NETWORKING AND THE INTERNET

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Contents

- Network Fundamentals
- The Internet
- The World Wide Web
- Internet Protocols
- Security
- About Networks and Telecommunications Department

NETWORK FUNDAMENTALS

Networks

- Links multiple computer systems and enables them to share data and resources

Network components

PC

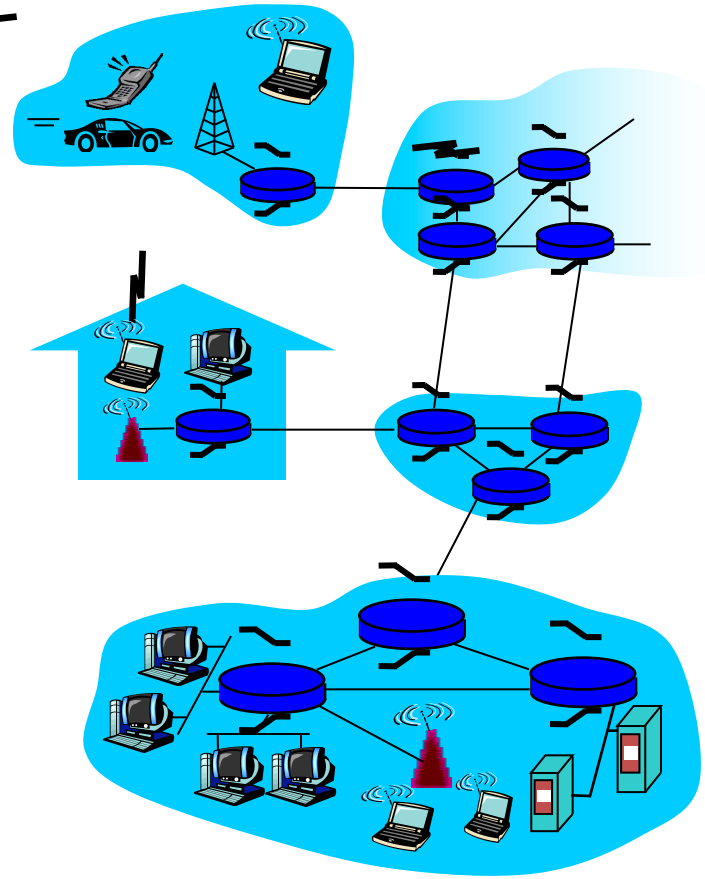
server

wireless laptop

cellular handheld

❑ *Thiết bị đầu cuối*

- ❖ chạy ứng dụng mạng



❑ *Phương tiện kết nối*

wireless

wired links

- ❖ cáp, sóng vô tuyến

router

❑ *Thiết bị liên mạng*

- ❖ Routers, switch,hub…
- ❖ Chuyển tiếp dữ liệu

Network components

- Node
  - Any device connected to a network
- Logical address
  - Unique name assigned to each node on the network
- Physical address
  - Unique numeric that identifies each node on the network built into the hardware
- Network interface card (NIC)
  - Expansion board or adapter that provides a connection between the computer and the network
  - Notebook computers have wireless NICs

Network components

- USB wireless network adapter
  - Plugs into a USB port
  - Usually provides an intuitive graphical user interface (GUI) for easy configuration
- Wireless PC card adapter
  - About the size of a credit card
  - Inserted into a slot on the side of most notebooks and netbooks
  - Has built-in WiFi antenna that provides wireless capability
  - LED lights that indicate whether the computer is connected

Connecting Networks

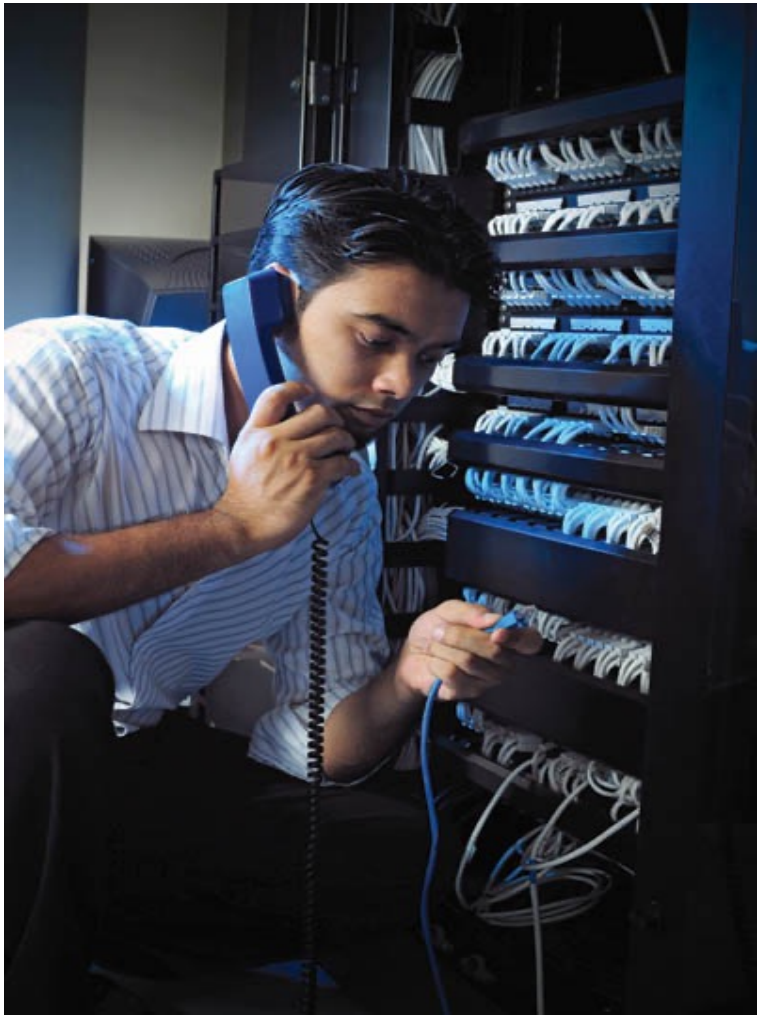
- **Repeater:** Extends a network
- **Hub:** also acts as a repeater with many ports
- **Bridge:** Connects two compatible networks
- **Switch:** Connects several compatible networks
- **Router:** Connects several incompatible networks, determine the best route to transmit data

Network components

- Server
  - Computer or device with software that manages network resources, such as files, e-mails, printers, databases
- File server
  - Most common type of server
  - High-speed computer that provides program and data files to network users
  - Contains the network operating system (NOS)
    - File directories for file and resource location on the LAN
    - Automated distribution of software updates to desktop computers on the WAN
    - Internet services support
    - Protection of services and data
    - Access to connected hardware by authorized users

Network Fundamentals

- **Network administrator**
  - Also called network engineer
  - Installs, maintains, supports computer networks
  - Interact with users
  - Handle security
  - Troubleshoot problems



