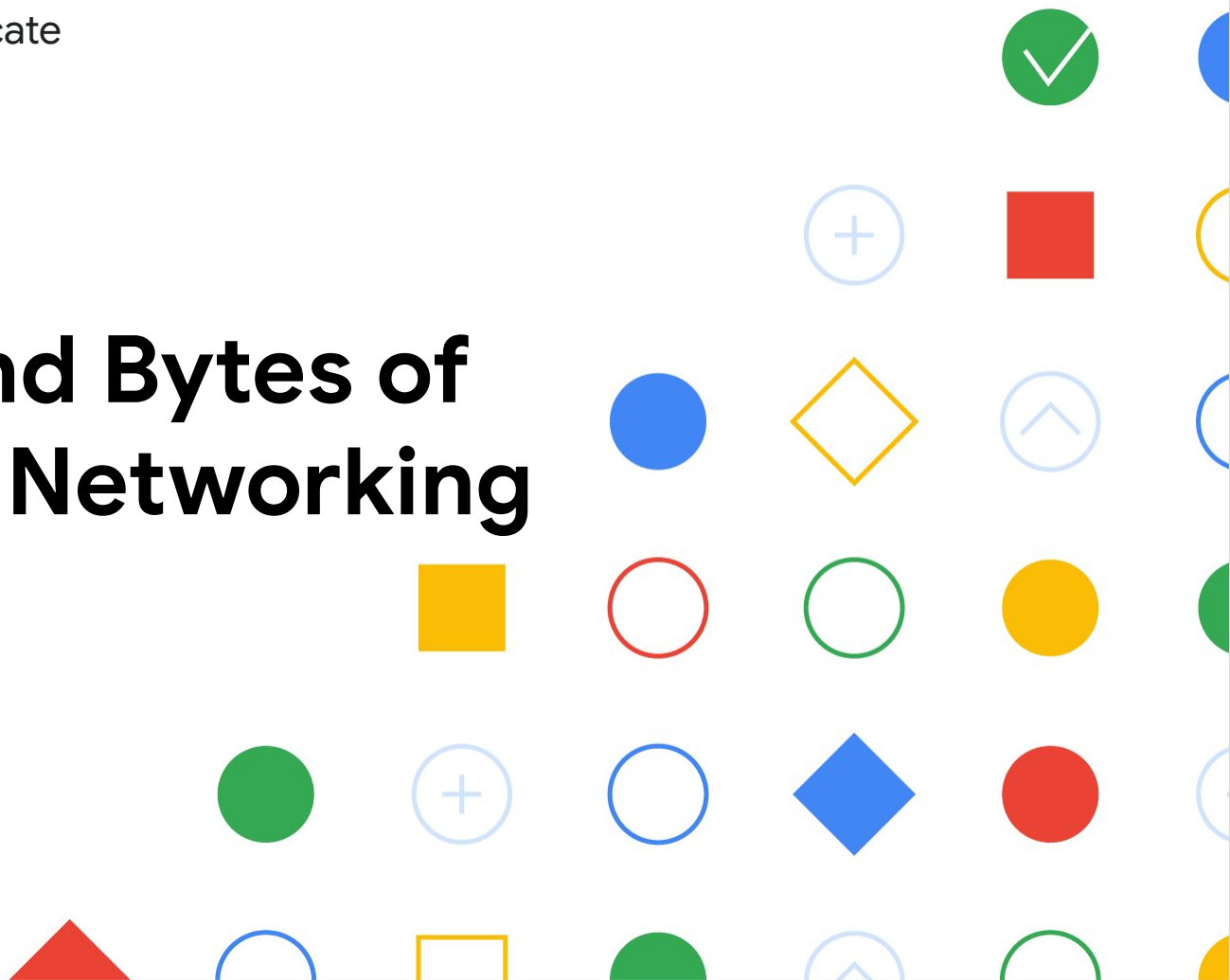
Google IT Support Certificate

The Bits and Bytes of Computer Networking

Course 2



Samart Skills
A Grow with Google PROGRAM

Skooldio

Overview:

01
Introduction to Networking

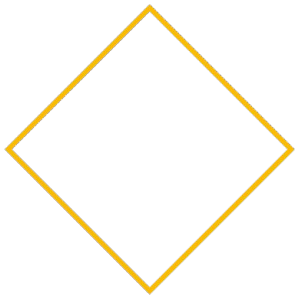
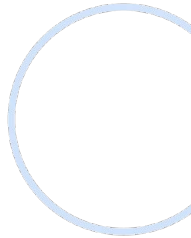
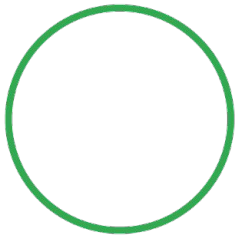
02
The Network Layer

03
The Transport and Application Layers

04
Networking Services

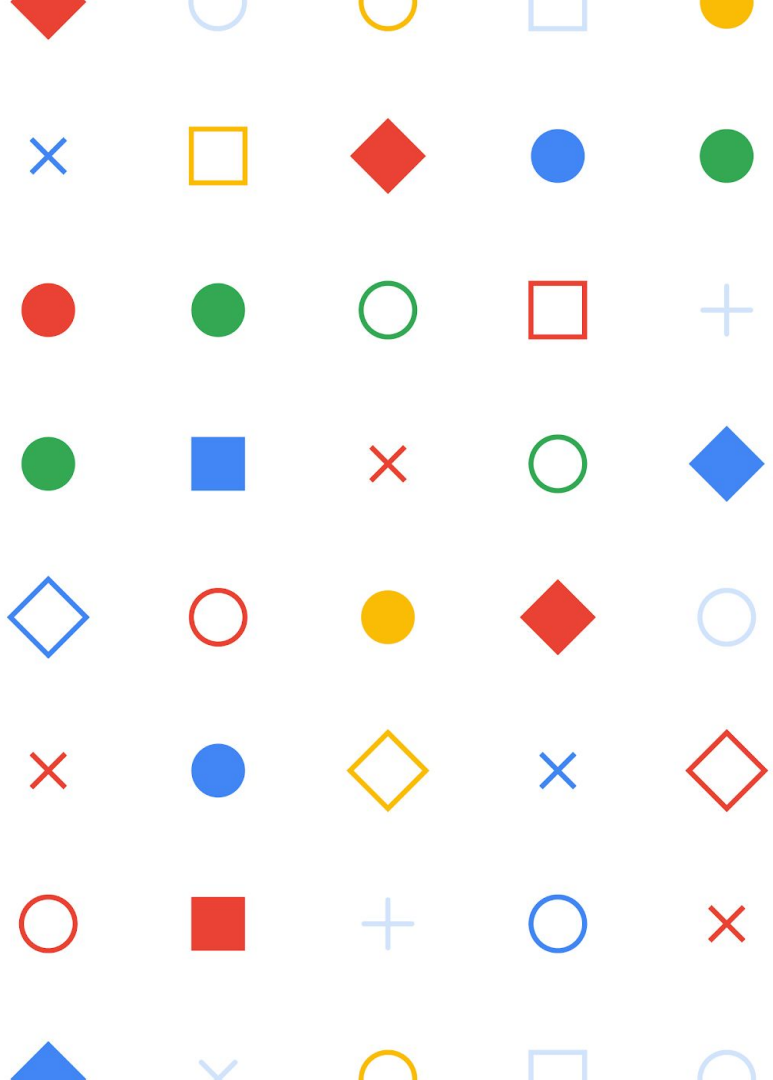
05
Connecting to the Internet

06
Troubleshooting and
the Future of Networking


Week 1

Introduction to Networking



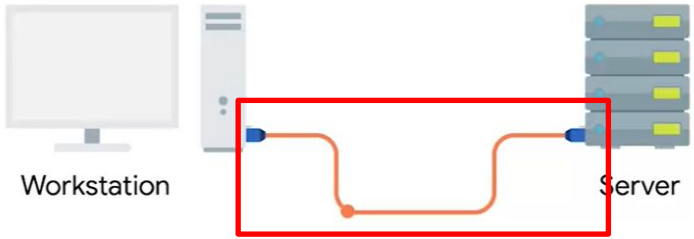
Samart Skills
A Grow with Google PROGRAM

