Networking and the Internet

Introduction to Computer

Yu-Ting Wu

(with some slides borrowed from Prof. Tian-Li Yu)

1

Outline

- Network fundamentals
- The Internet
- The World Wide Web
- Internet protocols
- Security

2

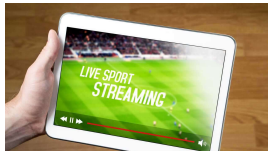
Outline

- Network fundamentals
- The Internet
- The World Wide Web
- Internet protocols
- Security

3

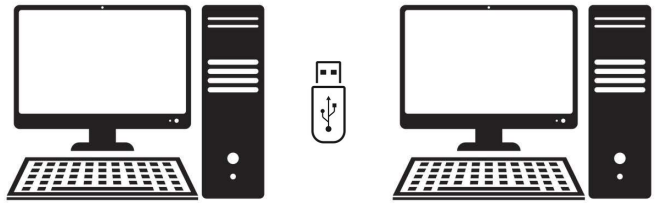
Network Fundamentals

- Network software allows users to exchange information and share resources
  - Content
  - Software
  - Data storage facilities



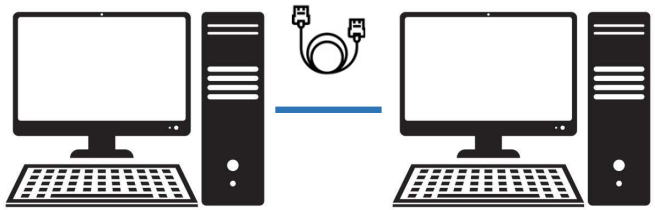
4

Network Classifications



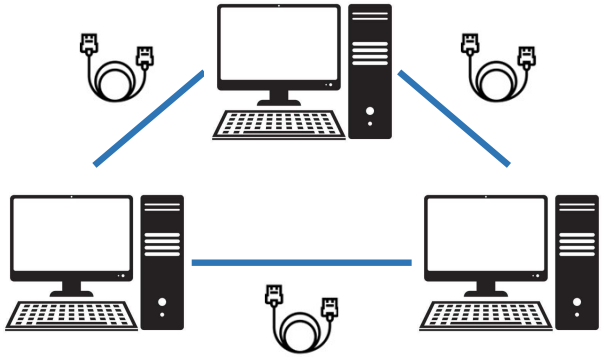
5

Network Classifications (cont.)



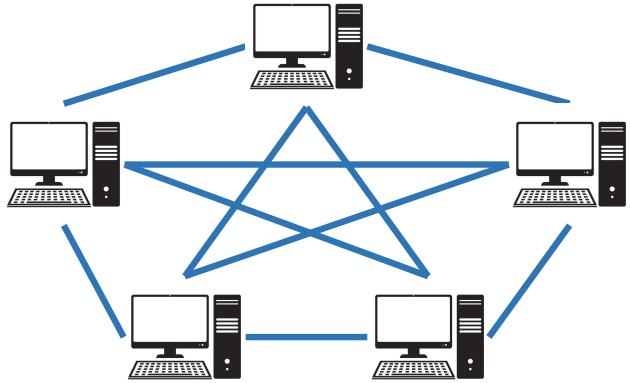
6

Network Classifications (cont.)



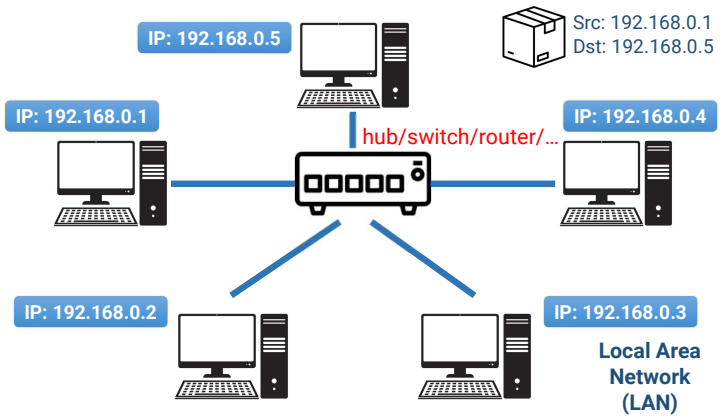
7

Network Classifications (cont.)



