



CPE 426 Computer Networks

Chapter 3:

Review 3: SPT & VLAN

Textbook Chapter 20: Internet Concept

Textbook Chapter 21: IP Address





TOPICS

- **1. Repeater/Bridges**
 - Chapter 17: 17.1-17.6
- **2. SPT**
 - Chapter 17: 17.7-17.8
- **3. VLAN**
 - Chapter 17: 17.9-17.11
- **4. X.25/FR/ATM/MPLS/ISDN**
 - Chapter 19: 19.1-19.4

ALSO Reference From CPE 326 (Stalling Book)

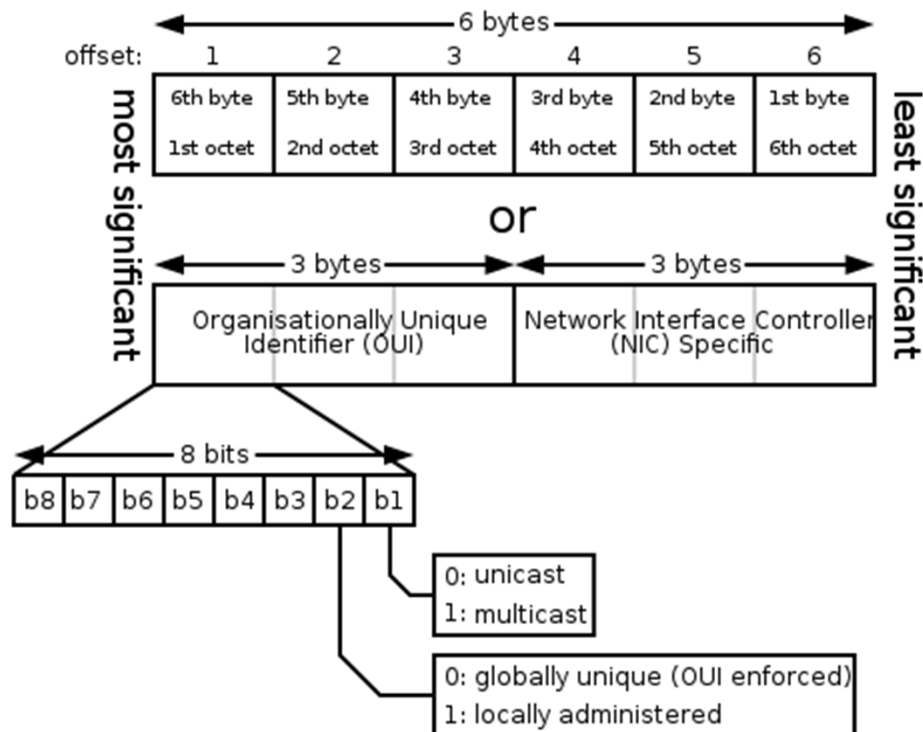
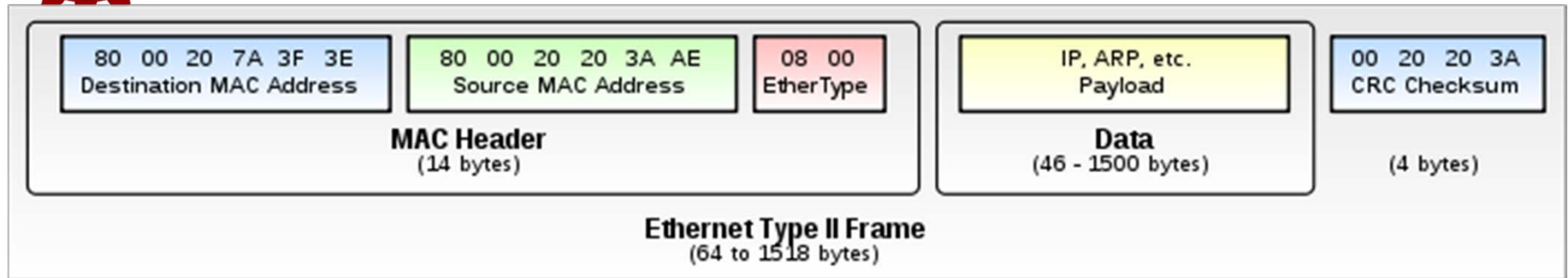


TOPICS

- **BREAK**
- **Chapter 20: Internetworking**
 - Motivation: Sec. 20.1-20.2
 - Concept: Sec. 20.3-20.4
 - Internetworking: Sec. 20.5-20.8
 - Protocol Architecture: Sec. 20.9-20.11
 - Routers: Sec. 20.12
- **Chapter 21: IP Address (Not Finish)**
 - Addressing Scheme/Prefix&Suffix: 21.1-21.8
 - Subnetting and Mask: 21.9-21.13



Ether Type II (DIX Frame)



MAC-48 Address
In Transmission Order

01-23-45-67-89-ab,

01:23:45:67:89:ab,

0123.4567.89ab

802.3/.4 Send LSBit First
(Canonical Format)

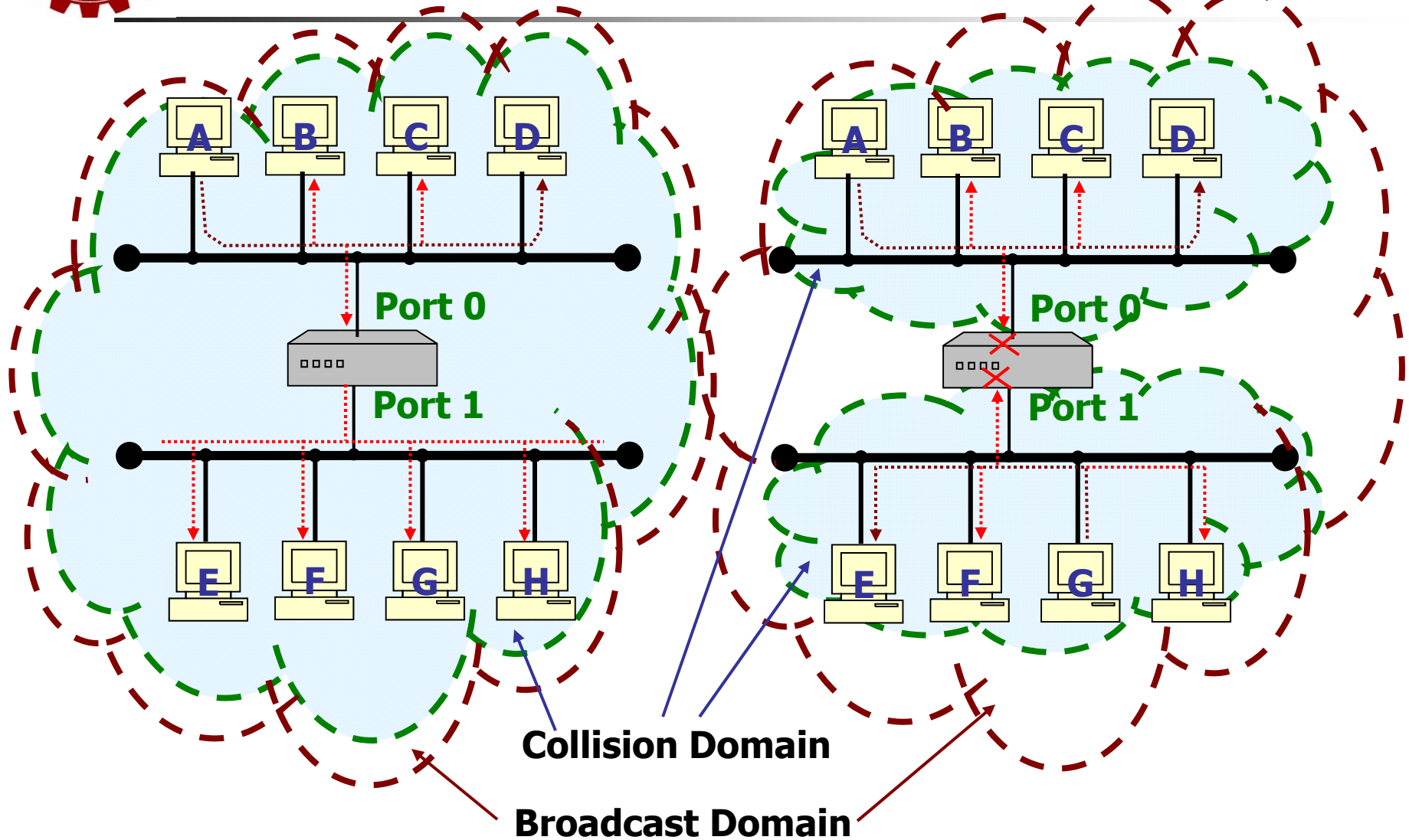
10000000 11000100 10100010 ...

802.5/.6 Send MSBit First
(Bit-Reverse/Non-canonical)

00000001 00100011 01000101 ...

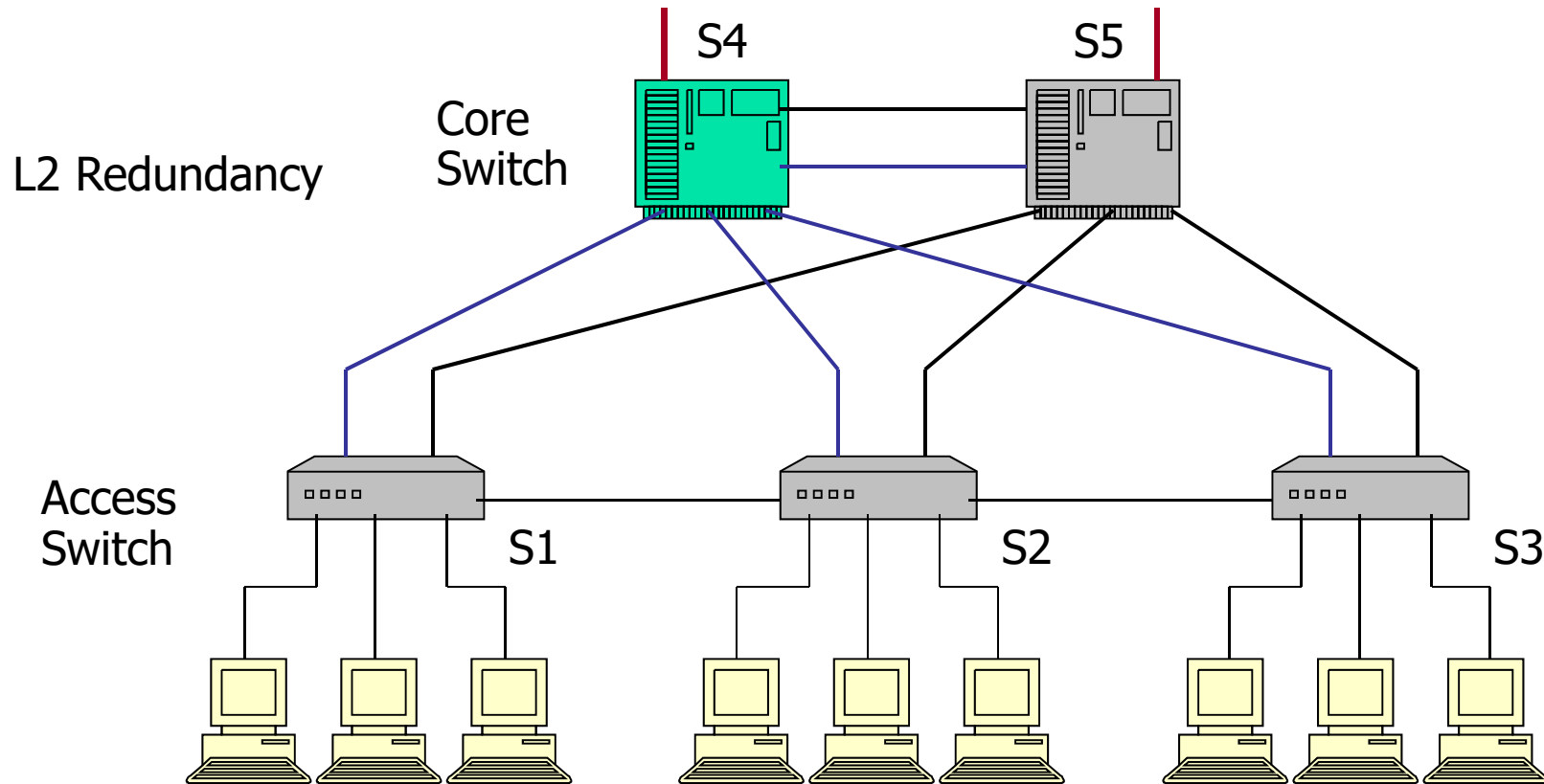


Bridge vs Repeater: Collision Domain vs Broadcast Domain



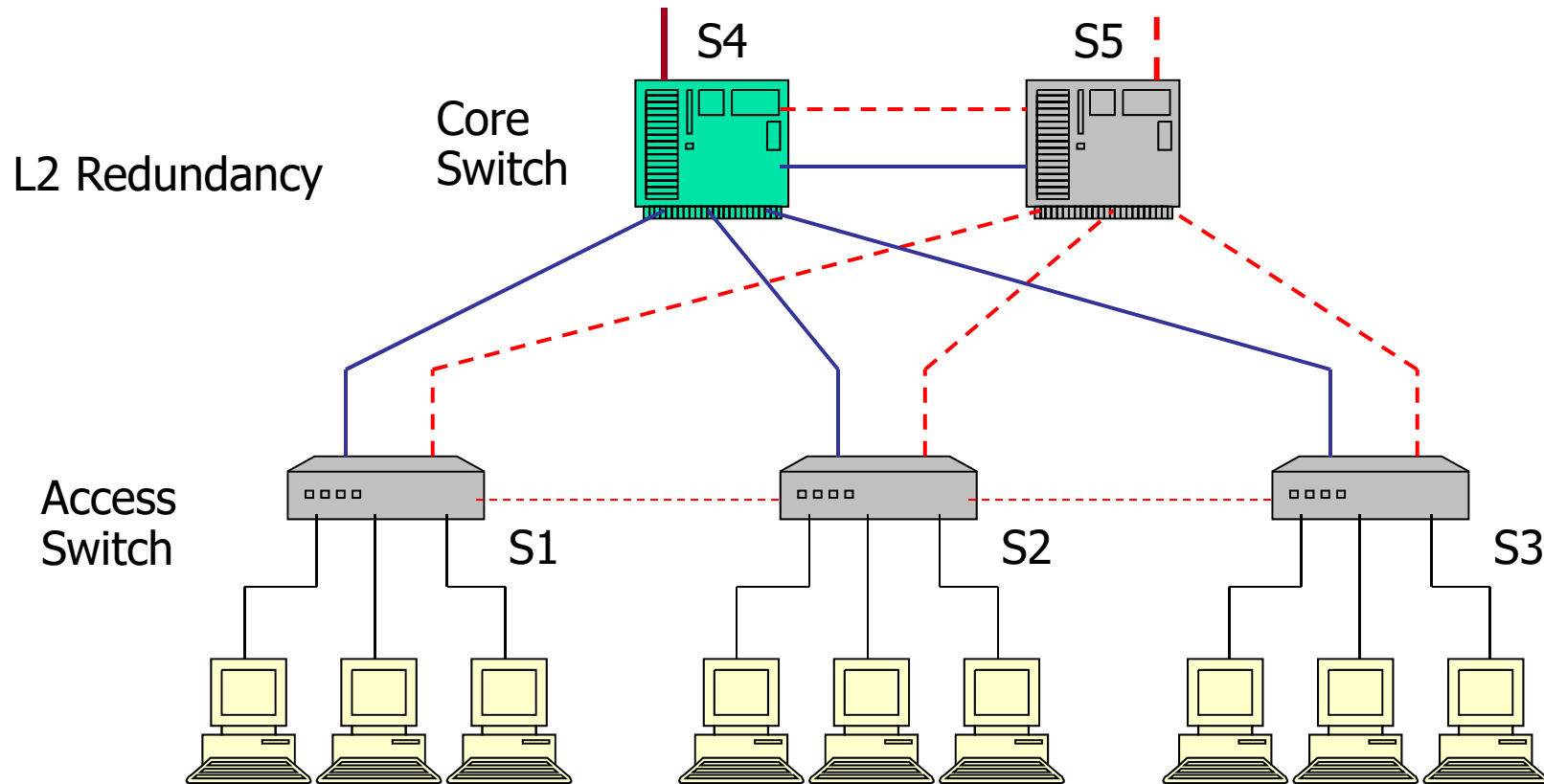


Layer 2 Redundancy: Active Link





Layer 2 Redundancy: SPT





Steps 1: Root Bridge Selection

- เลือก Root Bridge โดยทุก Switch ส่ง BPDUs ออกทุก Port และใส่ค่า Bridge ID
- $\text{Bridge ID} = \text{Bridge Priority (2 Octet)} + \text{MAC Address (6 Octet)}$
- Switch ที่มี Bridge ID ต่ำสุดจะเป็น Root
- Default Bridge Priority = 32768
- ถ้าไม่มีการ Configure ดังนั้น Switch ที่มี MAC Address ต่ำสุดจะได้รับเลือก