Skooldio

The TCP/IP Five-Layer Network Model

#	Layer Name	Protocol	Protocol Data Unit	Addressing	Components
5	Application	HTTP, SMTP, etc..	Messages	n/a	Web browser
4	Transport	TCP/UDP	Segment	Port #'s	Client/Server
3	Network	IP	Datagram	IP address	Router
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address	Switch
1	Physical	10 Base T, 802.11	Bits	n/a	Ethernet cable

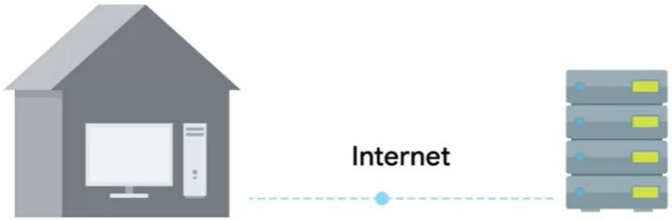
The TCP/IP Five-Layer Network Model



Physical Layer ทำหน้าที่เชื่อมต่อ Physical Devices เข้าด้วยกัน

- กำหนดรายละเอียดของสายสัญญาณ (Cables) และตัวเชื่อมต่อ (Connector) รวมถึงกำหนดวิธีการส่งสัญญาณ (Signals) บนการเชื่อมต่อ

The TCP/IP Five-Layer Network Model



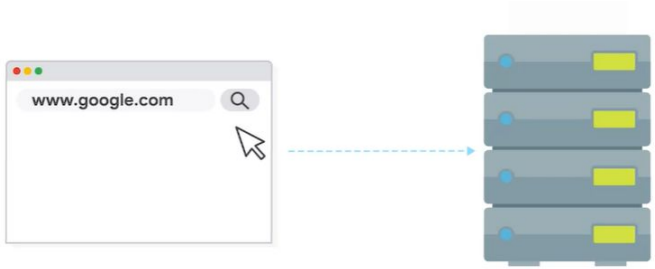
Data Link Layer ทำหน้าที่กำหนดวิธีการแปลความหมายของสัญญาณ (Interpret Signals) เพื่อให้ Network Devices สามารถสื่อสารกันได้

- **Protocol** คือ ชุดของมาตรฐานหรือกฎที่จะทำให้คอมพิวเตอร์สามารถสื่อสารกันได้
- **Ethernet** เป็น Protocol ที่ใช้สำหรับการเชื่อมต่อแบบมีสาย (Wired Connection)

Network Layer ทำหน้าที่ทำให้ Network ที่แตกต่างกันสามารถติดต่อกันได้ผ่านอุปกรณ์ที่เรียกว่า Router

- IP เป็น Protocol หลักบน Network Layer

The TCP/IP Five-Layer Network Model



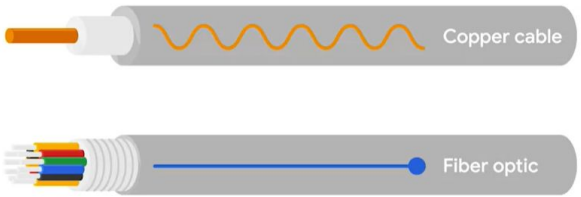
Transport Layer ทำหน้าที่จัดเรียงข้อมูล (Sorting) ที่โปรแกรม Client และ Server จะต้องได้รับ และทำให้ข้อมูลถูกส่งไปถึง Application ที่ต้องการได้

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Application Layer ทำหน้าที่จัดการให้ Application บนเครื่องคอมพิวเตอร์ต่างๆ สามารถสื่อสารกันได้ และเป็นส่วนเชื่อมต่อ (Interface) ระหว่าง Application และผู้ใช้งาน (Users)

- ตัวอย่าง Protocol: HTTP, FTP, DNS, DHCP

The Basics of Networking Devices



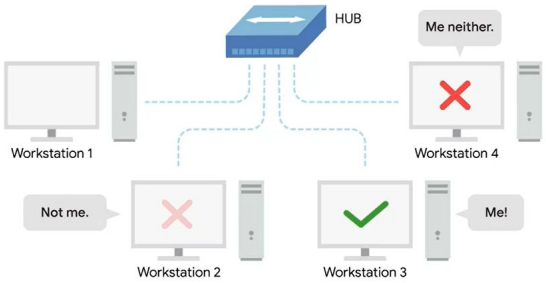
สายสัญญาณ (Cables) ทำหน้าที่เชื่อมต่อ Devices ต่าง ๆ เข้าด้วยกันทำให้ข้อมูลถูกส่งถึงกันได้

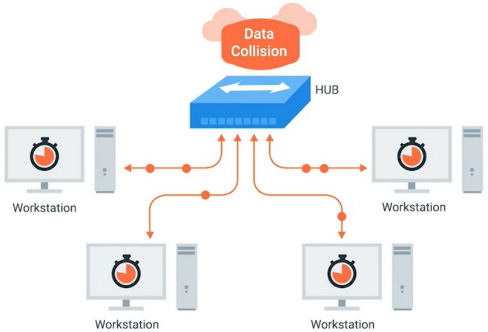
- สายทองแดง (Copper) ใช้สัญญาณไฟฟ้าในการส่งข้อมูล ใช้สำหรับระยะใกล้

สายใยแก้วนำแสง (Fiber) ใช้แสงในการส่งข้อมูล

- ใช้สำหรับระยะไกล

The Basics of Networking Devices



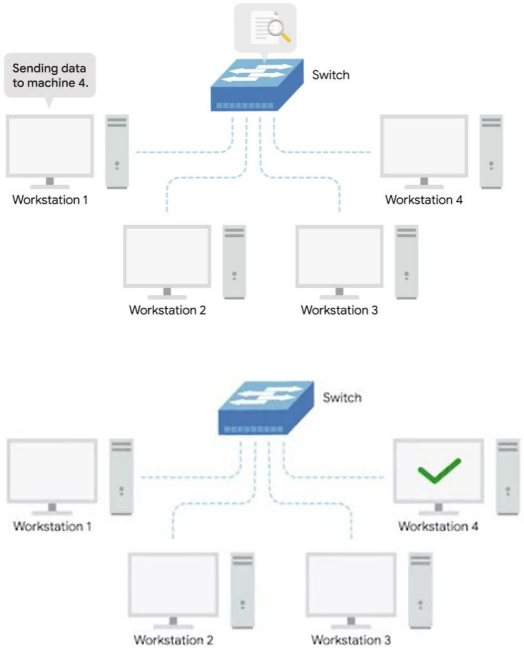


Hub เป็น Physical Layer Device ที่ประกอบด้วยช่องเสียบ (Network Ports) หลายช่อง ทำให้เราสามารถเชื่อมต่อคอมพิวเตอร์หลายเครื่องเข้าด้วยกันได้

Collision Domain คือ ส่วนของ Network ที่การรับส่งข้อมูลสามารถถูกรบกวนได้ ทำให้มีเพียงหนึ่งอุปกรณ์เท่านั้นที่สามารถสื่อสารได้ ณ เวลานั้น

