

Internet Technology

Chanankorn Jandaeng, Ph.D.
School of Informatics, WU

Course name. ICT60-231

Internet Technology

Credit 3 (2-2-5)

Course description

Layer architecture concept based on OSI model and TCP/IP model; introduction to computer communication; applications of internet technology; protocol in application layer; reliable communication; basic of network programming; security awareness in computer network communication.

Aims

- To understand in Layer architecture concept and computer communication, applications of internet technology and its protocol including reliable communication.
- To understand network communication mechanism in protocol level.
- To aware the security issues in computer communication
- Can setup and maintenance network applications or services
- Can implement network programming with any computer languages

Outlines

	Lecture	Workshop
1	Introduction to Computer Network	Linux Server Installation
2	Network Architecture	Network Configuration + DHCP
3	Data Communication	PC Router
4	Layer Architecture : OSI, TCP/IP, DoD model	Micro-service with docker
5	Network Access and Inter-networking	Docker-swarm
6	Web Technology	Web Server with Docker
7	HTTP Protocol	HTTP Protocol Analysis
8	Domain Name System	Design and Implement DNS
9	Reliable Protocol	TCP & UDP Protocol Analysis
10	Network Programming	Implement Socket Programming
11	Protocol Weakness	Protocol Weakness Analysis
12	Secured Protocol and Protection Mechanism	Implementation Secured Service

Grade Policy

Activities	%
Class Attendance	5
Online Quiz	30
Quiz (2 x 5%)	10
Midterm Examination (individual)	20
Final Examination (individual)	20
Workshop Examination (individual)	15
Total	100

Book and Reference

- Jerry Fitzgerald, Alan Dennis, Alexandra Durcikova. (2011). Business Data Communications and Networking. John Wiley & Sons. 11th edition. (E-book)
- Todd Lammle. (2012). CCNA Routing and Switching Study Guide. John Wiley & Sons. 11th edition. (E-book)
- ภัทรลินี ภัทรโกศล. (2555). เครือข่ายคอมพิวเตอร์. พิมพ์ครั้งที่ 1. กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.
- เอกลีทธ์ วิริยะjarie. (2548). เรียนรู้ระบบเน็ตเวิร์กจากอุปกรณ์ของ CISCO ภาคปฏิบัติ. พิมพ์ครั้งที่ 1. กรุงเทพฯ : ชีเอ็ดดี้เคชั่น.
- เอกสารประกอบการบรรยาย และ ปฏิบัติการ

Notes

Module 1

Introduction to Computer Network

Data Communication

Data communications (DC) is the **process** of using computing and communication technologies to **transfer data** from one place to another, and vice versa.

It enables the movement of **electronic** or **digital data** between two or more nodes, regardless of geographical location, technological medium or data contents.

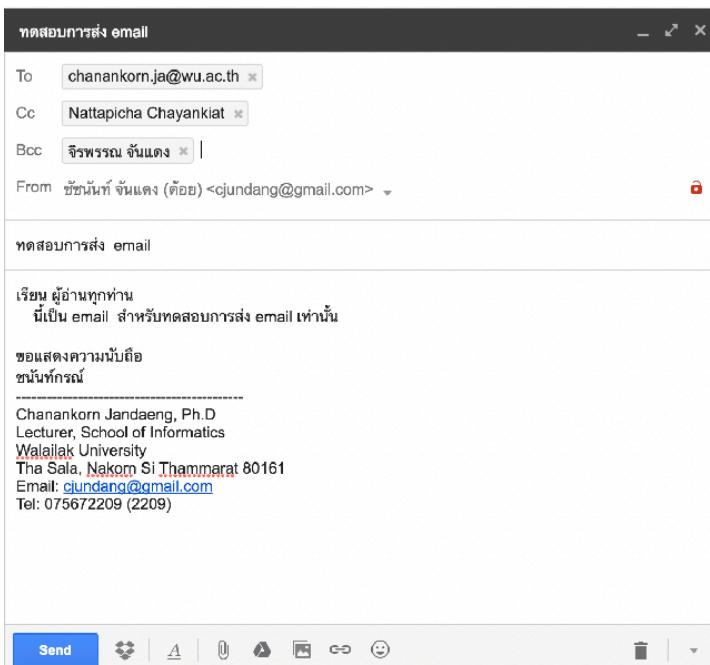
- **การสื่อสาร (communication)** หมายถึงกระบวนการที่ยินยอม ให้ข้อมูลสารสนเทศถูกส่งจาก ตำแหน่งไปยังอีกตำแหน่งหนึ่ง หรือจากผู้ส่งไปยังผู้รับสาร
- **การสื่อสารทางไกล (telecommunication)** หมายถึง การสื่อสารที่มีการส่งข้อมูลสารสนเทศ จาก ตำแหน่งไปยังอีกตำแหน่งที่อยู่ไกลกันมากด้วยการ ใช้กระเพลไฟฟ้า หรือ คลื่นแม่เหล็กไฟฟ้า ใน อุตสาหกรรม เช่น โทรทัศน์ วิทยุ โทรศัพท์ คอมพิวเตอร์ เป็นต้น

Contents

- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology

Applications

Email



- จดหมายอิเล็กทรอนิกส์ (electronic mail) หรือ อีเมล์ (email) เป็นบริการที่รับส่ง จดหมายซึ่งจัดเก็บ ในรูปแบบของอิเล็กทรอนิกซ์ อาจจะเป็นข้อความอย่างเดียว หรืออาจจะ ครอบคลุมไปถึง การส่ง ข้อมูลภาพ (image) เสียง (voice) หรือข้อมูลมัลติมีเดียอื่นๆ ไปยัง ผู้รับจดหมาย ซึ่งข้อมูลที่อยู่ ในรูป แบบเหล่านี้ จะถูกแนบ (attach) ไปพร้อมกับเอกสาร โดยระบุชื่อหัวเรื่อง (subject) และ กำหนดชื่อ ผู้รับ (receive)
- นอกจากนี้ ในข้อมูลข่าวสาร ชุดเดียวกันยังสามารถ สำเนาไปยังผู้รับคนอื่น (carbon copy หรือ cc) โดยที่ผู้รับหลักจะทราบว่า จดหมายฉบับ นี้ถูกส่งถึง ใคร อีกทั้งยังสามารถซ่อนชื่อ ผู้รับ (blind carbon copy หรือ bcc) ได้อีกด้วย การรับส่งอีเมล์อาจจะ ใช้ โปรแกรม ในกลุ่มของ mail client ได้แก่ Mail, Thunderbird หรือ Outlook เป็นต้น หรือรับส่งอีเมล์ผ่าน เว็บไซต์โดยผู้ให้บริการ ต่างๆ ได้แก่ gmail, yahoo หรือเมล์ขององค์กร เช่น @wu.ac.th หรือ @walailak.net เป็นต้น

Applications

Google

Gmail • COMPOSE

Inbox (39) Sent Mail Circles Friends Family (1) Acquaintances Following Lectures Student ...

Agoda's Best Hotel Offers Hurry up, these weekend offers only last 48 hours! - Hot 6:13 pm

Rornasak Wongverawatanak Review papers - Aj Toi krub. Here's my reviews krub. — Regan 1:43 pm

Udem Chanankorn, you've completed 75% of your course: ชั้น C 11:51 am

Tumblr These blogs? You'll like 5 of them - These blogs? You'll like! 4:57 am

AISStatement AIS eStatement 084 997 6675 : 20/02/59 - 19/03/59 - INVOICE Mar 25

ECTI CON 2016 ECTI CON 2016 · Start TPC review process - Dear Technical F Mar 24

Jitima Surkhamani กิจกรรมวิชาชีวการ ครั้งที่ 1/2556 เรียนผลการเรียนการสอนวิชาชีวการ 23 Mar 23

Sunisa Khojeeul สอบเข้มภาษาไทยครั้งที่ 4 22 Mar 22

Email

Junk — Google (93 messages, 57 unread)

Mailboxes Inbox (52) Sent Flagged Drafts

Sort by Date

Popular in your network 3:50 PM Popular in your network
Popular in your network
Popular in your network

Engineering Journal 3:08 PM Thomson Reuters Researcher! index...
ISSN 2347-6662 We Apologize, If You Have Received Multiple Mails Int...
SILKSPAN 2:46 PM Is this email not displaying correctly? View it in your browser. This message was sent via a mobile device.

Twitter 2:26 PM Follow Leontis, Jeffreys Česko and... Hey DrChananok, Here are some people we think you might like to follow... silkspan.com

Conference Alerts 3:25 PM Governing Business Systems - Business Systems Laboratory - 4th INTERNATIONAL SYMPOSIUM March 18, 25-29 SE at 3:25 PM CA

Governing Business Systems - Business Systems Laboratory - 4th INTERNATIONAL SYMPOSIUM 2016, Vilnius, Lithuania
Mykolas Romeris University - Vilnius, Lithuania

Submit your work today - submissions close Friday, April 15!

We welcome your extended abstract proposals. Become a part of the premier Business Systems forum for presenting your research at the 4th Business Systems Laboratory International Symposium.

Submitting is easy, please follow instructions at the following link:
<http://haab-symposium.net/4th-international-symposium-vilnius-2016/submit/>

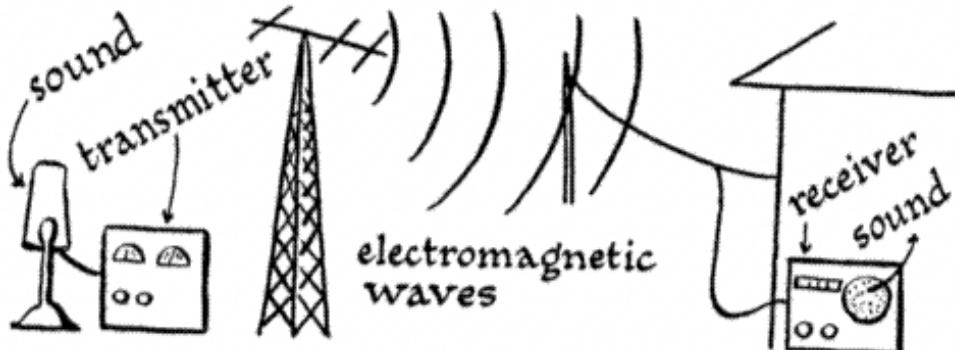
We hope to see you in Vilnius!

The 4th Business Systems Laboratory International Symposium focuses on the epistemological, theoretical, methodological, technical and practical contributions that can represent advancements in the theory and practice of Business Management.

Internet Technology

<http://cjundang.ubines.info>

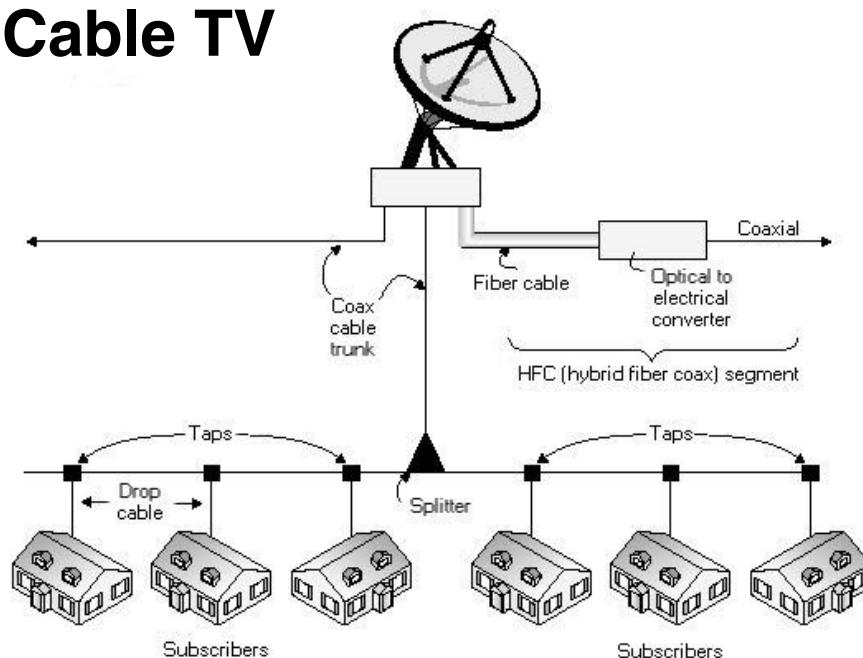
Radio



- การกระจายข่าววิทยุและโทรทัศน์ เป็นอีกรูปแบบหนึ่งของการให้บริการบนเครือข่าย ของการสื่อสาร โดยการกระจายข่าวสารนั้นอาศัยสถานีต้นทางเป็นผู้ส่งสัญญาณ ซึ่ง อาจจะเป็นแบบ กระจาย (broadcast) หรือส่งถึงผู้รับบางกลุ่ม (multicast) เป็นต้น โดย ส่งผ่านช่องสัญญาณจำเพาะ ซึ่งทาง ผู้รับต้องเป็นผู้ที่ปรับจูน (tune) ช่องสัญญาณ หรือความถี่ที่ตั้งกัน การกระจายสัญญาณโทรทัศน์ ในรูปแบบของเคเบิลทีวี เป็นวิธีการ กระจายสัญญาณอีกวิธีการที่นิยมทำระดับของเมืองเช่น เคเบิล ทีวีท้องถิ่น เป็นต้น นอกจากนี้ ยังมีการกระจายสัญญาณผ่านดาวเทียม ทั้งที่เป็นแบบฟรีและมีค่า ใช้จ่าย เป็นต้น

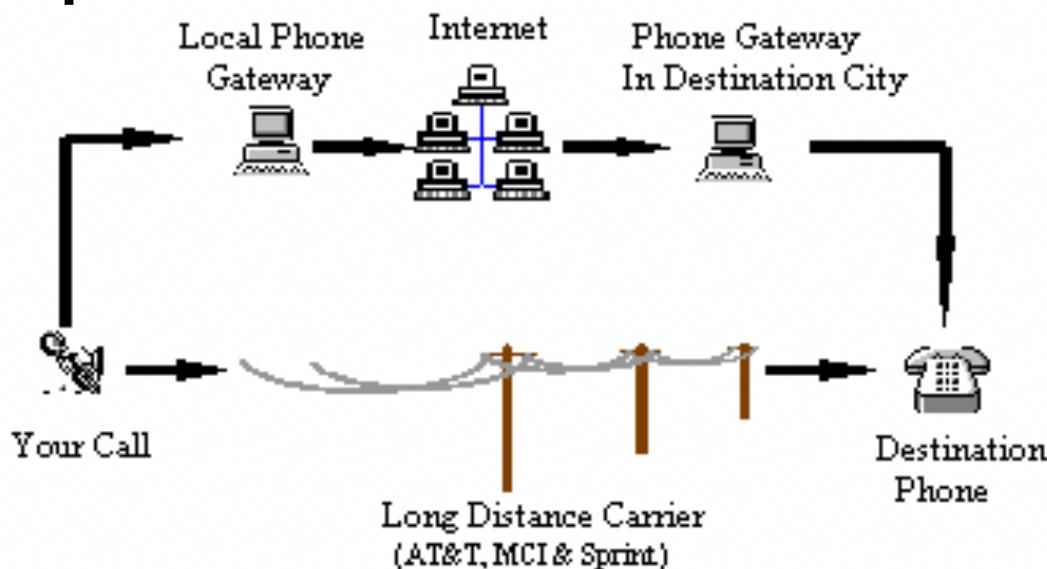
Applications

Cable TV



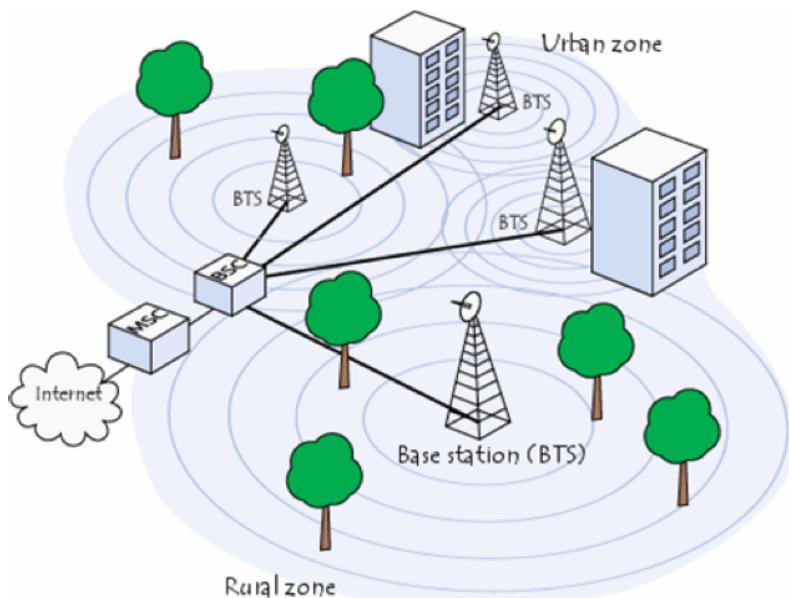
Applications

Telephone



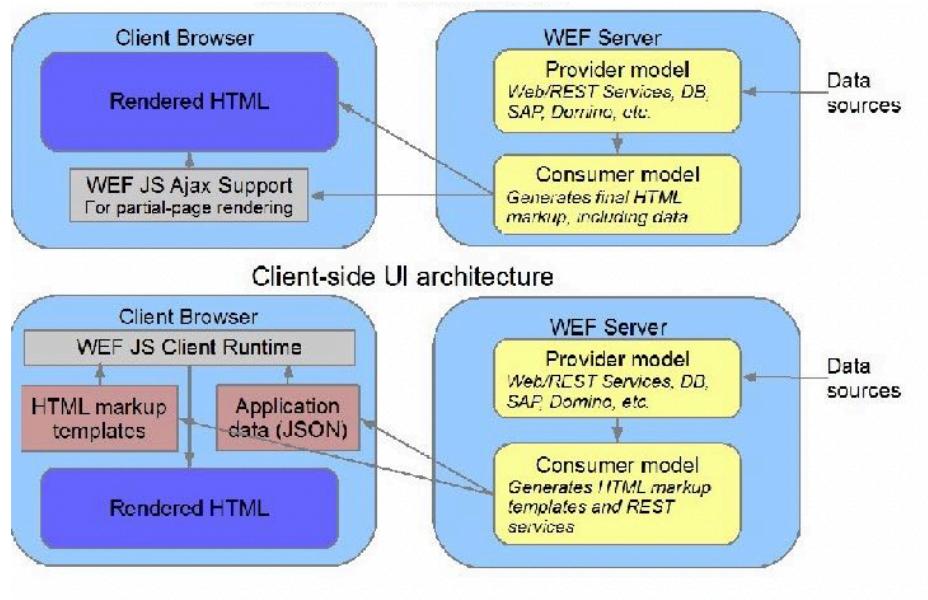
- ระบบโทรศัพท์แบบดั้งเดิมแบบ模拟 เป็นการสื่อสารแบบอนาล็อก ข้อมูลเสียงถูก แปลงเป็น สัญญาณไฟฟ้า และรวม (modulate) กับความถี่พาร์ (carrier frequency) เพื่อ ส่งข้อมูล ให้ไปถึง ปลายทาง เครื่องโทรศัพท์ทุกๆ เครื่องต้องเชื่อมต่อกับผู้ให้บริการ หรือ ชุมชน หลังจากนั้น ชุมชน จะเชื่อมต่อสัญญาณไปยังชุมชนอื่นๆ ที่เกี่ยวข้อง

Cellular Telephone



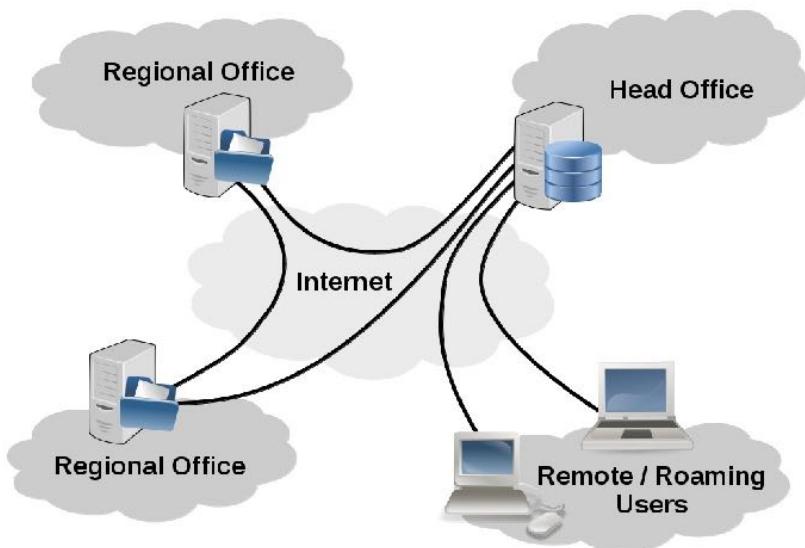
- การสื่อสารแบบรังผึ้ง (cellular telephone service) เป็นรูปแบบบริการในโทรศัพท์เคลื่อนที่ ซึ่งเป็นเทคนิคที่แบ่งช่องสัญญาณเป็นส่วนย่อยที่เรียกว่าเซลล์ (cell) เพื่อใช้สำหรับ การส่งเสียงตามช่อง สัญญาณ โดยเรียกเทคโนโลยีของการสื่อสารนี้ว่า โทรศัพท์รังผึ้ง (cellular telephone) โดยมีหลัก การคือ แบ่งพื้นที่ต่างๆ ออกเป็นส่วนย่อยเล็กๆ ซึ่งเรียกว่า เซลล์ ภายในเซลล์นั้นมีเสารับและส่งคลื่น ซึ่งมีการควบคุมการส่งจากสถานีขนาดย่อม เรียกว่า สถานีฐาน (base station หรือ BS) และเชื่อม ต่อไปยังสถานีกลางทำหน้าที่สลับช่อง สัญญาณของแต่ละเซลล์ เรียกว่า ศูนย์สลับสัญญาณเคลื่อนที่ (mobile service center หรือ MSC) โดย MSC นี้เชื่อมต่อกับเครือข่ายโทรศัพท์สาธารณะแบบสลับ สัญญาณ (public switched telephone network หรือ PSTN) ซึ่งเชื่อมต่อกับระบบโทรศัพท์บ้าน

Web Network



เครือข่ายเว็บ (web network) เป็นรูปแบบการให้บริการแบบเครื่องลูกข่าย/แม่ข่าย (client/server) โดย เครื่องแม่ข่าย (server) เป็นผู้ให้บริการ และเครื่องลูกข่าย (client) เป็นผู้ร้องขอบริการ การร้องขอบริการ ในรูปแบบเว็บนั้น อาศัยโปรโตคอลสำหรับการแลกเปลี่ยน ข้อมูลที่เขียนอยู่ในรูปแบบของภาษา มาร์กอัพ (markup language) เช่น Hypertext Markup Language (HTML) หรือ eXtensible Markup Language (XML) เป็นต้น การร้องขอเอกสารที่เขียนด้วย HTML หรือ XML นี้เป็นการร้องขอข้อมูลผ่าน เว็บโปรโตคอล (web protocol) ผ่านตัวชี้อ้างอิงที่อยู่ในอินเตอร์เน็ต (Universal Resource Locator หรือ URL)

Organizations



ด้านการบริการจัดการ

องค์กรแบ่งออกเป็นหน่วยงานย่อย โดยแต่ละหน่วยงานอาจจะอยู่ในอาคาร หรือบริเวณเดียวกัน หรือ บางองค์กร หน่วยงานบ่อย อยู่ต่างพื้นที่ แต่องค์กรเหล่านั้นต้องทำงานประสานกัน เช่น สำนักงานใหญ่ อยู่ในเมืองหลวง และมีสาขาย่อยอยู่ต่างภูมิภาค ในขณะที่โรงงานอยู่ที่นิคม อุตสาหกรรม แต่ละหน่วยงานนั้น ต้องทำงานประสานกัน จึงจำเป็นที่ต้องเชื่อมโยงข้อมูลเข้าด้วยกัน

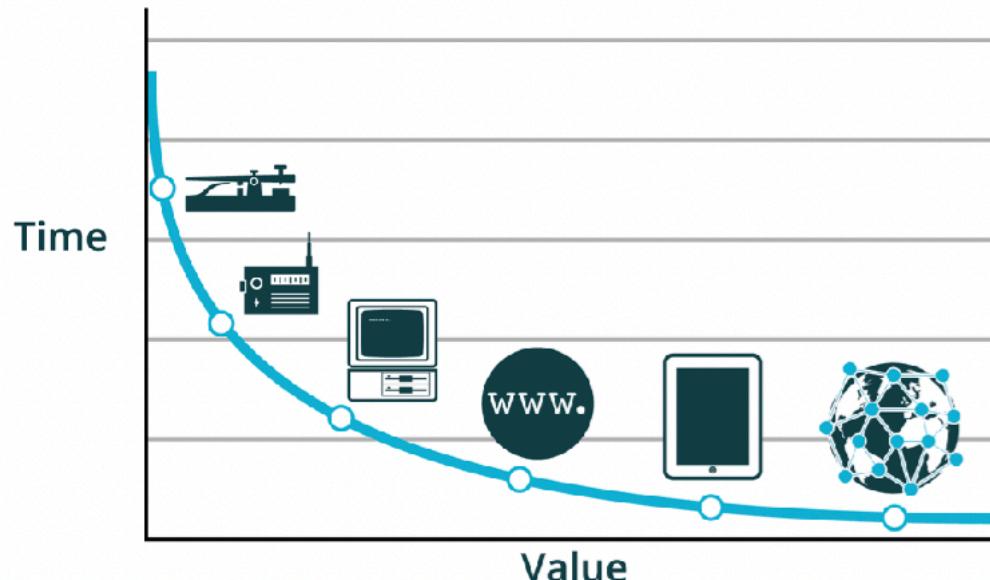
Finance & Bank



ด้านการเงิน การธนาคาร

การดำเนินกิจกรรมทางธุรกิจ การสื่อสารข้อมูลเป็น ปัจจัยต้นๆ ที่ช่วยสนับสนันการทำงาน เช่น ทางธนาคารได้ เปิดบริการ โอนเงินระหว่างธนาคาร ทั้ง ในและต่างประเทศ ยิ่งเป็นการ โอนเงินต่างประเทศ แล้วยังต้องการการสื่อสาร ข้อมูลเพื่อเทียบค่าเงิน ในปัจจุบัน เพื่อแปลงค่าเงินปัจจุบัน เป็นสกุลเงินปลายทาง การให้บริการ ATM ของธนาคาร เป็นการสื่อสารข้อมูลระหว่าง ตู้ ATM และธนาคารที่ดูแล เพื่อแลกเปลี่ยนจำนวนเงิน ในบัญชีของผู้ใช้ก่อนที่จะถอนเงิน ออกจากบัญชี

Data Exchange

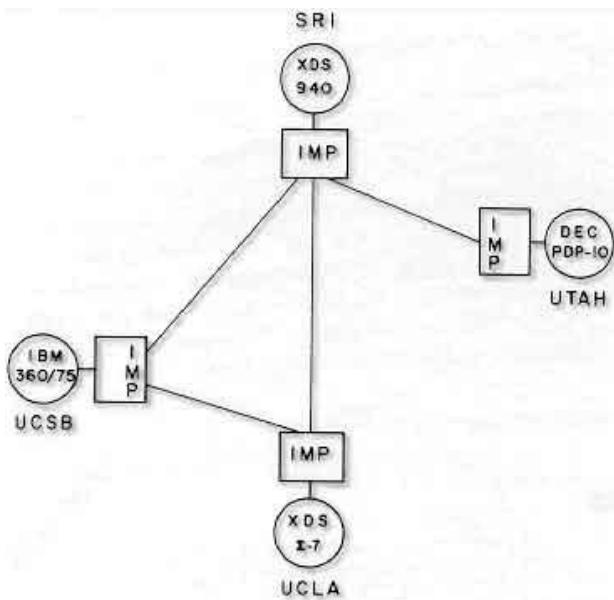


ด้านการแลกเปลี่ยนข่าวสาร

ข่าวสารเป็นปัจจัยที่ใช้ในการดำเนินการขององค์กร ในยุคแรกๆ แลกเปลี่ยนข้อมูลผ่าน จดหมาย เทคโนโลยีทางไฟฟ้าได้พัฒนาขึ้นจึงเกิดบริการผ่านทางโทรศัพท์ ส่งเสียงผ่านโทรศัพท์ ก้าวสู่ยุคของ อินเตอร์เน็ต การส่งข้อความผ่าน email การส่งข้อความลับ ผ่านระบบแชท เช่น โปรแกรม LINE หรือ MSN เป็นต้น เทคโนโลยีของการสื่อสารพัฒนาไปไกลขึ้น การส่งข้อมูลข่าว ในแบบ VDO Chat หรือ VDO Conference เป็นต้น มาตรฐานต่างๆ ที่เกี่ยวข้อง

Contents

- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology



คำว่า "อินเทอร์เน็ต" สำหรับภาษาไทยแล้วหมายถึงการสื่อสารข้อมูลแบบกว้างที่ครอบคลุม ทั่วทั้งโลก แต่สำหรับคำว่า internet และ Intetnet ในภาษาอังกฤษนั้นมีความหมายแตกต่างออกไป กล่าวคือ "internet is a network of network" ซึ่งหมายถึงการเชื่อมโยงเครือข่ายต่างๆ เข้าด้วยกัน ในขณะที่ "Internet is a collection of many separate networking" ซึ่งหมายถึงการเชื่อมโยงเครือข่ายที่มีความแตกต่างไว้ด้วยกัน จึงเป็นความหมายของคำว่า "อินเทอร์เน็ต" ตามความหมายของภาษาไทย

```
Return-path: kre@sritrang.psu.th
Received: from mulga.OZ by munnari.oz (5.5)
id AA06244; Thu, 2 Jun 88 21:22:14 EST
(from kre@sritrang.psu.th for kre)
Received: by mulga.oz (5.51)
id AA01438; Thu, 2 Jun 88 21:21:50 EST
Apparently-to: kre
Date: Thu, 2 Jun 88 21:21:50 EST
From: kre@sritrang.psu.th
Message-id: <8806021121.1438@mulga.OZ>
```

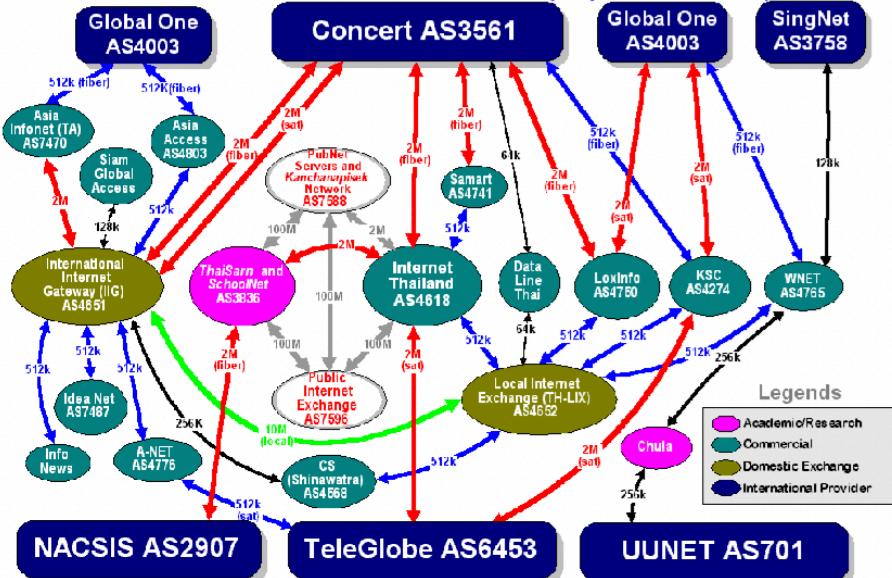
Hi.

Bye

(Courtesy of the Computing Center, Prince of Songkla University, Thailand)

Internet in Thailand

Internet Connectivities in Thailand (September 1997)



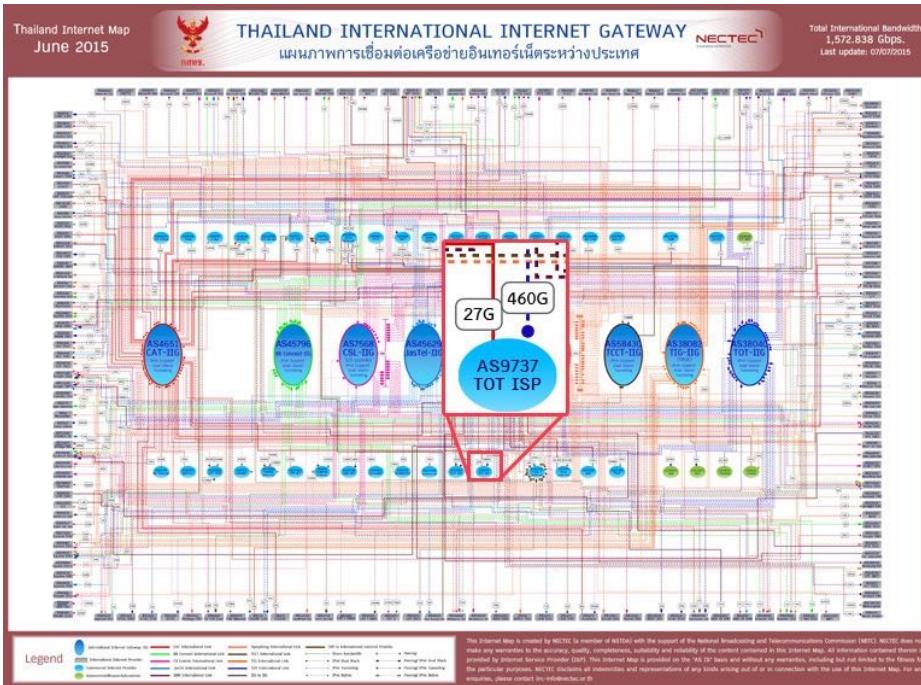
DISCLAIMER

This chart is designed, rendered and copyrighted by Junji J. Phumibol and Prasertsak Kornkraukul, NECTEC. All rights reserved. The information contained in this chart is based on our measurement and estimation. We welcome update information, otherwise we have the right to verify the accuracy of the given information. Please contact 4. <http://necnet.nict.go.th> For further information please contact Organization of Information and Communication Authority in Thailand.



Internet Gateway

UbIn3\$
Ubiquitous Networked Embedded System

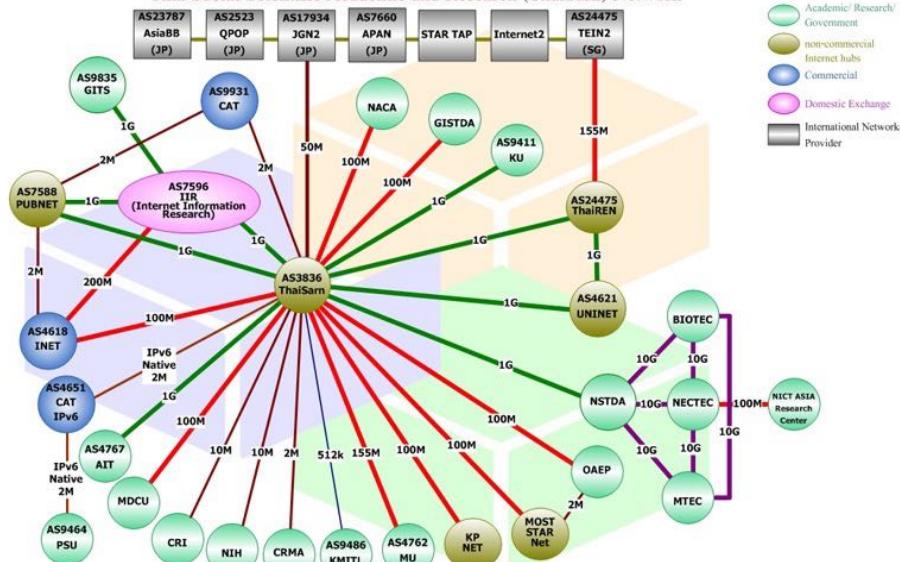


Internet Technology

<http://cjundang.ubines.info>

22

Thai Social/Scientific Academic and Research (ThaiSarn) Network



NECTEC
a member of NSTDA

This chart is designed, maintained copyrighted by Chatchai Chan-In ThaiSarn, NECTEC. All rights reserved.
The information contained in this chart is based actual measurements and estimation. We welcome update information, but reserve the rights
to verify the accuracy of the given information. Please contact us at noc@nectec.or.th



Contents

- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology

de facto standard



- บริษัทแต่ละบริษัทนั้นมักจะพัฒนาโปรโตคอลเครือข่ายของมาใช้งานและทำการตลาด โปรโตคอลแต่ละบริษัทไม่มีมาตรฐานกลาง จึงส่งผลให้ผลิตภัณฑ์ของแต่ละบริษัทไม่สามารถทำงานร่วมกันกับผลิตภัณฑ์ของบริษัทอื่น ส่งผลให้ผู้ใช้ต้องลงทุนกับอุปกรณ์ของบริษัทใดบริษัทหนึ่งเท่านั้น
- ดังนั้นจึงจำเป็นต้องสร้างมาตรฐานสำหรับอุปกรณ์เครือข่ายขึ้นมาเพื่อให้บริษัทต่างๆ ผลิต อุปกรณ์เครือข่าย ทำให้อุปกรณ์เครือข่ายจากต่างบริษัทกันสามารถใช้งานร่วมกันได้ โดยในเบื้องต้นของการสื่อสารข้อมูลนั้น มาตรฐานแบ่งออกเป็น 2 ประเภทคือ de jure และ de facto
- de facto standard หมายถึงมาตรฐานที่เกิดจากการใช้งานของผู้คนเป็นเวลากนานและเป็นที่ยอมรับโดยทั่วไป เช่น โปรโตคอลนั้นๆ จะกระทิ้งโปรโตคอลนั้นถือยกให้กลายเป็นมาตรฐานในที่สุด เช่น โปรโตคอล TCP/IP เป็นต้น

de jure standard



de jure standard หมายถึงมาตรฐานที่ได้ผ่านการรับรองจากองค์กรที่เชื่อถือ และเป็นที่ยอมรับตัวอย่าง องค์กรต่างๆ ได้แก่

- **International Organization for Standardization** One of the most important standards-making bodies is the *International Organization for Standardization (ISO)*,² which makes technical recommendations about data communication interfaces (see www.iso.org). ISO is based in Geneva, Switzerland. The membership is composed of the national standards organizations of each ISO member country.
- **International Telecommunications Union—Telecommunications Group** The **Telecommunications Group (ITU-T)** is the technical standards-setting organization of the United Nations International Telecommunications Union, which is also based in Geneva (see www.itu.int). ITU is composed of representatives from about 200 member countries. Membership was originally focused on just the public telephone companies in each country, but a major reorganization in 1993 changed this, and ITU now seeks members among public- and private-sector organizations who operate computer or communications networks (e.g., RBOCs) or build software and equipment for them (e.g., AT&T).

de jure standard



- **American National Standards Institute** The **American National Standards Institute (ANSI)** is the coordinating organization for the U.S. national system of standards for both technology and nontechnology (see www.ansi.org). ANSI has about 1,000 members from both public and private organizations in the United States. ANSI is a standardization organization, not a standards-making body, in that it accepts standards developed by other organizations and publishes them as American standards. Its role is to coordinate the development of voluntary national standards and to interact with ISO to develop national standards that comply with ISO's international recommendations. ANSI is a voting participant in the ISO.
- **Institute of Electrical and Electronics Engineers** The **Institute of Electrical and Electronics Engineers (IEEE)** is a professional society in the United States whose Standards Association (IEEE-SA) develops standards (see www.standards.ieee.org). The IEEE-SA is probably most known for its standards for LANs. Other countries have similar groups; for example, the British counterpart of IEEE is the Institution of Electrical Engineers (IEE).

RFC: Request for Comments UbiN3\$

Internet Engineering
Request for Comments
Category: Standards
ISSN: 2070-1721

Internet Engineering Task Force (IETF)
Request for Comments: 7540
Category: Standards Track
ISSN: 2070-1721

M. Belshe
BitGo
R. Peon
Google, Inc
M. Thomson, Ed.
Mozilla
May 2015

Hypertext Transfer Protocol Version 2 (HTTP/2)

Abstract

This specification defines a new version of the Hypertext Transfer Protocol (HTTP) for requesting, receiving, and transmitting hypertext resources and a new set of extensions for performing field compression over the same connection.

Hypertext Transfer Protocol Version 2 (HTTP/2)

This specification is an alternative to, but does not obsolete, the HTTP/1.1 message syntax. HTTP's existing semantics remain unchanged.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in [Section 2 of RFC 5741](#).

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc7540>.

28

Internet Technology

<http://cjundang.ubines.info>

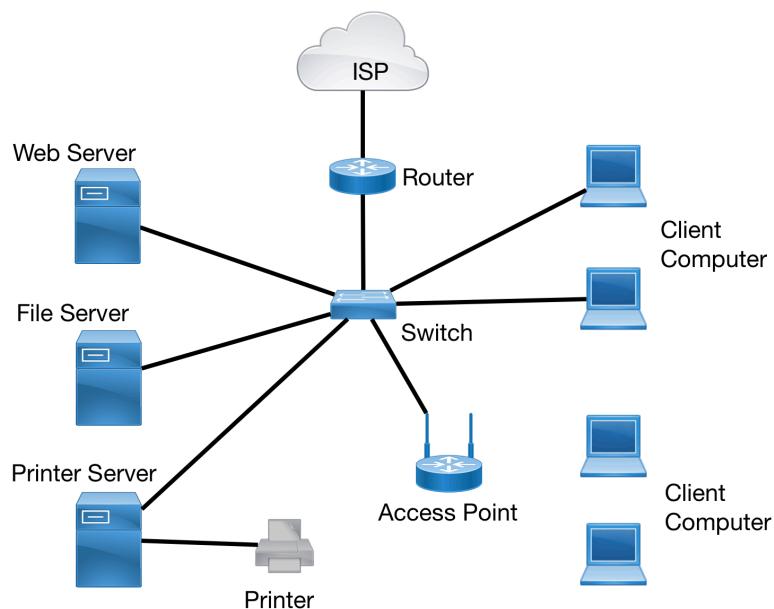
M1-introduction to computer network-LO3

Request for Comments (RFC) เป็น แนวคิดของการกำหนดมาตรฐานอินเทอร์เน็ต โดย เริ่มต้นจาก การร่างเอกสาร Internet Draft ที่ เกี่ยวข้องกับประเด็นที่ต้องการกำหนดมาตรฐาน หลังจากนั้นเผยแพร่ ให้คนทั่วไปทราบ ถ้าเอกสาร นั้นไม่ได้รับการพิจารณาจากผู้ทรงคุณวุฒิ เอกสาร นั้นจะตกไป แต่ถ้าเป็น ที่ยอมรับเอกสารนั้นจะได้รับ หมายเลขซึ่งเรียกว่า RFC ผู้ผลิตสามารถพัฒนา อุปกรณ์หรือโปรแกรมที่ เป็นไปตามมาตรฐานนั้นๆ จนกระทั่งวันนึงถ้ามีกลุ่มวิจัย ใดๆ ที่ได้ออกแบบ มาตรฐานเรื่องเดียวกันขึ้นมา ใหม่ ทำให้มาตรฐาน เดิมตกไปจะส่งผลให้ RFC เดิมถูกยกเลิก (Obsolete) และจะใช้งาน RFC หมายเลขใหม่

Contents

- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology

Network Components

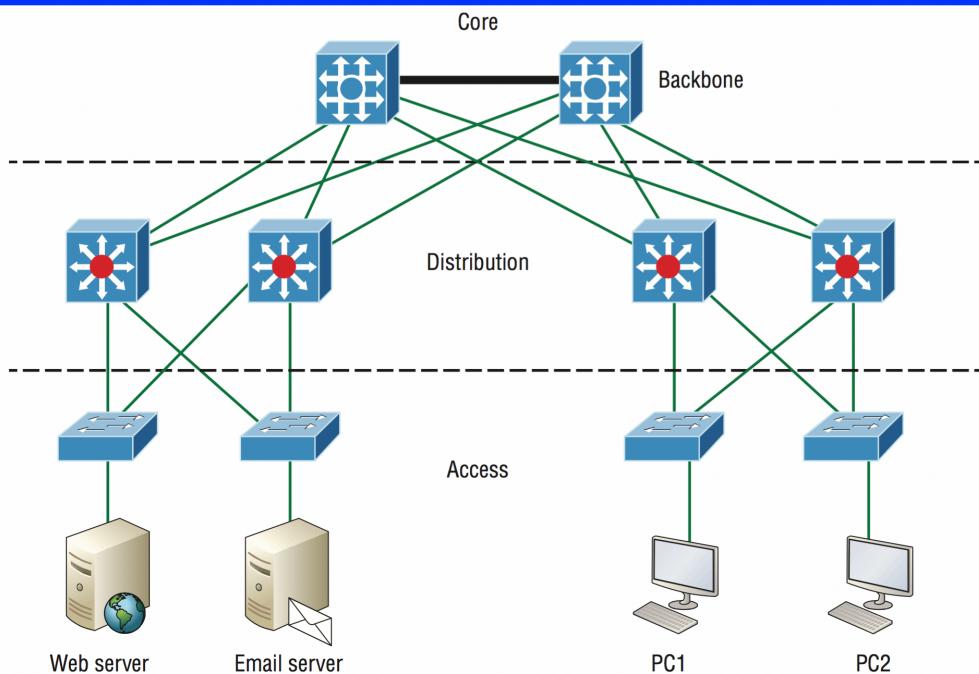


Contents

- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology

Hierarchical Network Architecture

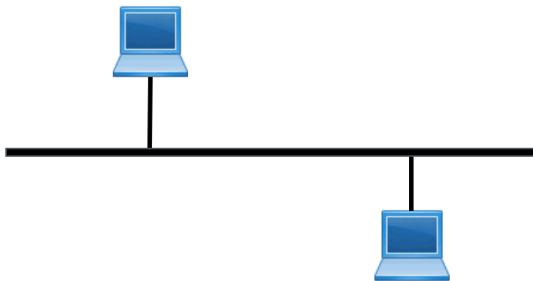
UbIn3\$
Ubiquitous Networked Embedded System



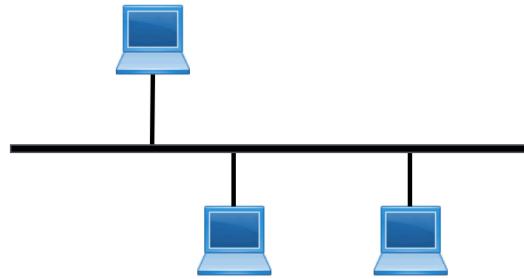
โครงสร้างเครือข่ายประกอบด้วยชั้นต่างๆ ได้แก่ ชั้นการเข้าถึง (Access Layer), ชั้นกระจาย (Distribution Layer) และ ชั้นแกน (Core Layer) โดยแต่ละโมเดล อธิบายได้ดังนี้

- ชั้นการเข้าถึง (Access Layer) เป็นชั้นที่อยู่ใกล้กับผู้ใช้งานที่สุด เป็นจุดที่นำเครื่องคอมพิวเตอร์ของผู้ใช้เข้าสู่ระบบเครือข่าย สำหรับ LAN และ Campus Network อุปกรณ์เครือข่ายที่ใช้งานในชั้นนี้คือ สวิตซ์ชั้น 2 (L2-Switch) หรือ ฮับ (Hub) (แต่ในทางปฏิบัติควรเป็นสวิตซ์ชั้นที่ 2 เพื่อลดการชนกันของเฟรม) โดยจำนวนพอร์ตที่ใช้งาน ควรมีให้เท่ากันกับอุปกรณ์ของผู้ใช้ หรือเชื่อมต่อกับอุปกรณ์เครือข่ายไร้สาย (Access Point) การเชื่อมต่อในกลุ่มนี้ จะมีพอร์ตอย่างน้อย 1 พอร์ต ใช้สำหรับเชื่อมต่อกับ Distribution Switch หรือ Core Switch ซึ่งเรียกพอร์ตนั้นว่า Up Link
- ชั้นกระจาย (Distribution Layer) เป็นชั้นที่รวม Access Switch ต่างๆ เข้าด้วยกัน เพื่อส่งผ่านไปยังชั้นแกน อุปกรณ์ในกลุ่มนี้ควรเป็นอุปกรณ์ที่มีประสิทธิภาพ มีฟังก์ชันเสริมการทำงานต่างๆ เช่น InterVLAN, Routing, Access Control List (ACL) รวมถึง QoS เป็นต้น
- ชั้นแกน (Core Layer) เป็นหัวใจหลักของเครือข่าย ซึ่งมีหน้าที่เชื่อมต่อ Distribution Switch ต่างๆ เข้าด้วยกัน อุปกรณ์ในชั้นนี้ ควรมีประสิทธิภาพสูง สามารถรับส่งข้อมูลได้รวดเร็ว