Steps 2: Minimum Cost Tree

- สร้าง Minimum Cost Tree โดยจาก Root ส่ง BPDUs ที่มี Cost = 0 ออกทุกๆ Port ที่มันต่อ ซึ่งถูกจัดว่าเป็น Designated Port
- เมื่อ Switch ได้รับ BPDUs มันจะบวกค่า Cost กับ Cost ของ Link ที่เข้ามา และส่งต่อ
- ถ้ามันได้รับมากกว่า 1 BPDUs แสดงว่ามีมากกว่าหนึ่งเส้นทางไปยัง Root (Loop)
- เลือกเส้นทางที่ Cost ต่ำกว่า เป็น **Root Port**
- ถ้ามีมากกว่าหนึ่งเส้นทางและ Cost เท่ากัน เลือก Port ไปยัง Bridge ID ต่ำกว่า
- ถ้ายังเท่ากันเลือก Port Priority ต่ำกว่า



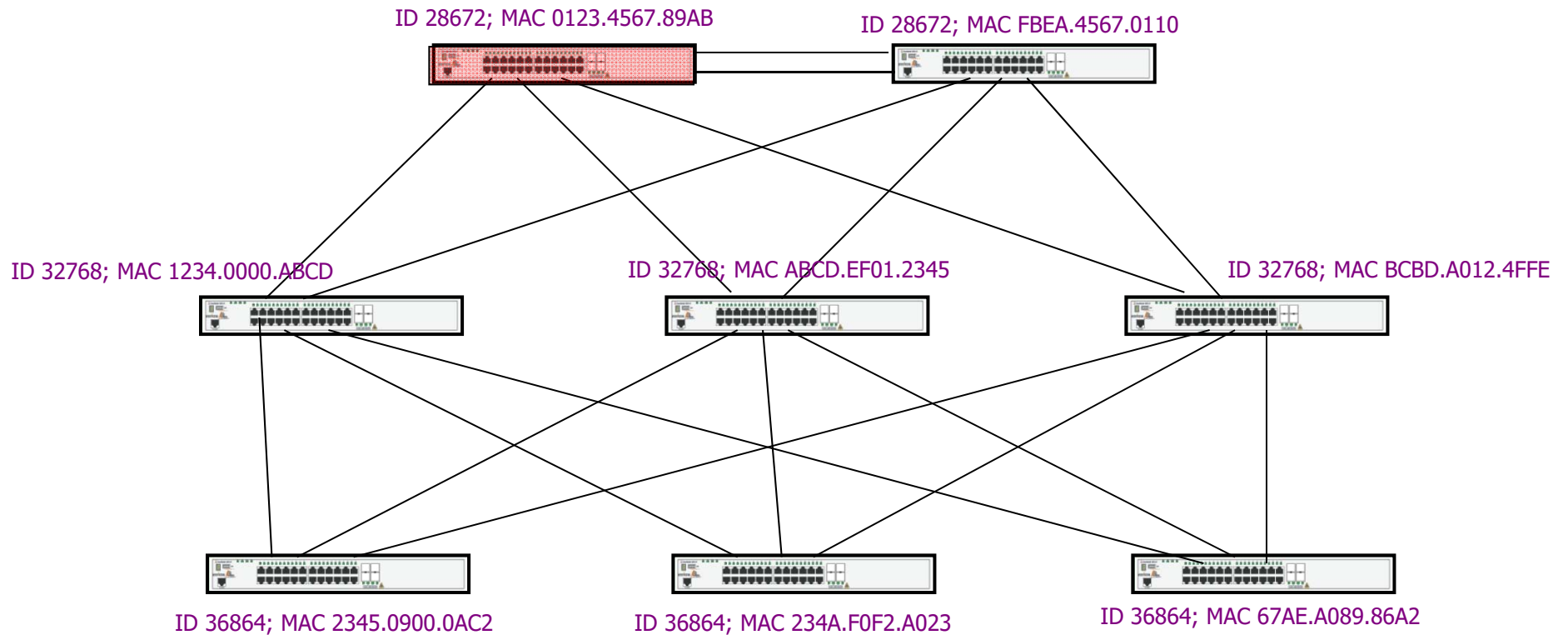
Steps 3: เลือก Designated Port และ Port Blocking

- เส้นทางที่ไม่ได้ถูกเลือกจะถูกปิด
- การปิด ทำโดย Blocking Port
- Port จะถูกปิดด้านเดียว
 - ปิด Port ที่มี Cost สูงกว่าไปยัง Root ถ้าเท่ากัน
 - ปิด Port Switch ที่มี Bridge ID สูงกว่า ถ้าเท่ากัน
 - ปิด Port ที่มี Port ID สูงกว่า
 - $\text{Port ID} = \text{Port Priority (1 Byte, Default = 128)} + \text{Port Number}$
- Port ที่เปิดเรียก Designated Port



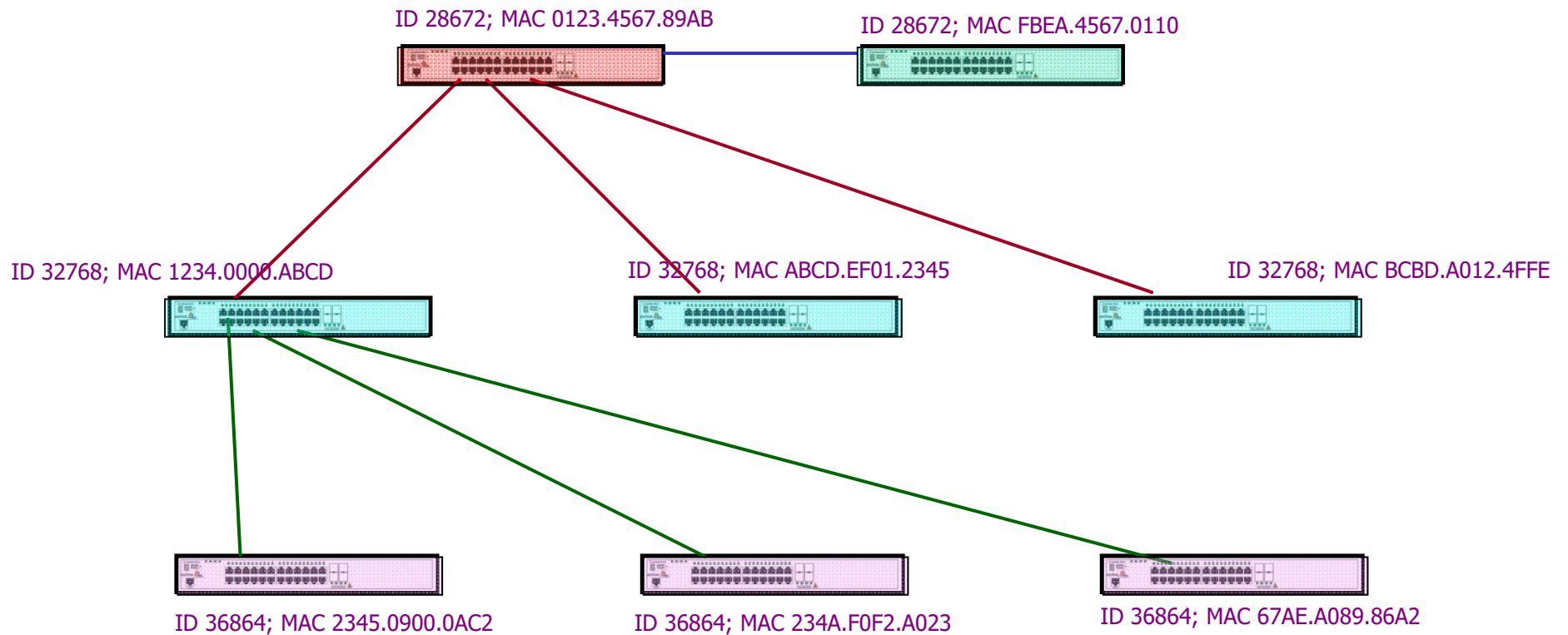
Order of Precedence

เลือก Root Bridge





Order of Precedence





VLAN

- แยก Broadcast Domain ออกจากใน Switch ตัวเดียว
- L2 Protocol
- เหมือนกับมีหลาย Switch ที่ไม่เชื่อมต่อกันในตัวเดียว
- สามารถทำการ Configure ได้ว่าจะแยกอย่างไร
 - VLAN by Port (Static) กำหนดแต่ละ Port ตายตัวว่าเป็นของ VLAN อะไร
 - Dynamic VLAN : ตาม MAC, IP, Protocol หรืออื่นๆ กรณีนี้แต่ละ Port จะเปลี่ยน VLAN ตาม Condition ที่กำหนด เราเรียกว่าเป็น Mobile Port



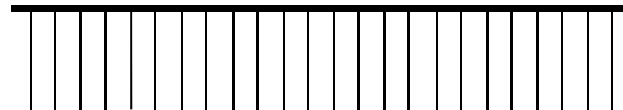
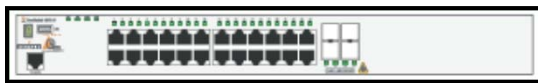
VLAN

- **VLAN 1 คือ Default VLAN ลบและสร้างไม่ได้**
- **ทุก Port ถ้าไม่มีการกำหนดจะอยู่ใน VLAN 1**
- **VLAN Number = 12 Bit แต่ปกติการสร้าง จะให้หมายเลขระหว่าง VLAN 2 – VLAN 4094**
- **การเชื่อมต่อสอง VLAN ด้วยกันต้องใช้ความสามารถของ L3**
- **VLAN สามารถแยก Physical NW ออกจาก Logical NW**

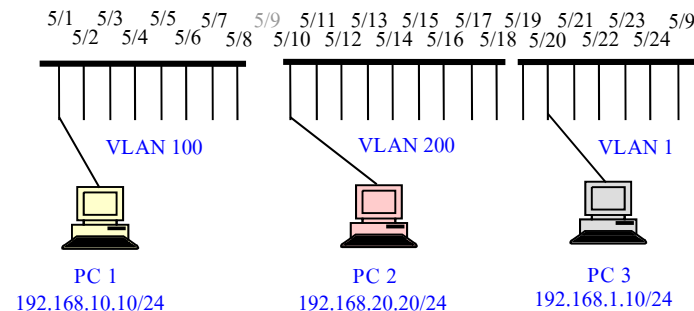
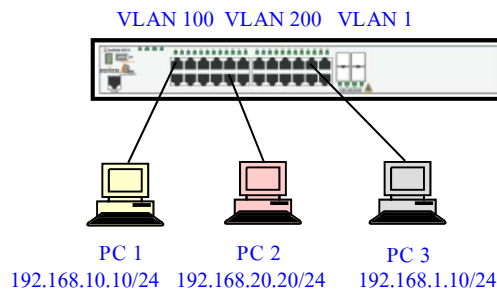


VLAN แบ่ง Switch เป็นหลายส่วน

Switch ปกติเมื่อไม่แบ่ง VLAN หรือไม่ใช่ Managed Switch



Switch ตัวเดียว ถูกแบ่งเป็น 3 VLAN

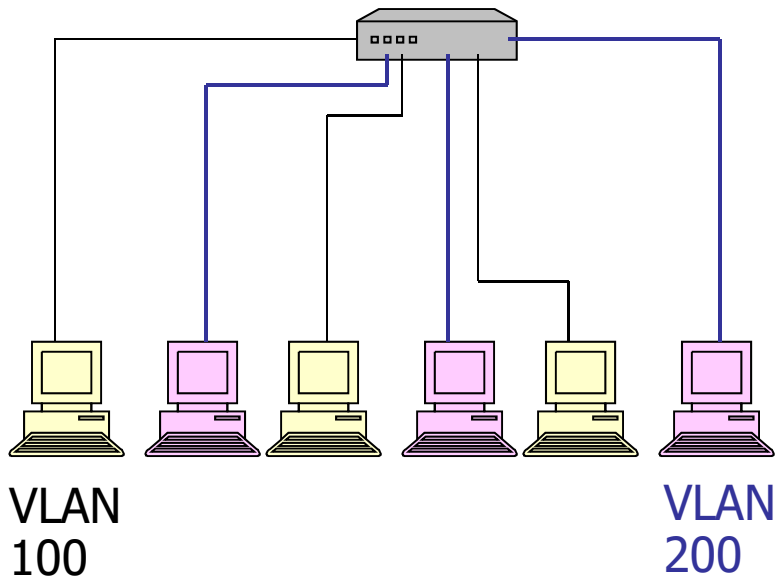


แต่ละ VLAN ถูกแยกออกจากกัน เสมือนอยู่คนละ Switch
จัดว่าอยู่คนละ Sub-network/Broadcast Domain
ต้องใช้อุปกรณ์ Layer 3(Router) มาเชื่อมต่อ