- หากมีมากกว่าหนึ่งอุปกรณ์ส่งข้อมูล ณ เวลาเดียวกัน จะทำให้ข้อมูลเกิดการชนกันและทำให้ข้อมูลนั้นเสียหาย
- ทำให้ประสิทธิภาพในการสื่อสารช้าลง

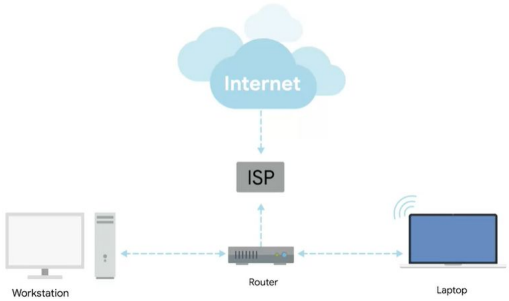
The Basics of Networking Devices

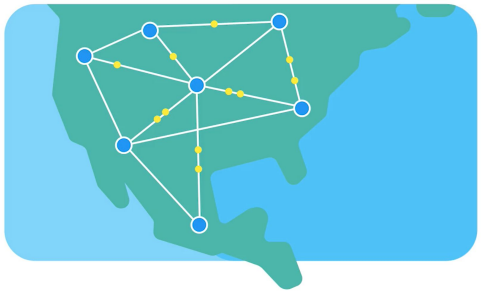


Switch เป็น Data Link Layer Device ที่ทำหน้าที่คล้าย Hub แต่ Switch สามารถวิเคราะห์และเลือกส่งข้อมูลไปให้เฉพาะเครื่องที่เกี่ยวข้องได้

- ช่วยลดขอบเขตของ Collision Domain ใน Network

The Basics of Networking Devices



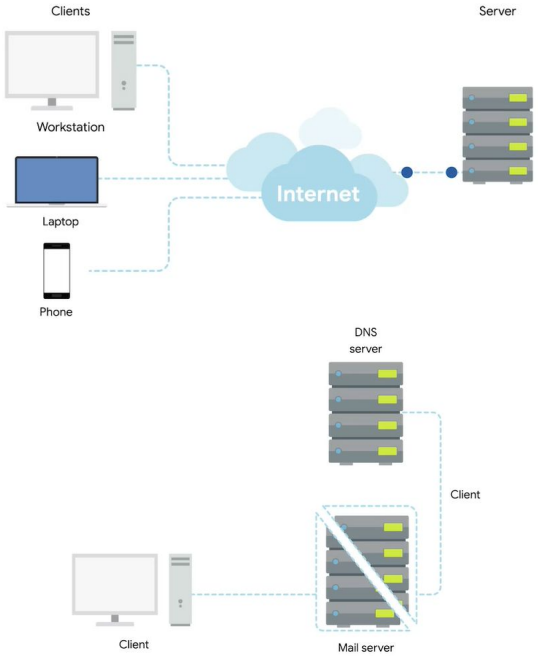


Hub และ Switch จะเชื่อมต่ออุปกรณ์ใน Network เดียวกันเท่านั้น

Router เป็น Network Layer Device ที่รู้วิธีการส่งต่อข้อมูลไปยัง Network อื่นได้ ทำให้สามารถเชื่อมต่ออุปกรณ์ข้าม Network ที่แตกต่างกันได้

- **Border Gateway Protocol (BGP)** ใช้สำหรับ Router ในการแชร์ข้อมูลเกี่ยวกับเส้นทางที่ดีที่สุด (Optimal Path) ที่จะใช้ในการส่งต่อข้อมูล

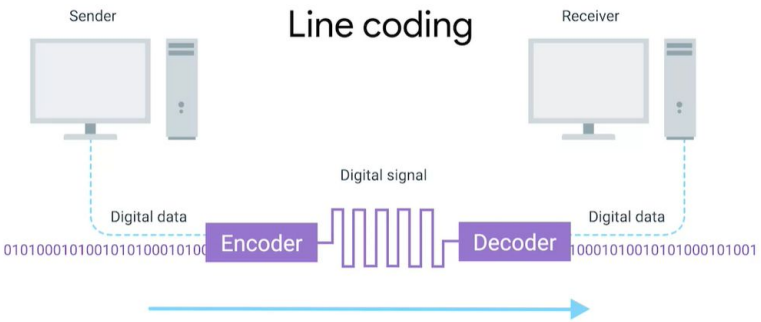
The Basics of Networking Devices



Nodes คือ อุปกรณ์ที่สามารถสื่อสารกันได้

- **Servers** คือ Node ที่ให้ข้อมูลหรือบริการ
- **Clients** คือ Node ที่ร้องขอข้อมูลหรือบริการ

The Physical Layer

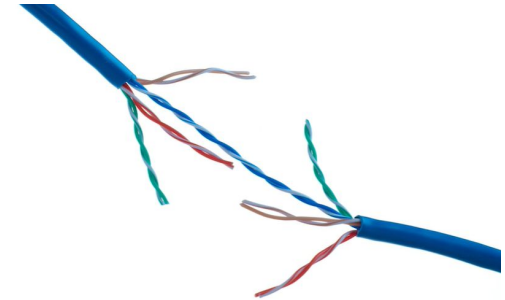


Bit คือ ข้อมูลที่เล็กที่สุดที่คอมพิวเตอร์สามารถเข้าใจได้ ซึ่งก็คือ 0 กับ 1

Modulation คือ กระบวนการในการส่งค่า 0 และ 1 ผ่าน Cable ซึ่งอาศัยการเปลี่ยนแปลงของ Voltage

- เราจะเรียก Modulation ที่ถูกนำมาใช้ใน Computer Network ว่า Line Coding

The Physical Layer

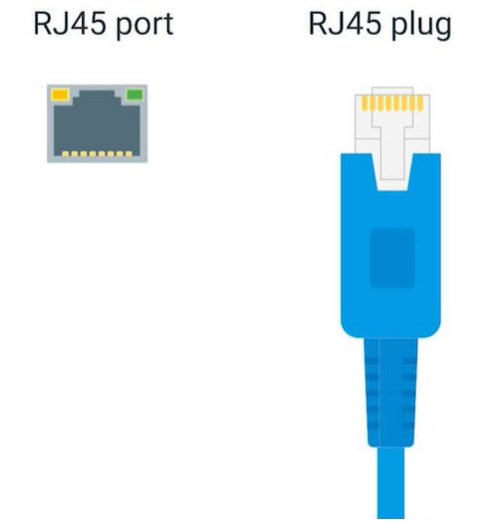


Twisted Pair Cables (สายคู่บิดเกลียว) เป็นคู่สายที่ทำมาจากทองแดง (Copper) แล้วนำมาบิดเกลียวเข้าด้วยกันเพื่อช่วยในการป้องกันคลื่นรบกวนและ Crosstalk จากคู่สายข้างเคียง

- **Crosstalk** เกิดขึ้นเมื่อสัญญาณไฟฟ้าบนสายหนึ่งถูกตรวจจับได้บนอีกสายหนึ่งโดยบังเอิญ

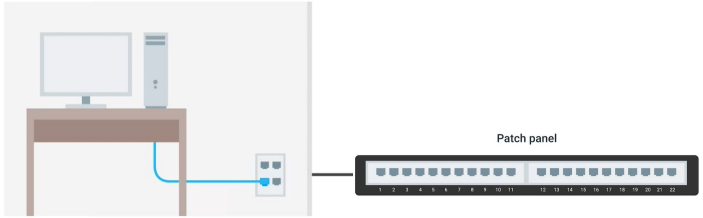
สายมาตรฐาน Category 6 (Cat 6) จะมีสายทองแดงบิดเกลียวทั้งหมด 4 คู่ (8 เส้น) อยู่ภายใต้ปลอก (Jacket)