Advantages - Disadvantages

Advantages

- Reduced hardware costs
- Application sharing
- Sharing information resources
- Data management centralization
- Connecting people

disadvantages

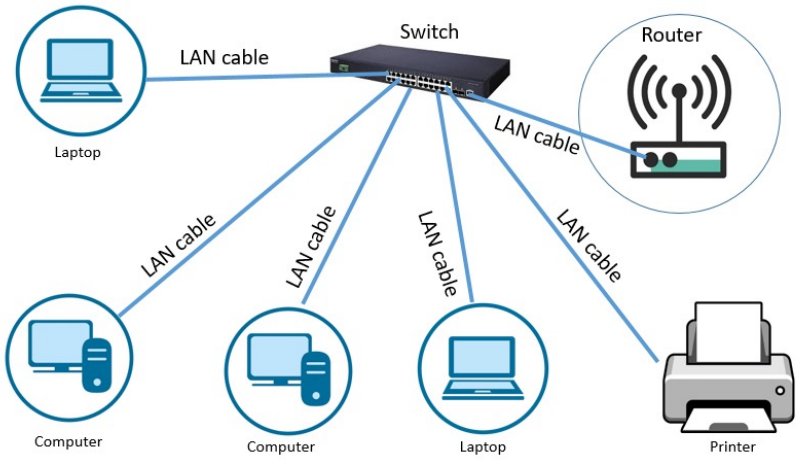
- Loss of autonomy
- Lack of privacy
- Security threats
- Loss of productivity

Network Classifications

- Scope
  - Personal area network (PAN)
  - Local area network (LAN)
  - Metropolitan area (MAN)
  - Wide area network (WAN)
- Ownership/Function
  - Closed versus open
- Topology (configuration)
  - Bus (Ethernet)
  - Star (Wireless networks with central Access Point)
  - Ring

Network classification by scope

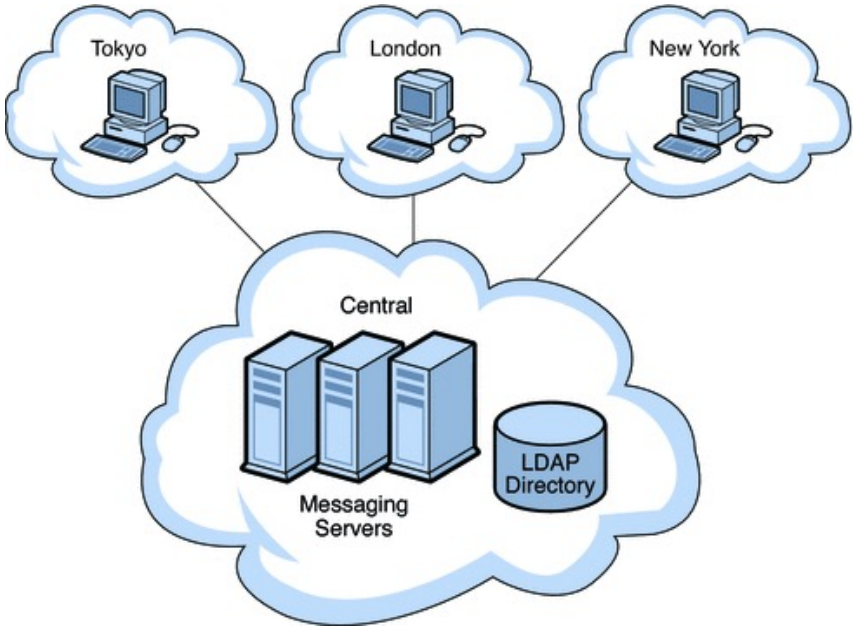
- **Local Area Network (LAN)**
  - Uses cables, radio waves, or infrared signals
  - Links computers in a limited geographic area



Local Area Network

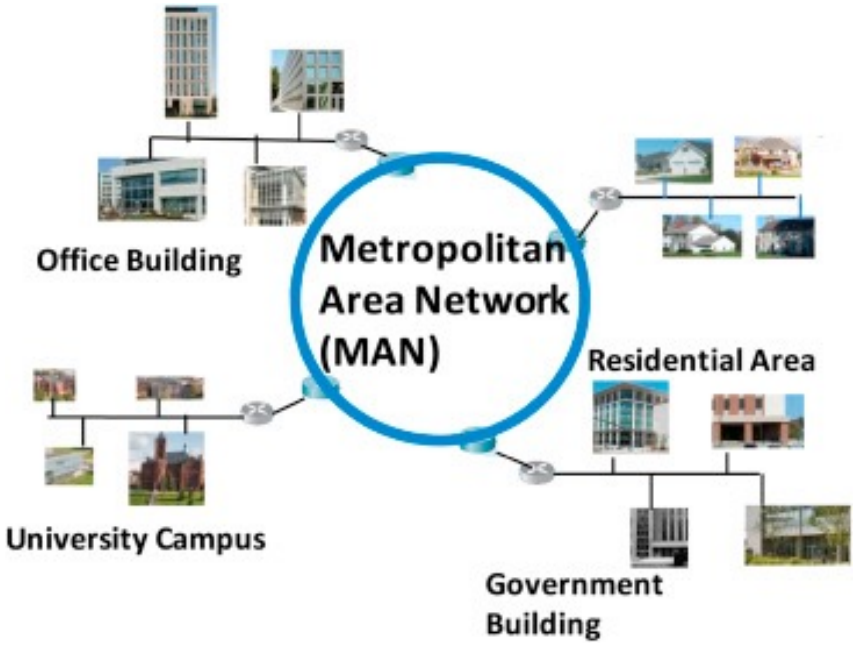
Network classification by scope

- **Wide Area Network (WAN)**
  - Uses long-distance transmission media
  - Links computer systems a few miles or thousands of miles
  - Internet is the largest WAN



Network classification by scope

- **Metropolitan Area Network (MAN)**
  - Designed for a city
  - Larger than a LAN, smaller than a WAN



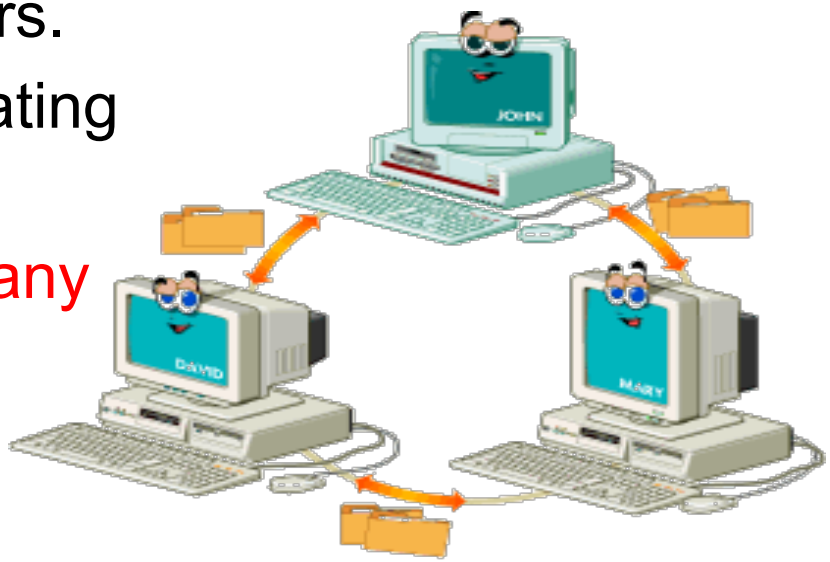
Network classification by scope

- **Campus Area Network (CAN)**
  - Several LANs located in various locations on a college or business campus
  - Smaller than a WAN
  - Use devices such as switches, hubs, and routers
- **Personal Area Network (PAN)**
  - Network of an individual's own personal devices
  - Usually within a range of 32 feet
  - Usually use wireless technology

Network classification by function

Peer to peer (P2P): The computers have the same role.

