

Part Lecture

Computer Network

By Art s1ckboy

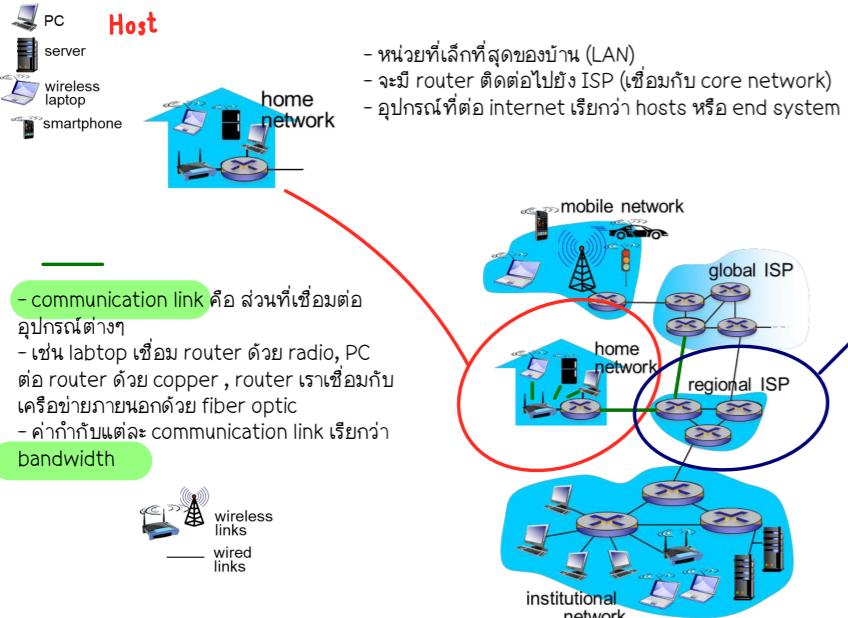
Midterm

523353 Computer Networks

Lecture 1: Introduction to Networking

The Internet

- computer network เป็นโครงสร้างของ internet
- internet มีความหลากหลาย ประกอบด้วยต้นทางไปจนถึงปลายทาง



What is the internet

Internet คือ "Network of networks"

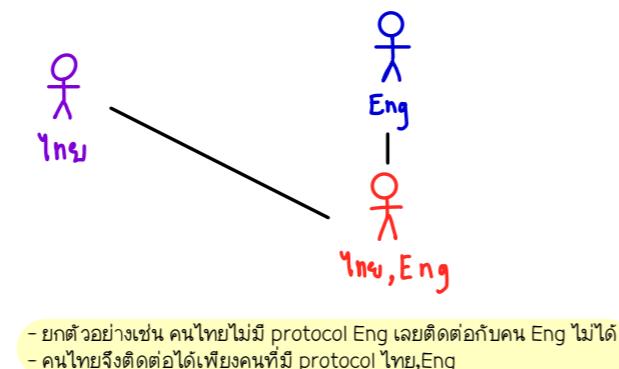
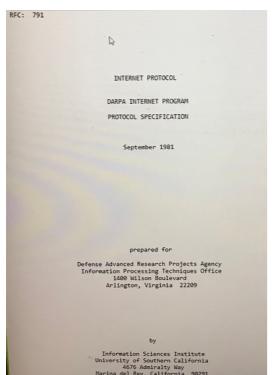
- คือ เครือข่ายของเครือข่ายอย่างหลากหลายอันมาเชื่อมกัน
- จำแนกง่ายๆ เช่น 1 เครือข่ายอยู่ภายใต้ router เดียวเท่านั้น

Protocols

- เครือข่ายสามารถติดต่อกันได้ เพราะมีการกำหนดข้อตกลงร่วมกัน
- เช่น http (GET,POST), TCP, IP, Skype, 802.11
- การทำตามมาตรฐานเหล่านี้เรียกว่า protocols
- มีไว้ควบคุม การส่ง การรับ หรือการใช้งาน service

Internet Standards

- protocol ต้องมีการอธิบายกับมาตรฐานด้วย
- RFC : Request for comments
- IETF : Internet Engineering Task Force



Internet in Thailand

- เริ่มปี 1988 โดย Kevin Robert Elz โดยเป็นการส่ง email จากไทยไปออลเตรลีย์

```

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

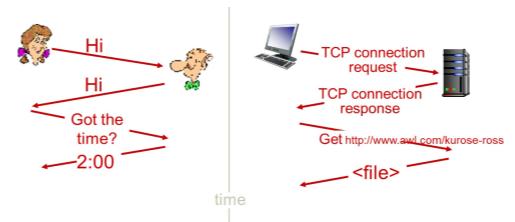
```

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

เพจที่ RFC : 791

What's a protocol

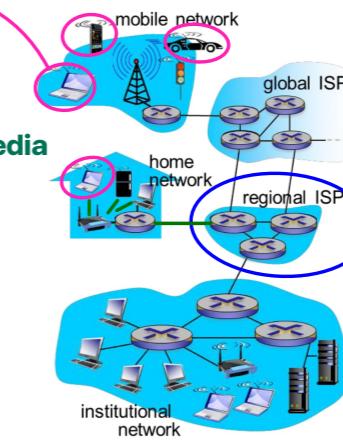
- เป็นข้อกำหนดตกลงที่เข้าใจร่วมกัน
- ใช้ติดต่อระหว่างอุปกรณ์ต้นทางกับปลายทาง



Network structure

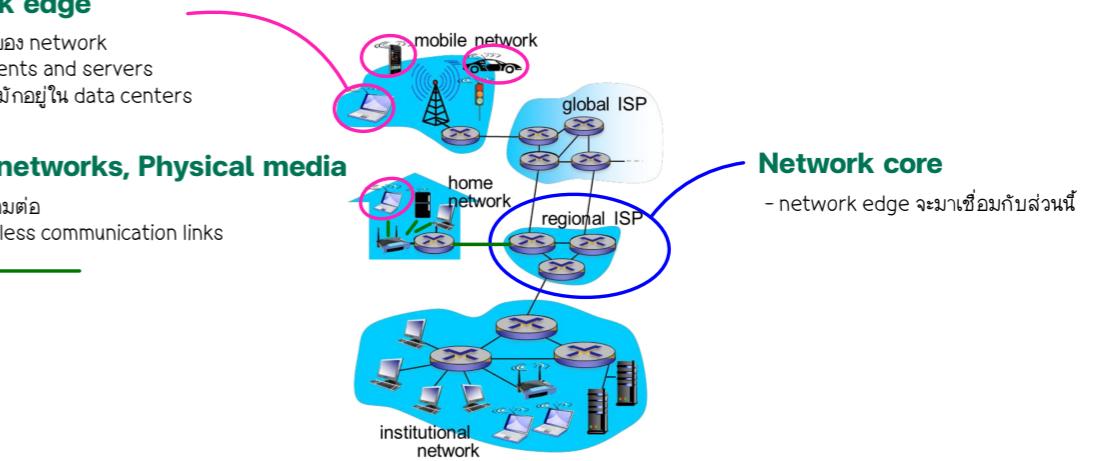
Network edge

- ส่วนปลายของ network
- hosts : clients and servers
- servers : มักอยู่ใน data centers



Access networks, Physical media

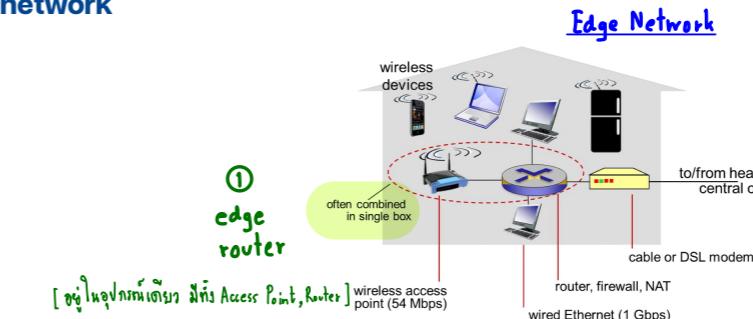
- ส่วนที่ใช้เชื่อมต่อ
- wired, wireless communication links



Access networks and physical media

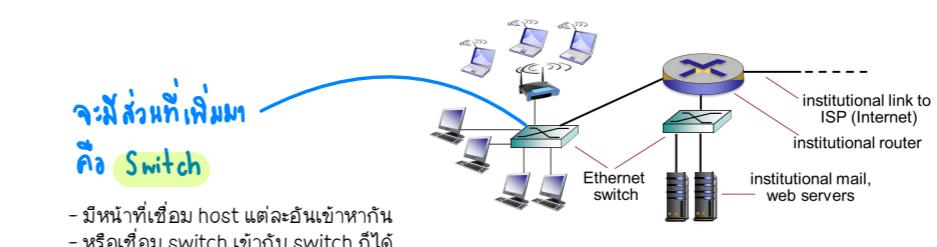
- เราจะเชื่อม end system (host) กับ edge router (router แรก) ได้อย่างไร

Home network



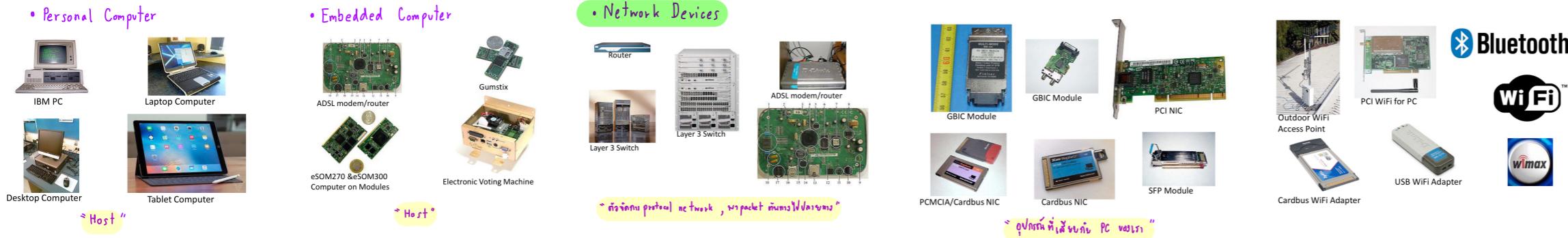
③ ผ่านตัวแปลง กับเป็น modem
เพื่อแปลงสัญญาณให้เท่ากับกันของสู่ภาษาของ

Enterprise



- มีการวัดความเร็วเรียกว่า transmission rate
- เช่น 10 Mbps, 100 Mbps, 1 Gbps เป็นต้น

Network and Internet connection



Physical media

Bit

- หน่วยที่เล็กที่สุดในการรับส่งข้อมูล ต้นทาง-ปลายทาง

Physical Link

- สาย หรือ wireless ที่ใช้รับส่งข้อมูล ต้นทาง-ปลายทาง

Guided Media

- ส่งสัญญาณผ่านของแข็ง เช่น copper, fiber, coax

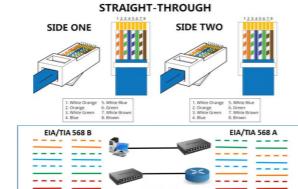
Unguided Media

- ส่งสัญญาณแบบ wireless เช่น radio

Ethernet Cable (RJ45) 纜网线

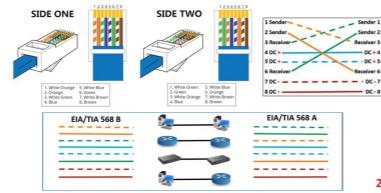
Straight Cable

- สายตรง
- ใช้แลี่ยบระหว่าง 2 อุปกรณ์ที่ต่างชนิดกัน
- ทั้ง 2 ด้านจะมีสีเดียวกัน



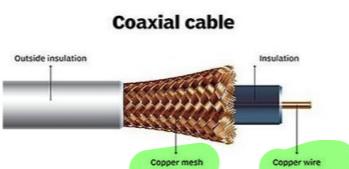
Crossover Cable

- สาย cross
- ใช้แลี่ยบระหว่าง 2 อุปกรณ์ที่ชนิดเดียวกัน
- ทั้ง 2 ด้านจะสีไม่เหมือนกัน



Coaxial Cable

- มี 2 copper คือ copper ที่เป็น shield ข้างนอก และ copper ที่เป็นแกนกลางข้างใน
- ใช้ในการทำ cable ที่เป็น multiple channels และ การทำ hybrid fiber-coaxial



Fiber Optic Cable

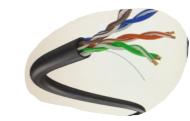
- ยิงสัญญาณเป็น pulse ของ bit
- มีข้อดีคือความเร็วและ error rate ต่ำ



• shielded



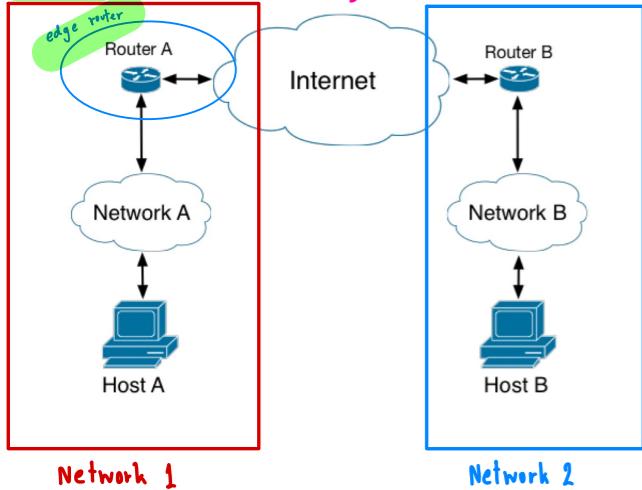
• Unshielded



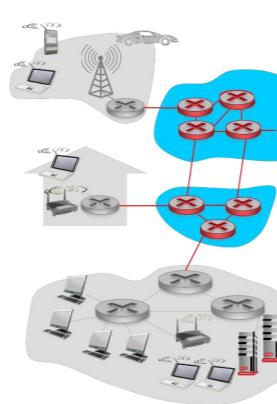
Network and Internet connection

Edge Network (LAN)

Edge = ตัวกรอง



The network core



- router หลายตัวที่ร่วมกันอยู่
- ทำหน้าที่เป็น packet-switching หรือ นำพา packet ไปตามเส้นทางที่เหมาะสม
- โดยจะส่ง packet ให้เดิมเท่าที่ link จะบรรจุได้
- ยกเว้นมีการ shape bandwidth หรือมีการควบคุม
- เช่น ทั้งหมดมีความเร็วเน็ต 100 Gbps ซึ่งคนที่ทำหน้าที่ดูแลเน็ตเวิร์กจะมีการแบ่งต่างๆ เช่น แบ่ง 20 Gbps ให้กับสตรีม แบ่ง 20 Gbps สำหรับเกมต่างๆ ส่วนที่เหลือไว้ให้หน่วยการรักษา

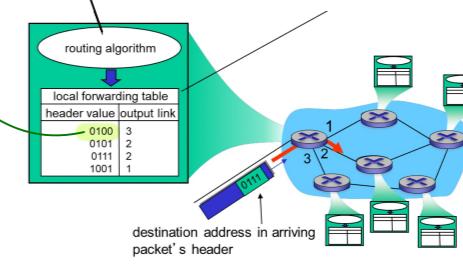
Router จะต้องรู้ได้อย่างไรว่า packet ไหนควรไปเส้นทางไหน...
สามารถรู้ได้จาก forwarding table

โดยการทำงานของ network-core จะแบ่งเป็น

Routing : การหาเส้นทาง (ต้นทางไปถึงปลายทางต้องผ่านเส้นไหนบ้าง)
เบริร์บเนื้อที่ของวงจร

Forwarding : การส่ง packet ไปตามที่กำหนดใน table
เบริร์บเนื้อที่ของวงจร

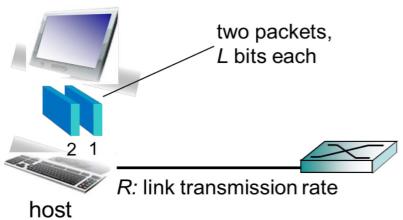
เส้นทางที่มีมากแต่ปลายทางเหล่านั้นจะถูก grouping เป็น subnet และ subnet ทั้งหมดจะถูกบันทึกไว้เป็น 1 record



- table แต่ละ router จะไม่เหมือนกัน แต่ถึงเส้นทางจากแหล่งเดียวกัน

Performance

Host : sends packets of data



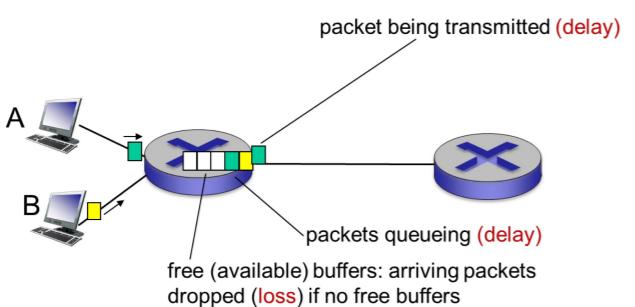
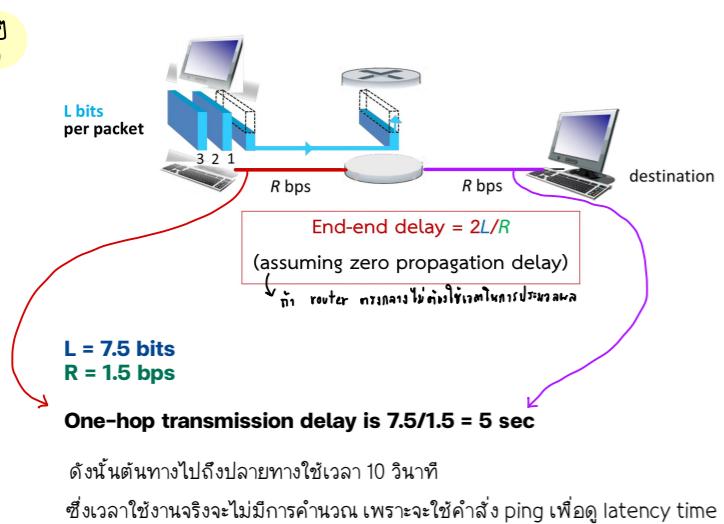
- ในการทำงานของ application อาจมีการส่ง message
- message เหล่านั้นจะถูกแบ่งออกเป็น message ชิ้นแต่ละ message จะมีขนาด L bits (**L**)
- ซึ่งการส่งข้อมูลข้อจะมีเรทที่เรียกว่า transmission rate หรือเรียกว่า bandwidth (**R**)

packet transmission delay

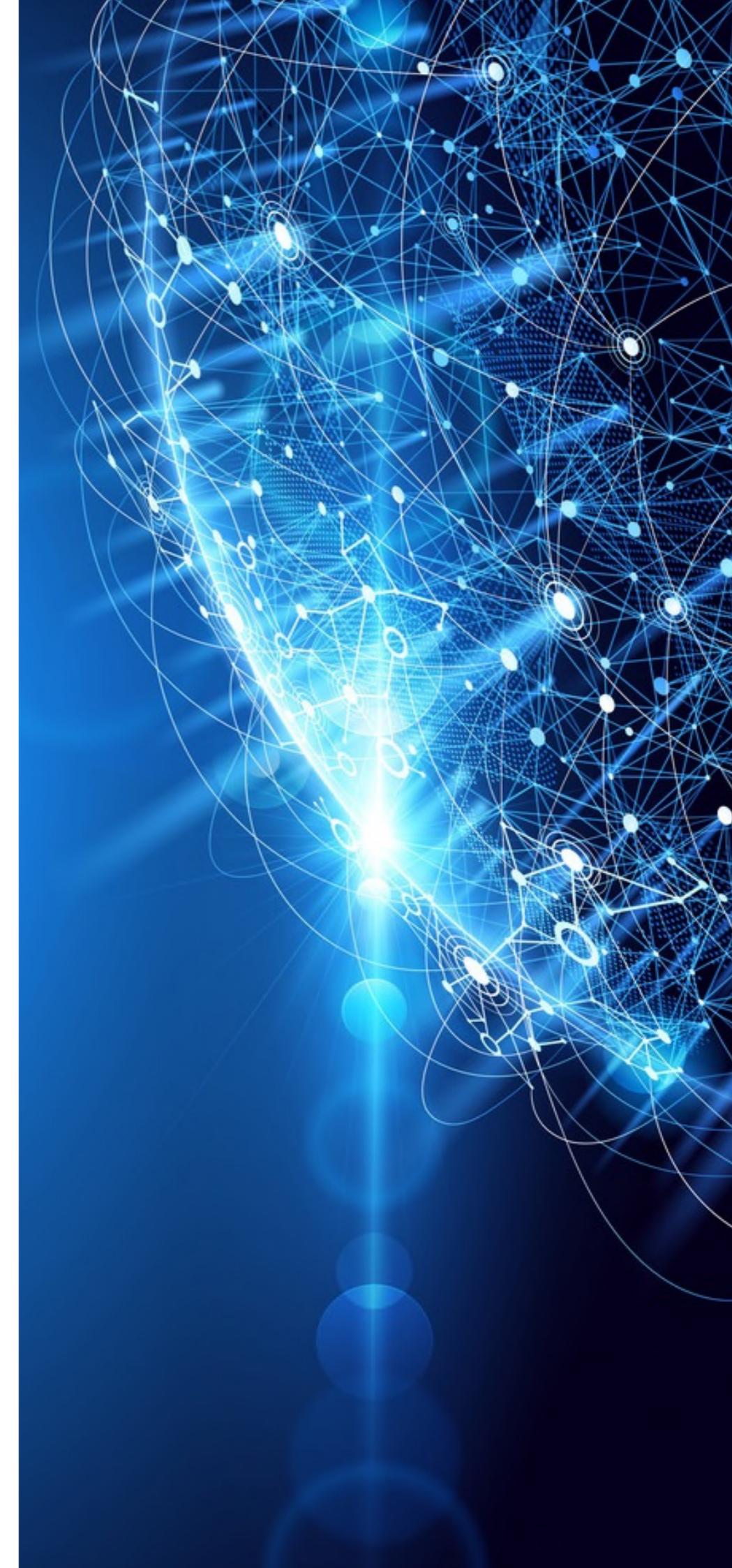
$$\text{packet transmission delay} = \frac{\text{time needed to transmit } L\text{-bit packet into link}}{R \text{ (bits/sec)}} = \frac{L \text{ (bits)}}{R \text{ (bits/sec)}}$$