The Physical Layer



RJ45 (Registered Jack 45) เป็น Network Port (ช่องเสียบ) และ Plug (เต้าเสียบ) ที่นิยมใช้ในการสิ้นสุดของสาย Twisted Pair

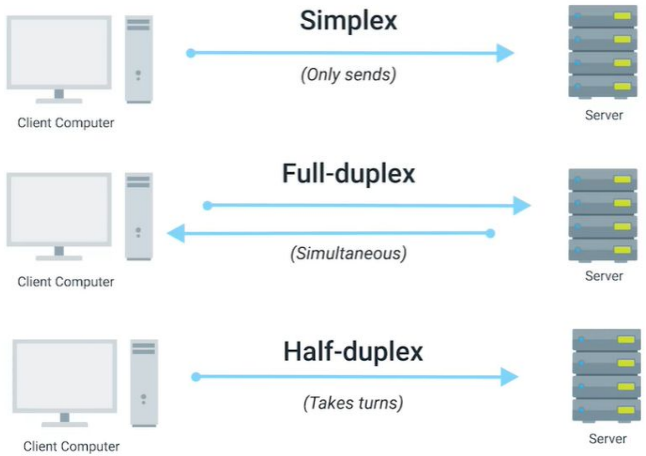
The Physical Layer



Patch Panel เป็นอุปกรณ์ที่ประกอบด้วย Ports จำนวนมาก เช่น 48 ports เป็นต้น

- Patch Panel ไม่ได้ทำหน้าที่อะไรเป็นพิเศษ ทำเพียงแค่เชื่อมต่อคอมพิวเตอร์ไปยัง Switch หรือ Router ที่อยู่อีกปลายของสายเท่านั้น

The Physical Layer



Simplex Communication คือ การสื่อสารข้อมูลแบบทิศทางเดียว ตัวอย่างเช่น Baby Monitor, วิทยุ (Radio)

Duplex Communication คือ การสื่อสารข้อมูลแบบสองทิศทาง ตัวอย่างเช่น การคุยโทรศัพท์ (Phone Call)

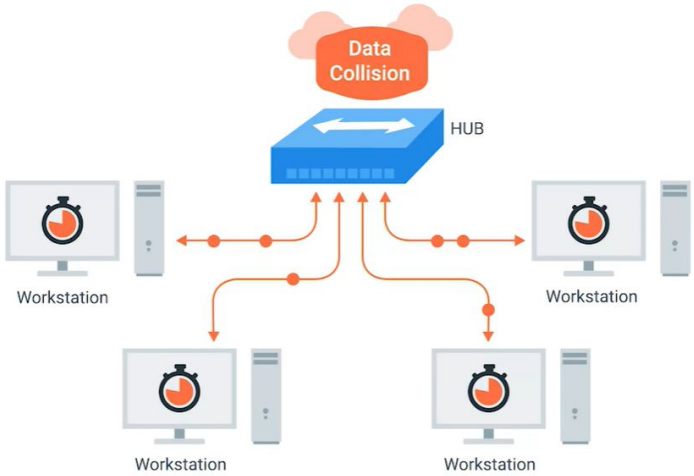
- **Full-duplex** คือ การที่อุปกรณ์ทั้งสองฝั่งสามารถสื่อสารพร้อมกันได้ ณ เวลาใดเวลาหนึ่ง
- **Half-duplex** คือ การที่อุปกรณ์ฝั่งเดียวเท่านั้นที่สามารถสื่อสารได้ ณ เวลาใดเวลาหนึ่ง

The Data Link Layer

Data Link Layer ทำหน้าที่กำหนดวิธีการแปลความหมายของสัญญาณ (Interpret Signals) เพื่อให้ Network Devices สามารถติดต่อกันได้

- Data Link Layer ทำให้ Layer อื่น ๆ ที่อยู่เหนือขึ้นไปนั้น ไม่ต้องสนใจว่าอุปกรณ์นั้นใช้ Hardware อะไรอยู่ (Abstraction) เช่น Web Browser ไม่จำเป็นต้องรู้ว่าอุปกรณ์เชื่อมต่อกับสาย Twisted Pair หรือ Fiber
- ข้อมูลบน Data Link Layer จะถูกเรียกว่า **Frame**

The Data Link Layer



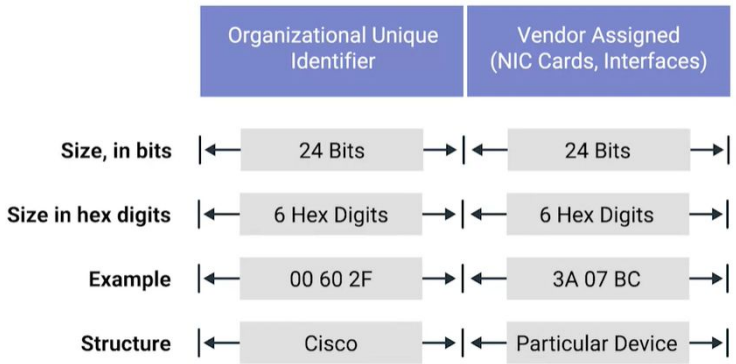
Ethernet เป็น Protocol บน Data Link Layer ที่ใช้ในการส่งข้อมูลใน Network ที่มีการเชื่อมต่อแบบมีสาย (Wired Connection)

- **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) เป็นเทคนิคที่ช่วยแก้ปัญหาเรื่องการชนกันของข้อมูล (Collision)

The Data Link Layer

00:60:2F:3A:07:BC

Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15



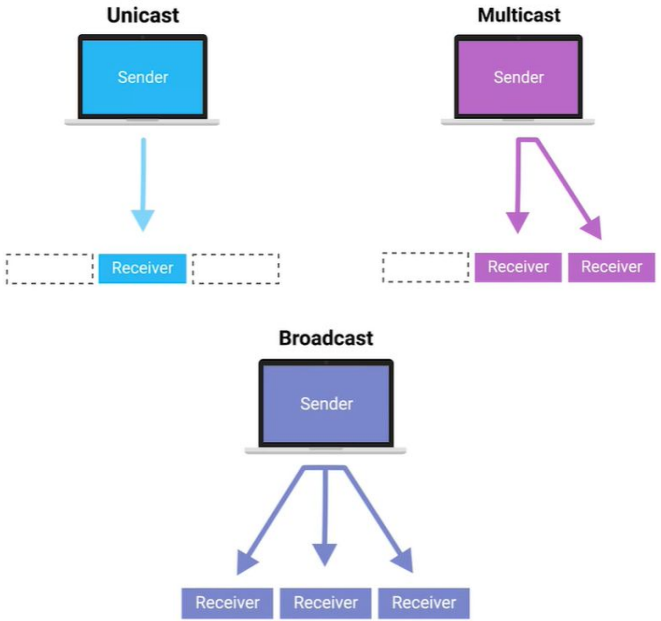
Media Access Control Address (MAC Address) เป็นตัวระบุที่เป็นเอกลักษณ์ (Unique Identifier) ที่ถูกฝังอยู่บน Network Interface

- เป็นเลข 48-bit ที่ถูกจัดอยู่ในรูปแบบของเลขฐานสิบหก (Hexadecimal) 2 หลัก จำนวน 6 ชุด หรืออาจเรียกได้ว่ามี 6 octets
- ความเป็นไปได้ของ MAC Address ทั้งหมดคือ 2^{48}