ในทางปฏิบัติ องค์กรได้รวม ชั้นกระจาย (Distribution Layer) และ ชั้นแกน (Core Layer) ไว้ด้วยกัน เนื่องจากองค์กรมีขนาดเล็ก หรือมีข้อจำกัดของงบประมาณ สำหรับองค์กรที่มีขนาดใหญ่ อาจจะมีการใช้งานเราเตอร์เป็น Core Layer เพื่อจัดการเครือข่ายให้มีประสิทธิภาพสูงสุด ซึ่งสิ่งที่ตามมาคือ งบประมาณและความรู้ความเข้าใจของผู้ดูแลระบบ จำเป็นต้องมีพร้อมเช่นกัน

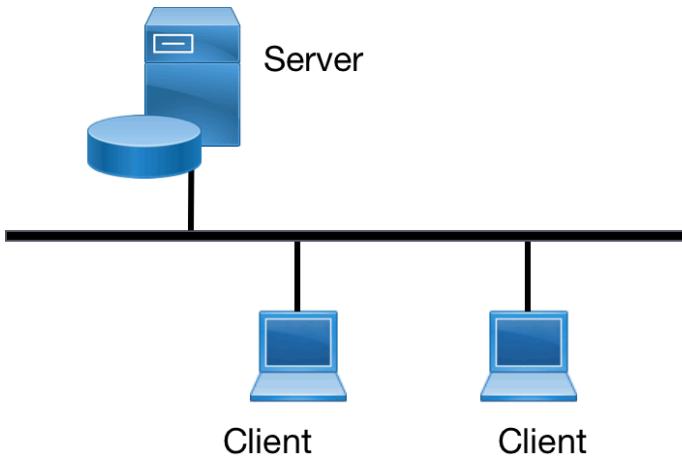


Point-to-Point



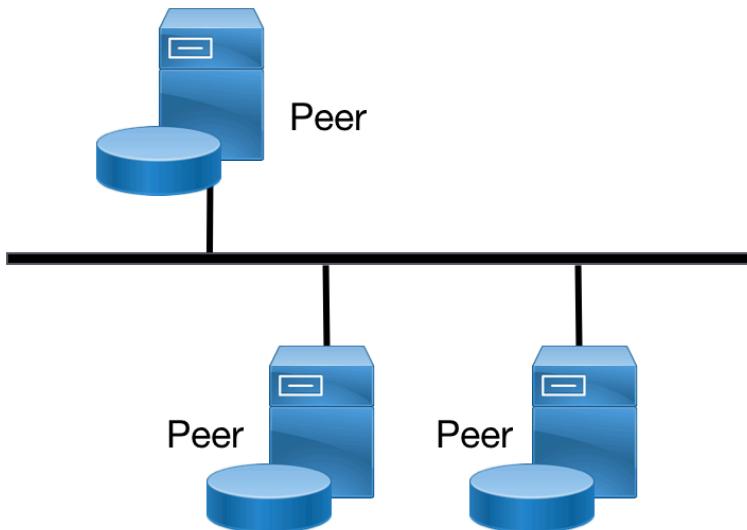
Multipoint

- เครือข่ายคอมพิวเตอร์คือกลุ่มของการสื่อสารข้อมูลของอุปกรณ์ ที่เชื่อมต่อกันด้วยลีโอลาง ต่างๆ ขนาดของเครือข่ายนั้นเริ่มต้นจากคู่สันทนาขนาดเล็กนั่นคือ การสื่อสารข้อมูลซึ่งเกิดจากการ สื่อสาร ข้อมูลของคอมพิวเตอร์เพียง 1 คู่ หากคอมพิวเตอร์แต่ละตัวนั้นเชื่อมต่อกับคอมพิวเตอร์ตัว อื่นๆ ได้ มากกว่า 1 ตัวจะส่งผล ให้มีจำนวนของคู่สันทนามากยิ่งขึ้น กลุ่มของการสื่อสารนั้นๆ เรียกว่า เครือข่ายคอมพิวเตอร์
- เครือข่ายคอมพิวเตอร์แบ่งออกเป็นสองประเภทได้แก่ Point-to-Point ซึ่งมีอุปกรณ์จำนวน 2 ตัวถูก เชื่อมต่อด้วยลิงค์เดียวกัน และไม่มีอุปกรณ์อื่นๆมา ใช้งานร่วม ในขณะที่ Multipoint เป็นเครือ ข่าย คอมพิวเตอร์ที่มีจำนวนอุปกรณ์มากกว่าสองตัวเชื่อมต่อที่สื่อสารร่วมกัน (เส้นเดียว กัน)



Client/Server

- ไอคลอนต์/เซิร์ฟเวอร์ เป็นตัวแบบเครือข่าย คอมพิวเตอร์ที่ให้บริการซึ่งประกอบด้วยอุปกรณ์ 2 ส่วน ได้แก่ เครื่องแม่ข่ายหรือเซิร์ฟเวอร์ (Server) และเครื่องลูก ข่ายหรือไอคลอนต์ (Client) โดยที่เครื่อง แม่ข่ายนั้นมีหน้าที่ ให้บริการข้อมูล ทรัพยากร หรือหน้าที่การทำงานใดๆ ตาม วัตถุประสงค์ของอุป ก กรณ์นั้นๆ ในขณะที่เครื่องลูกข่าย มีหน้า ที่สำหรับร้องขอข้อมูลหรือบริการจากเครื่องแม่ข่าย โดย ปกติแล้วเครื่องแม่ข่ายและเครื่องลูกข่ายนั้นมักจะมี สถาปัตยกรรมที่แตกต่างกัน แต่ไม่มีผลกระทบ ต่อการทำงาน เสมือนว่า อุปกรณ์ทั้งสองฝ่ายมีสถาปัตยกรรมแบบเดียวกัน
- ตัวอย่างตัวแบบไอคลอนต์เซิร์ฟเวอร์ที่เป็นที่รู้จักคือ การให้บริการเว็บไซต์ ผู้ใช้เข้าถึงเว็บ ไซต์ ได้ ผ่านเว็บเบราว์เซอร์ โดยพิมพ์ชื่อเครื่อง ให้บริการ จากเครื่องคอมพิวเตอร์หรืออุปกรณ์ เคลื่อนที่ของผู้ ใช้งาน การพิมพ์ชื่อเครื่อง ให้บริการข้างต้นผ่านเว็บเบราว์เซอร์นั้นหมายถึงการร้องขอ ข้อมูล เครื่อง ให้ บริการเว็บจะตอบกลับด้วยข้อความ ภาพ หรือเสียงขึ้นอยู่กับข้อมูลที่จัดเก็บอยู่ ใน เครื่อง ให้บริการ นั้นๆ เครื่องคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ที่เรียกว่า เว็บ เรียกว่า เครื่องลูกข่าย หรือ ไอคลอนต์ (Client) ในขณะที่เครื่องคอมพิวเตอร์ที่ติดตั้ง โปรแกรม ให้บริการเว็บ และจัดเก็บ ข้อมูลเว็บนั้นเรียกว่า เครื่องแม่ข่าย หรือเครื่องเซิร์ฟเวอร์ (Server)
- สำหรับเครื่องแม่ข่ายนั้นต้องติดตั้งและสั่งรัน โปรแกรมพิเศษที่ทำหน้าที่ ให้บริการเซ่นกัน โดยเรียก โปรแกรมข้างต้นว่า โปรแกรมแม่ข่าย (Server Program) และ ในขณะที่เครื่องลูกข่ายนั้น ต้องติดตั้ง โปรแกรมสำหรับเชื่อมต่อเครื่องแม่ข่ายเซ่นกัน เช่น โปรแกรมเว็บเบราว์เซอร์ ใช้สำหรับ การเข้าถึง เว็บไซต์ต่างๆ



Peer-to-Peer

เครือข่ายแบบเพียร์-ทู-เพียร์ หรือ P2P เป็น สถาปัตยกรรมประยุกต์แบบกระจายซึ่งแบ่งงานหรือ บริการ ต่างๆ ให้แก่ เพียร์ โดยที่แต่ละเพียร์จะมีสิทธิ์ที่ เท่าเทียมกัน ในแต่ละ โปรแกรมประยุกต์ โดยแบ่งส่วน ทรัพยากรต่างๆ เช่น การประมวลผล ดิสก์ หน่วยความจำ หรือแบบตัวทัชของเครือข่าย เพื่อประมวลผล การบริการที่ ต้องการ โดยที่ไม่มีอุปกรณ์ใดๆ เป็นศูนย์กลาง

Contents

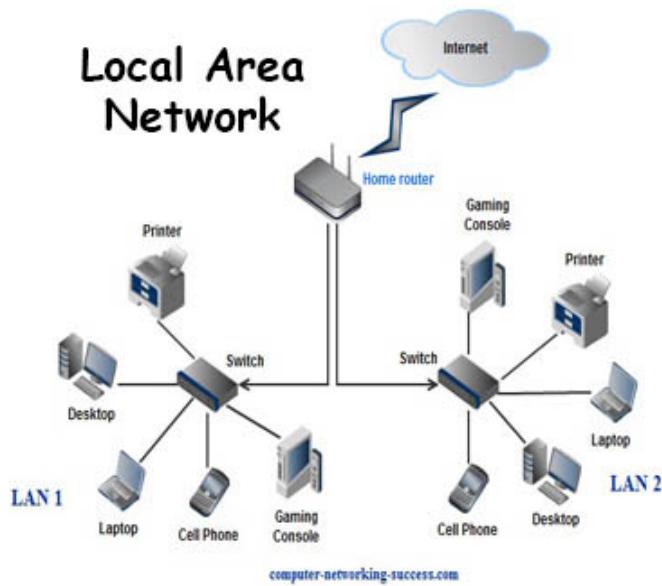
- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology

Area based: Personal Area Network (PAN)



- การจำแนกตามพื้นที่เชื่อมโยง เป็นโดยพิจารณาจากระยะของการเชื่อมต่อระหว่างอุปกรณ์ จำนวนช่วง (hop) ระหว่างอุปกรณ์ หลักการสื่อสารข้อมูลว่าเป็นแบบ broadband หรือ baseband จากหลักการจัดแบ่งข้างต้น จำแนกออกเป็น เครือข่ายส่วนบุคคล เครือข่ายท้องถิ่น เครือข่ายเมือง หลวง และ เครือข่ายแบบกว้าง เป็นต้น
- เครือข่ายส่วนบุคคล (personal area network หรือ PAN) เป็นเครือข่ายไร้สายขนาดเล็กที่ เชื่อมต่อ อุปกรณ์ขนาดเล็ก โดยสื่อสารระหว่างกันโดยตรง โครงสร้างเครือข่ายสามารถเปลี่ยนแปลงได้ ตลอดเวลา (ad hoc network) แต่ละช่วงเวลา ได้ มีอุปกรณ์เชื่อมต่อพร้อมกันหลายโหนด อาจจะมี จำนวน 8 - 255 โหนด ขึ้นอยู่เทคโนโลยีไร้สายที่เลือก ใช้ หรือระยะห่างระหว่างอุปกรณ์ตั้งแต่ 10 เมตร หรือห่างถึง 100 เมตร นั่นขึ้นอยู่กับมาตรฐานการ เชื่อมต่อ และสภาพแวดล้อม ในขณะนั้น ทั้ง ความชื้น อุณหภูมิ จะกระทบต่อคุณภาพการเชื่อมต่อและการ สื่อสาร
- ตัวอย่างการประยุกต์ใช้งานเครือข่าย PAN ได้แก่ การแชร์ทรัพยากร่างๆ ผ่านเครือข่ายบลูทูธ (Bluetooth) เช่น เครื่องคอมพิวเตอร์โน๊ตบุ๊คเชื่อมต่อ เม้าส์ แป้นพิมพ์ เครื่องพิมพ์ ลำโพงหรือหูฟัง เป็นต้น จากตัวอย่างข้างต้นแสดงให้เห็นว่า อุปกรณ์ต่างๆ เหล่า นั้นเชื่อมต่อด้วยเครือข่ายไร้สาย บลูทูธ
- นอกจากตัวอย่างข้างต้นแล้ว เครือข่าย PAN กำลังจากถูกนำมา ใช้งานมากยิ่งขึ้น ทั้งเชื่อม ต่อกับ เทคโนโลยีมือถือ เชื่อมต่อกับอุปกรณ์อื่นๆ ที่อยู่รอบตัว และก้าวสู่เทคโนโลยีของ Internet of Thing หรือ IoT เป็นต้น

Area based: Local Area Network (LAN)



เครือข่ายท้องถิ่น (local area network หรือ LAN) เป็นเครือข่ายที่เชื่อมโยงภายในองค์กร อาจจะมีพื้นที่ครอบคลุมห้อง อาคาร หรือกลุ่มอาคาร เพื่อใช้สำหรับการแชร์ทรัพยากร ได้แก่ งาน พิมพ์ ไฟล์ หรือ เครือข่ายอินเตอร์เน็ต เป็นต้น ภายในเครือข่ายแลนเดียวกันจะออกแบบให้มีการ เชื่อมต่อด้วย เทคโนโลยีเดียวกัน เพื่อให้ง่ายในการจัดการ โดยผู้ดูแลระบบ เช่นการออกแบบเครือข่าย ในบริษัท หรือซอฟต์แวร์เข้าสู่ขนาดเล็ก หรือการเชื่อมต่อเครือข่าย ในมหาวิทยาลัยลักษณ์

Area based: Local Area Network (LAN)

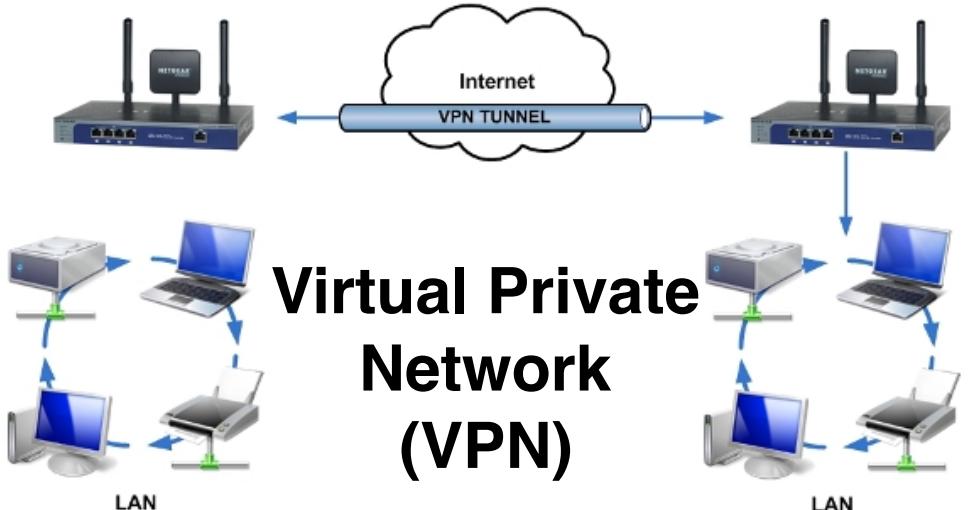


Home Network

ในปัจจุบันความก้าวหน้าของเทคโนโลยีเพิ่มขึ้น การจัดเครือข่ายในบ้านมีการใช้งานอย่างแพร่หลายมากขึ้น ที่พักอาศัยอาจจะมีอุปกรณ์เครือข่าย เพื่อเป็นตัวกลางในการเชื่อมต่อ เช่น Wireless Access Point หรือ AP หลังจากนั้นผู้ที่พักอาศัยสามารถเข้าถึงเครือข่ายได้ พร้อมทั้ง สามารถใช้งานทรัพยากรอื่นๆ ได้พร้อมกัน ซึ่งเรียกว่า Home Network

Area based: Local Area Network (LAN)

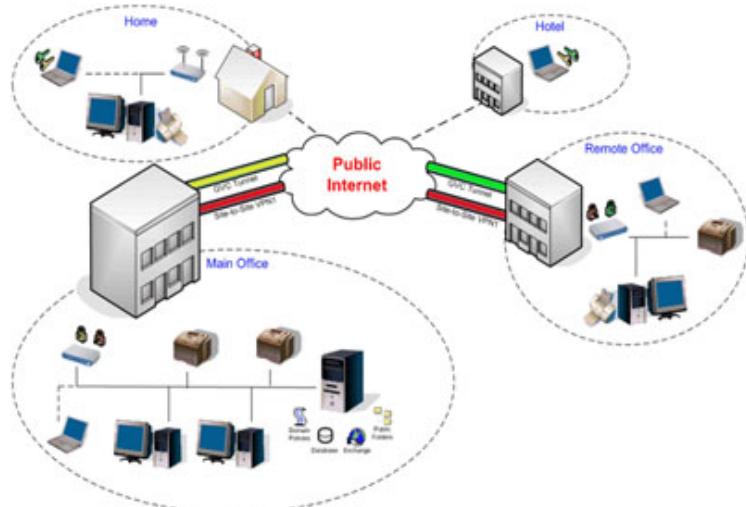
Netgear VPN Router



Virtual Private Network (VPN)

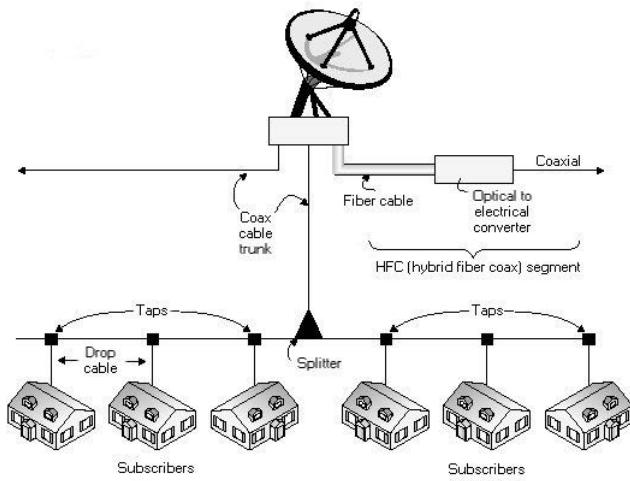
นอกจากนี้ หากนิยามเครือข่ายท้องถิ่นเพิ่มเติมด้วยสิทธิ์หรือจัดการเครือข่ายของผู้ดูแลระบบ เพียงคนเดียว แต่สถานที่อยู่ระหว่างเครือข่ายอยู่อยู่ห่างกัน อาจจะเป็นคนละอำเภอ หรือข้าม จังหวัด เช่น มหาวิทยาลัยลักษณ์มีหน่วยงานหลักที่ อ.ท่าศาลา จ.นครศรีธรรมราช นอกจากนี้ยัง มีหน่วยงานอยู่ที่ ตึก SM โรงพยาบาลชิรภูเก็ต และ จังหวัดสุราษฎร์ธานี ต่างมีเชื่อมต่อด้วยเครือ ข่ายเดียวกัน ผู้ดูแลระบบทีมเดียวกัน แต่อยู่ต่างพื้นที่หรือจังหวัดกัน

Area based: Local Area Network (LAN)



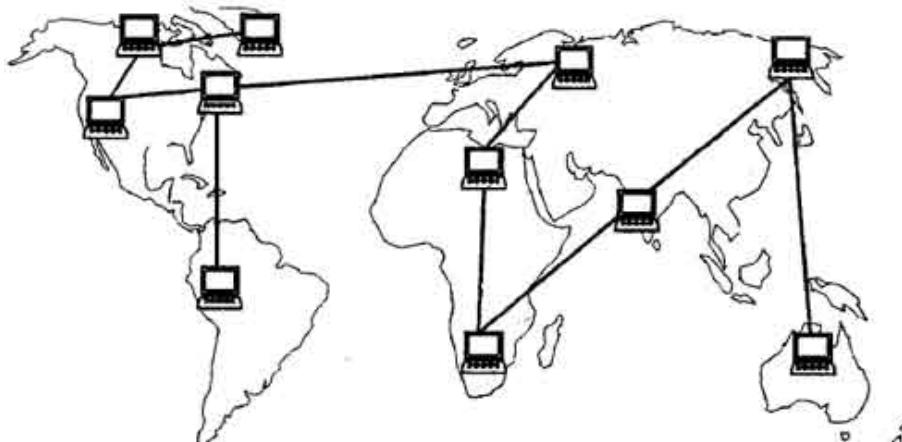
Virtual Private Network (VPN)

Area based: Metropolitan Area Network (MAN)



เครือข่ายนครหลวง (metropolitan area network หรือ MAN) เป็นการเชื่อมต่อเครือข่ายจากองค์กรต่างๆ ในพื้นที่ที่กว้างเข้าเป็นเครือข่ายเดียวกัน ในปัจจุบันเครือข่าย MAN ใช้งานใน เครือข่ายของเคเบิลทีวี เช่น ในเขตเมือง ภูเก็ต หาดใหญ่ เป็นต้น มีบริการเคเบิลทีวี สำหรับถ่ายทอดสัญญาณทีวีผ่านสายทองแดง โดยเชื่อมต่อกับ settopbox และ ศูนย์กระจายสัญญาณ

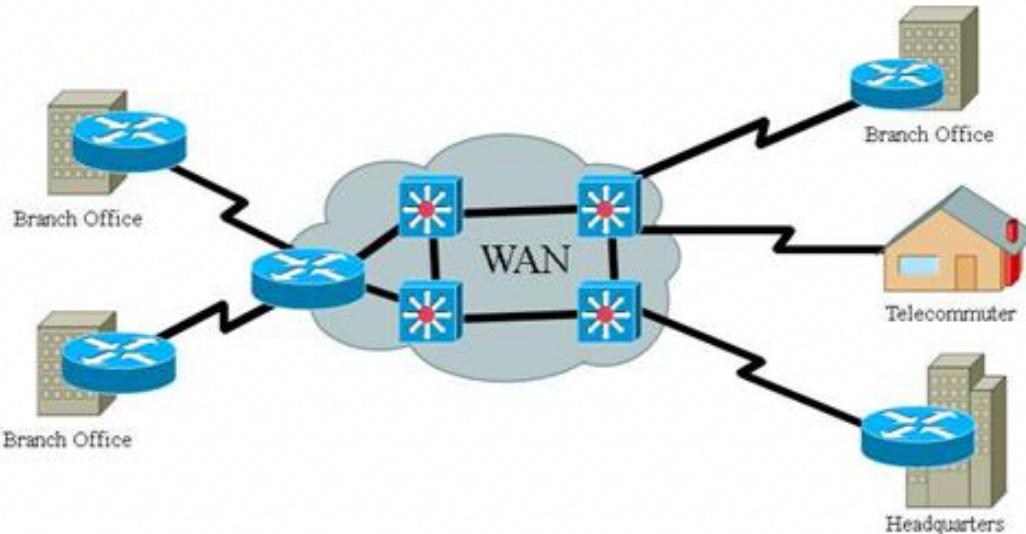
Area based: Wide Area Network (WAN)



Internet

- เครือข่ายเครือข่ายแบบกว้าง (Wide Area Network หรือ WAN) เกิดจากการเชื่อมต่อเครือ ข่ายแลน ต่างๆ เช้าด้วยกัน โดยเชื่อมต่อแบบจุดต่อจุด (point to point) โดยเครือข่ายย่อยนั้น กระจายอยู่ทั่วโลก เชื่อมตอกันด้วยลีส์ความเร็วสูง เช่น ดาวเทียม สายใยแก้วนำแสง เป็นต้น ความเร็วในการลีส์สามารถมีความเร็ว ในระดับของ 10 กิกะบิตต่อวินาที

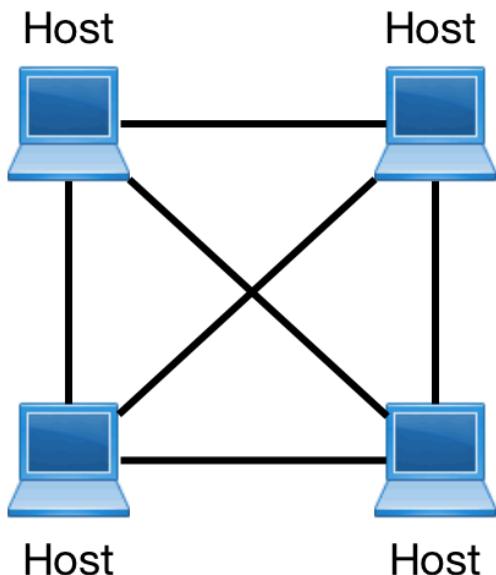
Area based: Wide Area Network (WAN)



- เครือข่ายแบบกว้าง เชื่อมต่อกันด้วยอุปกรณ์เรอเตอร์ (router) ทำหน้าที่ค้นหาเส้นทาง แม้ว่า การเชื่อมต่อเครือข่ายนั้นเป็นแบบจุดต่อจุด แต่สำหรับเครือข่ายขนาดใหญ่ระดับโลกนั้น ต้องอาศัย เรอเตอร์ แต่ละตัวส่งต่อ (forward) ข้อมูลที่ต้องการส่งไปยังเส้นทางที่ถูกต้อง

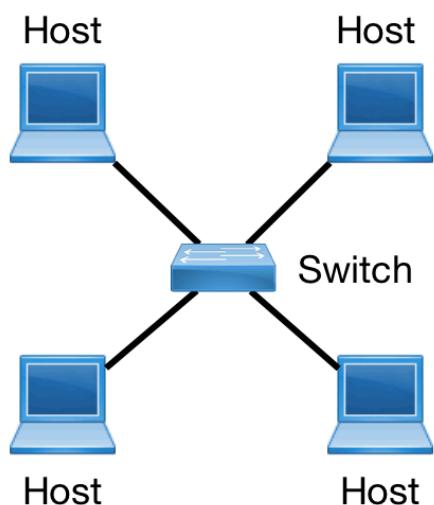
Contents

- Applications
- Internet
- Standard
- Network Component
- Network Architecture
- Network Categories
- Network Topology



Topology : Mesh

ໂທໂປໂລຢີແບບແນ່ງ (mesh) ເປັນການເຊື່ອມຕ່ວເຄືອຂ່າຍແບບ ຈຸດຕ່ອຈຸດໂດຍທີ່ໂທນດແຕ່ລະຕ້ວຈະເຊື່ອມດ້ວຍ ສື່ອຈຳນວນສູງສຸດ $g(g+1)/2$ ເສັ້ນ ຂໍອົດຂອງການເຊື່ອມຕ່ວແບບແນ່ງດີ່ວ່າ ບົກລິລະອະນຸມັດ ຂອງສາຍຈະສູງ ໃນ ກຣີນີທີ່ ສາຍເສັ້ນ ໄດ້ຂາດ ສາມາດຕຽບສອບໄດ້ທັນທີ ອີກທັງໝົດ ມີກະຮບກັນ ອຸປະກອນໜີ່ໃໝ່ ໃນເຄືອຂ່າຍ ປລອດກັບຈາກ ການດັກຟັງຫຼືອໍາໂມຍຂໍ້ອມມູລ ເນື່ອຈາກເຊື່ອມຕ່ວແບບຈຸດຕ່ອຈຸດແຕ່ຕັ້ນຖຸນທາງດ້ານສາຍຄ່ອນຂ້າງສູງ ເນື່ອຈາກ ຕ້ອງລົງຖຸນເພື່ອຊື້ອສາຍຈຳນວນມາດ ກາກເຄືອຂ່າຍມີຂາດ ໃຫຍຸ້ ຂຶ້ນແລ້ວ ຈະດູແລຍກຍິ່ງຂຶ້ນ



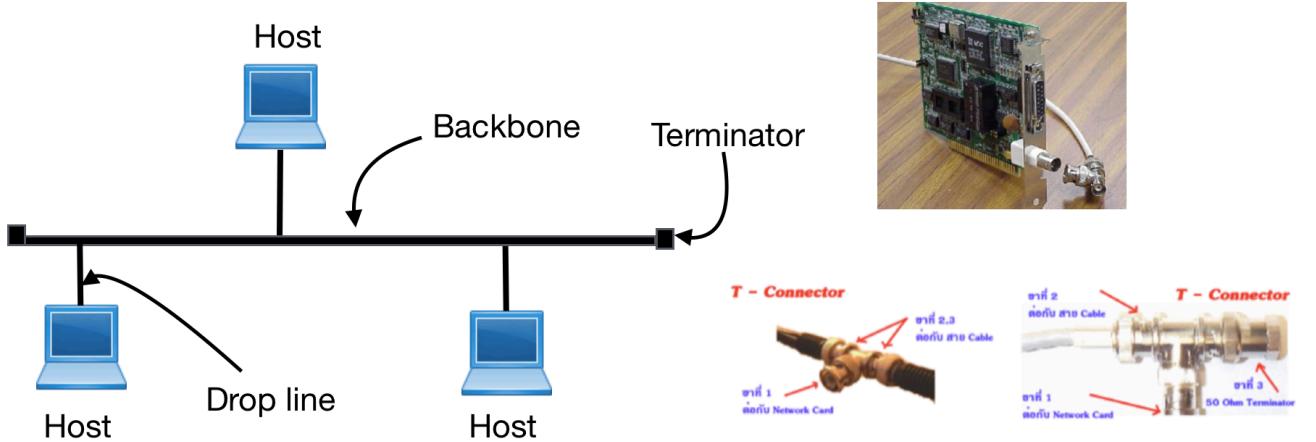
Topology : Star



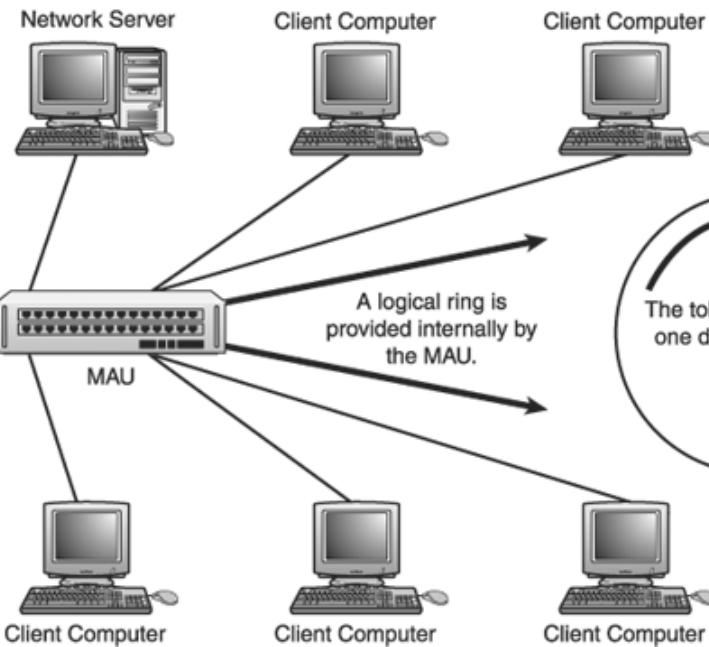
Switch

- โทโพโลยีแบบดาว (star) เป็นการเชื่อมโยงเครือ ข่ายแบบจุดต่อจุดที่มีศูนย์กลาง (centralized point-to-point) โดยที่อุปกรณ์ทุกๆ ตัวต้องเชื่อมต่อ กับอุปกรณ์ ส่วนกลาง โดยอาจจะเป็นฮับ (hub) หรือสวิตช์ (switch)
- การเชื่อมต่อแบบดาวมีข้อจำกัดคือ อาจจะเกิด ปัญหาคอขวดที่ หับหรือสวิตช์เนื่องจากข้อมูลทั้งหมด จะถูก ส่งผ่านมาที่ อุปกรณ์นั้นจุดเดียว หากหับเกิดความล้มเหลว ระบบเครือข่ายจะหยุดการทำงาน ทั้งหมด ซึ่งเป็นปัญหา single point of failure อีกทั้งอาจจะเกิดการดักฟังได้ หรือ ไม่เข้าอยู่กับ คุณสมบัติของอุปกรณ์ ค่า ใช้จ่าย (cost) จาก สายส่งจะน้อยลง เมื่อเปรียบเทียบกับ โทโพโลยีแบบ แมงมุม แต่ ถ้าเครือข่าย ใหญ่ขึ้น อาจจะส่งผลกระทบต่อ อุปกรณ์ ต่างๆ และ ความเร็วของ เครือข่าย โดยรวม

Topology : Bus



- โทปโโลยีแบบบัส (bus) เป็นการเชื่อมต่อแบบ หลายจุด (multipoint) โดยเครือข่ายจะมีลิงค์หลัก เรียกว่า แบคโบน (backbone) หลังจากนั้นอุปกรณ์ต่างๆ จะเชื่อมต่อ กับแบคโบนนั้น โดยจุดเชื่อม ต่อระหว่างแบคโบนเรียกว่า แทป (tap) และสายที่เชื่อมระหว่างแทปและอุปกรณ์คือdropline ในขณะที่ปลายสายของแบคโบนนั้นจะมี terminator อยู่ทั้งสองฝั่ง เพื่อลดการสะท้อนของ สัญญาณทาง ไฟฟ้า
- การเชื่อมต่อแบบบัสนั้น utilization ของเครือ ข่ายจะต่ำเนื่องจากแต่ละช่วงเวลาจะมีเพียงคู่สันทนา เดียวเท่านั้นที่สามารถเข้า ใช้สายได้ ถ้าหากแบคโบนขาด แล้วเครือข่ายจะถูกแยกออกเป็นสองกลุ่ม เครือข่าย แต่ละส่วน (segment) ยังสามารถสื่อสารกันได้ นอกจากนี้ ต้นทุนของสายจะต่ำกว่า แต่ถ้า จำนวนโหนดที่เชื่อมต่อมาก ยิ่งขึ้น การลดthonของสัญญาณจะมากยิ่งขึ้น และ utilization จะต่ำลง



Topology : Ring

โทปโลยีแบบวงแหวน (ring) เป็นการเชื่อมต่อเครือข่ายเป็นวงกลมซึ่งเชื่อมต่อแบบหลาย จุด โดยจุด เชื่อมต่อเรียกว่า repeater โหนดแต่ละตัวหากต้องการส่งข้อมูลต้องได้รับลิทธ์ในการ เชื่อมต่อผ่านตัว (token หรือ ticket) โหนดใดๆ ที่มีตัวสามารถส่งข้อมูลได้ เมื่อส่งเสร็จแล้ว ตัวจะ ถูกส่งต่อไปยังอุปกรณ์ ต่อไป ในวง สำหรับ utilization การเชื่อมต่อแบบนี้มีค่าต่ำ เช่นเดียวกันกับบัส เนื่องจากต้อง ใช้ช่อง สัญญาณร่วมกันกับโหนดอื่นๆ อีกทั้งต้องรอตัวเพื่อรับลิทธ์ ในการส่งข้อมูล นอกจากนี้การตัดฟังสามารถ เกิดขึ้นได้ ถ้าหากเครือข่ายมีขนาดใหญ่แล้วนั้น การรอคิวสำหรับส่ง ข้อมูลจะมีเวลามากยิ่งขึ้น

Notes

Module 2

Data Communication

Data communication is data transmission from node to other node via media

การสื่อสารข้อมูล (data communication) หมายถึง การรับส่งข้อมูลระหว่างโหนด (Node) ผ่านลีอต่างๆ เช่น การสั่งพิมพ์เอกสารจากเครื่องคอมพิวเตอร์ไปยังเครื่องพิมพ์ การพิมพ์ข้อความ ทางแป้นพิมพ์ การส่งไฟล์จากเครื่องคอมพิวเตอร์หนึ่งๆ ไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ เป็นต้น การรับส่งข้อมูลต่างๆ เหล่านั้น ต้องส่งผ่านลีอกลางอย่างน้อยหนึ่งอย่าง เช่น สาย universal serial bus (USB), สายสัญญาณ ต่างๆ หรือการสื่อสารแบบไร้สาย เป็นต้น

Objectives

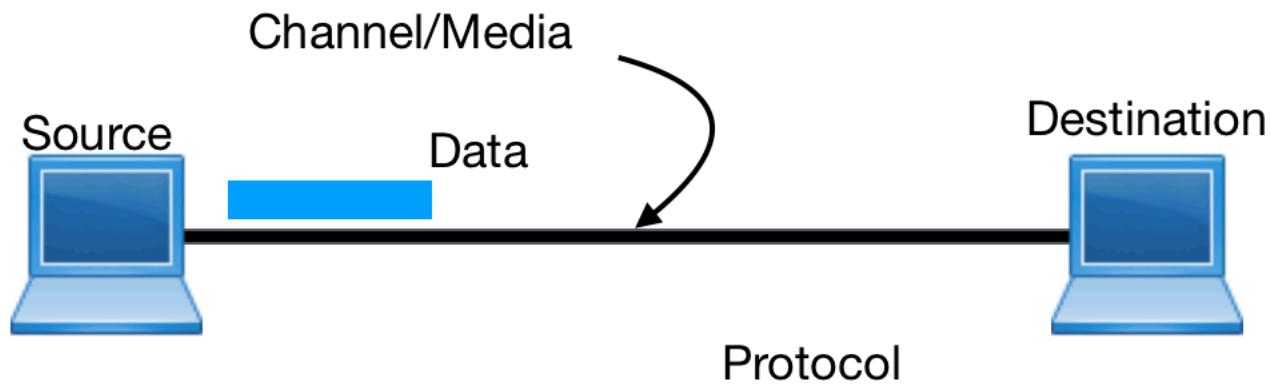
- Accuracy
- Delivery
- Realtime
 - Non-realtime
 - Soft Realtime
 - Hard Realtime

- การสื่อสารข้อมูลข้างต้นมีเป้าหมายที่สำคัญ 3 ประการได้แก่ ความแม่นยำ ความถูกต้อง และทันเวลา ซึ่งอธิบายได้ดังนี้
 - ความถูกต้องของข้อมูล (accuracy) ข้อมูลที่ถูกส่งจากต้นทางและข้อมูลที่รับโดยปลายทางนั้นต้องเหมือนกัน ข้อมูลต้องไม่ผิดเพี้ยน เช่น เครื่องคอมพิวเตอร์ A ส่งข้อความ "สวัสดี" ไปยังเครื่องคอมพิวเตอร์ B ทางคอมพิวเตอร์ B ต้องได้รับข้อความ "สวัสดี" เท่านั้นเมื่อเจ้าของข้อความอื่นๆ ได้เป็นต้น นอกจากนี้ ลำดับของข้อมูลจะต้องไม่สลับตำแหน่งกัน เช่น เครื่องคอมพิวเตอร์ A ส่งข้อความ "ABCDE" ไปยังเครื่องคอมพิวเตอร์ B ทางเครื่องคอมพิวเตอร์ B ต้องได้รับข้อความ "ABCDE" เท่านั้น ไม่สามารถเป็น "EDCBA" ได้ เป็นต้น
 - ความถูกต้องของการขนส่ง (delivery) การส่งข้อมูลทุกครั้งต้องระบุตำแหน่งของผู้รับ เสมอ การสื่อสารข้อมูลต้องส่งข้อมูลไปยังปลายทางที่ถูกต้อง เช่น เครื่องคอมพิวเตอร์ A ส่งข้อมูลไปยังเครื่องคอมพิวเตอร์ B ข้อมูลที่ส่งไปนั้นต้องถูกส่งไปถึงเครื่องคอมพิวเตอร์ B เท่านั้น ถึงแม้ว่าข้อมูลที่ส่งไปถูกต้อง แต่ผิดเป้าหมายดังนั้นการสื่อสารข้อมูลดังกล่าวถือว่าไม่ถูกต้อง

- Accuracy
- Delivery
- Realtime
 - Non-realtime
 - Soft Realtime
 - Hard Realtime

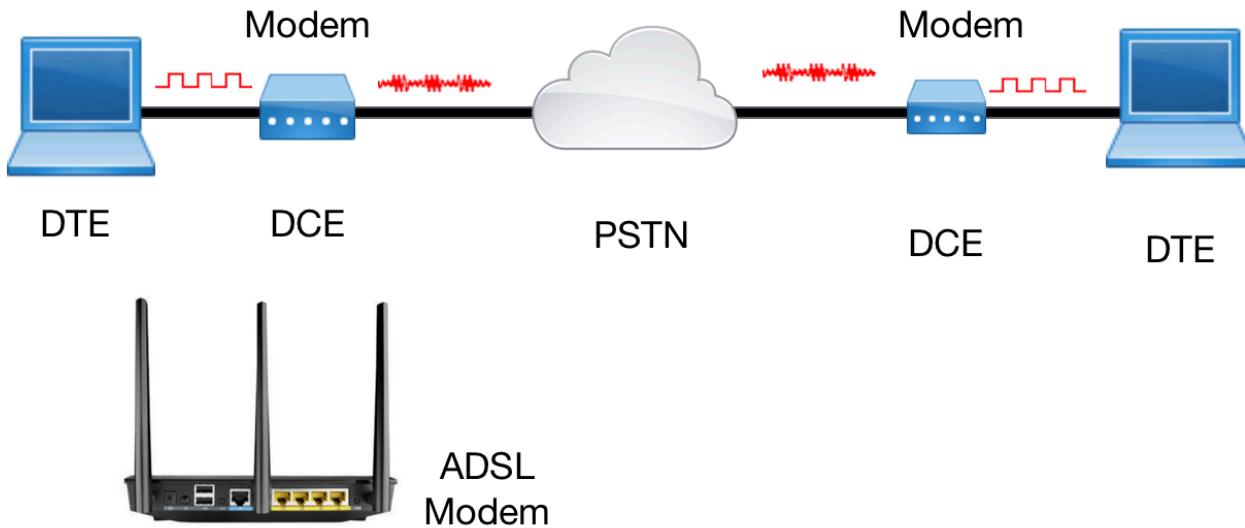
- การสื่อสารข้อมูลข้างต้นมีเป้าหมายที่สำคัญ 3 ประการได้แก่ ความแม่นยำ ความถูกต้อง และทันเวลา ซึ่งอธิบายได้ดังนี้
 - เวลาที่เหมาะสม (timeliness) เงื่อนไขของเวลาเป็นประเด็นที่สำคัญของการสื่อสาร ข้อมูลเนื่องจากไม่มีเครื่องฝ่ายรับใดๆ สามารถรอคอยข้อมูลได้ตลอดไป ข้อมูลที่ส่งจากต้นทาง นั้นต้องไปถึงปลายทางให้ทันเวลาหรือเรียลไทม์ (realtime) การทันเวลานั้นแบ่งออกเป็น 3 แบบ ได้แก่ none-realtime, soft realtime และ hard realtime
- การทันเวลาทั้ง 3 แบบนี้มีจุดพิจารณาของ เวลาที่ได้รับข้อมูลเป็นหลัก กล่าวคือ การส่งข้อมูล แบบ none-realtime นั้นจะไม่พิจารณาถึงเวลา ไม่ว่าข้อมูลจะถึงปลายทางก่อนหรือหลังจุดของเวลาที่กำหนด
 - ข้อมูลชุดนั้นต้องส่งไปถึงทางฝ่ายรับ และยอมรับข้อมูลชุดนั้นได้ ถ้าฝ่ายรับต้องการข้อมูล ณ เวลาใดๆ แล้วข้อมูลอาจจะมาถึงก่อนหรือหลังจุดของเวลา นั้น แต่เครื่องปลายทางยังสามารถ ประมวลผลข้อมูลนั้นได้ ถือว่าการสื่อสารข้อมูลดังกล่าวสมบูรณ์ จึงถือว่าเป็น soft realtime แต่ถ้า หาก ข้อมูลนั้นต้องมาถึงปลายทาง ณ เวลา นั้นๆ เท่านั้น มาก่อนหรือหลังจุดของเวลาไม่ได้ หากผิดเงื่อนไขถึงว่าการสื่อสารนั้นไม่สมบูรณ์ กรณีข้างต้นถือว่าเป็น hard realtime เป็นต้น
 - เวลาที่ใช้ในการรับส่งนั้นสำคัญต่อการสื่อสารข้อมูลคอมพิวเตอร์ เนื่องจากข้อมูลที่ถูกส่งมา จาก เครื่องต้นทางนั้น ต้องจัดเก็บไว้ในเครื่องปลายทางจนครบทุกส่วนก่อน เพื่อ ใช้ในการประมวลผล ข้อมูลนั้นๆ ถ้าข้อมูลมาถึงเครื่องปลายทางเร็วเกินไป เครื่องปลายทางต้องเลี้ยห่วงความจำ ใน การจัดเก็บข้อมูลส่วนนั้นก่อน

Components



การสื่อสารข้อมูลทางคอมพิวเตอร์นั้นหากจะให้สมบูรณ์ต้องประกอบด้วยองค์ประกอบต่างๆ ได้แก่ ต้นทาง (source), ปลายทาง (destination), ข้อมูล (data), ช่องทางสื่อสาร (channel/ media) และ โพรโตคอล (protocol)

Source/Destination



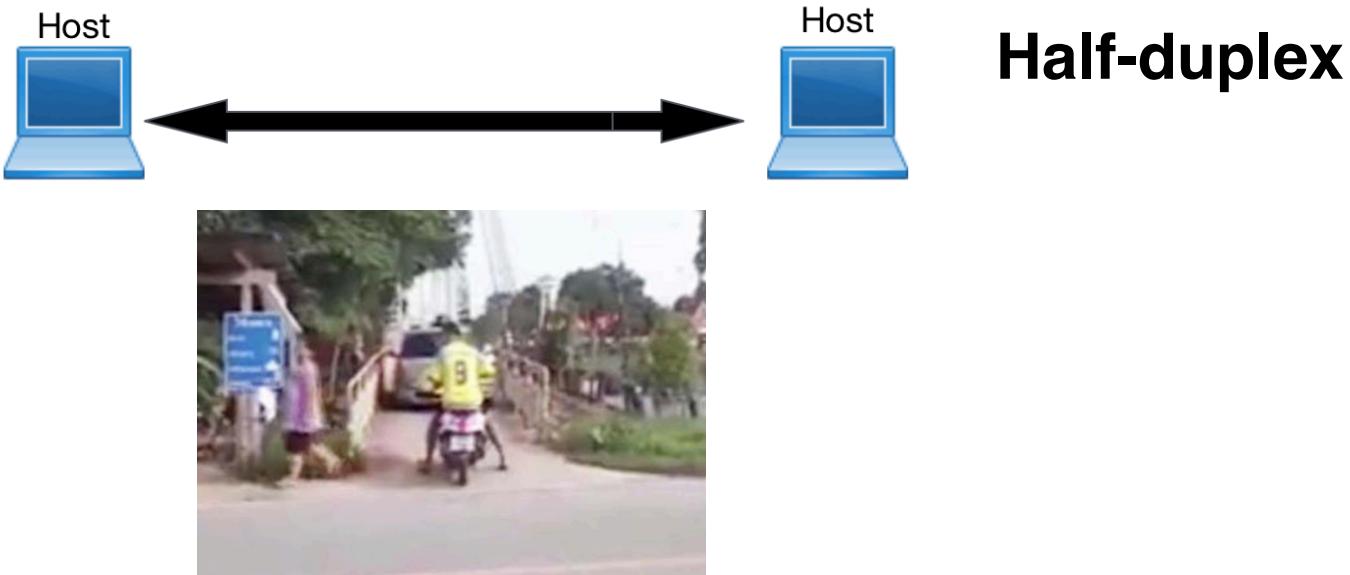
- ต้นทาง (source) / ปลายทาง (destination) ของการสื่อสารข้อมูลคอมพิวเตอร์นั้นได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย เครื่องพิมพ์ อุปกรณ์รีโมทต่างๆ ซึ่งครอบคลุมถึง มือถือ แท็บเล็ต เป็นต้น อุปกรณ์บางชนิดสามารถเป็นได้ทั้งอุปกรณ์ต้นทางและอุปกรณ์ปลายทาง แต่ อุปกรณ์บางชนิดเป็นได้เฉพาะเครื่องปลายทาง เช่น เครื่องพิมพ์ เป็นต้น (แต่ถ้าพิจารณาถึงฟังก์ชันการทำงาน เชิงลึกแล้ว อาจจะเป็นได้ทั้งโน๊ตบุ๊คต้นทางและโน๊ตบุ๊คปลายทาง)
- การสื่อสารคอมพิวเตอร์แบ่งอุปกรณ์ออกเป็น 2 ประเภทได้แก่
 - Data Terminal Equipment หรือ DTE เป็นอุปกรณ์ที่กำเนิดแหล่งข้อมูลหรือรับข้อมูล ได้แก่ เครื่องคอมพิวเตอร์ เครื่องพิมพ์ อุปกรณ์มือถือ เป็นต้น
 - Data Communication Equipment หรือ DCE เป็นอุปกรณ์ที่ใช้ในการสื่อสารข้อมูล ซึ่งเชื่อมต่อจาก DTE เช่น โมเด็ม หรืออุปกรณ์เครือข่ายต่างๆ เป็นต้น
- อุปกรณ์ทั้งสองส่วนจะเชื่อมโยงกันผ่านลีโอ เช่น เครื่องคอมพิวเตอร์ (ตัวแทนของ DTE) ส่ง ข้อมูลผ่าน อีเธอเรเน็ตการ์ด (เป็นตัวแทนของ DCE) หลังจากนั้น DCE ทั้งสองฝั่งจะเชื่อมต่อด้วยลีโอ อาจจะเป็น แบบมีสายหรือไร้สายซึ่งเป็นเครือข่ายสาธารณะ (public switched telephone network หรือ PSTN) ในปัจจุบันอาจจะใช้เป็น ใยแก้วนำแสง (fiber optic) แทน ซึ่งอีกฝั่งของ การสื่อสารจะมี DCE และ DTE เชื่อมโยงด้วยกันเช่นเดียวกันกับฝ่ายส่ง
- การสื่อสารข้อมูลผ่านเครือข่ายสาธารณะเป็นการส่งข้อมูลจาก เครื่องคอมพิวเตอร์ ซึ่งแทน ข้อมูลรูปแบบสัญญาณแบบดิจิทัล (digital data representation) หลังจากนั้นข้อมูลจะถูกแปลงเป็น สัญญาณอะนาล็อก (analog signal) ด้วยอุปกรณ์ที่เรียกว่า โมเด็ม (modem) สัญญาณจะน่าจะ ลือกส่งผ่าน เครือข่ายสาธารณะ เช่น ระบบโทรศัพท์ หรือ สาย ใยแก้วนำแสง เพื่อสัญญาณไฟฟ้าส่ง ถึงปลายทาง แล้ว โมเด็มที่เครื่องปลายทาง แปลงสัญญาณอะนาล็อก เป็นสัญญาณดิจิทัล (digital signal) และ แปลงเป็นข้อมูลดิจิทัล (digital data) เพื่อนำไปประมวลผล ในคอมพิวเตอร์ ในลำดับ ถัดไป

