Introduction to Computer Science
Lecture 4: Networking and the Internet

Tian-Li Yu

Taiwan Evolutionary Intelligence Laboratory (TEIL)
Department of Electrical Engineering
National Taiwan University

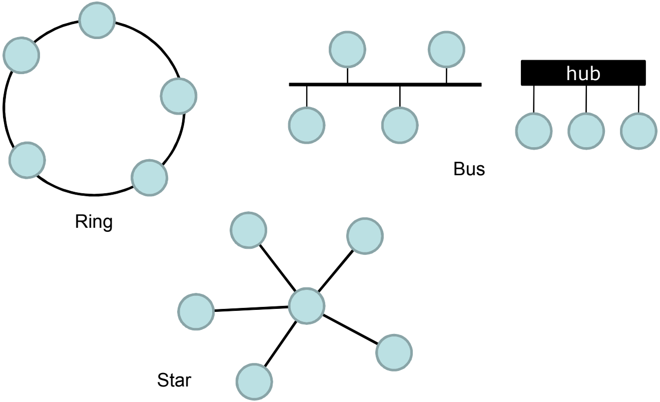
tianliyu@cc.ee.ntu.edu.tw

Slides made by Tian-Li Yu, Jie-Wei Wu, and Chu-Yu Hsu

Network Classifications

- Scope
  - LAN: local area network
  - MAN: metropolitan area network
  - WAN: wide area network
- Ownership
  - Closed
  - Open
- Topology

Network Topology



Protocols

- Token ring
  - Popular in ring topology.
  - Token and messages are passed in one direction.
  - Only the machine that gets the token can transmit its own message.
- CSMA/CD (carrier sense, multiple access with collision detection)
  - Popular in bus topology (wired Ethernet).
  - Broadcasting.
  - When collision, both machines wait for a brief random time before trying again.
- CSMA/CA (carrier sense, multiple access with collision avoidance)
  - Popular in wireless Ethernet.
  - 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.

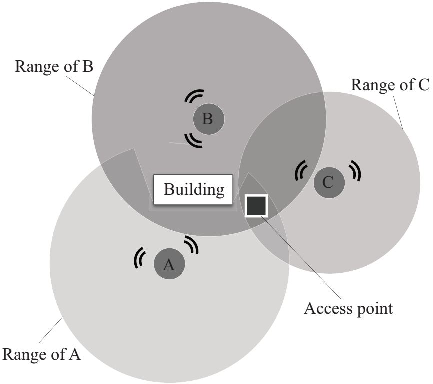
Dilbert on Token Ring

HERE'S YOUR PROBLEM. THE CONNECTION TO THE NETWORK IS BROKEN.
UH-OH. IT'S A "TOKEN RING" LAN. THAT MEANS THE TOKEN FELL OUT AND IT'S IN THIS ROOM SOMEPLACE.
YOU ARE THE WIND BENEATH MY WINGS.
I'LL WAIT A WEEK THEN TELL HIM THE TOKEN MUST BE IN THE "ETHERNET."
S. Adams
E-mail: SCOTTADAMS@AOL.COM
© 1996 United Feature Syndicate, Inc.(NYC)

Dilbert, Scott Adams

Wireless & Access Point

- Wi-Fi (wireless fidelity)
- IEEE 802.11 (b, g, i, n, ac, ...)

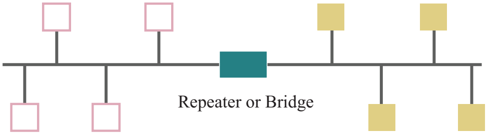


None of the end systems can hear each other but each can communicate with the AP

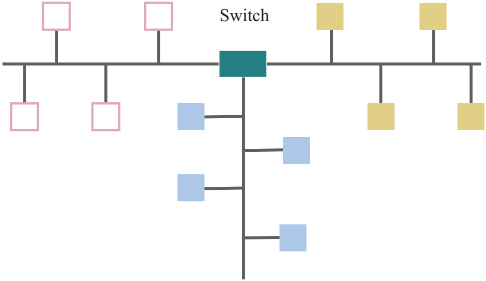
Connecting Compatible Networks

- Repeater
  - Simply passing through messages.
  - Connecting two compatible networks.
- Bridge
  - Only passing those messages addressed to the other side.
  - Connecting two compatible networks more efficiently.
- Switch
  - A bridge with multiple connections
  - Connecting several compatible networks more efficiently.