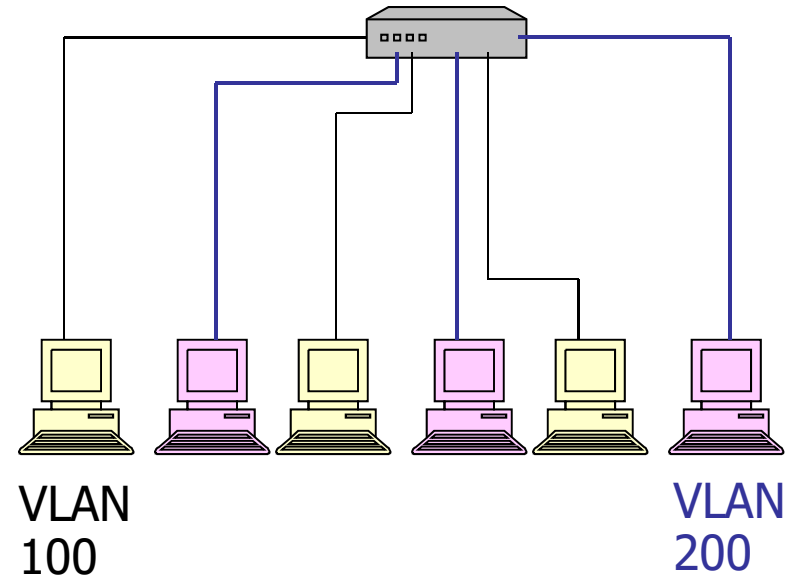


VLAN สามารถขยายผ่านมากกว่า 1 Switch

Room 1

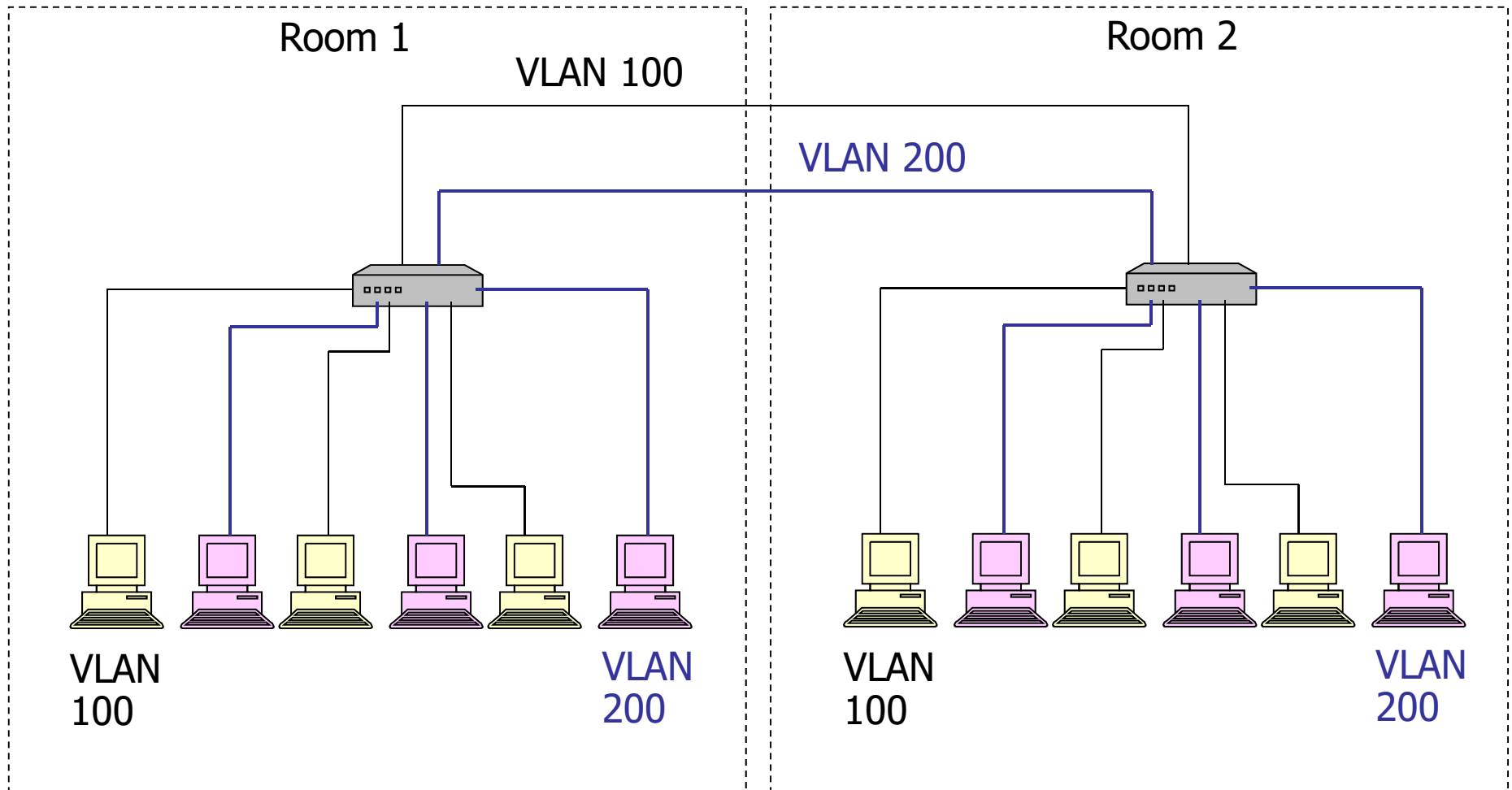


Room 2



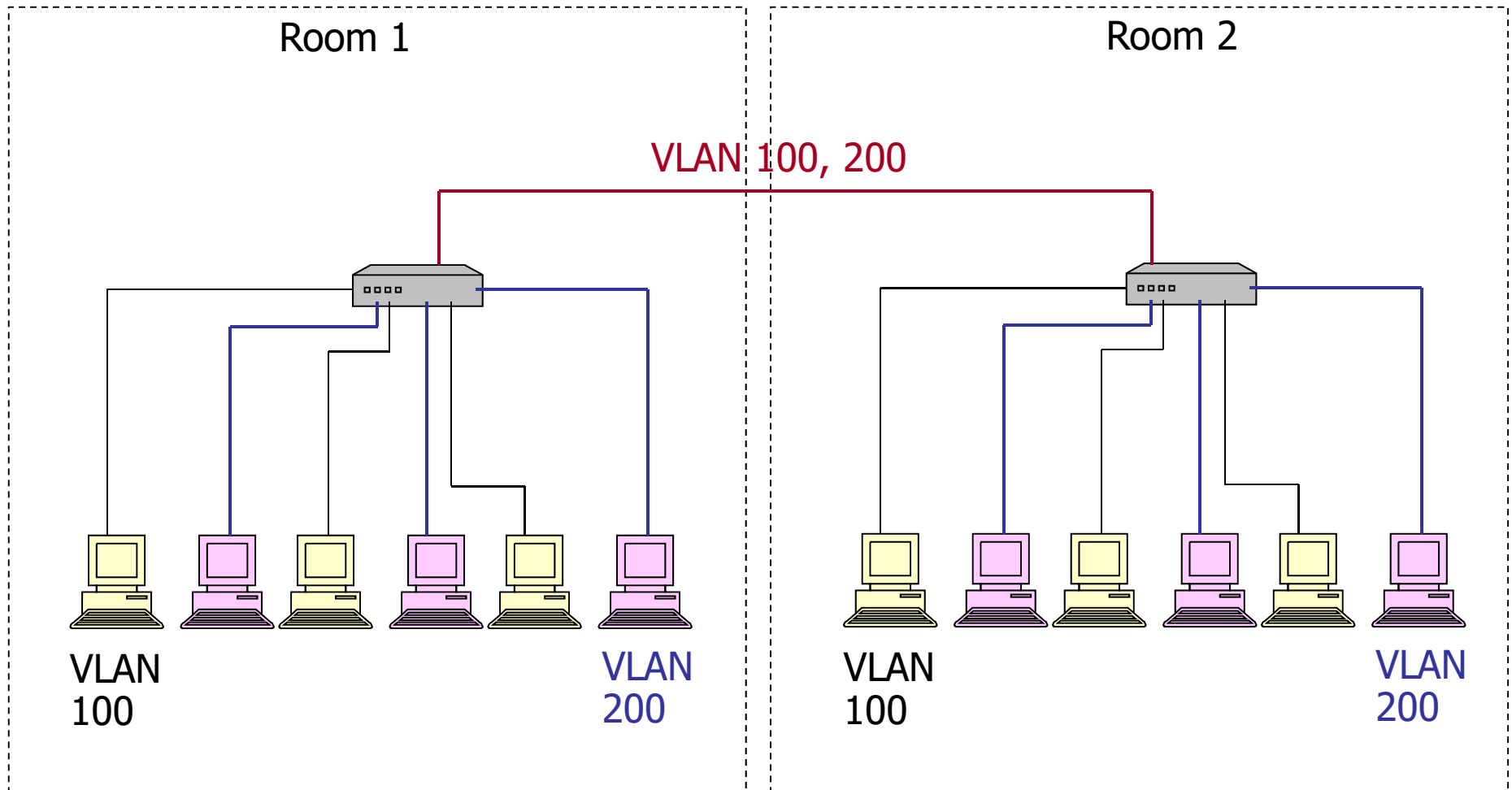


VLAN สามารถขยายผ่านมากกว่า 1 Switch



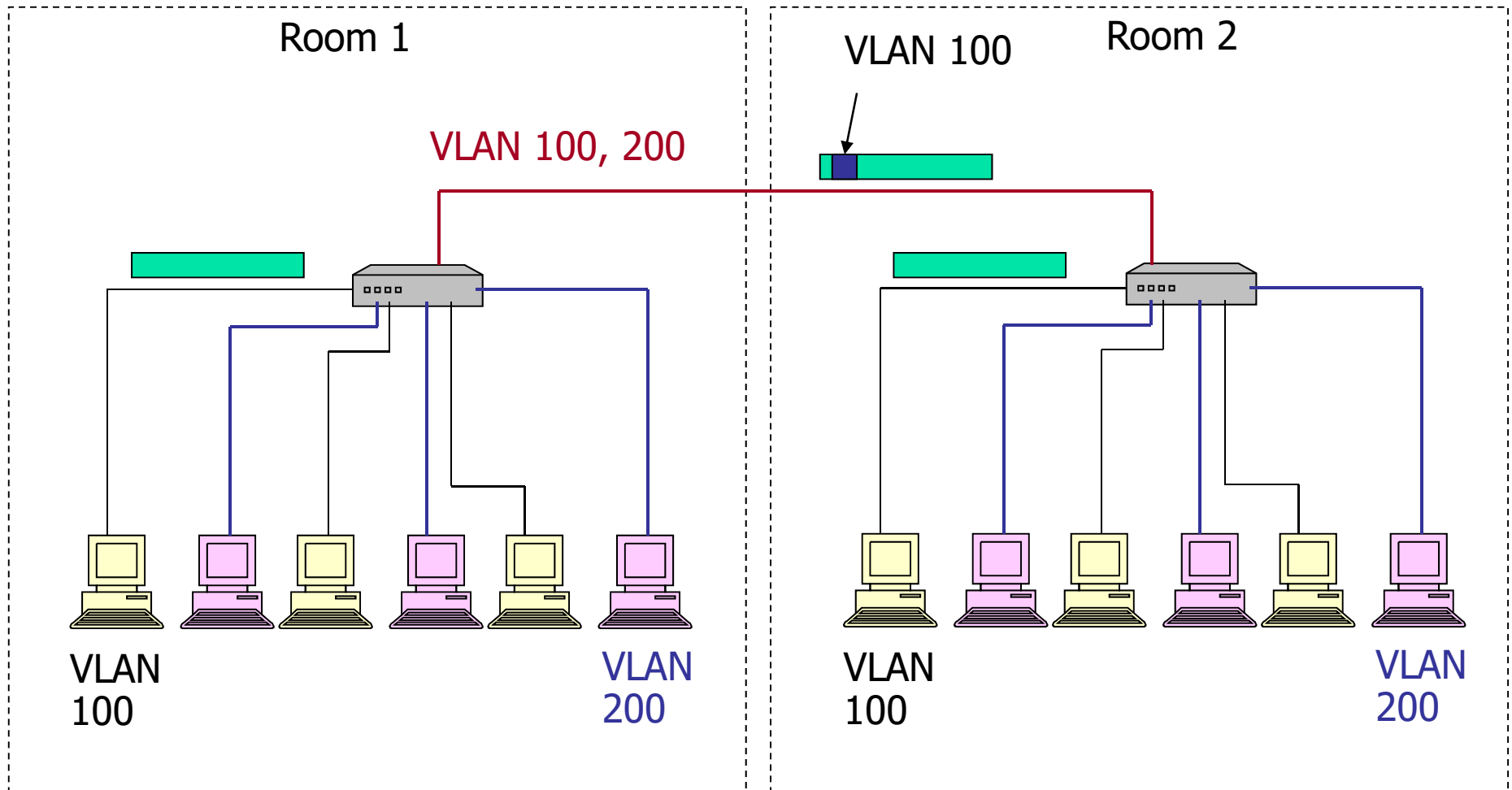


VLAN สามารถขยายผ่านมากกว่า 1 Switch





VLAN สามารถขยายผ่านมากกว่า 1 Switch







VLAN TAGGING

- **IEEE 802.1Q Standard**
 - 4 Byte เพิ่มในส่วนของ Header
 - 12 Bit เป็น VLAN Number
- **ISL(Cisco)**
 - Encapsulation



VLAN Tagging (IEEE 802.1Q)

- Port ของ Switch จะต้องถูกกำหนดเป็น Tag Port
- เมื่อข้อมูลถูกส่งออกไปยัง Tag Port จะมีการใส่ Tag กำหนด VLAN
- เมื่อข้อมูลมาถึง Tag Port จะถูกส่งไปยัง VLAN ตาม Tag และตัว Tag จะถูกนำออก
- VLAN Default ของ Port นั้นจะไม่ถูกใส่ Tag
 - VLAN Number จะเป็น Local ยกเว้นทำ Tagging
 - อุปกรณ์บางยี่ห้อจะมี Protocol สื่อสารระหว่าง SW (Interswitch Protocol)



Communication Between VLAN

- **Connect Through Router (L3)**
- **Using L3 Switch ดีกว่า**



VLAN Static vs Dynamic

- เมื่อ VLAN ถูกกำหนดโดย Port ของ Switch เราเรียก Static VLAN
 - อุปกรณ์ที่เชื่อมต่อกับ Port ดังกล่าวจะถูกจับไปอยู่ใน VLAN ที่กำหนด
- แต่ถ้าเรากำหนดให้อุปกรณ์ที่มาเชื่อมกับ Port ไปอยู่ใน VLAN ตามคุณสมบัติของอุปกรณ์ เช่น ตาม IP Address, MAC Address หรือตามการ Authentication เราเรียก Dynamic VLAN
 - Port ดังกล่าวจะเป็น "Mobile Port" และต้องกำหนด VLAN Rule ให้



การกำหนด VLAN

- **หนึ่ง Subnet ให้เป็น หนึ่ง VLAN**
- **เมื่อเรากำหนด Topology เราได้**
 - Subnet ของแต่ละ Network
 - กำหนด IP Address ให้กับแต่ละ Subnet
 - กำหนด VLAN ให้กับแต่ละ Subnet
 - ดังนั้นแต่ละ Subnet สามารถอยู่ร่วมกันบน Switch เดียวกันได้
 - แต่ละ Subnet สามารถกระจาย ครอบคลุมหลาย Switch ได้
 - กล่าวคือ Logical Network(Diagram) และ Physical Network(Wiring Diagram) สามารถแยกจากกัน
 - Network จะประกอบด้วยสอง Diagram



Spanning Tree and VLAN

- เนื่องจากมาตรฐานของ Spanning Tree(802.1D) นั้นได้ตั้งขึ้นมาก่อน VLAN ดังนั้นการทำ VLAN ใน Network จะมีมากกว่า 1 Spanning Tree ไม่ได้ นั่นหมายถึงทุกๆ VLAN จะต้องมีการมี Spanning Tree เดียว ซึ่งถ้าทำ VLAN แบบ ง่ายๆจะไม่มีปัญหา แต่บางครั้งถ้าเรามีการทำ Filter ของ Trunk Port อาจจะทำให้บาง VLAN หลุดจาก Spanning Tree ได้
- Cisco ได้เพิ่มส่วนของ Protocol ของ Spanning Tree ที่ทำให้สามารถมี Spanning Tree แยกสำหรับแต่ละ VLAN ได้ แต่ก็ใช้ได้กับ Switch ของ Cisco เท่านั้น อย่างไรก็ตามมาตรฐานใหม่ของ IEEE คือ IEEE 802.1s ซึ่งเป็นมาตรฐานสำหรับ Multiple Spanning Tree(MST) จะยอมให้มีหลาย Spanning Tree ได้

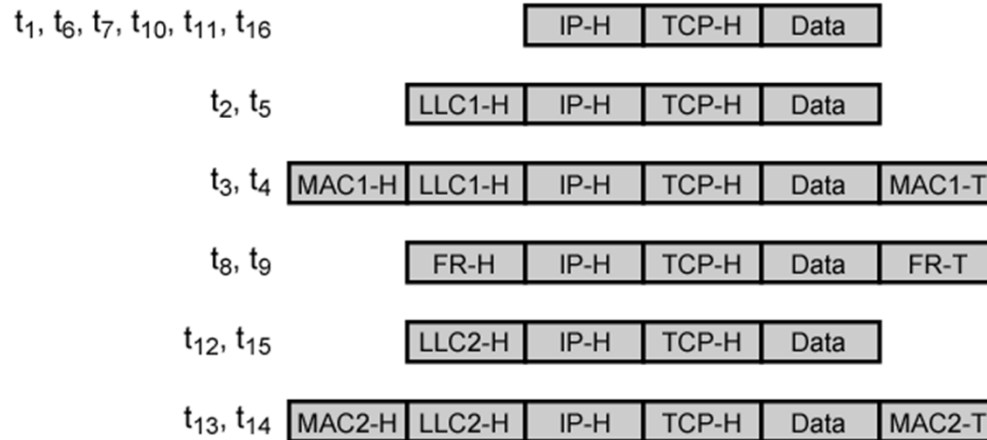
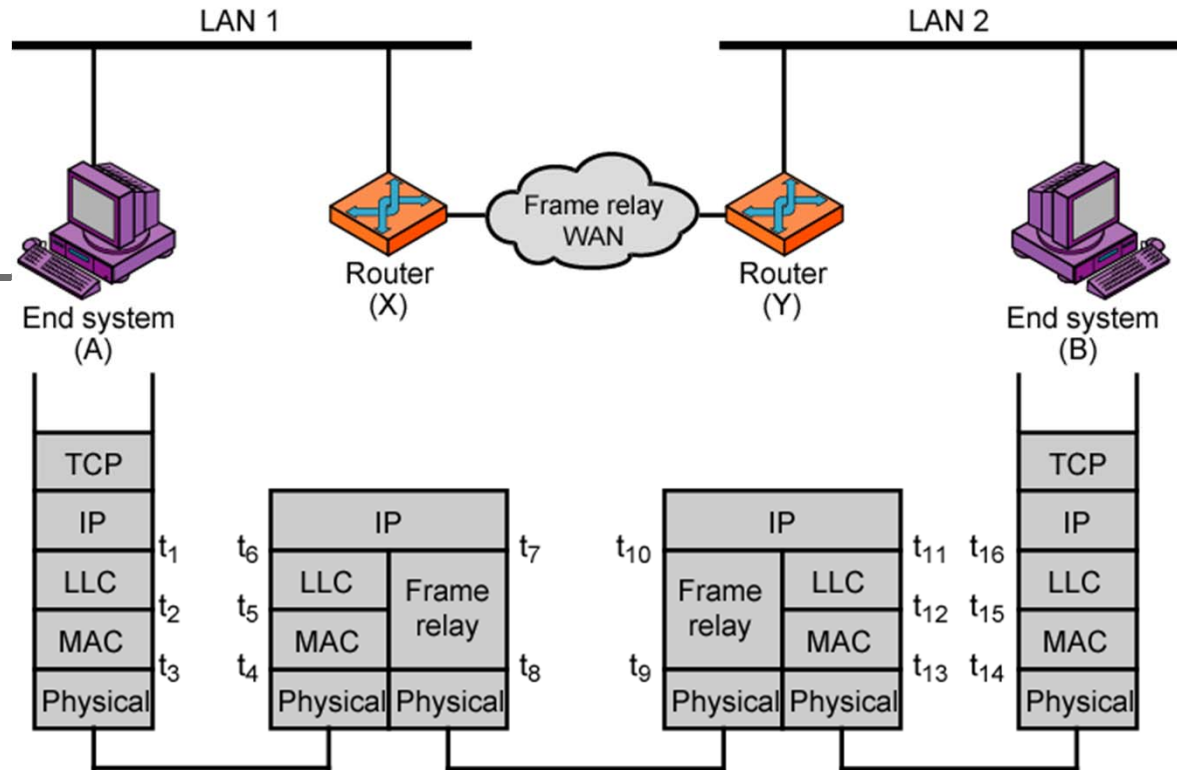


WAN Technologies

- ในการเชื่อมต่อระยะไกล, Ethernet Technologies ไม่สามารถนำมาใช้ได้
- IP เป็น WAN แต่อยู่ใน Layer 3 ดังนั้น ต้องการ Layer 2 และ Layer 1 เป็นตัวนำ IP Packet
 - IP บน Ethernet ใช้ได้ใน LAN เท่านั้น
 - ในการส่งไกลกว่านั้น ต้องหา WAN Technologies มานำ IP Packet
 - IP บรรจุใน WAN Layer 2 ส่งผ่าน Layer 1 (HDLC, FR, SDH, MPLS, ATM ผ่าน Modem, Fiber, ...)
 - IP บรรจุใน Layer 3 WAN Frame เช่นใน X.25