Simplex



- การให้หลังของข้อมูลระหว่างต้นทางและปลายทางนั้น มี 3 รูปแบบได้แก่ simplex, half-duplex และ full-duplex ซึ่งแต่ละรูปแบบการสื่อสารมี คุณลักษณะดังนี้
- การให้หลังของข้อมูลแบบซิมเพล็กซ์ (simplex data flow) หมายถึง การสื่อสารทางเดียว โดยที่อุปกรณ์ที่เชื่อม ต่อหนึ่นมีหน้าที่สำหรับส่งข้อมูลหรือรับข้อมูลเท่านั้น เช่น การพิมพ์งานไปยังเครื่องพิมพ์ ซึ่งเครื่องคอมพิวเตอร์เป็นฝ่ายส่ง และเครื่องพิมพ์เป็นฝ่ายรับเท่านั้น

Data Flow



การให้ของข้อมูลแบบhalf duplex (half duplex data flow) หมายถึง การสื่อสารกึ่งสองทาง ที่ อุปกรณ์ทั้งสองฝ่ายสามารถเป็นทั้งฝ่ายส่งและฝ่ายรับ แต่ใน ช่วงเวลาหนึ่งๆ จะมีเพียงฝ่ายใดฝ่ายหนึ่ง สามารถส่งข้อมูลได้ เท่านั้น เช่น วิทยุสื่อสารของตำรวจ ขณะที่ฝ่ายส่งกำลังส่ง ข้อมูลนั้น ทางฝ่ายรับทำ หน้าที่ได้เพียงรับข้อมูลเท่านั้น ไม่ สามารถส่งข้อมูลได้ ต้องรอจนกว่าทางฝ่ายส่งส่งข้อมูล เสร็จก่อนแล้ว ทางฝ่ายรับจะเปลี่ยนเป็นฝ่ายส่งข้อมูลแทน

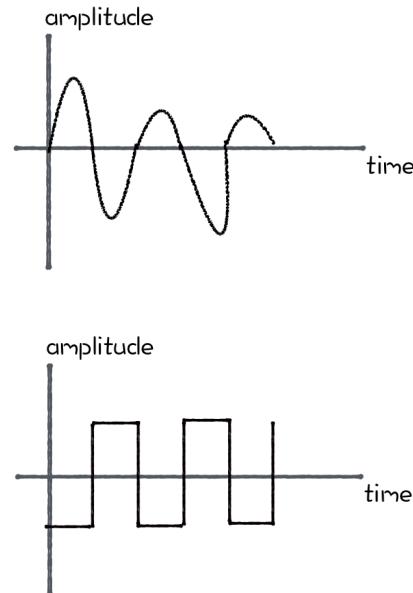
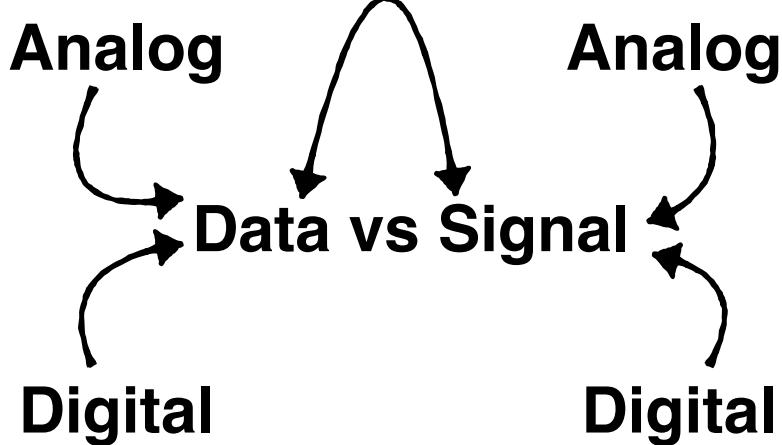


Full-duplex

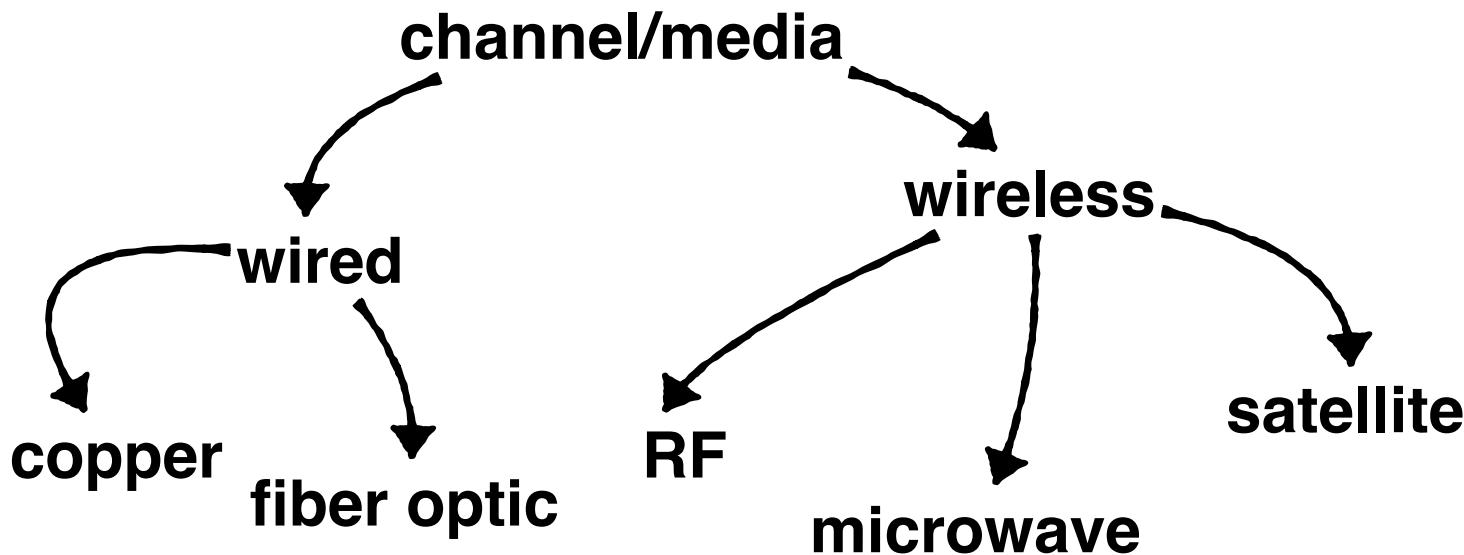


การไหลของข้อมูลแบบฟูลดูเพล็กซ์ (full duplex data flow) หมายถึง การสื่อสารสองทาง ที่ทั้งฝ่ายส่ง และ ฝ่ายรับสามารถรับส่งข้อมูลพร้อมกันได้ ในช่วงเวลาเดียวกัน เช่น การคุยโทรศัพท์มือถือ ทั้งสองฝ่ายสามารถพูดและฟัง โทรศัพท์ได้พร้อมกัน ในช่วงเวลาเดียวกัน

Conversion

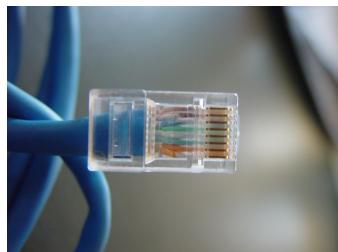
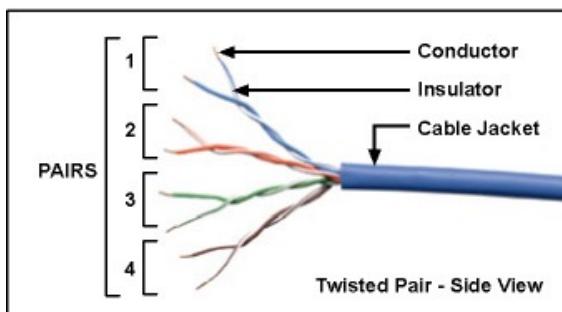


- ข้อมูล (Data) ได้แก่ ภาพ ข้อความ หรือสื่ออิเล็กทรอนิกซ์ใดๆ ที่แทนในรูปแบบของสัญญาณทางไฟฟ้า หลังจากนั้นนำส่งสัญญาณจากต้นทางไปยังปลายทาง โดยข้อมูลจะแบ่งออกเป็น 2 แบบ ได้แก่ ข้อมูลดิจิทัล และข้อมูลอนาล็อก ซึ่งข้อมูลแต่ละแบบมีคุณลักษณะดังนี้
- สัญญาณอนาล็อก (Analog Signal) เป็นสัญญาณแบบต่อเนื่อง มีการเปลี่ยนแปลงระดับ สัญญาณตามขนาดของแรงดันไฟฟ้าและความถี่ของสัญญาณนั้น เช่น สัญญาณเสียงพูด ข้อดีของสัญญาณอนาล็อกคือส่งสัญญาณได้ไกล แต่ถูก grub กวนได้ง่าย หากมีสัญญาณ grub กวนมาจะส่งผลให้ข้อมูลที่ได้รับผิดพลาด
- สัญญาณดิจิทัล (Digital Signal) เป็นสัญญาณที่มีการแทนด้วยระดับสัญญาณเป็น 0 หรือ 1 ซึ่งสัญญาณดิจิทัลนี้ใช้ในระบบคอมพิวเตอร์ ข้อดีของสัญญาณดิจิทัลคือความน่าเชื่อถือสูง และมีข้อจำกัดคือ หากส่งข้อมูลต่อไปในระยะไกลออกไปข้อมูลจะมีความผิดเพี้ยนได้ง่าย จึงต้องมีกระบวนการสร้างสัญญาณขึ้นใหม่

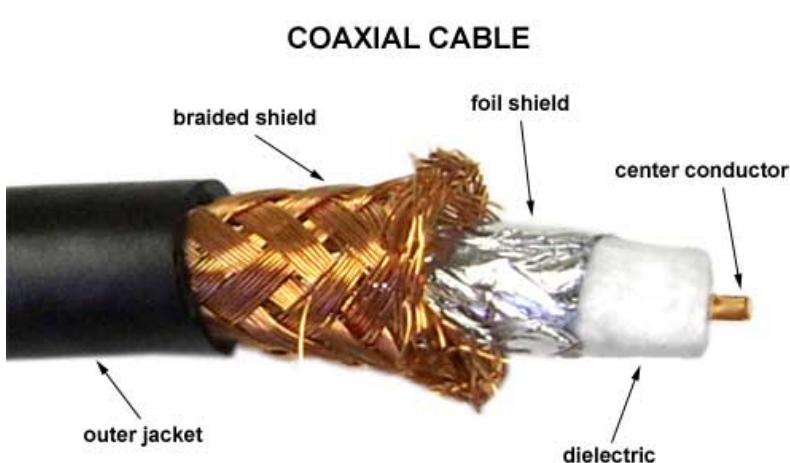


- ช่องทางลีอสาร เป็นตัวกลางส่งข้อมูลหรือเส้นทางที่ใช้ในการลีอสาร เพื่อนำข้อมูลจาก ต้นทาง ไปยังปลายทาง โดยตัวกลางแบ่งออกเป็น 2 ประเภทได้แก่ สื่อแบบมีสาย และสื่อแบบไร้สาย
 - ตัวกลางแบบมีสาย (Wired Media) เป็นตัวกลางที่ส่งสัญญาณทางไฟฟ้าผ่านวัสดุนำไฟฟ้า ได้แก่ ทองแดง หรือส่งข้อมูลด้วยแสง ตัวอย่างเช่น สายโอดแคกเชียล สายตีเกลี่ยวคู่ หรือ ไนแก้วนำแสง เป็นต้น
 - ตัวกลางแบบไร้สาย (Wireless Media) เป็นตัวกลางที่ส่งสัญญาณทางไฟฟ้าผ่านคลื่นแม่เหล็กไฟฟ้า เช่น คลื่นไมโครเวฟ ดาวเทียม คลื่นวิทยุ เป็นต้น

twisted pair

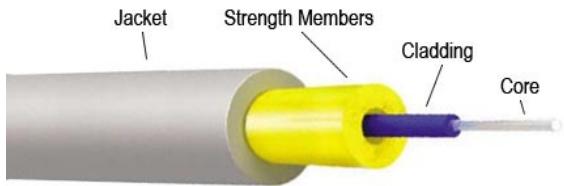


Channel/Media

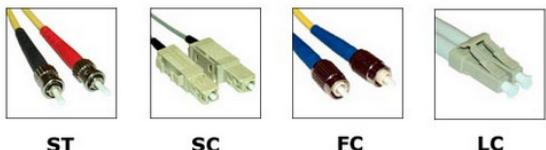
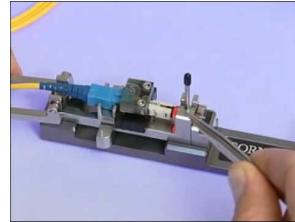


coaxial





Fiber optics



ST **SC** **FC** **LC**



MPO **ESCON** **MTRJ** **VF45**

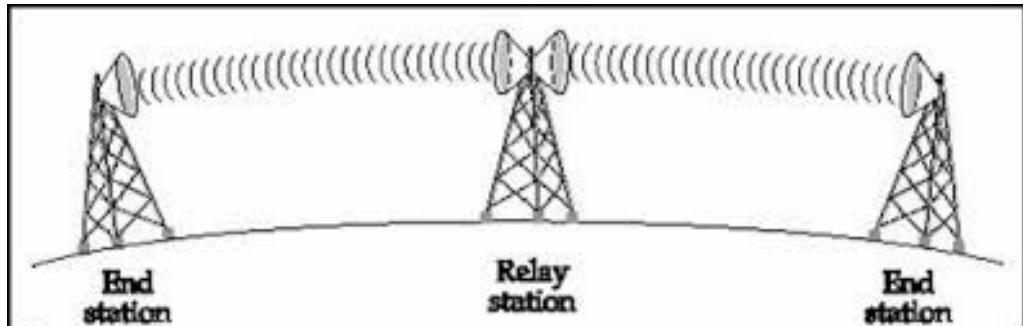
Radio Frequency (RF)



- Bluetooth based on IEEE 802.15.1 Standard
- WiFi based on IEEE 802.11 Standard

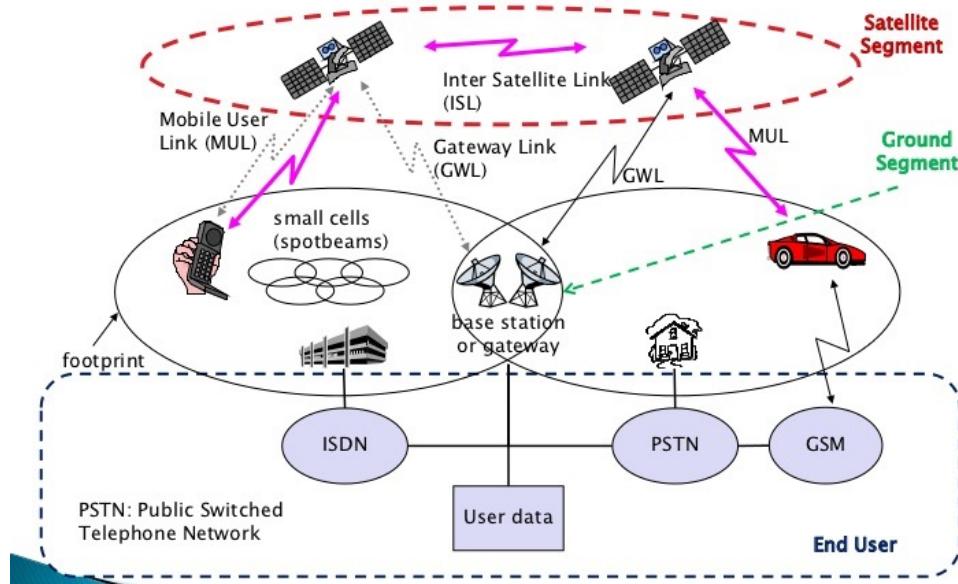


Terrestrial Microwave



- Point-to-Point communication
- Send microwave to next hop directly

Satellite System



Notes

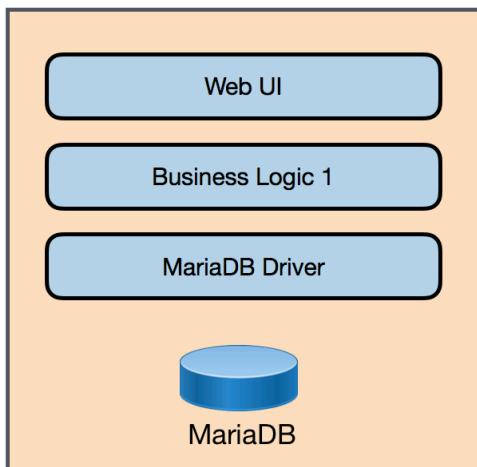
Module 3.

Network Architecture

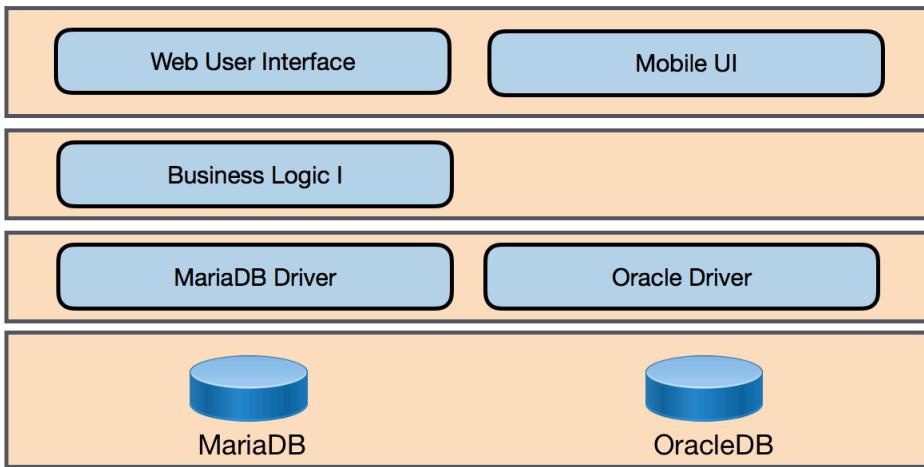
- Layer Architecture
- OSI Model
- TCP/IP Model
 - Network Access Layer
 - Internet Layer

Layer Architecture

Application A

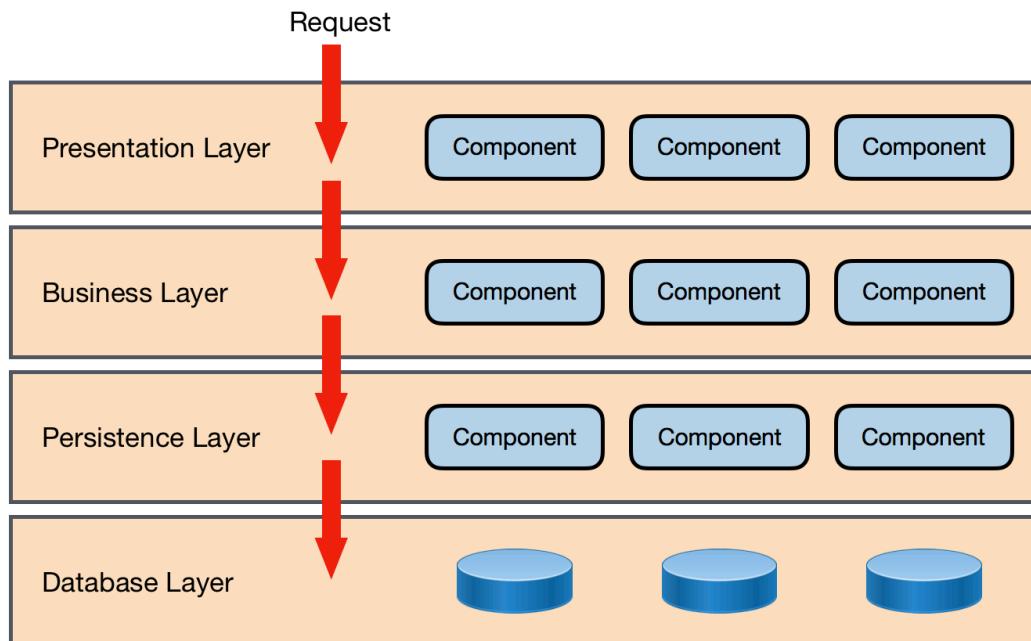


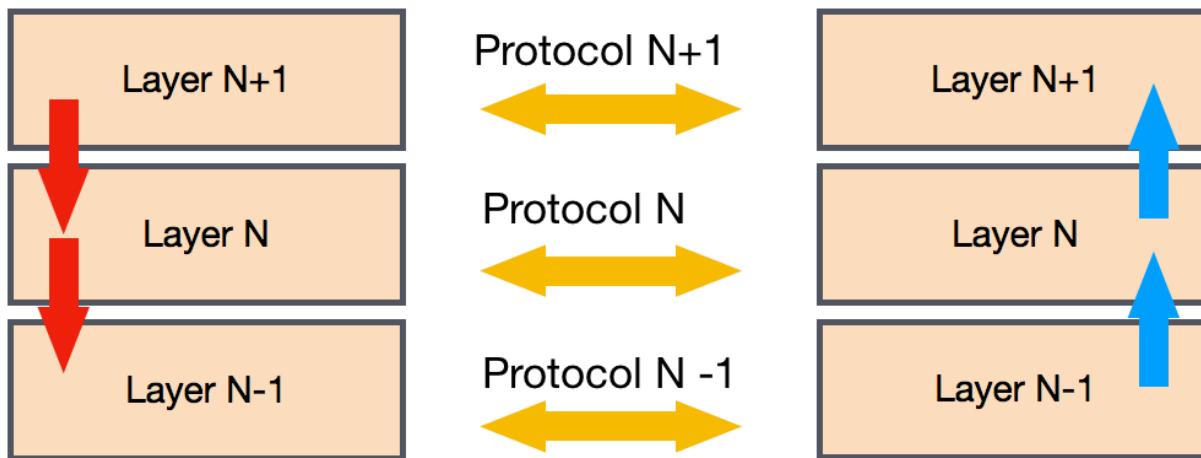
Application B



- การออกแบบและพัฒนาระบบ ได้ฯ หากระบบนั้นๆ มีขนาดเล็กการออกแบบระบบทำได้ง่ายเนื่องจากไม่ซับซ้อน
- แต่ถ้าระบบมีขนาดใหญ่ขึ้น ความซับซ้อนมากขึ้น ความหลากหลายของอุปกรณ์ที่เกี่ยวข้องมีมากขึ้น การออกแบบระบบที่จะให้ครอบคลุมทุกๆ อุปกรณ์นั้นเป็นไปได้ยากมาก
 - การพัฒนาระบบ ให้บริการข้อมูลผ่านเว็บ หากต้องการให้ระบบที่พัฒนาขึ้นนั้นสามารถใช้งานได้ทุกๆแพลตฟอร์ม ต้องวิเคราะห์โปรแกรมอย่างละเอียด ถ้าหากวันใดมีแพลตฟอร์มใหม่ๆ เกิดขึ้น ระบบที่ได้ออกแบบมาหนึ่งจะต้องมีการปรับเปลี่ยนให้เหมาะสมกับอุปกรณ์นั้นๆ เพื่อ ให้การออกแบบและพัฒนาระบบสำหรับเครือข่ายเป็นไปได้ง่ายยิ่งขึ้น
- ตัวแบบเครือข่ายแบบชั้น หรือสถาปัตยกรรมแบบชั้น (Layer Architecture) จึงถูกเลือก ใช้สำหรับการออกแบบและพัฒนา ซอฟต์แวร์เครือข่ายต่างๆ

Layer Architecture





สถาปัตยกรรมแบบชั้น ประกอบไปด้วย 3 องค์ประกอบที่สำคัญได้แก่ ชั้น (Layer), โพรโตคอล (Protocol), และ Interface โดยแต่ละองค์ประกอบมีรายละเอียดดังนี้

- **ชั้น (Layer)** เป็นการแบ่งงานทั้งระบบออกเป็นส่วนย่อย เพื่อลดความซับซ้อนในการจัดการ ติดต่อสื่อสารข้อมูล โครงสร้างของการสื่อสารข้อมูลภายในอุปกรณ์ต่างๆ ส่วนใหญ่จะถูกแบ่งย่อย โดยระบุการทำงานอย่างละเอียด โดยแต่ละชั้นเป็นอิสระต่อกัน ทุกๆ ฟังก์ชันการทำงานจะอิงตาม มาตรฐานต่างๆ ที่เคยกำหนดไว้ หรืออาจจะสร้างมาตรฐานใหม่ๆ ขึ้นมา จำนวนของชั้นจะมากหรือน้อยขึ้นอยู่กับความซับซ้อนของงาน
- **โพรโตคอล (Protocol)**
- **อินเทอร์เฟส (Interface)** เป็นช่องทางการเชื่อมต่อระหว่างชั้น ขึ้นอยู่กับว่า การออกแบบแต่ละชั้นแตกต่างกันอย่างไร ต้องการข้อมูลอะไรสำหรับการประมวลผล

แนวคิดของสถาปัตยกรรมชั้นแสดงในภาพอธิบายได้ว่า แต่ละชั้นนั้นมีฟังก์ชันการทำงานที่แตกต่างกัน และอิสระออกจากกัน โดยชั้นที่ N จะให้บริการแก่ชั้นที่ N+1 และใช้บริการชั้น N-1 โดยแต่ละชั้นนั้นจะสื่อสารผ่านอินเทอร์เฟส สำหรับชั้นที่ติดกันจะสื่อสารด้วยโพรโตคอลเฉพาะ ในชั้นนั้นๆ เช่นชั้นที่ N จะสื่อสารกันด้วยโพรโตคอล N เท่านั้น หากโพรโตคอลที่ N-1 หรือ N+1 เปลี่ยนแปลงไปจะไม่กระทบกับโพรโตคอลที่ N

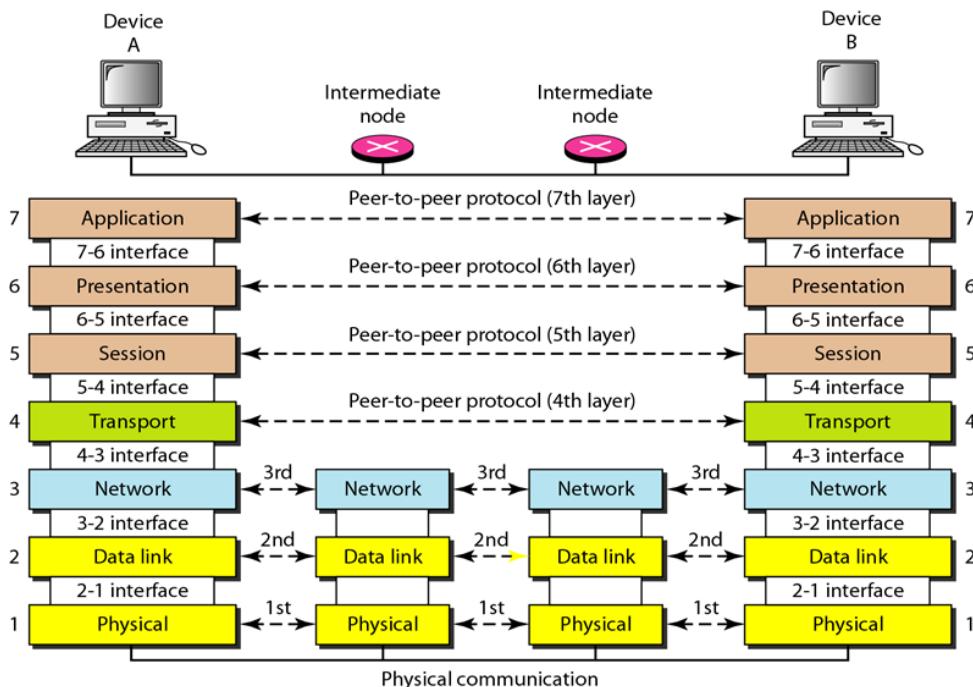
Layer Architecture



Contents

- Layer Architecture
- OSI Model
- TCP/IP Model
 - Network Access Layer
 - Internet Layer

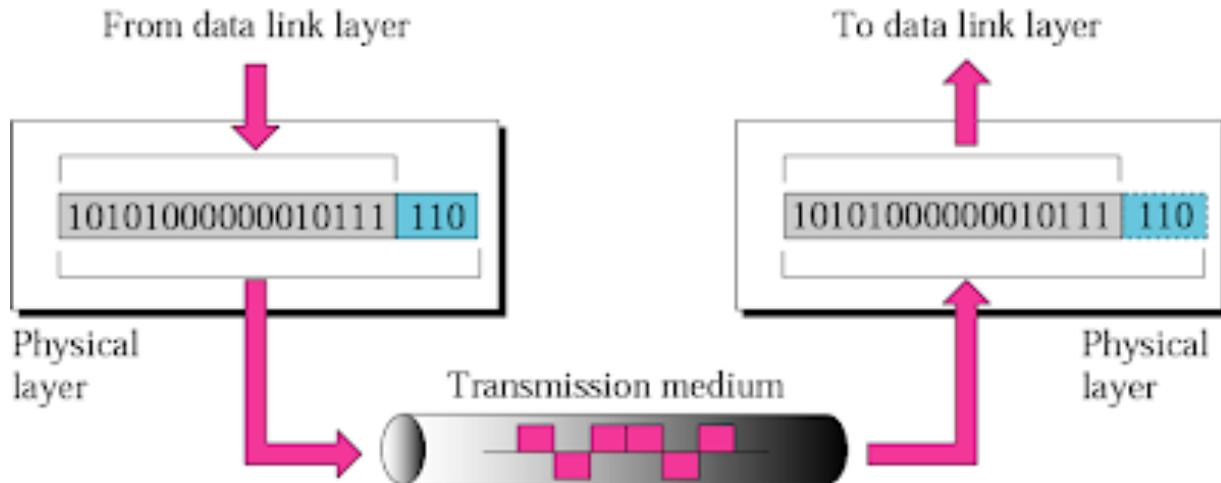
OSI Model



องค์กร ISO ซึ่งย่อมาจาก International Standard Organization เป็นองค์กรที่กำหนดมาตรฐานต่างๆ ระดับนานาชาติ ได้กำหนดข้อตกลงเกี่ยวกับการออกแบบและพัฒนาระบบเครือข่ายคอมพิวเตอร์ โดยเสนอตัวแบบ Open System Interconnection หรือ OSI Model โดยที่ OSI เป็นสถาปัตยกรรมแบบชั้นประกอบด้วยกันทั้งหมด 7 ชั้น ซึ่งเรียงลำดับจากบนลงล่าง ดังนี้

- **Application Layer** เป็นชั้นที่อยู่ใกล้ชิดกับผู้ใช้งานที่สุด ใช้สำหรับการเข้าถึงทรัพยากรต่างๆ ของระบบเครือข่าย เช่น www, Email, พิมพ์ หรือ ไฟล์ร่วมกัน เป็นต้น
- **Presentation Layer** เป็นชั้นที่กำหนดรูปแบบการแทนข้อมูล ในระบบคอมพิวเตอร์ได้แก่ ข้อความซึ่งหมายถึงการเข้ารหัสข้อมูลแบบ unicode, utf-8, utf-16 หรือภาษาใดๆ เป็นต้น การเข้ารหัสเสียง แบบ mp3, การเข้ารหัสภาพแบบ jpeg, png หรือบิทเมพ เป็นต้น หรือการเข้ารหัสวิดีโอแบบ mp4 เป็นต้น
- **Session Layer** เป็นชั้นที่กำหนดถึงการเริ่มหรือหยุดการเชื่อมต่อ การจัดการการเชื่อมต่อระหว่างโปรแกรมเครือข่ายต่างๆ เช่น การโหลดไฟล์ผ่านเว็บแต่ละไฟล์นั้นมีตัวควบคุมอย่างไรที่ป้องกันเนื้อหาของไฟล์ภายนั้นไม่ให้มีความผิดพลาด เป็นต้น
- **Transport Layer** เป็นการควบคุมการให้หลังของข้อมูล ในระดับของโปรเซส โดยเน้นการสื่อสารข้อมูลที่มีความน่าเชื่อถือ ถูกต้อง โดยเพิ่มกระบวนการตรวจสอบความถูกต้อง หรือกระบวนการส่งข้อมูลช้า ในกรณีที่ข้อมูลที่ได้รับมีความผิดพลาด เป็นต้น
- **Network Layer** เป็นการควบคุมกระบวนการรับส่งข้อมูลระหว่างโหนด โดยมีการกำหนดเลขที่อยู่ การค้นหาเส้นทาง เป็นต้น
- **Data Link Layer** เป็นการควบคุมกระบวนการรับส่งข้อมูลระหว่างโหนดที่อยู่ติดกัน โดยเน้นการควบคุมการให้หลังของข้อมูล ตรวจสอบข้อมูลหาย ช้า หรือเสียหายจากการรับ-ส่งข้อมูล เป็นต้น
- **Physical Layer** เป็นการควบคุมการส่งข้อมูล ในระดับของสัญญาณ โดยแปลงข้อมูลเป็นสัญญาณไฟฟ้าเพื่อส่งผ่านสื่อทั้งแบบมีสายและไร้สาย

Physical Layer

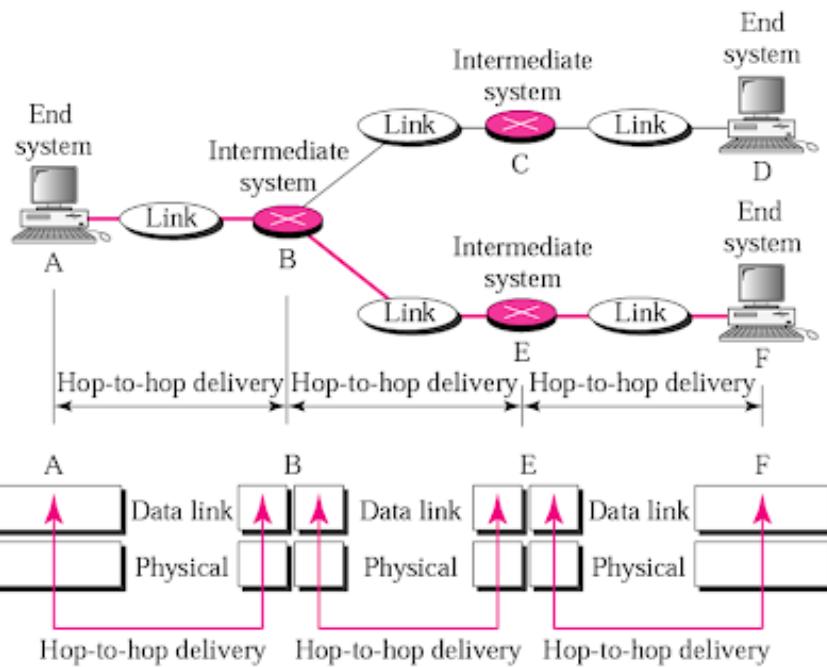


Physical Layer: It is responsible for movements of individual bits from one hop (node) to the next.

Functions:

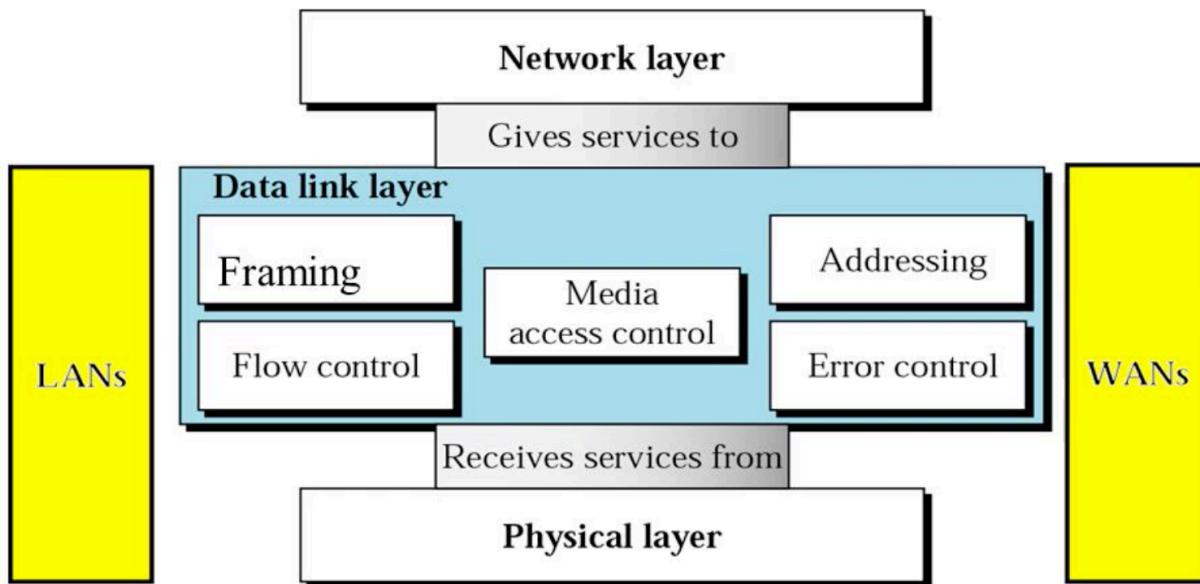
- i. To activate, maintain and deactivate the physical connection
- ii. To define voltages and data rates needed for transmission
- iii. To convert digital bits into electrical signal
- iv. To decide whether the transmission is simplex, half-duplex or full-duplex.
- v. A physical layer is concerned with the connection of devices to the media (Line configuration).
- vi. It also defines the physical topology.
- vii. It also helps in synchronization of bits.

Data Link layer



Data Link layer: It transforms the physical layer, a raw transmission facility to a reliable link. It is responsible for moving frames from one hop (node) to the next i.e Hop-to-Hop delivery.

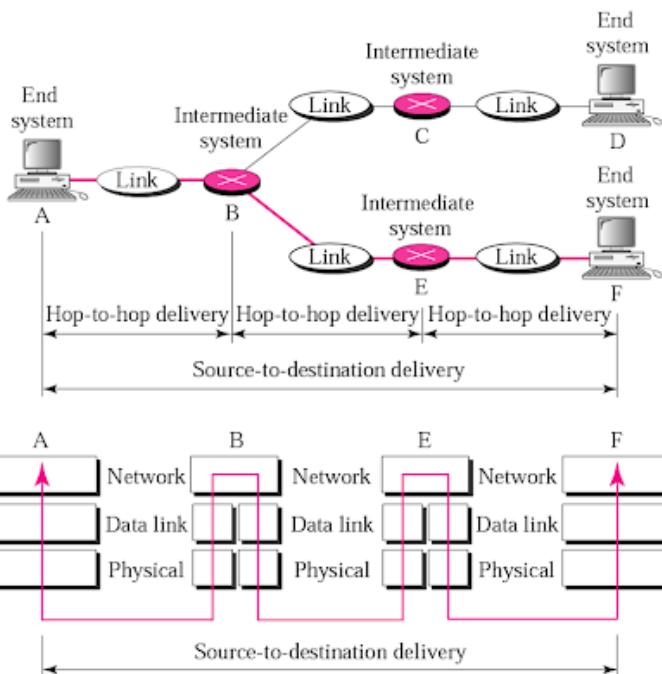
Data Link layer



Functions:

- i. Framing: The layer divides the stream of bits received from the network layer into manageable data units called frames.
- ii. Physical addressing: It adds a header to the frame to define the physical address of the sender and/or receiver of the frame.
- iii. Flow Control: It provides a flow control mechanism to avoid a fast transmitter from overrunning a slow receiver by buffering the extra bits.
- iv. Error control: It is achieved by adding a trailer at the end of the frame. It also uses a mechanism to prevent duplication of frames.
- v. Access Control: The layer determines which device has control over the link at any given time, when two or more devices are connected to the same link.

Network Layer

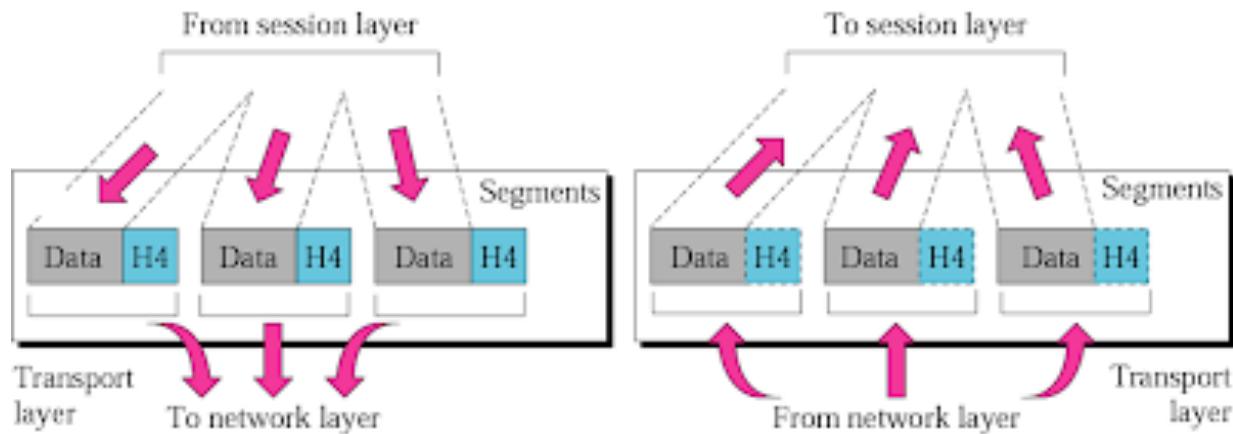


Network Layer: The network layer is responsible for the delivery of individual packets from the source host to the destination host i.e End to End delivery or source to destination delivery.

Functions:

- i. It translates logical network address into physical machine address i.e. the numbers used as destination IDs in the physical network cards
- ii. It determines the quality of service by deciding the priority of message and then route a message will take if there are several ways a message can get to its destination.
- iii. It breaks the larger packets into smaller packets if the packet is larger than the largest data frame the data link will accept.
- iv. Routers and gateways operate in the network layer.

Transport Layer

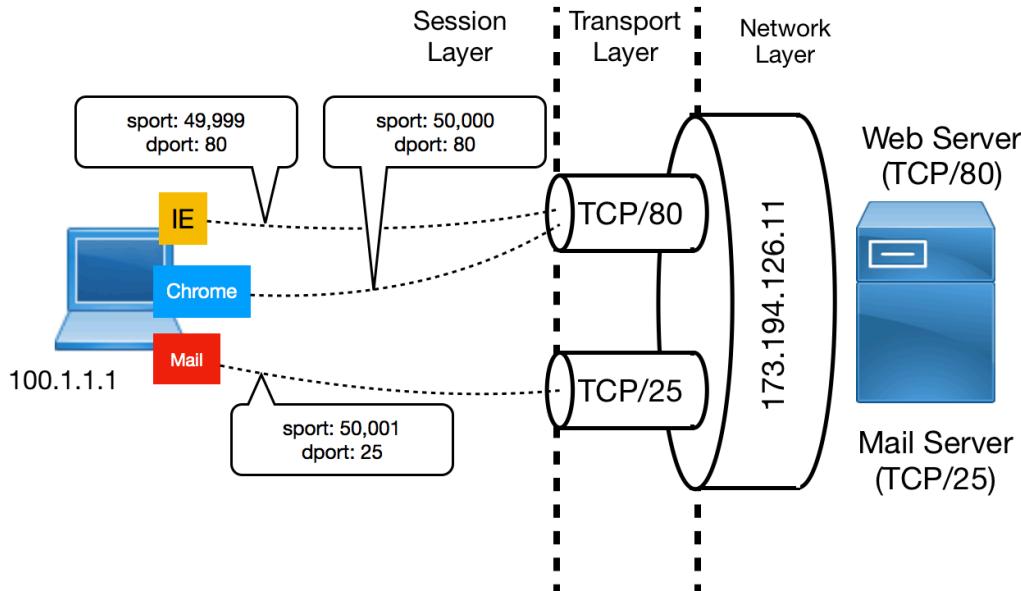


Transport layer: It is responsible for process-to-process delivery of the entire message.i.e. source to destination delivery of the entire message. It ensures that the whole message arrives intact and in order, ensuring both error control and flow control at source destination level.

Functions:

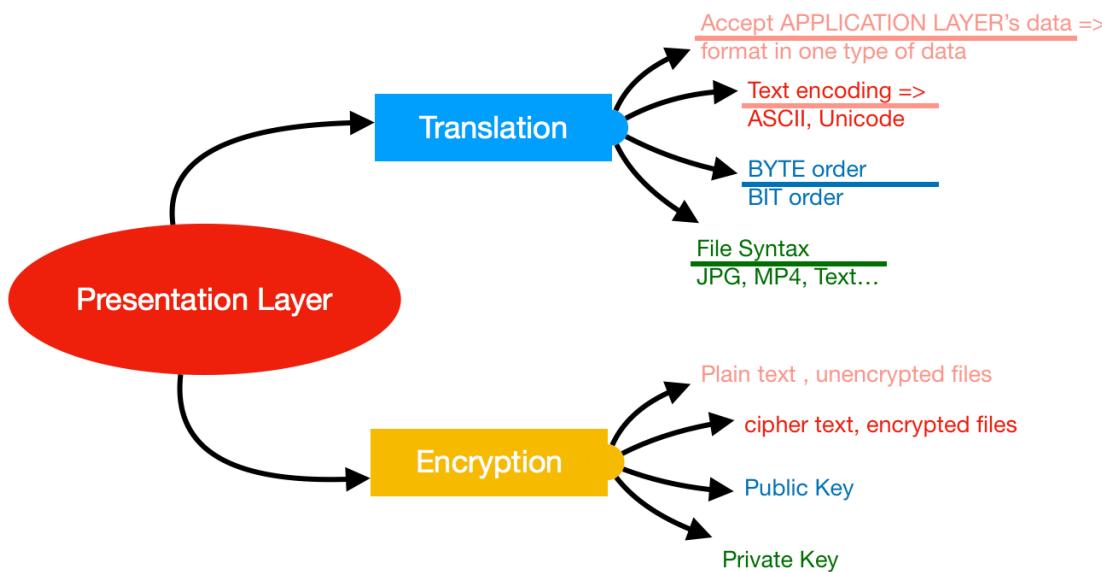
- i. Segmentation and re-assembley: It divides each message into packets at the source and reassembles than at the destination.
- ii. Service point addressing The transport layer header H4 includes service point to deliver a specific process from source to a specific process at the destination.
- iii. Connector Control: The layer can be either connectionless or connection oriented.
- iv. Flow Control: It provides end-to-end flow control rather than across a single link.
- v. Error Control: It ensures that the entire message arrives at the receiving transport layer without error.