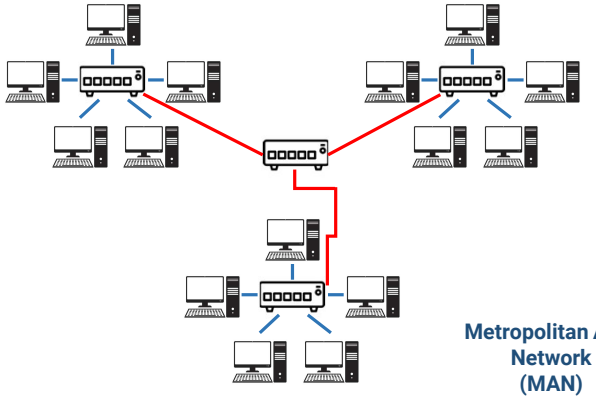
8

Network Classifications (cont.)



Local Area Network (LAN)

Network Classifications (cont.)



Metropolitan Area Network (MAN)

Network Classifications (cont.)

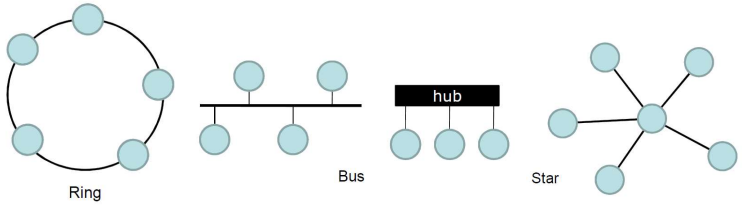
Wide Area Network (WAN)

Network Classifications (cont.)

- **Scope**
  - Local Area Network (LAN)
    - Building / Campus
  - Metropolitan Area Network (MAN)
    - Community
  - Wide Area Network (WAN)
    - Greater distances
- **Ownership**
  - Closed v.s. Open

Network Classifications

- **Topology (configuration)**
  - Ring
  - Bus (e.g., Ethernet)
  - Star (e.g., wireless networks with central Access Point)

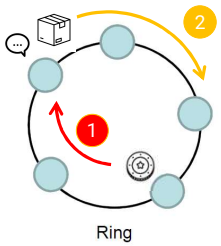


Protocols

- **Rules** by which activities are conducted on a network
- Coordinate the transmission of messages between computers
  - Need to avoid all machines transmitting at the same time
- Allows vendors to build products that are compatible with products from other vendors

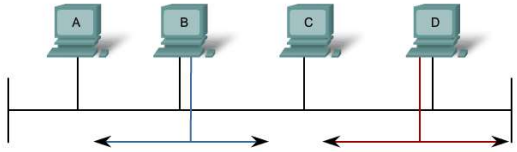
Protocols for Transmitting Messages

- **Token ring**
  - Popular in the ring topology
  - A token (special symbol) and messages are passed in **one direction**
  - Only the machine that gets the token can transmit its own message



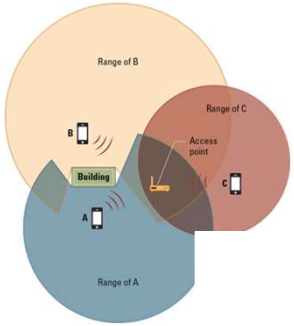
Protocols for Transmitting Messages (cont.)

- **CSMA/CD** (carrier sense, multiple access with collision detection)
  - Popular in the **bus topology (wired Ethernet)**
  - Broadcasting
  - When a collision occurs, both machines stop and wait for an **independent, random time** before trying again



Protocols for Transmitting Messages (cont.)