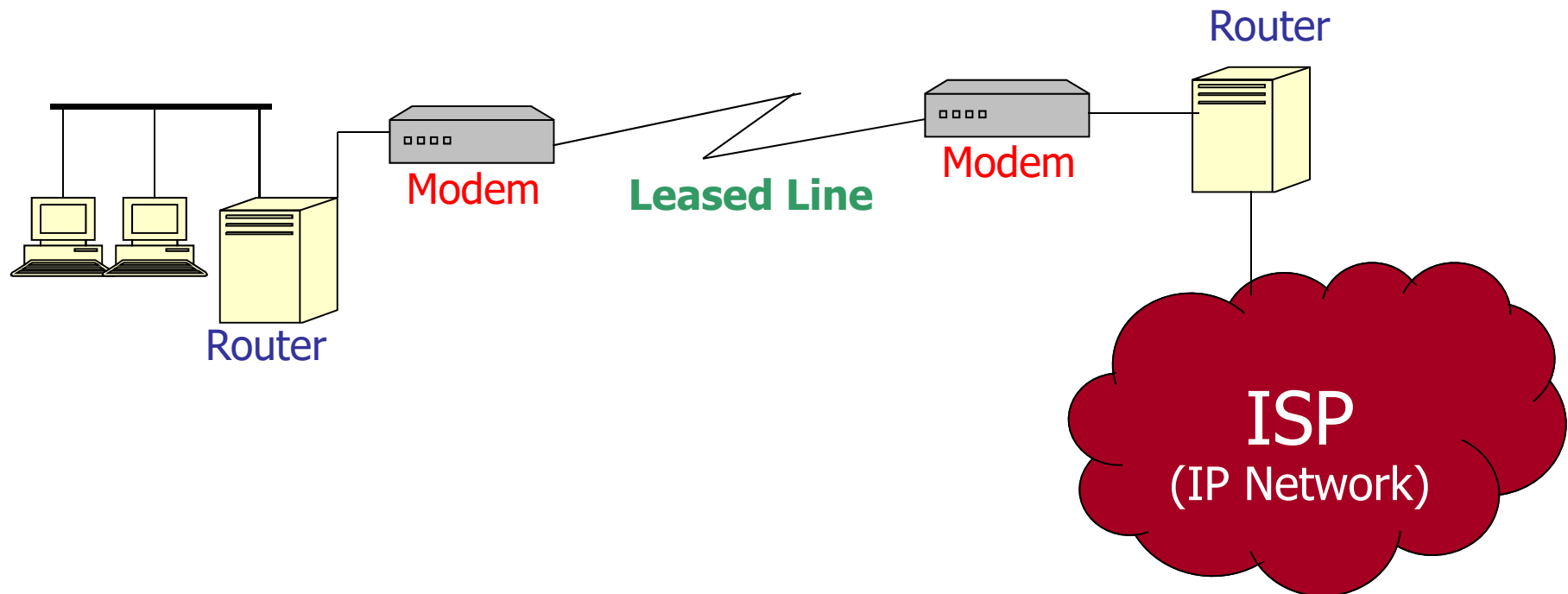
WAN Connection



TCP-H = TCP header
 IP-H = IP header
 LLCi-H = LLC header
 MACi-H = MAC header
 MACi-T = MAC trailer
 FR-H = Frame relay header
 FR-T = Frame relay trailer



Connect to ISP



Note: ปัจจุบัน Technology ของ Ethernet สามารถส่งได้ไกลขึ้น
ทำให้เราขยาย LAN ได้ในระยะทางหลายสิบกม. แต่เราไม่สามารถเดินสายได้เอง
ยังคงต้องพึ่ง Public Network



WAN Technologies

Option:	Description	Advantages	Disadvantages	Bandwidth range	Sample protocols used
<u>Leased line</u>	Point-to-Point connection between two computers or Local Area Networks (LANs)	Most secure	Expensive		<u>PPP</u> , <u>HDLC</u> , <u>SDLC</u> , <u>HNAS</u>
<u>Circuit switching</u>	A dedicated circuit path is created between end points. Best example is <u>dialup</u> connections	Less Expensive	Call Setup	28 kbit/s - 144 kbit/s	<u>PPP</u> , <u>ISDN</u>
<u>Packet switching</u>	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted over Permanent Virtual Circuits (<u>PVC</u>) or Switched Virtual Circuits (<u>SVC</u>)		Shared media across link		<u>X.25</u> <u>Frame-Relay</u>
<u>Cell relay</u>	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual circuits	best for simultaneous use of Voice and data	<u>Overhead</u> can be considerable		<u>ATM</u>

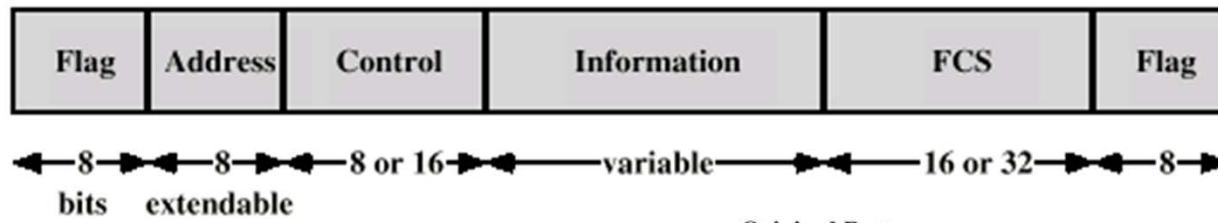


HDLC

- **High Level Data Link Control Protocol**
- **ISO Standard**
 - Current Standard = ISO 13239
- **Connection Oriented and Connectionless**
- **Most common mode = point-to-point using ABM (Asynchronous Balanced Mode)**
- **Transmission Mode/Station Type/Flow**
 - ดูใน CPE326 (Stalling Book)



HDLC Frame Format



(a) Frame format

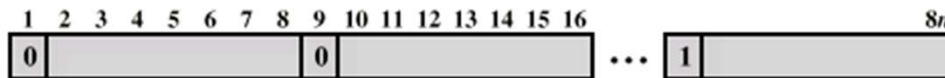
Original Pattern:

11111111111111110111111101111110

After bit-stuffing

111110111111011011111101011111010

(a) Example



(b) Extended Address Field

HDLC เป็นต้นกำเนิดของ Frame Format และ L2 Protocol อื่นๆ

- LLC
- MAC
- PPP
- LAPB
- LAPD
- LAPF
- ฯลฯ



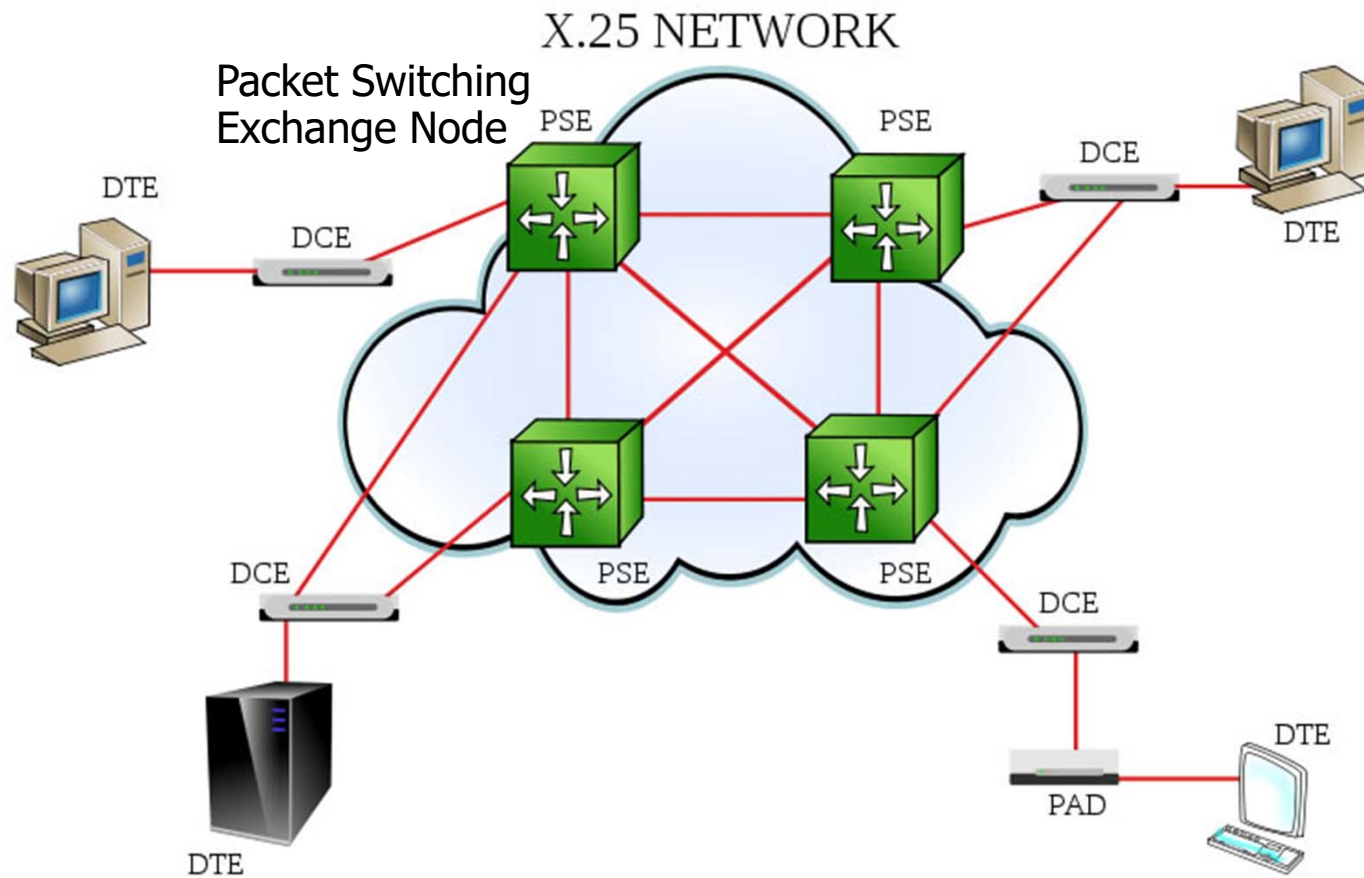
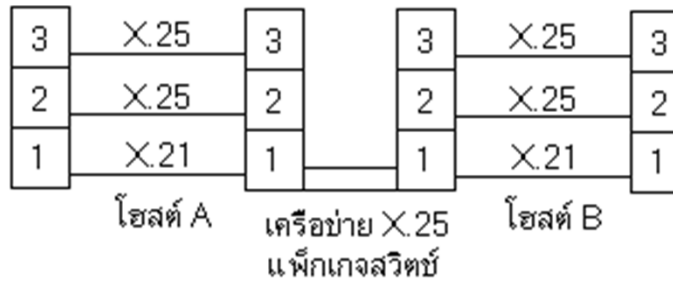
(b) An inverted bit splits a frame in two



(c) An inverted bit merges two frames

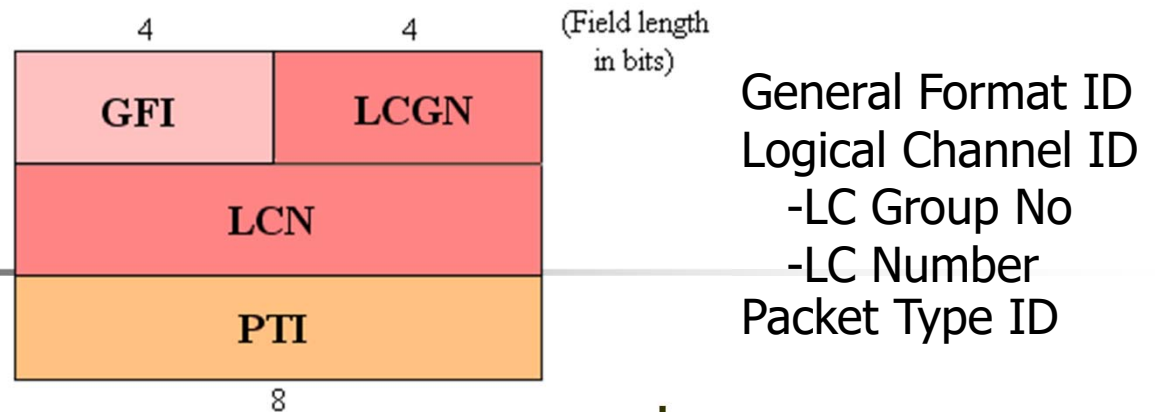


X.25





X.25



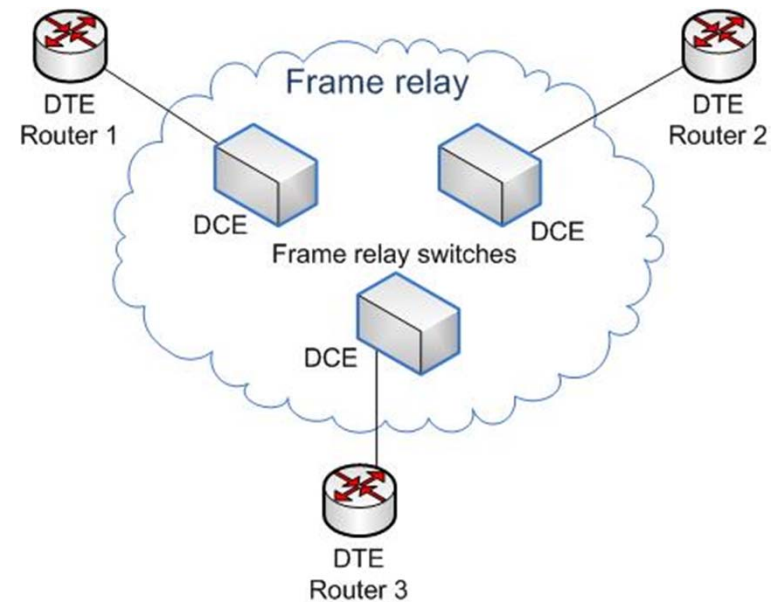
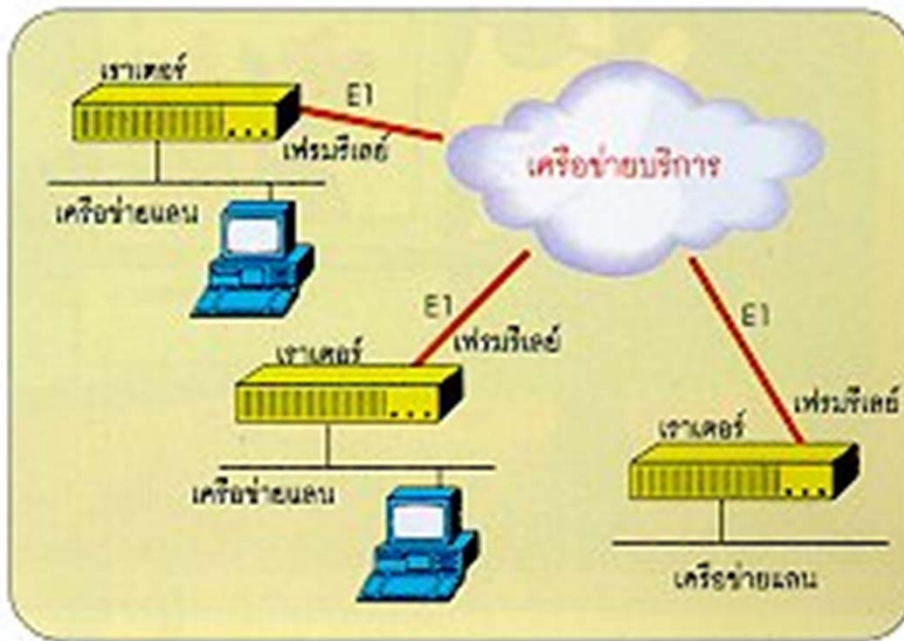
- **Physical Layer:** กำหนดการเชื่อมต่อทางไฟฟ้า ระหว่าง DTE/DCE จะอยู่ใน X.21 หรือจะใช้ EIA-232, EIA-449 หรือ Serial Protocol อื่น
- **Data Link Layer:** กำหนดขบวนการใช้ Link สำหรับการส่งข้อมูลระหว่าง DTE/DCE จะใช้ LAPB

Flag 01111110 (8bits)	Address (8bits)	Control (8bits)	Data (Variable)	Checksum (16 bits)	Flag 01111110 (8bits)
-----------------------------	--------------------	--------------------	--------------------	-----------------------	-----------------------------

- **Packet Layer** กำหนด Protocol ในระดับ Packet ในการแลกเปลี่ยน Control และ Data กับ PSN ผ่าน Virtual Circuit