Repeater, Bridge, and Switch



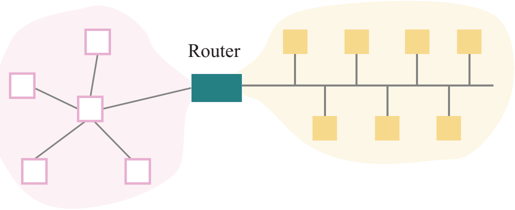
(a) A repeater or bridge connecting one bus.

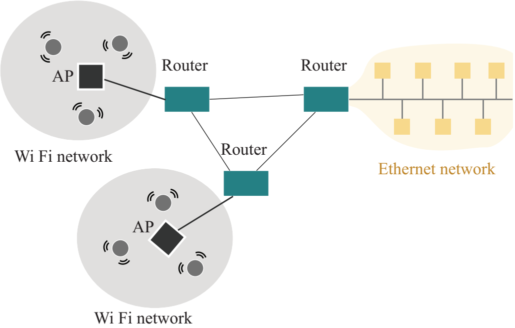


(b) A switch connecting multi bus.

Connecting Incompatible Networks

- Router
  - Building a network of networks, known as an internet.
  - Most come with firewall management.

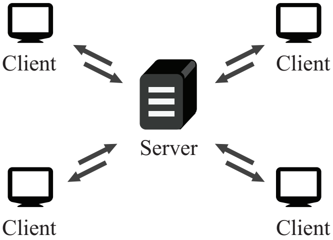




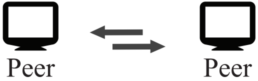
Interprocess Communication

- Server-client
  - One server, several clients.
  - Clients initiate communications by sending requests.
  - Server serves.
- P2P (peer-to-peer)
  - Two processes communicating as equals.
  - The most popular distribution mode nowadays.

Interprocess Communication (contd.)



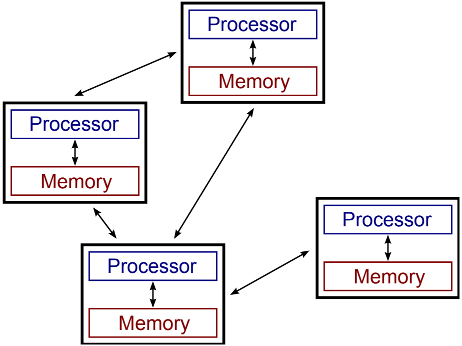
Server must be prepared to serve multiple clients at any time.



Peers communicate as equals on a one-to-one basis.

Distributed Systems

- Infrastructure can be provided by standardized toolkits.
  - Enterprise Java Beans by Sun Microsytems
  - .NET framework by Microsoft



The Internet

- The most notable example of an internet is the Internet.
- Original goal was to prevent disruptions caused by local disaster.
  - Deviated from the advanced research projects agency network (ARPANet) around 1960.
  - 4 nodes — UCLA, SRI, UCSB, UTAH,
- Now it‘s a commercial undertaking.

Left to right: Vinton Cerf, Robert Kahn, and US President George Bush
White House, Wednesday, Nov. 9, 2005

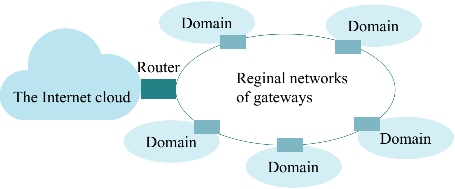
Internet Architecture

- Domain
  - a network or an internet controlled by one single authority.
- ICANN (Internet corporation for assigned names and numbers)
  - Oversee the registration of domains.
  - Registrar
- Gateway
  - A router that connects a domain to the rest of the Internet (the Internet cloud).

Internet Composition

- 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
  - Tier-2
  - Access ISP: Provides connectivity to the Internet
    - Traditional telephone (dial-up connection)
    - Cable connections
    - DSL
    - Wireless

Domains, Gateway, and the Internet



Domain

Domain

Router

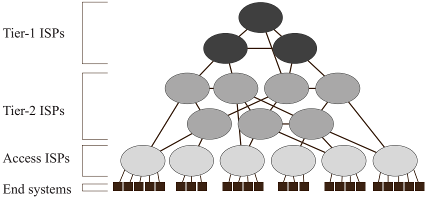
The Internet cloud

Reginal networks of gateways

Domain

Domain

Domain



Tier-1 ISPs

Tier-2 ISPs

Access ISPs

End systems

IP Addresses

- IP (Internet protocol) addresses
  - 32 bits in IPv4 (all are allocated in Feb. 2011)
  - 128 bits in IPv6
- Network identifier (by ICANN)
- Host address (domain administrator)
- Dotted decimal
  - 140.112.18.33

Host Names

- Mnemonic address made up of two parts
- Domain name
    - Assigned by a registrar
    - edu.tw
    - Top-level domain
        - By usage: .edu = education
        - .tw = Taiwan
- Subdomains and individual host names
    - Assigned by domain owner
    - <u>www.ee.ntu</u>.edu.tw
- Name server & domain name server (DNS)
    - www.ee.ntu.edu.tw → 140.112.18.33

Internet Applications

- VoIP (voice over Internet protocol)
- email (electronic mail)
- FTP (file transfer protocol)
- telnet & ssh (secure shell)
- P2P: bittorrent, edonkey, emule...