- Wireless and Access Point (AP)
  - Wi-Fi (wireless fidelity)
  - IEEE 802.11 (b, g, l, n, ac, …)



None of the end systems can hear each other, but each can communicate with the **AP**

17

Protocols for Transmitting Messages (cont.)

- **CSMA/CA** (carrier sense, multiple access with collision avoidance)
  - Popular in **wireless Ethernet**, where not all machines can hear each other (hidden terminal problem)
  - Broadcasting
  - Detect if a channel is idle, if so, **wait for a brief random time and then detect again**. If the channel is still idle, start sending

18

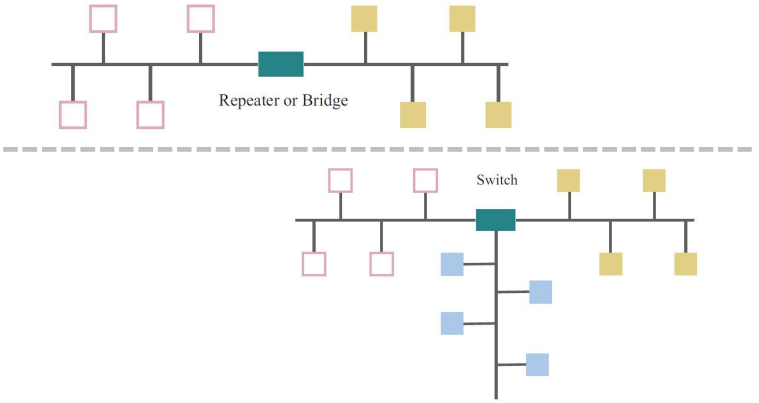
Combining Compatible Networks

- Compatible means using the **same protocol**
  - No need to translate messages

- **Repeater** 
  - Simply pass all messages across two networks (buses)
- **Bridge** 
  - Only pass the messages that are destined for computers on the other network (bus)
- **Switch** 
  - Act like a bridge, but with connections to multiple networks (buses)

19

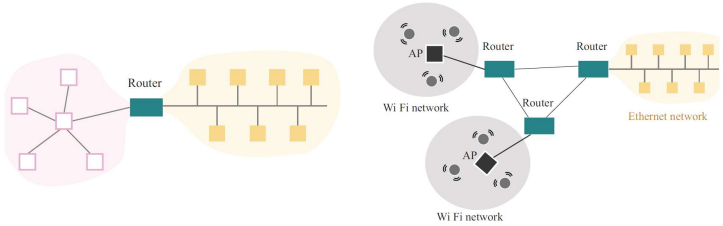
Repeater, Bridge, and Switch



20

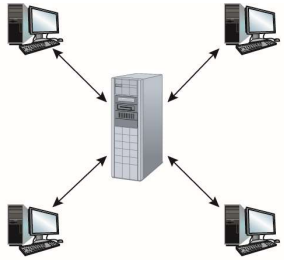
Combining Incompatible Networks

- **Router**
  - Connects two **incompatible** networks resulting in a network of networks known as an **internet**
  - Need to translate between different protocols
  - Most come with **firewall** management



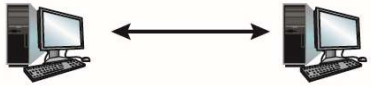
Methods of Process Communication

- **Client-server**
  - Many clients, one server (executing continuously)
  - Clients initiate communications by sending requests
  - Server satisfies requests made by clients



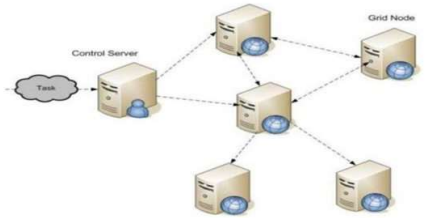
Methods of Process Communication (cont.)