Session Layer

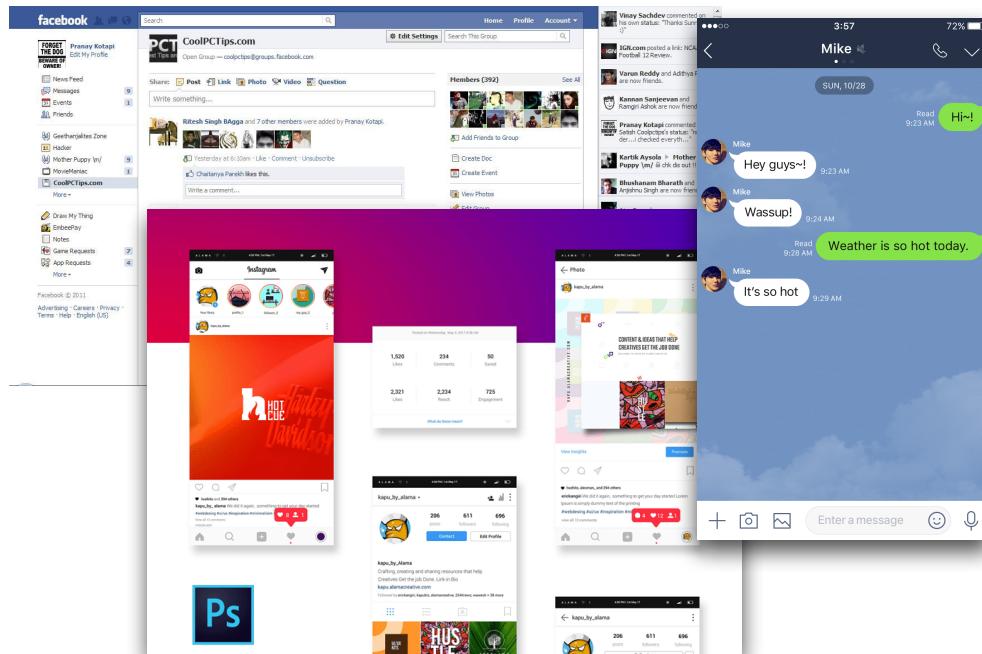


Session Layer: It is responsible for dialog control and synchronization i.e it is network dialog controller. It establishes maintains and synchronizes the interaction among communicating systems.

Presentation Layer



Application Layer



OSI Model

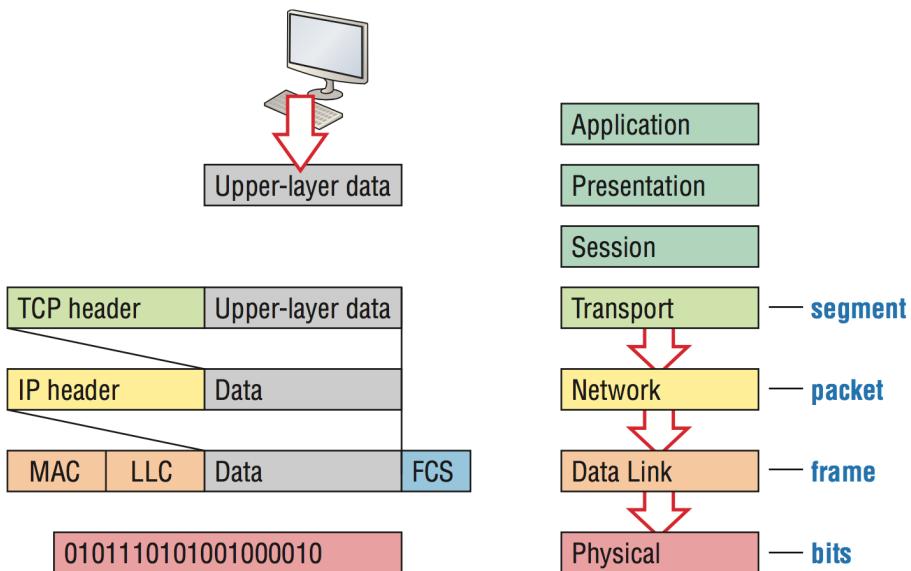
Layer	Application/Example
Application (7) <small>Serves as the window for users and application processes to access the network services.</small>	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management
Presentation (6) <small>Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.</small>	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation
Session (5) <small>Allows session establishment between processes running on different stations.</small>	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.
Transport (4) <small>Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.</small>	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing

F
I
L
T
E

OSI Model

Layer	Application/Example	
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	K E T R I N G
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	

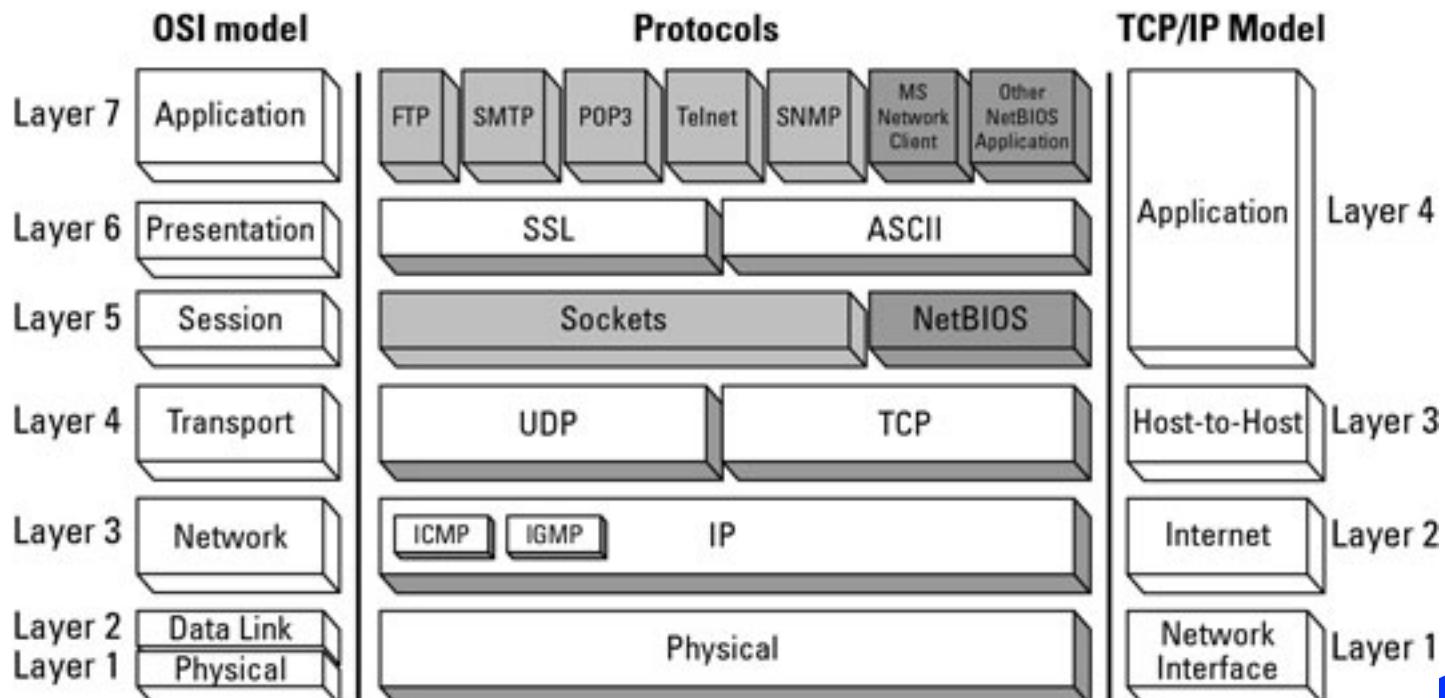
Encapsulation



Contents

- Layer Architecture
- OSI Model
- TCP/IP Model
 - Network Access Layer
 - Internet Layer

TCP/IP Model



ชุดโปรโตคอล Transmission Control Protocol/Internet Protocol หรือ TCP/IP ออกแบบโดยกระทรวงกลาโหม ประเทศสหรัฐอเมริกา อาจจะเรียกอีกชื่อว่า DoD Model เพื่อใช้สำหรับการสื่อสารข้อมูลคอมพิวเตอร์ ซึ่งใช้ในกิจกรรมสงคราม โปรโตคอลต่างๆ ที่ได้นั้นต้องมีความมั่นคง อิสระ ในการดำเนินงาน และมีความคงทน ในบทนี้เป็นการอธิบายถึงโปรโตคอลต่างๆ ใน TCP/IP อย่างคร่าวๆ เพื่อปรับพื้นฐานให้ผู้อ่านเข้าใจการนิยามคำศัพท์บางคำ หลักการทำงานเบื้องต้นของโปรโตคอลบางตัว เพื่อเป็นพื้นฐานแก่การทำความเข้าใจเนื้อหาของรายวิชาเครือข่าย ในบทอื่นๆ และบางโปรโตคอลอาจกล่าวถึงอีกครั้ง ในบทอื่น ที่เกี่ยวข้อง หรือในรายวิชาอื่น ต่อไป

ตัวแบบ DoD เป็นตัวแบบอย่างง่ายของ OSI Model ซึ่งประกอบด้วยชั้นต่างๆ จำนวน 4 ชั้น ได้แก่ Process/Application, Host-to-Host, Internet และ Network Access

เมื่อจัดจำแนกโปรโตคอลต่างๆ ตาม DoD model ตามภาพแล้วพบว่า โปรโตคอลโดยส่วนใหญ่แล้วจะอยู่ในชั้น Application เนื่องจากโปรโตคอลต่างๆ เหล่านี้เป็นบริการที่ตอบสนองความต้องการของผู้ใช้ ดังนั้นอาจจะมีการออกแบบโปรโตคอลใหม่ๆ เกิดขึ้นมาอย่างต่อเนื่อง โปรโตคอลในชั้น Host-to-Host และ Internet นั้นอาจจะไม่ค่อยเปลี่ยนแปลง จนกว่าจะมีการออกแบบแบบอื่นๆ ขึ้นมา เช่น การเปลี่ยนจาก IPv4 เป็น IPv6 และจะส่งผลให้ ICMP ปรับเปลี่ยนเป็น ICMPv6 แทน สำหรับชั้น Network Access นั้นโปรโตคอลต่างๆ จะขึ้นอยู่กับอุปกรณ์สื่อสารต่างๆ เช่น การสื่อสารแบบมีสาย ไร้สาย เป็นต้น เมื่อวิธีการสื่อสารเปลี่ยนแปลง โปรโตคอลในชั้นนี้อาจจะต้องมีการเปลี่ยนแปลงตามความเหมาะสม

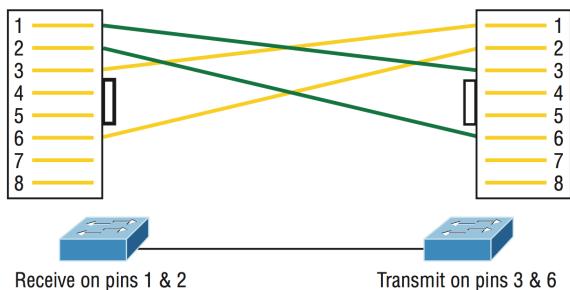
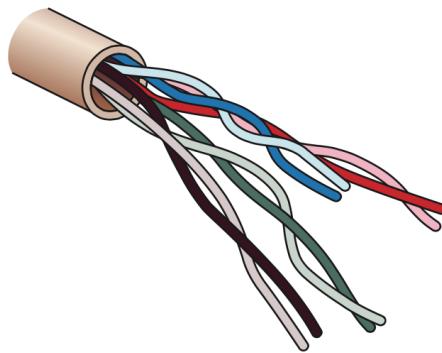
Network Access Layer

Physical Layer



Transmit on pins 1 & 2
Receive on pins 3 & 6

Receive on pins 1 & 2
Transmit on pins 3 & 6



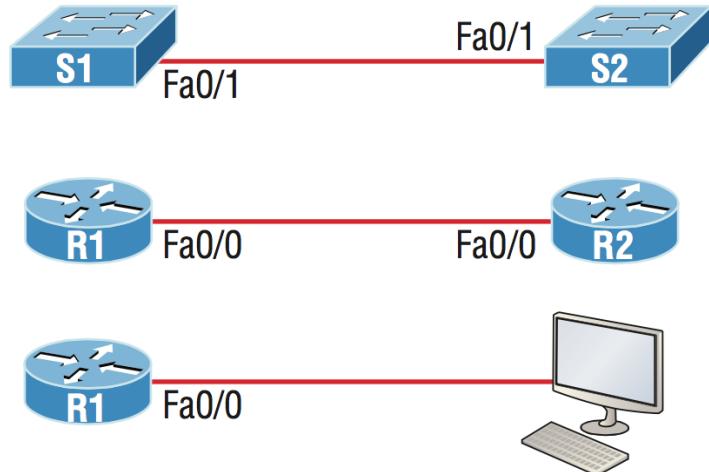
Receive on pins 1 & 2

Transmit on pins 3 & 6

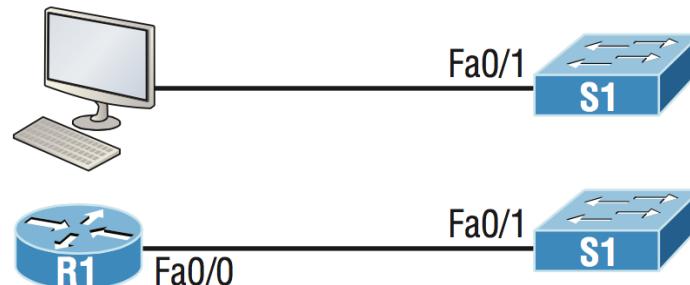
1. ชั้น Physical รับผิดชอบการส่งข้อมูล ในระดับบิต โดยแปลงข้อมูลดิจิทัล 1 บิต ให้กลายเป็นลักษณะทางไฟฟ้าซึ่งมีรูปแบบที่หลากหลาย เพื่อส่งผ่านสื่อแบบต่างๆ การกำหนดความเร็วในการรับส่งข้อมูล การประสานจังหวะระหว่างฝ่ายส่งและฝ่ายรับ การคำนึงถึงรูปแบบของอินเตอร์เฟส (Interface) ที่ต้องเลือกใช้ให้เหมาะสมกับชนิดของสื่อ (Media) โดยที่ชนิดของสื่อจะเป็นตัวกำหนดปริมาณของข้อมูลที่สามารถส่งผ่านสื่อชนิดนั้น ซึ่งเรียกว่า Maximum Transfer Unit หรือ MTU เครือข่ายปัจจุบันมีสื่อที่มักใช้งานคือ สื่อแบบมีสายซึ่งได้แก่สายคู่ตีเกลียว (Twisted Pair) และใยแก้วนำแสง (Fiber Optic) สื่อแบบไร้สายได้แก่ สัญญาณวิทยุซึ่งได้แก่ WiFi และ Bluetooth เป็นต้น

Network Cabling

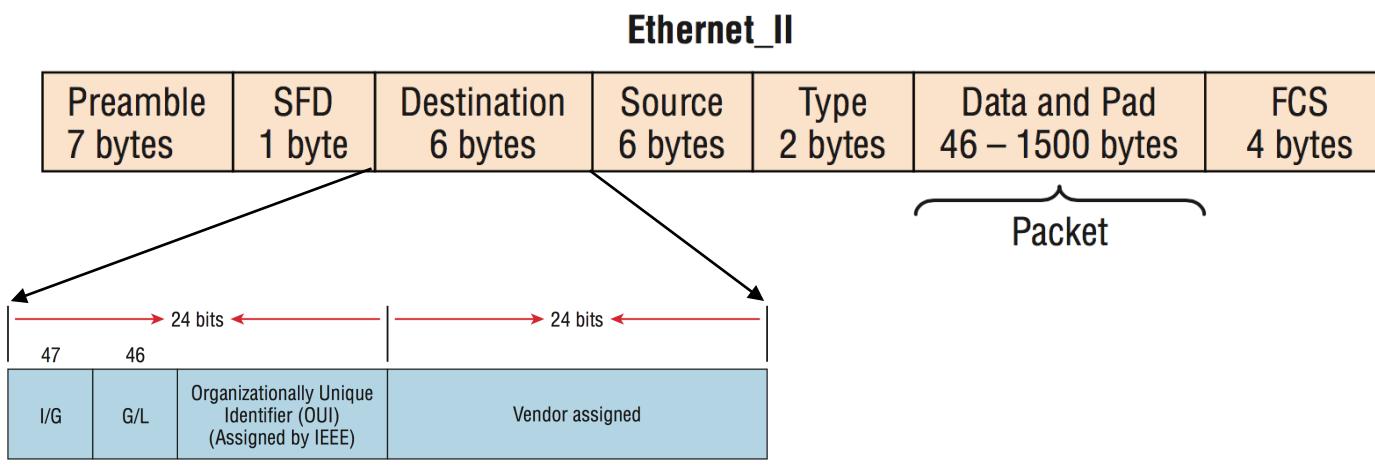
Crossover cable



Straight-through cable



Datalink Layer



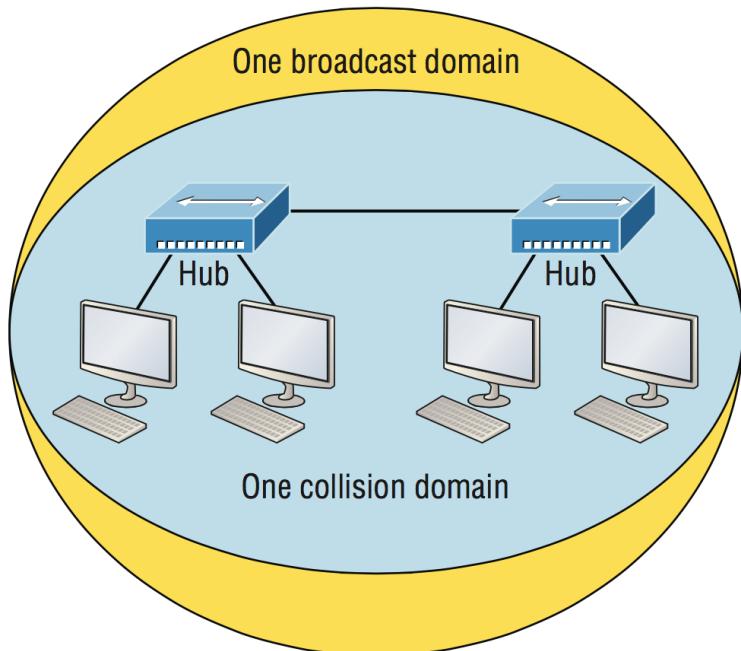
Internet Technology

<http://cjundang.ubines.info>

94

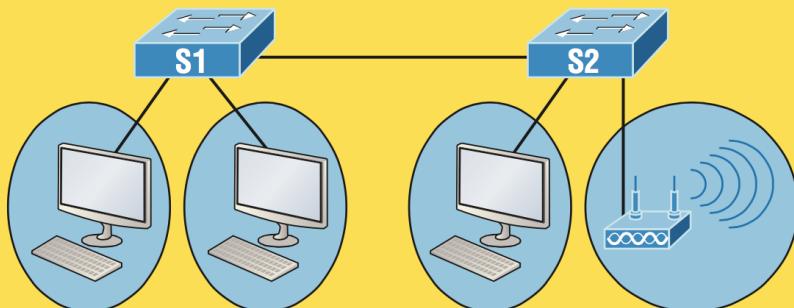
1.ชั้น Datalink เป็นการรับผิดชอบการส่งข้อมูลจากโทรศัพท์มือถือไปยังอีกโทรศัพท์มือถือที่อยู่ติดกันหรือเรียกว่าการสื่อสารแบบ Hop-to-Hop ข้อมูลที่สื่อสารจะถูกบรรจุในโครงสร้างข้อมูล叫做 Encapsulation เพื่อเพิ่ม Header และ Tailer ซึ่งเป็นส่วน Overhead ที่จำเป็น สำหรับการรับส่งข้อมูลไปยังโทรศัพท์มือถือต่อไป ที่อยู่ของโทรศัพท์มือถือจะถูกแทนด้วยเลขฐานสองขนาด 48 บิตซึ่งเรียกว่า MAC Address ควบคุมการให้ลูกค้าของข้อมูล ควบคุมความพยายามของผู้ใช้งานที่จะเข้าถึงข้อมูลที่ต้องการ ชั้น Datalink จะตรวจสอบและจัดการข้อมูลที่ได้รับมา เช่น การตรวจสอบข้อความที่ไม่ถูกต้อง (CRC Checksum) หรือการจัดการข้อมูลที่ถูกส่งผิดทาง (Frame Collision) ด้วยวิธีการต่างๆ

Collision Domain

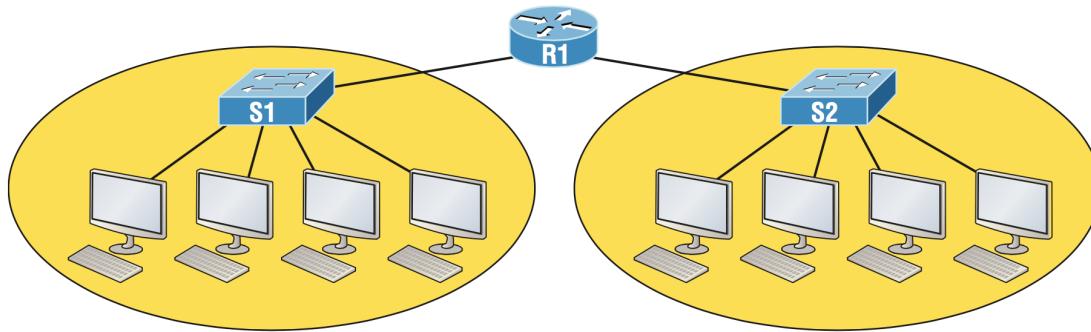


A typical Network today

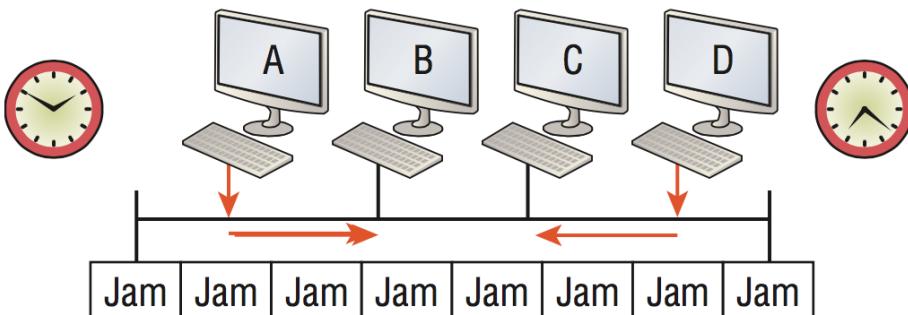
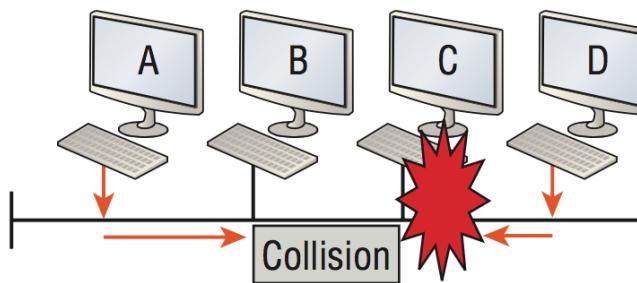
Each connection on a switch creates a separate collision domain.



Broadcast Domain



Two broadcast domains. How many collision domains do you see?



Contents

- Layer Architecture
- OSI Model
- TCP/IP Model
 - Network Access Layer
 - Internet Layer

Internet Layer

ชั้นเน็ตเวิร์ครับผิดชอบการรับส่งข้อมูลจากต้นทางถึงปลายทาง โดยผ่านเครือข่ายรูปแบบต่างๆ ซึ่งประกอบด้วยสองล่วนคือ การกำหนดเลขที่อัญญา และการค้นหาเส้นทาง

- bit
- byte
- octet
- Network Address
- Broadcast Address

การกำหนดเลขที่อยู่

- การกำหนดเลขที่อยู่ของอุปกรณ์สื่อสารนั้น กำหนดโดยใช้ IPv4 ซึ่งเป็นการแทนเลขที่ขนาด 32 บิต ซึ่งได้หยุดแจกจ่ายให้แก่ผู้ใช้ไปแล้วเนื่องจากไม่พอ ในขณะเดียวกันมีการวิจัยและกำหนด IPv6 ซึ่งมีขนาด 128 บิตมาใช้งานคู่ขนานกัน บางองค์กร ในประเทศไทยนั้นพร้อมใช้ IPv6 แล้ว แต่บางองค์กรนั้นยังคงใช้ IPv4 อยู่
- IP Address เป็นวิธีการอ้างอิงที่อยู่เชิงตัวเลขซึ่งกำหนดให้แก่อุปกรณ์เครือข่ายบนเครือข่าย IP วิธีการกำหนดเลขที่อยู่นี้เป็นแบบ Logical Address ใช้สำหรับการค้นหาเครื่องคอมพิวเตอร์ในเครือข่ายท้องถิ่น ก่อนที่จะเข้า ใจถึง IP Address นั้นควรทำความเข้าใจถึงคำศัพท์พื้นฐานบางคำก่อน ดังนี้

คำนิยาม

- **บิต (Bit)** คือ ข้อมูล 1 หรือ 0 จำนวนหนึ่งตัว
- **ไบต์ (Byte)** คือ ข้อมูลจำนวน 7 หรือ 8 บิต ขึ้นอยู่กับสถาปัตยกรรมของเครื่อง สำหรับรายวิชานี้ กำหนดให้ข้อมูล 1 ไบต์มีจำนวน 8 บิต
- **ออกเต็ก (Octet)** เกิดจากข้อมูลจำนวน 8 บิตเรียงต่อเนื่องกัน ในรายวิชานี้หมายความว่าข้อมูลที่ใช้ในการส่งข้อมูลขนาด 8 บิต
- **Network Address** คือเลขที่อยู่ที่ใช้ในการค้นหาเส้นทางเพื่อส่งแพ็คเกตไปยังเครือข่ายเป้าหมาย
- **Broadcast Address** คือเลขที่อยู่ที่ถูกใช้โดยโปรแกรมหรือเครื่องคอมพิวเตอร์เพื่อส่งข้อมูลไปยังเครื่องทุกเครื่อง ในเครือข่าย

1000 0000 0000 1011 0000 0011 0001 1111

128.11.3.31

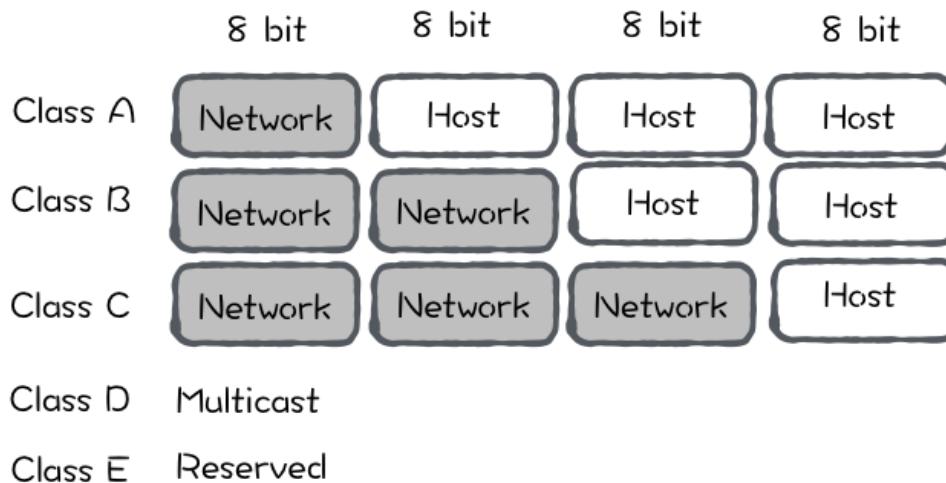
สัญลักษณ์

เลขที่อยู่อินเทอร์เน็ต (Internet Protocol หรือ IP Address) ใน IPv4 เป็นข้อมูลขนาด 32 บิตซึ่งแบ่งออกเป็น 4 กลุ่มซึ่งแบ่งออกเป็น Octet หรือ Byte ซึ่งแต่ละไบต์มีขนาด 8 บิต การเขียน IP Address นั้น เขียนแทนด้วยรูปแบบบิต ซึ่งเขียนได้ 2 ลักษณะได้แก่

1. การแสดงผลฐานสอง โดยที่หมายเลข IP Address แสดงในรูปแบบเลขฐานสองจำนวน 32 บิต
2. การแสดงผลฐานสิบ เป็นการจัดเลขฐานสองเป็น 4 กลุ่มๆ 8 บิตหลังจากนั้นแปลงเลขฐานดังกล่าว เป็นเลขฐานสิบ และแสดงตัวเลขนั้นโดยใช้เครื่องหมายจุดคั่นระหว่างตัวเลขแต่ละตัว

Classful Address

1000 0000 0000 1011 0000 0011 0001 1111



การแบ่งคลาส

IP Address ในคลาส A, B และ C ประกอบด้วย Network Address (หรือ Network ID) และ Host Address (หรือ Host ID)

- **Network Address** หรือเรียกอีกชื่อหนึ่งว่า Network Number โดยใช้สำหรับนิยามเครือข่ายแต่ละตัว โดยเครื่องคอมพิวเตอร์แต่ละตัวอยู่ในเครือข่ายเดียวกัน ส่วนหนึ่งของ IP Address จะเหมือนกัน เช่น IP Address 172.16.30.56 นั้นอยู่ในเครือข่ายหมายเลข 172.16
- **Host Address** ใช้สำหรับการกำหนดเลขที่อยู่ ให้แก่โหนดตัวเลขดังกว่าเป็นตัวเลขแบบ unique ซึ่งไม่ซ้ำกัน ตัวชุดนี้ใช้สำหรับการกำหนดให้เลขที่อยู่มีความแตกต่างกัน หากพิจารณา IP Address 172.16.30.56 แล้วพบว่าโหนดชุดนี้มี Host Address เป็น 30.56

Class	Start Bit	CIDR	Possible Address Values
A	0xxx	/8	0.0.0.0 - 127.255.255.255
B	10xx	/16	128.0.0.0 - 191.255.255.255
C	110x	/24	192.0.0.0 - 223.255.255.255
D	1110	/32	224.0.0.0 - 239.255.255.255
E	1111	Undefined	240.0.0.0 - 255.255.255.255

การแบ่ง Class ของ IP Address

- เครือข่าย ในคลาส A เป็นเครือข่ายที่มี Network Address ขนาดเล็ก โดยแต่ละเครือข่ายนั้นมีจำนวน โหนดบริบามมาก ในทางกลับกันหมายเลข IP Address คลาส C นั้นมีจำนวนกลุ่มของเครือข่าย จำนวนมาก แต่ละกลุ่มนั้นมีจำนวนโหนด 255 โหนด
- หากพิจารณา IP Address ขนาด 32 บิตแล้ว สีบิตแรกของ IP address แต่ละตัวนั้น หากขึ้นต้นด้วย 0 แล้วถือว่า IP Address ตัวนั้นอยู่ ในคลาส A บิตเริ่มต้นเป็น 10 นั้นกำหนดให้ IP Address นั้น เป็นคลาส B ในคอลัมภ์ที่ 3 นั้นคือ CIDR ใช้สำหรับการกำหนดกลุ่มของ IP Adress หรือเรียกว่า Netmask (ซึ่งจะอธิบายภายหลัง)

จากตารางนี้อธิบายโดยสรุปได้ว่า Network ID นั้นเป็นส่วนของ Address สำหรับการอ้างอิงถึง หมายเลขของกลุ่ม ในขณะที่ Host Address นั้น ใช้สำหรับการอ้างอิงโหนดต่างๆ ชั้นคลาส A มี Network ID จำนวน 1 ไบต์ และมี Host ID จำนวน 3 ไบต์

Netmask

Class	Binary	Decimal	CIDR
A	1111 1111 0000 0000 0000 0000 0000	255.0.0.0	/8
B	1111 1111 1111 1111 0000 0000 0000	255.255.0.0	/16
C	1111 1111 1111 1111 1111 0000 0000	255.255.255.0	/24

สำหรับ Netmask นั้นเป็นเลขที่อยู่สำหรับการบ่งชี้ถึงกลุ่มของหมายเลข IP address ซึ่ง Netmask นั้น เป็นตัวเลขขนาด 32 บิตที่เขียนแทนด้วยตัวเลขบิต 1 ต่อเนื่องกันหลังจากนั้นตามด้วยบิต 0 ต่อเนื่องกัน จำนวนของบิต 1 นั้นจะเท่ากับจำนวนของบิต ใน Network และจำนวนของบิต 0 เท่ากับจำนวนบิตของ Host เช่น คลาส A นั้นมี Netmask เป็น

1111 1111 0000 0000 0000 0000 0000

หรือเขียนแทนด้วยเลขฐานสิบเป็น 255.0.0.0

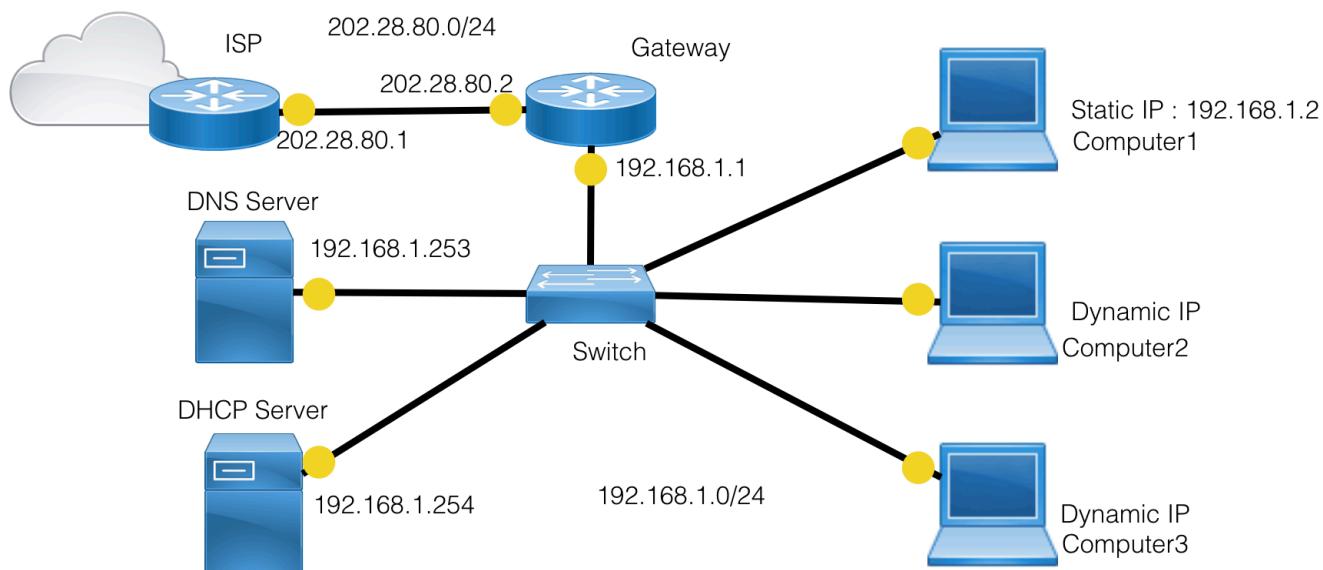
ดังตาราง แสดง Netmask ของ IP Address คลาสต่างๆ

Address Class	Reserved Address Space
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

Valid IP address

Address	Function
Network address of all 0s	Interpreted to mean "this network or segment."
Network address of all 1s	Interpreted to mean "all networks."
Network 127.0.0.1	Reserved for loopback tests. Designates the local node and allows that node to send a test packet to itself without generating network traffic.
Node address of all 0s	Interpreted to mean "network address" or any host on a specified network.
Node address of all 1s	Interpreted to mean "all nodes" on the specified network; for example, 128.2.255.255 means "all nodes" on network 128.2 (Class B address).
Entire IP address set to all 0s	Used by Cisco routers to designate the default route. Could also mean "any network."
Entire IP address set to all 1s (same as 255.255.255.255)	Broadcast to all nodes on the current network; sometimes called an "all 1s broadcast" or local broadcast.

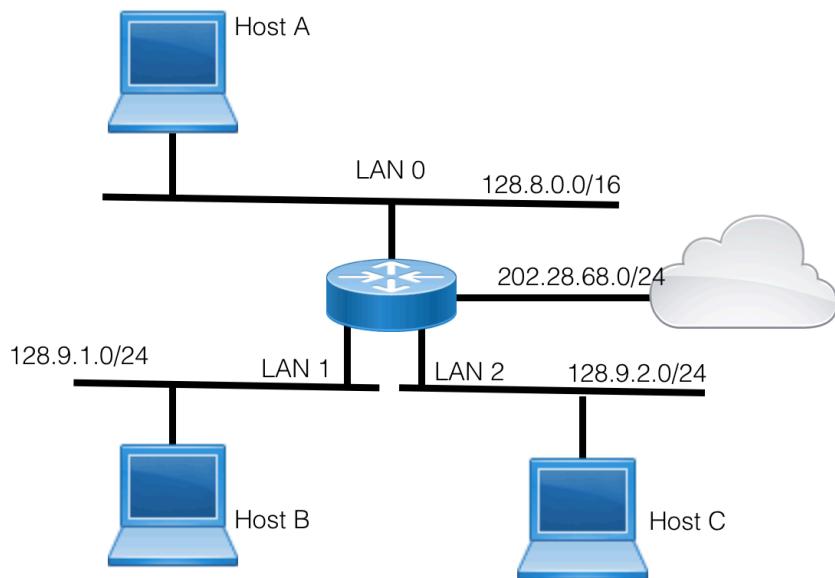
Components of Networks



ອີງຕາຍ

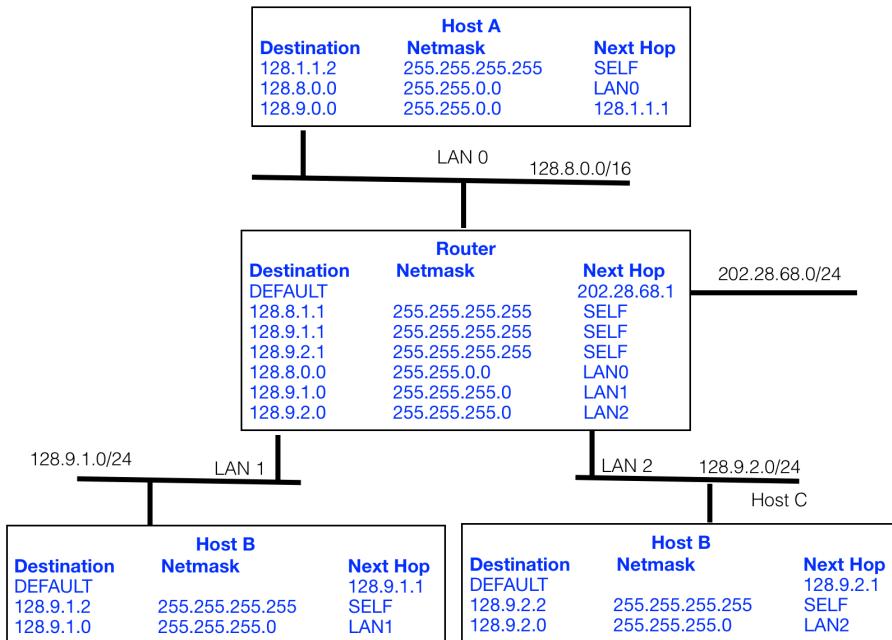
1. WAN
2. DNS Server
3. IP Address, Netmask, Gateway, DNS Server

Routing



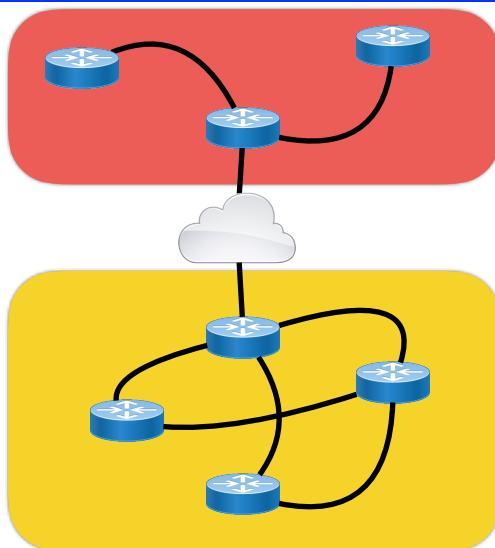
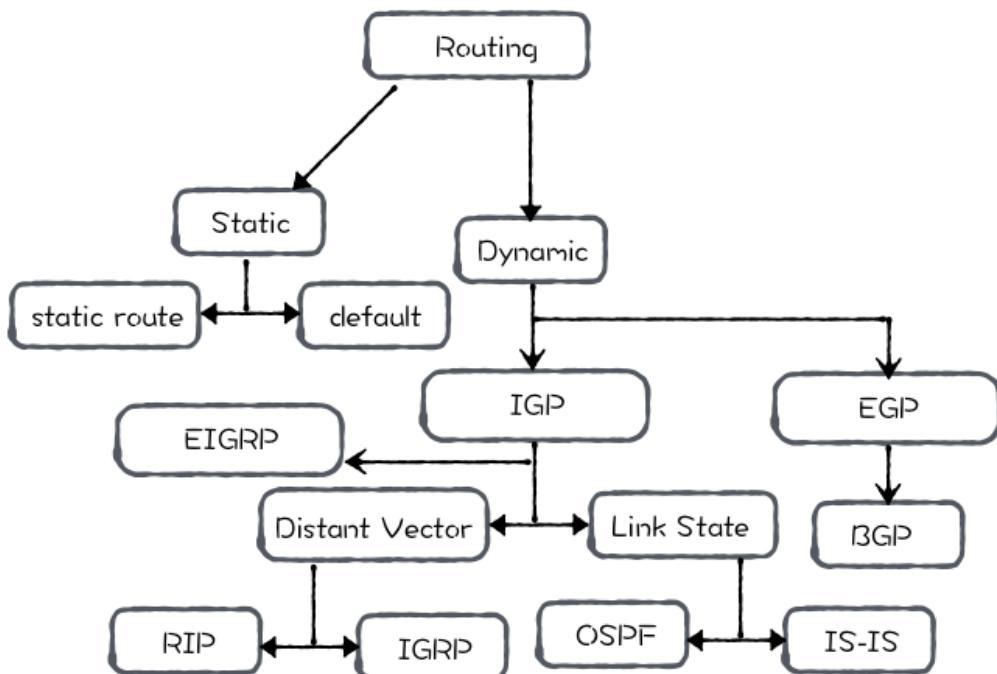
ອົບນາຍ ພັດທະນາ Routing

Routing



ອົບນາຍ ໜັກການ Routing

Routing Protocol



การค้นหาเส้นทางของแพ็คเก็ตเนื่องจาก เครื่องผู้ใช้ไม่เชื่อมต่อโดยตรงกับเครื่อง ให้บริการ โดยส่งผ่าน อุปกรณ์เครือข่ายซึ่งเชื่อมต่อแบบ Mesh จึงจำเป็นต้องมีโปรโตคอลสำหรับการค้นหาเส้นทาง โดยที่ Router แต่ละตัวนั้นจะมี Routing Table เพื่อใช้สำหรับการส่งต่อแพ็คเก็ต การสร้างและแก้ไข Routing Table นั้น ทำได้โดยโปรโตคอลค้นหาเส้นทาง 2 แบบ คือ Static Routing Protocol และ Dynamic Routing Protocol โดยที่โปรโตคอลแบบ Static นั้นจะสร้าง Routing Table ล่วงหน้าโดยผู้ดูแลระบบ ในขณะที่โปรโตคอลแบบ Dynamic นั้นจะแก้ไข Routing Table แบบอัตโนมัติขึ้นอยู่กับสถานการณ์ในขณะนั้น

Notes

Module 4

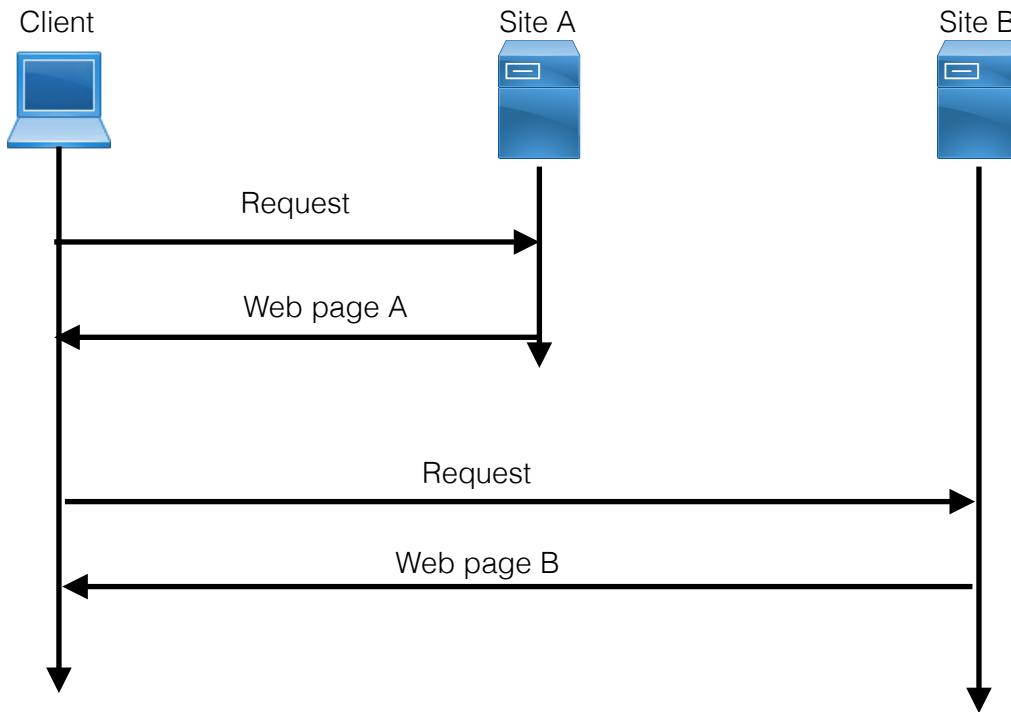
Application Protocol

Contents

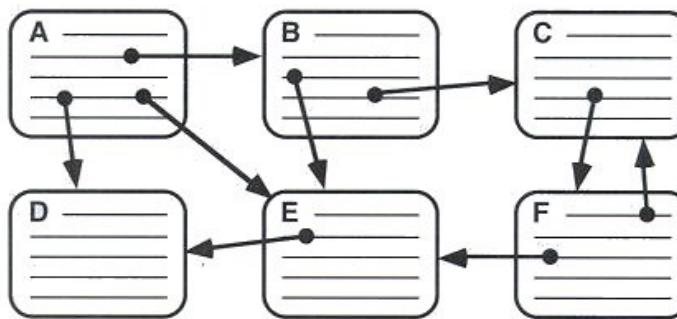
- Web Technology
 - Browser
 - Web Document
 - Web Architecture
 - HTTP Protocol
- File Sharing
 - File Transfer Protocol
 - Network File System
- Domain Name System