หมายความว่า

Packet-switching : store-and-forward



- เมื่อมาสั่งเกตด้าแล้ว router บุรียบเลือกจุดเก็บ packet ก่อนที่จะส่งบันโคนอกไป
 - ซึ่งจะเกิด propagation delay (เวลาที่สัญญาณไปใน router) (เพราะ packet มันจะไปรอคิว)
 - ถ้า input rate(packet arrival rate) สูงกว่า output rate มากรา จะยิ่งทำให้คิวยาว (delay เยอะ)
 - หรือบางทีอาจจะเกิดการ lost ได้ เช่น สถานการณ์ที่ router เก็บ packet ได้ 5 slot เมื่อถัดไป packet ตัวที่ 6 เข้ามา มันจะเกิดการ drop the packet ออกมานี้ ซึ่งทำให้ packet นั้น lost ได้
- ↓ เท็มๆแล้ว ก้าวที่เข้ามาก็มีกุกหึ้ง



523353 Computer Networks

Lecture 2: IPv4 Addressing

A Protocol

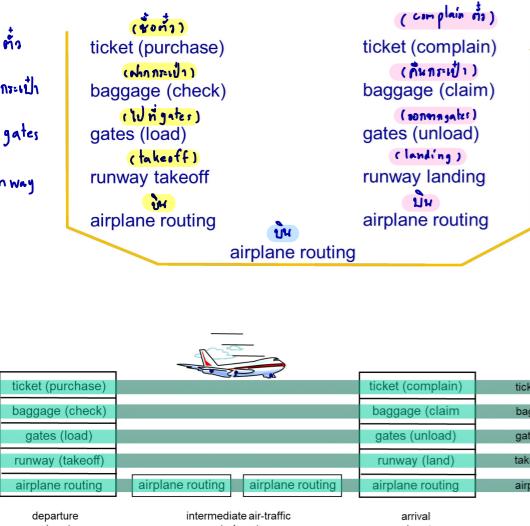
Protocol "layers"

- Networks are complex, with many "pieces"

host
routers
links of various media
applications
protocols
hardware, software

- ที่มองเป็น layers เพราะ layer ตัวบนจะพึ่งพาชั้นล่างๆ ด้วย

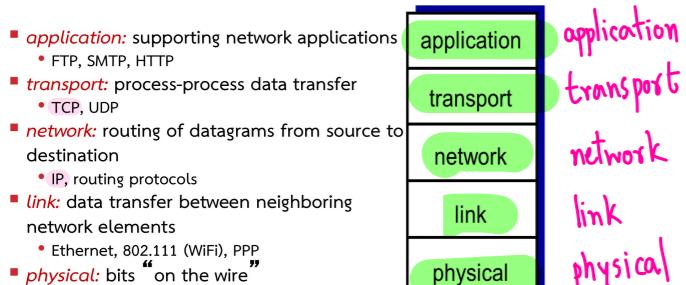
Ex. ยกตัวอย่างการเดินทางด้วยเครื่องบิน



- layers จะทำงานคล้ายฟังก์ชัน
- เป็นการทำงานของแต่ละ layer ไป โดย layer ด้านบนจะพึ่งพา layer ล่างๆ

Internet protocol stack (TCP/IP Model)

- ในโลก internet ของมาตรฐานนี้แบ่งเป็น 5 layers
- บางมาตรฐานอาจแบ่งเป็น 7 layers
- ip คือ internet protocol หรือ protocol ที่ใช้ทำงานใน internet
- พิกัดเลข 127.168.1.1 เรียกว่า IP address
- protocols ที่เราใช้ในโลกอินเทอร์เน็ตทุกรันนี 80% ใช้งาน TCP



Ex. ยกตัวอย่างการใช้งาน Netflix

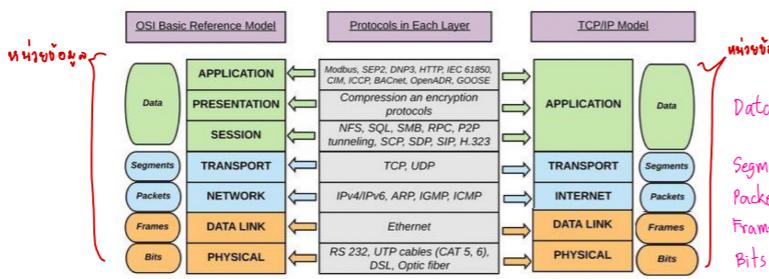
- Application [N]
- Transport [TCP, UDP]
- Network [IP (โปรโตคอล), routing protocol]
[รันนี อิส Forwarding Table]
- Link ทำหน้าที่ใน layer Media
- Physical bits "on the wire"

OSI reference model

- เป็นมาตรฐานที่แบ่งการทำงานเป็น 7 layers
- ทำการแบ่ง session และ presentation ออกมาจาก application layer
- presentation ทำภาระ encryption , การบีบอัดข้อมูล , การเข้าใจ spec ต่างๆ ของเครื่อง
- session ทำงานในส่วนของ การบันทึก checkpoint ของ data หลายถ่าย
- ถ้าจะแบ่งเป็น 5 layers เราสามารถรวม presentation กับ session เข้าด้วยกันได้

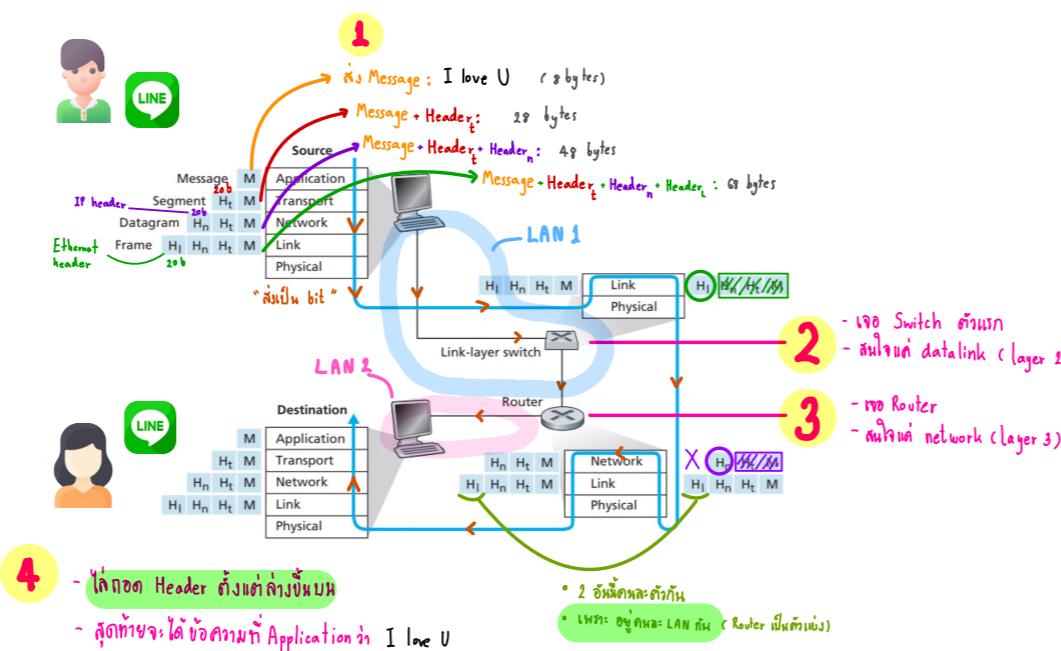


OSI model vs TCP/IP model

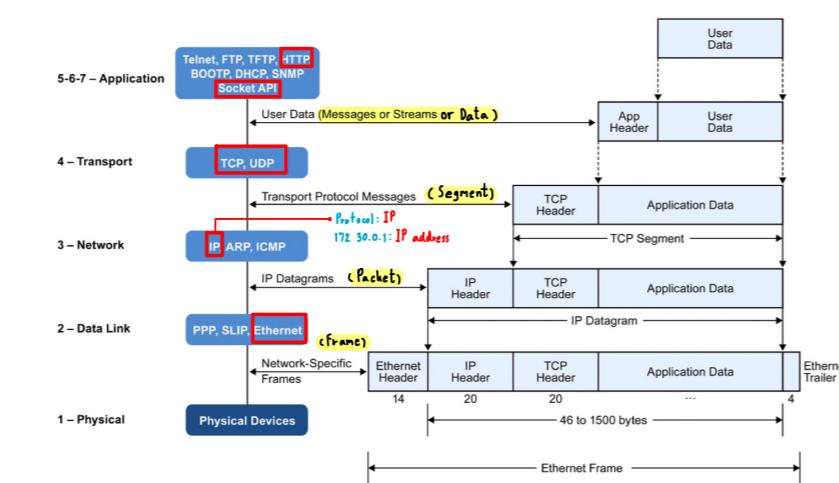


Data Encapsulation

- หน่วยแต่ละ layer ยาวขึ้นเรื่อยๆ เพราะมีการใส่ header (H) เพิ่มเข้ามา



TCP/IP Model

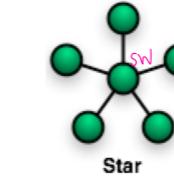


Network Terminology

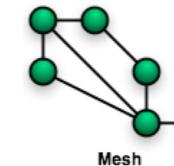
Physical Network Topology

- การต่อใน network เรียกว่า network topology
- เป็นการต่อสายโดยใช้ตัวกลางที่เชื่อมตามรูปแบบต่างๆ เช่น

การเชื่อมกันบันทึกในปัจจุบัน



- แบบดาว (star)
- ปัจจุบันส่วนใหญ่ใช้แบบนี้
- เช่น ใช้ switch ไว้ต่อ gland แล้ว pc ต่างๆ ก็เชื่อมสายเข้ากับ switch



- แบบ mesh
- เช่น wifi mesh, router mesh ในบ้าน
- มีการซึ่งกันยังไงก็ได้ให้มีงานได้
- ไม่มีภัยเดียวของการเชื่อมขาดเจน

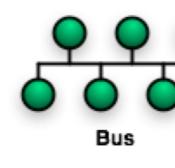


- แบบ fully Connected
- ต้องซึ่งกันหมดทุก node ที่เหลือ
- ผลแบบ p2p ไปในตัว wow!

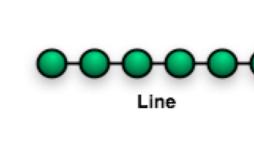
การเชื่อมกันบันทึกในปัจจุบันฝั่งบ้าน



- แบบวงแหวน (ring)
- แต่ละ node มีสองขา จับตั้งสองข้าง
- โดดการล่วงข้อมูลจะล่วงไปทาง
- มีปัญหาดื้อในเวลาใดเวลาหนึ่งต้องมีคนลงคุณเดียวกันคนที่ถือ token



- แบบ bus
- การเชื่อมที่จะมีสายกลากอันนึง
- ทุกๆ node จะมีเวลาที่ถูกกำหนด



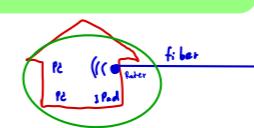
- แบบ line
- แต่ละ node มีสองขา จับตั้งสองข้าง
- ล่วงทาง แต่ไม่ได้จับกันเป็นวง
- แต่เมื่อเป็นจับกันเป็นแคร์ชัน
- หมายเหตุการ search

Public Standards

- IETF [รับรอง Internet , Protocol]
 - IPv4, IPv6, and Internet RFCs
- IEEE [มาตรฐาน, 3G-5G, ตัวไฟเบอร์]
 - IEEE 802.3, IEEE 802.11, etc.
- ISO [มาตรฐานทั่วไป ex Security]
 - ISO 17799, ISO27001, etc.

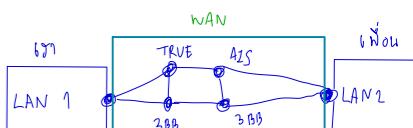
Local Area Network (LAN)

- network วงเล็กๆ เช่น Network ในบ้าน
- อยู่ภายใต้ router เดียวทั้งหมด
- อยู่ภายใต้ภาระค่าใช้จ่ายที่ต่ำกว่า
- มีความเร็วของ data rate เร็วเท่าที่ router สนับสนุน
- คนที่จัดการ Network คือ local admin



Wide Area Network (WAN)

- network วงใหญ่
- เป็นภูมิภาคตั้งแต่บ้าน
- การ connect กันในวงกว้าง



อุปกรณ์ WAN

- Router
 - รับส่งข้อมูลจากทั่วโลก ทั่วโลก ส่งสัญญาณไปยังทุกแห่ง
- Modem , DSU / CSU
 - แปลงสัญญาณจากบ้าน ออกทั่วโลก
 - รับส่งข้อมูลจาก Router

Internet Structure

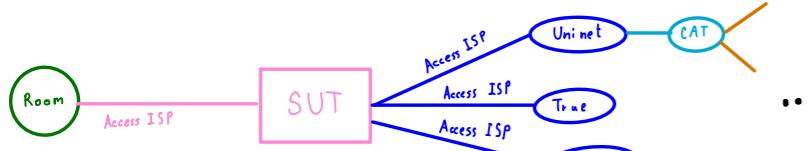
- โครงสร้าง Internet

ยกตัวอย่าง Internet Structure : Network of networks

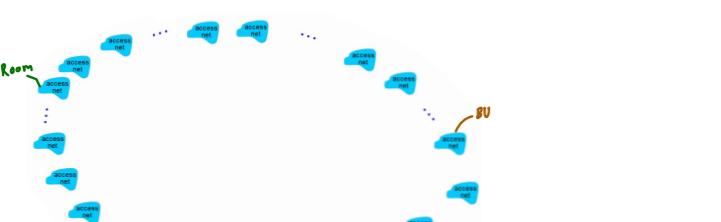
host
- End system เชื่อมอินเทอร์เน็ตผ่าน access ISPs (Internet Service Providers) ห้องพักนักศึกษา เชื่อมกับ ISPs ระดับมหาลัยฯ

- Access ISPs คือชื่อของ ISP ที่ให้บริการสู่ host สามารถติดต่อ กันได้

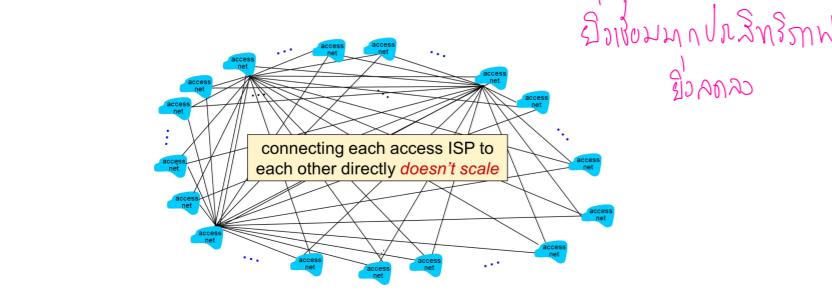
- ทำให้เกิด network of networks ที่ซับซ้อนมาก โดยมีจุดเชื่อมต่อที่มีความสำคัญ เช่น economics และ national policies ของแต่ละประเทศด้วย



- และเราสามารถเชื่อม access ISPs เป็นล้านๆ ตัวได้อย่างไร

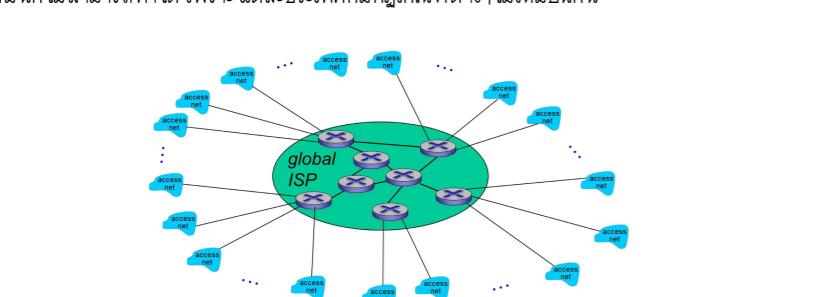


- เราสามารถเชื่อมทุก node บนโลก แบบ fully connected ได้ แต่จะมีข้อเสียที่มีขนาดไม่ scale และเปลืองทรัพยากรถ

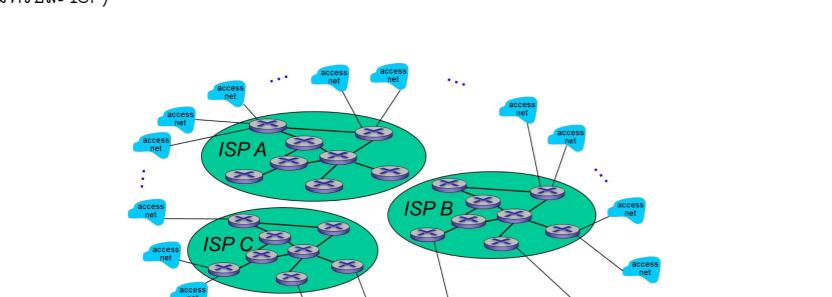


- เราจึงหันมาใช้แบบที่มีเพียง 1 global transit ISP และเชื่อมกับ access net ของแต่ละที่

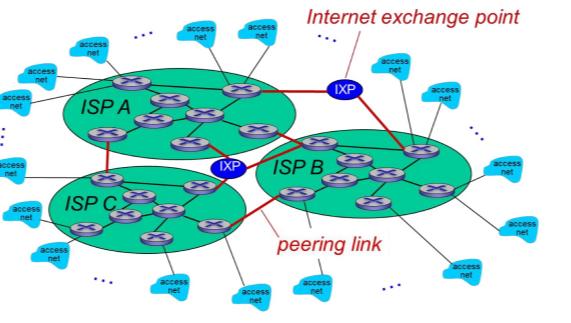
- แต่มันก็ไม่สามารถทำได้ เพราะแต่ละประเทศก็มีภูมิภาคที่ต่างกัน