- **Peer-to-peer (P2P)**
  - Two processes communicating as equals
  - The most popular distribution mode nowadays



Distributed Systems

- Systems units that execute processes on **different computers**
  - Cluster computing
    - Independent computers work closely together instead of a single, much larger machine



Outline

- Network fundamentals
- The Internet
- The World Wide Web
- Internet protocols
- Security

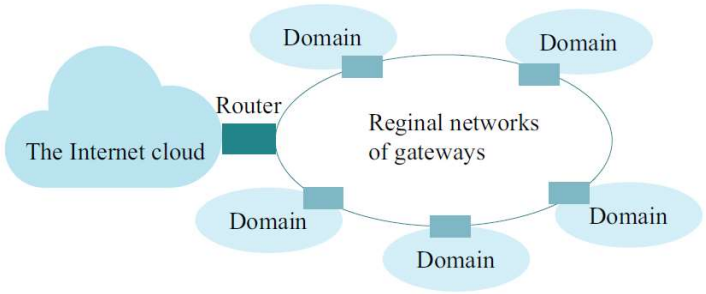
The Internet

- The **Internet** is an internet that spans the world
- Original goal was to link a variety of networks into a connected system unaffected by local disasters
  - Deviated from the advanced research projects agency network (ARPANet) around 1960
  - Only 4 nodes: UCLA, SRI, UCSB, UTAH
- Today, it is a commercial undertaking that links a worldwide combination of LANs, MANs, and WANs involving millions of computers

Internet Architecture

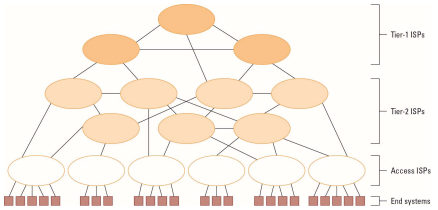
- **Domain**
  - A network or an internet controlled by one single authority
- **ICANN** (Internet corporation for assigned names and numbers)
  - Allocate blocks of IP addresses to ISPs who then assign those addresses within their regions
  - Oversee the registration of domains
- **Gateway**
  - A router that connects a domain to the rest of the Internet (the Internet cloud)

Internet Architecture (cont.)



Internet Architecture (cont.)

- **Internet Service Provider (ISP)**
  - Allow customers to connect their domain to the ISP's equipment or join the domain already established by the ISP
  - Tier-1 (Internet backbone)
  - Tier-2
  - Access or Tier-3 ISP: provides connectivity to the Internet



29

Internet Addressing

- **IP (Internet protocol) address**
  - 32 bits in IPv4
    - Network identifier (by ICANN)
    - Host address (domain administrator)

8 bit 8 bit 8 bit 8 bit (0 ~ 255)

nptu 120.126.55.66

nctu 140.113.95.88

dorm#9 my host

can host 2^{32} = 4,294,967,295 different addresses

  - 128 bits in IPv6

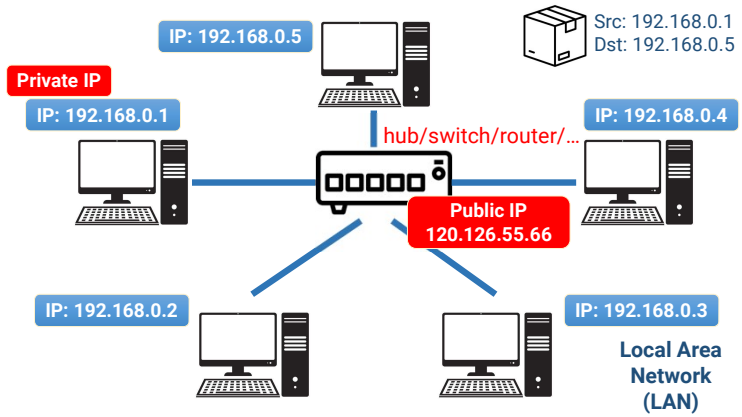
4 * 4 = 16 bit

3FFE:D110:0234:AB03:0123:5566:7788:ABAB

can host 2^{128} = 3.4028237e+38 different addresses

30

Private and Public IP



31

Host Names

- Mnemonic address made up of two parts
  - **Domain names**
    - Assigned by a registrar
    - Example: edu.tw
    - Top-Level domain
      - By usage: .edu = education; .tw = Taiwan
  - **Subdomains and individual host names**
    - Assigned by the domain owner
    - www.csie.ntpu.edu.tw
- Name server and domain name server (DNS)
  - www.csie.ntpu.edu.tw ➔ 120.126.153.1