Web Technology

The Hypertext Transfer Protocol (HTTP) เป็นโปรโตคอล หลักที่ใช้ ในการเข้าถึงข้อมูล บนเว็บตัวเว็บ (World Wide Web หรือ WWW) เว็บตัวเว็บเป็นที่เก็บของข้อมูลที่กระจายไปทั่วโลก และเชื่อมโยงเข้าด้วยกัน โดย www เป็นบริการแบบ client/server แบบกระจายโดยเข้าถึงบริการผ่านเว็บเบราว์เซอร์ เพื่อเชื่อมต่อไปยังเครื่องให้บริการ (Server) ซึ่งกระจายไปยังแหล่งต่างๆ ซึ่งเรียกว่า site



Hypertext คือ ข้อความที่ปรากฏบนคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ ที่มีการอ้างอิง ด้วยไฮเปอร์ลิงค์ (Hyperlinks) กับข้อความอื่นๆ ที่ผู้อ่านสามารถเข้าถึงได้ทันที โดยการคลิกเมาส์ หรือกดปุ่ม



Hypermedia ใช้กราฟิก (graphic), เสียง (audio), วิดีโอ (video), ข้อความธรรมชาติ และไฮเปอร์ลิงค์ (hyperlink) เป็นส่วนขยายทางตรรกะ (logical) ของไฮเปอร์เท็กซ์

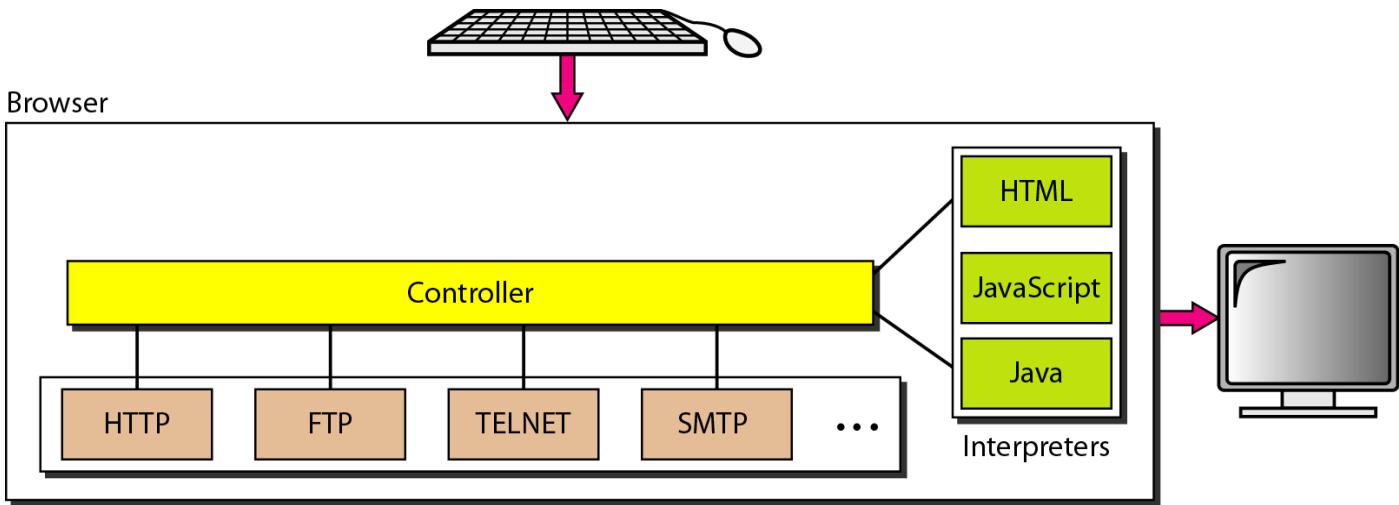
jacaranda.in.th Chatchanan Jandaeng, Lecturer at School of Informatics, WU

2010

[Show as slideshow]

หวานๆ แมวงานเขียนที่บ้าน

เว็บเบราว์เซอร์ (Web Browser)

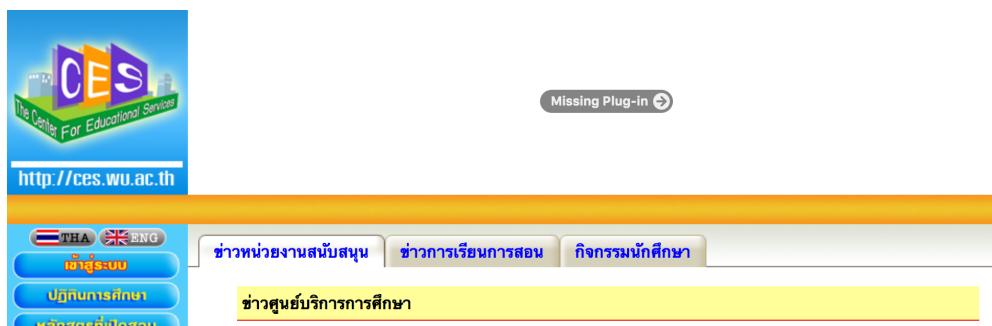


เบราว์เซอร์เป็นโปรแกรม client ที่ทำหน้าที่ร้องขอข้อมูล ตีความและแสดงเอกสารที่อยู่บนเว็บ โปรแกรมเว็บเบราว์เซอร์นั้นประกอบไปด้วย คอนโทรลเลอร์ โปรแกรมโคลเลนต์ และ อินเทอร์พรีเตอร์

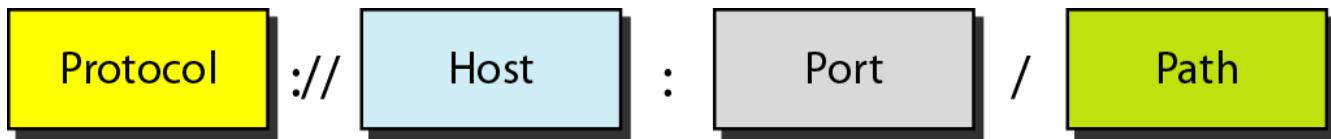
1. คอนโทรลเลอร์ (Controller) เป็นโมดูลกลางของโปรแกรมเว็บเบราว์เซอร์ ทำหน้าที่รับการป้อนข้อมูลจากแป้นพิมพ์และเมาส์ โดยอ่านเลขที่อยู่ของผู้ให้บริการเว็บ และร้องขอข้อมูลผ่าน client program

2. โปรแกรม client เป็นส่วนที่ใช้สำหรับการเชื่อมต่อเครือข่าย โดยเชื่อมโยงผ่านโปรโตคอลต่างๆ ได้แก่ HTTP, FTP, TELNET หรือ SMTP เป็นต้น ซึ่งส่งผลถึงความสามารถในการร้องขอサービスต่างๆ ของโปรแกรมเบราว์เซอร์นั้น

3. อินเทอร์พรีเตอร์ เป็นตัวแปลภาษาซึ่งสนับสนุนการตีความ ภาษา HTML, JavaScript, หรือภาษาอื่นๆที่สนับสนุนในการพัฒนาเว็บไซต์



Uniform Resource Locator (URL)



Uniform Resource Locator (URL) คือที่อยู่ของหน้าเว็บเพจ ซึ่งเครื่อง client จะเป็นต้องรับ URL ของเว็บไซต์นั้น โดย URL เป็นมาตรฐานสำหรับการระบุชิ้นดูของข้อมูลบนอินเทอร์เน็ต

- โปรโตคอล (Protocol) เป็นโปรแกรมไคลเอนต์ / เชิร์ฟเวอร์ ที่ใช้ในการร้องขอเอกสาร : HTTP , FTP ฯลฯ
- โฮสต์ (Host) เป็นคอมพิวเตอร์ที่เก็บข้อมูลนั้นๆอยู่
- พอร์ต (Port) เป็นการเลือกช่องทางเชื่อมต่อของชั้น transport เช่น หากต้องการเข้าใช้ HTTP ต้องร้องขอผ่านพอร์ต 80
- พาธ (Path) เป็นเส้นทางไปยังที่อยู่ของแฟ้มข้อมูล หากไม่ได้ระบุเส้นทาง จะถูกตั้งค่าไปที่ค่าเริ่มต้น (default) เช่น index.html หรือ index.php

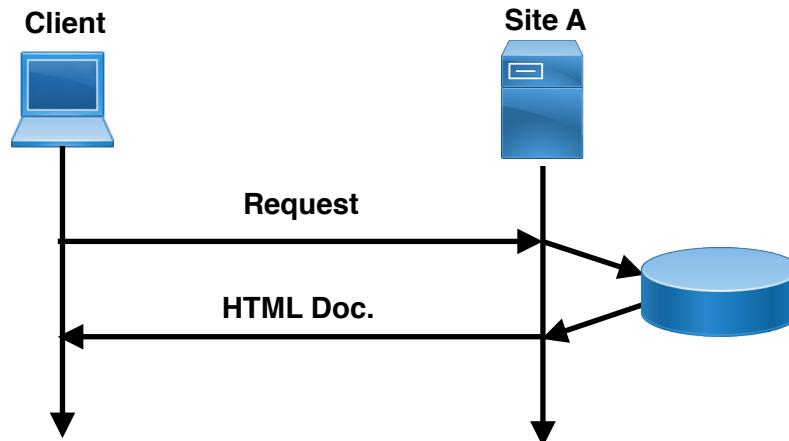
ตัวอย่าง <http://jacaranda.in.th:80/index.php> เป็นการอ้างอิง URL แบบเต็ม ซึ่งสามารถเขียนย่อได้ เป็น <http://jacaranda.in.th>

Uniform Resource Identifier (URI) เป็นตัวอักษรที่ใช้ในการระบุชื่อ หรือทรัพยากรบนอินเทอร์เน็ต วิธีการระบุตัวตน ดังกล่าวช่วยให้ผู้ใช้มีปฏิสัมพันธ์กับตัวแทนของทรัพยากรผ่านเครือข่าย (โดยปกติแล้วคือ เว็บด้วยเว็บ) โดยใช้โปรโตคอลที่เฉพาะเจาะจงนั้น

Web document

Web document หมายถึงรูปแบบของเอกสารเว็บ โดยจัดแบ่งออกเป็น 3 รูปแบบได้แก่ เอกสารแบบสแตติก เอกสารแบบไดนามิก และเอกสารแบบ Active

- Static document เรียกอีกชื่อว่า Passive Document เป็นเอกสารที่มีเนื้อหาที่ผ่านการแก้ไขแล้วเก็บไว้ในเซิร์ฟเวอร์ ลูกค้าสามารถจัดเก็บเอกสารบนเซิร์ฟเวอร์โดยไม่จำเป็นต้องมีการเปลี่ยนแปลงใดๆ โดยใช้ Hypertext Markup Language (HTML) เป็นภาษาที่ใช้ในการสร้างหน้าเว็บแบบสแตติกนี้ โดย เบราว์เซอร์สามารถอ่านคำสั่งที่มีรูปแบบ หรือเรียกว่า แท็ก (tags) ที่ฝังอยู่ในเอกสาร HTML นั้น ตัวอย่างการประมวลผล static แสดงในภาพประกอบ

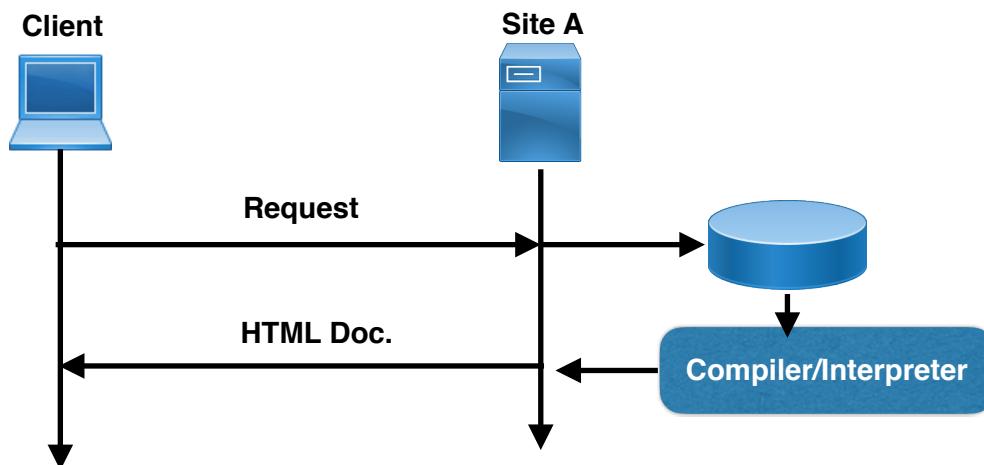


```
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body>
    <p>A code element is displayed like this:</p>
    <code>A piece of computer code</code>
    <p>Change the default CSS settings to see the effect.</p>
  </body>
</html>
```

Web document

Web document หมายถึงรูปแบบของเอกสารเว็บ โดยจัดแบ่งออกเป็น 3 รูปแบบได้แก่ เอกสารแบบสแตติก เอกสารแบบไดนามิก และเอกสารแบบ Active

- Dynamic Web document หรือ Server-site Script เป็นการสร้างเอกสารตามคำขอเชิร์ฟเวอร์โดยสร้างไฟล์ HTML ด้วยโปรแกรมในกลุ่ม Common Gateway Interface (CGI) ซึ่งเป็นเทคโนโลยีสำหรับการสร้างและการจัดการเอกสารเว็บแบบไดนามิก ภาษาคอมพิวเตอต์ที่ใช้สำหรับการสร้าง web document แบบ dynamic ได้แก่ C, C++, เชลล์ สคริปต์ shell script หรือ Perl และเทคโนโลยีของเว็บสมัยใหม่ ได้แก่ php, .net Framework เป็นต้น เครื่องเซิร์ฟเวอร์จะส่งผลลัพธ์ของการประมวลผลด้วยโปรแกรม CGI ซึ่งแสดงผลเป็น HTML ไปยังเบราว์เซอร์ ซึ่งอาจเป็นเครื่องพิมพ์ที่อยู่ห่างไกลจากเซิร์ฟเวอร์ จึงเรียกว่า “Dynamic Web Document”



```
#include <stdio.h>
void main(){
    printf("content-type: text/html\n\n");
    printf("<h1>Hello</h1>");
}
```

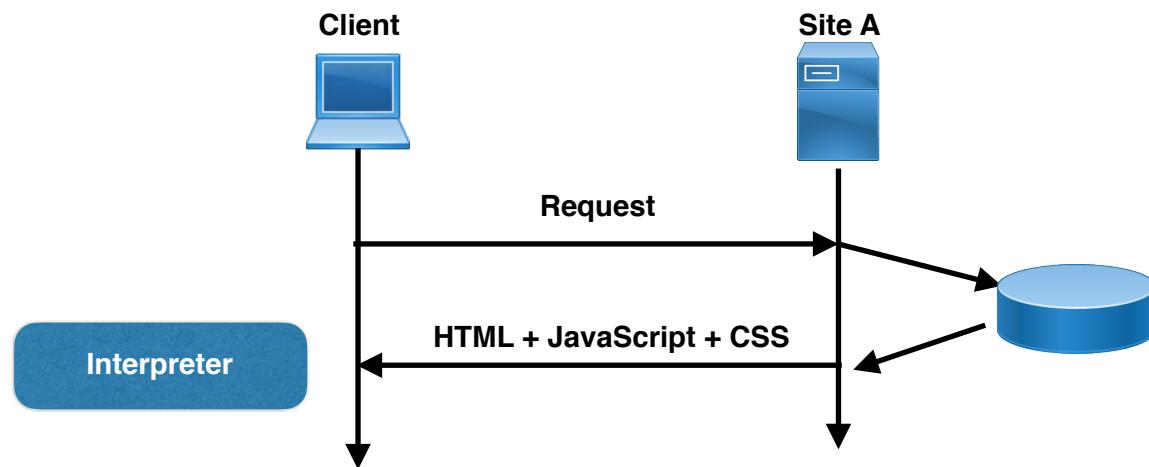
```
<?php
$x = 1;

while($x <= 5) {
    echo "The number is: $x <br>";
    $x++;
}
?>
```

Web document

Web document หมายถึงรูปแบบของเอกสารเว็บ โดยจัดแบ่งออกเป็น 3 รูปแบบได้แก่ เอกสารแบบสแตติก เอกสารแบบไดนามิก และเอกสารแบบ Active

- Active document หรือ Client-site Script เป็นเอกสารเว็บที่ประกอบด้วยเทคโนโลยีต่างๆ ที่ต้องประมวลผลทางฝั่ง client โดยทางเว็บเบราว์เซอร์ประมวลผลข้อมูลโดยใช้ interpreter module ของโปรแกรมเว็บเบราว์เซอร์ เว็บเทคโนโลยีบางตัวของ client site script นั้น ต้องอาศัยโปรแกรมหรือ plugin พิเศษในการสั่งรันโปรแกรม เช่น shockwave เป็นต้น หากโปรแกรมเว็บเบราว์เซอร์ไม่ติดตั้งโปรแกรมเหล่านั้นไว้แล้ว การแสดงผลบนเว็บจะไม่สมบูรณ์



```

<!DOCTYPE html>
<html>
  <head>
    <style>
      H1{
        color:green;
      }
    </style>
    <script>
      document.write("Hello");
    </script>
  </head>
  <body>
    <p>A code element is displayed like this:</p>
    <code>A piece of computer code</code>
    <p>Change the default CSS settings to see the effect.</p>
  </body>
</html>
    
```

2-Tier Web Architecture

TWO-TIER ARCHITECTURE

CLIENT
TIER



Client Computer

DATABASE
TIER



DataBase Server

© www.SoftwareTestingMaterial.com

```

<!DOCTYPE html>
<html>
<head>
<body>
<?php
$servername = "localhost";
$username = "username";
$password = "password";
$dbname = "myDB";

// Create connection
$conn = new mysqli($servername, $username, $password, $dbname);
// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}

$sql = "SELECT id, firstname, lastname FROM MyGuests";
$result = $conn->query($sql);

if ($result->num_rows > 0) {
    echo "<table><tr><th>ID</th><th>Name</th></tr>";
    // output data of each row
    while($row = $result->fetch_assoc()) {
        echo "<tr><td>" . $row["id"] . "</td><td>" . $row["firstname"] . " " .
$row["lastname"] . "</td></tr>";
    }
    echo "</table>";
} else {
    echo "0 results";
}

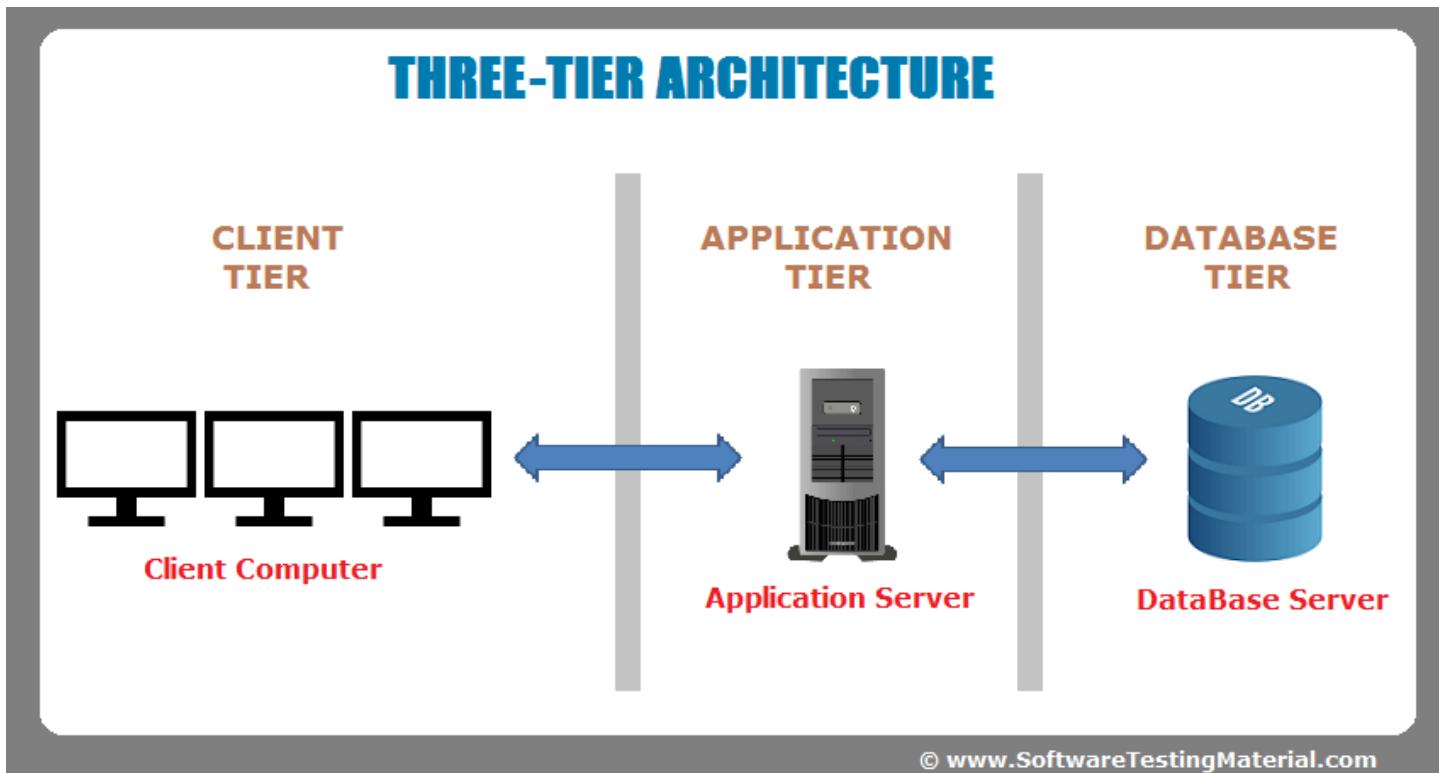
$conn->close();
?>

</body>
</html>

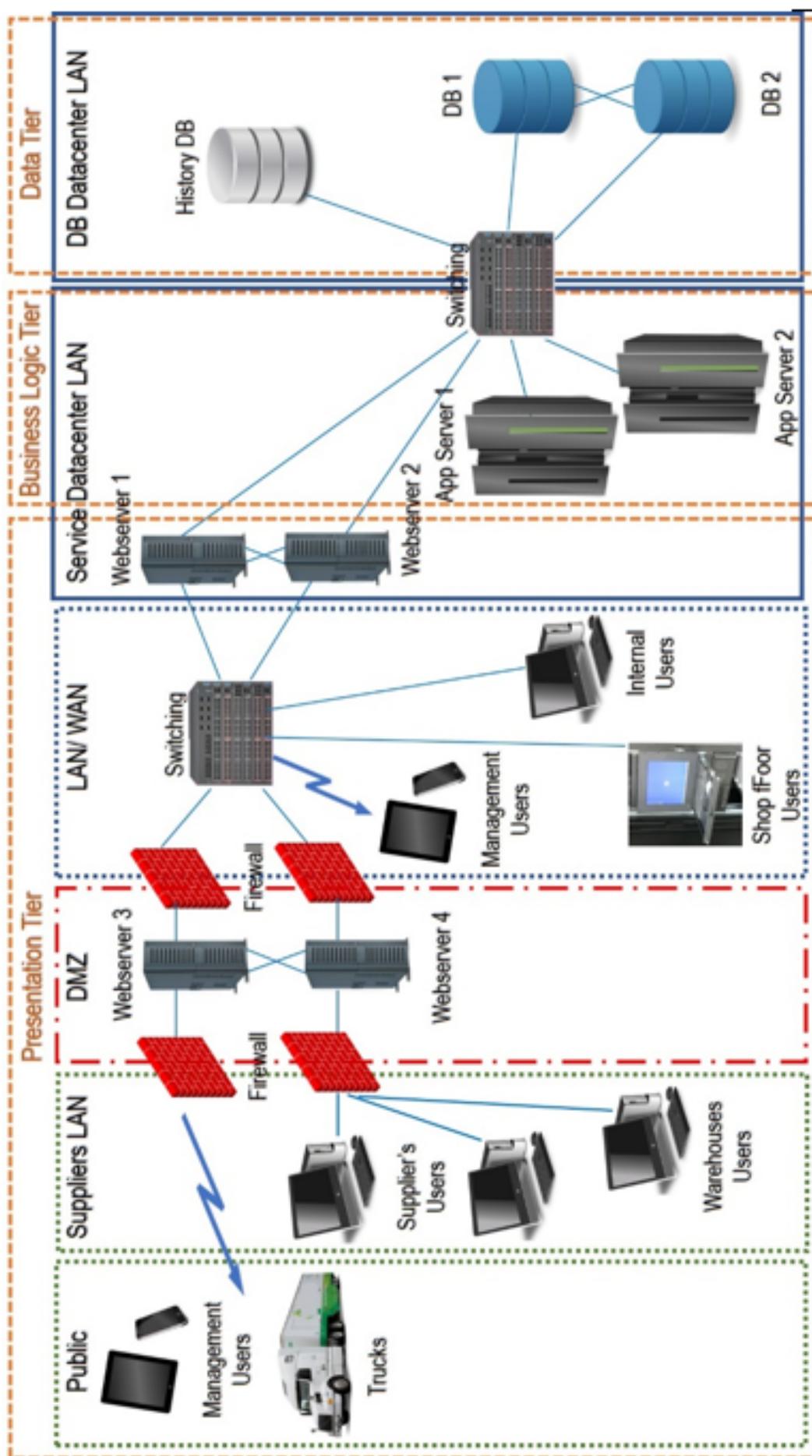
```

ID	Name
1	John Doe
2	Mary Moe
3	Julie Dooley

3-Tier Web Architecture



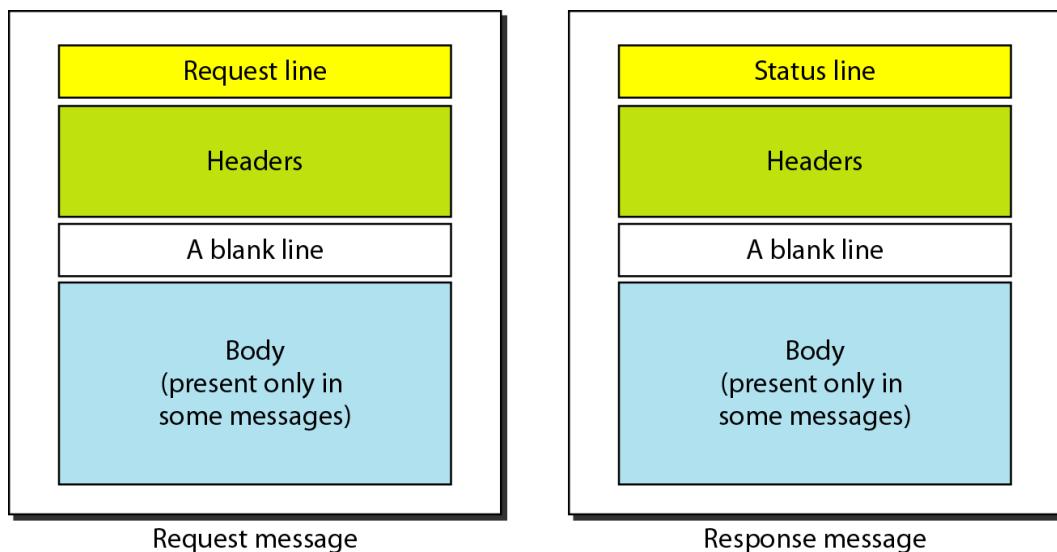
n-Tier Web Architecture



HTTP Protocol

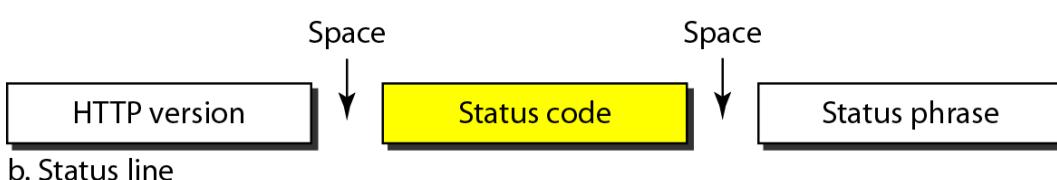
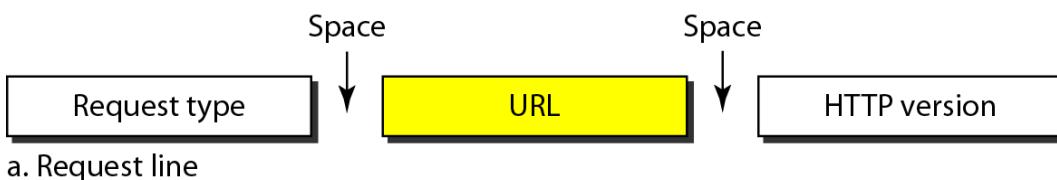
Hypertext Transfer Protocol (HTTP) เป็น โปรโตคอลที่ใช้เป็นหลักในการเข้าถึงข้อมูลบนเว็บไซต์ โดย HTTP จะใช้บริการของ TCP ผ่าน wellknown port หมายเลข 80 โดยแลกเปลี่ยน HTTP Transaction การลีสื่อสารของ HTTP เป็น โปรโตคอลที่ไม่จำสถานะ (Stateless Protocol) แม้ว่ามันจะใช้บริการของ TCP ก็ตาม ซึ่งการลีสื่อสารทุกครั้งของต้องร้องขอการ เชื่อมต่อเครือข่ายก่อนทุกๆ ครั้งซึ่งแตกต่างกับโปรโตคอลที่จำสถานะ หรือ stateful protocol

HTTP Transaction จะห่วงโซ่คลื่นเรื่องเดียวโดยความ 2 แบบคือ: การร้องขอ (Request) และ การตอบสนอง (Response) โดยที่เครื่องคอมพิวเตอร์เริ่มต้นการติดต่อ โดยการส่งข้อความ ร้องขอ หลังจากนั้นเครื่องให้บริการ หรือ เครื่อง server จะตอบกลับด้วย response message



HTTP message ทั้งข้อความแบบการร้องขอ และการตอบสนอง ต่างก็มีรูปแบบที่คล้ายคลึงกัน

- Request message ประกอบด้วย request line, header, และ body
- Response message ประกอบด้วย response line, header และ body



HTTP Message

องค์ประกอบของ message

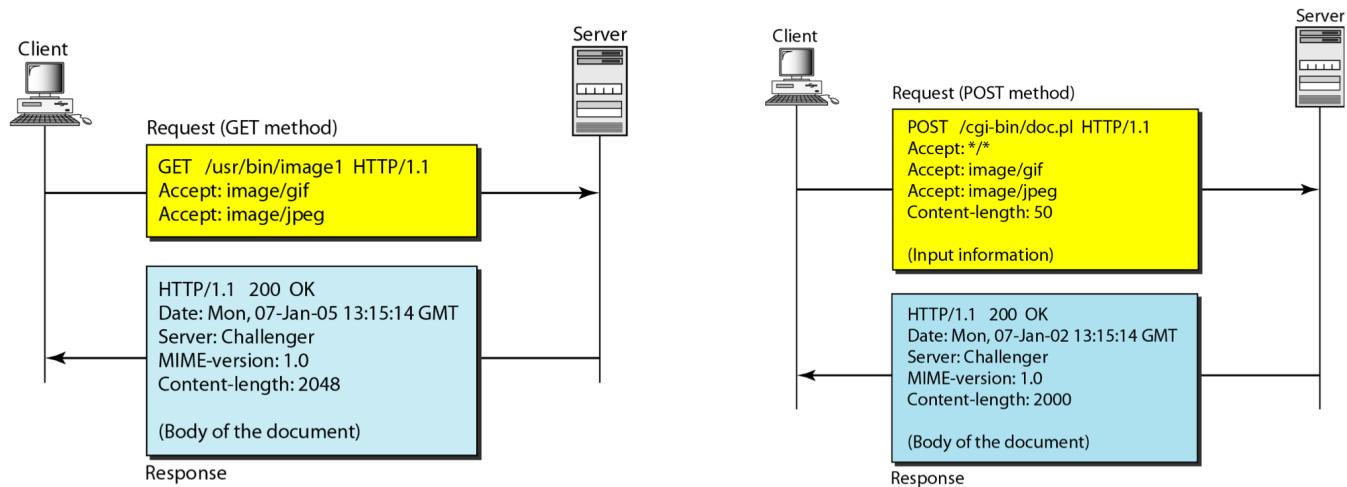
- Request type เป็นส่วนที่ใช้ในข้อความร้องขอนั่นๆ ซึ่ง Request type ใน HTTP/1.1
- HTTP version เวอร์ชันล่าสุดของ HTTP คือ 1.1
- Status code จะใช้ใน Response message ซึ่ง Status code จะมีความคล้ายคลึงกับ FTP และ SMTP โพรโตคอล โดยจะคำอธิบาย Status code ในรูปแบบของข้อความด้วย
- Status phrase ส่วนนี้จะใช้ใน Response message ซึ่งอธิบาย Status code ในรูปแบบของข้อความ

Method	Action
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
OPTION	Inquires about available options

Code	Phrase	Description
Informational		
100	Continue	The initial part of the request has been received, and the client may continue with its request.
101	Switching	The server is complying with a client request to switch protocols defined in the upgrade header.
Success		
200	OK	The request is successful.
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.

Code	Phrase	Description
Redirection		
301	Moved permanently	The requested URL is no longer used by the server.
302	Moved temporarily	The requested URL has moved temporarily.
304	Not modified	The document has not been modified.
Client Error		
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
Server Error		
500	Internal server error	There is an error, such as a crash, at the server site.
501	Not implemented	The action requested cannot be performed.
503	Service unavailable	The service is temporarily unavailable, but may be requested in the future.

HTTP Message



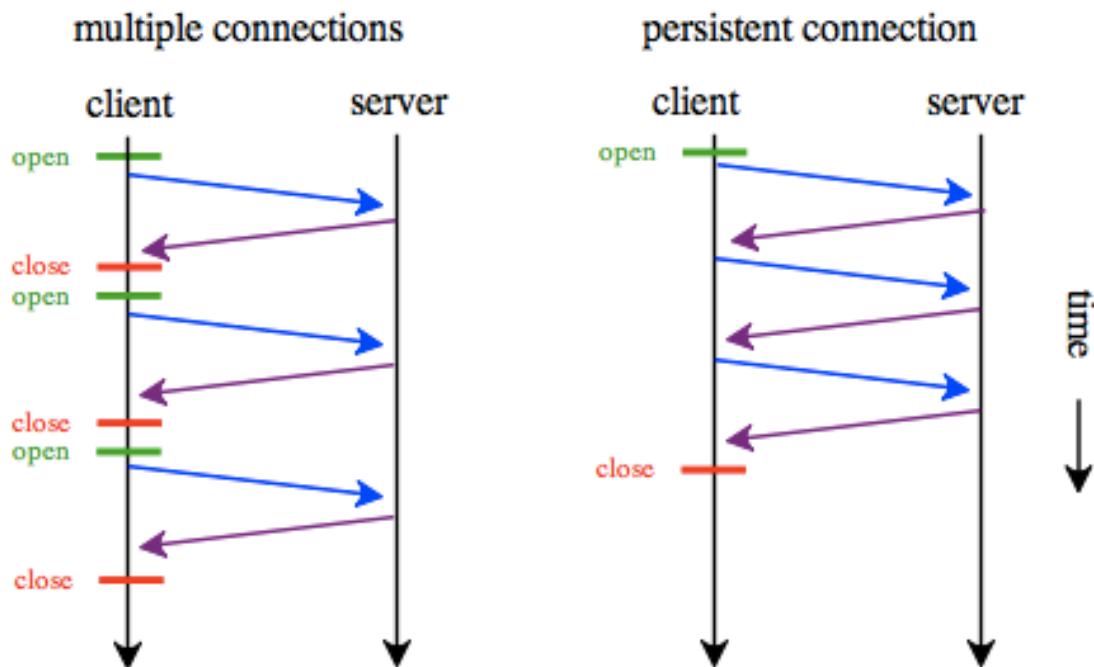
```
cjundang:~ jacaran$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /~jacaran/2011/index.php HTTP/1.0
```

```
HTTP/1.1 200 OK
Date: Sat, 14 Jan 2012 05:34:33 GMT
Server: Apache/2.2.20 (Unix) mod_ssl/2.2.20 OpenSSL/0.9.8r DAV/2 PHP/5.3.6
X-Powered-By: PHP/5.3.6
Content-Length: 1733
Connection: close
Content-Type: text/html
```

```
<!DOCTYPE html
PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html lang="en">
<head>
```

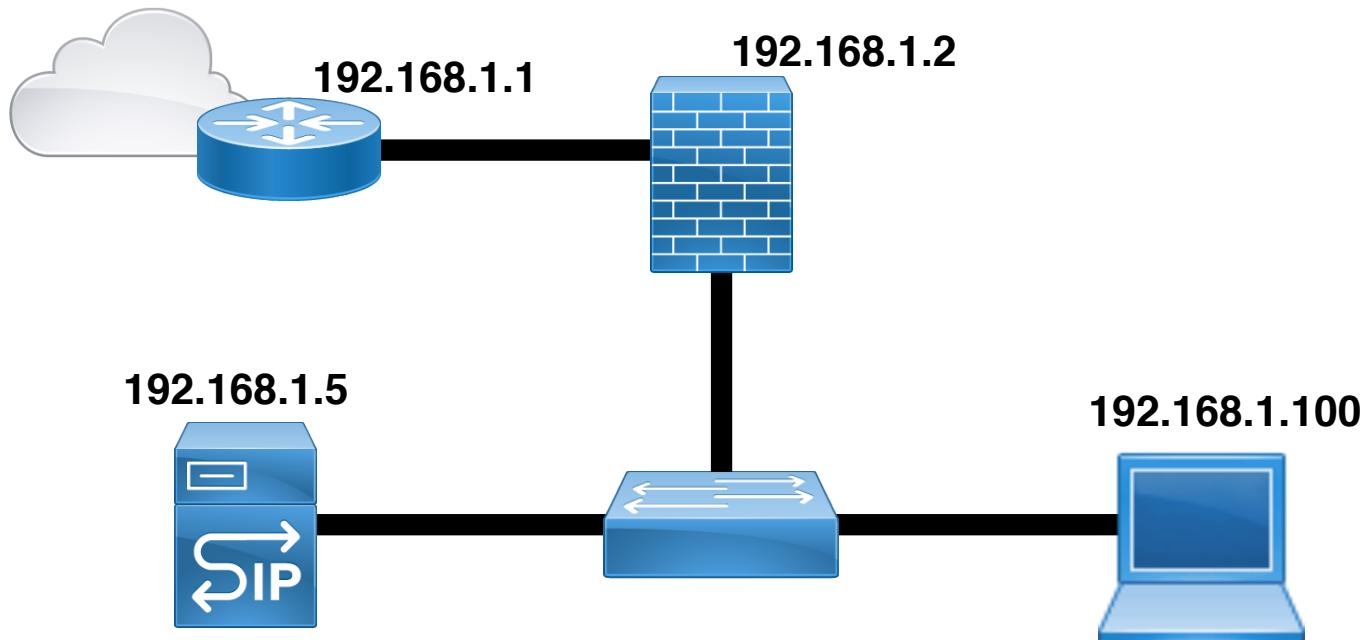
```
<link rel="stylesheet" type="text/css" href="style.css" />
```

Persistent/None Persistent Connection



Web Proxy

Proxy server เป็นคอมพิวเตอร์ที่เก็บสำเนาของการตอบสนองของการตอบต่อการร้องขอ ที่ผ่านมานั้น เมื่อไคลเอนท์ส่งคำร้องขอไปยัง Proxy server ซึ่งเซิร์ฟเวอร์จะตรวจสอบแคช (Cache) ถ้าหากว่าการตอบสนองนั้นไม่ได้เก็บไว้ในแคช เซิร์ฟเวอร์ก็จะส่งคำร้องขอที่ส่งมานั้นไปยังเซิร์ฟเวอร์ที่ตรงกัน ซึ่งข้อความการตอบสนองที่ส่งมานั้น จะถูกส่งไปยัง Proxy server และเก็บไว้สำหรับการร้องขอในครั้งต่อไปจากไคลเอนท์อีกด้วย



File Transfer Protocol - FTP

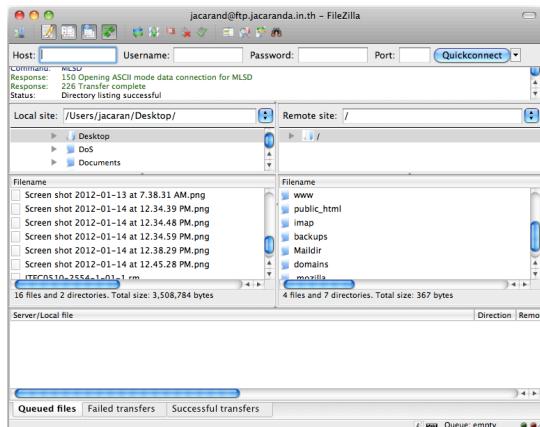
File Transfer Protocol (FTP) เป็นโปรโตคอลแบบ client-server และทำงานบนเครือข่ายแบบ TCP/IP ใช้สำหรับการคัดลอกไฟล์จากโฮสต์หนึ่งไปยังอีกโฮสต์หนึ่ง โดยโปรแกรม FTP client จะติดต่อกับ FTP server ที่พอร์ต 21 ซึ่งเป็น wellknown port และถ่ายโอนข้อมูลที่พอร์ต 20

FTP เป็นโปรโตคอลชั้นแอปพลิเคชัน ที่รองรับไฟล์แลกเปลี่ยนระหว่างระบบที่แตกต่างกัน โดยโปรโตคอล FTP สื่อสารระหว่างระบบที่แตกต่างกันโดยการเข้ารหัส (encoding) ด้วยรหัส ASCII ซึ่งไฟล์จะถูกคัดลอกและส่งต่อไปยังระบบภายใต้เครือข่าย โดยไฟล์ต้นฉบับจะยังคงไม่เปลี่ยนแปลง นอกจากนี้มีกระบวนการป้องกันการเข้าถึง (Access Control) ไฟล์จะกระทำการผ่านชั้นตอนการเข้าสู่ระบบ คือ ใช้ชื่อ เล็กอินและรหัสผ่าน

อย่างไรก็ตาม ก่อนที่ไฟล์จะมีการถ่ายโอนจริงนั้น ประเภทของไฟล์ (file type) โครงสร้างข้อมูล (data structure) และโหมดของการขนส่ง (transmission mode) จะถูกกำหนดโดย ไดเลอเน็ต ก่อน โดยส่วนใหญ่คุณการเชื่อมต่อผ่านพอร์ต 21 การตอบสนองจากเครื่องให้บริการถูกส่งจากเซิร์ฟเวอร์ไปยังไดเลอเน็ต ซึ่งการขนส่งข้อมูลนั้นมีการสื่อสาร 3 แบบ ได้แก่

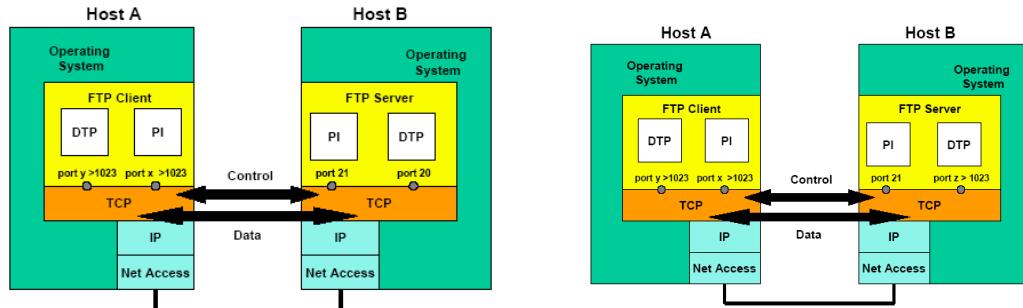
- การสำเนาไฟล์ จากเครื่อง ให้บริการไปยังเครื่องถูกเข้ารหัส
- การสำเนาไฟล์ จากเครื่อง ให้ลูกเขยไปยังเครื่องแม่เขย
- การส่งรายชื่อของไดเรกทอรีหรือรายชื่อไฟล์ ที่ถูกส่งจากเซิร์ฟเวอร์ไปให้ไดเลอเน็ต

โปรแกรม FTP เป็นโปรแกรมชั้นประยุกต์ใช้สำหรับการถ่ายโอนไฟล์ โดยไม่จำเป็นต้องปฏิสัมพันธ์พื้นฐานกับโปรโตคอล FTP โดยตรง ระบบปฏิบัติการส่วนใหญ่ให้บริการโปรแกรมที่มีล้วนติดต่อผู้ใช้ที่ใช้งานได้ง่าย (user-friendly interface) ระหว่างโปรแกรม FTP และผู้ใช้ทั้งในรูปแบบของ command line หรือโปรแกรมแบบ GUI ได้แก่ FileZilla เป็นต้น



```
cjundang:Desktop jacaran$ ftp ftp.jacaranda.in.th
Connected to ftp.jacaranda.in.th.
220 ProFTPD 1.3.3e Server ready.
Name (ftp.jacaranda.in.th:jacaran): jacaran
331 Password required for jacaran
Password:
530 Login incorrect.
ftp: Login failed
ftp> quit
221 Goodbye.
cjundang:Desktop jacaran$
```

File Transfer Protocol - FTP



ในการถ่ายโอนข้อมูล FTP ต้องใช้การเชื่อมต่อ 2 แบบ ได้แก่ การควบคุมการเชื่อมต่อ (connection control) และการเชื่อมต่อข้อมูล (data control) โปรแกรมไคลเอนต์ได้รับการอนุมัติ จากการควบคุมการเชื่อมต่อ ไคลเอนต์จะรีโมทเพื่อเรียกดู ได้เรียกทรัพย์ โดยการส่งคำสั่งผ่านการควบคุมการเชื่อมต่อ เมื่อเซิร์ฟเวอร์ ได้รับคำสั่งสำหรับการถ่ายโอนไฟล์แล้ว เซิร์ฟเวอร์จะเปิด การเชื่อมต่อข้อมูล TCP (พอร์ต 20) ให้กับไคลเอนต์ หลังจากได้ถ่ายโอนพียงหนึ่งไฟล์ เซิร์ฟเวอร์ก็จะปิดการเชื่อมต่อ และ เซิร์ฟเวอร์จะเปิดการเชื่อมต่อข้อมูล TCP อีก ครั้งที่สอง เพื่อการถ่ายโอนไฟล์อีกต่อไป

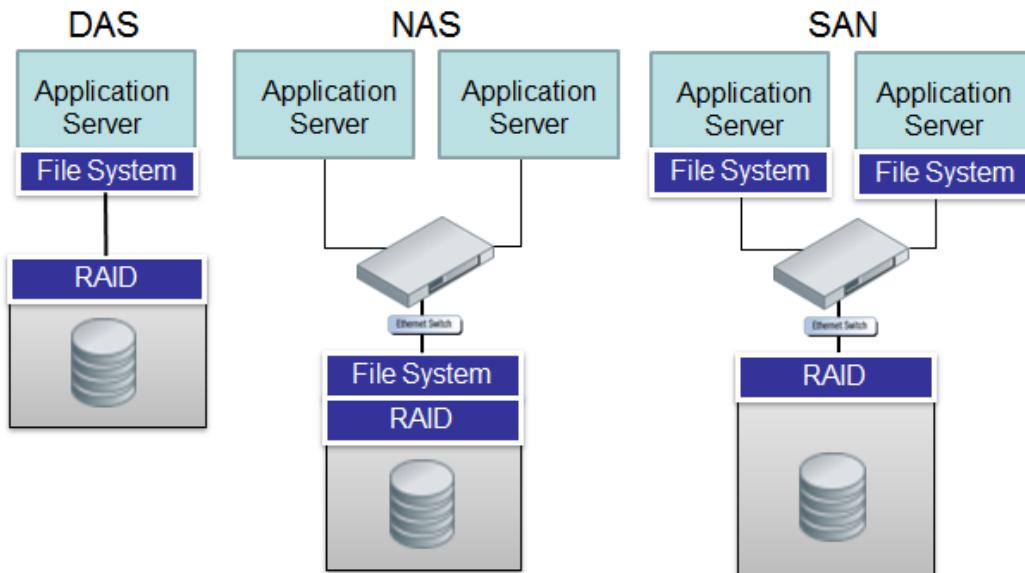
Anonymous FTP เป็นการสร้างชื่อบัญชีผู้ใช้ เพื่อให้ผู้ใช้บริการสามารถเข้าถึงบริการ ftp ได้โดยที่ไม่จำเป็นต้องเป็น สมาชิก ในองค์กรนั้นๆ โดยปกติแล้วการเข้าถึงบริการต้องอาศัย account และ รหัสผ่าน แต่บางครั้ง องค์กร ให้แจกจ่ายไฟล์บาง ไฟล์ที่ไม่จำเป็นต้องตรวจสอบตัวตน หรือ ให้บริการแก่บุคคลคลั่วทั่วไป ดังนั้นผู้ใช้สามารถเข้าถึงได้ด้วยชื่อบัญชีพิเศษ anonymous โดยกำหนดรหัสผ่าน ในรูปแบบของ email เช่น toi@jacaranda ผู้ใช้สามารถเข้าถึงระบบได้ แต่อาจได้ด้วยสิทธิ์ที่ให้จำกัดเพียง เท่านั้น