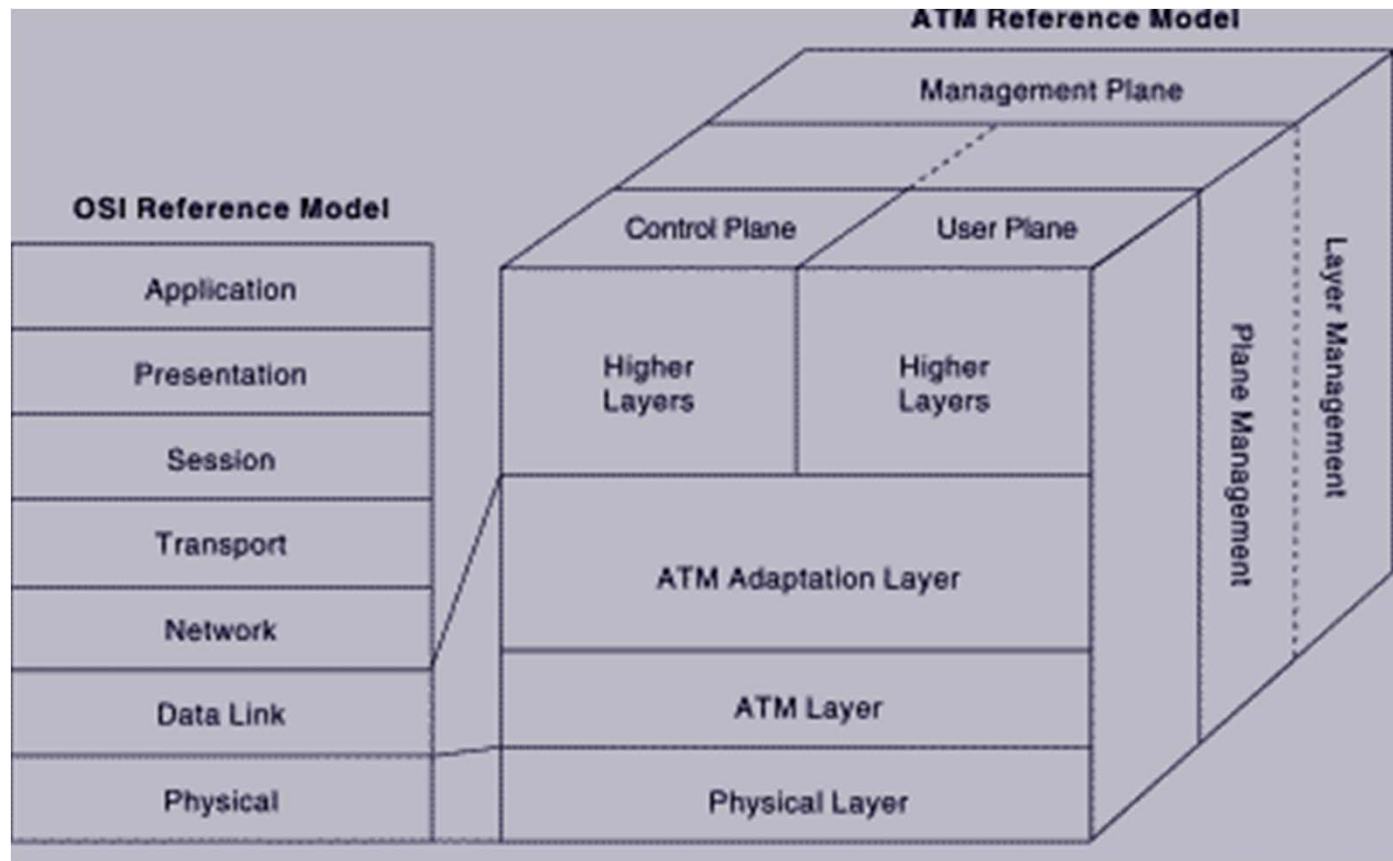
Frame Relay



พัฒนาต่อจาก X.25 ใช้ LAP-D ในการส่ง Data, ตัดส่วน Flow Control ออก และ Switch ใน L2 ทำให้ส่งข้อมูลได้เร็วและเป็น Stream มากขึ้น

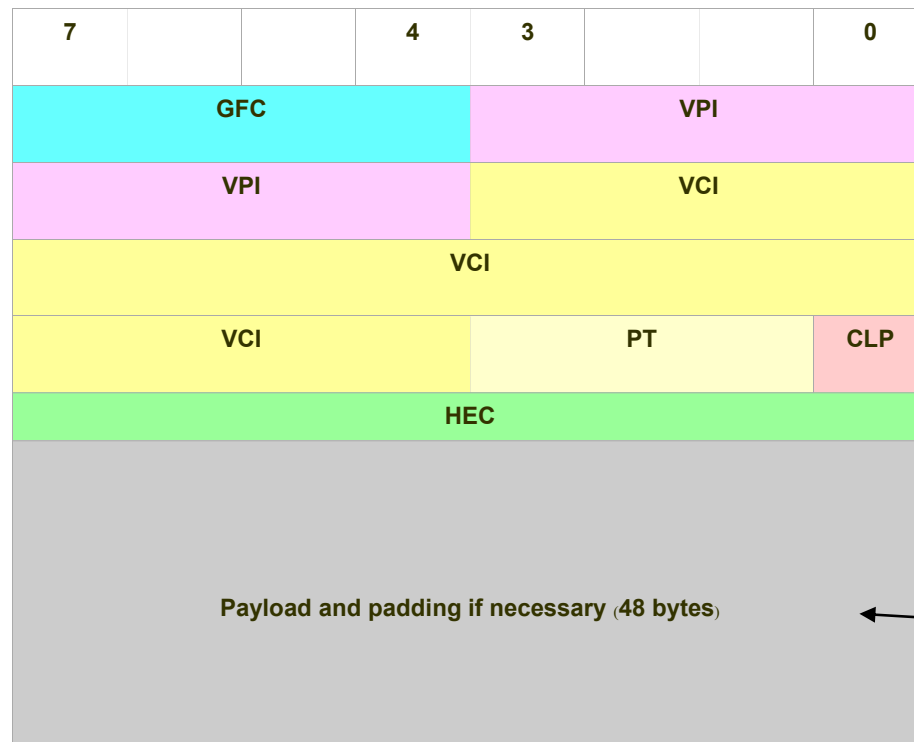


ATM (Cell Switching)





ATM (Cell Switching)



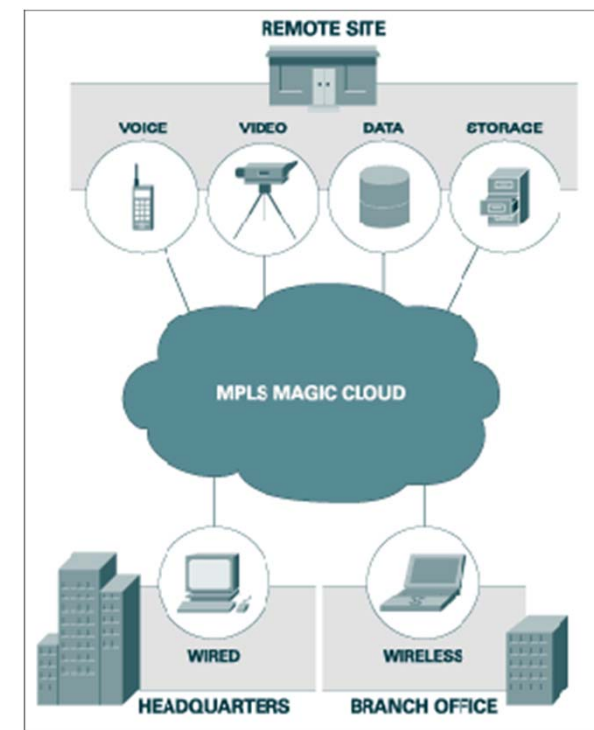
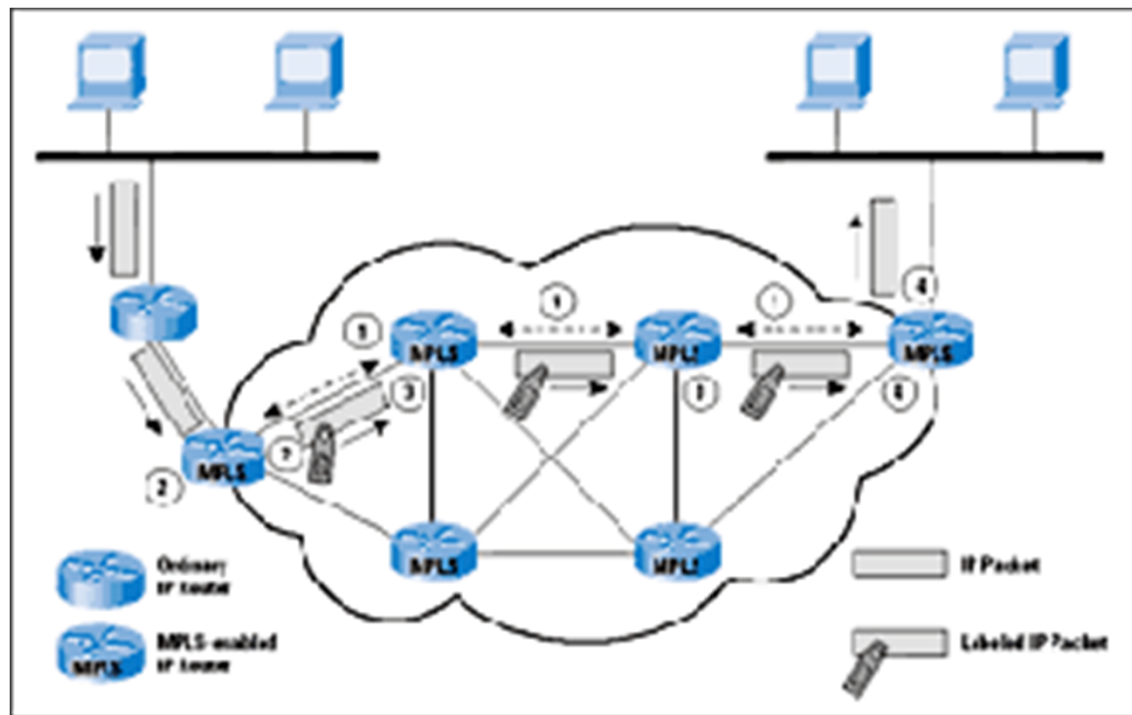
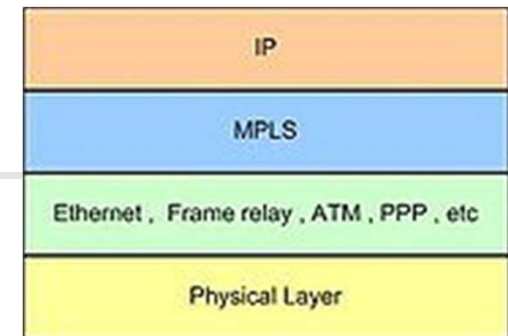
ปัจจุบัน SDH ถูกใช้ในการ
Transport ATM

CBR
VBR
ABR
UBR

AAL Type 1-5



MPLS (Multiprotocol Label Switching)



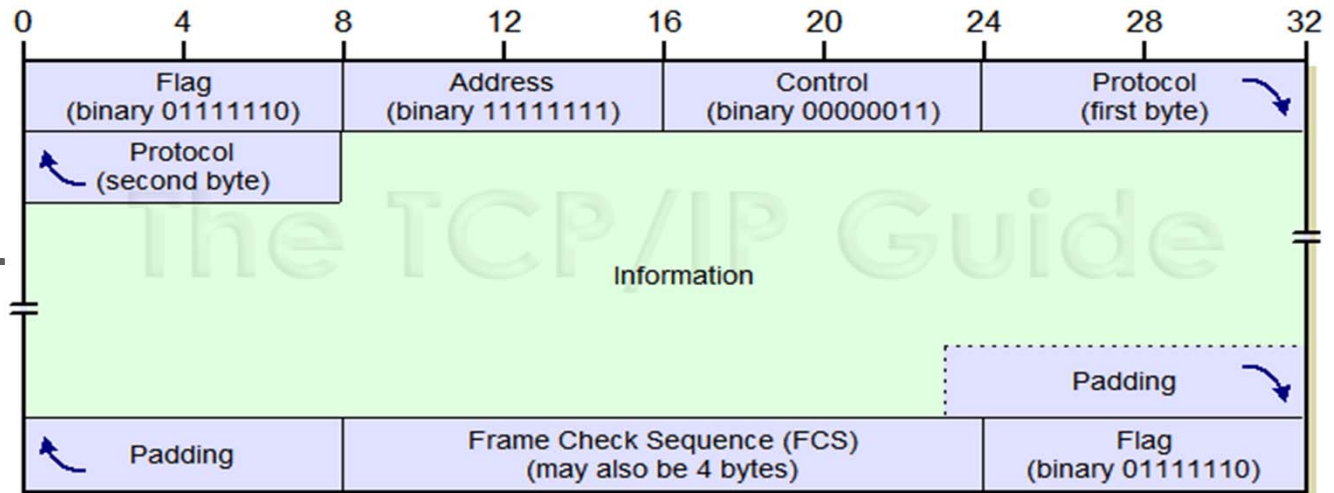


PPP (Point-to-Point Protocol)

- นิยมใช้ในปัจจุบัน สำหรับเป็น Data Link Protocol ในการเชื่อมต่อโดยตรงระหว่าง Node (Point-to-Point)
- ใช้ได้ผ่าน Physical Link หลายแบบ เช่น Serial Cable, Phone Line, Cell Phone, SONET โดยที่ ISP ส่วนใหญ่จะใช้สำหรับลูกค้าที่จะ Dial-Up Access กับ Internet
- มาแทนที่ Protocol เก่าได้แก่
 - SLIP (Serial Line Internet Protocol)
 - LAPB ใน X.25
- ถูกออกแบบมาให้ใช้กับ Network Layer ต่างๆ รวมถึง IP
- ยังถูกใช้เป็น Protocol ในการเชื่อมต่อ Broadband ด้วย ใน PPPoE และ PPPoA