MAC Address สามารถถูกแบ่งได้เป็น 2 ส่วน

- 3 octets แรก จะเรียกว่า **Organizationally Unique Identifier (OUI)** ซึ่งจะบอกถึงผู้ผลิต Network Interface ชิ้นนั้น
- 3 octets หลัง จะเรียกว่า **Vendor Assigned** ซึ่งจะเป็นเลขที่ผู้ผลิตเป็นผู้ระบุให้ โดยแต่ละ Network Interface จะต้องมีเลขที่ไม่ซ้ำกัน (Unique)

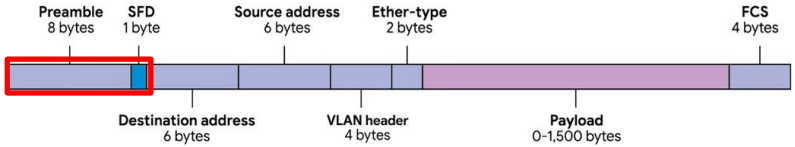
The Data Link Layer



Type of Transmission

- **Unicast** คือ การส่งข้อมูลไปหาผู้รับเพียงแค่เครื่องเดียว
  - ถ้า Least Significant Bit (Special Bit) ใน Octet แรกของ Destination Address มีค่าเป็น “0” แสดงว่า Frame นี้ถูกส่งมาสำหรับ Destination Address นั้นเท่านั้น
- **Multicast** คือ การส่งข้อมูลไปหาผู้รับหลายเครื่อง
  - ถ้า Least Significant Bit (Special Bit) ใน Octet แรกของ Destination Address มีค่าเป็น “1” แสดงว่า Frame นี้ถูกส่งมาสำหรับหลาย Destination Addresses
- **Broadcast** คือ การส่งข้อมูลไปหาผู้รับทุกเครื่องใน Network เดียวกัน
  - Broadcast Address คือ FF:FF:FF:FF:FF:FF

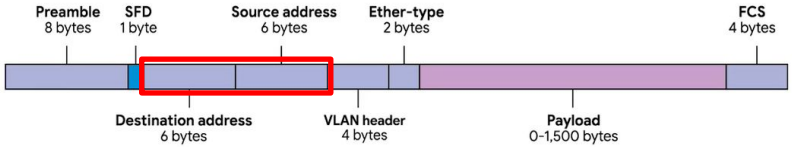
The Data Link Layer



ข้อมูลใน Ethernet จะเรียกว่า Ethernet Frame ซึ่งประกอบด้วยข้อมูลต่าง ๆ ที่ถูกจัดเรียงไว้ตามลำดับดังนี้

- **Preamble**: มีความยาว 8 bytes (64-bit) ใช้ในการบอกเครื่องผู้รับว่า Ethernet Frame กำลังเข้ามา ซึ่งถูกแบ่งเป็น 2 ส่วน
  - 7 bytes แรก คือ ชุดข้อมูล 1 และ 0 ที่สลับกันไปมา เอาไว้ใช้เป็น Buffer ระหว่าง Frame นอกจากนั้นยังใช้ในการ Synchronize Clock เพื่อปรับความเร็วในการส่งข้อมูลด้วย
  - 1 byte หลัง เรียกว่า Start Frame Delimiter (SFD) คือ สัญญาณที่เครื่องผู้รับว่า Preamble สิ้นสุดลงและเนื้อหา Frame จะเริ่มหลังจากนี้

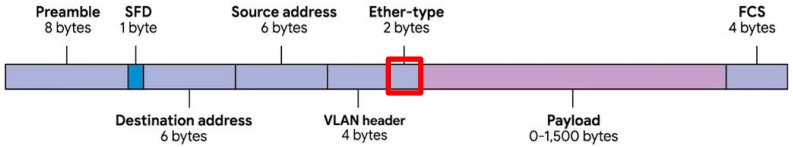
The Data Link Layer

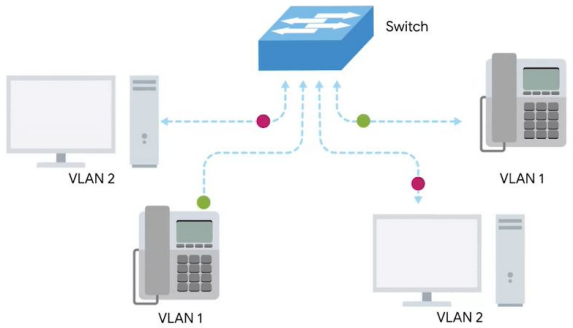


Destination Address คือ MAC Address ของเครื่องผู้รับ มีความยาว 6 bytes (48-bit)

Source Address คือ MAC Address ของเครื่องผู้ส่ง มีความยาว 6 bytes (48-bit)

The Data Link Layer





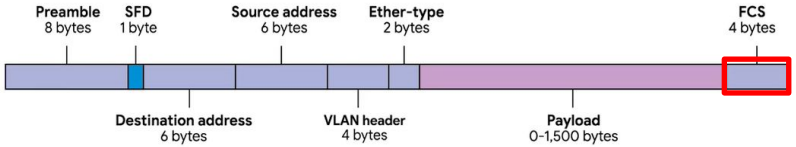
Ether-type: มีความยาว 2 bytes (16-bit) ใช้ในการบอกว่าเนื้อหา Frame เป็น Protocol อะไร

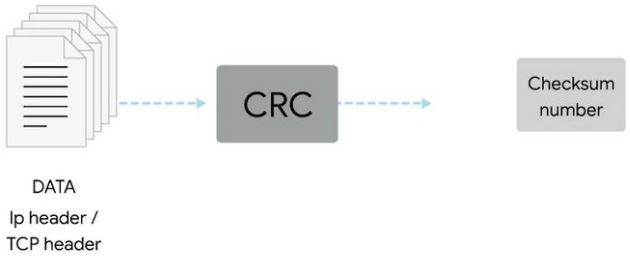
VLAN Header: มีความยาว 4 bytes (32-bit) ใช้ในการบอกว่า Frame เป็น VLAN Frame หรือไม่

- ถ้ามี VLAN Header ปรากฏอยู่ใน Ethernet Frame แล้ว ต่อไปจะตามด้วย Ether-type Field
- VLAN (Virtual LAN) เป็นเทคนิคที่ทำให้เรามีหลาย LANs ได้โดยใช้บนอุปกรณ์เดียวกัน

Payload คือ ข้อมูลจริงที่จะถูกส่งไป ซึ่งก็คือข้อมูลของ Layer อื่น ๆ ที่อยู่เหนือ Data Link Layer