Network File System

Network File System หรือ NFS คือ บริการที่ทำให้เครื่องคอมพิวเตอร์สามารถเข้าถึง File และ Directory บนคอมพิวเตอร์เครื่องอื่นๆ ได้เหมือนกับใช้งานเครื่องของตัวเอง โดยสามารถใช้บริการได้อย่างสะดวก ง่ายและมีประสิทธิภาพผ่านระบบเครือข่าย Network โดยระบบปฏิบัติการของเครื่องลูกข่ายไม่จำเป็นต้องเป็นระบบปฏิบัติการเดียวกันกับเครื่องแม่ข่ายที่ให้บริการ NFS

Storage ประเภทต่างๆ

- DAS (Direct Attach Storage) เชื่อมต่อโดยตรงกับคอมพิวเตอร์
- NAS (Network Attach Storage) เชื่อมต่อใช้งานผ่านระบบ Network มีระบบบริหารจัดการอยู่ในตัวเอง
- SAN (Storage Area Network) เชื่อมต่อใช้งานผ่านระบบ Network โดยเทคโนโลยี Fiber Channel นิยมใช้กับเครื่องแม่ข่าย มีการรับส่งข้อมูลแบบบล็อก



12

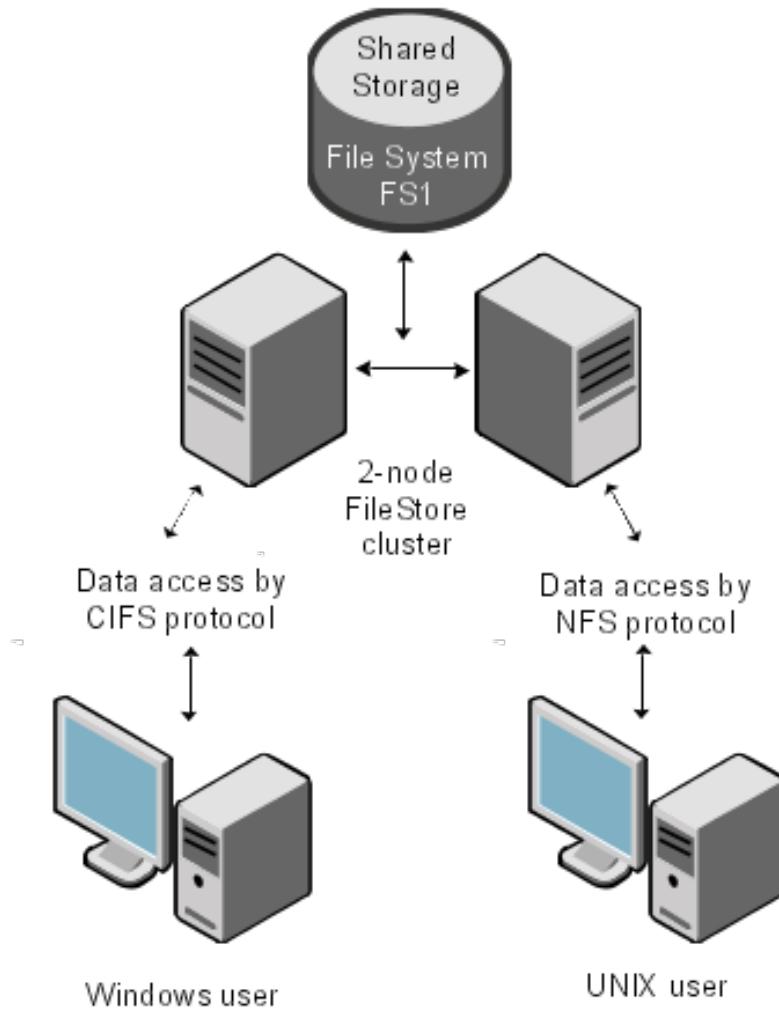
Network File System

Network File System (NFS) เป็นรูปแบบที่ถูกใช้โดยระบบ Unix และ Linux ทำให้ไฟล์ต่างๆ สามารถถูกแชร์แบบ transparently หรือเรียกใช้งานระหว่างเครื่องเซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ ฯลฯ ทำให้ผู้ใช้งานสามารถดู เก็บ หรือแก้ไขไฟล์ข้อมูลต่างๆ ที่อยู่ในเครื่องปลายทาง (remote computer) ได้ผ่านเครื่องคอมพิวเตอร์ที่กำลังใช้งานอยู่ ผู้ใช้งานจะสามารถเรียกใช้ไฟล์หรือโฟลเดอร์ผ่านระบบเครือข่ายซึ่งอยู่ในเครื่องคอมพิวเตอร์ปลายทางได้โดยตรง (วิธีการนี้เรียกว่าการ mount NFS)

Common Internet File System (CIFS) เป็นรูปแบบที่ถูกใช้โดยระบบปฏิบัติการ Windows เพื่อการแชร์ไฟล์หรือข้อมูล โดยใช้โมเดล client/server ในการเรียกใช้งาน ตัวโปรแกรมบนเครื่อง client จะร้องขอ (request) ไปยังฝั่ง server เพื่อการเข้าใช้งานไฟล์หรือส่งคำสั่งไปเพื่อให้โปรแกรมฝั่ง server ทำงาน จากนั้นก็จะมีการส่งคำสั่งตอบสนอง (response) กลับไปยังฝั่ง client เพื่อเป็นการแจ้งผลการทำงาน

CIFS เป็นระบบเปิดสามารถนำไปพัฒนาต่อเองได้ ทาง Microsoft จึงได้นำมาพัฒนาต่อภายเป็น Server Message Block Protocol (SMB) โดยใช้งานผ่าน TCP/IP protocol

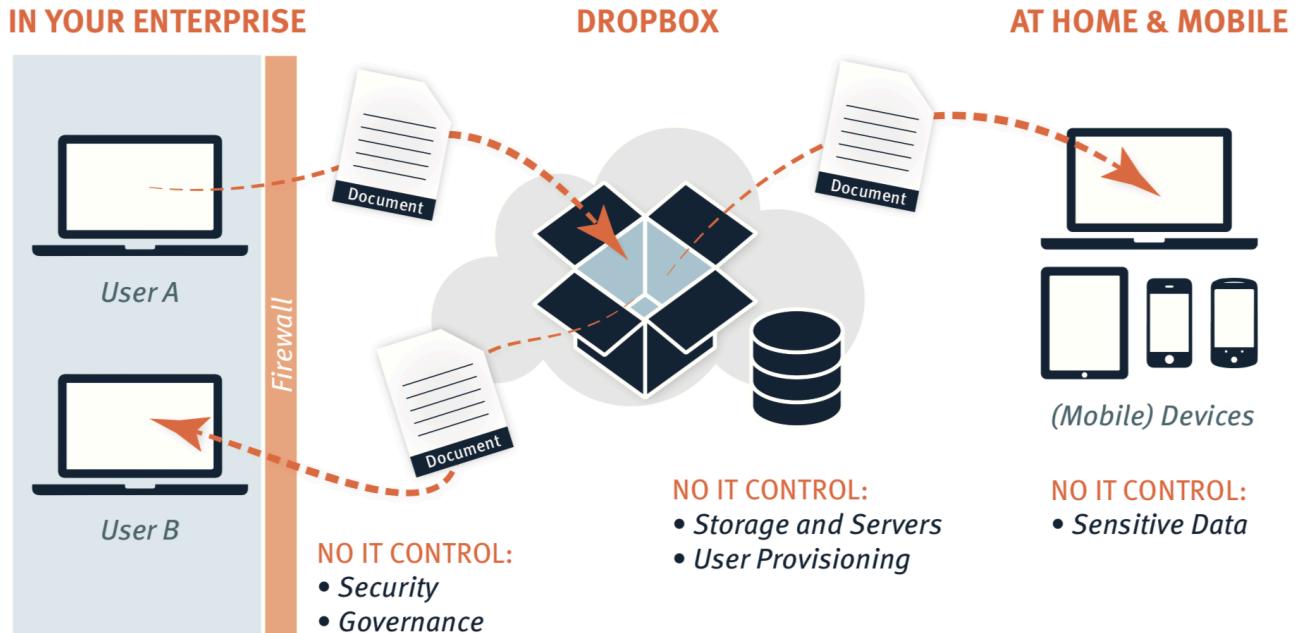
การเชื่อมต่อ storage แบบ NAS ก็ได้นำ NFS และ CIFS มาใช้เพื่อรับข้อมูลที่เป็น primary file system ของระบบอีกด้วย เนื่องด้วย CIFS มีระบบลีโอาร์ที่ชับช้อน (chatty) มากกว่า ดังนั้นการนำไปใช้งานผ่าน WAN จึงจำเป็นต้องอาศัยโปรแกรมหรืออุปกรณ์ประเภท file protocol optimization เพื่อช่วยรักษาเสถียรภาพและประสิทธิภาพให้คงที่



File Sharing

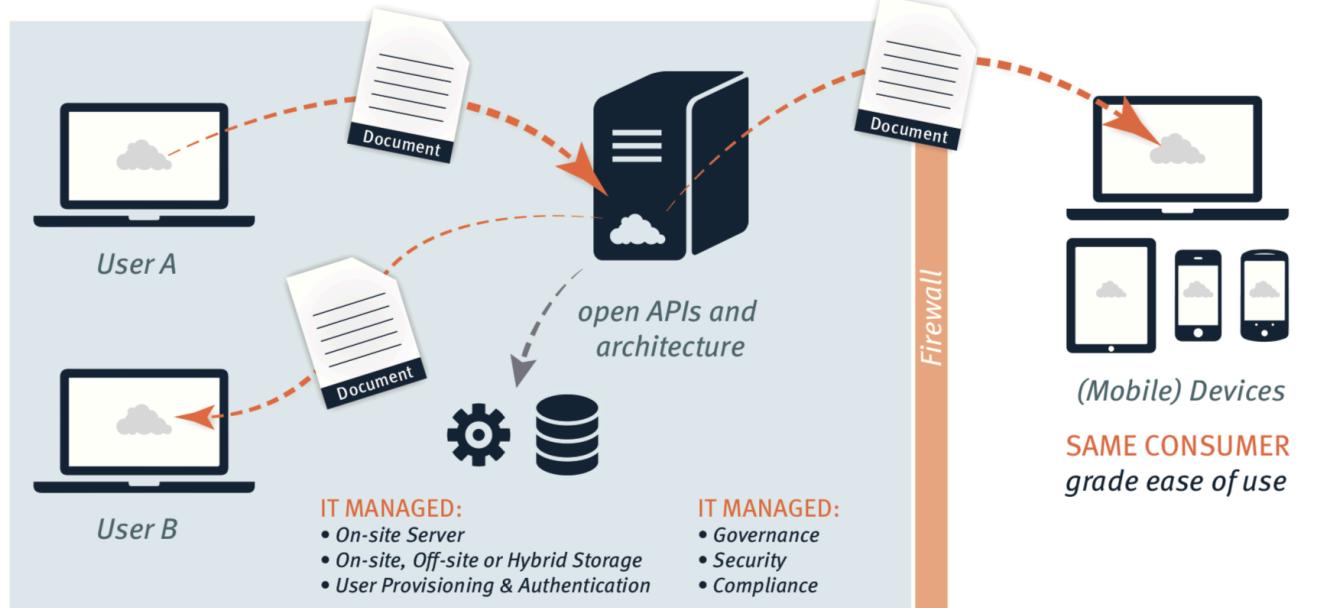
ownCloud

Dropbox Problem in Actions



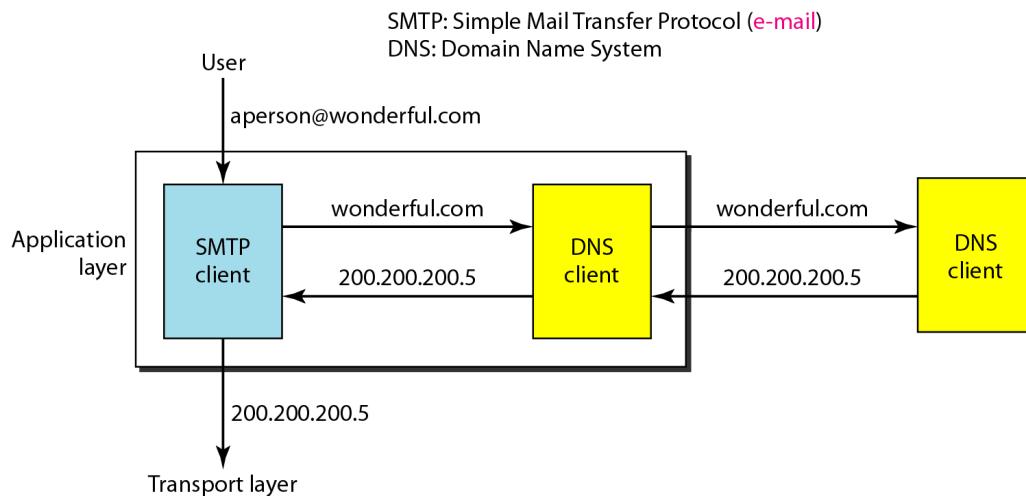
ownCloud in Actions

IN YOUR ENTERPRISE



Domain Name System

การใช้งานแอพพลิเคชัน ในหลายแอพพลิเคชันเลยอร์ของอินเทอร์เน็ตโภคเด่นนี้เป็นการร้องขอข้อมูลแบบโคลอนต์/เชิร์ฟเวอร์ (Client/Server Paradigm) ซึ่งโปรแกรมโคลอนต์ / เชิร์ฟเวอร์ สามารถแบ่งออกเป็น 2 ประเภท ได้แก่ 1) สนับสนุนผู้ใช้ เช่น การใช้งานโปรแกรม email เป็นต้น หรือระบบที่สนับสนุนการทำงานของโปรแกรมประยุกต์ ได้แก่ Domain Name System (DNS) เป็นต้น



เมื่อเครือข่ายมีขนาดเล็กการจัดการระบบซื้อทำได้ง่าย โดยจับคู่ชื่อ และ IP Address แล้วบันทึกไว้ในไฟล์ โดยไฟล์ที่เก็บข้อมูลนั้นมีขนาดเล็กซึ่งเรียกว่าไฟล์ hosts โดยจัดเก็บไว้ในดิสก์ หลังจากนั้นไฟล์ดังกล่าวจะถูกปรับปรุงเป็นระยะ

เมื่อเครือข่ายมีขนาดใหญ่ขึ้นแล้ว ไฟล์ hosts ที่มีอยู่นั้นใหญ่เกินกว่าที่จะเก็บไว้ในไฟล์เพียงไฟล์เดียว อีกทั้งยากที่จะปรับปรุงข้อมูลให้ทันสมัยเมื่อโฉลกใดๆ มีการเปลี่ยนแปลง นอกจากนี้ การเก็บไฟล์ hosts ไว้ที่เครื่องให้บริการเครื่องเดียว จะเกิด traffic jam ที่พอร์ตของเครื่องให้บริการ

แนวทางแก้ไขคือการแบ่งไฟล์ hosts เป็นไฟล์ย่อยๆ ขนาดเล็ก แล้วแยกไฟล์เหล่านั้นไปเก็บไว้ในเครื่องที่ให้บริการต่างๆ เครื่องคอมพิวเตอร์ที่ต้องการค้นหา IP address จากชื่อเครื่อง จะสอบถามข้อมูลจากเครื่องให้บริการที่อยู่ใกล้เครื่องจัดเก็บไฟล์ hosts ขนาดเล็ก เพื่อสอบถามข้อมูลจากเครื่องที่อยู่ใกล้ที่สุด วิธีการนี้จะถูกนำมาใช้โดย Domain Name System (DNS)

Domain Name System

Domain Name System (DNS) เป็นโปรแกรมแบบไคลเอนต์/เซิร์ฟเวอร์ที่ใช้ในการระบุชื่อเครื่องแบบไม่ซ้ำกันและเป็นชื่อที่คนเข้าใจได้ง่าย มีความหมายชัดเจนโดยละเอียดมากนั้นถูกกำหนดให้แก่เครื่องคอมพิวเตอร์ ได้เลือกจาก name space

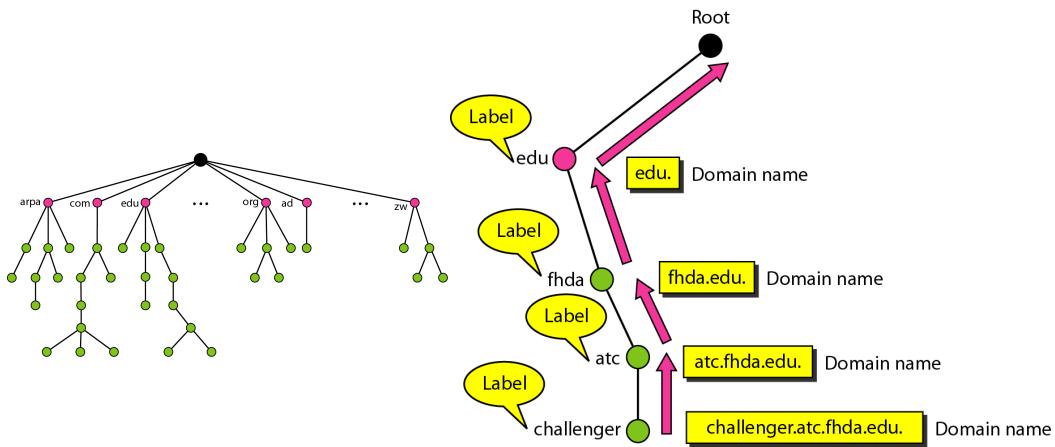
- Flat Name Space เป็นการกำหนดชื่ออย่างง่ายโดยเรียงลำดับชื่อตามตัวอักษรโดยที่ไม่มีโครงสร้างข้อตีอีกเมื่อสำหรับเครือข่ายที่มีขนาดเล็ก

- Hierarchical Name Space เป็นการกำหนดองค์ประกอบของชื่อมาจากหลายส่วนได้แก่ 1) กำหนดจากลักษณะขององค์กร 2) กำหนดจากชื่อขององค์กร 3) กำหนดจากชื่อของแผนก ผู้มีอำนาจ (authority) สามารถกำหนดและควบคุมการใช้งานชื่อโดยใช้วิธีการ Decentralized ได้ ผู้มีสิทธิ์สูงสุดของส่วนกลางกำหนดส่วนหนึ่งของชื่อ โดยนิยามตามลักษณะขององค์กรและชื่อขององค์กร ความรับผิดชอบในส่วนที่เหลือของชื่อก็สามารถให้กับผู้ได้รับมอบหมายขององค์กรดูแล

Hierarchical Name Space

Hierarchical Name Space เป็นชื่อโดเมนจะได้รับการออกแบบขึ้นโดยอาศัยโครงสร้างแบบต้นไม้ โดยให้ชื่อถูกเก็บไว้ใน Inverted-tree Structure ที่มีส่วนราชการยู่ด้านบน และต้นไม้นี้จะมีเพียง 128 ระดับด้วยกัน : ระดับ 0 (root) จนถึง ระดับ 127

ในแต่ละโหนดในโครงสร้างต้นไม้นั้นจะมี **label** ที่เป็น String ยาวสูงสุด 63 ตัวอักษร root label เป็น Null String สำหรับ DNS นั้นต้องการโหลดลูกที่มี label ที่แตกต่างกัน เพื่อการันตีได้ว่า ชื่อของโดเมนจะไม่ซ้ำกัน โหนดแต่ละตัวของโครงสร้างต้นไม้ถูกกำหนดเป็นชื่อของโดเมน ชื่อโดเมนแบบเต็ม (Full name) คือลำดับของโหนดที่คั่นโดยจุด (.) ชื่อ โดเมนอ่านจากโหนดถึง root ซึ่งเป็นคำ กpull



Fully Qualifies Domain Name (FQDN)

Fully Qualifies Domain Name (FQDN) เป็นชื่อโดเมนที่ปิดโดย null string ซึ่งมีชื่อเต็มของโฮสต์ โดยกำหนดชื่อของโฮสต์ที่ไม่ซ้ำกัน ตัวอย่างเช่น jacaranda.informatic.wu.ac.th : Jacaranda คือชื่อคอมพิวเตอร์ ตั้งอยู่ที่ สำนักสารสนเทศศาสตร์ มหาวิทยาลัยลักษณ์, ประเทศไทย เป็นต้น

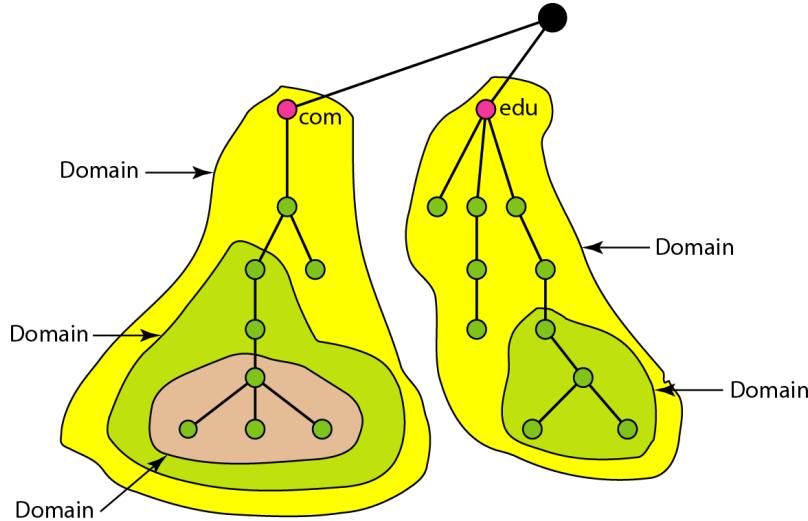
Partially Qualified Domain Name (PQDN)

Partially Qualified Domain Name (PQDN) เป็นชื่อโดเมนที่จะไม่ถูกปิดโดย null เริ่มต้น จากโหนดแต่ยังไม่ถึง root PQDN จะถูกใช้เมื่อชื่อที่จะแปลง (resolve) นั้นเป็นของเว็บไซต์เดียวกันกับไคลเอนต์ ตัวอย่างเช่น หากผู้ใช้จาก informative.wu.ac.th ต้องการที่จะหา IP Address ของเครื่อง Jacaranda สามารถกำหนดชื่อเพียงแค่ Jacaranda เท่านั้น DNS ไคลเอนต์จะเพิ่ม informative.wu.ac.th ต่อท้ายที่อยู่นั้น ก่อนที่จะส่งไปยังเซิร์ฟเวอร์

Domain Name System

Name Space

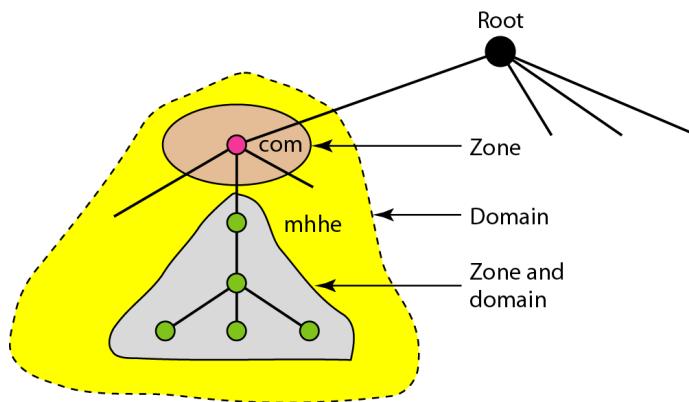
โดเมน (domain) คุกกำหนดให้เป็นส่วนย่อยของต้นไม้ ของ Domain Name Space ซึ่งเป็นข้อมูลที่อยู่ใน Domain Name Space จะต้องถูกเก็บไว้ แต่ก็จะไม่มีประสิทธิภาพมาก และก็ยังไม่น่าเชื่อถือ ที่จะมีคอมพิวเตอร์เพียงเครื่องเดียวเก็บข้อมูล เป็นจำนวนมาก



วิธีการแก้ปัญหาเหล่านี้คือ การกระจายข้อมูลระหว่างเครื่องคอมพิวเตอร์จำนวนมาก ที่เรียกว่า **DNS Server** นี้ คือการ แบ่งพื้นที่ทั้งหมดออกเป็นหลายโดเมน ในชั้นแรก Root เพียงหนึ่งเดียว และ สามารถสร้าง subtrees ได้หลายโดเมน ในขณะที่ Tree เป็นโหนดชั้นแรก และ DNS อนุญาตให้โดเมนถูกแบ่งออกไปอีกเป็นโดเมนที่มีขนาดเล็กลง แต่ละเซิร์ฟเวอร์สามารถรับผิดชอบ (authoritative) ได้ทั้งโดเมนขนาดใหญ่หรือ ขนาดเล็ก

Zone : ชั้นของ domain name ที่สมบูรณ์นั้น ไม่สามารถเก็บไว้บนเซิร์ฟเวอร์เดียวได้ ก็จะแบ่งออกไปเก็บไว้กับ เซิร์ฟเวอร์จำนวนมาก สิ่งที่เซิร์ฟเวอร์เป็นผู้รับผิดชอบ หรือ มีอำนาจจัดการ เรียกว่า โซน (Zone)

เราสามารถกำหนด โซน เป็นส่วนหนึ่งที่อยู่ติดกัน ของต้นไม้ทั้งหมด ถ้าเซิร์ฟเวอร์ตอบรับความรับผิดชอบในโดเมนนั้น และไม่ได้แบ่งโดเมนออกเป็นโดเมนย่อยที่มีขนาดเล็ก เป็นเช่นนี้โดเมนและโซนจะหมายถึง สิ่งเดียวกัน ในทางกลับกัน ถ้า เซิร์ฟเวอร์ทำการแบ่งโดเมนออกเป็นโดเมนย่อยๆ และมอบหมายอำนาจหน้าที่ส่วนหนึ่งไปยังเซิร์ฟเวอร์อื่นๆแล้วนั้น โดเมนและ โซนจะหมายถึงสิ่งที่แตกต่างกัน



Domain Name System

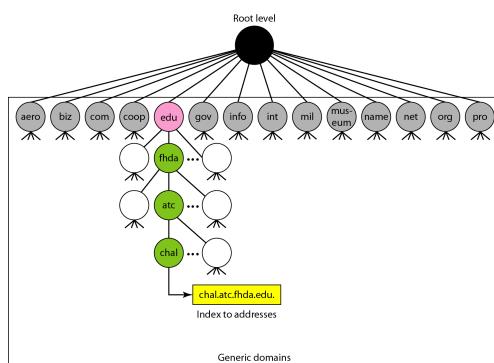
Root server เป็นเซิร์ฟเวอร์ ที่โอนจะมีส่วนประกอบของต้นไม้ทั้งต้น และมักจะไม่ได้เก็บข้อมูลเกี่ยวกับโดเมนใดๆ แต่ผู้ได้รับมอบหมายจากไปยังเซิร์ฟเวอร์อื่นนั้น จะทำการอ้างอิงไปยังเซิร์ฟเวอร์เหล่านั้น DNS กำหนดเซิร์ฟเวอร์เป็น 2 ประเภท ได้แก่: Primary server และ Secondary server

Primary server เป็นเซิร์ฟเวอร์ ที่เก็บไฟล์ซึ่งเกี่ยวกับโฉน เป็นอำนาจหน้าที่และความรับผิดชอบในการสร้าง บำรุงรักษา และปรับปรุง ไฟล์โฉนที่อยู่บนโลคอลดิสก์ (Local Disk)

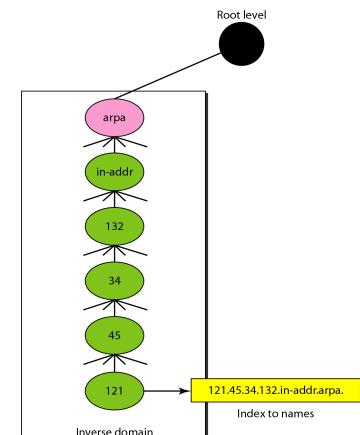
Secondary server เป็นเซิร์ฟเวอร์ ที่โอนถ่ายข้อมูลที่ได้รับจากเซิร์ฟเวอร์ อื่น และเก็บไฟล์บนโลคอลดิสก์ Secondary server จะไม่ได้สร้างหรือปรับปรุงไฟล์โฉน แต่ถ้าหากจำเป็นต้องมีการปรับปรุง ก็จะต้องดำเนินการโดย Primary server เท่านั้น เมื่อแก้ไขปรับปรุงแล้ว ก็จะส่งเวอร์ชันอัพเดทนั้นไปยัง Secondary server ตามลำดับต่อไป

Domain name space บนอินเทอร์เน็ตนั้น แบ่งออกเป็น 3 ส่วน: Generic domains, Country domains และ Inverse domains

- **Generic domains:** มี 7 generic labels แบบดั้งเดิม ซึ่งแต่ละแบบจะสามารถระบุถึงชนิดหรือคุณลักษณะขององค์กร และเมื่อเร็วๆ นี้ได้มีการเพิ่ม labels ใหม่เข้ามาด้วย ตัวอย่างของ Generic domains ได้แก่ .com .net และ .biz เป็นต้น
- **Country domains:** ในแต่ละ Country domains จะสามารถระบุประเทศ ซึ่งจะใช้ตัวย่อ 2 ตัวของประเทศนั้นๆ (เช่น th สำหรับประเทศไทย) Label ลำดับที่สอง สามารถเป็นชนิดหรือคุณลักษณะขององค์กรนั้นๆ (เช่น ac.th สำหรับสถานศึกษาในประเทศไทย)
- **Inverse domains** เป็นชื่อโดเมนให้สำหรับ IP Address ที่กำหนดไว้ ซึ่งเรียกว่า address-to-name เซิร์ฟเวอร์จะถาม resolver และส่งคำร้องขอไปยังเซิร์ฟเวอร์ DNS เพื่อจับคู่ที่อยู่กับชื่อ โดยเครื่องไคลเอนท์ที่ได้รับอนุญาตเท่านั้น

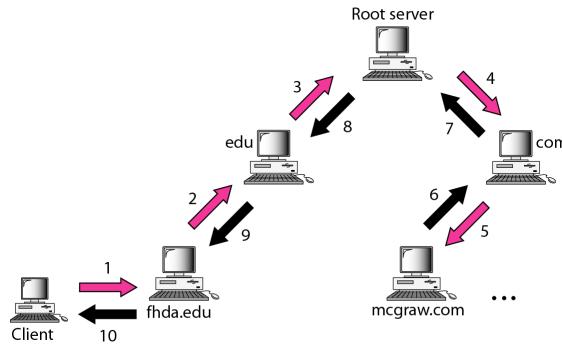


Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

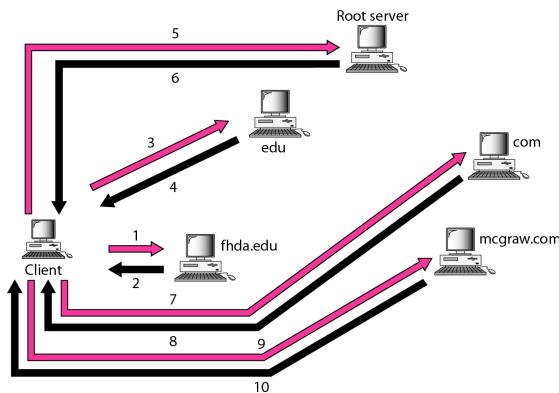


Domain Name System

Resolution เป็นกระบวนการจับคู่ชื่อกับที่อยู่ หรือที่อยู่กับชื่อนั้น เรียกว่า **Name-address Resolution** Name Servers เป็นคอมพิวเตอร์ที่เรียกว่า **DNS server program** ซึ่งถูกจัดให้อยู่ในลักษณะของลำดับชั้น **DNS client** นั้นจะเรียกว่า **Resolver** ซึ่งหมายถึง การจับคู่ชื่อกับที่อยู่ หรือที่อยู่กับชื่อนั้น



ใน **Recursive Resolution** โคลอเอนท์จะส่งคำร้องขอไปยังเซิร์ฟเวอร์ที่ติดต่อกัน เป็นลักษณะต่อเนื่องกันเป็นทอดๆ ซึ่งถ้าเป็นเซิร์ฟเวอร์ที่มีอำนาจของชื่อโดเมนนั้นๆ เชิร์ฟเวอร์ก็จะตอบคำร้องขอ แต่ถ้าเซิร์ฟเวอร์นั้นไม่ได้เป็นผู้มีอำนาจ ก็จะส่งคำร้องขอนั้นต่อไปยังเซิร์ฟเวอร์อื่นเพื่อดำเนินการต่อๆ ไปจนได้คำตอบ



ใน **Iterative resolution** โคลอเอนท์จะส่งคำร้องขอไปยังเซิร์ฟเวอร์ที่ติดต่อกัน ซึ่งถ้าเป็นเซิร์ฟเวอร์ที่มีอำนาจของชื่อโดเมนนั้นๆ แต่ถ้าเซิร์ฟเวอร์นั้นไม่ได้เป็นผู้มีอำนาจ ก็จะส่ง IP Address ของ DNS Server ยืน ที่คิดว่าสามารถตอบคำร้องขอได้แทน

อุปสรรคของแต่ละเซิร์ฟเวอร์ มักจะได้รับมาจากการคำร้องขอชื่อที่ไม่ได้มีสิทธิ์หรืออำนาจ ในชื่อโดเมนนั้นๆ ซึ่งเซิร์ฟเวอร์ก็ต้องใช้เวลาในการค้นหา IP address ของเซิร์ฟเวอร์จากฐานข้อมูลตน เพื่อที่จะลดเวลาการค้นหา ซึ่งจะต้องเพิ่มประสิทธิภาพในการจัดการ DNS โดยใช้กลไกที่เรียกว่า แอดเชชัน (**Caching**) เมื่อเซิร์ฟเวอร์ร้องขอการจับคู่ จากเซิร์ฟเวอร์อื่นแล้วได้รับการตอบสนอง เซิร์ฟเวอร์ก็จะจัดเก็บข้อมูลนั้นไว้ในหน่วยความจำแอดเชชัน (**Cache Memory**) ก่อนที่จะส่งไปยังโคลอเอนท์ ซึ่งถ้าโคลอเอนท์ได้หันที่ อย่างไรก็ตาม เพื่อแจ้งให้โคลอเอนท์ที่ตอบสนองมาจากหน่วยความจำแอดเชชัน และไม่ได้มาจากแหล่งที่มาที่มีอำนาจสิทธิ์ของชื่อโดเมนนั้นๆ เซิร์ฟเวอร์จะใส่เครื่องหมายในการตอบกลับเป็น **Unauthoritative**

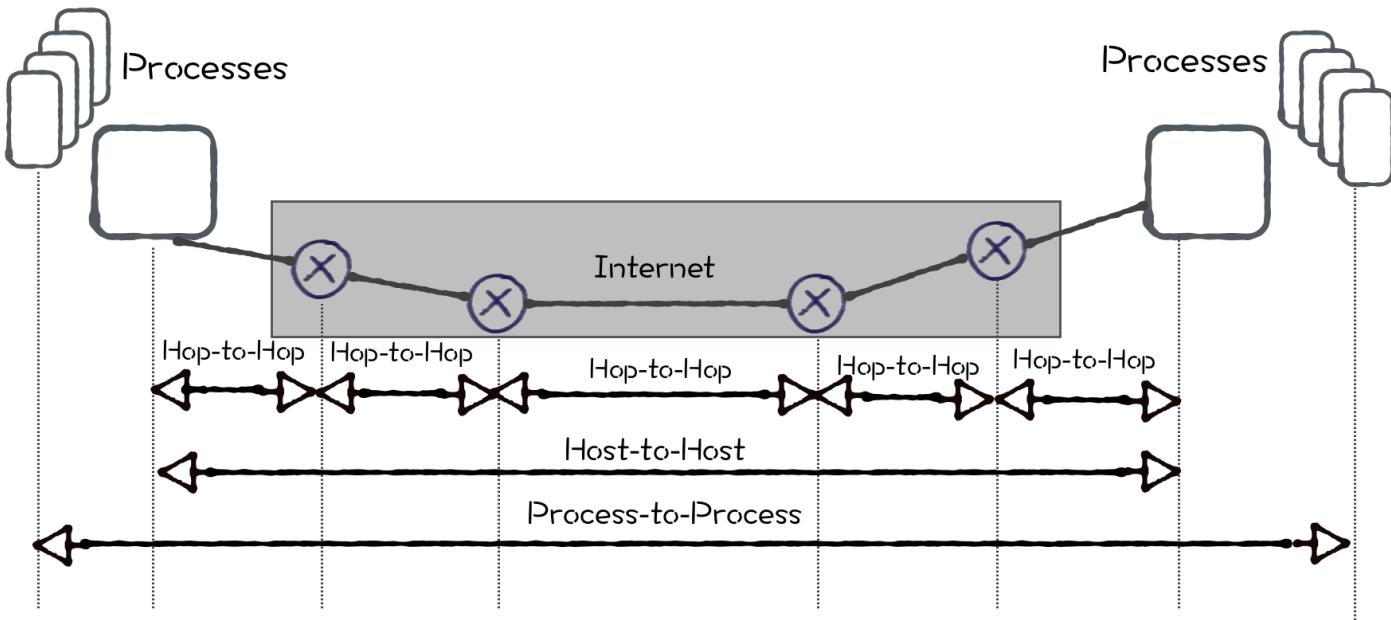
Notes

Module 5

Reliable Protocol

Contents

- Process-to-Process Communication
- Port Address
- Socket Address
- Multiplexing
- Reliable Service
- Connection Establishment
- Transport Control Protocol
- User Defined Protocol



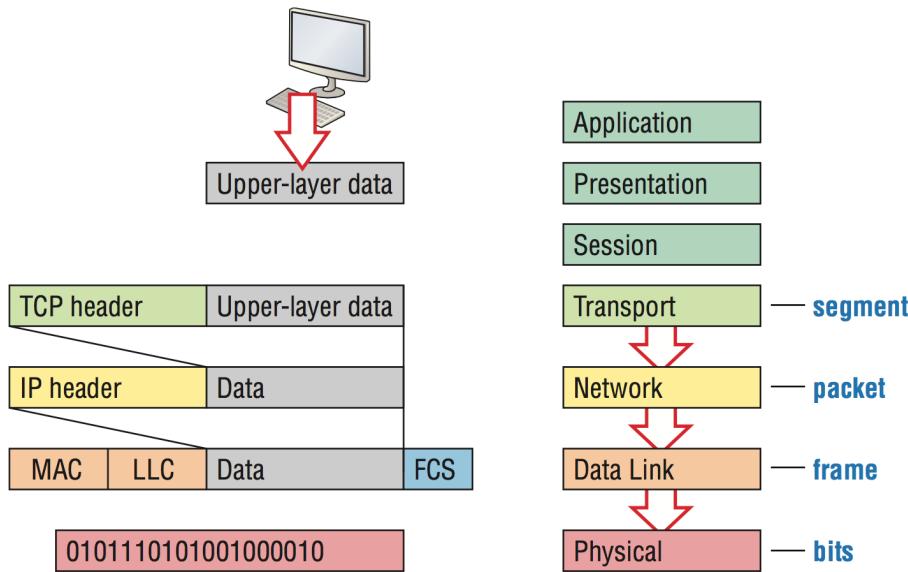
การสื่อสารระหว่าง โปรเซส

การส่งข้อมูลแบบ โหนดถึงโหนด (Node-to-Node Delivery) เป็นการสื่อสาร ในชั้นเชื่อม โยงข้อมูล ซึ่ง สื่อสารโดยตรงจากผู้ส่งถึงผู้รับที่เชื่อมโยงถึงกันผ่านสื่อ หรือเรียกว่า "ฮอน (Hop)" การสื่อสาร ในรูปแบบนี้อาจจะเรียกว่า การสื่อสารแบบจุดถึงจุด (Point-to-Point) และแต่่บินที่เกี่ยวข้อง เป้าหมายหลักของการสื่อสารแบบนี้คือ ส่งข้อมูล ระหว่างโหนด ให้ถูกต้อง ไม่มีข้อผิดพลาด ข้อมูลไม่หาย และไม่ชำรุด

การส่งข้อมูลแบบต้นทางถึงปลายทาง (Source-to-Destination Delivery) เป็นการส่งข้อมูลจากเครื่องต้นทาง ถึงเครื่องปลายทาง โดยส่งผ่านเครือข่ายที่มีโหนดโดยล็อกต์ต่างกัน หรือต่างเครือข่ายกันผ่านอุปกรณ์คันหาเส้นทางหรือ ออยู่ต่างคอลลิชันโดเมน (Collision Domain) อุปกรณ์ที่เป็นตัวกลางมีพิงก์ชันการคันหาเส้นทาง การกำหนดเลขที่อยู่ หรือแม้แต่การแบ่งข้อมูลเป็นส่วนย่อย หากช่องทางที่ผ่านนั้นมีขนาดของเอ็มที่ยู หรือ Maximum Transfer Unit (MTU) น้อยกว่าขนาดของข้อมูล

การสื่อสารดังกล่าว เป็นความสัมพันธ์แบบ ไคลเอนต์เซิร์ฟเวอร์ (Client/Server) ซึ่งความสัมพันธ์ระหว่างฝ่ายส่งและฝ่ายรับนั้นอาจจะอยู่ ในรูปแบบของผู้ให้บริการหรือเซิร์ฟเวอร์ (Server) และ ผู้ร้องขอหรือไคลเอนต์ (Client) ในบริบทของการ สื่อสารข้อมูล รียกความสัมพันธ์ชั้นต้นว่า ไคลเอนต์เซิร์ฟเวอร์ โพรเซสที่ทำตัวเป็นโพรเซสลูกข่าย (Client Process) ซึ่งติดตั้ง ใน เครื่องลูกข่าย จะร้องขอบริการจากโพรเซสแม่ข่าย (Server Process) ซึ่งถูกติดตั้งอยู่ ในเครื่องแม่ข่าย เครื่องคอมพิวเตอร์ที่เป็นคู่ ส่วนใหญ่ทั้งสองเครื่องนั้น มีการติดตั้งระบบปฏิบัติการ เพื่อรับและจัดการ โพรเซสล่วนนำเข้า/ส่งออก (Input/Output) อีกทั้ง สนับสนุนการทำงานแบบมัลติโพรแกรม (Multiprogramming) เครื่องลูกข่ายนั้นสามารถรัน โพรเซสที่นำหน้าที่ เป็นเครื่องแม่ข่าย ได้หลายๆ ตัวพร้อมๆ กัน ในขณะที่ เครื่องลูกข่ายสามารถร้องขอบริการ ได้หลากหลายบริการ จากเครื่องแม่ข่ายหลายๆ แหล่ง เช่น กัน

การส่งข้อมูลแบบ โพรเซสถึง โพรเซส (Process-to-Process Delivery) เป็นหน้าที่และความรับผิดชอบของ โพรโทคอล ชั้นทranสปอร์ต (Transport Layer) เครื่องคอมพิวเตอร์ใดๆ อาจจะสั่งรัน โพรเซสมากกว่า 1 โพรเซส หากพิจารณาเชิงลึกแล้วพบ ว่า การเชื่อมต่อทางอินเทอร์เน็ตนั้น เป็นการสื่อสารระหว่าง โพรเซสถึง โพรเซส เช่น ผู้ใช้เปิดเว็บเบราว์เซอร์เพื่อ ใช้งาน www.google.co.th, www.facebook.com และ ces.wu.ac.th กิจกรรมชั้งต้นเป็นการ ใช้งาน โพรเซสสิ่ง 3 โพรเซส โดยแต่ละ โพรเซสเชื่อมต่อเครื่องปลายทางที่แตกต่างกัน ข้อมูลจาก โพรเซสหนึ่งจะไม่ส่งไปยัง โพรเซสอื่น จิตนาการเล่นๆ ว่า หากผู้อ่านได้ โพสข้อความลง ใน www.facebook.com แต่ข้อความตอบกลับแสดง ในเว็บไซต์ ces.wu.ac.th จะเกิดอะไรขึ้น ระบบ คอมพิวเตอร์และเครือข่ายมีกิลไก ได้ที่ป้องกันการเกิดปัญหาดังกล่าว



การกำหนดเลขที่อยู่ (Addressing)

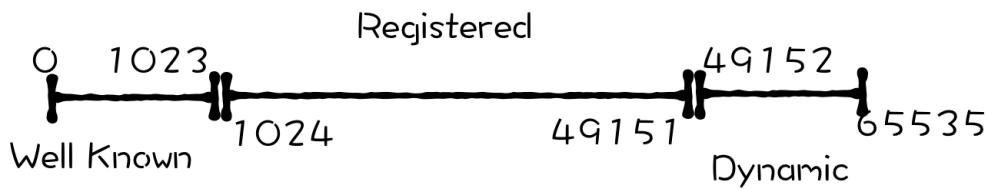
เมื่อเครื่องต้นทางต้องการส่งข้อมูลไปยังเครื่องปลายทาง จำเป็นต้องระบุเลขที่อยู่ของเครื่องปลายทางนั้นๆ อีกทั้งต้องระบุที่อยู่ของแหล่งที่มา เช่น กัน

การกำหนดเลขที่อยู่นั้นแบ่งออกเป็น 3 ระดับขึ้นอยู่กับรูปแบบของการสื่อสาร ได้แก่ อินเตอร์เฟสแอดเดรส (Interface Address), เน็ตเวิร์คแอดเดรส (Network Address) และพอร์ตแอดเดรส (Port Address):

- **อินเตอร์เฟสแอดเดรส (Interface Address)** เป็นหมายเลขของอินเทอร์เฟสการ์ด (Interface Card) การกำหนดซึ่งเรียกเลขที่อยู่นี้ขึ้นอยู่กับโปรโตคอลที่ใช้ในการสื่อสารแบบโหนด สำหรับการสื่อสารของเครือข่ายคอมพิวเตอร์นั้น ใช้โปรโตคอลอีเธอร์เน็ต ดังนั้นจึงส่งข้อมูลผ่านอีเธอร์เน็ตการ์ด (Ethernet Card) หรือการ์ดแลน (LAN Card) ตามที่ผู้อ่านอาจจะคุ้นชุ้น และเรียกเลขที่อยู่ของอินเตอร์เฟสนั้นว่าแมคแอดเดรส (MAC Address)
- **เน็ตเวิร์คแอดเดรส (Network Address)** เป็นการกำหนดเลขที่อยู่ของเครื่องซึ่งใช้ในการระบุเครื่องต้นทางและเครื่องปลายทาง วิธีการกำหนดซึ่งเรียกเป็นแบบเดียวกันกับอินเตอร์เฟสแอดเดรส ซึ่งในชั้นเครือข่ายนั้นเชื่อมต่อถึงกันด้วยโปรโตคอลอินเตอร์เน็ต (Internet Protocol หรือ IP) ดังนั้นมักเรียกเน็ตเวิร์คแอดเดรสว่า หมายเลขไอพี (IP Address) ซึ่ง ในวันนี้มีการใช้งาน IPv4 และกำลังก้าวสู่ IPv6
- **พอร์ตแอดเดรส (Port Address)** เป็นการกำหนดเลขที่อยู่ให้แก่การสื่อสารแบบโปรเซสสิ่ง โปรเซส โดยกำหนดหมายเลขของช่องทางที่ผูกกันระหว่าง เลขจำนวนเต็ม 16 บิตและโปรเซสที่กำลังใช้งานโดยระบบปฏิบัติการ หากระบบปฏิบัติการได้รับข้อมูลที่ถูกส่งมาแล้วจะตรวจสอบว่าพอร์ตแอดเดรส นั้นผูกติดกับโปรเซสใดๆ แล้วข้อมูลที่ได้รับจะถูกส่งต่อไปยังโปรเซสดังกล่าว