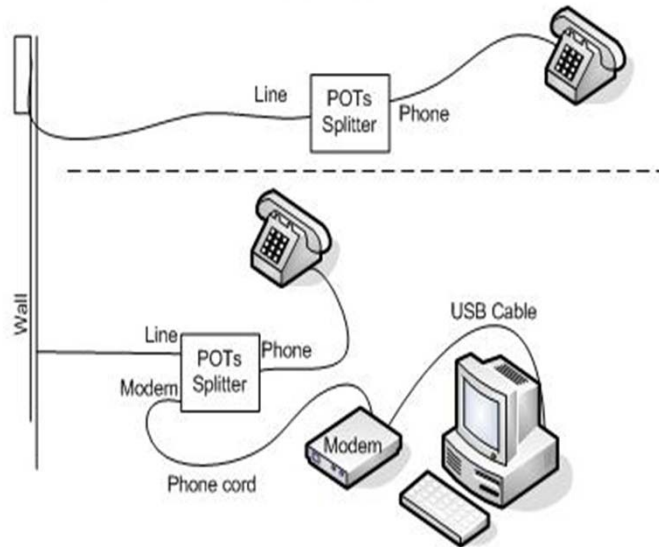
PPP Frame



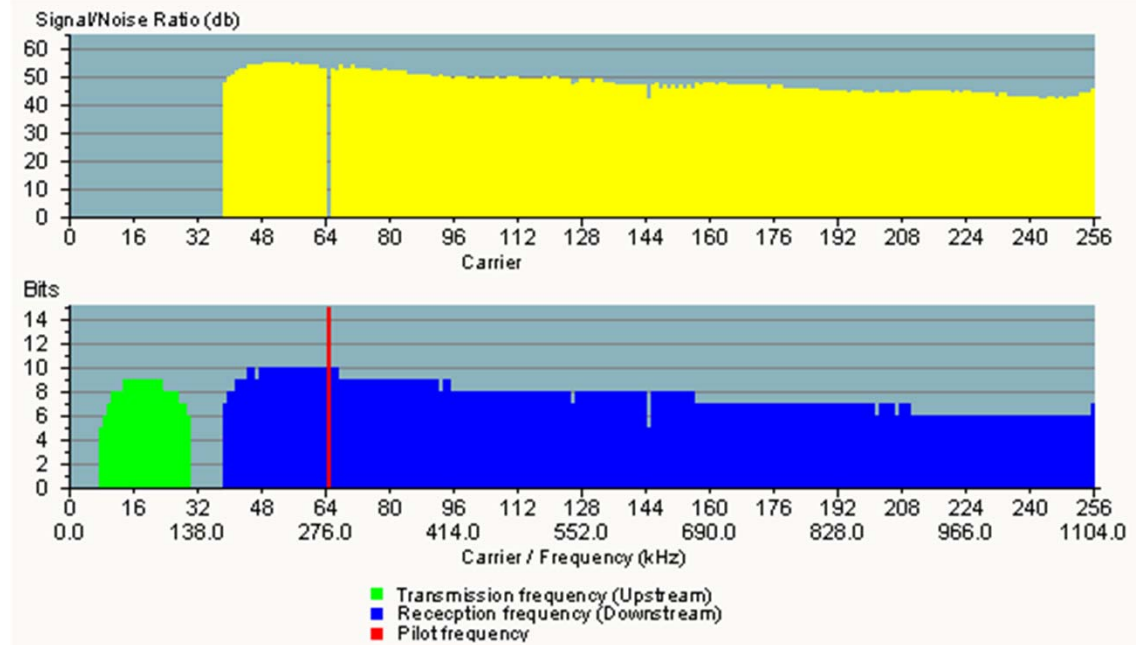
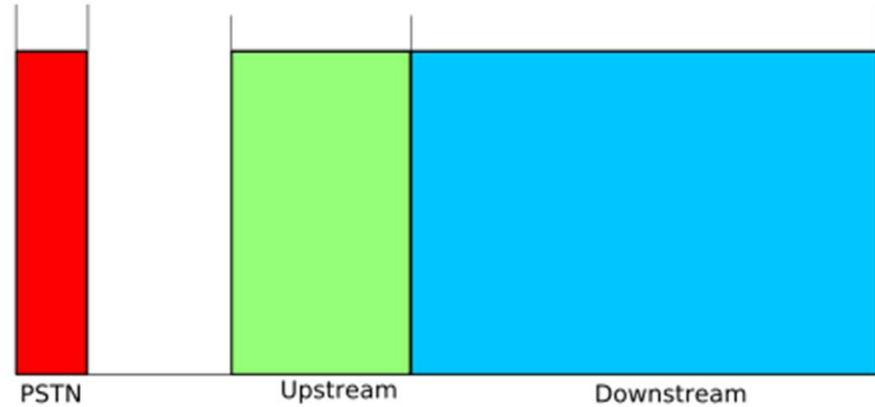
Field Name	Size (bytes)	Description
<i>Flag</i>	1	<i>Flag:</i> Indicates the start of a PPP frame. Always has the value “01111110” binary (0x7E hexadecimal, or 126 decimal).
<i>Address</i>	1	<i>Address:</i> In HDLC this is the address of the destination of the frame. But in PPP we are dealing with a direct link between two devices, so this field has no real meaning. It is thus always set to “11111111” (0xFF or 255 decimal), which is equivalent to a broadcast (it means “all stations”).
<i>Control</i>	1	<i>Control:</i> This field is used in HDLC for various control purposes, but in PPP it is set to “00000011” (3 decimal).
<i>Protocol</i>	2	<i>Protocol:</i> Identifies the protocol of the datagram encapsulated in the Information field of the frame. See below for more information on the <i>Protocol</i> field.
<i>Information</i>	Variable	<i>Information:</i> Zero or more bytes of payload that contains either data or control information, depending on the frame type. For regular PPP data frames the network-layer datagram is encapsulated here. For control frames, the control information fields are placed here instead.
<i>Padding</i>	Variable	<i>Padding:</i> In some cases, additional dummy bytes may be added to pad out the size of the PPP frame.
<i>FCS</i>	2 (or 4)	<i>Frame Check Sequence (FCS):</i> A checksum computed over the frame to provide basic protection against errors in transmission. This is a CRC code similar to the one used for other layer two protocol error protection schemes such as the one used in Ethernet. It can be either 16 bits or 32 bits in size (default is 16 bits). The FCS is calculated over the <i>Address</i> , <i>Control</i> , <i>Protocol</i> , <i>Information</i> and <i>Padding</i> fields.
<i>Flag</i>	1	<i>Flag:</i> Indicates the end of a PPP frame. Always has the value “01111110” binary (0x7E hexadecimal, or 126 decimal).

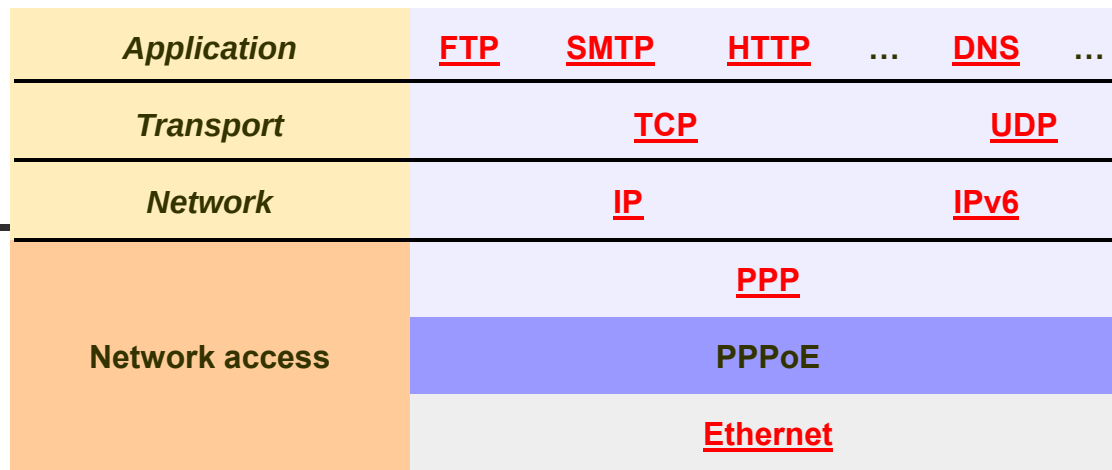


Broad-band (ADSL)

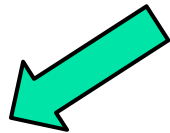


0 4 kHz 25.875 kHz 138 kHz 1104 kHz

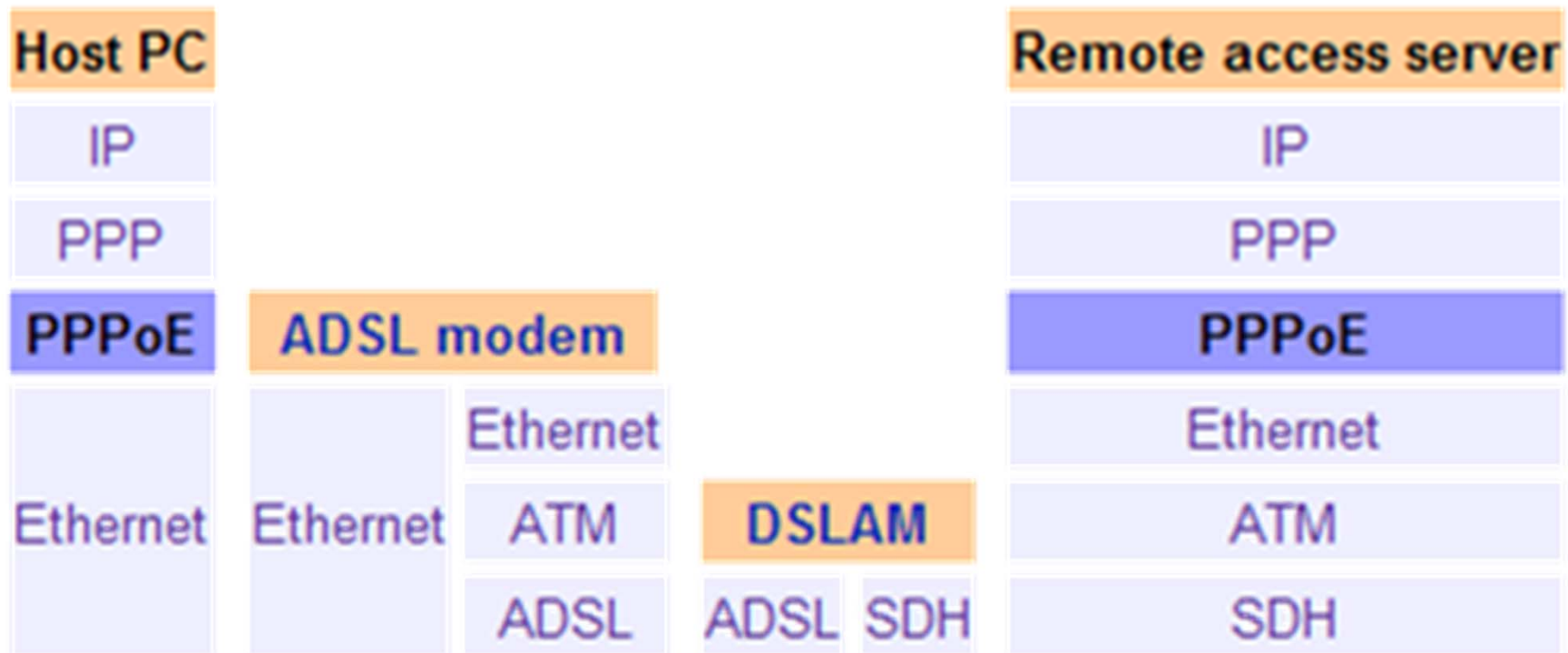




PPPoE

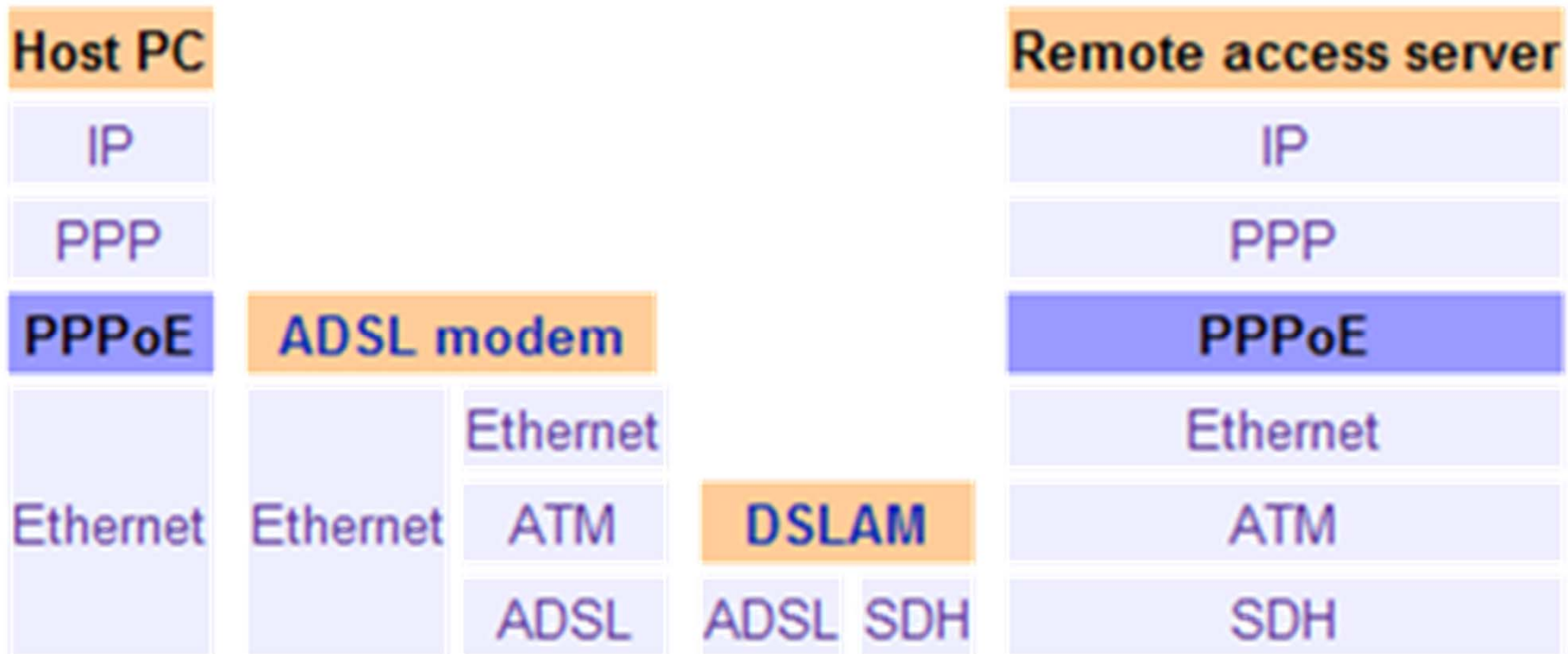
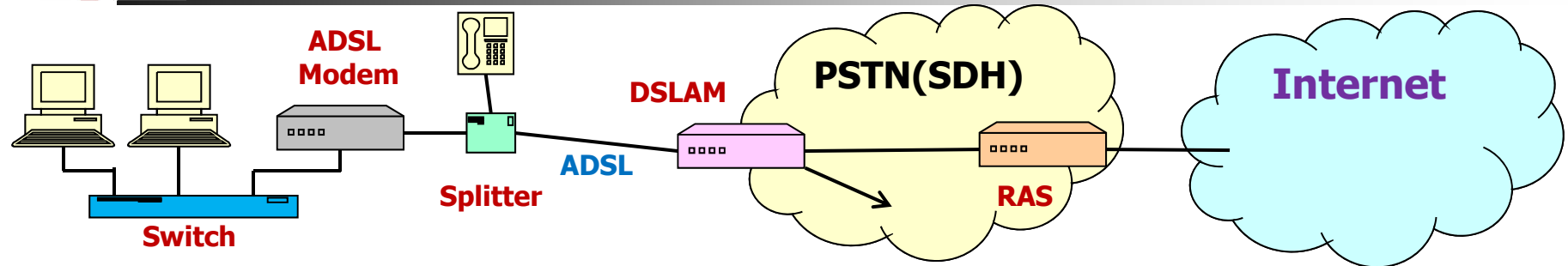


ADSL internet access architecture





PPPoE





Importance Ethernet Standards

Ethernet Standard	Date	Description
Experimental Ethernet	1973 ^[1]	2.94 <u>Mbit/s</u> (367 <u>kB/s</u>) over <u>coaxial cable</u> (coax) <u>bus</u>
Ethernet II (DIX v2.0)	1982	10 Mbit/s (1.25 <u>MB/s</u>) over thick coax. Frames have a Type field. This frame format is used on all forms of Ethernet by protocols in the <u>Internet protocol suite</u> .
IEEE 802.3 standard	1983	<u>10BASE5</u> 10 Mbit/s (1.25 MB/s) over thick coax. Same as Ethernet II (above) except Type field is replaced by Length, and an <u>802.2</u> LLC header follows the 802.3 header. Based on the <u>CSMA/CD</u> Process.
<u>802.3a</u>	1985	<u>10BASE2</u> 10 Mbit/s (1.25 MB/s) over thin Coax (a.k.a. thinnet or cheapernet)
<u>802.3i</u>	1990	<u>10BASE-T</u> 10 Mbit/s (1.25 MB/s) over twisted pair
<u>802.3j</u>	1993	<u>10BASE-F</u> 10 Mbit/s (1.25 MB/s) over Fiber-Optic



Importance Ethernet Standards

Ethernet Standard	Date	Description
<u>802.3u</u>	1995	<u>100BASE-TX</u> , <u>100BASE-T4</u> , <u>100BASE-FX</u> Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/ <u>autonegotiation</u>
<u>802.3x</u>	1997	Full Duplex and <u>flow control</u> ; also incorporates DIX framing, so there's no longer a DIX/802.3 split
<u>802.3ab</u>	1999	<u>1000BASE-T</u> Gbit/s Ethernet over twisted pair at 1 Gbit/s (125 MB/s)
<u>802.3ad</u>	2000	<u>Link aggregation</u> for parallel links, since moved to <u>IEEE 802.1AX</u>
<u>802.3ae</u>	2002	<u>10 Gigabit Ethernet</u> over fiber; 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW
<u>802.3af</u>	2003	<u>Power over Ethernet</u> (15.4 W)
<u>802.3an</u>	2006	<u>10GBASE-T</u> 10 Gbit/s (1,250 MB/s) Ethernet over unshielded twisted pair (UTP)
<u>802.3at</u>	2009	<u>Power over Ethernet</u> enhancements (25.5 W)



Ethernet Standard	Date	Description
<u>802.3ba</u>	2010	40 Gbit/s and 100 Gbit/s Ethernet. 40 Gbit/s over 1m backplane, 10 m Cu cable assembly (4x25 Gbit or 10x10 Gbit lanes) and 100 m of <u>MMF</u> and 100 Gbit/s up to 10 m of Cu cable assembly, 100 m of <u>MMF</u> or 40 km of <u>SMF</u> respectively
802.3.1	2011	MIB definitions for Ethernet. It consolidates the Ethernet related <u>MIBs</u> present in Annex 30A&B, various <u>IETF RFCs</u> , and 802.1AB annex F into one master document with a machine readable extract. (workgroup name was P802.3be)
802.3bm	2015	<u>100G/40G Ethernet</u> for optical fiber
802.3bq	~Feb 2016	<u>40GBASE-T</u> for 4-pair balanced twisted-pair cabling with 2 connectors over 30 m distances
802.3bs	~ 2017	400 Gbit/s Ethernet over optical fiber using multiple 25G/50G lanes
802.3by	~Sep 2016	<u>25G Ethernet</u>
802.3bz	TBD	2.5 Gigabit and 5 Gigabit Ethernet over twisted pair - 2.5GBASE-T and 5GBASE-T