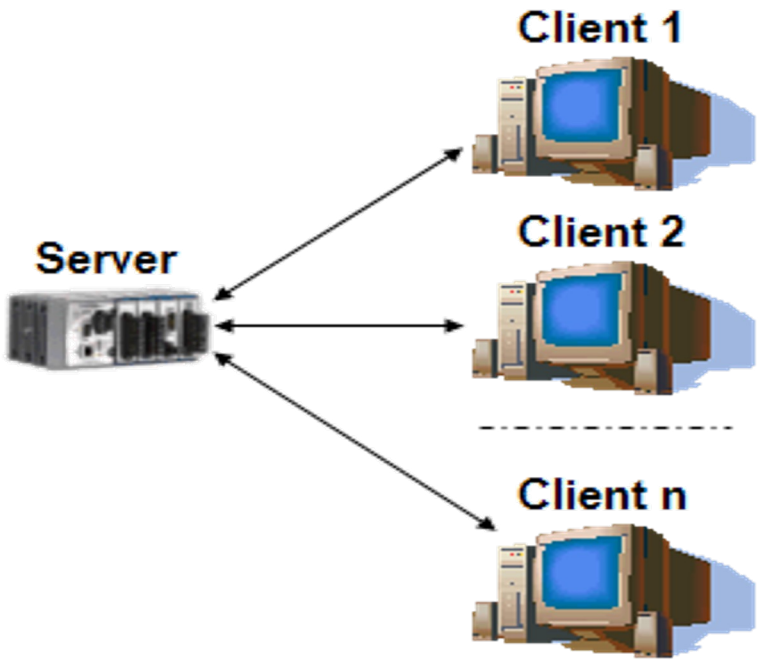
- Share files without a file server.
- Easy to set up.
- Best used for home or small offices with no more than 10 computers.
- Do not require a network operating system.
- Can be slow if there are too many users.
- Security not strong.



Network classification by function

Client/server:

- Made up of one or more file servers and clients (any type of computer).
- Client software enables requests to be sent to the server.
- Wired or wireless connections
- Do not slow down with heavy use.



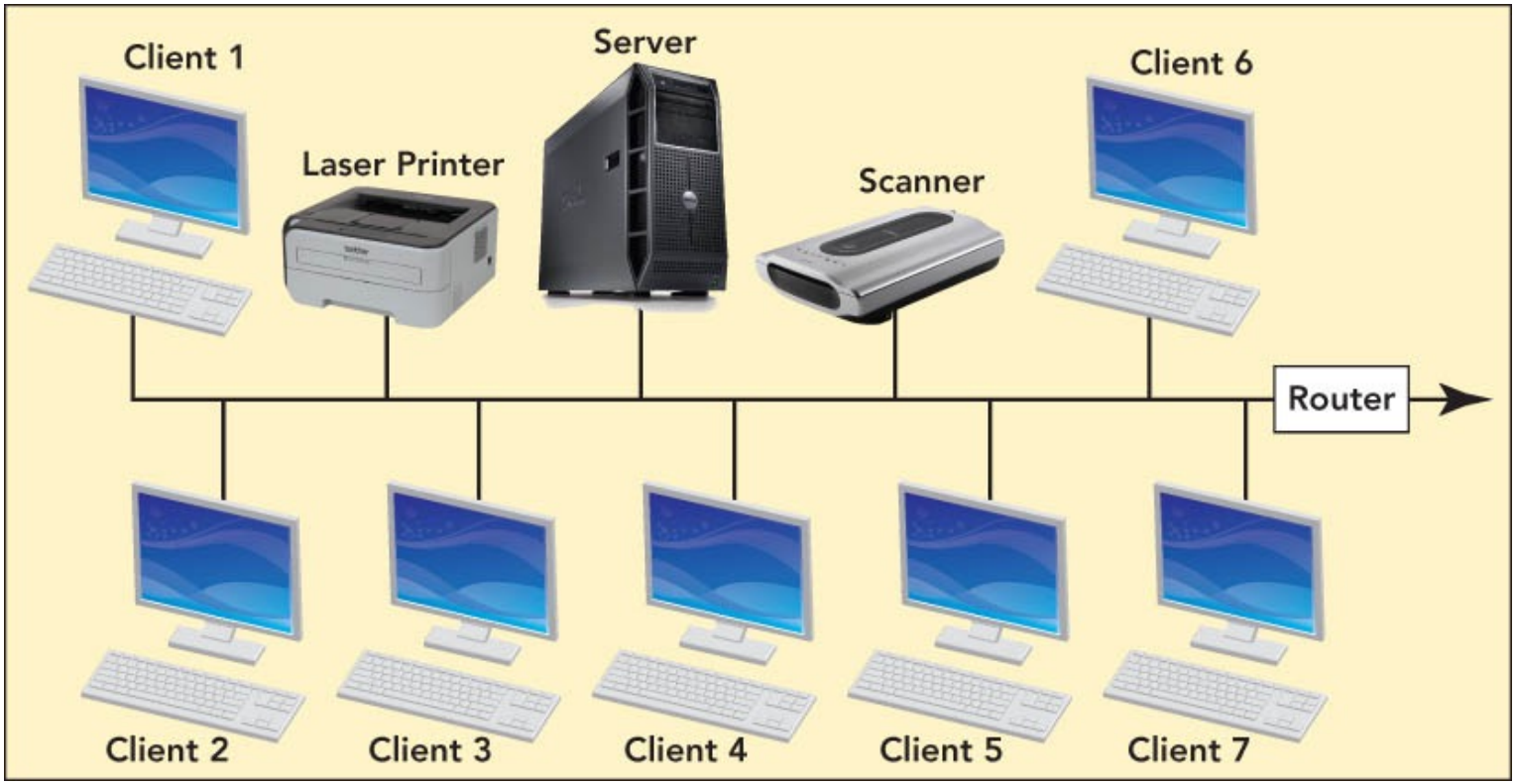
Network classification by topologies

- Network topology
  - Physical design of a LAN
- Topology resolves contention—conflict that occurs when two or more computers on the network attempt to transmit at the same time
- Contention sometimes results in collisions—corruption of network data caused when two computers transmit at the same time