32

Early Internet Applications

- Electronic Mail (email)
- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Telnet and Secure Shell (SSH)
- Voice over IP (VoIP)
- P2P
- Internet Multimedia Streaming

Outline

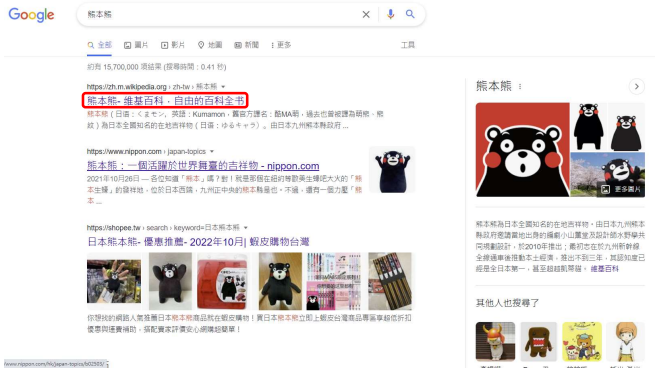
- Network fundamentals
- The Internet
- The World Wide Web
- Internet protocols
- Security

World Wide Web

- **Also called www, w3, web**
- **Hypertext** combines internet technology with the concept of linked-documents
  - **Web page** is a hypertext document
  - **Website** is a collection of closely related web pages
  - Embeds **hyperlinks** to other documents
  - May contain **hypermedia**
- Webservers provide access to documents
  - Documents are identified by **URLs** and transferred using HTTP
- Browsers present materials to the user

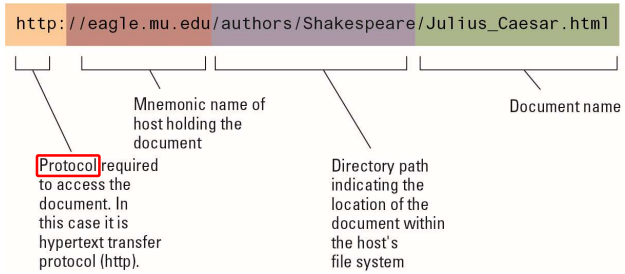
World Wide Web (cont.)

- **Hyperlinks**



Browsers

- Present the web pages downloaded from the Internet
- **HTTP** (hypertext transfer **protocol**)
- **URL** (uniform resource locator)



Hypertext Markup Language (HTML)

- Encoded as **text files**
- Contains **tags** to communicate with browsers
  - 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 = . . . >
- Try it!
  https://www.w3schools.com/html/html_examples.asp

Extensible Markup Languages (XML)

- A language for constructing markup languages similar to HTML
  - Standard style to represent data as text
  - **Restricted** mapping of each opening to each ending
    - <x property="yyy" … </x>

- XHTML
  - HTML that follows XML format

Client Side v.s. Server Side

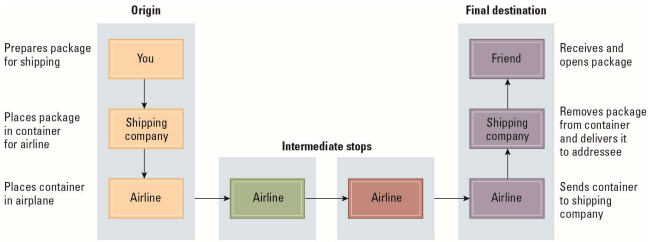
- **Client-side activities (browser)**
  - Macromedia Flash
  - Java applets
  - JavaScript
  - WebGL
- **Server-side activities (webserver)**
  - Common Gateway Interface (CGI)
  - Servlets (JSP, ASP)
  - PHP
- **Hybrid**
  - Online games