-
- **END OF REVIEW**
 - **BREAK**
 - **CHAPTER 20: TCP/IP Concept**



Chapter 20: TCP/IP Concept/ ที่มาของปัญหา

- สมัยก่อน การนำ **Network** มาใช้งาน จะขึ้นอยู่กับงานที่ต้องการทำให้ **NW** นั้นมีหลากหลาย
 - แต่ละองค์กร มี **NW** ที่ใช้ **Technology** ต่างๆกัน
- การที่จะเชื่อม **NW** ต่างๆเหล่านี้ด้วยกัน เพื่อ **Share** ข้อมูลไม่สามารถทำได้ เพราะ **Protocol** ที่ใช้ไม่เหมือนกัน
 - คอมพิวเตอร์ใน **NW** หนึ่งสื่อสารได้กับคอมพิวเตอร์ใน **NW** เดียวกันเท่านั้น
 - องค์กรมีหลาย **NW** เพื่อที่จะทำงานหลายๆอย่าง ผู้ใช้งานต้องมีคอมพิวเตอร์หลายตัว เพื่อเชื่อมต่อแต่ละ **NW** สำหรับงานแต่ละประเภท
- สรุปแล้ว **NW** สมัยก่อนเป็น **Heterogeneous**
- เราต้องการหา **Technology** ที่สามารถจะเชื่อมต่อ **NW** เหล่านี้เข้าด้วยกัน เพื่อจะสื่อสารและแลกเปลี่ยนข้อมูลกันได้
 - ปัญหาที่ต้องแก้มีมากมาย เช่น
 - เรื่องของสัญญาณและ **Hardware** ที่ต่างกัน
 - **Frame Format** ที่ไม่เหมือนกัน
 - ระบบการใช้ **Address** ที่ไม่เหมือนกัน

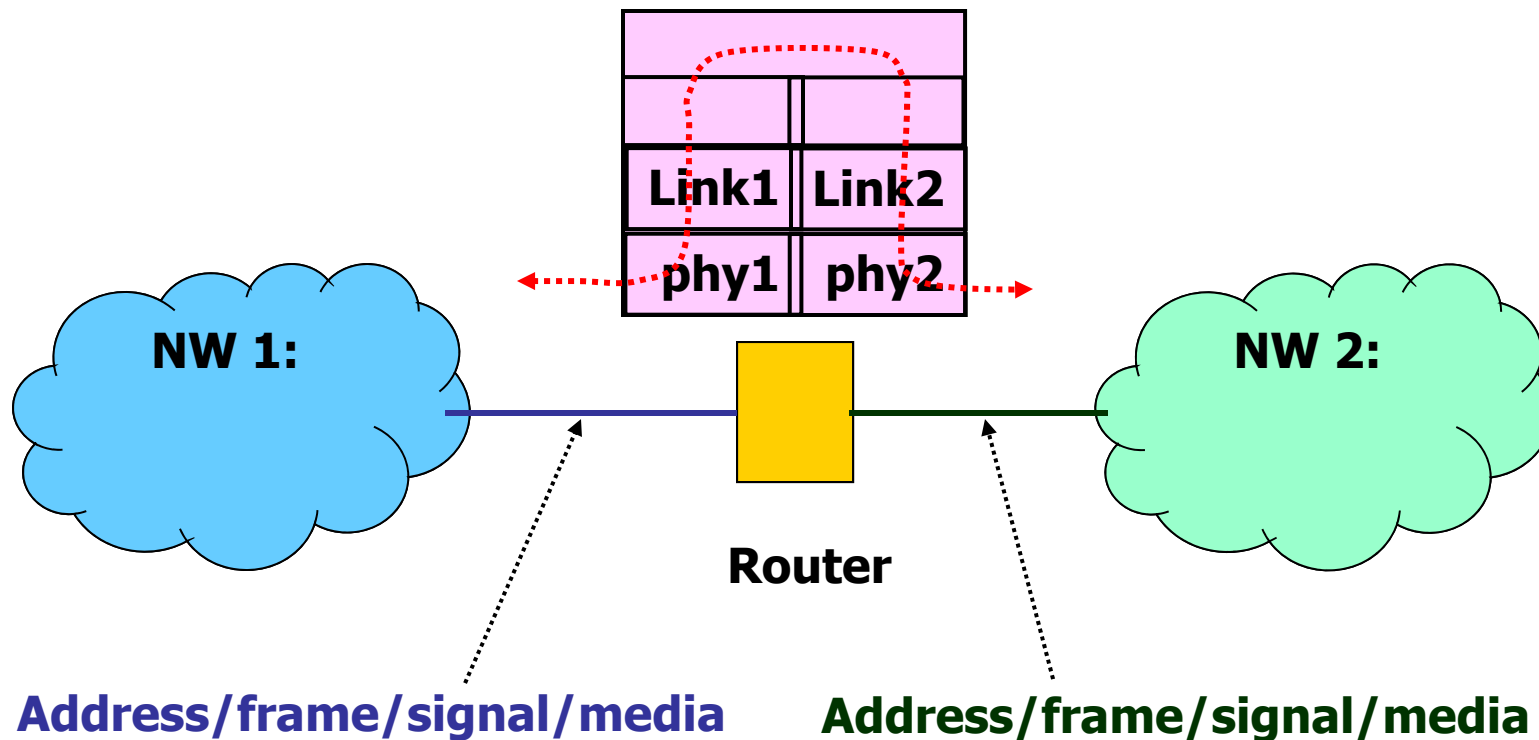


Chapter 20: TCP/IP ที่มาของปัญหา → Solution: internetworking

- เทคโนโลยีที่จะทำให้หลายๆ **Network** สามารถเชื่อมต่อกันได้เรียก
 - Internetworking หรือ internet
 - (กรณีนี้ ยังไม่เจาะจงว่าเป็น IP Network ดังนั้นเราจะใช้คำว่า 'a internet' ไม่ใช่ 'the Internet')
- รูปแบบการเชื่อมต่อ **Network** เข้าด้วยกัน จะใช้การต่อผ่านอุปกรณ์ที่ชื่อ '**Router**'
 - Router จะเชื่อมต่อ NW สองด้าน(หรือมากกว่า) เข้าด้วยกัน
 - หมายความว่า Port หนึ่งของ Router อาจจะ Run Protocol หนึ่ง ในขณะที่อีก Port หนึ่งจะ Run Protocol ที่ต่างกัน
 - แต่ละ Port ของ Router เราเรียก "Interface"
 - NW แต่ละด้าน อาจจะเป็นคนละ Technology รวมถึงใช้ Frame Format/Media/Address/Signal ที่แตกต่างกัน



Chapter 20: Internetworking with Router

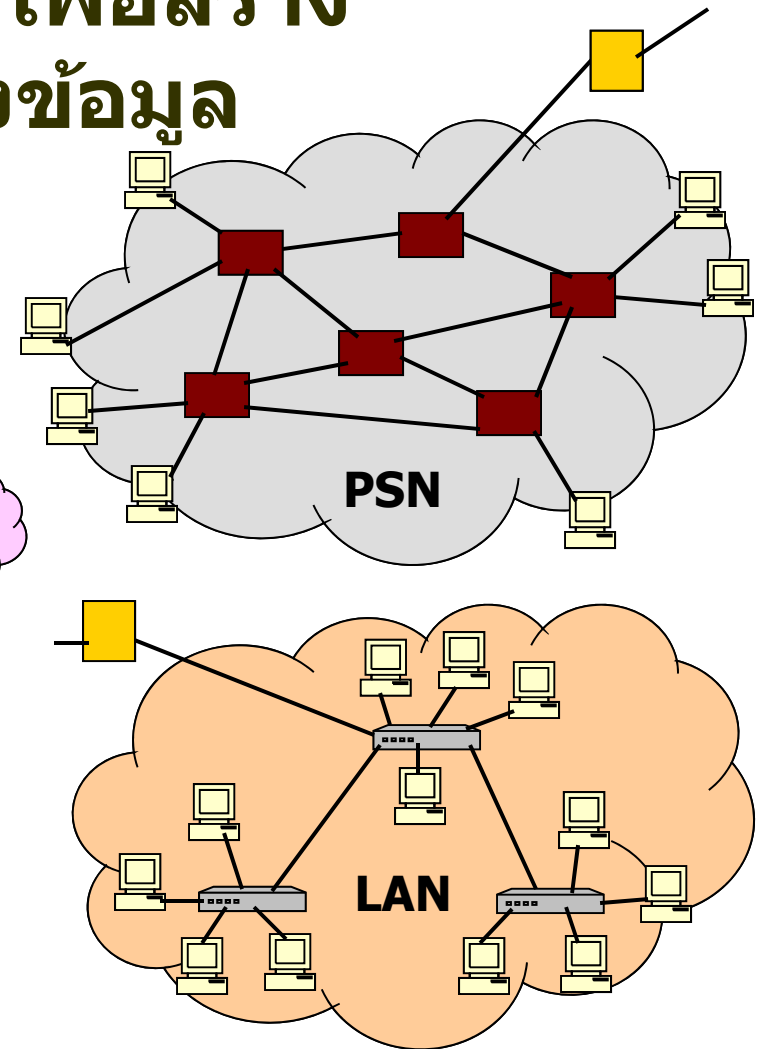
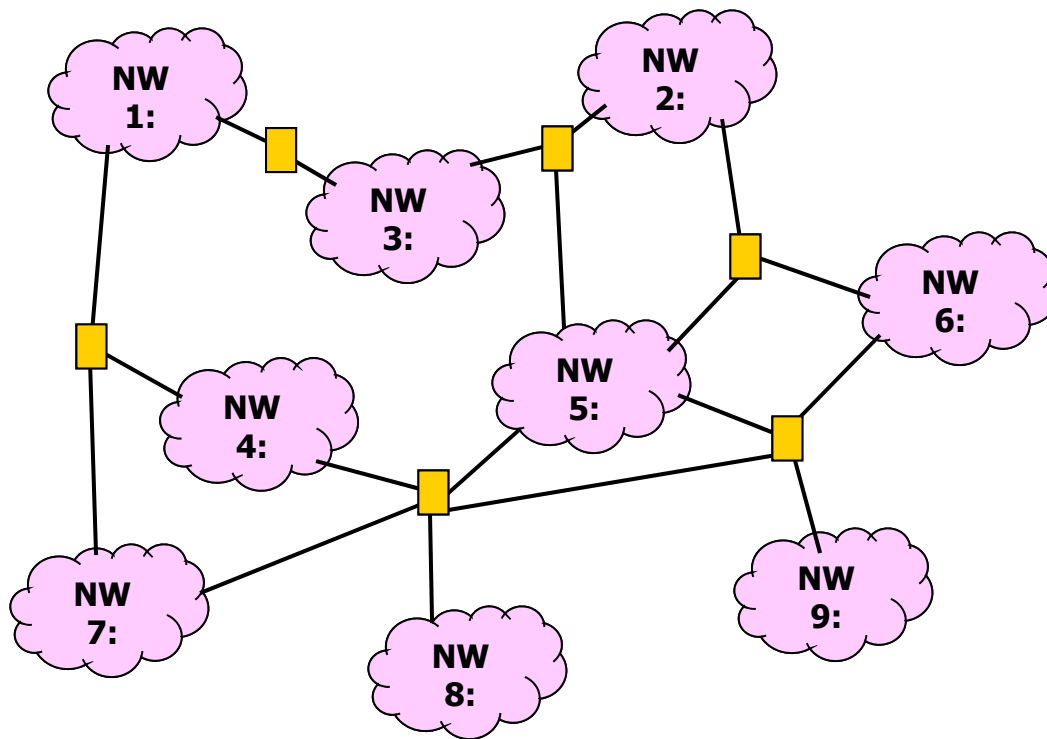


An internet ประกอบด้วย NW หลายๆตัว เชื่อมต่อกันผ่าน Router



Chapter 20: Internet Architecture

- มักจะใช้ **Partial Mesh** เพื่อสร้าง **Redundancy** ในการส่งข้อมูล



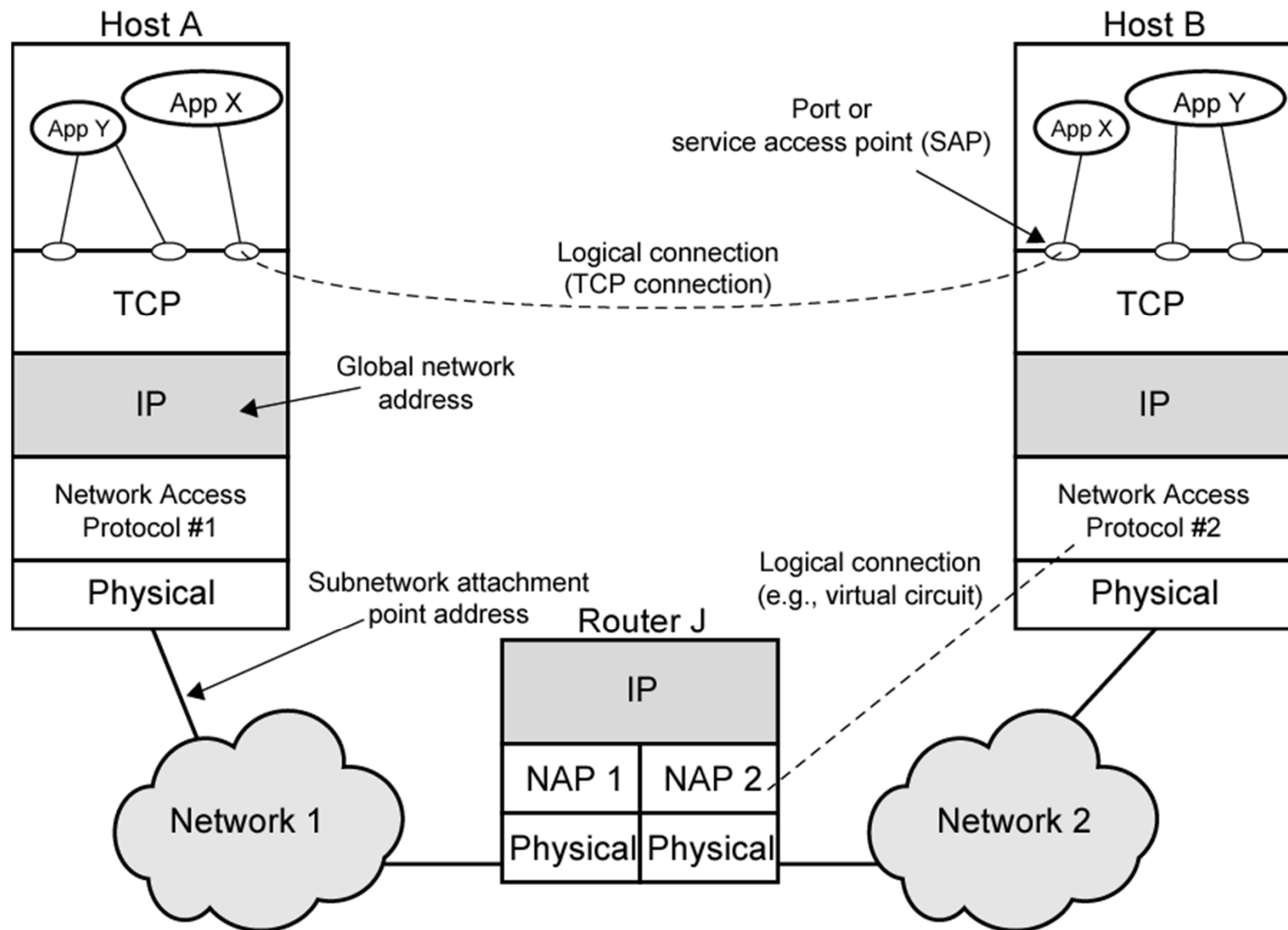


Internet Universal Service

- แม้ว่า Router จะมาช่วยแก้ปัญหาในการเชื่อมต่อระหว่าง Network
 - ปัญหายังคงอยู่ในการส่งข้อมูลผ่านระหว่าง Network เนื่องจาก Address ที่ใช้ในแต่ละ Network ต่างกัน
 - เราสามารถทำ Network Address Translation แต่จะยุ่งยาก
 - เราต้องการ Protocol กลางที่จะสามารถเชื่อมต่อคอมพิวเตอร์ต้นทาง ผ่าน Router ไปยังคอมพิวเตอร์ปลายทางที่ต่าง Network
 - Software Protocol นี้ต้อง Run ที่คอมพิวเตอร์ต้นทางและปลายทาง รวมถึงที่ Router ด้วย
 - Protocol ดังกล่าวจะใช้ Network Address ที่เป็น Universal สามารถบ่งบอกตำแหน่งอุปกรณ์ทั้งต้นทางและปลายทาง
 - Packet และรับข้อมูลส่งให้ลำดับชั้นบนของ Internet Protocol จนถึง Application Layer