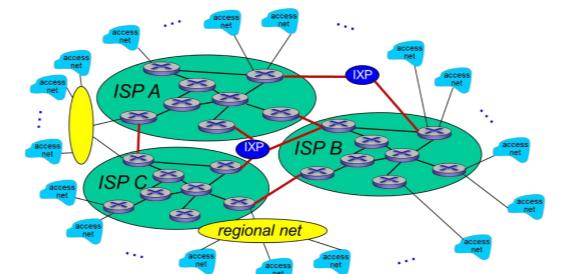
- ในเมื่อ 1 global ISP ไม่สามารถทำได้แล้ว เรากลับมาใช้ต่อเฉพาะ ISP ที่ใกล้เคียงกัน เชื่อมกันดู (อาจจะรวมกลุ่มไว้เป็น ISP)



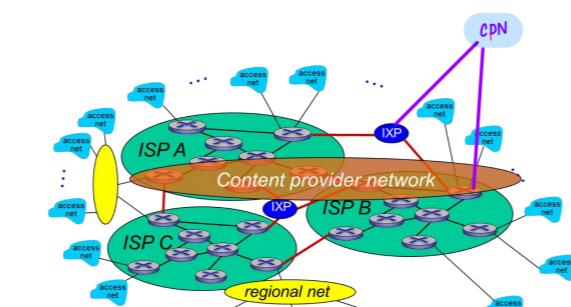
- โดยจะมีสุดยอดเรื่องต่อ internet แต่ละ ISP เรียกว่า Internet Exchange Point (IXP)
- โดยหากมีกรณีที่มี ISP ที่เป็นพันธมิตรกัน (เช่น ISP C กับ ISP B) และไม่อยากผ่าน IXP กลางแต่ต้องร่วมกันไปเลย สามารถทำได้โดย link ที่ต่อต่องานนี้เรียกว่า Peering Link โดยใน link นี้อาจจะมีการเก็บค่าธรรมเนียม และมีการกำหนดภูมิภาคที่ซึ่งกันและกันเอง



- หลายๆ Access ISP อาจเชื่อมกันจนหนาแน่น (แต่เล็กกว่า ISP : tier 1) เรียกว่า Regional net (ISP tier 2)

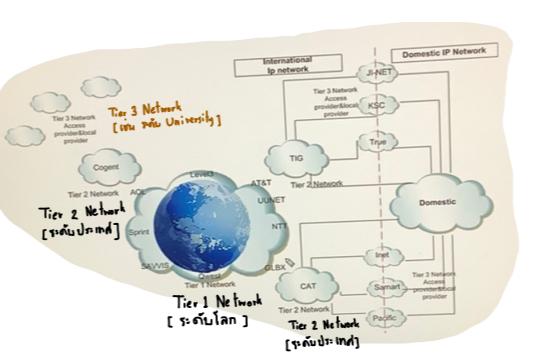
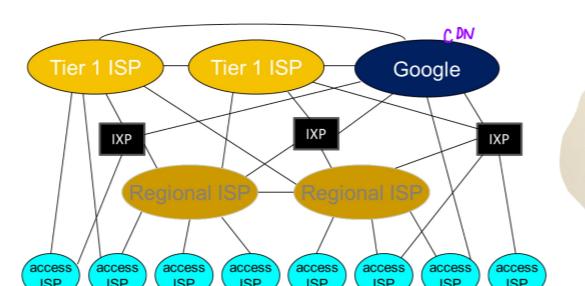


- ในโลกปัจจุบัน เริ่มมีบริการของ content เป็นหลัก และหาก content ไปกระถูกตัวที่ ISP เดียวบ้านจะไม่สมเหตุสมผล เหล่า content provider network (e.g. Google, Microsoft, Netflix) จึงมีการวางแผนต่อรองให้เชื่อมกับ IXP เพื่อให้เชื่อมกับ ISP ต่างๆ ได้ง่าย รวมถึงบาง CPN อาจทำ peering link ต่อต่องาน ISP หรืออาจจ้างตัวของตน ISP เลยก็ได้



- tier 1 นั้นเป็น ISP level สูงๆ (e.g. Level 3, AT&T) เป็นการเชื่อมต่อระดับประเทศ - content provider network (cpn) e.g. Google จะเป็น private network

สรุป : Internet Structure



History of the Internet

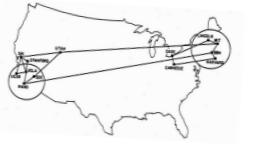
ARPANET

▪ 1969: first ARPANET node operational



- 4 มหาวิทยาลัยได้เชื่อมต่อ กัน ระหว่าง UCLA's Network Measurement Center Stanford Research Institute(SRI) University of California-Santa Barbara University of Utah
- เป็นการลองเชื่อม network ครั้งแรก

ARPANET expands



- 4 มหาวิทยาลัยที่เชื่อมต่อ ได้เชื่อมต่อข้ามประเทศไปยังมหาลัยอื่น ต่อเนื่องจากเดิม 3 มหาวิทยาลัย Harward, MIT, BBN
- network เริ่มใหญ่ขึ้น

ARPANET goes international



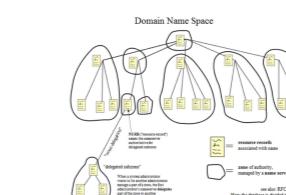
- เริ่มมีการเชื่อมต่อระหว่างประเทศ
- ในปี 1971 มีการใช้ email ครั้งแรก และมีการใช้ @ ระบุที่อยู่ และ domain ของเรา
- ในปี 1973 มีการเชื่อม Internet ข้ามประเทศไปยัง London ประเทศอังกฤษ โดย 75% ของการใช้ Internet จะเป็นการส่ง email

TCP/IP กลายเป็น Standard ของ ARPANET



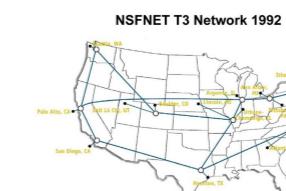
- ที่ TCP/IP ก็ยังคงเป็นมาตรฐานที่ใช้มาจนถึงปัจจุบัน
- Internet เริ่มมีการเชื่อมต่อมากขึ้น

Domain Name System (DNS)



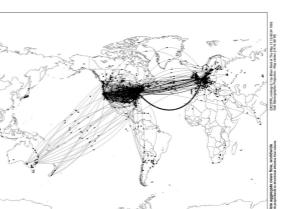
- มีการพัฒนา โปรโตคอล Domain name หรือ DNS ที่มีการใช้งาน url (เช่น www.google.com)
- โดยการค้นหาใช้หลักการ tree โดยมี top คือ root DNS เชื่อมอยู่กับ level 1 ทั้งหมด (top level เช่น .com, .gov, .ac.th)
- ลง top level ก็จะมีอยู่ทุกอีก

NSFNET : The first internet backbone



- มีการเปลี่ยนชื่อ ARPANET เป็น NSFNET
- เริ่มมี backbone internet หรือ link ใหญ่ของ network
- ความเร็ว 45 Mbit/s

Global Internet Network



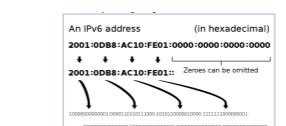
- เกิดปัญหา กับ IPv4 เพราะมีการจัดสรร IP address ที่ล้นเปลือง
- มีการแนะนำให้ใช้ CIDR (Classless Inter-Domain Routing)
- ร่วมร่วมมือการจัดสรรอเป็นทั่วไป
- ทั่วโลกของ APNIC (Asia-Pacific Network Information Centre)

Internet Registries



- ผู้ให้บริการจัดสรร IP address ของทวีปต่างๆ ทั่วโลก
- เช่น APNIC จัดสรรบล็อกให้กับประเทศไทย และก็จะจัดสรรบล็อกให้กับ มหาลัย อีกด้วย

IPv6 Address



- IPv4 เริ่มหมดโลก
- IPv4 ของ APNIC ไม่สามารถจัดสรรได้พอ
- เริ่มมี IPv6
- ในปี 2015 มีการใช้ IPv6 เพียง 5%

1969

1970

1973

1983

1984

1992

1993

1997

2011

523353 Computer Networks

Lecture 3 : Ethernet LANs - Part 1

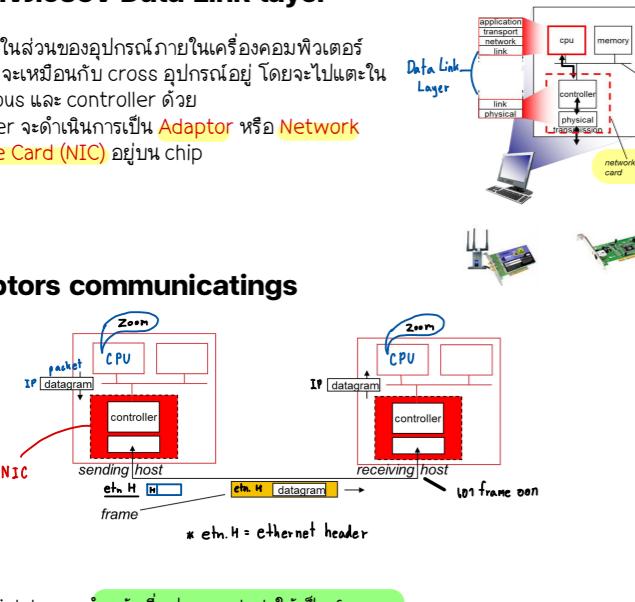
Introduction

- ในบทนี้จะเน้นในชั้นของ Data Link layer หรือ layer ที่ 2
- ทำงานโดยเน้นไปที่ links หรือการเชื่อมต่ออุปกรณ์ network
- link จะเชื่อมต่อระหว่าง node ที่อยู่ติดกัน ไม่ว่าจะเป็นการเชื่อมแบบ wire หรือ wireless ก็ตาม
- การเชื่อมต่อแบบ link ที่เราเน้นในเรื่องนี้คือแบบ LAN และ WAN
- โดยใน layer 2 นี้ เรียกว่า frame คือ frame
- โดย frame คือการที่ใส่ head ให้กับ packet หรือ datagram ของ layer ที่ 3
- หน้าที่หลักของ Data Link layer ในบทนี้คือ
 - รับ-ส่งข้อมูลกับ node ที่อยู่ติดกัน ใน link เดียวกัน

การวางแผนของ Data Link layer

- หางานในส่วนของอุปกรณ์ภายในเครื่องคอมพิวเตอร์ data link จะเห็นกับ cross อุปกรณ์อยู่ โดยจะแบ่งออกในส่วนของ bus และ controller ด้วย
- link layer จะดำเนินการเป็น Adaptor หรือ Network Interface Card (NIC) อยู่บน chip

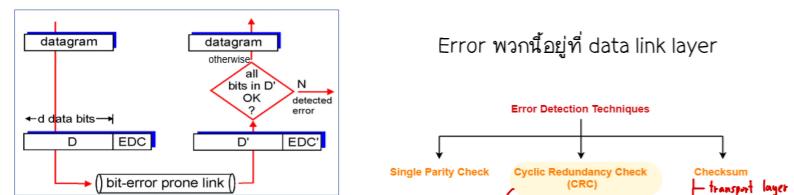
Adaptors communicating



- data link layer ทำหน้าที่แปลง packet ให้เป็น frame
- มีการเพิ่ม error checking, flow control, etc.

- ผู้รับ
 - ตรวจสอบ error, flow control, etc.
 - ถอด packet ออกมา แล้วส่งไป upper layer (จาก Application)

Error Detection and Correction (EDC)



- flow นี้แสดงให้เห็นว่า data frame (packet) จาก data link layer จะมีการเพิ่มอะไรบางอย่างเข้ามาด้วย กذاในภาพนี้คือเพิ่มตัว checking หรือ EDC
- ส่วนที่รับจะเช็ค EDC หรือ CRC ว่าถูกต้องไหม ถ้าถูกต้องจะส่งชี้ให้ upper layer
- data link ไม่ได้ลดมาก เพราะมันนั้นความเร็ว ต้องนั้นซึ่งยังไม่น่าเชื่อถือ 100%
- layer นี้มีแค่การ check พอเป็นพื้นที่ เพราะในทุก layer ก็จะมีการ check อยู่แล้ว

Multiple Access Links and Protocols

เราสามารถแยก node ที่อยู่ติดกันออกได้เป็น 2 ประเภท

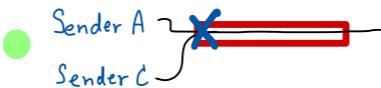
- Point-to-Point
 - PC1 ต่อับ PC2 โดยตรง
 - มี switch คุ้ลแล ในการรับความถูกต้อง

- Broadcast (shared wire or medium)
 - การ share link กัน
 - upstream Hybrid fiber-coaxial (HFC)
 - 802.11 wireless LAN



Broadcast links

- เมื่อการสื่อสารของหลายคนผ่าน link เดียว (single shared broadcast ch)
- อาจเกิดการชน (collision) ซึ่งไม่ดี
- เหตุการณ์ เช่น ผู้ส่ง A จะส่งไปให้ B และใน link เดียวกันด้วยผู้ส่ง C เช่นมาแจ่ม ทำให้อาจเกิดการชนได้



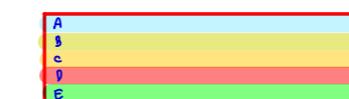
Multiple Access Protocol

- มีหน้าที่ในการจัดแหน่ง channel ที่มีการ share กัน ทำให้ node มีการส่งที่ไม่ชิงกันได้
- โดยต้องห้ามส่ง out-of-band channel หรือ การลงแบบมี secondary link

โดยรวมรู้จักกันในชื่อของ Multiple Access Control (MAC) protocols

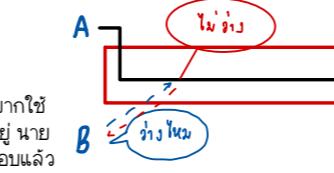
- protocol ที่ดูแลในเรื่องของการชิงกัน
- ทำงานใน data link layer
- มี 3 วิธีในการแก้ไขการชน

* แก้ไขตัวที่ 3 ด้วย Scalability



1. Channel Partitioning

- เป็นการสร้างงานในครอนนั้น
- การแบ่งเวลาใช้ time slots, frequency, code



2. Random Access

- ใช้ CSMA protocols
- CSMA/CD used in Ethernet
- CSMA/CA used in 802.11
- เป็นการ share link แบบไม่แนบเนิน ต้องน้ำใจกับการชิงกันได้
- มีการลดความล่าช้าของการชิง ด้วยการใช้ logic เก็บเวลาช่วย
- เช่น นาย A กำลังใช้ channel อยู่ โดยเดิน เวลาเดียว กันนั้น นาย B อยากใช้ channel นั้นด้วย จึงต้องดูว่ามีใครใช้ channel ใหม่ ถ้ามีคนใช้อยู่ นาย B ก็จะยังไม่ใช้ channel นั้น 10 วินาที แล้วรอกสามีก่อน พอดีกับเวลาที่นาย B ถึงจะใช้ channel นั้น

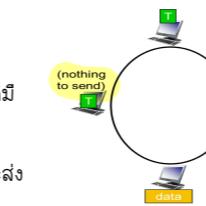
3. Taking turns

- Polling
 - ถ้ามี master อยู่เครื่องนึง แล้วจะมีเครื่องที่ต่ออยู่ใน link เดียวกัน
 - โดย master จะต้องมีการ invite เครื่องอย่างไรจะสามารถลงข้อมูลได้
 - ปัญหาที่เกิดคือ overhead หรือ มีการเพิ่มส่วนที่ไม่จำเป็นติดมากับ packet เรา (invite เป็น overhead), latency (เพราะต้องมีการรอ), single point of failure (ถ้า master พัง ต้องรอนะจะพังไปด้วย)

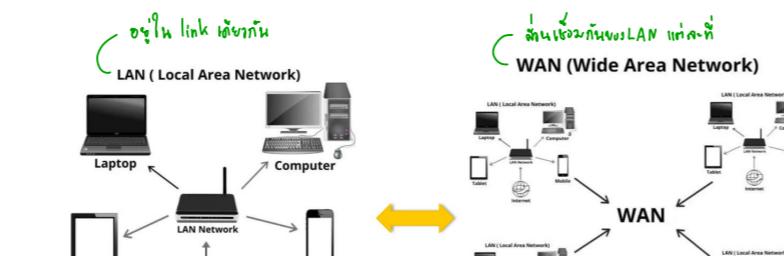


Token passing

- คล้ายกับแบบ polling แต่เปลี่ยนจาก invite เป็น token
- เปลี่ยนจากที่ polling ต้องเป็น bus เป็น ring
- จะไม่มี master
- มองว่าจะมีแหวนวิเคราะห์นึงที่สามารถเดินเรื่อยๆ ให้คนอื่นไม่ได้
- ปัญหาที่เกิดคือ overhead (invite เป็น overhead), latency (เพราะต้องรอนะ), single point of failure (ถ้าคนที่ถือ token พัง token ก็จะลุกให้คนอื่นไม่ได้)



Local Area Network (LAN)



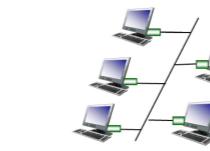
Types of LAN



<https://digitalworld839.b-cdn.net/wp-content/uploads/LAN-vs-WAN-vs-MAN-Comparison.jpg> 12

การต่อ Ethernet LAN

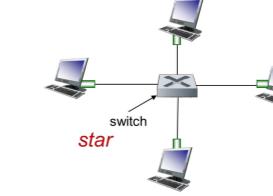
Bus



bus: coaxial cable

- ใช้ในปี 90
- เมื่อ晚晚 adaptor ของแต่ละ PC จึงเข้ากับสาย coaxial
- ทุก node นี้ collision domain เดียวกัน

Star



- ใช้ในปัจจุบัน
- มีอุปกรณ์ตัวหนึ่งอยู่กลาง (อาจเป็น hub หรือ switch)

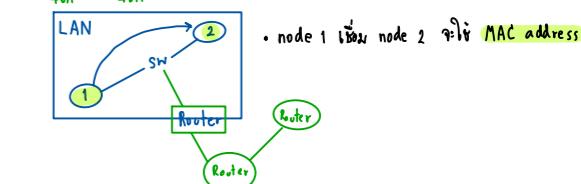
IP address vs MAC address

IP address

- 32 bit address
- อยู่ที่ network layer (layer 3)

MAC address or LAN or physical or Ethernet address

- 48 bit address
- ทำงานใน Data link layer (layer 2)
- Ethernet LAN ใช้ MAC address ในการติดต่อ
- MAC address จะถูกกรุ๊ปไว้ที่ NIC หรือ card LAN
- e.g. 1A-2F-BB-76-09-AD

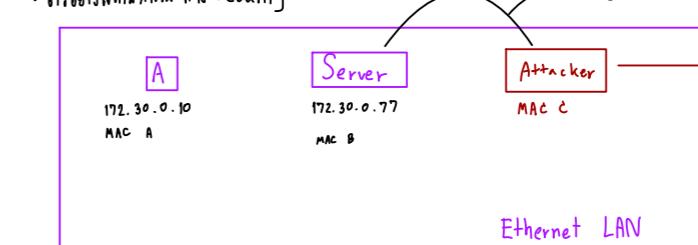


วิธีตั้ง MAC address ของเครื่อง (Window)

- cmd
- ipconfig /all

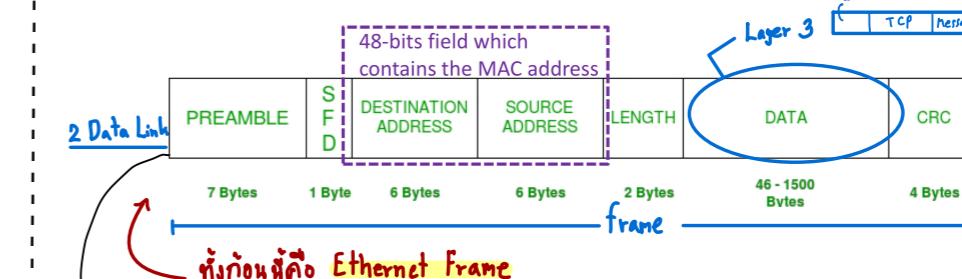
- เวลาติดต่อร้านระหว่างเครื่องที่อยู่ใน link เดียวกัน จะใช้ MAC address ในการติดต่อ

• ตั้งชื่อสกุลภารกิจ ทาง Security

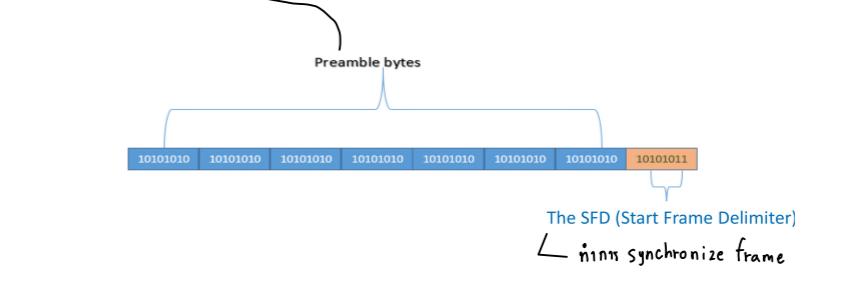


- ร้าน A ต้องต่อ Server ทางตัวเอง ip .77 เลยนะ
- Attacker ต้องต่อ Attacker ต่อ ip address .77 แทนที่ MAC C น่ะจ้า!