การสื่อสารในโปรโตคอลทีซีพี (TCP) นั้น หมายเลขพอร์ตนั้นเป็นตัวเลขจำนวนเต็มขนาด 16 บิต หรืออยู่ระหว่าง 0-65535 ซึ่งเครื่องปลายทางนั้นจะสุ่มหมายเลขพอร์ตขึ้นมา 1 ตัวซึ่งเรียกว่า **พอร์ตอีพิเมอรอล (Ephemeral Port)** เพื่อเปิดช่องทางเชื่อมต่อไปยังพอร์ตของเครื่องปลายทางโดยที่เครื่องปลายทางต้องประกาศให้ทราบโดยทั่วโลกว่าหมายเลขพอร์ตที่ต้องการเชื่อมต่อนั้นคือ หมายเลขใดซึ่งเรียกว่า **เวลไนพอร์ต (Well Known Port)** สำหรับเวลไนพอร์ต นั้นเป็นตัวเลขที่กำหนดขึ้นมาโดยตรงไม่ผ่านการสุ่ม

องค์กรที่ควบคุมหมายเลขพอร์ตนั้นคือ IANA ซึ่งย่อจาก Internet Assigned Number Authority โดยแบ่งเลขที่อยู่ไว้ 3 ช่วง ได้แก่ เวลไน (Well Known), รегистเตอร์ (Register) และ ไนดามิก (Dynamic) ดังภาพประกอบ



IANA Ranges

- **เวลไนพอร์ต (Well Known port)** เป็นหมายเลขพอร์ตที่อยู่ในช่วง 0-1023 ควบคุมการใช้งานโดย IANA ซึ่งหากมีการกำหนดโปรโตคอลใดๆ เพื่อเป็นมาตรฐานแล้วต้องร้องขอหมายเลขพอร์ตที่ว่างจาก IANA และประกาศให้ผู้ใช้หรือผู้พัฒนาระบบทรบฯ โดยทั่วโลกว่า หมายเลขใดๆ ถูกกำหนดขึ้นมาเพื่อโปรโตคอลใดๆ วิธีการดังกล่าวมีช่วยป้องกันการกำหนดหมายเลขซ้ำกัน
- **รегистเตอร์พอร์ต (Registers Port)** เป็นหมายเลขที่อยู่ในช่วง 1024-49151 ซึ่งไม่ได้รับกำหนดโดย IANA โปรโตคอลใหม่ๆ ที่ไม่ใช่มาตรฐานสามารถกำหนดและใช้งานได้เองโดยไม่ต้องขออนุญาต อย่างไรก็ตามต้องอยู่ในช่วงที่กำหนดโดย IANA ไม่ใช่ช่วงที่กำหนดโดยผู้ใช้ เช่น สำหรับโปรโตคอล HTTP หมายเลข 80 ถูกกำหนดให้เป็นชุดที่ 1024-49151
- **ไนดามิกพอร์ต (Dynamic Port)** หรือ **อีพิเมอรอล (Ephemeral Port)** เป็นหมายเลขที่อยู่ในช่วง 49152 ถึง 65,535 ซึ่งเป็นพอร์ตที่ได้จากการสุ่มโดยคุณหนานฝัง โดยทั่วไปแล้วเพื่อป้องกันการซ้ำกัน

ชื่อคเกตแอดเดรส (Socket Address) เป็นเลขที่อยู่แบบพิเศษ ถูกใช้ในการส่งข้อมูลระหว่างโปรแกรมซึ่งประกอบด้วยหมายเลขไอพีและหมายเลขพอร์ต ของคุณหน้าทั้งสองฝ่าย โดยที่เครื่องลูกข่ายและเครื่องแม่ข่ายต้องสร้างเลขที่อยู่ดังกล่าวขึ้นมาตามหลักการกำหนดหมายเลขพอร์ตต่างๆ ที่ได้ก่อตัวมาแล้วก่อนหน้า ดังภาพประกอบ

Socket Address

192.168.36.197

8080

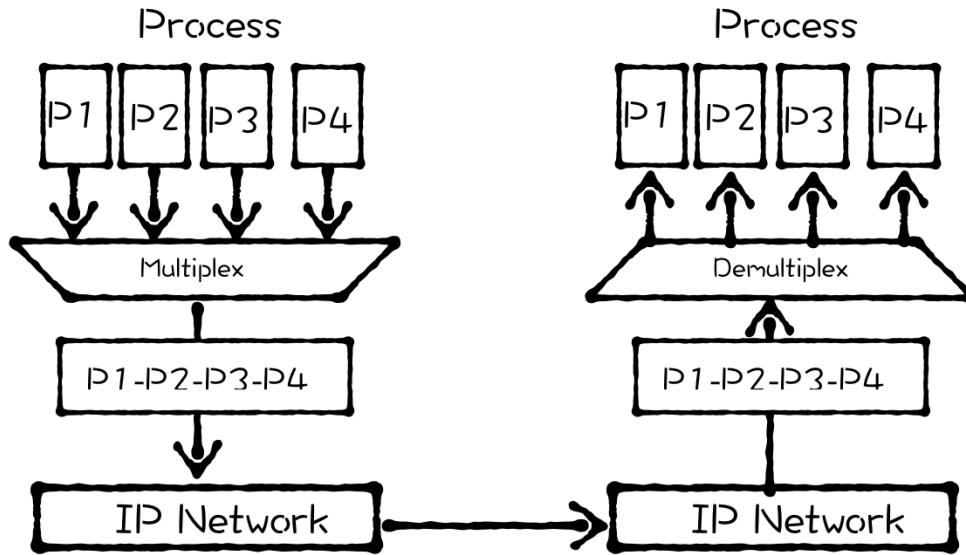
IP Address

Port Address

โดยภาพประกอบเป็นตัวอย่างของชื่อคเกตแอดเดรส ซึ่งกำหนดจากเครื่องคอมพิวเตอร์เพียงฝ่ายเดียว โดยที่หมายเลขไอพีเป็น 192.168.36.197 ได้จดหมายเลขพอร์ต 8080 เพื่อใช้สำหรับการลือสารกับคุณหน้าอีกฝ่ายที่ต้องจดหมายเลขพอร์ตเพื่อสร้างช่องทางสื่อสารซึ่งกันและกัน

มัลติเพล็กซิ่ง (Multiplexing)

มัลติเพล็กซิ่ง (Multiplexing) เป็นคุณสมบัติของการสื่อสารชั้นทرانสปอร์ต ซึ่งเป็นการแชร์ช่องทางสื่อสารเดียวให้โปรเซสสามารถใช้งานได้มากกว่า 1 โปรเซส โดยอาศัยหมายเลขซีดเคตดังภาพประกอบ



จากภาพประกอบข้างบนได้ว่า เครื่องคอมพิวเตอร์ทั้งฝ่ายส่งและฝ่ายรับมีช่องทางสื่อสารชั้นเครือข่ายเพียงช่องทางเดียว หรือมีซีดเคตแอดเดรสเพียงตัวเดียว ต้องการส่งข้อมูลจากหลายโปรเซสผ่านช่องทางดังกล่าว ในชั้นทرانสปอร์ต ทางเครื่องฝ่ายส่งมีโปรเซสมากกว่า 1 ตัว ซึ่งต้องการส่งข้อมูลผ่านโปรโตคอลในชั้นทرانสปอร์ตและเครือข่าย ซึ่งมีเพียง 1 ช่องทาง ในเวลาเดียวกัน กระบวนการส่งข้อมูลดังกล่าวเป็นรูปแบบ Many-to-One ซึ่งหมายถึง โปรเซสหลายตัวต้องการเข้าถึงช่องทางเพียงช่องเดียว ทางออกเดียวที่สามารถดำเนินการได้คือกระบวนการมัลติเพล็กซิ่ง โปรโตคอลจะยอมรับข้อมูลที่มาจากโปรเซสที่แตกต่างกัน โดยแยกความแตกต่างมาจากการหมายเลขพอร์ต ทางฝ่ายรับมีโปรเซสมากกว่า 1 ตัวเช่นกัน ระบบปฏิบัติการรับข้อมูลจากชั้นเครือข่าย และส่งต่อให้ชั้นทرانสปอร์ต หลังจากนั้นตรวจสอบความถูกต้องของข้อมูล ตัดล่วนหัวของแพ็คเกต หลังจากนั้นข้อมูลต่างๆ เหล่านั้นถูกจัดแบ่งด้วยหมายเลขพอร์ตเพื่อกำหนด โปรเซสของทางฝ่ายรับ กระบวนการทำงานที่กล่าวถึ่นี้เรียกว่า **ดิมัลติเพล็กซิ่ง (Demultiplexing)**

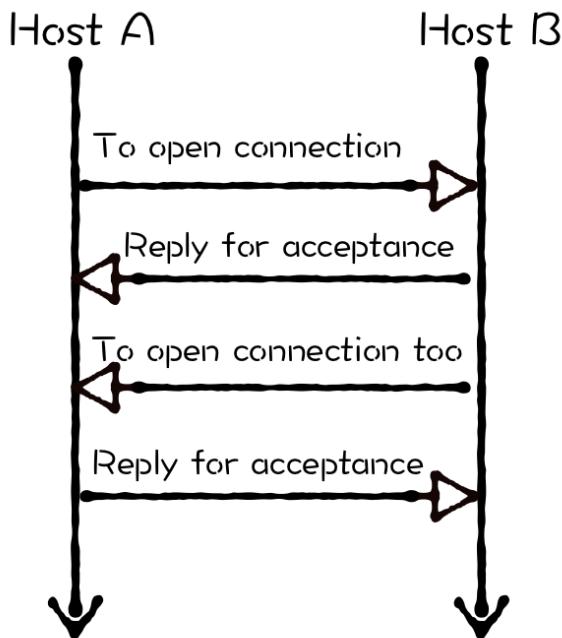
บริการที่ต้องการความน่าเชื่อถือ

บริการจากชั้นทرانส์ฟอร์มเน็ตนับสนุนทั้งบริการที่เน้นความน่าเชื่อถือ (Reliable) และ ไม่นเน้นความน่าเชื่อถือ (Unreliable) ถ้าโปรแกรมใช้ชั้นประยุกต์ต้องการการสื่อสารที่น่าเชื่อถือแล้ว ชั้นทرانส์ฟอร์มจะใช้ฟังก์ชันการควบคุมการไหลของข้อมูล (Flow Control) และฟังก์ชันตรวจสอบความผิดพลาด (Error Control) แต่สิ่งที่เพิ่มเติมเข้ามาคือ ความซับซ้อน (Complexity) และ ความหน่วง (Delay) ที่เพิ่มขึ้น

ในทางกลับกันโปรแกรมใดๆ ไม่นเน้นความถูกต้องของข้อมูลแล้ว ฟังก์ชันต่างๆ ที่กล่าวถึงนั้นจะถูกระงับ การสื่อสารจะเร็วขึ้น ลดความซับซ้อน แต่ไม่มีกระบวนการตรวจสอบความถูกต้องของข้อมูล ดังนั้นจึงเป็นภาระของโพรโทคอลระดับบนในการแก้ไขความผิดพลาด หรือบางความผิดพลาดนั้นอยู่ในระดับที่ยอมรับได้ เช่น การฟังเพลงออนไลน์ หากไฟล์เสียงหายบางส่วนแต่ไม่กระทบ จนฟังเพลงไม่ได้หรืออยู่ในระดับที่ยอมรับไม่ได้แล้ว ถือว่าการสื่อสารข้อมูลข้างต้นไม่ผิดพลาด

อย่างไรก็ตาม ในชั้นเชื่อมโยงข้อมูล (Data Link Layer) นั้นยังมีกระบวนการตรวจสอบความผิดพลาดและควบคุมการให้ของข้อมูลระหว่างโหนด ซึ่งเป็นส่วนช่วยในระดับนึงเท่านั้น หากต้องการการสื่อสารที่มีความน่าเชื่อถือแล้ว จะต้องเปิดพังก์ชัน ในชั้นทรานส์พอร์ตตาม ใช้งานด้วย

เพื่อให้การสื่อสารมีความน่าเชื่อถือนั้น ต้องเริ่มต้นตั้งแต่กระบวนการสร้างช่องทางการเชื่อมต่อ โดยที่ทั้งฝ่ายรับและฝ่ายส่งต้องมั่นใจได้ว่า ต้องมีช่องทางสำหรับรับส่งตลอดเวลา ดังนั้นจึงต้องมีกระบวนการจองช่องทางก่อน เมื่อเชื่อมต่อและส่งข้อมูลเรียบร้อยแล้ว ต้องมีการปิดช่องทางหรือคืนช่องทาง ให้แก่ระบบปฏิบัติการ กระบวนการสื่อสารดังที่กล่าวมานี้เรียกว่าบริการที่มุ่งเน้นการเชื่อมต่อ (Connection Oriented Service)



การสถาปนาการเชื่อมต่อ

จากภาพประกอบเป็นการแสดงกลไกการเพิ่มความน่าเชื่อถือของบริการแบบมุ่งเน้นการเชื่อมต่อนั้น สามารถกระทำด้วยวิธีการต่างๆ ได้แก่

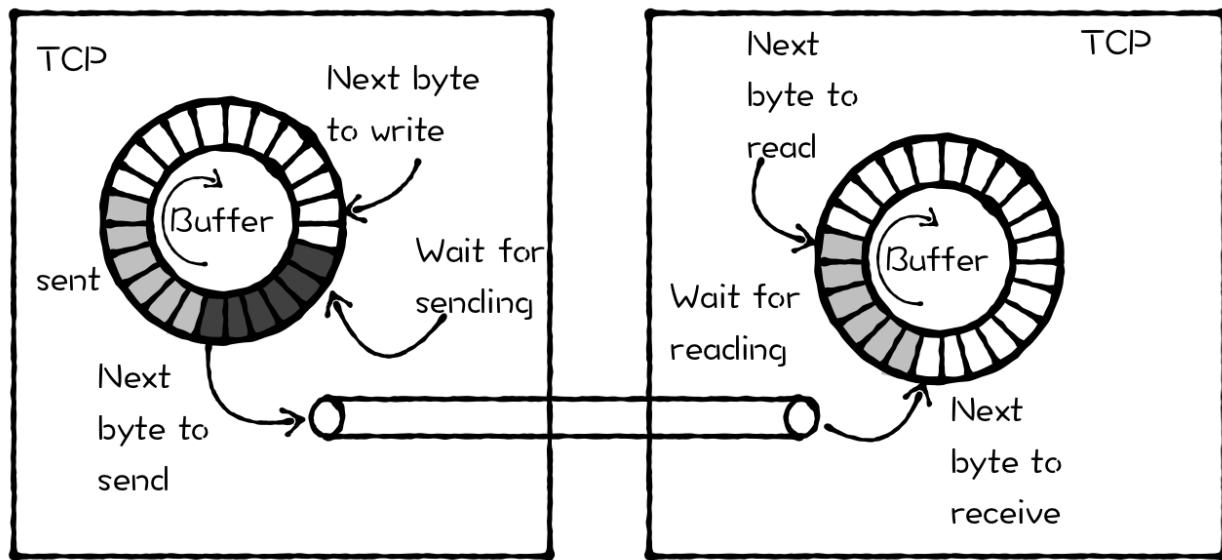
1. เครื่องคอมพิวเตอร์ที่ต้องการ (กำหนดชื่อ A) เริ่มการสนทนารองส่งคำขอเพื่อขอเปิดการเชื่อมต่อ (Establish Connection)
2. เครื่องคอมพิวเตอร์ปลายทาง (กำหนดชื่อ B) ตอบรับการร้องขอด้วยแพ็คเก็ตตอบกลับ (Acknowledge Packet)
3. หลังจากนั้น เครื่องคอมพิวเตอร์ B จะร้องขอเพื่อขอเปิดช่องทางการเชื่อมต่อเช่นกัน
4. เครื่องคอมพิวเตอร์ A ตอบรับการเชื่อมต่อข้างต้น และส่งผลให้การเชื่อมต่อสมมูล (Virtual Connection) ถูกสร้างขึ้น

ในทางกลับกัน ถ้าเป็นการสื่อสารที่ไม่มีการจองเส้นทางล่วงหน้า หากเครื่องลูกข่ายมีความชัดข้องของข้อมูลแล้ว เครื่องลูกข่ายจะร้องขอข้อมูลทันที โดยไม่มีการตรวจสอบล่วงหน้าว่า เครื่องแม่ข่าย หรือช่องทางว่างหรือไม่ หากไม่สามารถเชื่อมต่อได้จะทำซ้ำจนครบ 3 ครั้ง หรือมากกว่านั้น หากยังไม่สามารถเชื่อมต่อได้อีก การเชื่อมต่อจะยุติและแจ้งข้อผิดพลาด บริการของชั้นทรานส์พอร์ตตามที่กล่าวมาข้างต้นเรียกว่า บริการแบบไม่มุ่งเน้นการเชื่อมต่อ (Connectionless Service)

บริการส่งข้อมูลแบบสตรีม

โปรโตคอล TCP สนับสนุนการส่งข้อมูลแบบสตรีม (Stream) ซึ่งเป็นการส่งข้อมูลรูปแบบของไบต์ที่ต่อเนื่องกัน ในขณะที่ทางฝ่ายรับ จะรับข้อมูลเป็นสตรีมเช่นเดียวกัน โปรเซสทั้งสองฝ่ายสร้าง "ท่อ (Tube)" โดยเชื่อมต่อ โปรเซสทั้งสองฝ่ายเข้าด้วยกันผ่านเครือข่ายอินเตอร์เน็ต หลังจากนั้นข้อมูลจะถูกส่งเป็นสตรีมจากต้นทางถึงปลายทาง

เพื่อให้การรับส่งข้อมูลมีประสิทธิภาพข้อมูลไม่สูญหายต่อเนื่องแล้ว ทั้งฝ่ายรับและฝ่ายส่งต้องของหน่วยความจำขึ้นมาล่วงหนึ่งเพื่อกีบข้อมูลไว้ก่อนส่ง และสำรองข้อมูลไว้ทางฝ่ายรับจนกว่าจะได้ข้อมูลจนครบแล้วส่งต่อไปประมวลผล ในโปรโตคอลชั้นบน



ภาพประกอบแสดงหน่วยความจำซึ่งเรียกว่าบัฟเฟอร์แบบวงกลม (Circular Buffer) ถูกจัดไว้ทั้งสองฝ่าย ทางฝ่ายส่งแบ่งความหน่วยความจำเป็น 3 ส่วนได้แก่ ส่วนสีขาว เป็นส่วนที่ว่าง ใช้สำหรับเก็บข้อมูลที่โปรโตคอลชั้นบนส่งมา และรอการส่ง ส่วนสีเทา ใช้สำหรับเก็บข้อมูลที่รอส่ง ส่วนสีดำ ใช้สำหรับเก็บข้อมูลที่ได้ส่งไปแล้วและรอการตอบกลับ

ทางฝ่ายรับได้จดบันทึกของบัฟเฟอร์แบบวงกลมเพื่อใช้สำหรับเก็บข้อมูล 2 ส่วนคือ ส่วนสีเทาเป็นส่วนของหน่วยความจำที่เก็บข้อมูลที่ได้รับและการอ่านเพื่อไปใช้งาน ส่วนพื้นที่สีขาวนั้นเป็นหน่วยความจำที่ว่างรอการรับข้อมูลเข้ามา ซึ่งในกรณีที่หน่วยความจำเต็มไปด้วยพื้นที่สีเทาหมายความว่า หน่วยความจำทางฝ่ายรับเต็ม ไม่สามารถรับข้อมูลเพิ่มเติมได้

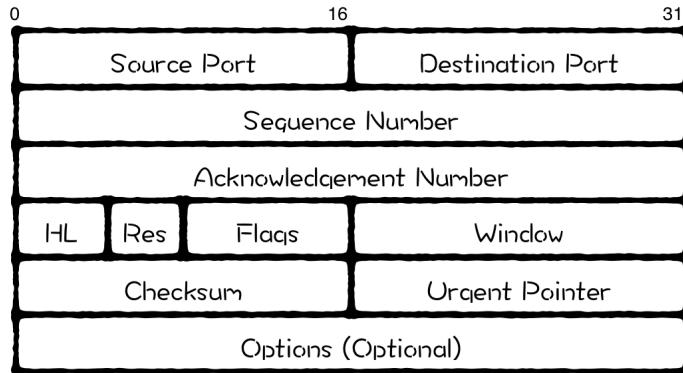
อย่างไรก็ตามจากภาพประกอบนี้ เป็นการสื่อสารข้อมูลทางเดียว (Simplex) เท่านั้น หากต้องการให้การสื่อสารเป็นแบบ 2 ทาง (Full Duplex) แล้ว แต่ละฝ่ายต้องของหน่วยความจำสำหรับการรับและการส่งแยกต่างหาก และสร้างท่อสำหรับการรับและการส่งแยกต่างหาก ซึ่งกระบวนการสร้างท่อทั้งสองนั้น เกิดขึ้นอย่างสมบูรณ์ในขั้นตอนของการสถาปนาการเชื่อมต่อ (Connection Establish)

โปรโตคอลทีซีพี (TCP)

โปรโตคอลควบคุมการขนส่ง (Transport Control Protocol หรือ TCP) เป็นโปรโตคอลแบบมุ่งเน้นการเชื่อมต่อโดยสร้างการเชื่อมต่อเสมือน (Virtual Connection) ระหว่างโพรเซสที่เชื่อมต่อและแลกเปลี่ยนข้อมูลกัน นอกจากนี้โปรโตคอล TCP ได้ใช้กลไกควบคุมการให้ผลของข้อมูลและตรวจสอบความผิดพลาด ในระดับชั้นทرانสปอร์ตเพื่อเพิ่มความน่าเชื่อถือของการขนส่งข้อมูลระหว่างกัน

โปรโตคอล TCP เป็นโปรโตคอลระดับทرانสปอร์ตทำหน้าที่รับข้อมูลจากโพรโตคอลประยุกต์ไปยังชั้นไอพี ข้อมูลที่รวมระหว่างส่วนหัวของญูดีพีและข้อมูล เรียกว่า ทีซีพีเซ็กเมนต์ (TCP Segment) ซึ่งมีรูปแบบการอีนเคนดูเลต ดังภาพ





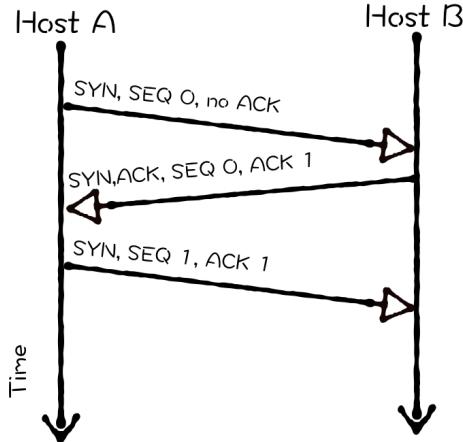
โปรโตคอลที่ซีพีรับข้อมูลจากโปรโตคอลระดับบน หลังจากนั้นแบ่งข้อมูลเหล่านั้นเป็นส่วนย่อย ในชั้นทرانสปอร์ต สำหรับโปรโตคอลที่ซีพี นั้นเรียกหน่วยนับข้อมูลเหล่านั้นว่า เช็กเมนต์ (Segment) ซึ่งส่งต่อให้ชั้นเครือข่ายโดยซ่อน (Encapsulate) เช็กเมนต์ไว้ในไอพีเดต้าแกรม (IP Datagram) และส่งต่อไปยังโปรโตคอลชั้นเชื่อม โดยข้อมูลตามลำดับ องค์ประกอบของที่ซีพีเช็กเมนต์นั้นแสดง ดังภาพโครงสร้างของเช็กเมนต์ของโปรโตคอล TCP จากภาพประกอบแสดงโครงสร้างของเช็กเมนต์ซึ่งประกอบด้วยส่วนต่างๆ และมีคำอธิบายดังนี้

- พอร์ตต้นทาง (Source Port) และ พอร์ตปลายทาง (Destination Port) เป็นข้อมูลขนาด 16 บิต ใช้สำหรับกำหนดชนิดของโปรเซส ในระดับบน ซึ่งเป็นโปรเซสผู้ส่งหรือโปรเซสผู้รับ
- หมายเลขลำดับ (Sequence Number) เป็นข้อมูลขนาด 32 บิตที่กำหนดลำดับที่ของเช็กเมนต์ที่ได้รับ โดยบอกให้ทราบว่า ใบต์แรกของเช็กเมนต์ นี้คือลำดับที่เท่าไรของข้อมูลทั้งหมด อย่างไรก็ตาม ตัวเลขเริ่มต้นของค่านี้เกิดจากการสุ่มขึ้นมาเอง หลังจากนั้นปรับเปลี่ยนหมายเลขตามขนาดของเช็กเมนต์นั้นๆ
- หมายเลขการตอบกลับ (Acknowledge Number) กำหนดหมายเลขใบต์ถัดไปของเช็กเมนต์อีกฝั่งว่าเช็กเมนต์ที่คาดหวังว่าได้รับนั้นคืออะไร เช่น หากได้รับหมายเลขเช็กเมนต์เป็นค่า x หมายเลขตัวต่อไปคือ x+1 โดยปกติแล้ว ข้อความตอบกลับนั้นจะถูกส่งมาพร้อมกับข้อมูลเพื่อลดจำนวนของเช็กเมนต์ ซึ่งเรียกเทคนิคนี้ว่าพิกกี้แบค (Piggyback)
- ความยาวของส่วนหัวเช็กเมนต์ (Header Length) เก็บขนาดของความยาวของส่วนหัวเช็กเมนต์โดยปกติแล้วขนาดของส่วนหัวเช็กเมนต์นั้นอยู่ระหว่าง 20-60 ใบต์ โดยแทนข้อมูลระหว่าง 5-15 ช่องແเนคคาระระหว่าง ($5 \times 5 = 20$) ถึง ($15 \times 4 = 60$)
- ส่วนสงวน (Reserved) จดไว้โดยที่ยังไม่ใช้ในปัจจุบัน
- ส่วนควบคุมที่ซีพี (TCP Control) เป็นข้อมูลขนาด 6 บิต เพื่อใช้สำหรับแสดงสถานะหรือชนิดของเช็กเมนต์นั้นๆ โดยแต่ละบิตมีความหมาย

U	1	Consult urgent pointer, notify server application of urgent data
A	1	Consult acknowledgement field
P	1	Push data
R	1	Reset connection
S	1	Synchronize sequence numbers
F	1	No more data; Finish connection

- ขนาดวินโดว์ (Window Size) กำหนดขนาดของบัฟเฟอร์ที่ใช้ในการรับส่งข้อมูล
- Checksum จะใช้สำหรับการตรวจสอบความถูกต้องของส่วนหัวของเช็กเมนต์โดยวิธี วันคอมพลีเมนต์ ($1^{st}/st$ complement)
- เออเจนต์พอยต์เตอร์ หรือ (Urgent Pointer) ชี้ไปยังตำแหน่งของข้อมูลที่ต้องการประมวลผลอย่างเร่งด่วน ซึ่งจะมีผลเมื่อมีการกำหนดแฟลก URG ในส่วนควบคุมที่ซีพี
- ออฟชัน (Option) เป็นการกำหนดคุณสมบัติต่างๆ เพิ่มเติมของโปรโตคอลที่ซีพี

โปรโตคอลที่ซึ่งเป็นโปรโตคอลที่ต้องมีการสร้างเส้นทางเสมือน (Virtual Path) ก่อนการส่งข้อมูล หลังจากนั้นรับส่งข้อมูล จนกระทั่งการส่งข้อมูลสำเร็จ หลังจากนั้นเข้าสู่กระบวนการตัดการเชื่อมต่อ บางเชิ้กเม้นต์ไม่จำเป็นต้องส่งโดยตรง แต่อาจจะส่งข้อมูลแบบพิกัดแบคกลับไปได้ ดังนั้นขั้นตอนการสร้างเส้นทางเสมือนนั้น ไม่จำเป็นต้องส่งข้อมูลถึง 4 เชิ้กเม้นต์ แต่ส่งเพียง 3 เชิ้กเม้นต์เท่านั้น โดยเรียกกระบวนการทำงานนี้ว่า Three Way Handshake ดังภาพประกอบ



กระบวนการ Three Way Handshake

ขั้นตอนการทำงานในภาพประกอบนั้นอธิบายได้ว่า

1. ทางฝั่งเครื่องลูกข่ายส่งคำร้องขอไปยังเครื่องให้บริการเพื่อเปิดการเชื่อมต่อโดยส่งเชิ้กเม้นต์ SYN ไปยังเครื่องแม่ข่าย ภายในเชิ้กเม้นต์ SYN นั้นประกอบด้วยข้อมูลสำคัญได้แก่ พอร์ตต้นทางและพอร์ตปลายทาง นอกจากนี้ยังต้องกำหนดให้แฟลก SYN ในส่วนควบคุมที่ซึ่งมีค่าเป็น 1 นอกจากนี้ ส่วนของหมายเลขลำดับจะกำหนดขึ้นมาแบบสุ่มเพื่อเริ่มต้นการเชื่อมต่อ

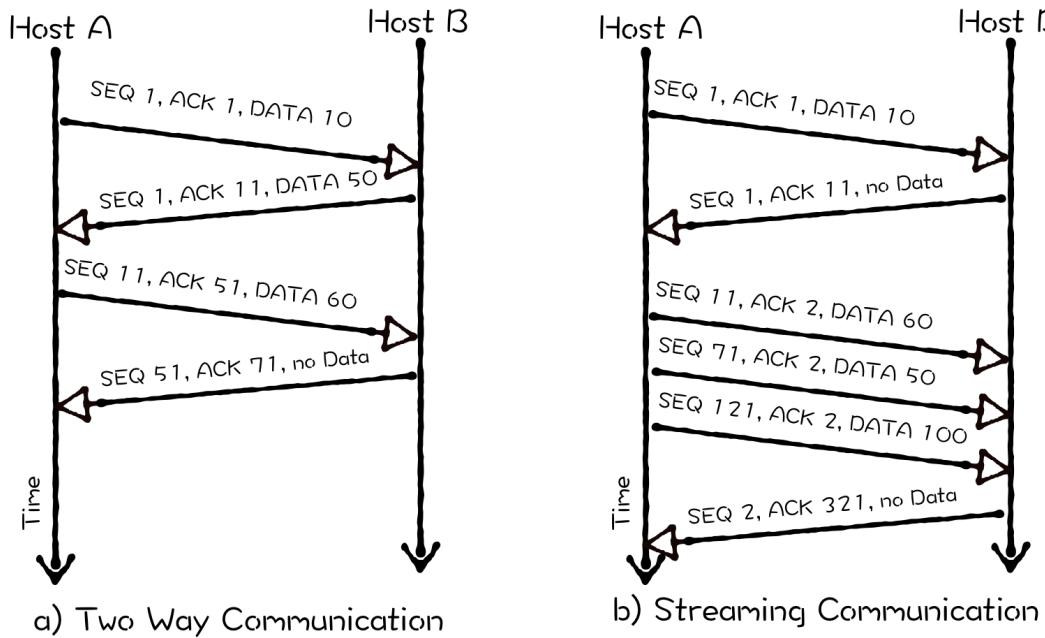
2. เมื่อเครื่องให้บริการได้รับเชิ้กเม้นต์แล้ว จะตอบกลับด้วยเชิ้กเม้นต์ โดยส่วนหัวของเชิ้กเม้นต์นั้นประกอบด้วย หมายเลขการตอบกลับ ตอบกลับการร้องขอเพื่อเปิดการเชื่อมต่อ โดยกำหนดพอร์ตต้นทางและพอร์ตปลายทางให้จำหมายเลขการตอบกลับ หรือหมายเลขเลขลำดับ ที่คาดหวังว่าได้รับ ในรูปต่อไปจากอีกฝั่งนึง นอกจากนี้ได้กำหนดให้แฟลก SYN และ ACK ของส่วนควบคุมที่ซึ่งมีค่าเป็น 1 เพื่อตอบรับการร้องขอ และขอเปิดช่องทางการส่งข้อมูล เช่นกัน

3. เมื่อเครื่องลูกข่ายได้รับแฟลก SYN และ ACK จากเครื่องให้บริการแล้ว ทางฝ่ายเครื่องลูกข่ายจะตอบกลับด้วยเชิ้กเม้นต์ ACK เพื่อยืนยันการเชื่อมต่อ และสร้างเส้นทางเสมือนเช่นกัน

Data Transferring

หลังจากที่การส่งข้อมูลไปแล้ว คอมพิวเตอร์ที่เป็นผู้เชื่อมต่อก่อน อาจจะเป็นผู้ที่เริ่มต้นการถ่ายโอนข้อมูล ซึ่งขึ้นอยู่กับโปรโตคอลนั้นๆ

การถ่ายโอนข้อมูลที่มีความน่าเชื่อถือมีกระบวนการยืนยันผลการทำงาน โดยตอบกลับด้วย Acknowledge Segment ซึ่งเป็นการยืนยันว่า การส่งข้อมูลก่อนหน้าเสร็จสมบูรณ์ และร้องขอข้อมูลชุดถัดไป แต่การตอบกลับด้วย Acknowledge หลายครั้งนั้นเป็นการเพิ่มเชิงเม้นต์เข้าไปในเครือข่ายซึ่งเป็นการสร้างภาระให้แก่เครือข่าย หรือเรียกว่า Overhead ของการสื่อสาร



กระบวนการถ่ายโอนข้อมูล

จากภาพประกอบนี้ได้แสดงกระบวนการถ่ายโอนข้อมูล 2 แบบกล่าวคือ การสื่อสารแบบสองทาง (Two Way Communication) และ การสื่อสารแบบสตรีม (Stream Communication)

โดยที่การสื่อสารแบบสองทางนั้นจะตอบกลับ Acknowledge ทุกครั้งที่ได้รับข้อมูล แต่สำหรับการดาวน์โหลดข้อมูลแบบสตรีมนั้น เป็นการดาวน์โหลดไฟล์ขนาดใหญ่ หากต้องตอบกลับทุกๆ ครั้งนั้นเป็นการเปลืองทรัพยากรเครือข่าย ดังนั้นอาจจะมีการส่ง Acknowledge กลับทุกๆ $2^k - 1$ เชิงเม้นต์

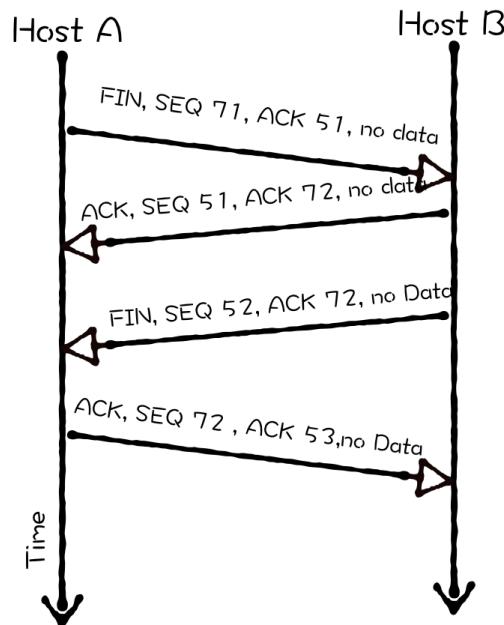
นอกจากนี้ วิธีการปรับเปลี่ยนหมายเลขลำดับเชิงเม้นต์ (Segment Sequence Number) นั้นมีหลักการปรับเปลี่ยนคือ

- หมายเลขของลำดับ (SEQ) นั้นจะสุ่ม ใหม่ทุกครั้งที่มีการเปิดการเชื่อมต่อใหม่
- ทางฝ่ายรับต้องกำหนดหมายเลข Acknowledge โดยมีแนวคิด 2 วิธีการคือ

A. หากเชิงเม้นต์ที่ได้รับเป็นเชิงเม้นต์ควบคุม เช่น SYN Segment เป็นต้น หมายเลข Acknowledge จะเพิ่มขึ้นครั้งละ 1 ซึ่งหมายถึงว่า เชิงเม้นต์ถัดไปควรที่จะเป็นหมายเลขนั้น

B. ในกรณีที่เชิงเม้นต์ที่ได้รับเป็นเชิงเม้นต์ของข้อมูล หมายเลข Acknowledge จะเพิ่มขึ้นเท่ากับความยาวของข้อมูลที่ได้รับ

การสร้างสันทางเชื่อมต่อไว้ตลอดเวลา คือการของทรัพยากรสำหรับการเชื่อมต่อไว้ตลอดเวลา หลังจากที่ใช้ช่องทางเรียบร้อยแล้ว โปรเซสทั้งสองฝ่ายต้องคืนทรัพยากรให้แก่ระบบปฏิบัติการ ดังนั้น จึงต้องตัดการเชื่อมต่อให้สมบูรณ์ โดยขั้นตอนการตัดการเชื่อมต่อนั้น ประกอบด้วย 4 ขั้นตอนดังภาพ



กระบวนการตัดการเชื่อมต่อ

จากภาพอธิบายได้ว่า

1. โปรแกรมผู้ใช้เครือข่ายได้ส่งเช็คเม้นต์ FIN เพื่อขอปิดการเชื่อมต่อ
2. โปรแกรมทางผู้ใช้เครือข่ายได้ส่งเช็คเม้นต์ ACK หลังจากที่ได้รับเช็คเม้นต์ FIN จากเครื่องอื่น โดยที่หมายเลขตอบกลับนั้นคำนวณจากหมายเลขลำดับที่ได้รับมากกว่า 1
3. โปรแกรมทางผู้ใช้เครือข่ายได้ส่งเช็คเม้นต์ FIN เพื่อขอปิดการเชื่อมต่อ เช่นกัน โดยส่งไปยังเครื่องอื่น
4. ท้ายที่สุด เครื่องอื่นได้รับเช็คเม้นต์ FIN จากเครื่องให้บริการแล้ว จะส่งเช็คเม้นต์ ACK เพื่อยืนยันการจบการเชื่อมต่อ หลังจากนั้น ทั้งสองฝ่ายจะคืนทรัพยากรให้แก่ระบบปฏิบัติการ

โปรโตคอลยูสเซอร์เดต้าแกรม

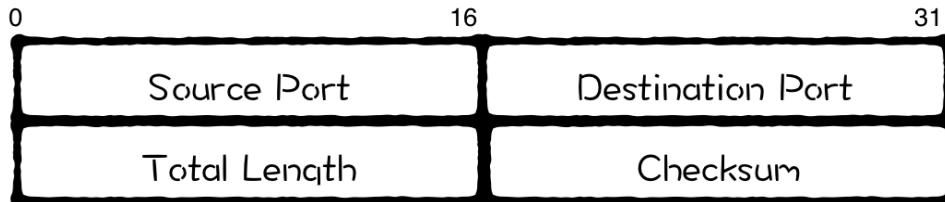
โปรโตคอลยูสเซอร์เดต้าแกรม (User Datagram Protocol หรือ UDP) เป็นโปรโตคอลระดับทرانสปอร์ตทำหน้าที่รับข้อมูลจากโปรโตคอลประยุกต์ไปยังชั้นไอพี ข้อมูลที่รวมระหว่างส่วนหัวของยูดีพีและข้อมูลเรียกว่า ยูดีพีเดต้าแกรม ซึ่งมีรูปแบบการอ้างอิงดังภาพ



การอ้างอิงแบบชั้ลเลตยูดีพี

ยูดีพีเป็นการบริการแบบ Connectionless กล่าวคือไม่สามารถเชื่อมต่อระหว่างสถานีต้นทางและปลายทาง ยูดีพีส่งเดต้าแกรมโดยไม่ตรวจสอบว่า สถานีปลายทางพร้อมที่จะรับข้อมูลหรือไม่ หากการส่งข้อมูลนั้นมีข้อผิดพลาด หรือข้อมูลสูญหาย จะไม่มีกระบวนการใดๆ ที่จะแก้ไขหรือคืนข้อมูลเหล่านั้น โปรโตคอลชั้นประยุกต์ต้องดำเนินการตรวจสอบและแก้ไขความผิดพลาดนั้นเอง

โครงสร้างของยูดีพีเดต้าแกรมประกอบด้วยส่วนหัว 64 บิตดังภาพ



ยูดีพีเดต้าแกรม

- **Source Port** มีขนาด 16 บิตกำหนดถึงหมายเลขพอร์ตต้นทาง
- **Destination Port** มีขนาด 16 บิตกำหนดถึงหมายเลขพอร์ตปลายทาง และกำหนดบริการที่ต้องเข้าถึง
- **Length** มีขนาด 16 บิตกำหนดความยาวของข้อมูล โดยรวมทั้งส่วนหัวและข้อมูลโดยมีหน่วยเป็นไบต์
- **Checksum** มีขนาด 16 บิตกำหนดผลรวมตรวจสอบ คำนวณจากผลรวมของส่วนหัวและข้อมูล

Module 6

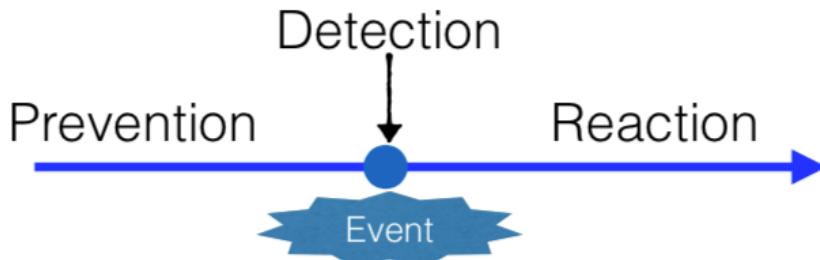
Introduction to Computer Security

Contents

- What is Security
- Threat
- Protection
- Email Security
- Cloud Security
- Software Security
- Secure Web Browsing
- Secure HTTP

What is Security

- **Definition**
 - Security is protection of assets
- **Protection**



- **Computer Security**

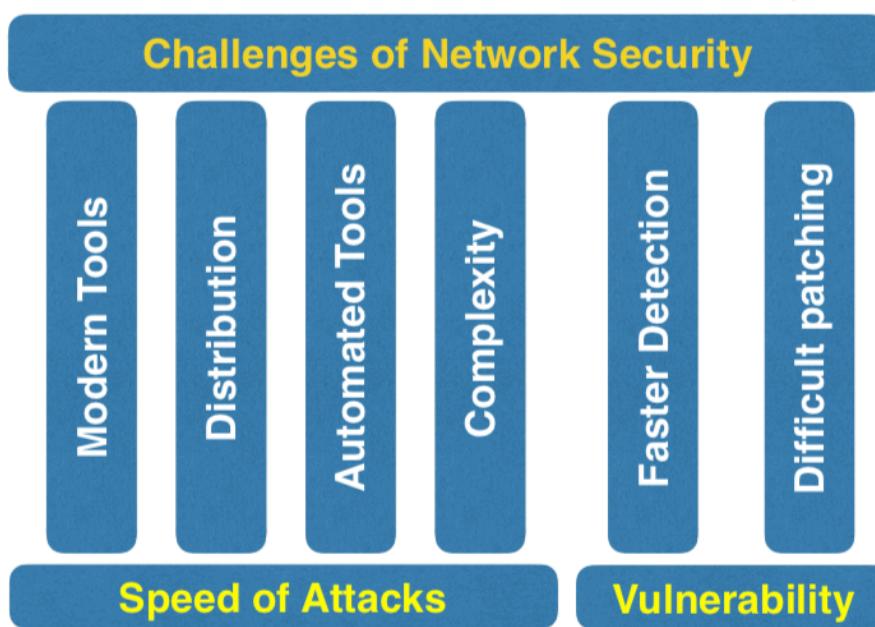
- Computer Security concern with the protection and detection the unauthorised user in computer system
- The objectives is to protect resources and data
 - Almost occurs in time-sharing OS
- **NO GLOBAL SOLUTION**

- **Network Security**

- It is the security of communications exclude computer
 - Network link
 - Store-and-Forward Node
 - such as Router and Switch
 - End point
 - such as files email or hardcopy

- **Network Security is more than computer security**

- The intruder come from any time any where
- Automatic attacking
- The physical security mechanism is not enough
- There are many condition and objectives
 - Application, Service, Protocol, File etc.
- Many administrators



Security Objectives



Threats: Hacker



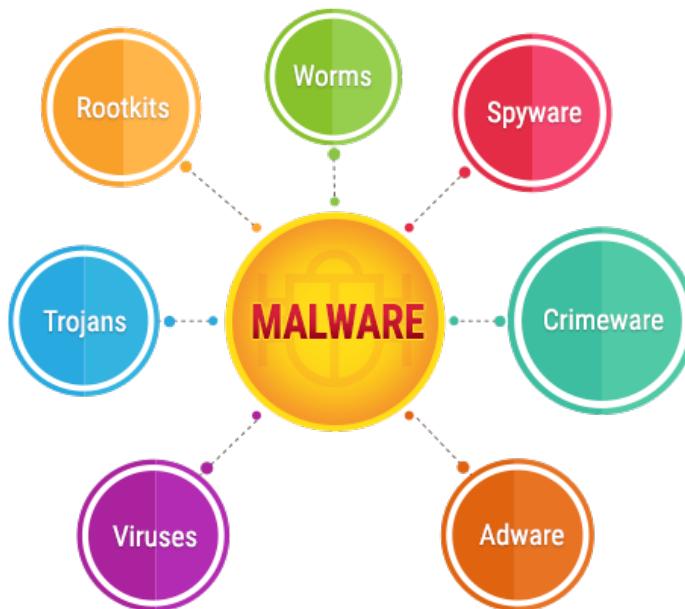
Hackers and *attackers* are related terms for individuals who have the skills to gain access to computer systems through unauthorized or unapproved means. Originally, a hacker was a neutral term for a user who excelled at computer programming and computer system administration. Hacking into a system was a sign of technical skill and creativity that also became associated with illegal or malicious system intrusions. Attacker is a term that always represents a malicious system intruder.

A *white hat* is a hacker who discovers and exposes security flaws in applications and operating systems so that manufacturers can fix them before they become widespread problems. The white hat often does this professionally, working for a security organization or a system manufacturer. This is sometimes called an ethical hack.

A *black hat* is a hacker who discovers and exposes security vulnerabilities for financial gain or for some malicious purpose. Although the black hats might not break directly into systems the way attackers do, widely publicizing security flaws can potentially cause financial or other damage to an organization.

People who consider themselves white hats also discover and publicize security problems, but without the organization's knowledge or permission. They consider themselves to be acting for the common good. In this case, the only distinction between a white hat and a black hat is one of intent. There is some debate over whether this kind of unauthorized revelation of security issues really serves the public good or simply provides an avenue of attack.

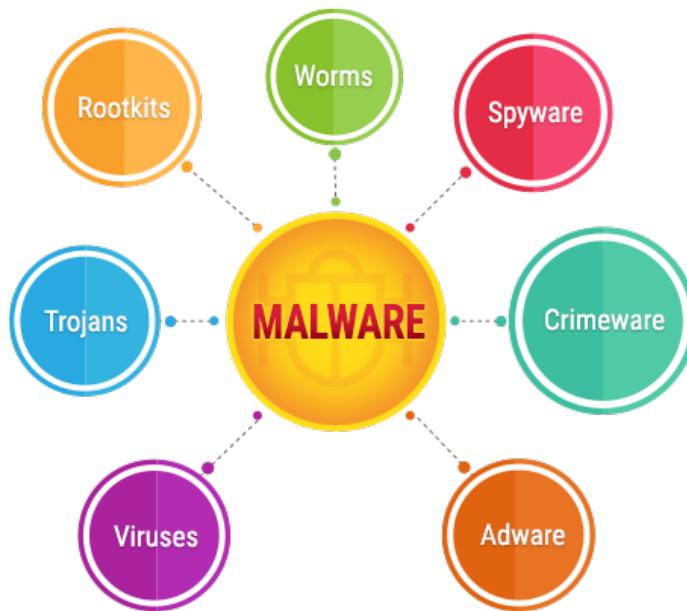
White hats and black hats get their names from characters in old Western movies: The good guys always wore white hats and the bad guys wore black hats.