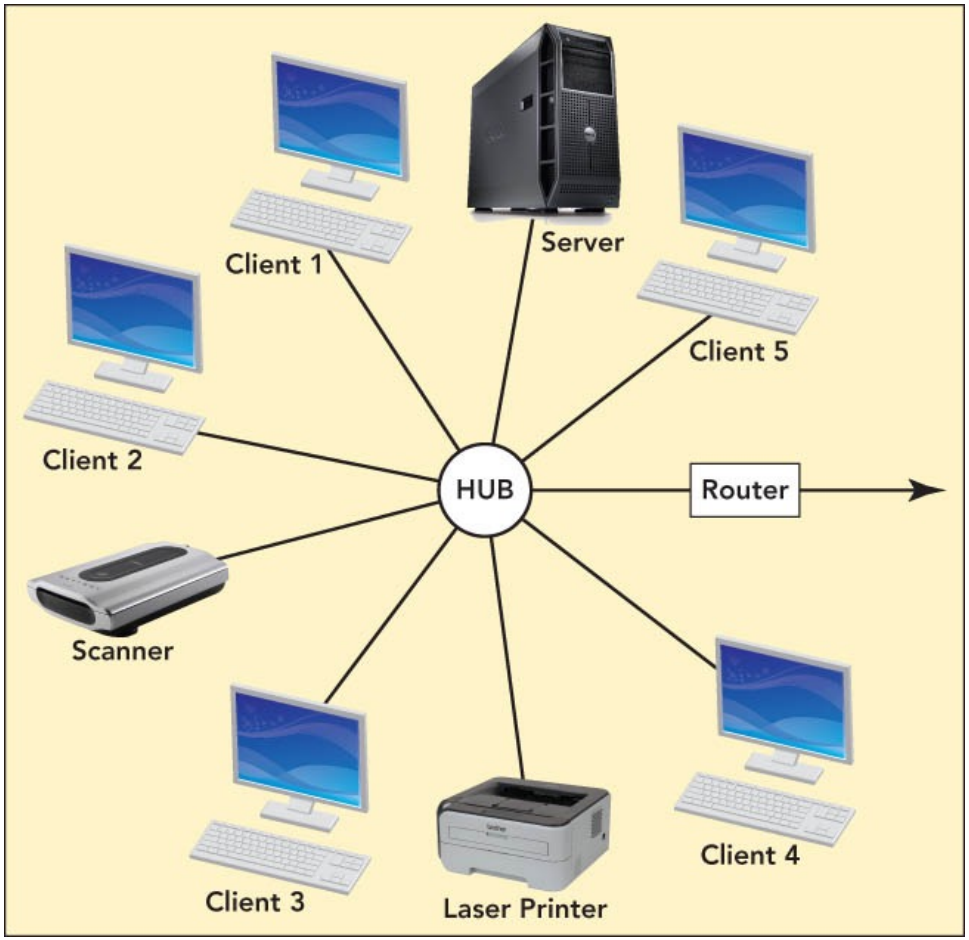
Network classification by topologies

- **Bus topology**
  - Practical for home or small office
  - One node transmits at a time
  - Terminators signify the end of the circuit
  - Uses contention management—technique that specifies what happens when a collision occurs
- **Star topology**
  - For office buildings, computer labs, and WANs
  - Easy to add users
- **Ring topology**
  - For a division of a company or one floor
  - Not in common use today
  - Node can transmit only when it has the token—special unit of data that travels around the ring