Ethernet (IEEE 802.3) frame structure

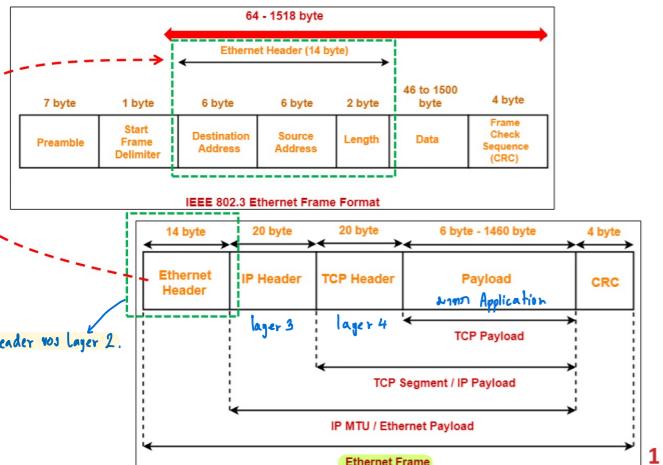


หัวก้อนหัวคือ Ethernet Frame



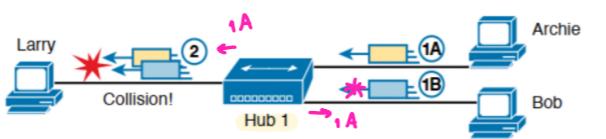
Header

IP datagram sits inside the Ethernet payload field



Using half-duplex with LAN Hubs

- ช่วงปี 1990 IEEE ได้นำเสนอมาตรฐานความเร็วแค่ 10 Mbps และยุคหนึ่งไม่มี switch เลยใช้ hub
- hub คือ repeater (ทำงานที่ physical layer ; layer 1 ในการ repeat สัญญาณไฟฟ้าธรรมด้า)
- ไม่มี MAC ที่ป้องกันการชน
- ไม่มี concept ของ Ethernet frame

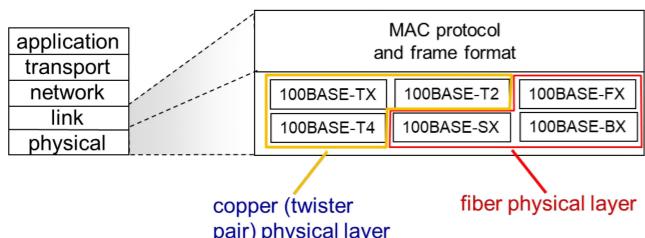


- hub จะมีการ repeat สัญญาณทุกทาง ยกเว้น port input (ทางที่มีนั้นเข้ามา)
- ทำให้เกิดการชนได้ (collision)

- อย่างไรก็ตาม Hub ก็ยังมีตัวป้องกัน collision โดยใช้ half-duplex logic เช่น CSMA/CD แต่ตัวบันทึกไม่ได้ทำงานใน hub บันทึกการทำงานที่ตัว PC

802.3 Ethernet standards : link & physical layers

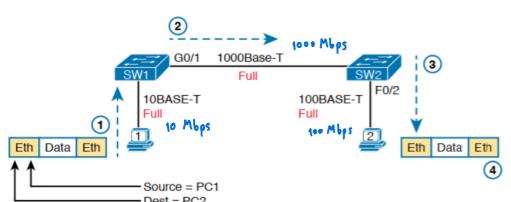
- มาตรฐานความเร็วของ Ethernet : 2 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps, 100 Gbps



| | Ethernet | Ethernet Speed | Cabling System |
|--------------------|-------------|----------------|---|
| 802.3 | 10 Base-2 | 10 Mbps | BNC (coaxial cable) |
| 802.3i | 10 Base-T | 10 Mbps | RJ45 , Cat 3 (10Mbps) |
| 802.3u | 100 Base-TX | 100 Mbps | RJ45 , Cat 5 (100Mbps) |
| 802.3ab | 1000 Base-T | 1000 Mbps | RJ45 , Cat 6 (250Mbps) |
| 802.3ae | 10G Base-SR | 10 Gbs | 62.5 μ, multi-mode (Fiber Optic) |
| 802.3ae | 10G Base-ER | 10 Gbs | 9 μ, single-mode (Fiber Optic) |
| 802.3an (proposed) | 10GBASE-T | 10 Gbs | RJ45 , Cat 6A(350Mbps), Level 7(proposed) |

Hub & Ethernet Switch

- เวลาที่มีการส่ง frame กันจริงๆ ใน LAN เราจะใช้ตัว switch (data link layer)
- ซึ่งจริงแล้วการต่อ LAN จะใช้ switch หรือ hub ก็ได้ (แต่ hub ไม่ค่อยนิยมใช้แล้ว)
- switch จะเป็น full duplex logic ส่วน hub จะเป็น half duplex logic

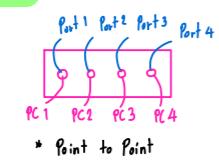


Half-duplex

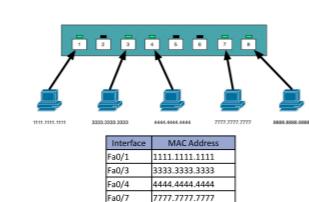
- เวลาเดียวเราส่งและรับส่งไม่สามารถรับ-ส่งพร้อมกันได้

Full-duplex (no LAN hubs)

- point-to-point only
- เวลาเดียวเราสามารถรับ-ส่งพร้อมกันได้
- device ไม่ต้องรอ

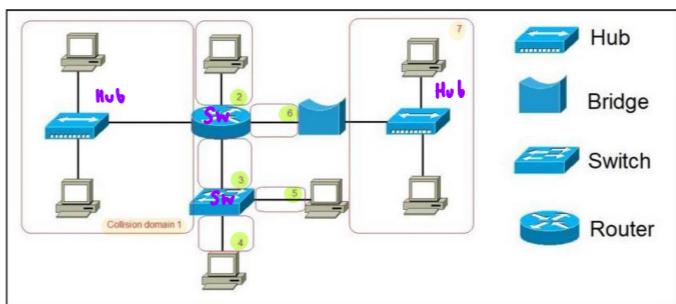


Switching Table



- ลักษณะของ switch มีคลาดกับ hub คือ มันจะมีการตัดต่อข้อมูลนี้เมื่อเรียกว่า Switching table โดยมันจะจับ port ไหนต่ออยู่กับ MAC address ไหนใหม่ โดยมันจะจำนำจากการที่ switch ทำงานที่ data link layer แปลว่ามันจะลงใน Ethernet header
- MAC address ปลายทาง, ต้นทาง
- Length/Type
- Data
- CRC

Collision domain

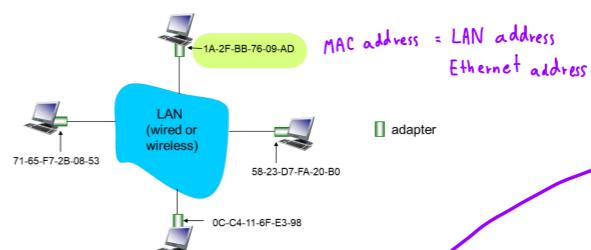


- ขอบเขตที่มีโอกาสชนได้
- เป็นการบอกว่าขอบเขตไหนมีโอกาสชนได้
- ถ้าเป็น hub จะมี collision domain คือ ทั้งก้อนที่ต่ออยู่กับ hub หรือมี 1 collision domain
- ถ้าเป็น switch จะมี collision domain แค่เพียงลังที่เชื่อมอยู่กับ port เดียวเท่านั้น หาก switch เชื่อมอยู่กับ port ก็จะมี collision domain เท่ากับเท่านั้น

Address Resolution Protocol (ARP)

- เหตุความลัง Data link ที่เรานำใจ จะทำงานในขอบเขตที่เป็น LAN ซึ่งมีพื้นฐานบน Ethernet LAN และใช้ address เป็น MAC address
- แต่เวลาที่เราต้องต่อ กัน เราจะใช้ ip address
- จึงมี ARP หรือ address resolution protocol ที่ทำหน้าที่ในการหาว่า ip address นั้น มี MAC address อะไร

LAN address and ARP

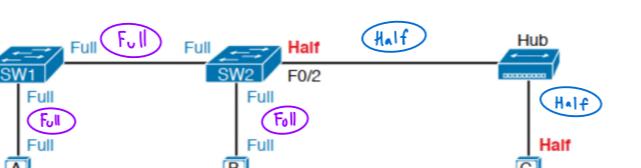


หน้าที่ของ ARP

- หาว่า IP ปลายทางที่เราสนใจ มี MAC address อะไร
- เช่น หาว่า ip address 137.196.7.14 นี้ มี MAC address อะไร
- เครื่องเราต้องเครื่องจะ查 ARP table เพื่อเป็นการบอกว่า เครื่อง A มี MAC address อะไร เครื่อง B มี MAC address อะไร ...
- บุคลากร ARP table นี้ทำหน้าที่ map IP กับ MAC address และอยู่ในการเก็บ <IP address; MAC address; TTL (time to live)>
- TTL : time to live หรืออายุที่เก็บ ปกติแล้วอยู่ที่ประมาณ 20นาที หากหมดอายุเราต้องถามใหม่



Full and Half Duplex in an Ethernet LAN



- ถ้า switch ต่อ switch กันให้ link นั้นเป็น full duplex เพราะ switch ทำงานแบบ point to point แต่ละเครื่องเป็นอิสระต่อ กัน
- ถ้า switch ต่อ กับ hub ทำให้ link นั้นเป็น half duplex โดย half duplex ต้องทำงานที่ CSMA/CD เพื่อไม่ให้มีการ collision ได้

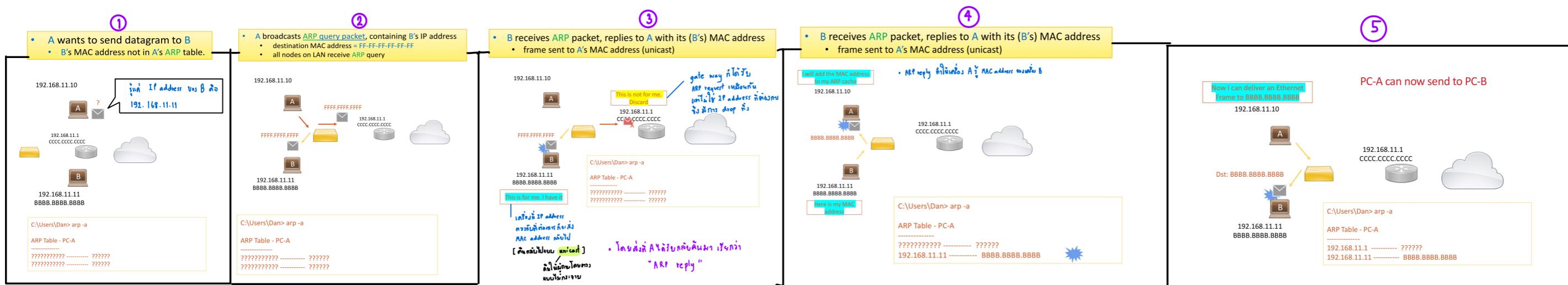
Half-duplex

- เวลาเดียวเราส่งและรับส่งไม่สามารถรับ-ส่งพร้อมกันได้

Full-duplex (no LAN hubs)

- point-to-point only
- เวลาเดียวเราสามารถรับ-ส่งพร้อมกันได้
- device ไม่ต้องรอ

Example



- A ต้องการส่ง datagram ไปให้ B โดยที่ A รู้แค่ IP address ของ B (ไม่รู้ MAC address) ซึ่งทั้งสองเครื่องอยู่บน LAN เดียวกัน

- A จะส่ง ARP query packet กระจายออกไป (เพราบีร์แค่ IP broadcast [ffff.ffff.ffff])
- จะมีเครื่องใดเครื่องหนึ่งที่ได้ IP address ตามที่ต้องการ 192.168.11.10 ให้มอกกลับมาที่ IP address 192.168.11.10 พร้อม
- การที่เราถูก MAC address ห้าม LAN เราเรียกว่า การทำ ARP request

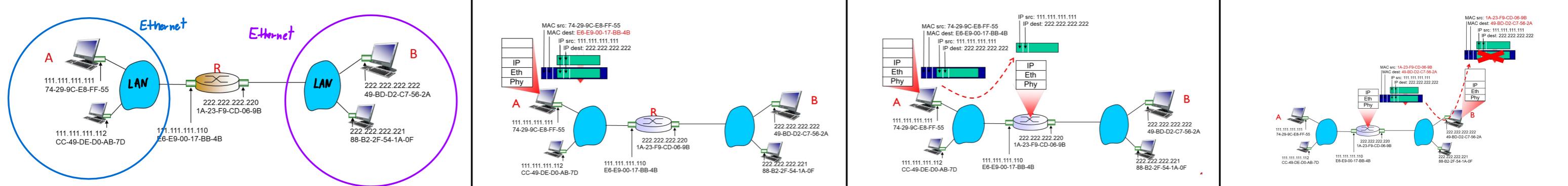
- เครื่องไหนที่ได้รับ request แต่ไม่ใช่เลข IP address ที่ต้องการก็จะทำการ drop ทิ้งไป
- ส่วนเครื่องไหนที่ได้รับ request และเลข IP address ตรงกับที่ต้องการก็จะส่ง MAC address กลับไปแบบ unicast หรือ ส่งให้ผู้ถูกโดยตรง แบบที่ไม่กระจาย
- และเครื่องที่ได้รับ MAC address คืนมาจะเรียกว่า ARP reply

- A ได้รับ ARP reply และทราบ MAC address ของ B ด้วย
- เครื่อง A ก็จะสามารถส่ง datagram ให้เครื่อง B ได้ โดยใช้ MAC address ที่ทราบมา

- คราวนี้หาก A ต้องการส่ง Ethernet frame หรือ packet ออกไปหา B ก็จะมีการระบุ destination MAC ได้แล้ว เพราะเราทราบ MAC address ใน table แล้ว

Addressing : Routing to another LAN

- หากมีการติดต่อกันใน LAN ก็จะมีการใช้ MAC address
- แล้วหากติดต่อทั่วโลก LAN ล่ะ จะทำอย่างไร



- A รู้ ip address ของ B
- A รู้ gateway

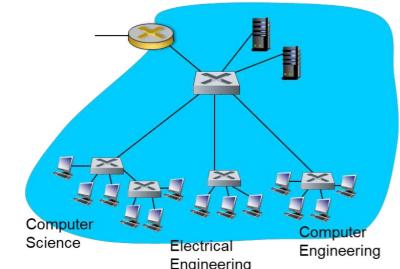
- A เป็น PC (ทำงานตั้งแต่ application layer จนถึง physical layer)
- เวลา A จะส่ง data ก็จะส่ง packet ขึ้นมา
- พอดีกับ network layer ก็จะมีการใส่ ip address
- พอดีกับ datalink layer จะมีการสร้าง frame ซึ่งจะลงใน MAC address ซึ่งมันจะรู้ MAC address แต่พิเศษใน LAN เดียวท่านเท่านั้น เวลาใช้ชีวนิจ ใช้ MAC address ของ gate way (R)

- frame จะถูกส่งจาก A ไปถึง R
- เมื่อ R (Router ทำงานที่ Network layer) ได้รับ ก็จะทดสอบ frame ของ A เหลือแต่ ส่วน network layer
- เหลือ src address และ destination address
- ถ้า port นั้นของ Router ก็จะต่ออยู่กับป้ายทาง ซึ่งเป็นคนละ LAN กับต้นทาง และเป็น Ethernet จึงลงใน MAC address ซึ่งต้องมีการใส่ MAC address ใหม่

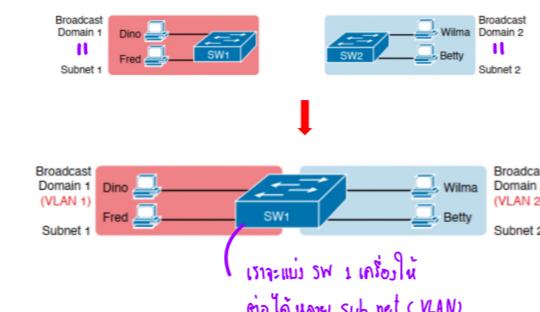
- มีการตั้ง MAC address ของต้นทางให้เป็นของ R(Router) และเปลี่ยน ทางเป็น MAC address ของตัวปลายทาง (โดยทราบ MAC address จากการ ดำเนิน ARP)

Ethernet Virtual LANs (VLANs)

- แรงบันดาลใจจากการที่ ลมมีวิธี SW ตัวเดียวคลื่น 200k บาท (core sw)
แล้วว่า SW อย่าหลงฯตัวเดียวจะประมาณ 10k บาท
- สงสัยว่า คนจาก computer science ต้องการอะไรห้องทำงานไปที่ห้องของ EE แต่ยังต้องการใช้ LAN ของ CS อยู่ จะทำได้อย่างไร?