The Data Link Layer



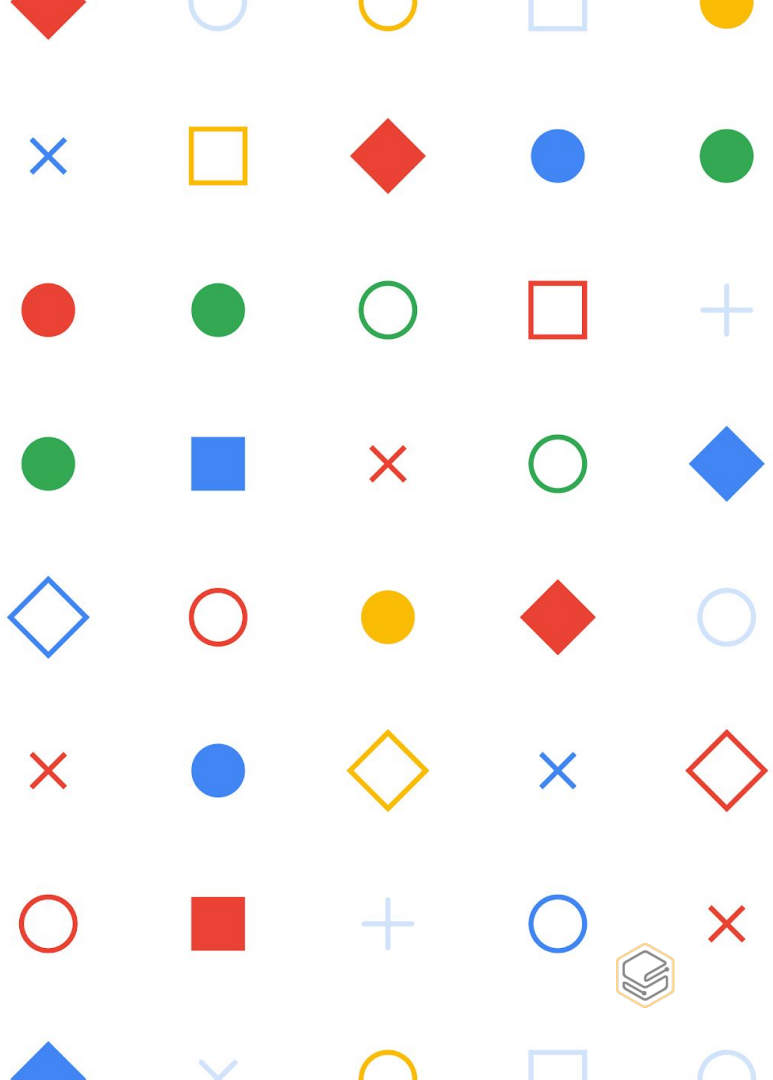


Frame Check Sequence (FCS) มีความยาว 4 bytes (32-bit) เป็นเลขที่แสดงค่าผลรวมตรวจสอบ (Checksum) สำหรับทั้ง Frame นั้น

- **Checksum** คือ ค่าที่ถูกคำนวณโดยการนำ Frame ไปเข้าวิธีการคำนวณที่เรียกว่า Cyclical Redundancy Check (CRC)
  - ใช้ในการตรวจสอบความถูกต้องสมบูรณ์ของข้อมูล (Data Integrity)
  - ถ้าหากเครื่องผู้รับคำนวณค่า Checksum ได้ไม่ตรงกับค่าใน FCS ที่ส่งมา เครื่องผู้รับจะทิ้ง Frame นั้น

Week 2

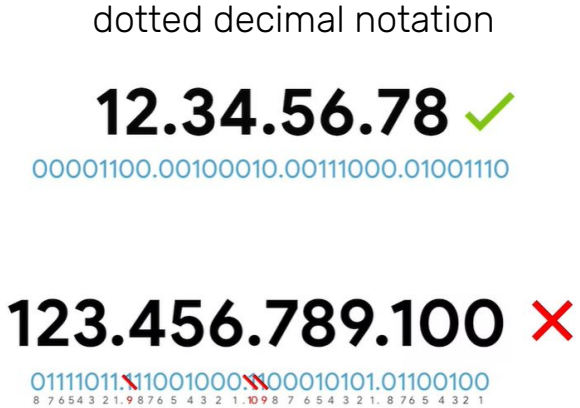
The Network Layer



Samart Skills
A Grow with Google PROGRAM

Skooldio

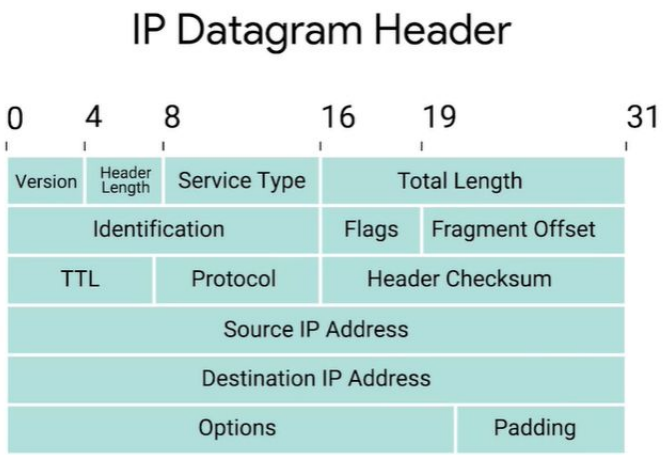
The Network Layer



IP Addresses เป็นเลขความยาว 32 bits ถูกแบ่งเป็น 4 octets โดยแต่ละ octet (8-bit) สามารถเขียนเป็น Decimal ได้ตั้งแต่ 0-255

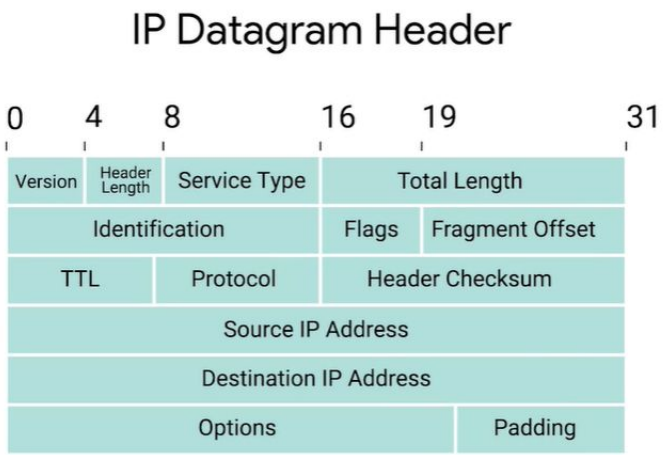
- IP Addresses เป็นของ Network ไม่ใช่ของอุปกรณ์ ซึ่ง IP Addresses จะแตกต่างกันเมื่อเชื่อมต่อ Network ที่ต่างกัน
- Dynamic IP Address □ DHCP
- Static IP Address □ manually

The Network Layer



- ภายใต้ IP Protocol ข้อมูลจะถูกเรียกว่า **IP Datagram**
- IP Datagram Header ประกอบด้วยข้อมูลต่าง ๆ ดังนี้
  - **Version**: มีความยาว 4 bits เอาไว้บอก Version ของ IP ซึ่งส่วนมากจะใช้ IP Version 4 (IPv4)
  - **Header Length**: มีความยาว 4 bits เอาไว้บอกความยาวของ Header ซึ่งโดยปกติจะเป็น 20 bytes หากใช้ IPv4
  - **Service Type**: มีความยาว 8 bits ใช้ในการบอกรายละเอียดเกี่ยวกับ Quality of Service (QoS) ซึ่งเป็น Service ที่ทำให้ Router รู้ว่า IP Datagram ไหนสำคัญกว่ากัน