World Wide Web

- www, w3, web
- hypertext, hyperlink, hypermedia.
- Web page: hypertext document
- Website: a collection of closely related web pages.

Browsers

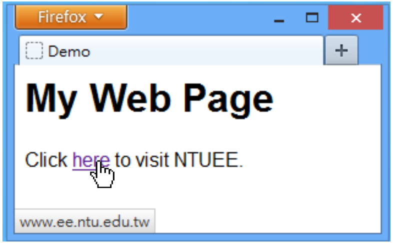
- Presenting the web pages downloaded from the Internet.
- HTTP (hypertext transfer protocol)
- URL (uniform resource locator)

(1) (2) (3) (4)

http://www.ee.ntu.edu.tw/hischool/excellence.html

1. Protocol required to access the document. Here it is hypertext transfer protocol (http).
2. Mnemonic name of host holding the document.
3. Directory path indicating the location of the document within the host's file system.
4. Document name

Hyper-Text Markup Language



My Web Page

Click here to visit NTUEE.

www.ee.ntu.edu.tw

HTML Code

```
<html>
<head>
  <title>Demo</title>
</head>
<h1>My Web Page</h1>
<p>
  Click <a href="http://www.ee.ntu.edu.tw">here</a>
to visit NTUEE.
</p>
</html>
```

eXtensible Markup Language

- XML
- Standard style to represent data as text.
- Restricted mapping each opening to each ending.
- <x property=”yyy”> ...... </x>
- XHTML
    - HTML that follows XML format.

```
<name code=”ISO-8859-1”> Tian-Li Yu </name>
<education>
<BS> NTUEE, 1997</BS>
<MS> UIUCCS, 2003 </MS>
<PhD> UIUCCS, 2006 </PhD>
</education>
```

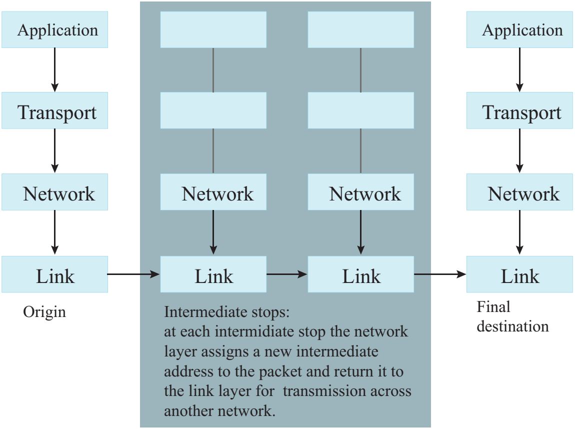
Client-side & Server-side

- Client-side
  - Java applets
  - Javascripts
  - Flash
- Server-side
  - CGI
  - Servlets (jsp, asp)
  - PHP (Personal Home Page, PHP Hypertext Processor)

Internet Protocol

- Layers
  - Application: constructs message with address
  - Transport: chops message into packets
  - Network: handles routing through the Internet
  - Link: handles actual transmission of packets
- For OSI 7-layer model, check out `http://en.wikipedia.org/wiki/OSI_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), etc.

Layers



Prepares messages and attaches destination address.

Chops messages into packages.

Assigns intermediate address to each packet.

Transfers packet to its intermediate address.

Origin

Intermediate stops:
at each intermidiate stop the network layer assigns a new intermediate address to the packet and return it to the link layer for transmission across another network.

Final destination

Recives message

Collects packages and reassembles message

Detects that package has reached its final destination.