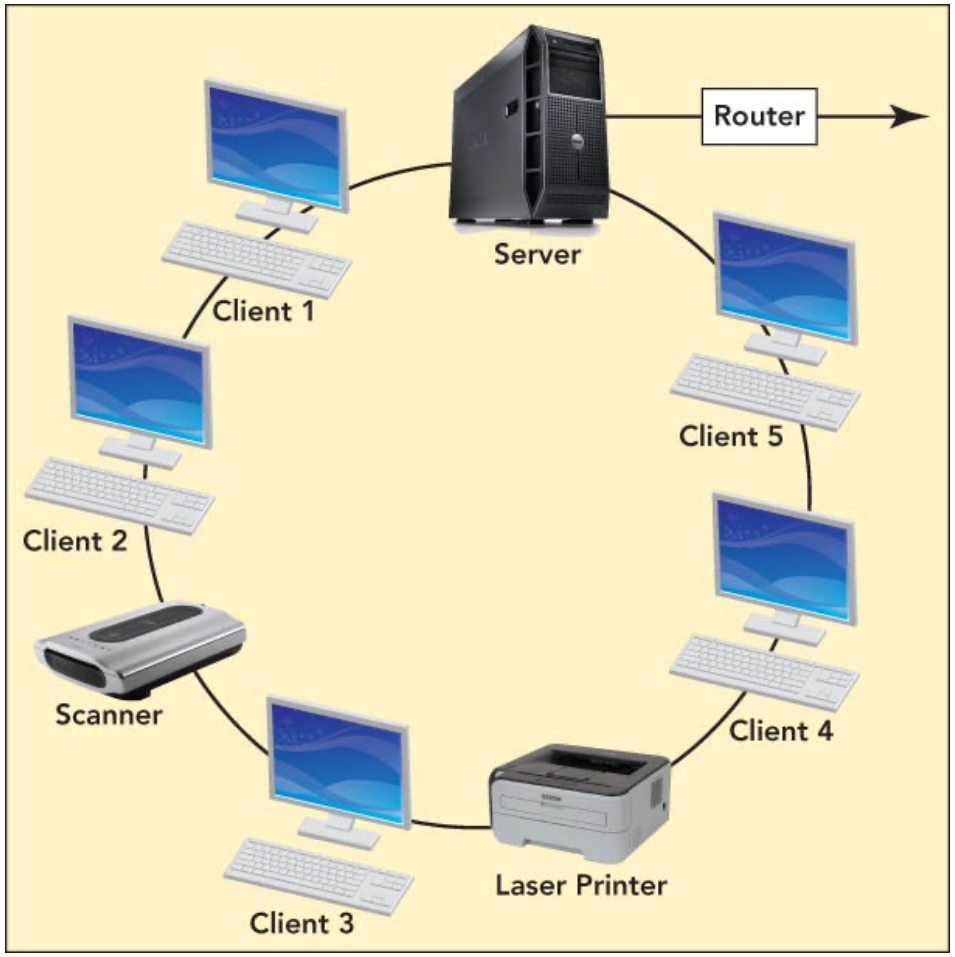
Bus topology



Star topology



Ring topologies



THE INTERNET

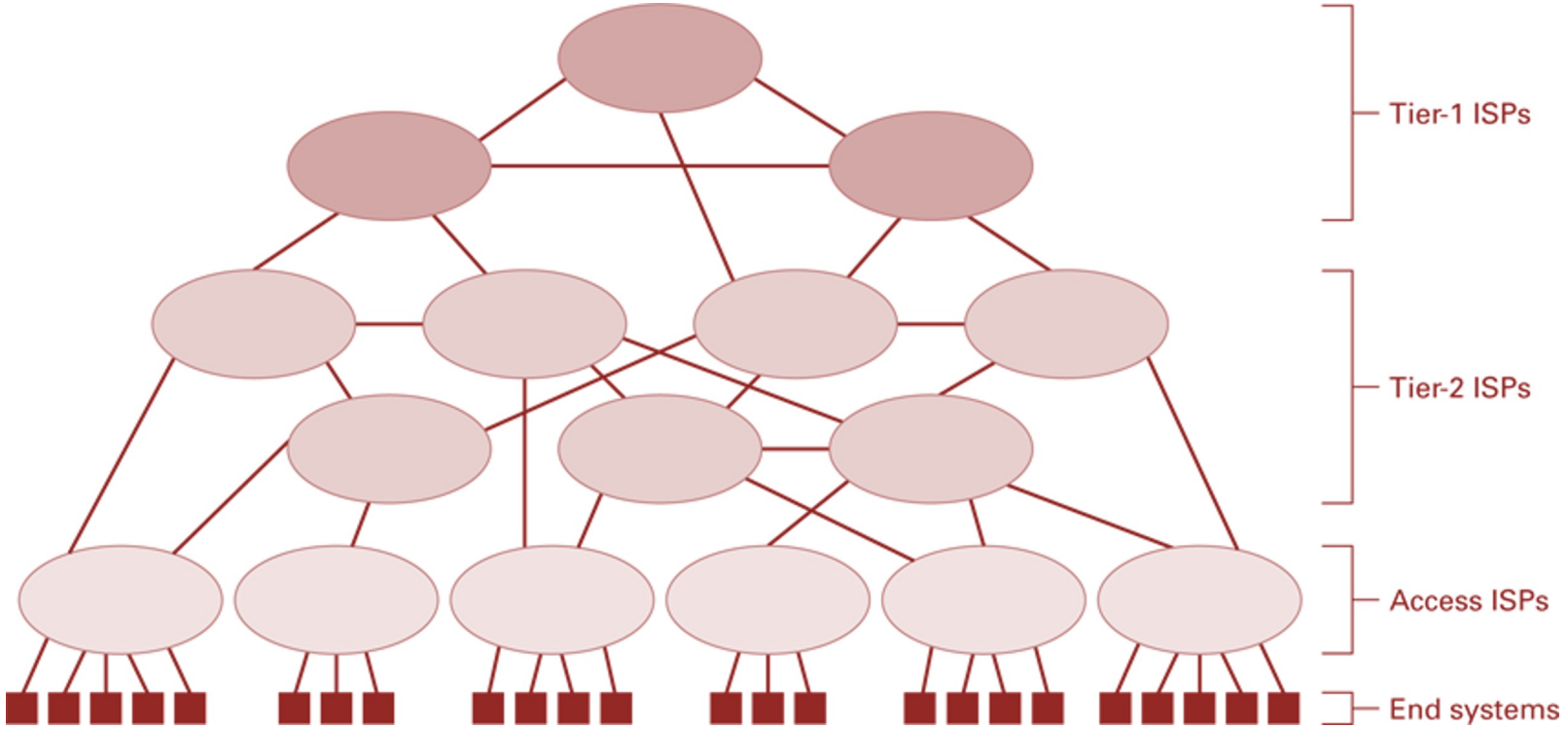
The Internet

- The Internet: An internet that spans the world
  - Original goal was to develop a means of connecting networks that would not be disrupted by local disasters
  - Today a commercial undertaking that links a worldwide combination of PANs, LANs, MANs, and WANs involving millions of computers

Internet Architecture

- Internet Service Provider (ISP)
  - Tier-1
  - Tier-2
- Access or tier-3 ISP: Provides connectivity to the Internet
  - Hot spot (wireless)
  - Telephone lines
  - Cable/Satellite systems DSL
  - Fiber optics

Internet Composition



Internet Addressing

- IP address: pattern of 32 or 128 bits often represented in dotted decimal notation

Example: private IP: 192.168.1.1

public IP: 8.8.8.8

- Mnemonic address:
  - Domain names
  - Top-Level Domains
- Domain name system (DNS)
  - Name servers
  - DNS lookup

ICANN

- **Internet Corporation for Assigned Names & Numbers (ICANN).**
- Allocates IP addresses to ISPs who then assign those addresses within their regions.
- Oversees the registration of domains and domain names.

Early Internet Applications

- Network News Transfer Protocol (NNTP)
- Transmission Control Protocol (TCP)
- File Transfer Protocol (FTP)
- Telnet and SSH (Secured Shell)
- Hypertext Transfer Protocol (HTTP)
- Electronic Mail (email)
  - Domain mail server collects incoming mail and transmits outing mail
  - Mail server delivers collected incoming mail to clients via POP3 (Post Office Protocol version 3) or IMAP (Internet Mail Access Protocol)

WORLD WIDE WEB

Word Wide Web

- ***Hypertext*** combines internet technology with concept of linked-documents. Embeds hyperlinks to other documents.
- Hypertext is written in the **HTML** (hypertext markup language).
- Each hypertext is referred to by the term ***"web page"***.

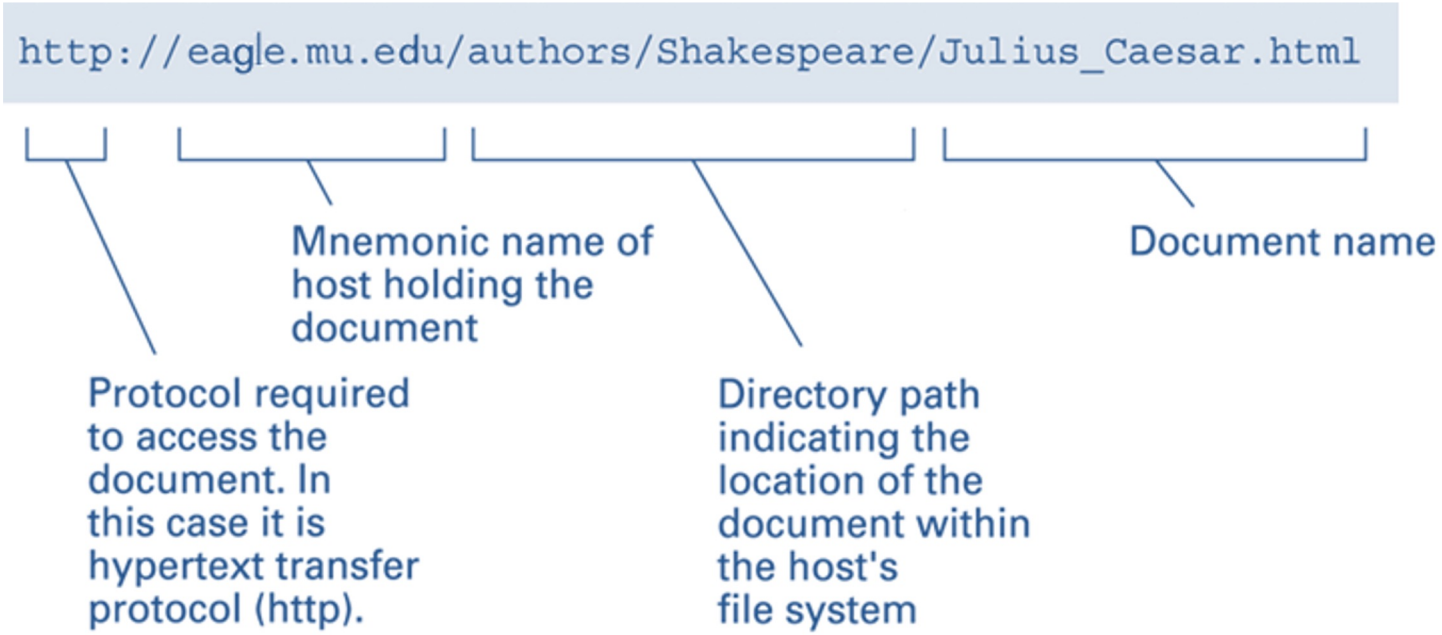
```
<!DOCTYPE html PUB
"http://www.w3.org
<html xmlns="http:

<head>
<meta name="keywor
"thinkquest,web,to
<meta name="descri
```