The Network Layer

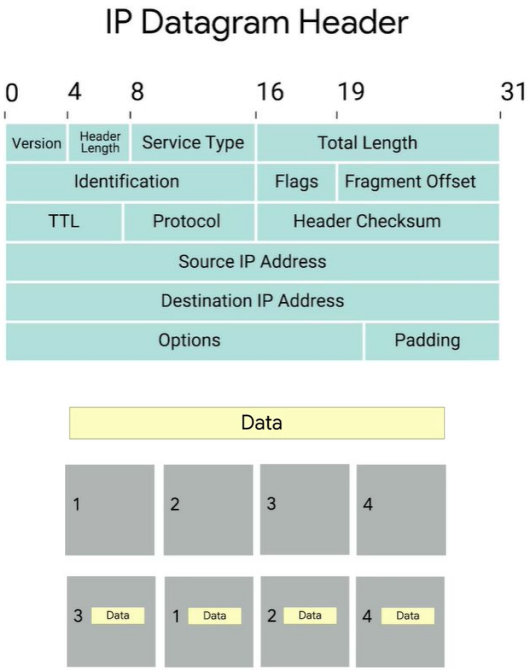


Total Length: มีความยาว 16 bits เอาไว้บอกความยาวทั้งหมดของ IP Datagram

- Maximum Size คือ 2^{16} = 65,535 bytes

Identification: มีความยาว 16 bits ใช้ในการจับกลุ่มข้อมูลเข้าด้วยกัน

The Network Layer



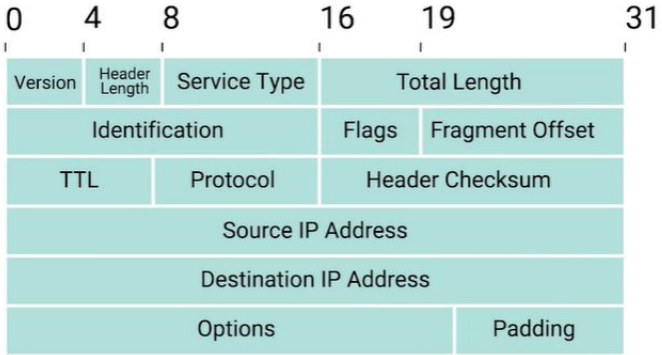
Flags: มีความยาว 3 bits ใช้ในการบอกว่า IP Datagram นั้นสามารถถูกตัดแบ่งย่อย (Fragmentation) ได้หรือไม่

- **Fragmentation** เป็นกระบวนการที่นำ IP Datagram มาตัดแบ่งย่อยเป็น IP Datagram หลาย ๆ ส่วน

Fragment Offset: มีความยาว 13 bits ใช้ในการบอกเครื่องผู้รับให้สามารถประกอบข้อมูลที่ถูกแบ่งย่อยแล้ว ให้กลับมาเป็นข้อมูลตั้งต้นได้

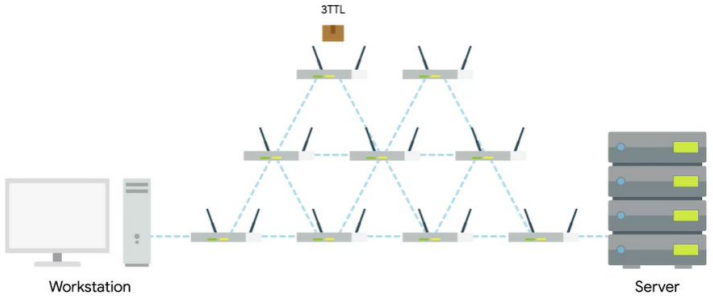
The Network Layer

IP Datagram Header

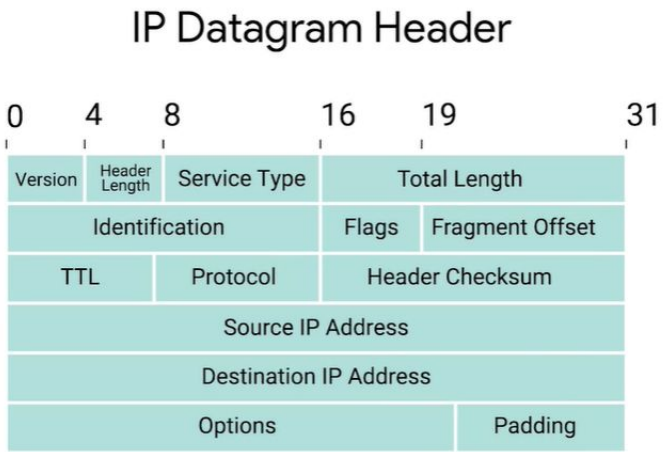


Time To Live (TTL): มีความยาว 8 bits ใช้ในการบอกจำนวน Router Hops ที่ Datagram สามารถเดินทางได้ ก่อนจะถูกทิ้งข้อมูล

- มีจุดประสงค์เพื่อป้องกัน Endless Loop
- ทุกครั้งที่ Datagram ไปถึง Router ตัวใหม่ Router ตัวนั้นจะลดค่า TTL ลงหนึ่ง
- หาก TTL เป็น 0 แล้ว Router จะทิ้งข้อมูลนั้น



The Network Layer



Protocol: มีความยาว 8 bits ใช้ในการบอก Transport Layer Protocol (TCP หรือ UDP)

Header Checksum: มีความยาว 16 bits ใช้ในการบอก

ค่า Checksum ของ IP Datagram

- ค่า Checksum จะเปลี่ยนทุก Hop เพราะ TTL มีการเปลี่ยนแปลง

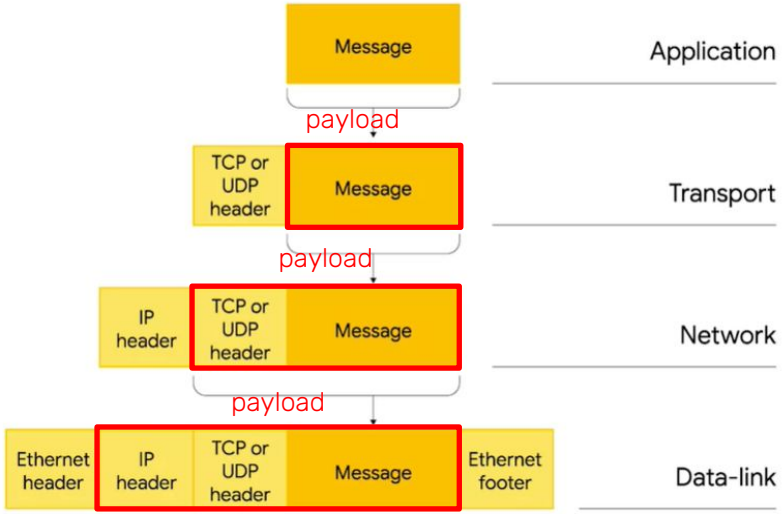
Source IP Address: มีความยาว 32 bits

Destination IP Address: มีความยาว 32 bits

Options: ใช้ในการตั้งค่าพิเศษให้กับ Datagram โดยมากแล้วใช้สำหรับทดสอบ

Padding: ชุดของเลข 0 ที่ถูกใช้ทำให้ Header มีขนาดที่ถูกต้อง

The Network Layer



Encapsulation คือ การที่ข้อมูลทั้งหมดของ Layer ก่อนหน้ากลายมาเป็น Payload ที่ถูกห่อหุ้มด้วย Header หรือ Footer

Decapsulation คือ การถอด Header หรือ Footer ออก

The Network Layer

Address Class System เป็นระบบที่บอกถึงวิธีการแบ่งส่วน IP Address

- IP Address ถูกแบ่งออกเป็น 2 ส่วน คือ **Network ID** และ **Host ID**

Class A	Class B	Class C
123.456.780.00 network ID	123.456.780.00 network ID	123.456.780.00 network ID
123.456.780.00 host ID	123.456.780.00 host ID	123.456.780.00 host ID
2^{24} = 16,777,216	2^{16} = 65536	2^{8} = 256

The Network Layer

- Address Class System

Class	Left-most bit	Starting IP address	Last IP address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