Receives package

TCP/IP Suite

- Transport Layer
  - TCP (transmission control protocol)
  - UDP (user datagram protocol)
    - No notification before sending message, no retransmission service, no acknowledge of receiving message.
- Network Layer
  - routing based on IP (IPv4 and IPv6)

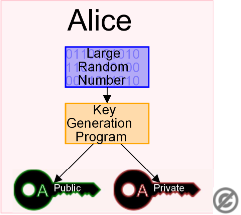
- TCP and IP are two protocols, TCP/IP refers to a collection of protocols more than just TCP and IP.
  - TCP: more reliable, less efficient
  - UDP: more efficient, less reliable

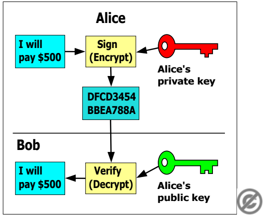
Security

- Attacks
  - Malware (malicious software)
    - Virus, worm, Trojan horse, spyware, phishing
  - Denial of service (DoS)
  - Spam
- Protections
  - Firewall
  - Spam filter
  - Proxy
  - Antivirus, antispyware

Public/Private keys

- SSL (secure socket layer).
- sftp (ftps as in the textbook), https, ssh,
- Sending secret message:
  - Sender encrypt m with the receiver's public key $\rightarrow s$.
  - Receiver decrypt message s with its private key.





Public/Private Key Issues

- Authentication
  - Make sure the author of a message is, in fact, the party it claims to be.
  - Use private key to encrypt; public key to decrypt.
- Certificate authority (CA)
  - Ensure the public key is given by the trusted one.

RSA

- 1977, 1978
- Ron Rivest, Adi Shamir, Leonard Adleman in MIT.
- Security greatly depends on integer factoring.
- Currently no known polynomial-time algorithm exists (only sub-exponential).

RSA Key Generation

- Choose 2 big distinct primes: p and q.
- Let $N = pq$.
- Compute $\phi = (p-1)(q-1)$.
  - There are ϕ integers $\leq N$ that are co-prime with N.
- Choose an integer e that is co-prime with ϕ.
- Compute d such that $d \times e \equiv 1 \pmod{\phi}$.
- Destroy to record of p and q.

- (N, e) is the public key (everyone can get it).
- (N, d) is the private key (only the owner has it).

Encryption

- Bob wants to send a message m to Alice.
    - $\gcd(m, p) = 1 \qquad \gcd(m, q) = 1$
    - What if not? Prob. same as guessing p, q right.
- He gets Alice's public key (N, e).
- He then computes

$$m^e \equiv s \pmod{N}$$

and then send s to Alice.

Decryption

- Alice got s from Bob. She has her own private key (N, d).
- She then computes

$$s^d \equiv m \pmod{N}$$

and got the message back.

Why?

$$s^d \equiv (m^e)^d \pmod{N} \equiv m^{ed} \pmod{N}$$

Fermat's little theorem

$a^p \equiv a \pmod{p}$. If a co-primes p, $a^{p-1} \equiv 1 \pmod{p}$

$$ed \equiv 1 \pmod{p-1} \Rightarrow \text{Let } ed = k(p-1)+1.$$

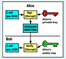
$$m^{ed} \equiv m \cdot \left(m^{p-1}\right)^k \pmod{p} \equiv m \pmod{p}$$

$$\text{Similarly, } m^{ed} \equiv m \pmod{q}$$

By **Chinese remainder theorem**,

$$m^{ed} \equiv m \pmod{pq}$$
$$s^d \equiv m \pmod{N}$$

License

Page	File	Licensing	Source/ author
5	HERE'S YOUR PROBLEM. THE CONNECTION TO THE NETWORK IS BROKEN. UH-OH. IT'S A "TOKEN RING" LAN. THAT MEANS THE TOKEN FELL OUT AND IT'S IN THIS ROOM SOMEPLACE. YOU ARE THE WIND BENEATH MY WINGS I'LL WAIT A WEEK THEN TELL HIM THE TOKEN MUST BE IN THE "ETHERNET." Dilbert, Scott Adams	📖	"Dilbert".,Author:Scott Adams, May 2, 1996 Source: http://dilbert.com/strips/comic/1996-05-02/, Date:2013/03/06, Fair use under copyright law 46,52,65.
13		🅮	"Cerf Kahn Medal Of Freedom".,Author:Paul Morse, Nov 9, 2005 Source: http://en.wikipedia.org/wiki/File:CerfKahnMedalOfFreedom.jpg, Date:2013/05/14, The image is in the public domain.
29	Alice Large Random Number Key Generation Program Public Private	🅮	"Public-key-crypto".,Author:KohanX, Sep 7, 2009 Source: http://en.wikipedia.org/wiki/File:Public-key-crypto-1.svg, Date:2013/05/14, The image is in the public domain.
29	 Alice I will pay $500 Sign (Encrypt) Alice's private key DFCD3454 BBEA788A Bob I will pay $500 Verify (Decrypt) Alice's public key	🅮	"Public key encryption".,Author:David Gthberg, Sep 7, 2009 Source: http://commons.wikimedia.org/wiki/File:Public_key_encryption.svg, Date:2013/05/14, The image is in the public domain.