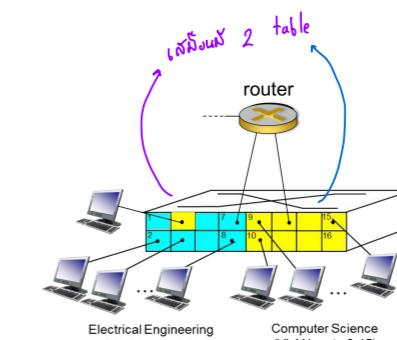
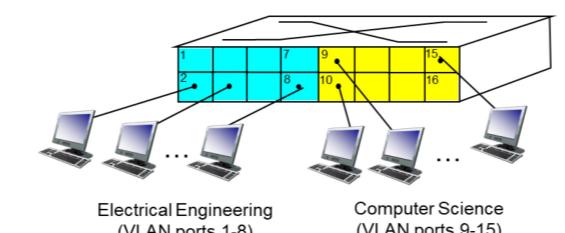


- ปกติแล้ว single broadcast domain(ที่ว่า subnet เดียวกัน)
เราสามารถแบ่ง LAN ย่อยๆ โดยใช้ VLAN



เราแบ่ง SW 1 เดียว成
成 2 了个子网 (VLAN)

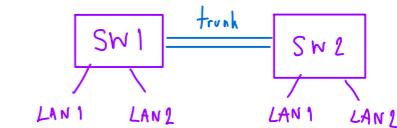
- วิธีการทำ เราใช้กระบวนการ Port-based VLAN
- เป็นการตั้ง VLAN ขึ้นกับ port
- รวมเชือก เช่น VLAN port 1-8 เป็น LAN 1
VLAN port 9-16 เป็น LAN 2
- หากเราไม่มีการตั้งไว้เพิ่ม ก็จะส่งหาทุกหัวทาง 2 VLAN ไปได้



- มีประโยชน์ คือ ทำให้เกิด traffic isolation ได้
- ถ้ามี bot net เน็มมา แล้วส่ง broadcast address ที่อยู่ที่ LAN นั้นจะทำลายได้แค่ port ใน VLAN เดียว
(ใช้ network เล็กที่กว้าง)

- เรายังสามารถกำหนดว่า port จะรับอะไรอยู่ VLAN ไหนบ้าง (dynamic membership)

- ถ้าเราต้องการตัดห้อง LAN เอาต้องเพิ่มความสามารถ ของ router หรือไม่ใช้ sw ที่มีความสามารถ layer 3 [enabler routing]

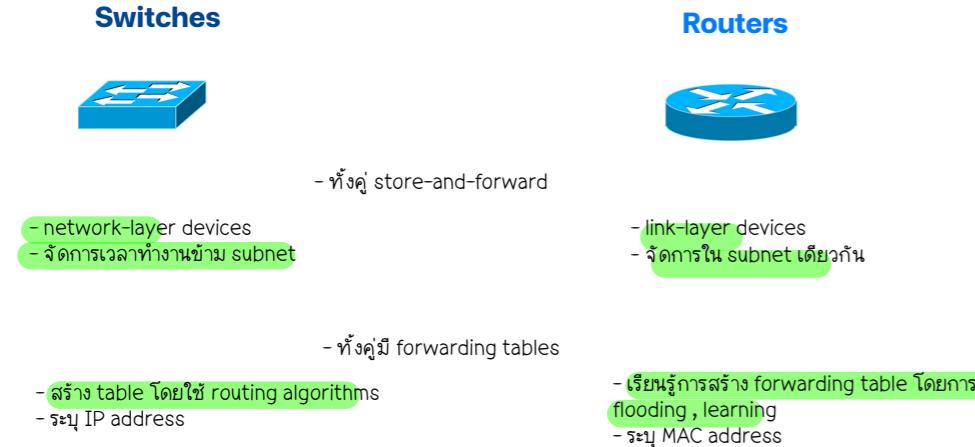


- เรายังสามารถต่อ 2 sw โดย ให้ LAN1 sw1 ติดต่อ LAN1 sw2 ได้โดย การทำ trunk

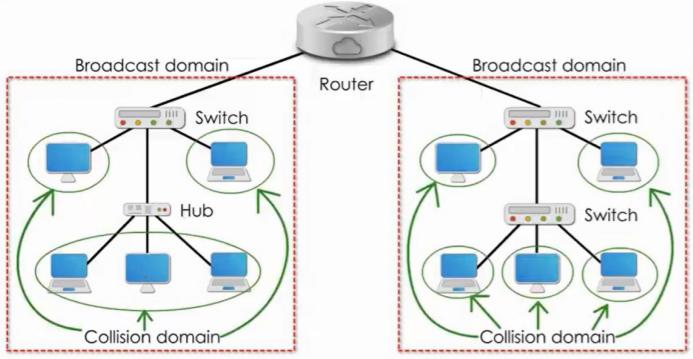
523353 Computer Networks

Lecture 4 : Ethernet LANs - Part 2

Switches vs Routers



Collision domain vs Broadcast domain



Collision domain

- การส่ง packet ให้ระดับของ subnet
- ถ้า network ในนี้ subnet เดียวกัน แสดงว่ามี Broadcast domain เดียวกัน

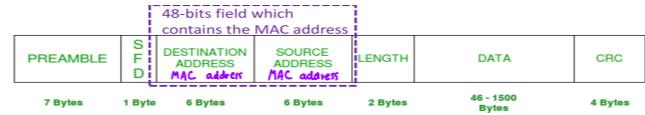
ex. 192.168.0.0/24
 1-254
 • ต้อง ping ต้อง broadcast, address ทุกต่อ กับ ได้รับ
 192.168.0.255

Ethernet Virtual LANs (VLANs)

Trunk port

แล้วการทำงานข้าม switch มันจะรู้ได้อย่างไรว่าอยู่ LAN เดียวกัน ?

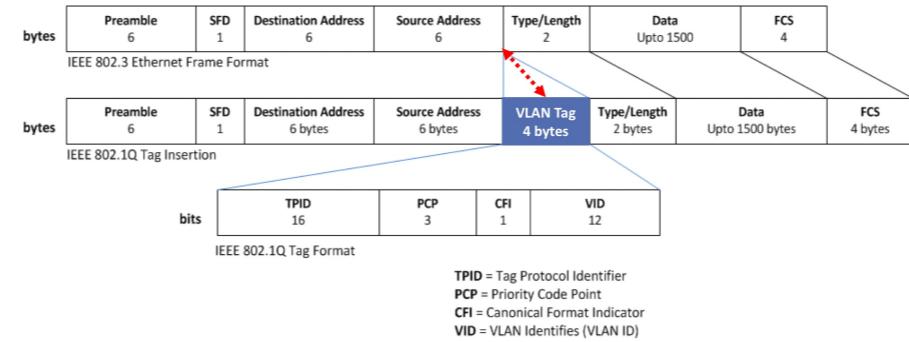
- มันจะมีการเปลี่ยนแปลงบางอย่างใน frame
- ภายใน Ethernet frame จะมี



- จะสังเกตว่าไม่มี VLAN อยู่ใน frame นี้เลย

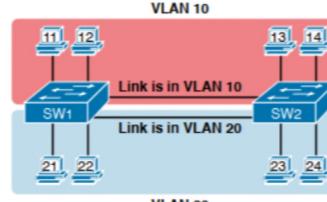
...แล้วมันจำแนก VLAN อย่างไร?

802.1Q VLAN frame format



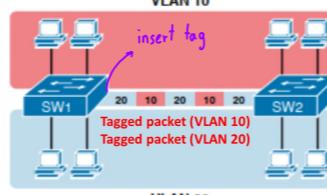
- ในการรุก 802.1q จะมีการแทรก VLAN tag 4 bytes ไปหลัง Src address
- เช่น VLAN tag เป็นการระบุ VLAN id (VID) และ TPID หรือ ลิ๊งที่ไว้จำแนกว่าเป็น vlan tag หรือ untagged frame (native vlan)

Multi-switch VLAN



Multi switch ที่ไม่มีการทำ VLAN trunking

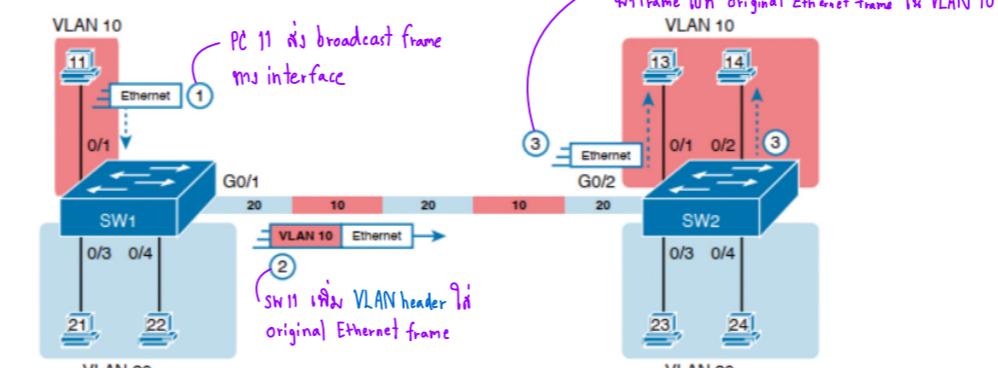
- เช็ค port เอก เช่น g1/0/23 mode access access vlan 10
- หากเราต้องการ 10 vlan เราต้องเลี่ยง interface ไป 10 interface
- ข้อเสีย คือลื้นเปลือง



Multi switch ที่ทำ VLAN trunking

- หากเราต้องการ 10 vlan เราสามารถทำได้โดยเลี่ยงแค่ 1 interface
- ประยุกต์ port มากกว่าไม่มี trunk
- จะมีการ tag packet ว่าเป็น vlan ที่เรา set ไว้

VLAN trunking between two SW

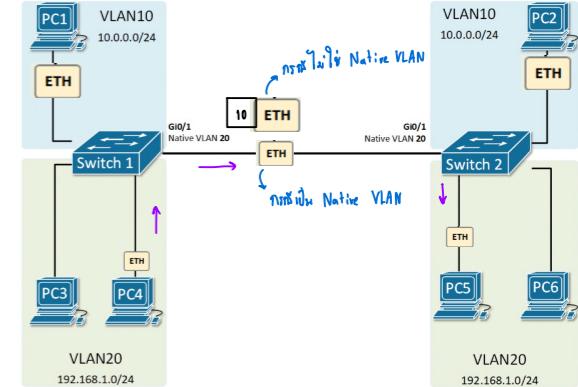


* ก็จะต้องมี table แห้ง

- สังเกตว่าไม่มีการใช้ IP address เลย เพราะเวลาส่งใน data link เป็นการทำที่ MAC address
- แต่ให้เน้นว่าเรา ping เราจะใช้คำสั่ง ping <ip address> และที่มันสามารถ ping ได้ เพราะ มีการแปลงเป็น MAC address โดย ARP

Trunk Native VLAN

- หรือที่เรียกว่า untagged
- default ของ Native VLAN คือ 1 (ถ้าไม่เปลี่ยน Native VLAN อาจโดน attack ได้)
- ส่วนมากจะกำหนด Native VLAN ไม่ให้เป็น default



ex. Native VLAN var trunk = 20

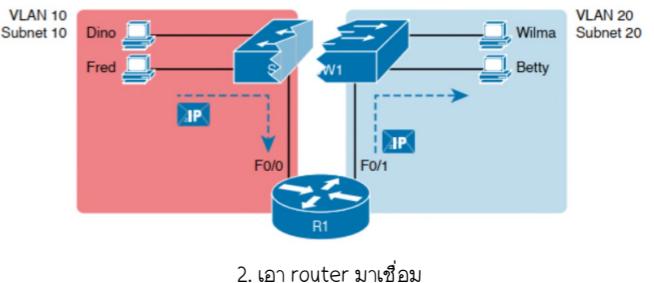
- PC 4 จะส่ง packet ของตัวเองที่ไม่ต้องผ่าน SW
- แต่ packet ที่ต้อง VLAN 20 จะเป็น untagged packet (Native VLAN)

Routing between VLANs (Inter VLANs Routing)

- ปกติจะไม่มีการทำการข้าม VLAN เพียง SW เป็น layer 2
- แต่หากต้องการการข้าม การข้าม VLAN ทำได้ 2 วิธี คือจะเอา router มาเชื่อม หรือไม่เอา router มาเชื่อมก็ได้



1. หาก SW เป็นแบบ multilayer sw หรือ sw level 3 ให้เรา enable ความสามารถ layer 3 ของ sw อกมา คำสั่ง ip routing



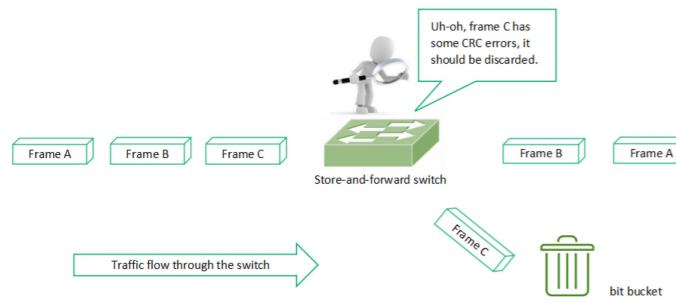
2. เอา router มาเชื่อม



Switching Techniques

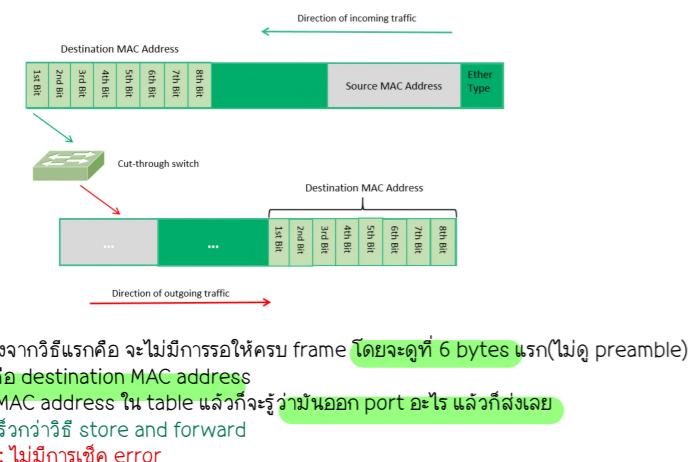
- ใน switch ที่เรา set ไว้ให้อุปกรณ์ มีอยู่ 3 เทคนิค

1. Store and Forward



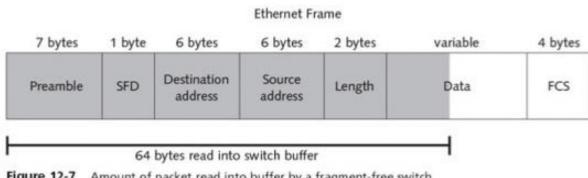
- จะมีการรอ frame ให้เข้ามาใน SW ให้หมดทั้ง 1 frame ก่อน แล้วค่อยประมวลผลว่า frame นั้นควรไปออกที่ port ไหน
- ที่รอให้ frame เข้ามาก็หมดกี๊ดเช็ค crc
- ข้อดี : มีการเช็ค error ที่ crc ถ้าไม่มี error ก็จะ forward ไปตาม table ปกติ

2. Cut-Through



- แต่ก่อต่างจากวิธีแรกก็จะไม่มีการรอให้ครบ frame โดยจะดูที่ 6 bytes แรก(ไม่ดู preamble)
- เช็ค destination MAC address
- เช็ค D MAC address ใน table และก็จะรู้ว่ามี哪個 port อะไร แล้วก็ส่งเลย
- ข้อดี : เร็วกว่า store and forward
- ข้อเสีย : ไม่มีการเช็ค error

3. Fragment-Free

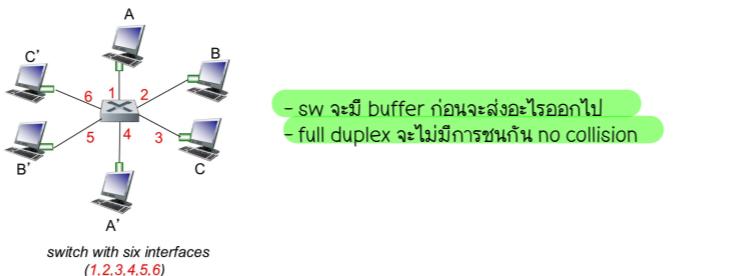


- เป็นการรวมวิธีที่ 1 + 2
- Fragment-free คือต้นทางสายกลาง รอ 64 bytes แรก
- เพราะ ใน Ethernet LAN หากมีการชน มักเกิดที่ 64 bytes แรก
- ข้อดี : เร็วกว่า store and forward , โอกาสชนน้อยกว่า cut through
- ข้อเสีย : no error check , ช้ากว่า cut through

- ส่วนใหญ่การเลือกวิธี คือ จะดูว่า scaling หรือความหนาแน่นของ traffic
- หากหนาแน่นสูง จะใช้ fragment free หรือ cut through
- ex. ACL คล้ายกับ firewall มันใช้ cut through ไม่ได้

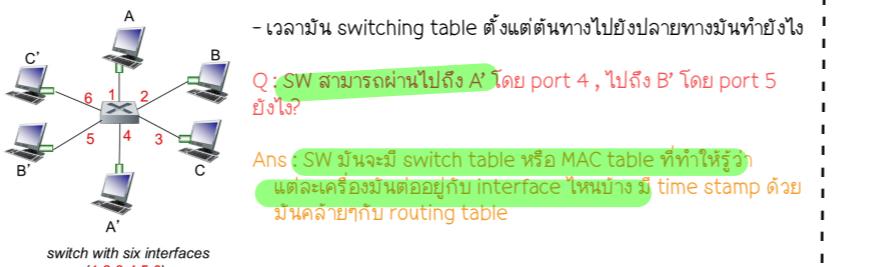
Switch

Multiple simultaneous transmissions



- SW จะมี buffer ก่อนจะส่งออกไป
- full duplex จะไม่มีการชนกัน no collision

Switch forwarding table



เวลา main switching table ตั้งแต่ต้นทางไปยังปลายทางมันทำยังไง
Q: SW สามารถส่งไปยัง A' โดย port 4 , ไปยัง B' โดย port 5 ได้จริงๆ?
Ans: SW นั้นจะมี switch table หรือ MAC table ที่ทำให้รู้ว่า แต่ละเครื่องมีต้องอยู่กับ interface ไหนบ้าง มี time stamp ด้วย มันคล้ายกับ routing table

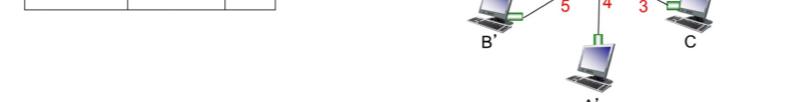
Q: มัน maintained ใน switch table อย่างไร

Ans: หากมีการส่ง packet มันจะอัปเดต switch table เสีย呀

Self-learning

- ตัว SW มีลักษณะการทำงานที่เรียกว่า self-learning
- เป็นการ learn เพื่อสร้าง switch table

| MAC addr | interface | TTL |
|----------|-----------|-----|
| A | 1 | 60 |



ยกตัวอย่างการ learn

0. เริ่มจากที่ table ว่างเปล่า ไม่มีข้อมูลอะไรเลย

| MAC addr | interface | TTL |
|----------|-----------|-----|
| | | |

empty

1. เครื่อง A ต้องการส่งไปหา A' (ping A')

- เครื่อง A ก็จะส่งไปตาม port 1
- เวลาสร้าง table ขึ้นต้นมันจะดู MAC address ต้นทางของ frame ที่เข้ามา ให้ port ไหน

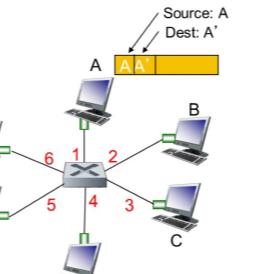
| MAC addr | interface | TTL |
|----------|-----------|-----|
| A | 1 | 60 |

initial

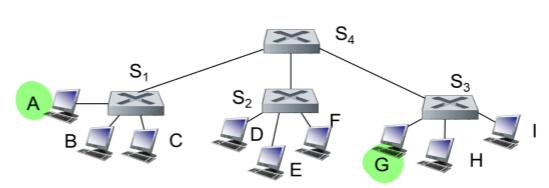
2. จะมีการ flood เพราะ มันไม่รู้ MAC address ของ A' (ไม่มีในตาราง)

- A' ที่ได้รับ ping ก็จะ reply กลับไป โดยจะดูว่าต้นทางอยู่ที่ไหนใน table ก็จะ reply กลับไปแบบไม่ flood
- มีการใส่ A' กับ port ใน table

| MAC addr | interface | TTL |
|----------|-----------|-----|
| A | 1 | 60 |
| A' | 4 | 60 |



Interconnecting switches



ยกตัวอย่างการ learning ขั้นตอน

ตัวการส่งจาก A ไป G โดยเดินทาง S1 โดยผ่าน S4 และ S3

- การส่งจะถูกตัดขาดอย่างเมื่อที่
- 0. เริ่มจาก table ของทุก SW จะ blank คือ
 1. เกิดการเรียนรู้โดย self learning (รู้ต้นทาง : ไป A)
 2. เกิดการ flood เพื่อหา G ไปทุกที่ ที่ไม่ใช่ต้นทาง
 - การ flood ไปถึง S4 ด้วย
 - S4 ก็จะ flood ต่อ ซึ่งไปถึง S3 ด้วย
 3. เจอ G ที่ SW 3 ซึ่งมีการสร้าง table (ใส่ G และ port)
 - reply กลับไปหาต้นทาง

Institutional network

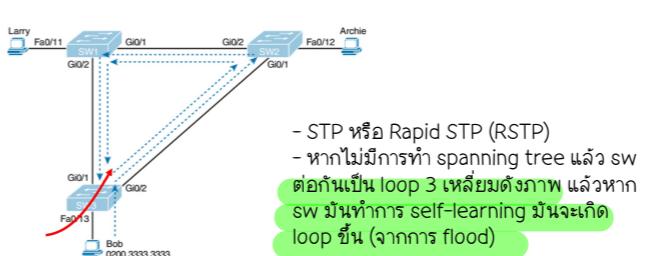


- SW นี้เป็น subnet เดียวกัน
- ล่า network ใหญ่ performance ก็จะตก
- จึงมีการทำ department ย่อย

Spanning Tree Protocol

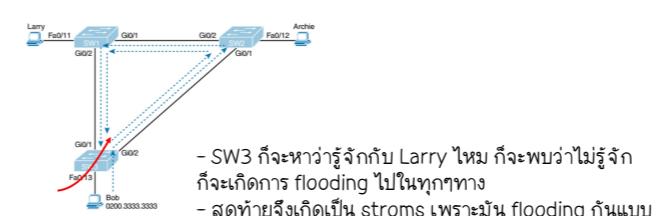
- เรื่องนี้สำคัญกับ lecture (ออกแบบด้วย)
- แต่ไม่สำคัญกับการปฏิบัติ เพราะอุปกรณ์มันทำให้ได้เอง
- จุดมุ่งหมายของมันคือการป้องกัน loop

Spanning tree คืออะไร



- STP หรือ Rapid STP (RSTP)
- หากรู้ว่ามีการทำ spanning tree แล้ว SW ต้องนั้นเป็น loop 3 เหตุยังคงภาพ แล้วหาก SW มันทำการ self-learning มันจะเกิด loop ซึ่ง (จากการ flood)

1. Broadcast storms happen : เช่น Bob ต้องการส่งไปหา Larry



- SW3 ก็จะหาว่ารู้จักกับ Larry ใหม่ ก็จะพบว่าไม่รู้จัก ก็จะเกิดการ flooding ไปทุกทาง
- สุดท้ายจะเกิดเป็น storms เพราะมัน flooding แบบไม่รู้จบ

2. MAC table instability

- : ถ้าสุดท้ายแล้วมีการแก้ปัญหา storm ได้ อาจเกิดปัญหานี้ได้ ซึ่งมันคือการที่ Mac address ไม่คงที่

- เช่น SW3 ตอนแรกร่าง table ขึ้นมา ดังนี้

| Fa0/1 | Fa0/6 |
|-------|-------|
| Bob | |

มีการ flooding ไปที่ SW2 และมีการสร้าง table

| Fa0/1 | Fa0/6 |
|-------|-------|
| Bob | |

มีการ flooding ไปที่ SW1 และมีการสร้าง table ขึ้นมา



แล้วก็ยังมีการ flooding อีก ซึ่งอาจเกิด loop และ table ที่สร้างขึ้นมาที่ SW3 มาก คือ

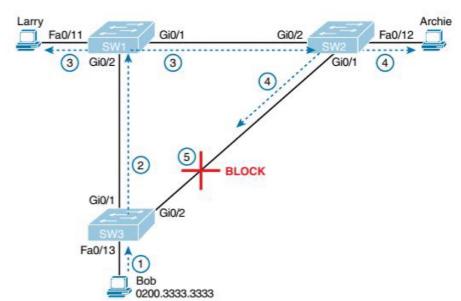


ซึ่งการเปลี่ยนแบบนี้ คือ MAC instability

จึงมีการแก้ไขปัญหา loop ข้างต้นโดย....