Outline

- Network fundamentals
- The Internet
- The World Wide Web
- Internet protocols
- Security

Internet Protocols

- Control how messages are transferred over the Internet
- This software must reside on every computer on the Internet
- Accomplished by a multi-level hierarchy

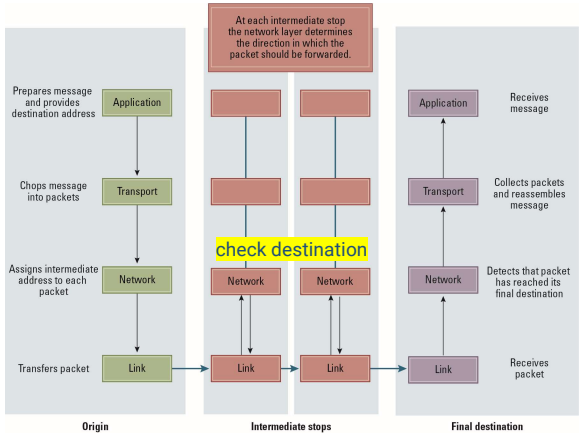


Internet Software Layers

- **4-layer model**
  - **Application:** constructs message with the address
  - **Transport:** chops message into packets
  - **Network:** handles routing through the Internet
  - **Link:** handles actual transmission of packets
- Can be further divided to OSI 7-layer model

- **Port** (not the I/O port)
  - Incoming messages are delivered to different applications by unique port numbers
  - Some typical ports: ftp (21), telnet (23), ssh (22), http (80)

Internet Software Layers (cont.)



TCP/IP Protocol Suite

- Transport Layer
  - **Transmission Control Protocol (TCP)**
    - Reliable transmission (handshaking, retransmission)
  - **User Datagram Protocol (UDP)**
    - No notification before sending messages
    - No retransmission services
    - No acknowledgment of receiving messages
- Network Layer
  - Routing based on Internet Protocol (IP)
    - IPv4
    - IPv6

45

Outline

- Network fundamentals
- The Internet
- The World Wide Web
- Internet protocols
- Security

46

Security

- Forms of Attack
  - Malware (malicious software)
    - Viruses, worms, Trojan horses, spyware, phishing software
  - Denial of service (DoS)
  - Spam (common medium for delivering malware)
- Protection and Cures
  - Firewalls
  - Spam filters
  - Proxy servers (e.g., VPN)
  - Antivirus software

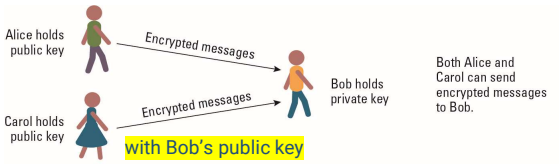
47

Cryptography

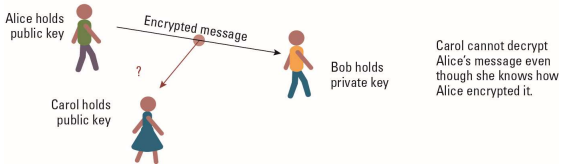
- Sending secret messages
  - Sender encrypts messages with the receiver's **public key**
  - Receiver decrypts messages with its **private key**
  - The public key and the private key are **inverse functions** of each other
- Applications with improved security
  - **https** for secure Internet access
  - sftp (or ftps)
  - ssh

48

Public / Private Key



Use the **public key to encrypt**; the **private key to decrypt**



Authentication

- Make sure the author of a message is, in fact, the party it claims to be
- Use the **private key to encrypt**; the **public key to decrypt**

- **Certificate Authorities (CA)**
  - Ensure the public key is given by the trusted one
  - Provide **Certificates** to clients containing a party's name and its public key

Any Questions?