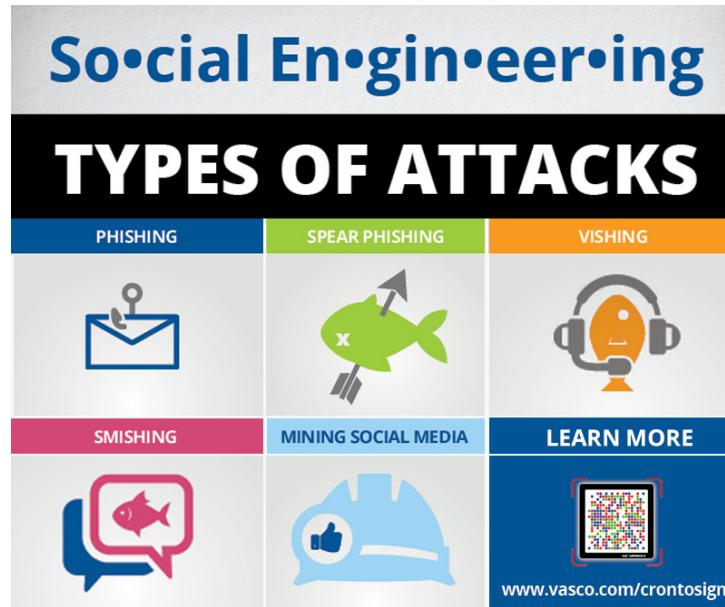
Malware is any unwanted software that has the potential to damage a system, impede performance, or create a nuisance condition. The software might be introduced deliberately or inadvertently and might or might not be able to propagate itself to other systems. Many malicious code attacks fall into the general malware category. Having a good antivirus program installed and running prevents most of these types of attacks from affecting you, your files, and your computer.

- Virus : A piece of code that spreads from one computer to another by attaching itself to other files. The code in a virus executes when the file it is attached to is opened. Frequently, viruses are intended to enable further attacks, send data back to the attacker, or even corrupt or destroy data.
- Worm : A piece of code that spreads from one computer to another on its own, not by attaching itself to another file. Like a virus, a worm can enable further attacks, transmit data, or corrupt or erase files.
- Trojan horse: An insidious type of malware that is itself a software attack and can pave the way for a number of other types of attacks. There is a social engineering component to a Trojan horse attack since the user has to be fooled into executing it.
- Logic bomb : A piece of code that sits dormant on a target computer until it is triggered by a specific event, such as a specific date. Once the code is triggered, the logic bomb detonates, and performs whatever actions it was programmed to do. Often, this includes erasing and corrupting data on the target system.
- Spyware : Surreptitiously installed malicious software that is intended to track and report the usage of a target system, or to collect other data the author wishes to obtain. Data collected can include web browsing history, personal information, banking and other financial information, and user names and passwords.

Threats: Malware

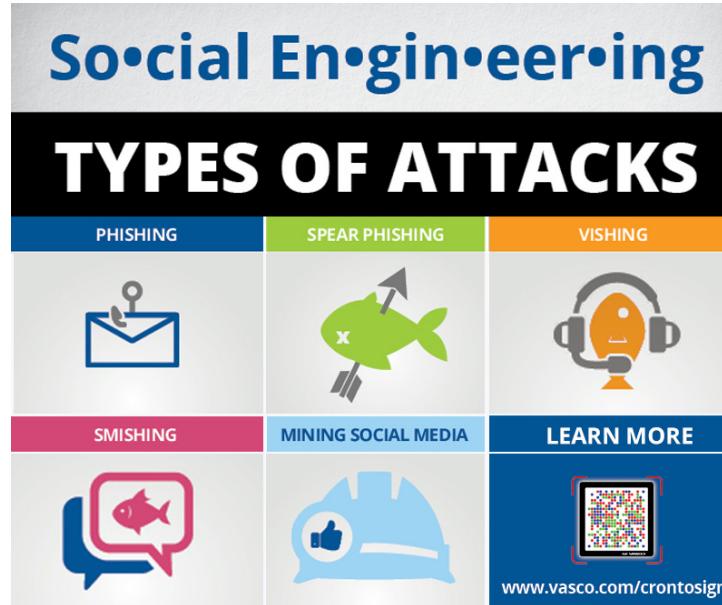


- Adware : Software that automatically displays or downloads advertisements when it is used. Although not all adware is malicious, many adware programs have been associated with spyware and other types of malicious software. Also, it can reduce user productivity by slowing down systems and simply by creating annoyances.
- Rootkit : Code that is intended to take full or partial control of a system at the lowest levels. Rootkits often attempt to hide themselves from monitoring or detection, and modify low-level system files when integrating themselves into a system. Rootkits can be used for non-malicious purposes such as virtualization; however, most rootkit infections install backdoors, spyware, or other malicious code once they have control of the target system.
- Spam : Spam is an email-based threat that presents various advertising materials, promotional content, or get-rich-quick schemes to users. The messages can quickly fill a user's inbox and cause storage issues. Spam can also carry malicious code and other types of malware.
- Ransomware : Ransomware is malicious software that prevents you from using your computer. It usually displays a message stating that you must pay a fee or face some other penalty before you can access your files and computer again. Paying the ransom doesn't necessarily mean that you will regain access to your files or computer.

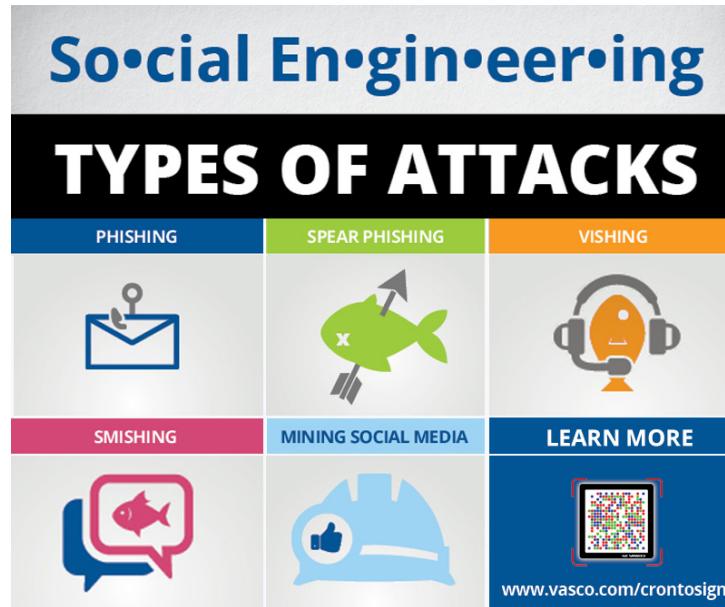


A *social engineering attack* is a type of attack that uses deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines. Social engineering is often a precursor to another type of attack. Because these attacks depend on human factors rather than on technology, their symptoms can be vague and hard to identify. Social engineering attacks can come in a variety of methods: in person, through email, or over the phone. Social engineering typically takes advantage of users who are not technically knowledgeable, but it can also be directed against technical support staff if the attacker pretends to be a user who needs help. Social engineering attacks can be prevented with effective user education.

- Shoulder surfing : This is a human-based attack where the goal is to look over the shoulder of an individual as he or she enters password information or a PIN. Shoulder surfing can happen in an office environment, a retail environment, at an ATM or at the entryway of a secure physical facility. When you are setting up workstations, the monitors should be placed so that they are not facing hallways or windows and giving passersby an opportunity to view information on the screen. This also applies to employees who work from home. Their equipment should not be accessible by other family members or visible to people walking past their homes.
- Spoofing : This is a human-based or software-based attack where the goal is to pretend to be someone else for the purpose of identity concealment. Spoofing can occur in Internet Protocol (IP) addresses, network adapter's hardware (Media Access Control [MAC]) addresses, and email. If employed in email, various email message headers are changed to conceal the originator's identity.



- Impersonation : This is a human-based attack where an attacker pretends to be someone he is not. A common scenario is when the attacker calls an employee and pretends to be calling from the help desk. The attacker tells the employee he is reprogramming the order-entry database, and he needs the employee's user name and password to make sure it gets entered into the new system.
- Hoax : This is an email-based or web-based attack that is intended to trick the user into performing undesired actions, such as deleting important system files in an attempt to remove a virus. It could also be a scam to convince users to give up important information or money for an interesting offer.
- Phishing : This is a common type of email-based social engineering attack. In a phishing attack, the attacker sends an email that seems to come from a respected bank or other financial institution. The email claims that the recipient needs to provide an account number, Social Security number, or other private information to the sender in order to verify an account. Ironically, the phishing attack often claims that the account verification is necessary for security reasons. Individuals should never provide personal financial information to someone who requests it, whether through email or over the phone. Legitimate financial institutions never solicit this information from their clients. A similar form of phishing called *pharming* can be done by redirecting a request for a website, typically an e-commerce site, to a similar-looking, but fake, website.
- Vishing : This is a human-based attack where the goal is to extract personal, financial, or confidential information from the victim by using services such as the telephone system and IP-based voice messaging services (Voice over Internet Protocol [VoIP]) as the communication medium. This is also called *voice phishing*.



- Whaling : This is a form of phishing that targets individuals who are known to possess a good deal of wealth. It is also known as *spear phishing*. Whaling targets individuals that work in Fortune 500 companies or financial institutions whose salaries are expected to be high.
- Spam and spim : Spam is an email-based threat that presents various advertising materials, promotional content, or get-rich-quick schemes to users. The messages can quickly fill a user's inbox and cause storage issues. Spam can also carry malicious code and other types of malware. Spam can also be categorized as a type of social engineering because it can be used within social networking sites such as Facebook and Twitter. Spim is an Internet messaging (IM)-based attack similar to spam that is propagated through IM instead of through email.
- Dumpster diving : Most people and companies are environmentally aware and recycle papers that they are done using. If that piece of paper contains company confidential information, be sure that it is shredded and placed in a secure recycle bin. Attackers are not above jumping into a Dumpster or large recycling location in an attempt to obtain information they can use or sell. Outdated hardware should never be thrown in the trash. The hardware contains heavy metals that could contaminate the soil. Also, hard drives and other storage devices might contain sensitive information. It is not uncommon to find thieves searching for such hardware in the hopes of finding valuable information on the devices. By properly disposing of paper and hardware, you can protect your organization from Dumpster divers.

Threats: Password Attacking

UbIn3\$
Ubiquitous Networked Embedded System

```
[Mon May 21 03:58:46] maldev@maldev: ~/ssh_brute_force (master)
$ ./sshbrute -t 127.0.0.1 -uf username.txt -pf password.txt
```

```
[*] Username: username
[+] Password: toor      -> Incorrect Password
[+] Password: root      -> Incorrect Password
[+] Password: password  -> Incorrect Password
[+] Password: maldev    -> Incorrect Password
[+] Password: correctpwd -> Incorrect Password
```

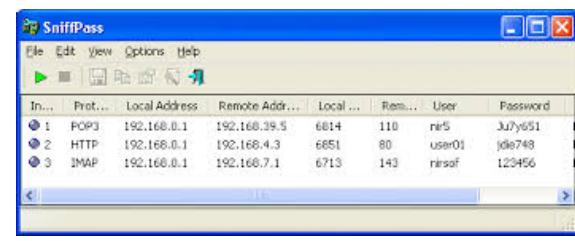
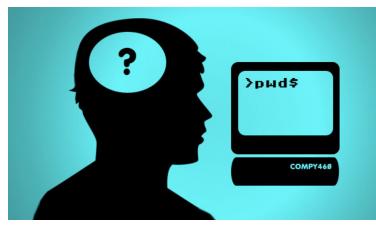
```
[*] Username: print
[+] Password: toor      -> Incorrect Password
[+] Password: root      -> Incorrect Password
[+] Password: password  -> Incorrect Password
[+] Password: maldev    -> Incorrect Password
[+] Password: correctpwd -> Incorrect Password
```

```
[*] Username: maldev
[+] Password: toor      -> Incorrect Password
[+] Password: root      -> Incorrect Password
[+] Password: password  -> Incorrect Password
[+] Password: maldev    -> Correct Password
```

```
[#] Connected.
[#]Username: maldev
[#]Password: maldev
```

Rank	Password	# of Users
1	123456	290,731
2	12345	79,078
3	123456789	76,790
4	password	61,958
5	iiloveyou	51,622
6	princess	35,231
7	rockyou	22,588
8	1234567	21,726
9	12345678	20,553
10	abc123	17,542

Rank	Password	# of Users
11	nicole	17,168
12	daniel	16,409
13	babygirl	16,094
14	monkey	15,294
15	jessica	15,162
16	Lovely	14,950
17	michael	14,898
18	ashley	14,329
19	654321	13,984
20	qwerty	13,856



Internet Technology

<http://cjundang.ubines.info>

167

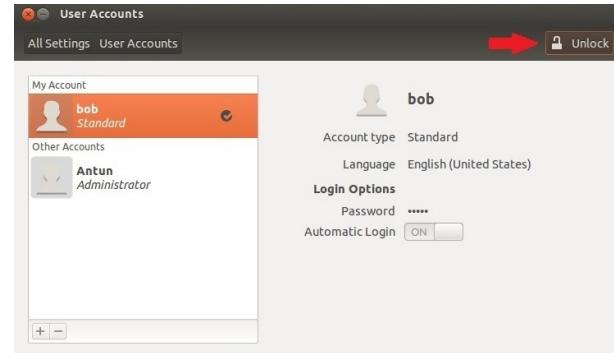
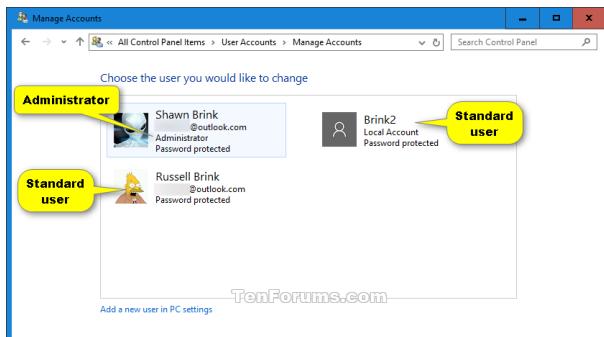
A *password attack* is any type of attack in which the attacker attempts to obtain and make use of passwords illegitimately. The attacker can guess or steal passwords or crack encrypted password files. A password attack can show up in audit logs as repeatedly failed logons and then a successful logon, or it can show as several successful logon attempts at unusual times or locations. Hackers use several common categories of password attacks. Creating complex passwords can increase the amount of time it takes for an attack to succeed.

- Guessing : A *guessing attack* is the simplest type of password attack and involves an individual making repeated attempts to guess a password by entering different common password values, such as the user's name, a spouse's name, or a significant date. Most systems have a feature that will lock out an account after a specified number of incorrect password attempts. Stealing
- Stealing : Passwords can be stolen by various means, including sniffing network communications, reading handwritten password notes, or observing a user in the act of entering the password.
- Dictionary attack : A *dictionary attack* automates password guessing by comparing encrypted passwords against a predetermined list of possible password values. Dictionary attacks are successful against only fairly simple and obvious passwords, because they rely on a dictionary of common words and predictable variations, such as adding a single digit to the end of a word.
- Brute force attack : In a *brute force attack*, the attacker uses password-cracking software to attempt every possible alphanumeric password combination.
- Hybrid password attack : A *hybrid password attack* utilizes multiple attack vectors including dictionary, brute-force, and other attack methodologies when trying to crack a password.



- Fire, whether natural or deliberately set, is a serious network environment security threat because it can destroy hardware and therefore the data contained in it. In addition, it is hazardous to people and systems. You need to ensure that key systems are installed in a fire-resistant facility, and that there are high-quality fire detection and suppression systems on-site so that the damage due to fire is reduced.
- Hurricanes and tornadoes : Catastrophic weather events such as hurricanes and tornadoes are major network security threats due to the magnitude of the damage they can cause to hardware and data. You need to ensure that your information systems are well-contained and that your physical plant is built to appropriate codes and standards so that damage due to severe weather is reduced.
- Flood : A flood is another major network security threat that can cause as much damage as fire can. Your organization should check the history of an area to see if you are in a flood plain before constructing your physical plant, and follow appropriate building codes as well as purchase flood insurance. When possible, construct the building so that the lowest floor is above flood level; this saves the systems when flooding does occur. Spatial planning together with protective planning in concurrence with building regulations and functional regulations are precautionary measures that should be looked into as well.
- Extreme temperatures, especially heat, can cause some sensitive hardware components to melt and degrade, resulting in data loss. You can avoid this threat by implementing controls that keep the temperature in your data center within acceptable ranges.
- Extreme humidity can cause computer components, data storage media, and other devices to rust, deteriorate, and degrade, resulting in data loss. You can avoid this threat by ensuring that there is enough ventilation in your data centers and storage locations, and by using temperature and humidity controls and monitors.

Protect: User Level



Windows includes several built-in user accounts to provide you with initial access to a computer.

- **Administrator** : Complete administrative access to a computer. This is the most powerful account on a computer and should be protected with a strong password. In some situations, you might also consider renaming this account.
- **Standard User** : Access to use most of the computing software on the computer. However, higher permission is required to uninstall or install software and hardware. This account also limits the configuration of security settings, operational settings, and deletion of necessary system files. This account is sometimes referred to as a non-privileged user account.
- **Guest** : Limited computer access to individuals without a user account. By default, the Guest account is disabled when you install the operating system. You enable this account only if you want to permit users to log on as a guest.



Authentication

User authentication is a network security measure in which a computer user or some other network component proves its identity in order to gain access to network resources. There are many possible authentication methods; one of the most common is a combination of a user name and a password.

There are three phases in the user access process that a person or system must perform in order to gain access to resources:

- Identification: The claim of identity made by the user when entering a user name and password.
- Authentication: The verification of that claim.
- Authorisation: The action taken as a result of verifying the claim.

Authentication Factor

Most authentication schemes are based on the use of one or more authentication factors. You can combine these authentication factors for multi-factor authentication. The factors include:

- Something you know, such as a password.
- Something you have, such as a key or an ID card.
- Something you are, including physical characteristics, such as fingerprints.

Multifactor authentication is any authentication scheme that requires validation of two or more authentication factors. It can be any combination of who you are, what you have, what you know, where you are or are not, and what you do. Requiring a physical ID card along with a secret password is an example of multi-factor authentication. A bank ATM card is a common example of this. Keep in mind that multi-factor authentication requires the factors to be different, not just the specific objects or methods.

Protect: Single Sign On



Single sign-on (SSO) is an access control property that you can use to provide users with one-time authentication to multiple resources, servers, or sites. Users log in once with a single user name and password to gain access to a number of different systems, without being asked to log in at each access point. Different systems may use different mechanisms for user authentication, so SSO has to use different credentials to perform authentication. With the widespread use of SSO, it is important to ensure that user authentication is strong for the login; with one potential user name and password providing access to a host of systems, it is critical that this single access point is being properly secured.



You should **always** change any default passwords to strong passwords to protect your computer and data. A strong password is one that cannot be easily guessed by others and is often referred to as a complex password.

To create a strong password:

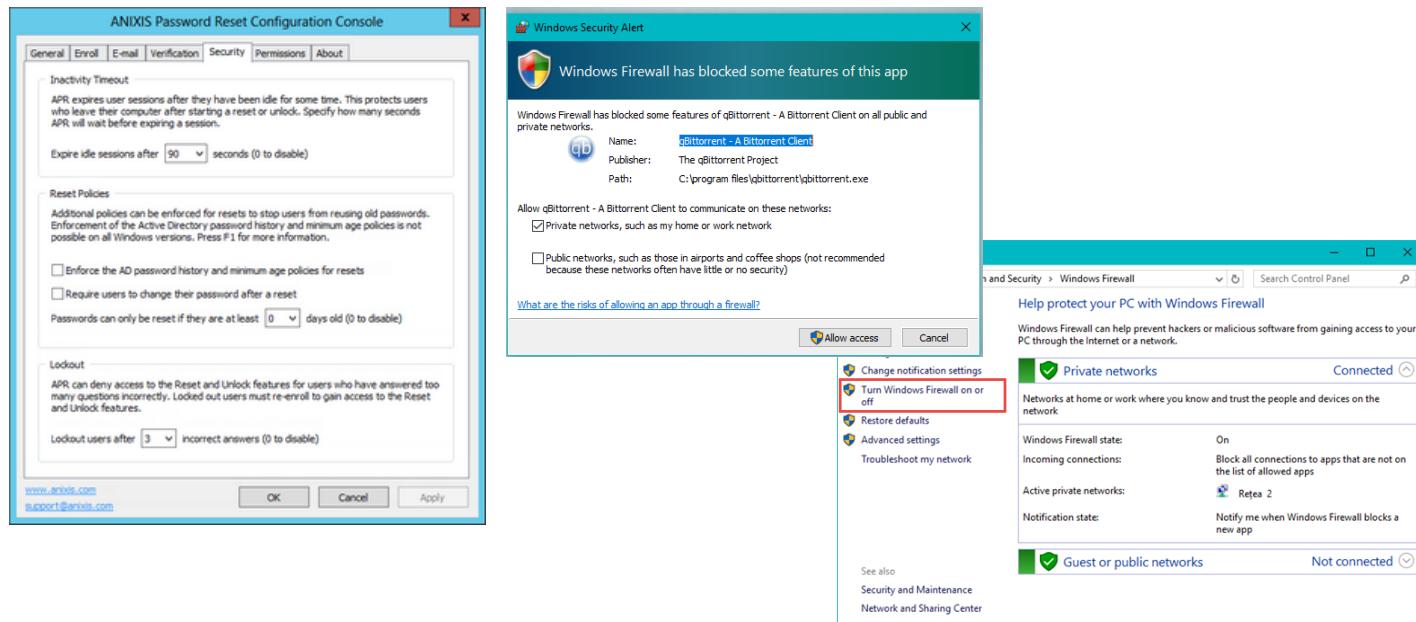
- Use at least seven characters.
- Use a combination of uppercase letters, lowercase letters, numbers, and symbols.
- If you are replacing a previously created password, make sure that your new password is significantly different from the last one.
- Do not use common words, your name, your user name, or other words that people might associate with you, such as a pet's name.

A password is your access to your computer, and it should be protected so that the information on your computer is safe and inaccessible to others.

To protect your password, make sure that you:

- Do not write it down or share it with others.
- Do not use your network password for other purposes.
- If you are a computer administrator, create a new administrator account other than the normal login for security purposes.
- Do not re-use passwords.
- Change your password at least every 60 to 90 days, especially if your account is not configured so that the password expires automatically.
- Always use password protection whenever you're given the option.
- Change your password if you suspect that it has been compromised.
- Do not save your password on the computer.

Protect: Device Hardening



One important risk mitigation technique is device hardening. *Device hardening* is a collection of security tasks used to reduce the scope of the device's vulnerability and attack surface. There are many technologies included with today's devices, some of which you use often, some that you need to use only occasionally, or some that you never use. You might not always be in front of your device and attackers might take advantage of an unattended device to illicitly access information on the device or the network to which it is connected. Disabling features you don't regularly use is one way you can harden your device against attack. Making sure you lock the screen on unattended devices is another prudent method of hardening devices against unwanted intruders.

- **Timeouts and lockout :** User accounts should be configured so that after a specified number of incorrect login attempts, the account is locked. The account can be configured to remain locked until an administrator unlocks it for the user, or it can be configured to remain locked for a specified amount of time. The lockouts and timeouts are a common method used to prevent attackers from breaching a user account by trying to guess the user's password.
- **Software firewall :** Although most desktop and server operating systems ship with a pre-configured software firewall, today's mobile devices still do not have any such protection. *Firewalls* use administrator-defined rules to inspect traffic flowing in and out of a device. They look for and block malicious packets. A firewall can inspect each packet individually (stateless packet filtering) or watch whole conversations between the device and some other node on the network (stateful packet filtering).
- **Antimalware:** As we have mentioned previously, make sure that a good antivirus program is installed on your system. Make sure the virus definitions are kept up-to-date. In addition, you might install ad blocking software. Be sure to use antivirus software on desktop, laptop, tablet, and smartphone devices.

Protect: Device Hardening

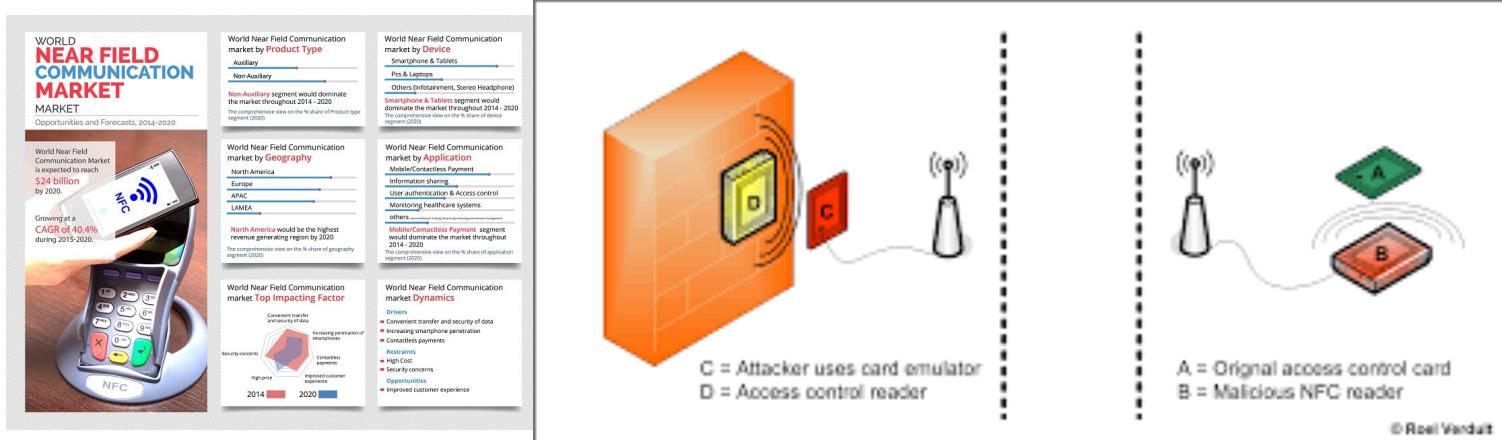
UbIn3\$
Ubiquitous Networked Embedded System



- Disable Bluetooth : Bluetooth technology connects headsets and audio headphones, keyboards, and even printers to computing devices, especially mobile devices. It is rarely secured. For this reason, these devices are also potentially subject to bluejacking and bluesnarfing as their communications and data can be accessed easily. If you don't use Bluetooth devices, or only use them occasionally, you should consider disabling the service so it isn't used to compromise your system.
- *Bluejacking* is a method used by attackers to send out unwanted Bluetooth signals from mobile phones and laptops to other Bluetooth-enabled devices. Because Bluetooth has a 30-foot transmission limit, this is a very close-range attack. With the advanced technology available today, attackers can send out unsolicited messages along with images and video. These types of signals can lead to many different types of threats. They can lead to device malfunctions or even propagate viruses, including Trojan horses. Users should reject anonymous contacts and configure their mobile devices to the non-discoverable mode.
- *Bluesnarfing* is a method in which attackers gain access to unauthorized information on a wireless device by using a Bluetooth connection within the 30-foot Bluetooth transmission limit. Unlike bluejacking, access to wireless devices such as mobile phones and laptops by bluesnarfing can lead to the exploitation of private information including email messages, contact information, calendar entries, images, videos, and any data stored on the device.

Protect: Device Hardening

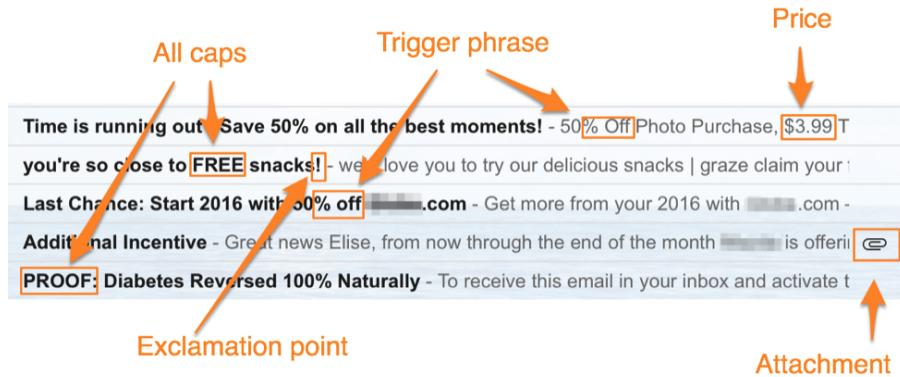
UbIn3\$
Ubiquitous Networked Embedded System



NFC : Near Field Communication

- Disable NFC : *Near Field Communications (NFC)* is used on smartphones and other mobile devices to enable radio communication when the devices touch each other or are a few centimeters apart. Any time you don't need to use this feature, turn it off to prevent intruders from accessing your phone or mobile device.
- Encryption options : *Encryption* is the process of converting data into a form that is not easily recognized or understood by anyone who is not authorized to access the data. Only authorized parties with the necessary decryption information can decode and read the data. Encryption can be one-way, which means the encryption is designed to hide only the cleartext and is never decrypted, or it can be two-way, in which the encryption can be decrypted back to cleartext and read.

Email Security



If there are noticeable changes to an email account, such as an excess amount of spam or you find that there have been emails sent from the account that the email account owner was unaware of, then the computer's security has been jeopardized. Suspicious email issues to be aware of include:

- **Spam** is an email-based threat where the user's inbox is flooded with emails that act as vehicles carrying advertising material for products or promotions for get-rich-quick schemes and can sometimes deliver viruses or malware. Spam can harbor malicious code in addition to filling up your inbox. Spam can also be utilized within social networking sites such as Facebook and Twitter.
- **Hijacked email** is an account that has been accessed by an attacker and is being used by the attacker to send and receive emails. This means that an attacker can read, edit, and send email messages from an account. In a corporate environment, a hijacked email account can result in unauthorized data access.

Avoid selecting links in emails whenever possible. Sometimes an email message looks like it came from a legitimate source with the correct logos, but look for misspellings and bad grammar. This is a good indication that the message is not actually from specified source. Look at the address of the sender as well. If the email address doesn't seem to match the content, then delete the message.

If you don't know the sender, do not open any attachments to the email message. Even if you do know the sender, be careful of opening attachments that you weren't expecting to receive. Someone may have hacked the sender's account and the message could easily contain malware.

If you discover that your email account has been compromised, the first thing to do is change your password and alert the network administrator. You should also perform a complete scan of your system with antivirus software to locate and remove any malware that might have been introduced onto your system.



Cloud storage has become a very popular method for backing up data and for sharing data. Many providers offer cloud storage. Some of the most popular include Microsoft's OneDrive, Google's GoogleDrive, Apple's iCloud, and Dropbox. There are other providers as well. You will need to research to see which one provides the amount of storage and access you are seeking and how much it will cost.

Some things to consider when deciding to use cloud storage include:

- Which data do you feel comfortable storing in the cloud?
- How much encryption will you place on content stored in the cloud?
- Will the cloud be your primary backup location?
- What other backup locations will you need?

As with any other service that has user names and passwords, make sure not to share your credentials.

Security Software Alert

We've got an update for you

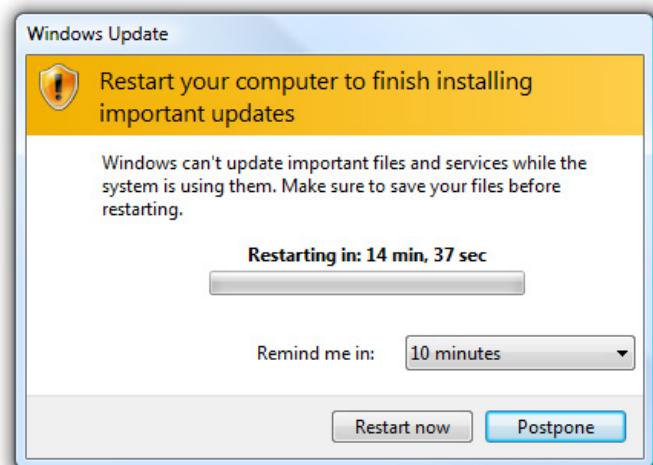
Windows is a service and updates are a normal part of keeping it running smoothly. We need your help installing this one.

Ready? Restart now. Not ready? Pick a time that works for you.

[Restart now](#)

[Pick a time](#)

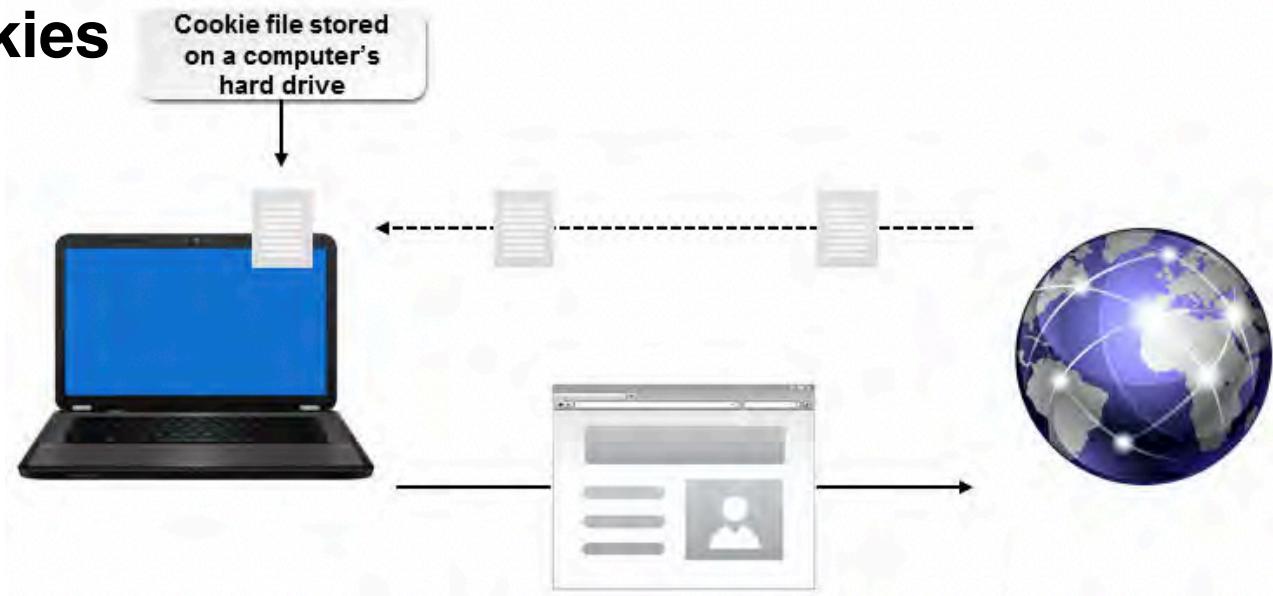
[Snooze](#)



As fast as software companies update and patch vulnerabilities in their software, attackers come up with new ways to breach the software. This includes operating system software as well as application software and mobile apps. You might see alert boxes pop up on your display letting you know that new patches and updates are available for your software. Be sure to apply them in a timely manner. In some organizations, users are not allowed to install the updates themselves. This is usually because the IT department needs to test the patch before deploying it throughout the organization. The patch might cause issues with features that you use in the software or with how the application interacts with other applications on your system.

You might see pop-up messages saying that you need to install updates to your software, but it is for software that you don't actually have installed on your device. This is often the case for alerts from antivirus software that you don't have installed. If you see such an alert for an application that you don't have installed, but sure **not** to select the link for the update. Having conflicting antivirus software applications on your system can prevent either of them from trapping attacks on your system.

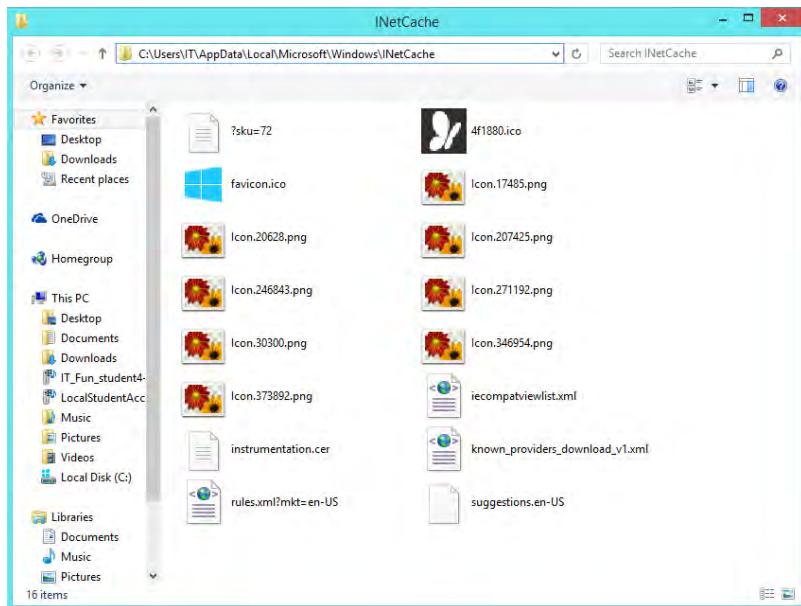
Cookies



A *cookie* is a text file that is created by a website and placed on a computer's hard drive to store information that is used to identify users and, possibly, to prepare customized web pages for them. A cookie can store technical information about the user's actions at a website, such as the links the user clicked. It also stores personal information, but not before the user completes a form or clicks buttons that indicate interests.

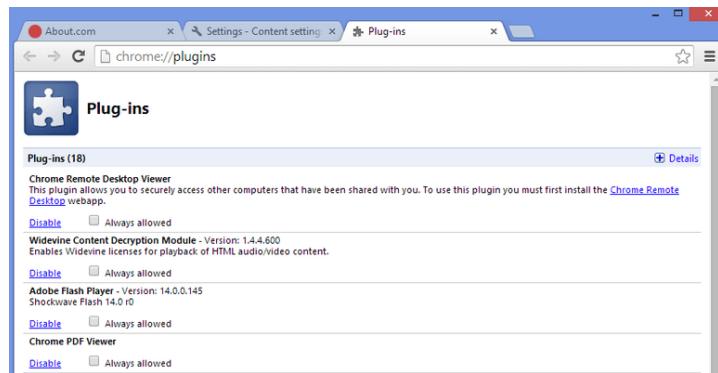
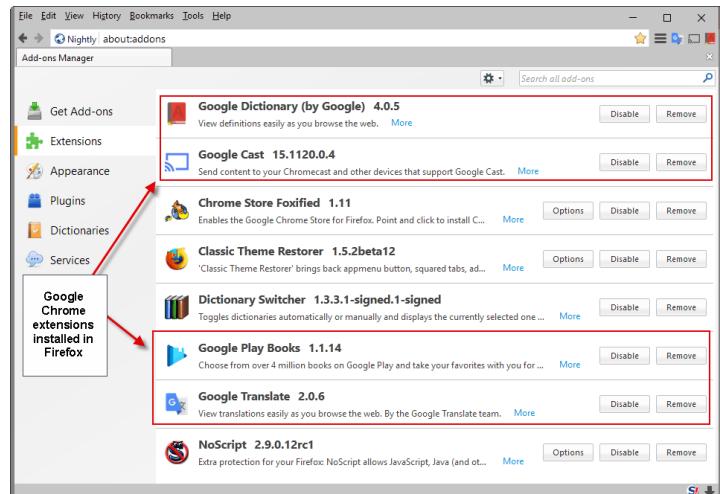
Cookies can be temporary or persistent. Temporary cookies, which are also referred to as session cookies, are stored on a computer only for the duration of the web session. They are deleted once the browsing session ends. Persistent cookies are saved on the hard drive and remain there even after the browsing session ends. Once a website's persistent cookie is stored on a computer, the browser sends the cookie back to the originating website to be reread or updated on any subsequent visit or request from that website.

Internet Cache



An *Internet cache* is a local storage area that holds the files saved by a web browser to decrease the time it takes to reload a web page. The browser cache includes all the text, image, and script files necessary to create and display a given web page when you first access it. When a web page that has been cached is changed, you might not see the most current information unless you clear the cache or manually reload the page. Also, some secure websites, such as those associated with banks, might cache personal information that you supply. If you visit secure websites on a shared computer, clearing the browser cache can help keep your personal information safe. In Internet Explorer, the browser cache is referred to as **Temporary Internet Files**.

Plugin



By default, web browsers can process and display HTML code, but many websites include additional content that the browser isn't initially designed to display. You can install additional software that enables you to view and interact with this additional content.

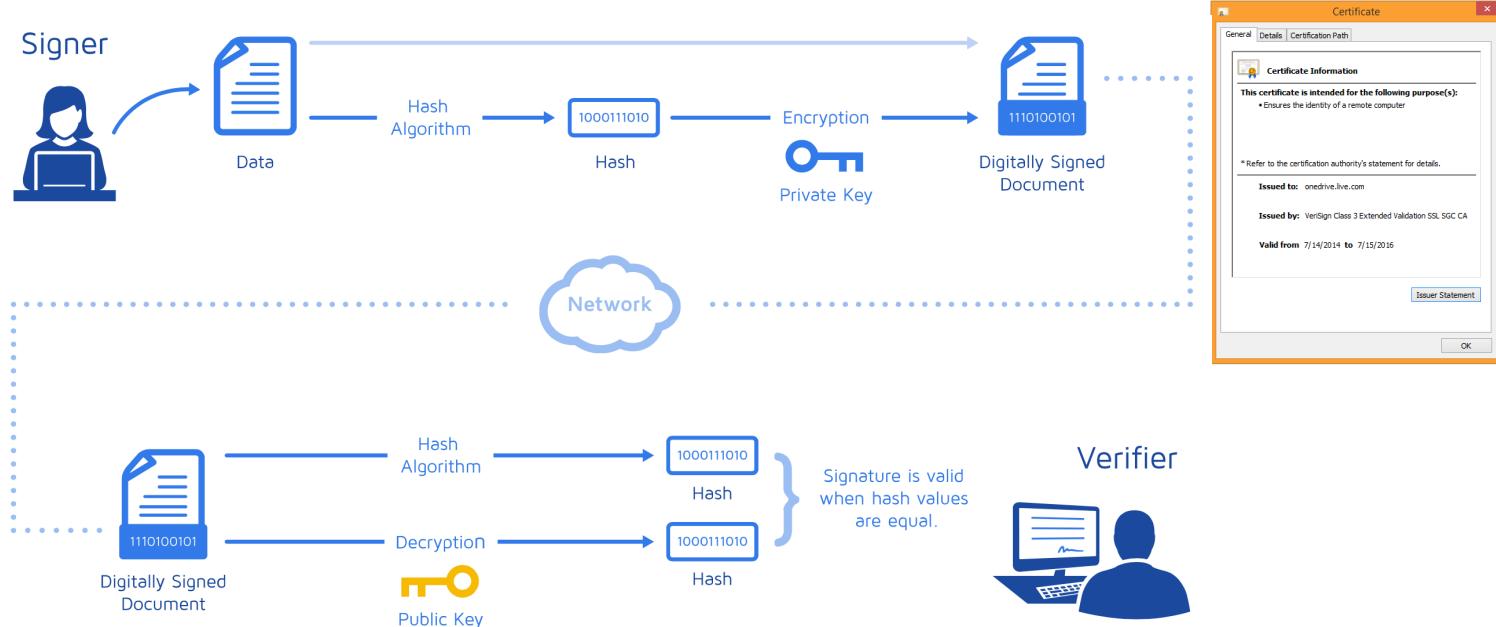
Browser enhancements include:

- **Plug-ins:** A *plug-in* enables the browser to process specific types of content. For example, the Adobe® Flash® player plug-in enables you to view Flash files. Other commonly installed plug-ins include the Java plug-in to allow Java applets on the page to run in a Java virtual machine on your computer and video player plug-ins. If you browse to a site that uses a plug-in that you don't currently have installed, a message will appear at the top of the browser page prompting you to install the plug-in. Typically, you will download an installation file, and then run the executable file to install the plug-in.
- **Extensions:** An extension adds additional features to the browser and becomes part of the browser application. Some of the extensions users install might enhance the browser by adding toolbars, shortcut menu options, or helper objects that are loaded each time the browser is launched.

As with other software, developers often need to update plug-ins and extensions. This might be to address security concerns or to increase or enhance functionality. You should update the plug-ins and extensions whenever you are prompted to do so.

If you find that you are not using a plug-in, or that a plug-in has been installed without your knowledge, you should disable it. If you find that a plug-in is a security risk, you should block it. Some browsers will automatically block any plug-in that is outdated or hasn't been used for some time. Plug-ins can be disabled by using the Settings feature of your browser.

Digital Certificate



digital certificate is an electronic document that provides for the secure exchange of information over a network. A certificate can verify the validity of a website, the identity of a person, or the integrity of a file. Certificates are digitally signed by the issuing authority and can be issued to users, computers, services, or files. In many cases, digital certificates work in the background, but sometimes you have to decide whether or not to accept one when you are downloading programs or files. If you do not accept the certificate, you probably won't get access to the file or service.

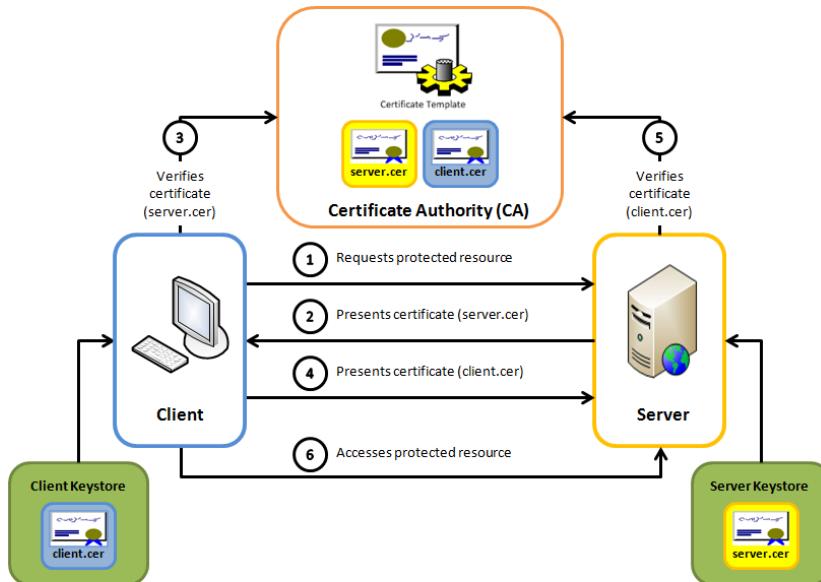
Invalid certificate

When you attempt to access a site, you might receive a warning that the digital certificate is invalid. If this is happening on all of the sites you visit, you should check to see if there is a browser update available or try a different web browser. You should also check that your date and time are correct on your computer. Certificates are issued to be valid for a set period of time. If you access the site before or after the certificate is valid, then you will receive a message that the certificate is invalid.

If the certificate has been tampered with, then you will also receive an invalid certificate warning message. If the site content has been tampered with, it can also invalidate the certificate.

Unless you are very sure that the site is safe, do not access a site that displays an invalid certificate warning. In fact, most browsers will not allow you to access a site if the warning is displayed.

Secure HTTP



Mutual SSL authentication / Certificate based mutual authentication

Attackers often use seemingly valid web page components such as links and banner ads to mask their activities. Before you select a link to access an ad or a website, hover over the link or ad and look closely at the URL of the site to which you will be taken. Attackers often copy the content of legitimate sites onto their own server, but modify the content so that your information is directed to their server instead of the server of the site you thought you were accessing.

One of the first things to look at is whether they are using HTTP or HTTPS. Banks, PayPal, and other secure sites will always use a secure HTTPS URL. Attackers usually just use HTTP addresses. Look for additional information in the URL that shouldn't be there. In most cases, the address should be **https://www.sitename.com**. Attackers usually alter that address to include additional words or letters so that they could register the domain name, but still keep the *site.com* portion of the address. For example **https://www.paypal.com** would be the actual PayPal address, but **http://www.mypaypal.com** would not actually take you to the official PayPal website.

Look for the secure lock icon in the address bar or in the status bar, depending on which browser you are using. If you are going to a secure HTTPS site, the lock icon should be closed, indicating that you are actually on a secured HTTPS site.