Spanning Tree

- เป็นการทำให้ไม่เกิด loop

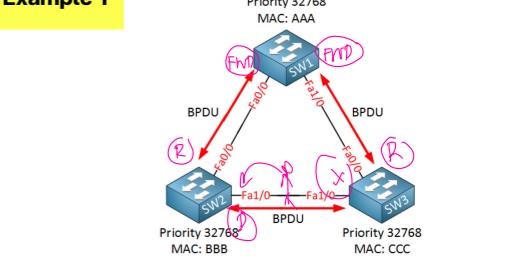


ตัวอย่างการทำ spanning tree

1. Bob 送 frame ไปที่ sw3
 - ก็จะมีการสร้าง table ที่ sw3
2. sw3 มีการ block port (blocking state) ที่ g0/2 ทำให้ในการ flood สามารถ forwards ไปได้แล้ว พอไหวกัน
3. sw1 flood และเรียนรู้
 - จะมีการสร้าง table คือ
4. sw2 ที่ถูก flood มาก็จะมีการ learning
 - และสร้าง table คือ
5. sw2 ที่ส่งไปที่ sw3 จะเจอ block port จึงเกิดการ ignore
 - และมีการ drop ที่

แล้วมันทำการ block อย่างไร

Example 1



Spanning tree เป็นการหาว่า block port ควรเป็น port ไหน

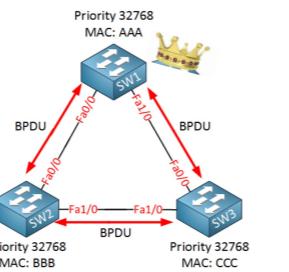
1. เริ่มจาก SW มีอยู่ 3 ตัว
 - จะมีการส่ง msg ระหว่าง SW ซึ่งเรียกว่า BPDU(Bridge Protocol Data Unit) เป็นตัวที่ใช้ส่ง MAC address กับ Priority
2. MAC address กับ Priority จะเป็นตัวที่ระบุ bridge id
 - เช่น 32768.BBB
3. จะมีการหา root bit
 - จากตัวที่ว่า bit id น้อยที่สุด
 - หาก Priority เท่ากัน ให้หาที่ MAC id ไหน ต่ำที่สุด
 - จากตัวที่อยู่远ที่สุด SW1 จึงเป็น root bridge เพราะ bridge id ต่ำสุด
 - SW ตัวอื่นที่ไม่ใช่ root bridge จะจัดเรียงกัน non root

โดยจากขั้นตอนที่กล่าวมา สามารถสรุปเป็นข้อๆได้ดังนี้

Spanning Tree solves loops

1. To elect a Root Bridge

- หา best bridge ID ให้มานี่เป็น Root Bridge (lowest bridge id)



4. เราจะตั้งให้ทุก port ของ root bridge เป็น designated port (D)
หรือ forwarding state (FWD)

5. มาตรฐานที่ non-root switch พากษ์ต้องหา shortest path เพื่อไปยัง root bridge

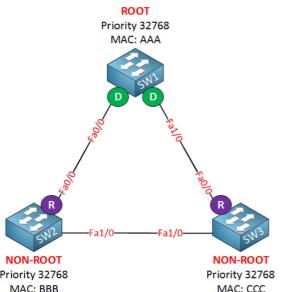
- shortest path คือ ทางที่ cost น้อยที่สุด โดยเราจะดูที่ความเร็วของ link

- 10 Mbit = Cost 100
- 100 Mbit = Cost 19
- 1000 Mbit = Cost 4

Fa คือ fast ethernet จะมีความเร็ว 100 Mbps (Cost=19)

Ga คือ gigabit ethernet จะมีความเร็ว 1000 Mbps (Cost=4)

6. จะได้ Root port (R: shortest path ต่างภาพ)



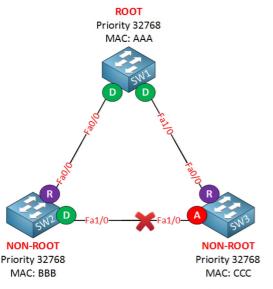
7. ต้องเช็คก่อนว่า designated port จะต้องอยู่ตรงข้ามกับ root port

8. กำหนด port ที่ว่าง

- เราจะมองที่ลีกอกันว่าไปทาง SW ไหนจะใช้ cost น้อยสุดในการไป root bridge (หาก cost เท่ากันให้มองที่ bridge id)

- ผังที่เราเลือกจะเป็น designated port ล้วนผังที่เหลือก็จะเป็น block port

9. จึงได้ Blocking state ที่ port Fa1/0 ที่ SW3



3. Each non-root switch selects its Root Port

- ของที่ non-root ยื่นๆ เพื่อหา Root Port
- The least-cost path to send frames to the root switch (path ไหนใช้ cost น้อยสุดในการไป Root bridge)
- The best bridge id (ถ้า cost เท่ากันให้ดูที่ bridge id ต่ำสุด)
- The lowest internal interface number (ถ้ายังเท่ากันอีก ให้ดูที่ internal interface number)

3.1 Optional - Designated ports opposite to Root Port

- ของที่ non-root ยื่นๆ เพื่อหา Root Port

- The least-cost path to send frames to the root switch (path ไหนใช้ cost น้อยสุดในการไป Root bridge)
- The best bridge id (ถ้า cost เท่ากันให้ดูที่ bridge id ต่ำสุด)
- The lowest internal interface number (ถ้ายังเท่ากันอีก ให้ดูที่ internal interface number)

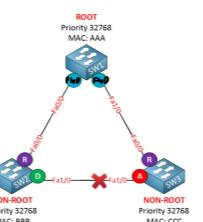
3.1 Optional - Designated ports opposite to Root Port

- port ไหนที่ตรงข้าม designated port จะเป็น root port

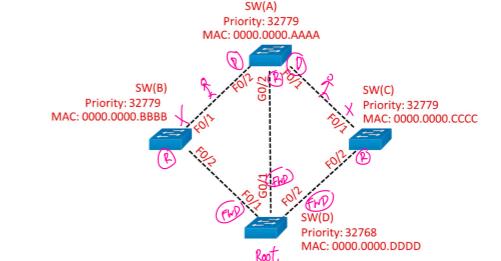
4. Remaining links choose a Designated Port (each LAN segment)

- The link ที่เหลือ
- The SW with the lowest root path cost (ดู SW ซ้ายหรือขวาที่มี root path ต่ำที่สุด)
- The best Bridge ID (โดยดูจาก best bridge id)
- The lowest internal interface number (ดูที่ lowest internal interface number ด้วย)

5. All other ports are put into a Blocking state

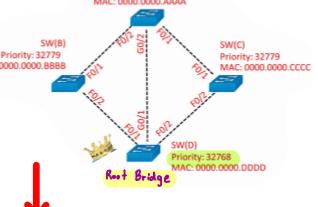


Example 2



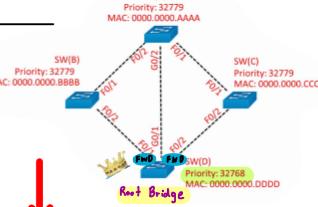
1. To elect a Root Bridge

- หา best bridge ID ให้มานี่เป็น Root Bridge (lowest bridge id)



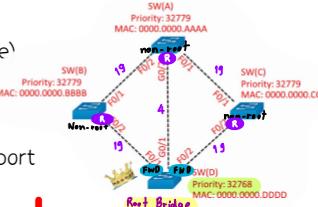
2. Root interface into a Forwarding state (Designated ports)

- ser root interface ทุกตัวให้เป็น forwarding state (FWD) [มันคือตัวเดียวกับ D]



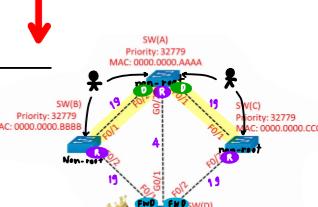
3. Each non-root switch selects its Root Port

- ของที่ non-root ยื่นๆ เพื่อหา Root Port
- The least-cost path to send frames to the root switch (path ไหนใช้ cost น้อยสุดในการไป Root bridge)
- The best bridge id (ถ้า cost เท่ากันให้ดูที่ bridge id ต่ำสุด)
- The lowest internal interface number (ถ้ายังเท่ากันอีก ให้ดูที่ internal interface number)



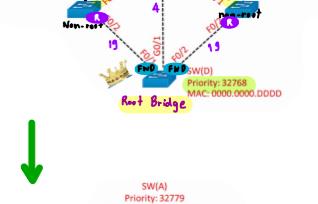
3.1 Optional - Designated ports opposite to Root Port

- port ไหนที่ตรงข้าม designated port จะเป็น root port



4. Remaining links choose a Designated Port (each LAN segment)

- The link ที่เหลือ
- The best Bridge ID (โดยดูจาก best bridge id)
- The lowest internal interface number (ดูที่ lowest internal interface number ด้วย)



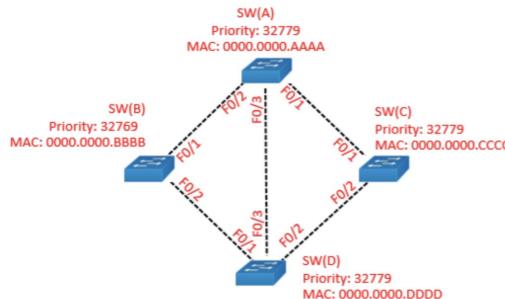
5. All other ports are put into a Blocking state



Example 3

แสดงขั้นตอนตามที่บันทึกใน Slide หน้า 32

Classroom 4



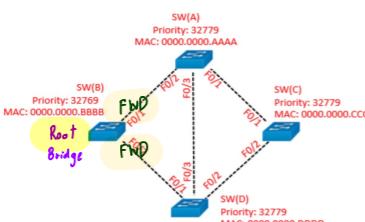
Step

1. To elect a Root Bridge

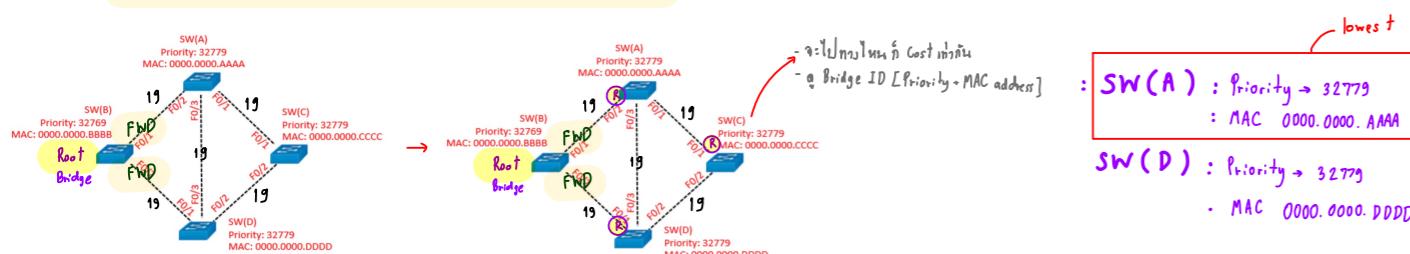
- The best Bridge ID

priority ก็ต้องดูจาก MAC address
SW(A) : 32779
SW(B) : 32769 Root
SW(C) : 32779
SW(D) : 32779

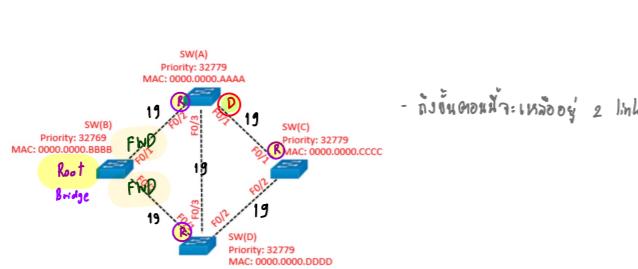
2. Root interface to the Forwarding state



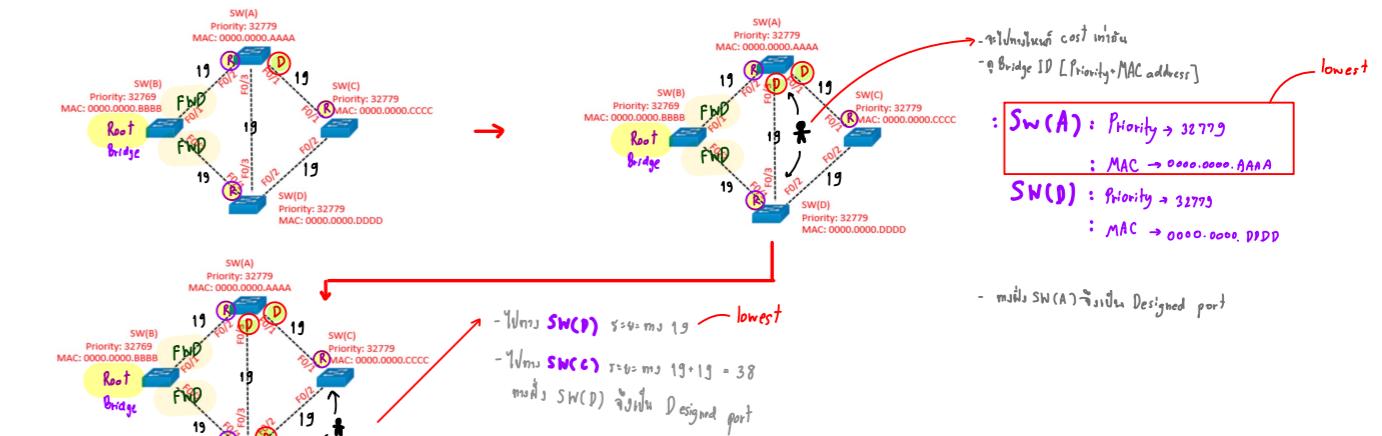
3. Each non-root switch selects its Root Port



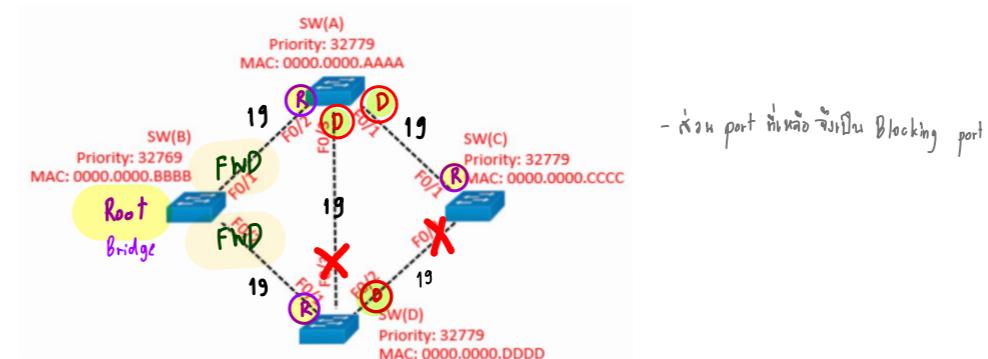
3.1 Optional - Designated ports opposite to Root port



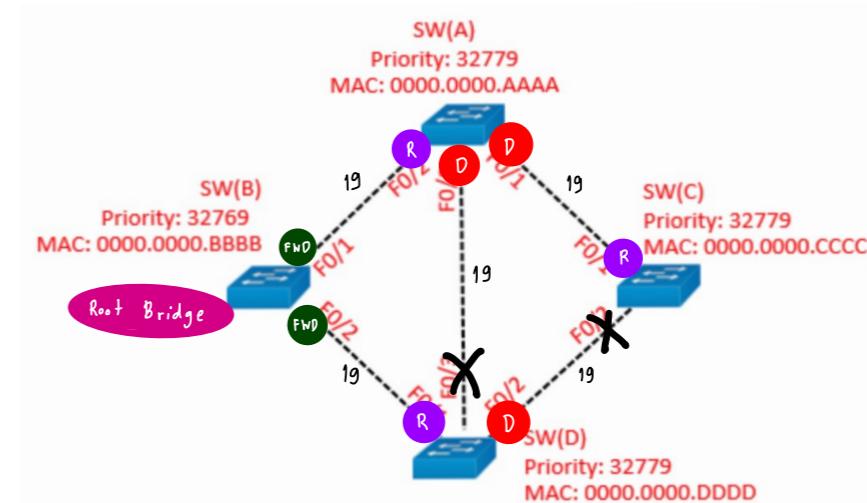
4. Remaining links choose a Designated Port (each LAN segment)



5. All other ports are put into a Blocking state



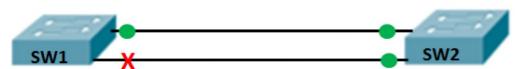
หมายเหตุ



EtherChannel

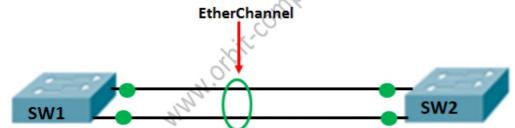
- เป็นสิ่งที่เพิ่มประสิทธิภาพให้ spanning tree

How EtherChannel Works.



Spanning Tree blocks one redundant port link to prevent loops.