Word Wide Web

- **Website**: A collection of many webpages located on a computer on the network and assigned a domain name.
- **WWW hay Web:** a service that allows the transfer of hypertext between computers on a network.
- **Trình duyệt (web browser)**: Program to display hypertext: Edge, FireFox, Google Chrome...
- **Hypertext Transfer Protocol (HTTP)**
  - Is a transfer protocol between browser and web server.
- **Uniform Resource Locator (URL)**
  - Is the only address of a document on the web

A typical URL

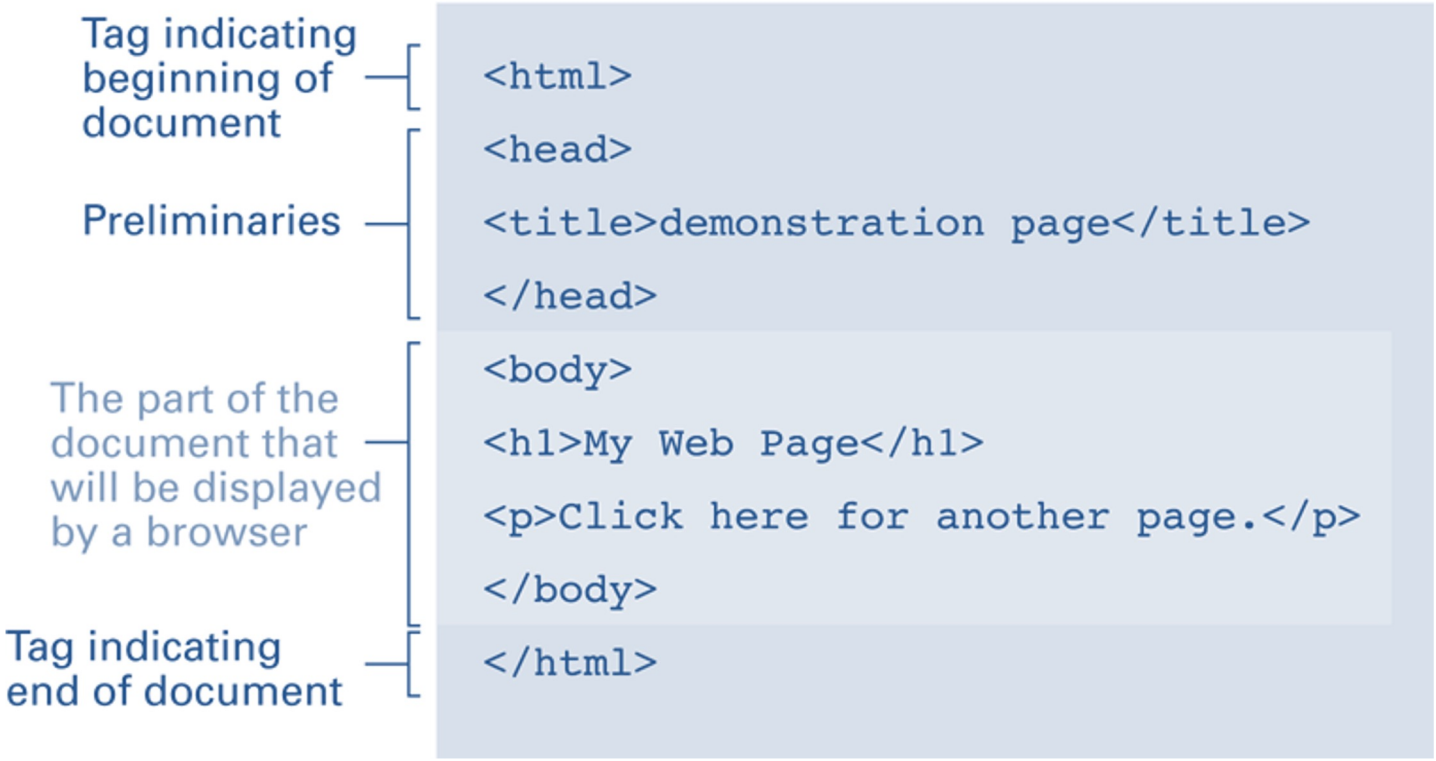


Hypertext Markup Language (HTML)

- Encoded as text file
- Contains tags to communicate with browser
  - Appearance
    - <h1> to start a level one heading
    - <p> to start a new paragraph
  - Links to other documents and content
    - <a href = . . . >
  - Insert images
    - <img src = . . . >

A simple webpage

a. The page encoded using HTML.



A simple webpage

b. The page as it would appear on a computer screen.

Extensible Markup Language (XML)

- XML: A language for constructing markup languages similar to HTML
  - A descendant of SGML
  - Opens door to a World Wide *Semantic* Web

SECURITY

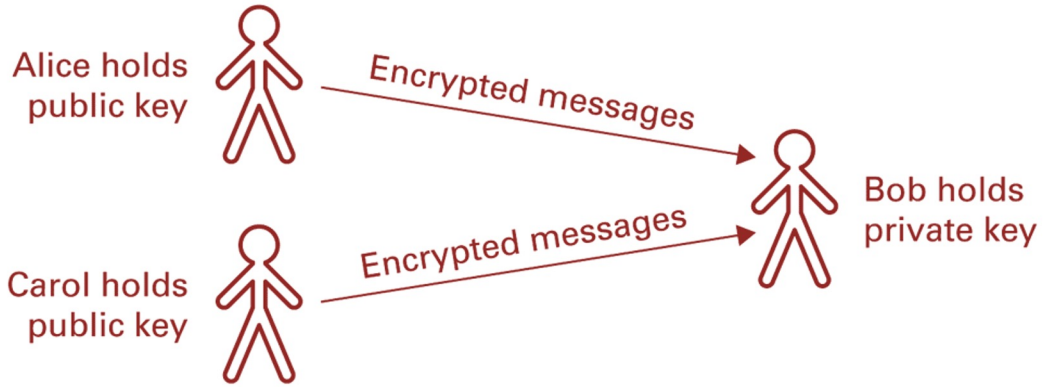
Security

- Attacks
  - Malware (viruses, worms, Trojan horses, spyware, phishing software)
  - Denial of service (DoS)
  - Spam
- Protection
  - Firewalls
  - Spam filters
  - Proxy Servers
  - Antivirus software

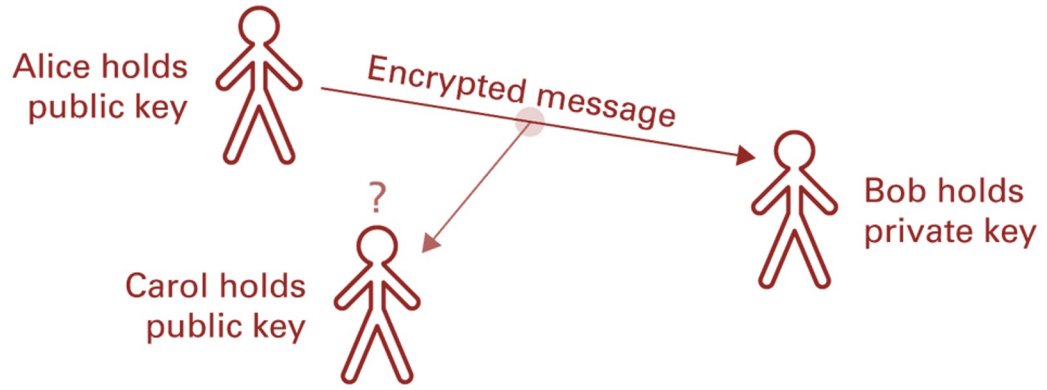
Encryption

- HTTPS and SSL
- Public-key Encryption
  - Public key: Used to encrypt messages
  - Private key: Used to decrypt messages
- Certificates and Digital Signatures
  - Certificate authorities

Public-key encryption



Both Alice and Carol can send encrypted messages to Bob.