- แม้ว่า Router จะมาช่วยแก้ปัญหาในการเชื่อมต่อระหว่าง Network
 - การทำงาน
 - ที่ PC ต้นทาง จะ Run Internet Protocol ที่กล่าว จากนั้นเมื่อส่งข้อมูลผ่าน Network1 จะส่ง Packet ของ Protocol นั้น ผ่าน Network Protocol ที่มันเชื่อมต่ออยู่ไปยัง Router (บางที่เราเรียกว่าเป็นการทำ Tunneling)
 - ที่ Router เมื่อได้รับ Packet จะปลดออก Network Protocol ที่เชื่อมต่อออก จนเหลือ Internet Protocol จากนั้นจะใช้ Address ของ Internet Protocol ทำการหาเส้นทางเพื่อส่งข้อมูลต่อออกไปยัง Interface ที่ถูกต้อง ซึ่งจะ Run Network Protocol ที่อาจจะแตกต่างกัน ดังนั้นมันจะจับ Internet Packet ใส่ลงใน Protocol ของ Interface ที่เชื่อมต่อ นั้นส่งออกไป
 - ข้อมูลอาจจะต้องส่งผ่านหลาย Network และหลาย Router แต่ละช่วงเรียกว่า Hop จะมีการปลดออก Packet จนถึง Internet Protocol และประกอบด้วย Protocol ใหม่ตาม Interface ขาออกที่ต้องส่งออกไป
 - เมื่อข้อมูลถึงคอมพิวเตอร์ปลายทาง คอมพิวเตอร์ปลายทางจะปลดออก Packet จนถึง Internet Protocol จากนั้นจะตรวจสอบ Internet Packet และรับข้อมูลส่งให้ลำดับชั้นบนของ Internet Protocol จนถึง Application Layer



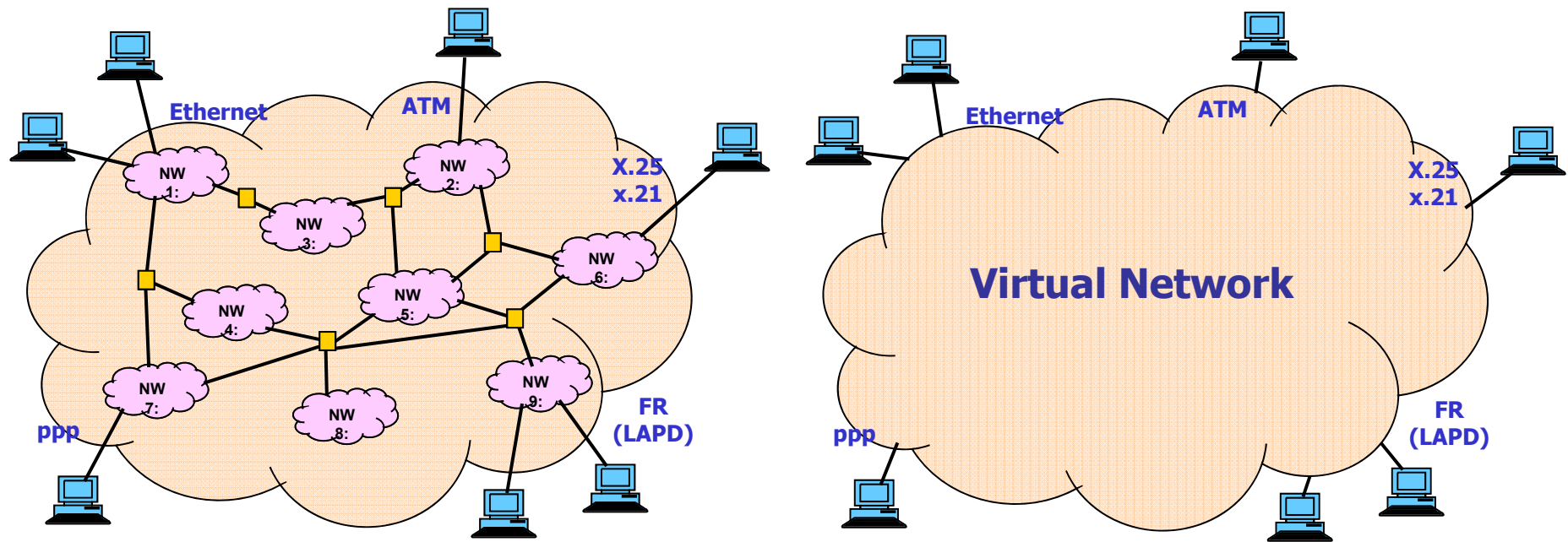


Virtual Network

- ลักษณะของ Internet Software ได้ถูกออกแบบมาเพื่อซ่อน Layer ที่อยู่ด้านล่าง
 - Layer ล่างจะเป็นอะไรก็ได้ (ปกติจะเป็น Protocol L2 หรือ L3) ผู้ใช้จะมองไม่เห็นและไม่ต้องสนใจ เพราะ Protocol เหล่านี้ใช้ในการทำ Network Access ในมุมมองของ Internet
 - Ethernet, HDLC, ppp, X.25, FR, ATM, ฯลฯ
 - ผู้ใช้แค่กำหนด Application ที่จะ Run และกำหนด Internet Address ปลายทางที่จะส่ง
 - การต่อกับ Internet ผู้ใช้เลือก Protocol ที่เหมาะสมที่จะไปเชื่อมต่อกับ Network ที่ต่ออยู่แล้วภายใน Internet
 - L1+L2+(L3)
 - นี่คือ Concept ของ Virtual Network



Virtual Network



Concept ของ The Internet คือถ้าเราต้องการต่อกับ Internet เราเลือก **Network Access Protocol** ที่เหมาะสม ทำการเชื่อมต่อกับ **Network** ที่ต่ออยู่แล้วใน Internet ในทางปฏิบัติ คงไม่มีใครที่อยากให้เราต่อพ่วงด้วย ดังนั้นจึงเกิด **ISP (Internet Service Provider)** ที่จะรับการเชื่อมต่อดังกล่าว โดยมีการคิดค่าบริการ



Internetworking Protocol

- แม้ว่ามึหลาย Protocol ที่ถูกเสนอขึ้นมา แต่มีเพียงชุดของ Protocol เดียวที่ได้รับความนิยมอย่างกว้างขวาง นั่นคือ ชุดของ Protocol TCP/IP
 - พัฒนาเริ่มจากปี 1970s ซึ่งเป็นเวลาเดียวกันกับที่ Ethernet ถูกพัฒนาขึ้นมา
 - ต่อมาในปี 1990s Protocol นี้ได้ถูกปล่อยและนำมาใช้ใน Commercial



TCP/IP Protocol Stack

OSI	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport (host-to-host)
Network	Internet
Data Link	Network Access
Physical	Physical

- ที่สำคัญคือ **Layer 3: Internet Protocol(IP)** ทำหน้าที่กำหนดรูปแบบของ **Packet** ที่จะส่งผ่านตลอดทั้ง **Network** โดยที่ส่วน **Address** ของ **Layer** นี้ (**IP Address**) จะถูกใช้โดย **Router** เพื่อที่จะทำการส่งข้อมูลผ่าน **Router** ที่เชื่อมต่อกัน จนกระทั่งถึงเครื่อง (**Host**) ปลายทาง ดังนั้น **Protocol** นี้จะต้องถูก **Run** ใน **Router** ทุกตัว รวมทั้ง **Host**
- **Layer 4: Transport Layer (Host-to-Host)** ที่สำคัญคือ **TCP** จะถูกใช้เพื่อที่จะให้แน่ใจว่าข้อมูลที่ส่งจากต้นทาง(**Host**) ไปถึงปลายทาง (**Host**) ได้อย่างถูกต้อง ซึ่ง **Protocol** นี้จะถูก **Run** ที่ **Host** ต้นทางและปลายทางเท่านั้น



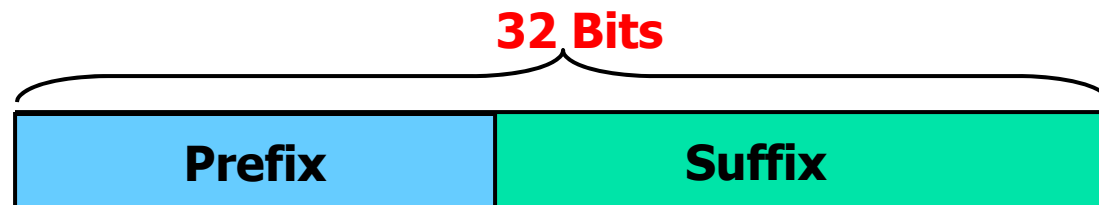
Chapter 21: IP Addressing

- **IP Address เป็นตัวกำหนด End System (Host) ตลอดทั้งเครือข่าย Internet**
 - ดังนั้นมันจะต้องเป็น Global Address ขณะที่ MAC Address จะหมดอายุเมื่อออกจาก LAN
 - เป็นแค่ Local Address ใน LAN
 - เครื่องสองเครื่องในเครือข่าย จะมีหมายเลขเดียวกันไม่ได้
 - เครื่องที่ต่อใน LAN ออก Internet จะมีทั้ง MAC Address และ IP Address ที่ Match กัน
 - Protocol ARP จะกล่าวในบทที่ 23
- **ปัจจุบันใช้ตามมาตรฐานของ IPv4**
 - Address ขนาด 32 บิต
 - เรียก IP Address, Internet Address หรือ Internet Protocol Address
 - กำหนดหมายเลขเครื่องได้โดยไม่เกี่ยวข้องกับ MAC Address



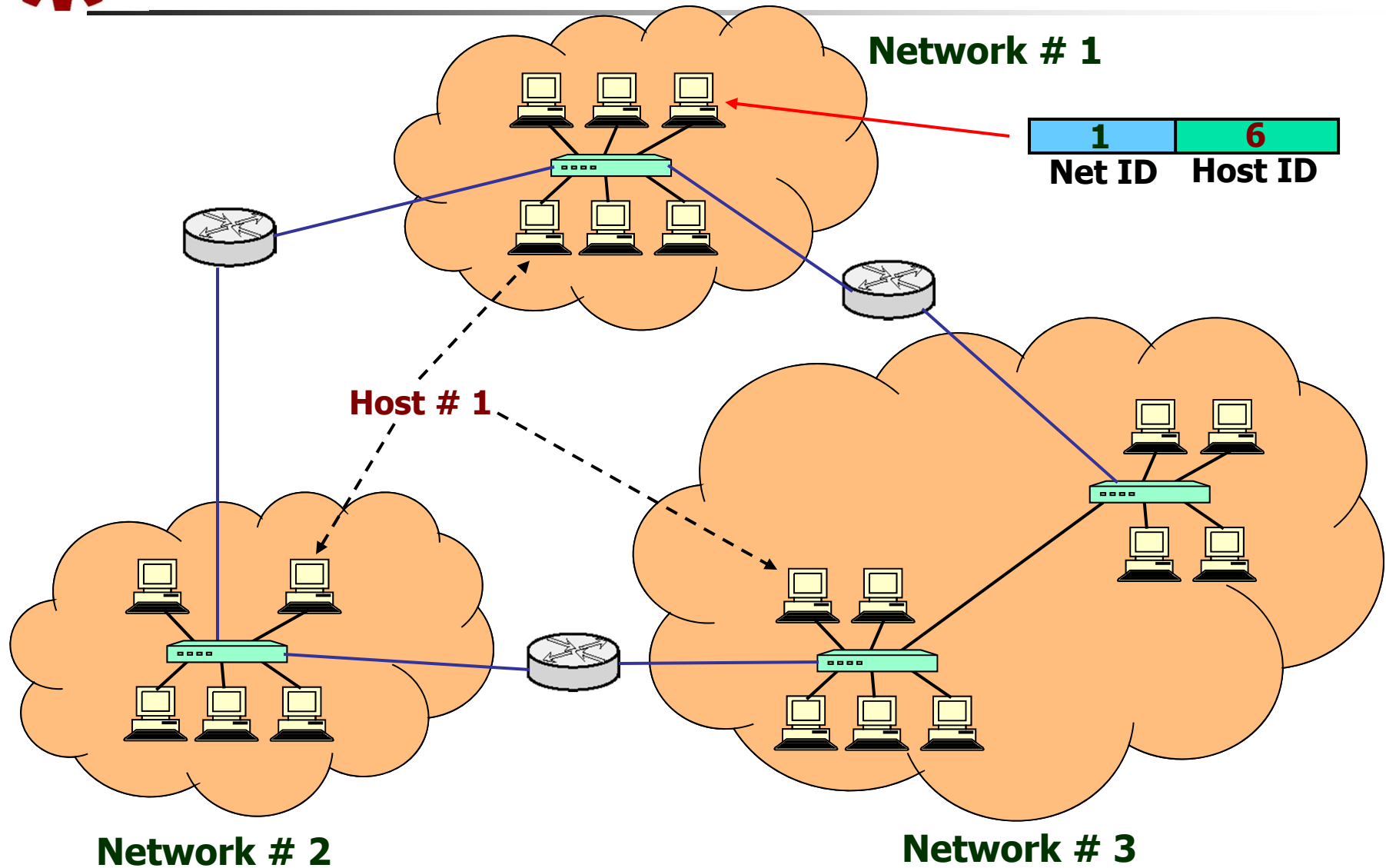
Ch. 21: 21.4 IP Address Hierarchy

- แต่ละ IP Address ขนาด 32 บิต จะถูกแบ่งออกเป็นสองส่วน
 - ส่วนต้น เรียก Prefix เป็นตัวกำหนดหมายเลข Network (Network ID)
 - ส่วนที่เหลือ เรียก Suffix เป็นตัวกำหนดหมายเลข Host ใน Network นั้นๆ
 - หมายเลข Host ใน Network เดียวกันจะซ้ำกันไม่ได้
 - หมายเลข Host ที่อยู่คนละ Network สามารถซ้ำกันได้ เพราะส่วน Prefix (Net ID) นั้นไม่เหมือนกัน





Ch. 21: 21.4 IP Address Hierarchy





Ch. 21: 21.5 Original Classful IP Addressing

- เราควรกำหนดกี่บิตเป็น **Prefix** และ **Suffix**
 - จำนวน = 2bit ที่ใช้กำหนด ทั้ง Prefix และ Suffix
 - Prefix มากเกินไป ทำให้จำนวน Suffix Bit มีน้อย ไม่พอรองรับจำนวน Host ใน Network ขนาดใหญ่
 - Prefix น้อยไป จำนวน Network ใน Internet มีได้น้อย ไม่เพียงพอในการทำงาน
 - เนื่องจาก Network มีขนาดหลากหลาย จึงกำหนด 4 บิตแรก บ่งบอก Class ของ IP Address ซึ่งจะเป็นการกำหนดจำนวนบิตที่เป็นทั้ง Prefix และ Suffix
 - Class A-C ใช้ปกติ
 - Class D สำหรับทำ Multicast (ไม่มี Prefix และ Suffix)
 - Class E Reserved



Ch. 21: 21.5 Original Classful IP Addressing

	bits	0	1	2	3	4	8	16	24	31
Class A		0	prefix				suffix			
Class B		1	0	prefix						suffix
Class C		1	1	0	prefix					suffix
Class D		1	1	1	0	multicast address				
Class E		1	1	1	1	reserved (not assigned)				

Figure 21.1 The five classes of IP addresses in the original classful scheme.



Ch. 21: 21.6 Dotted Decimal Notation

- ใน 32 บิต IP Address จะถูกแบ่งเป็นส่วนสี่ ส่วน ส่วนละ 8 บิต
 - แต่ละส่วนจะเขียนเป็นเลขฐาน 10 มีค่าได้ระหว่าง 0 – 255
 - แต่ละส่วนจะเขียนต่อกัน ขึ้นด้วย “จุด”
- เรียก Dotted Decimal Notation
 - Address ต่ำสุดคือ 0.0.0.0
 - Address สูงสุดคือ 255.255.255.255
 - แต่ละ Class สามารถสังเกตได้จาก Octet แรกของ IP Address



Ch. 21: 21.6 Dotted Decimal Notation

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

Figure 21.2 Examples of 32-bit binary numbers and their equivalent in dotted decimal notation.



Ch. 21: 21.7 Division of Address Space

- สังเกตว่า แม้ว่า Class A จะมีแค่ 128 Network แต่มันประกอบด้วยครึ่งหนึ่งของ Address Space ทั้งหมด

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Figure 21.3 The number of networks and hosts per network in each of the original three primary IP address classes.



Ch. 21: 21.8 Authority for Address

- องค์การที่ดูแลจัดการเรื่อง IP Address คือ ICANN
 - Internet Corporation for Assigned Names and Numbers
- ปกติ ICANN จะกำหนดให้ Registrar เป็นผู้จัดสรรในแต่ละภูมิภาคอีกทีหนึ่ง
- Registrar จะจัดสรร Block ของ IP Address ให้แก่ ISP แต่ละราย
 - ผู้ใช้งานจะได้รับ IP Address จาก ISP อีกที



Summary of IP Classful

	octet 1	octet 2	octet 3	octet 4	Range of addresses
	Network ID		Host ID		
Class A:	1 to 127	0 to 255	0 to 255	0 to 255	1.0.0.0 to 127.255.255.255
	Network ID		Host ID		
Class B:	128 to 191	0 to 255	0 to 255	0 to 255	128.0.0.0 to 191.255.255.255
	Network ID		Host ID		
Class C:	192 to 223	0 to 255	0 to 255	1 to 254	192.0.0.0 to 223.255.255.255
	Multicast address				
Class D (multicast):	224 to 239	0 to 255	0 to 255	1 to 254	224.0.0.0 to 239.255.255.255
Class E (reserved):	240 to 255	0 to 255	0 to 255	1 to 254	240.0.0.0 to 255.255.255.255



- **END of Week 3**
- **Download HW 2: WK 3**
- **พิมพ์ผลงานกระดาษ A4**
- **ทำการบ้านลงในช่องที่กำหนด**
- **ส่งสัปดาห์หน้า ต้นชั่วโมง**