- ตัวอย่างจาก spanning tree
- SW1 ต่อ กับ SW2 มีนกานเกิด loop จึงมีการทำ spanning tree (block port)
- ซึ่งมันทำให้ ถ้าเมื่อเวลาจะเลี้ยง 2 link แต่ว่ามีความสามารถใช้ได้ link เดียว
- ข้อดี : ป้องกัน loop
- ข้อเสีย : performance ลดลง



EtherChannel allows spanning-tree to treat the two physical links as one logical port and enabling both ports to operate in full forwarding mode.

- การทำ EtherChannel เราสามารถทำให้ 2 physical link (ที่เรียกว่า link ก็ได้ที่เป็นแลบคู่) รวมเป็น 1 logical link ได้ โดยสามารถกัน loop ได้โดยไม่ต้องใช้ spanning tree
- เป็นการรวมกลุ่ม link
- ช่วยให้เรื่อง load balancing
- ข้อดี : เพิ่ม load balancing และไม่ต้องใช้ spanning tree ที่ป้องกัน loop ได้

Cisco's version is called Port Aggregation

PAgP

- Cisco's version is called Port Aggregation Protocol (PAgP)

Mode:

- Desirable: actively ask if the other side can/will
- Auto: passively wait for other side to ask
- Off: EtherChannel not configured on interface

มาตรฐาน IEEE 802.3ad standard

- IEEE 802.3ad standard is called Link Aggregation Control Protocol (LACP)

LACP

Mode:

- Active: actively ask if the other side can/will
- Passive: passively wait for other side to ask
- Off: EtherChannel not configured on interface

523353 Computer Networks

Lecture 5 : Network Layer - Part 1

Network layer

- internetwork ใช้ router เพื่อเชื่อมต่อรัน LAN ที่ๆ นา
- ถ้าเป็น WAN มีคือการที่เป็น link ระหว่าง routers หลายๆ ตัว

Two key network-layer functions

Network-layer functions:

- forwarding : เคลื่อนย้าย packets จาก router's input ไปยัง router's output ที่เหมาะสม จะมีตาราง route บอกว่าจะส่งไปยัง output ไหน
- routing : กำหนดเส้นทางที่ผ่านจาก src ไปพิ้ง destination เป็นการสร้างตาราง route \rightarrow dynamic routing routing algorithm (dynamic routing)

Analogy: taking a trip

- forwarding : กระบวนการผ่านช่องทางเดียว เช่นทางแยกเลี้ยวซ้ายขวา
- routing : process จาก planning trip ตั้งแต่ src ไปยัง destination เช่นการปักหมุด map จากต้นทางไปยังปลายทาง

* routing คือการสร้าง table ขึ้นมา

* forwarding คือการทำตามตัว table ที่ถูกสร้างขึ้นมา

Network layer: data plane, control plane

- router สามารถแยก โดยอิงจากการทำงาน

1. Data plane :

- อิงตาม forwarding, มองเป็น data packet ดูว่า input ที่เข้ามายัง port ไหน

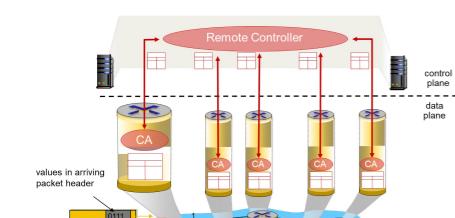
2. Control plane :

- มอง signaling
router และเปลี่ยนเส้นทางกัน ก็ได้ตาราง

Per-router control plane

- ส่วนประกอบของ routing algorithm ของแต่ละ router

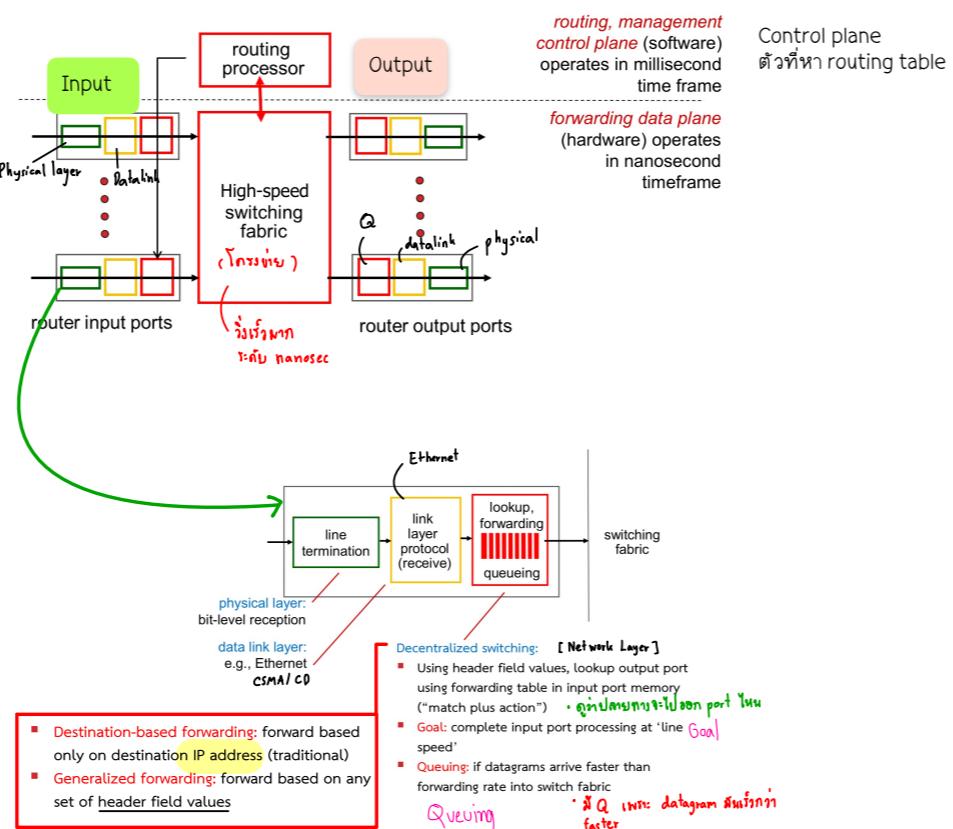
Logically centralized control plane



Router

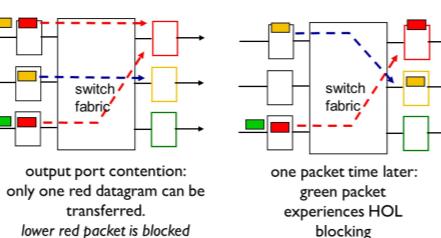
Router architecture overview

- นี่คือ สถาปัตยกรรมของ Router



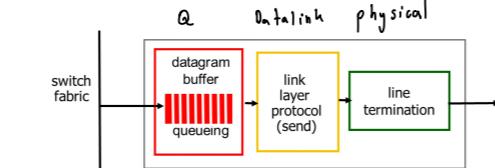
Input port queuing

- ถ้าโครงข่ายต้องการมีช่องกว้างข้อมูลที่เข้ามายัง input มันจะมีการเก็บเอาไว้ใน queue
- ถ้าคิวเต็ม มันทำให้เกิดการ delay หรือ lost ได้ (ล้วนใหญ่เกิดที่ buffer)
- head of line (hol) blocking : ถ้าจราจรปูกันลง packet แล้วจะออกไป output ที่ว่างซึ่งไม่ได้ เพราะต้องรอ packet ลีดเดนออกไปก่อน

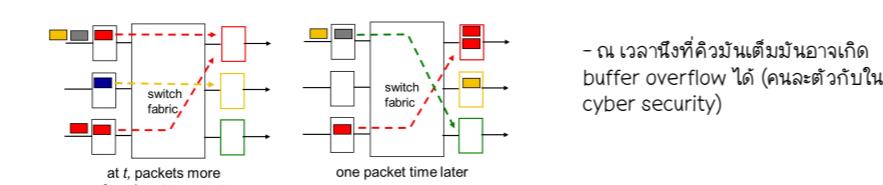


Output ports

- Buffering : จะเกิดการเติมเมื่อ fabric บริการได้เร็วกว่าการส่งออกไปข้างนอก ทำให้อาจเกิดการ delay, lost ได้
- Scheduling : ข้อนี้ง่าย สำหรับเรื่องการจัดการการนำส่ง packet เช่น Priority Scheduling - ถ้าคิวเต็ม จะส่ง packet ไปยัง performance ที่ดีกว่า



Output port queueing



How much buffering?

- ในมาตรฐาน RFC 3439 มีหลักการคำนวณขนาดของ buffer ที่ควรจะมีโดย

ให้ C เป็น link capacity (ความเร็วของ link)
RTT เวลาในการปักลับ 1 รอบ (ปกติที่ 250 ms)

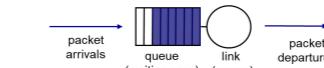
E.g. C = 10 Gbps link: 2.5 Gbit buffer
 $B = RTT * C$
 $2.5 \text{ Gbit} = 10 \text{ Gbps} * 250 \text{ ms}$

- ในความเป็นจริง ระบบอินเทอร์เน็ตปัจจุบัน การใช้งานมันไม่ได้เป็น flow เดียว โดยมีจังหวะ connection มากขึ้น connection ต่อๆ กัน

$$\frac{RTT * C}{\sqrt{N}}$$

Scheduling mechanisms

- scheduling มีวิธีการจัดการอย่างไร หาก buffer เต็ม
- หาก buffer เต็ม scheduling จะมีบทบาทสำคัญมาก โดยมีจะจัดการโดย FIFO (first in first out)
- โดยทั่วไปจะมี 3 นโยบาย
 1. Tail drop : หาก packet ที่เรามีมาแล้วล่วงหน้าไปกว่า buffer ที่เราตั้งไว้ ให้丢弃
 2. Priority : หากมี packet ที่มี priority สูงข้าม packet ใหม่ที่มี priority ต่ำกว่าที่จะถูก drop ที่นั่น
 3. Random : หากมี packet ใหม่ข้าม จะมีการ Random packet เก่าที่ drop ที่นั่นไป

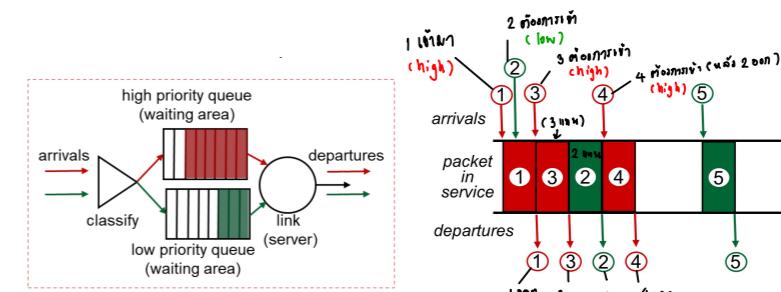


ซึ่งจริงๆ แล้ว Scheduling เนี่ย มันไม่ได้มีแค่ FIFO

มันมี...

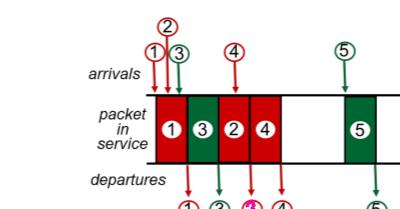
1. Priority Scheduling

- คือ วิธีการเลือกว่า packet ไหนที่เข้ามา ใคร high priority ใคร low priority และมันก็จะมีการจับแยกสองคิว
- แล้วก่อนจะ output มันจะต้องตัดสินใจอยู่ที่ตัวเอง
- การส่ง output ออกจากตัวที่ high priority ออกก่อนแล้ว
- ถ้าในคิวมี high อยู่ ต้องเอา high ออกก่อนให้หมดก่อน low ถึงเข้าได้



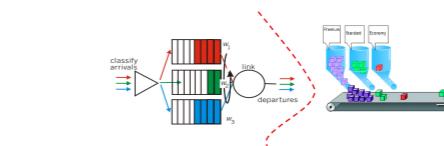
2. Round Robin (RR) Scheduling

- ไม่ได้แบ่งตาม priority แต่มีการแบ่ง class
- เป็นการแบ่ง class ที่มีการผลัดกันทำ โดยจะทำ class สูงแล้วล็อกเป็น class ต่อไปทำ class ต่อไป



3. Weighted Fair Queuing (WFQ)

- หลักการมันคือ RR แต่มีการ weight หรือปรับขนาดหัวให้ใหญ่ไปเท่านั้น
- เพื่อให้คนที่มี packet แพ๊คฯ ใช้งานได้มีประสิทธิภาพมากกว่า
- ผุดง่ายๆ คือมีการผลัดกันทำ แต่พอถึงคราวของ พรีเมียม จะมีการส่ง packet ออกได้มากกว่า



Destination-based forwarding

| forwarding table | | Link Interface |
|---|-------------------------------|----------------|
| Destination Address Range | | |
| 11001000 00010111 00010000 00000000 | through 10.0.1.0 - 10.0.1.255 | 0 |
| 11001000 00010111 00011000 00000000 | through 10.0.1.0 - 10.0.1.255 | 1 |
| 11001000 00010111 00011000 00000000 | through 10.0.1.0 - 10.0.1.255 | 2 |
| otherwise | | 3 |
| 11001000 00010111 00010000 00000000 = 200.23.16.0 | | |
| 11001000 00010111 00011000 00000000 = 200.23.24.0 | | |

- routing table หรือ forwarding table มั่น哪ได้อย่างไรว่า ip นี้ต้องไปทางไหน?
- มั่น哪จะป้อนตารางแล้วก็ port มั่น

Longest prefix matching

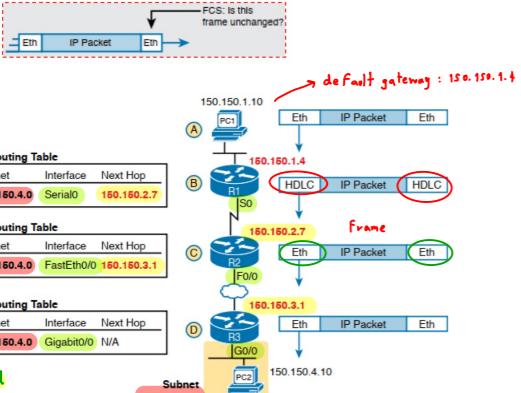
- คือวิธีการ map ของ router
- เป็นเหตุการณ์ที่เก็บ prefix ที่จำนวนเลข bit เห็นอกมากที่สุด
- prefix คือ network address ลักษณะ bit ด้วย subnet mask

| Prefix | Link interface |
|----------------------------------|----------------|
| 11001000 00010111 00010000 ***** | 0 |
| 11001000 00010111 00011000 ***** | 1 |
| 11001000 00010111 00011000 ***** | 2 |
| Otherwise = ? | 3 |

examples:
DA: 11001000 00010111 00010000 10100001 which interface?
DA: 11001000 00010111 00011000 10101010 which interface?
DA: 11001000 00010111 00011000 10101111 1

Sending IP datagrams

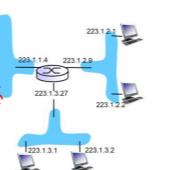
- เมื่อรouter จะมี routing table ที่บอก subnet, interface, nexthop



ยกตัวอย่าง หาก PC1 ต้องการส่งไปหา PC2 จะเกิดกระบวนการใดบ้าง

Example 1

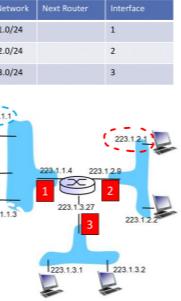
Source : 223.1.1.1 /24
Destination : 223.1.1.3 /24



- จากโจทย์จะเห็นได้ว่า /24 ซึ่งล็อก 3 วรรคแรกเหมือนกัน มั่นคือ same subnet (same vlan)
แล้วว่าไม่ได้ผ่าน router
อยู่ใน Ethernet frame เดียวกัน
ใช้ ARP table

Example 2

Source : 223.1.1.1 /24
Destination : 223.1.2.1 /24



- จากโจทย์ เป็นการล็อกชั้น vlan (อยู่คนละ subnet) แสดงว่าต้องพึ่ง network layer หรือต้องผ่าน router
- 1. PC จะมองหา default gateway ว่าจะไปไหน [1]
- 2. router จะ check ปลายทาง แล้วมองมาที่ table ของมั่น ซึ่งจะเห็นว่าตรงกับออกที่ interface 2 มากที่สุด

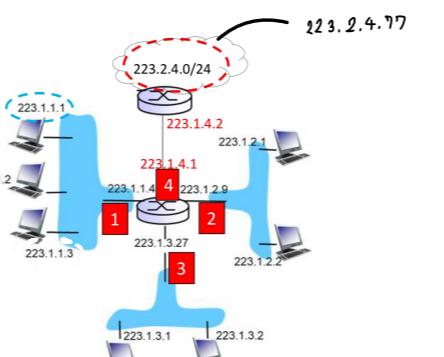
| Dest. Network | Next Router | Interface |
|---------------|-------------|-----------|
| 223.1.1.0/24 | | 1 |
| 223.1.2.0/24 | 2 | |
| 223.1.3.0/24 | | 3 |

3. เนื่องจาก router ต้องกับ interface 2 โดยตรง Next hop จึงเป็น N/A (ไม่มีต้อง Lis)

| Dest. Network | Next Router | Interface |
|---------------|-------------|-----------|
| 223.1.1.0/24 | | 1 |
| 223.1.2.0/24 | N/A | 2 |
| 223.1.3.0/24 | | 3 |

Example 3

Source : 223.1.1.1 /24
Destination : 223.2.4.77 /24



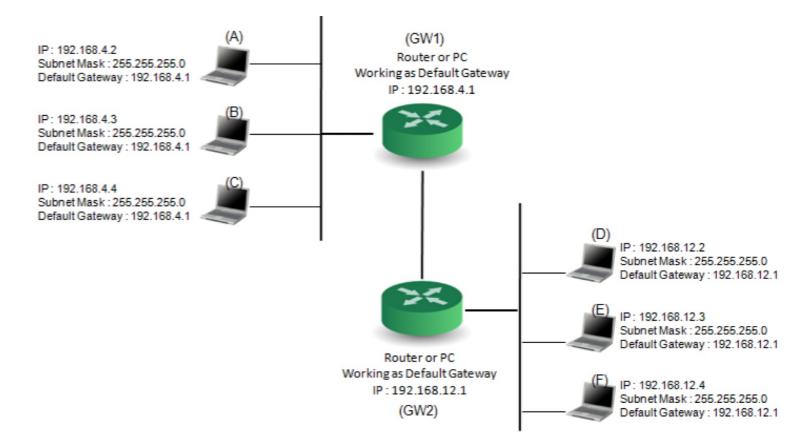
- จากโจทย์จะเห็นได้ว่าปลายทางอยู่คนละ router เลย
- 1. Set ตัวที่มั่นไม่ไว้เดียว ให้ไปที่ default gateway [1] = เป็นประตูด้านใน คือ 223.1.1.4
- 2. จะมาที่ router ซึ่งมีการ set ตาราง routing table ไว้ โดยเราจะเอาปลายทางมาเทียบกับ prefix ภายใน table ว่าใกล้เคียงตัวไหนมากที่สุด
- 3. พบร่วมกันตัวที่มากที่สุด จึงให้ next hop เป็นประตูที่ไปยัง interface ที่เราต้องการ

| Dest. Network | Next Router | Interface |
|---------------|-------------|-----------|
| 223.1.1.0/24 | | 1 |
| 223.1.2.0/24 | 2 | |
| 223.1.3.0/24 | 3 | |
| 223.1.4.0/24 | 4 | |
| 223.2.4.0/24 | 223.1.4.2 | 4 |

* ลังที่ packet ส่งออกมั่นไม่ได้ลงว่า router ปลายทางคืออะไร แต่มั่นลงว่ามั่นที่ต้องกับ link มั่น มั่นจึงเกิดการตัดจัม packet ที่ link ได้ แสดงว่าแค่ set int ถูก แต่ไม่ set next hop ยังไงเดย

Default gateway

- default route ต้องเป็นอะไรที่อยู่ใน LAN เดียวกัน ที่เรามองเห็น
- มั่นคือประตูที่เราสองเห็นที่เป็นทางออก
- มีไว้เพื่อ จัดการเรื่องรุ่งไปทางไหน มั่นจะอ่านมาทาง default gateway
- หรือถ้าไม่ใช่ชื่อรุ่น ให้เลือกตัวที่อยู่ใน subnet เดียวกัน



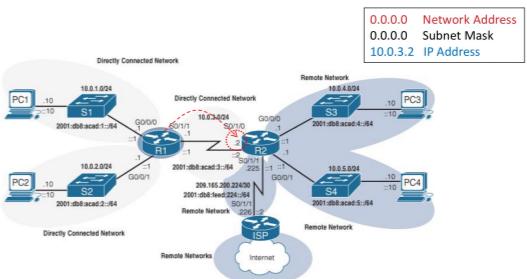
Default Route

- ในชั้นของ router เราก็สามารถเช็คได้
- โดยเปลี่ยนจาก gateway เป็น route
- หลักการคือ หากเราไม่สามารถใช้ longest matching ได้ (ไม่มี idea สำหรับปลายทาง) มั่นจะไปที่ default route

ยกตัวอย่าง

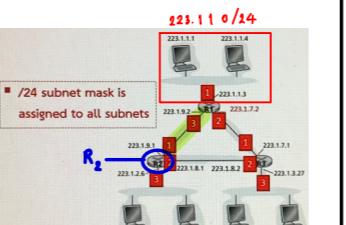
ต้องการให้ default route ของ router R1 ไปยังที่เราสองกลุ่มด้านขวา ทำได้โดย

R1(config) # ip route 0.0.0.0 0.0.0.0 10.0.3.2



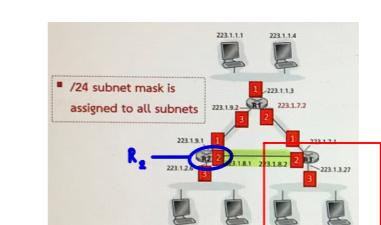
Example

Routing Table ที่ [R2] ถ้าต้องการไป 223.1.1.0 /24 จะมี Next Router และ Interface คือ?