Carol cannot decrypt Alice's message even though she knows how Alice encrypted it.

Types of computer crime

- Identify theft—criminal access to personal information in order to impersonate someone
- Dumpster diving—disgruntled employees or thieves go through a company's trash to find information they can steal
- Phishing attacks—legitimate-looking e-mails or Web sites created in an attempt to obtain confidential data about a person
- Spear phishing (similar to phishing)—uses targeted fake e-mails and social engineering to trick recipients into providing personal information to enable identity theft

Types of computer crime

- Malware (short for malicious software)—programs that intentionally harm a computer system or allow individuals to gain access without permission
  - Tips to protect yourself from malware:
    - Know who you are dealing with
    - Keep your Web browser and operating system up to date
    - Back up important files
    - Protect children online
    - Use security software tools and keep them up to date
    - Use strong passwords
    - Learn what to do if something goes wrong

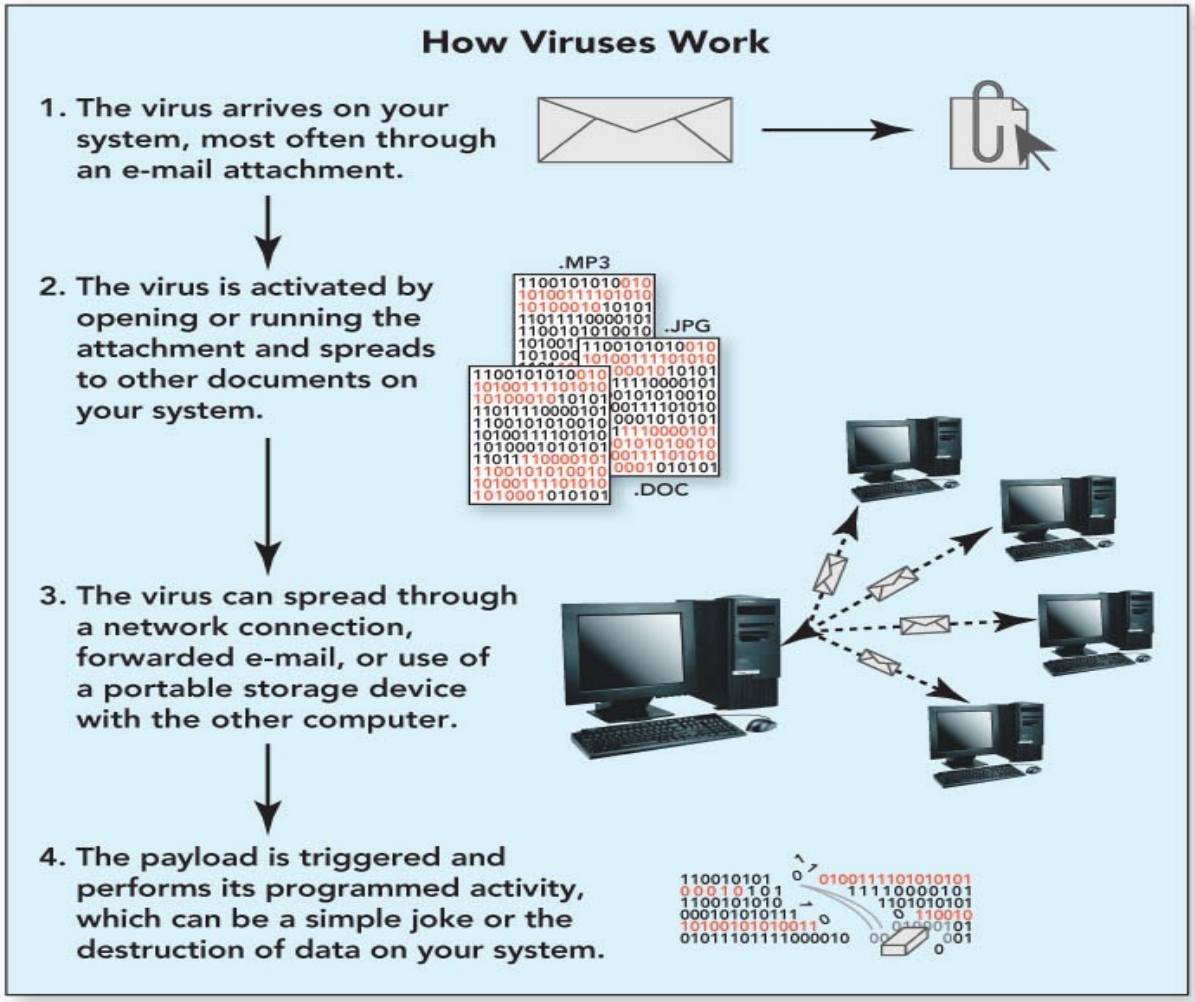
Types of computer crime

- Spyware—software that gathers private information and tracks Web use
  - Adware—form of spyware that generates annoying pop-up and banner ads
  - Keyloggers—record keystrokes to provide cybercriminals with confidential data

Types of computer crime

- Computer virus—code concealed inside a program that can harm or destroy files
  - Many spread through e-mail attachments
  - File infectors—attach themselves to files
  - Payload—refers to the dangerous actions a virus performs.
  - Macro viruses—attach to data files and take advantage of application macros
  - Boot sector viruses—execute each time you start the computer
  - SPIM—spam text message sent via a cell phone or instant messaging service

Computer Crime and Cybercrime



Types of computer crime

- Rogue programs
  - Logic bomb—hidden computer code that sits dormant on a system until triggered
  - Time bomb—virus program that remains dormant on a computer system until activated
  - Worm—similar to a virus but does not need action of a user to execute

Types of computer crime

- Denial of service (DoS) attack—assaults an Internet server with so many requests it can't function
  - Distributed denial of service (DDoS)—attack involves multiple computer systems
    - Commandeered computers form a botnet (robot network)
    - Bot (short for robot)—connects individual computers to the controller, usually a server under the control of the botnet controller
    - The individual computers are called zombies.

Computer Crime and Cybercrime

- More rogue programs (con't.)
  - Syn flooding—form of denial of service attack in which synchronization packets are repeatedly sent to every port on the server
    - Uses up all available network connections
    - Locks them until they time out
  - Rootkit—malicious program that is disguised as a useful program
    - Enables attacker to gain administrator level access
    - Allows attacker to have repeated and undetected access
  - Trojan horse—normal-looking program that includes concealed instructions to cause harm

COMPUTER CRIME

Computer Crime

- cyber crime, e-crime, electronic crime, or hi-tech crime.
- Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information.
- In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Computer crime

- **Child pornography** - Making or distributing child pornography.
- **Copyright violation** - Stealing or using another person's copyrighted material without permission.
- **Cracking** - Breaking or deciphering codes that are being used to protect data.
- **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
- **Cyberbully** or **Cyberstalking** - Harassing or stalking others online.
- **Cybersquatting** - Setting up a domain of another person or company with the sole intentions of selling it to them later at a premium price.
- **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
- **Espionage** - Spying on a person or business.

