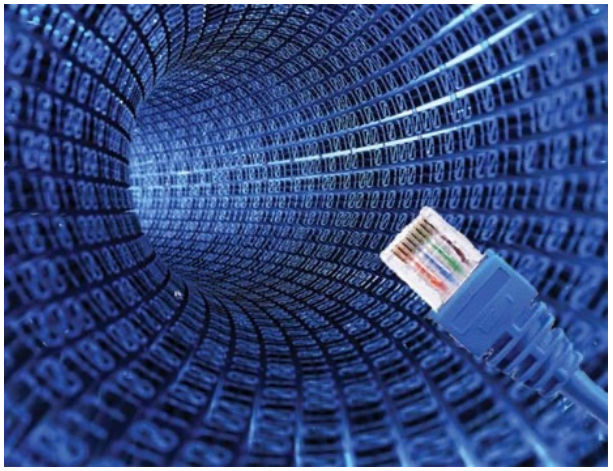
1. Information gathering—identify symptoms and problems.
2. Identify the affected areas of the network.
3. Determine if anything has changed.
4. Establish the most probable cause.
5. Determine if escalation is necessary.
6. Create an action plan and solution identifying potential effects.
7. Implement and test the solution.
8. Identify the results and effects of the solution.
9. Document the solution and the entire process.

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

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



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