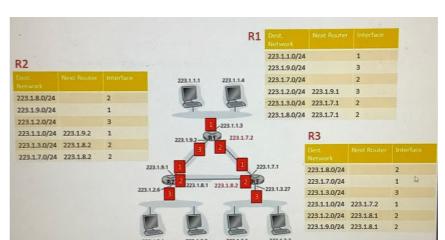
- Next Router : 223.1.9.2 (มั่นที่เดียว)
- Interface : 1 (มั่นที่เดียว)

Routing Table ที่ [R2] ถ้าต้องการไป 223.1.3.0 /24 จะมี Next Router และ Interface คือ?



- Next Router : 223.1.8.2 (มั่นที่เดียว)
- Interface : 2 (มั่นที่เดียว)

Routing Table ที่ [R1] ถ้าต้องการไป 223.1.8.0 /24 จะมี Next Router และ Interface คือ?

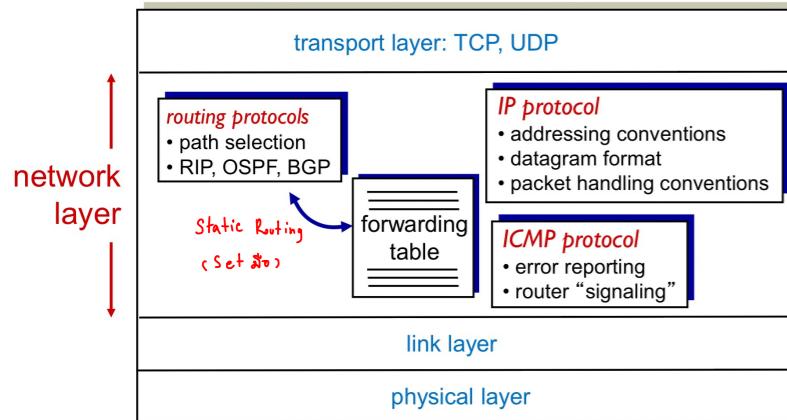


- ต้องมาได้ 2 กะ
- ทางเดียว : • Next Router : 223.1.9.1
- Interface : 3

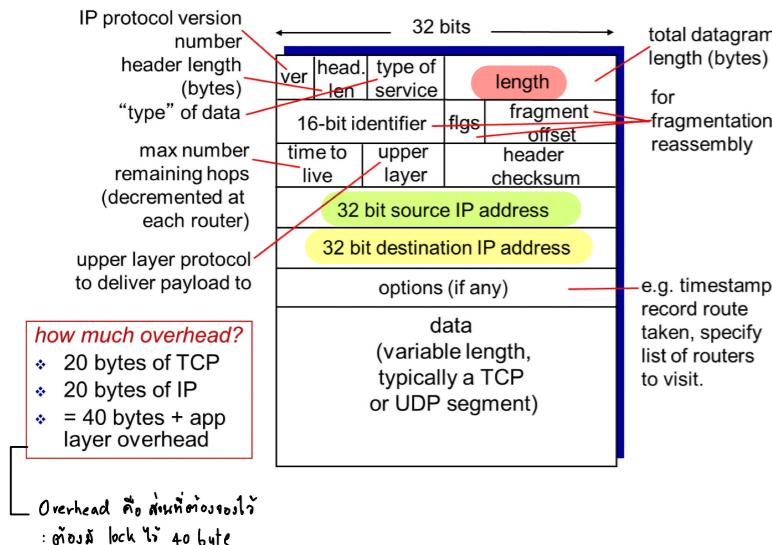
- ทางเดียว : • Next Router: 223.1.7.1
- Interface : 2

IP (Internet Protocol)

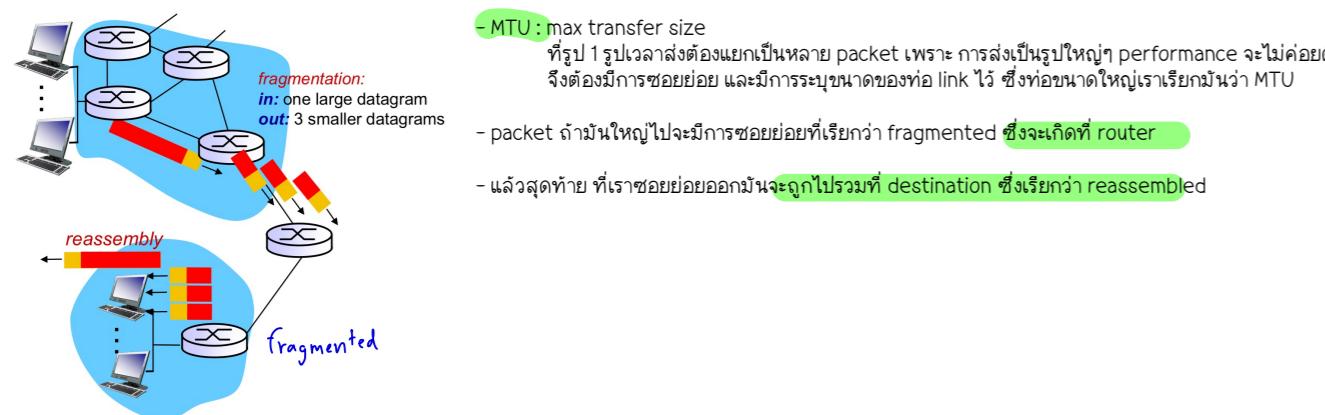
The Internet network layer



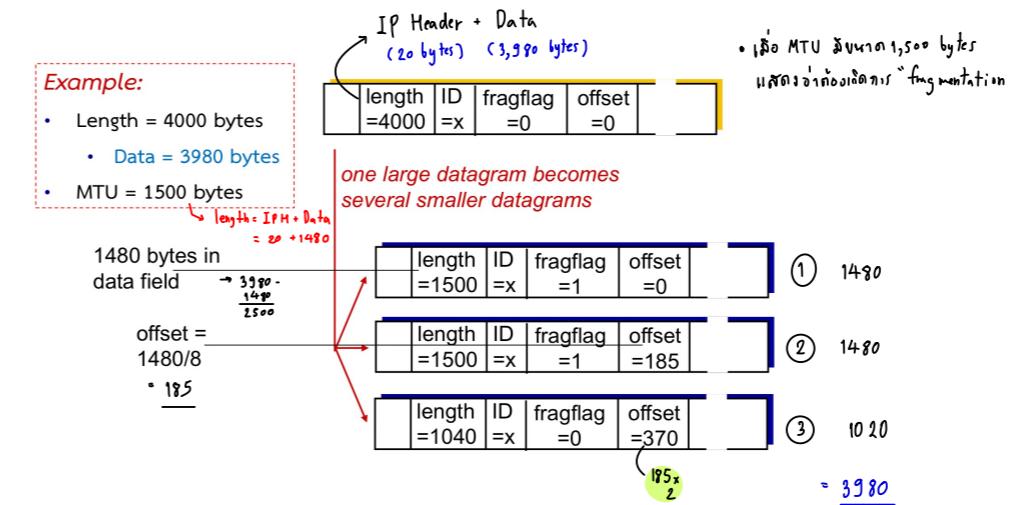
IP Datagram format



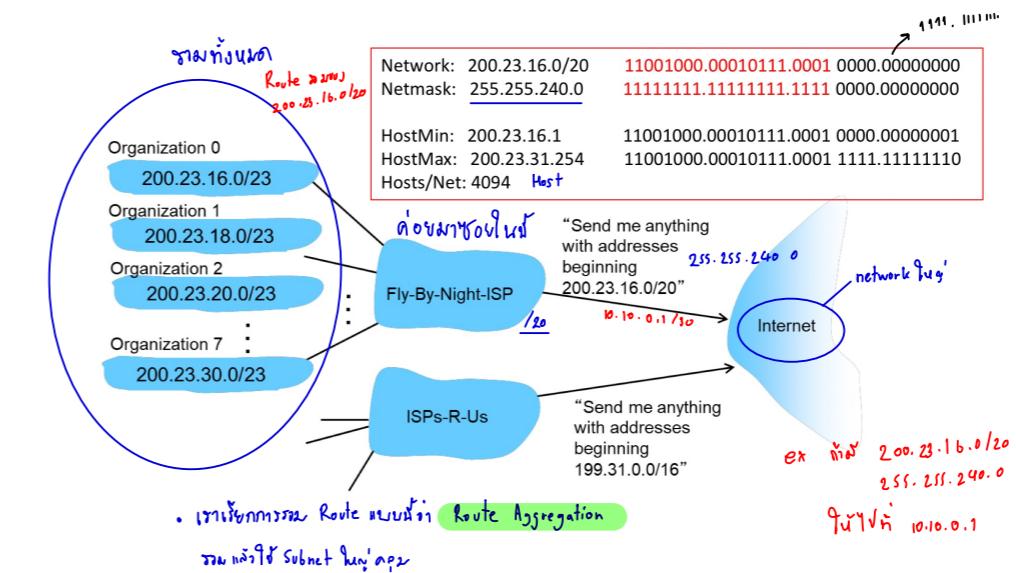
IP Fragmentation, reassembly



การคำนวณ fragmentation

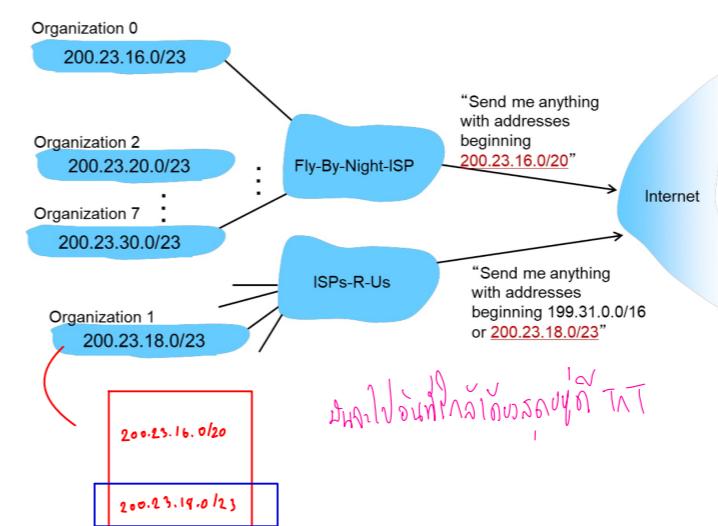


Hierarchical addressing : route aggregation



More specific routes

- ถ้าใช้ในทุกรอบวนการ
ต้องมีการรวม route ก็จะมีการดู longest prefix matching เมื่อเวลาเดิม



Lecture เสธ.ใน

Network Design Fundamentals

- ฟื้นฐานของการ design network ที่ดี ว่าควรเป็นอย่างไร

Introduction

Type of networks

LAN (Local Area Network)

MAN (Metropolitan Area Network)

WAN (Wide Area Network)

Ethernet standards

| Speed | Common Name | Informal IEEE Standard Name | Formal IEEE Standard Name | Cable Type, Maximum Length |
|-----------|------------------|-----------------------------|---------------------------|----------------------------|
| 10 Mbps | Ethernet | 10BASE-T | 802.3 | Copper, 100 m |
| 100 Mbps | Fast Ethernet | 100BASE-T | 802.3u | Copper, 100 m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-LX | 802.3z | Fiber, 5000 m |
| 1000 Mbps | Gigabit Ethernet | 1000BASE-T | 802.3ab | Copper, 100 m |
| 10 Gbps | 10 Gig Ethernet | 10GBASE-T | 802.3an | Copper, 100 m |

• T : สีน้ำเงิน copper
• LX: สีฟ้า fiber-optic
• lab เรียบเรียง

Wireless Standard

| Amendment | 2.4 GHz | 5 GHz | Max Data Rate | Notes |
|-------------|---------|-------|---------------|---|
| 802.11-1997 | Yes | No | 2 Mbps | The original 802.11 standard ratified in 1997 |
| 802.11b | Yes | No | 11 Mbps | Introduced in 1999 |
| 802.11g | Yes | No | 54 Mbps | Introduced in 2003 |
| 802.11a | No | Yes | 54 Mbps | Introduced in 1999 |
| 802.11n | Yes | Yes | 600 Mbps | HT (high throughput), introduced in 2009 |
| 802.11ac | No | Yes | 6.93 Gbps | VHT (very high throughput), introduced in 2013 |
| 802.11ax | Yes | Yes | 4x 802.11ac | High Efficiency Wireless, Wi-Fi6; expected late 2019; will operate on other bands too, as they become available |

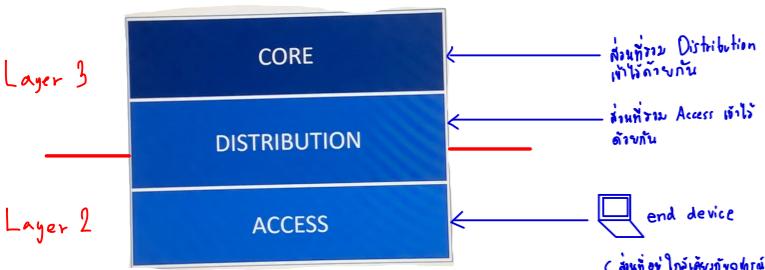
Great features of the network

- High speed
 - Low cost
 - Cost Efficiency
 - Great Security
 - Availability (Can be use the network)
 - Scalability
 - Reliability (Strong network)
 - Topology **
- Wired and wireless
- Device cost (ต้นทุน device)
- Great Security (มั่นคงต้องการป้องกัน)
- Availability (ใช้งานได้)
- Scalability (เพิ่ม ลดงบประมาณได้ / รองรับเพิ่ม device ใหม่ได้)
- Reliability (Strong network) (ต้องมี High speed และ Scalability)
- Topology ** (กារออกแบบโครงสร้าง network)

Best practice of network topology

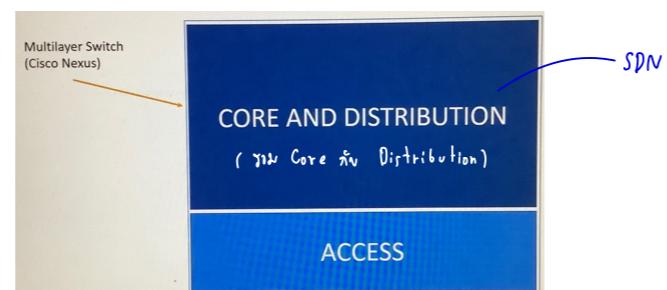
- ที่ทัวโลกใช้ในปัจจุบัน คือการทำงานแบบ hierarchy (แยกชั้น)

แบบที่ 1



แบบที่ 2

(ចំណាំសង្គម ទីផ្សារ)



There is no right or wrong - ไม่มีอะไรถูกอะไรผิด มันมีแต่ส่าວច្ចាវិក់ហេរាមសមាគមនខ្លះ

Everything is 'Ideal' - គុណយោងមានយូវឱ្យឲ្យអុដមកតិ

Start

Company A

• Requirements

- บริษัท A มีจำนวนพนักงานทั้งหมด 150 คน มีจำนวนอาคารอยู่ 2 อาคาร อาคารที่ 1 มี 1 ชั้น อาคารที่ 2 มี 2 ชั้น บริษัท A เป็นบริษัทเปิดใหม่ที่ต้องการระบบเครือข่ายที่มีความปลอดภัยภายในองค์กร ณ ปัจจุบัน บริษัท A ได้เข้าบริการอินเทอร์เน็ตจากผู้ให้บริการมา 2 ผู้ให้บริการ โดยเข้าจากผู้ให้บริการละ 1 เส้น เพื่อการใช้งานอินเทอร์เน็ตที่ต่อเนื่อง บริษัท A จึงต้องการให้จัดสรรงานที่เวิร์กภาระในองค์กรให้สามารถใช้งานได้และใช้งานอินเทอร์เน็ตเพียงแค่สายเท่านั้น เส้นที่เหลือไว้ Backup ในแต่ละชั้นจะมี Switch ชั้นละ 1 ตัว โดยเน็ตเวิร์กจะต้องแยก Subnet ระหว่างชั้นและสามารถใช้งานได้ต่อเนื่องถ้ามีพนักงานเพิ่ม

- ตรวจสอบ issues จาก requirements

• Issues

- Internet 2 ISP
- There are 2 buildings
- Building 1 has 1 floor
- Building 2 has 2 floors
- Need a security system
- the requirement of minimum 150 hosts per subnet (152 IP addresses)
- Need a network isolated (VLANs) ชั้น
- Need a scalability แห่งความต้องการ : ต้องปรับเปลี่ยน
• Wired network only - ไม่สามารถต่อ WiFi

• Resolved

- To Do
 - Planning devices ต้องการ devices គ្នា
 - Network redundancy with the router ពីរ Network គ្នាដែលចងចាំ
 - Insert firewall between internet and secure network ពីរ security
 - 3 Network Isolated (VLANs) នេះគឺ បាន 3 តារាង VLAN
 - IP planning
 - For core network (L3)
 - About 150 hosts and scalable (L2)
- Best practices
 - CORE -> DISTRIBUTION -> ACCESS

Result

Planning

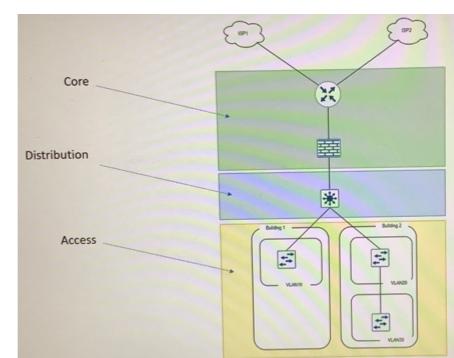
กำหนด IP ของส่วน

- Private-IP planning
 - Core network CIDR
 - 172.16.1.0/29
 - About 150 people and scalability
 - Subnet must more than 152 hosts (150 + 1 NA + 1 BA)
 - Due to the scalability with CIDR need to provide more appropriate
 - VLANs
 - VLAN10 – 192.168.10.0/24
 - VLAN20 – 192.168.20.0/24
 - VLAN30 – 192.168.30.0/24
- Device planning
 - Router
 - Firewall
 - L3 Switch
 - L2 Switch

1
1
1
3

} Core

Topology



- เป็นลักษณะ network engineering, consult, architect, เข้าใจกัน

Terminology

Public-IP : unicast ip , เป็น ip ที่เราได้มาจาก provider ISP, หรือ ip ที่เป็น global
Private-IP : ip ที่เราสร้างขึ้นมาใช้กันเองในองค์กรของเรา

Site scenario from experience of instructor