Computer crime

- Fraud - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- Harvesting - Collect account or other account related information on other people.
- Human trafficking - Participating in the illegal act of buying or selling other humans.
- Identity theft - Pretending to be someone you are not.
- Illegal sales - Buying or selling illicit goods online including drugs, guns, and psychotropic substances.
- Intellectual property theft - Stealing practical or conceptual information developed by another person or company.
- IPR violation - An intellectual property rights violation is any infringement of another's copyright, patent, or trademark.
- Phishing - Deceiving individuals to gain private or personal information about that person.

Computer crime

- **Salami slicing** - Stealing tiny amounts of money from each transaction.
- **Scam** - Tricking people into believing something that is not true.
- Slander - Posting libel or slander against another person or company.
- Software piracy - Copying, distributing, or using software that is copyrighted that you did not purchase.
- Spamming - Distributed unsolicited e-mail to dozens or hundreds of different addresses.
- **Spoofing** - Deceiving a system into thinking you are someone you really are not.
- **Typosquatting** - Setting up a domain that is a misspelling of another domain.
- Unauthorized access - Gaining access to systems you have no permission to access.
- **Wiretapping** - Connecting a device to a phone line to listen to conversations.

Cyberbully

- Alternatively referred to as a cyberstalker, a cyberbully is someone who posts inappropriate or unwanted things about another person, or otherwise harasses them in e-mails, IMs, or SMS.

Spyware

- Spyware or **snoopware**
  - a software program that is intentionally installed on a computer by to monitor what other users of the same computer are doing.
  - a program designed to gather information about a user's activity secretly. Spyware programs are often used to track users' habits to target them with advertisements better.

Computer fraud

- Computer fraud
  - any act using computers, the Internet, Internet devices, and Internet services to defraud people, companies, or government agencies of money, revenue, or Internet access.
  - Illegal computer activities include **phishing**, **social engineering,** viruses, and DDoS attacks are some examples used to disrupt service or gain access to another's funds.

Identity theft

- Identity theft is the act of a person obtaining information illegally about someone else.
- Thieves try to find such information as full name, maiden name, address, date of birth, social security number, passwords, phone number, e-mail, and credit card numbers.
- The thief can then use this information to gain access to bank accounts, e-mail, cell phones, identify themselves as you, or sells your information.

Phishing

- describe a malicious individual or group of individuals who scam users.
- They do so by sending e-mails or creating web pages that are designed to collect an individual's online bank, credit card, or other login information. Because these e-mails and web pages look like legitimate companies users trust them and enter their personal information.

DEPARTMENT OF NETWORKS AND TELECOMMUNICATIONS

Overview

- Since 1998
- Room: I.74
- Tel: (028) 38.324.467 (ext: 711)
- Head: Prof. Tran Trung Dung
- Vice Head: Msc. Huynh Thuy Bao Tran

GOALs

Bachelor in Computer Networks and Telecommunications (CN&T)

- Provide a strong background in computer networking
- This program focuses on providing knowledge and skill regarding to design, implementation, installation, operation and maintenance computer network & telecommunication systems.

GOALs

- Research methodology in CN&T field
- Be able to self learning new technologies as well as applying them in real life problems.
- After graduated, students are able to work in worldwide environment.

Career orientation- Future career

- Computer Systems & Networking administration, Design and consulting of Computer networks & telecommunications systems
- Computer networking programming
- Computer & computer networks securities
- Internet of Things

Required courses

Students accumulate at least 5 courses

STT	MÃ SỐ	TÊN HỌC PHẦN	TC	LT	TH
1	CTT601	Hệ điều hành nâng cao	4	45	30
2	CTT602	Hệ thống viễn thông	4	45	30
3	CTT603	Lập trình mạng	4	45	30
4	CTT604	Mạng máy tính nâng cao	4	45	30
5	CTT605	Thực tập mạng máy tính	4	45	30

Optional courses

Students accumulate at least 5 courses, which contain at least 2 courses (8 credits) of CN&T department

STT	MÃ SỐ	TÊN HỌC PHẦN	TC	LT	TH
11	*CTT124*	*Kiến tập nghề nghiệp*	*2*	*15*	*30*
12	*CTT125*	*Khởi nghiệp*	*3*	*30*	*30*
13	CTT621	An ninh mạng	4	45	30
14	CTT622	An ninh mạng nâng cao	4	45	30
15	CTT623	Chuyên đề Hệ điều hành Linux	4	45	30
16	CTT624	Kiến trúc máy tính nâng cao	4	45	30
17	CTT625	Mạng cảm ứng không dây	4	45	30
18	CTT626	Mô hình hóa và mô phỏng mạng	4	45	30
19	CTT627	Seminar mạng máy tính	4	45	30
20	CTT628	Thiết kế mạng	4	45	30

Optional courses

STT	MÃ SỐ	TÊN HỌC PHẦN	TC	LT	TH
21	CTT629	Thực tập hệ điều hành mạng	4	45	30
22	CTT630	Thực tập hệ thống viễn thông	4	45	30
23	CTT631	Truyền thông không dây	4	45	30
24	CTT631	Truyền thông kỹ thuật quang	4	45	30
25	CTT633	Truyền thông kỹ thuật số	4	45	30
26	CTT634	Xử lý và tính toán song song	4	45	30

Courses & Career orientation

Mã MH	Tên môn học	Môn học trước	QTM	TKM	Tư vấn	PMM	NC & GD
CTT601	Hệ điều hành nâng cao	HĐH		*	*		*
CTT602	Hệ thống viễn thông	MMT	*	*	**	*	**
CTT603	Lập trình mạng	HĐH	*	*	*	**	**
CTT604	Mạng máy tính nâng cao	HĐH	**	*	**	**	**
CTT605	Thực tập mạng máy tính	MMT nâng cao	**	*	**	*	**
CTT621	An ninh mạng	MMT nâng cao	**	*	*		*
CTT622	An ninh mạng nâng cao	An ninh mạng	**	*	*		*
CTT623	CĐề Hệ điều hành Linux	HĐH, MMT	**		*	*	*
CTT624	Kiến trúc MT nâng cao	KTMT và h.ngữ			**		*
CTT625	Mạng cảm ứng không dây	MMT		*	*		*

Courses & Career orientation

Mã MH	Tên môn học	Môn học trước	QTM	TKM	Tư vấn	PMM	NC & GD
CTT625	Mạng cảm ứng không dây	MMT		*	*		*
CTT626	Mô hình hóa và mô phỏng mạng	XS thống kê B, MMT NC		*	*		**
CTT627	Seminar mạng máy tính	MMT nâng cao	*	*	*	*	*
CTT628	Thiết kế mạng	MMT nâng cao	*	**	*		*
CTT629	Thực tập HĐH mạng	HĐH	**	*	*	*	*
CTT630	Thực tập HT viễn thông	HĐH, HT VT	**				*
CTT631	Truyền thông không dây	MMT	**	*	*	*	*
CTT632	Tr.thông kỹ thuật quang	MMT	*		**		*
CTT633	Truyền thông kỹ thuật số	MMT	*	*	**		*
CTT634	Xử lý và tính toán s.song	MMT			*	**	*

Q&A