- Class D ใช้สำหรับ Multicast
- Class E ใช้สำหรับการทดสอบเท่านั้น

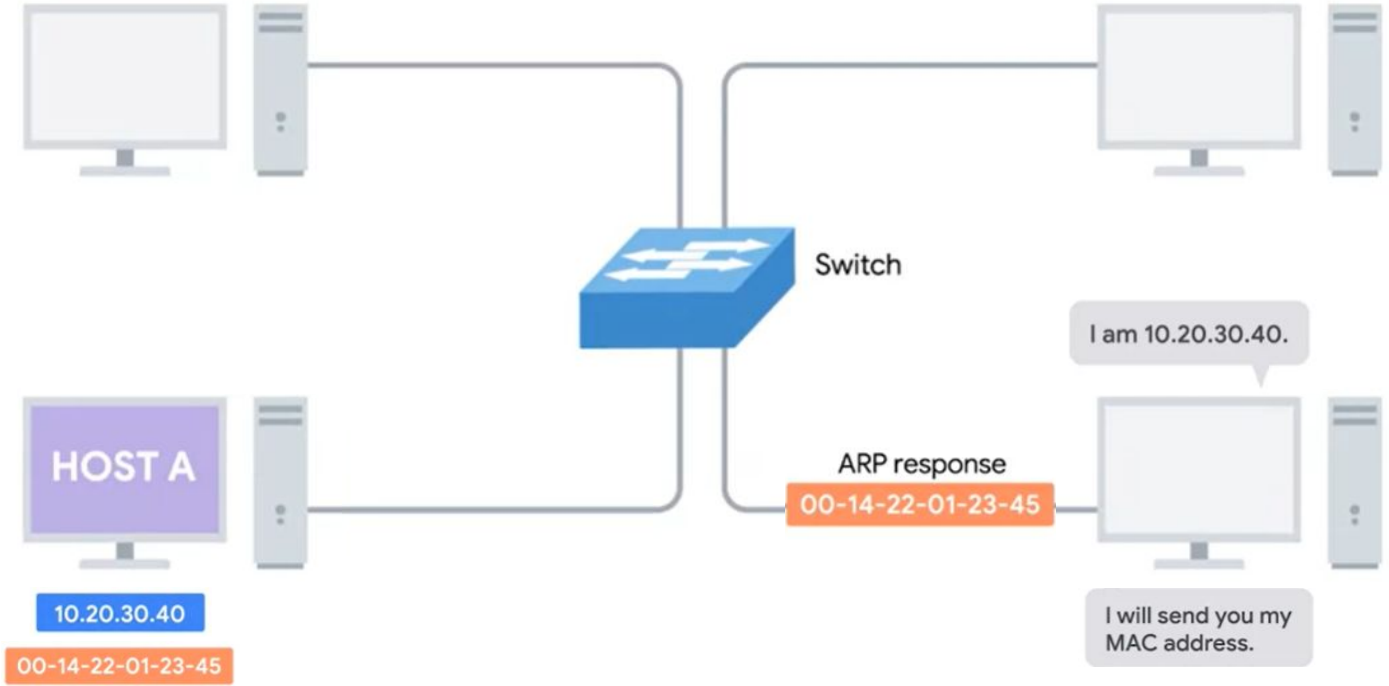
The Network Layer

Address Resolution Protocol (ARP) เป็น Protocol ที่ใช้ในการหา MAC Address (Hardware Address) สำหรับ IP Address หนึ่ง

- ARP Table เป็นตารางที่จับคู่ระหว่าง IP Address และ MAC Address

The Network Layer

ARP Process

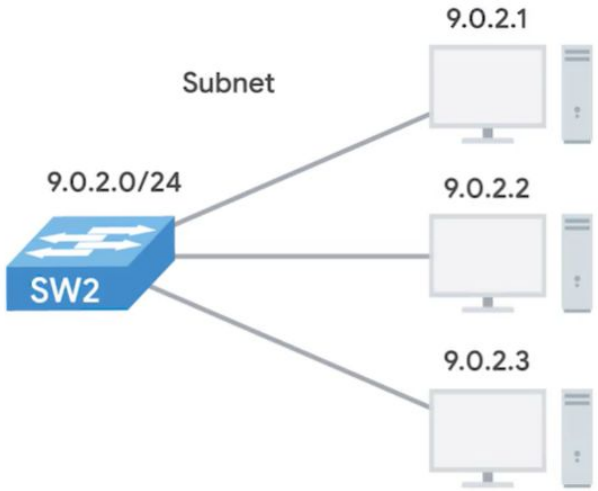


Subnetting

Subnetting คือ การแบ่ง Network ใหญ่ออกเป็น Network ย่อย ๆ เรียกว่า Subnet

IP address classes

Class	Range	Max Hosts
A	0-126	16 Million
B	128-191	64,000
C	192-224	254
D	224-239	N/A
E	240-255	N/A



Subnetting

Basic Binary Math

Binary						Decimal	
32	16	08	04	02	01	10	01
					1		1
				1	0		2
				1	1		3
			1	0	0		4
			1	0	1		5
			1	1	0		6
			1	1	1		7
		1	0	0	0		8
		1	0	0	1		9
		1	0	1	0	1	0
		1	0	1	1	1	1

4 bit	$2^4 = 16$	
8 bit	$2^8 = 256$	0-255
16 bit	$2^{16} = 65536$	

Subnetting

Basic Binary Math

- Operators

การบวก
(Addition)

0 + 0 = 0

0 + 1 = 1

1 + 0 = 1

1 + 1 = 10

และ
(AND)

1 AND 1 = 1
1 AND 0 = 0
0 AND 0 = 0

หรือ
(OR)

1 OR 1 = 1
1 OR 0 = 1
0 OR 0 = 0

Subnetting

IP address	9	100	100	100
IP address *(in binary)*	0000 1001	0110 0100	0110 0100	0110 0100
Subnet mask *(in binary)*	1111 1111	1111 1111	1111 1111	0000 0000

255.255.255.0

Subnet ID = 9.100.100.0

- ความเป็นไปได้ของ Host ID ทั้งหมดคือ $2^8 = 256$
- แต่มี Host ID ใช้ได้ทั้งหมด 256 - 2 = 254

Subnet ID เป็นตัวระบุ Subnet

Subnet Masks เป็นเลข binary 32-bit ที่ใช้คำนวณ Subnet ID โดยใช้ Operator “AND”

- “1” จะเป็นตัวบอก Router ว่าส่วนไหนเป็น Subnet ID
- “0” จะเป็นตัวบอกส่วนของ Host ID

ขนาดของ Subnet จะขึ้นอยู่กับ Subnet Mask

- Subnet หนึ่งจะมี Host ID ที่ใช้ได้ “น้อยลงไป 2 IDs” เนื่องจาก ID แรกจะถูกจองไว้ใช้เป็น Subnet ID และ ID สุดท้ายจะถูกจองไว้ใช้เป็น Broadcast Address

Subnetting

9.100.100.100

255 . 255 . 255 . 224

11111111 11111111 11111111 11100000

9.100.100.100/27

- ความเป็นไปได้ของ Host ID ทั้งหมดคือ $2^5 = 32$
- แต่มี Host ID ใช้ได้ทั้งหมด 32 - 2 = 30

เราไม่จำเป็นต้องใช้ Subnet Mask ให้เต็ม Octet ก็ได้

Subnetting

Subnet masks and IP address

Class		Mask short name	Max Hosts
A	255.0.0.0 11111111.00000000.00000000.00000000	/8	16,777,214
B	255.255.0.0 11111111.11111111.00000000.00000000	/16	65,534
C	255.255.255.0 11111111.11111111.11111111.00000000	/24	254
	255.255.240.0 11111111.11111111.11110000.00000000	/20	4,094
	255.255.255.224 11111111.11111111.11111111.11100000	/27	30
	255.255.255.252 11111111.11111111.11111111.11111100	/30	2

9.100.100.100

255.255.255.0

9.100.100.100/24

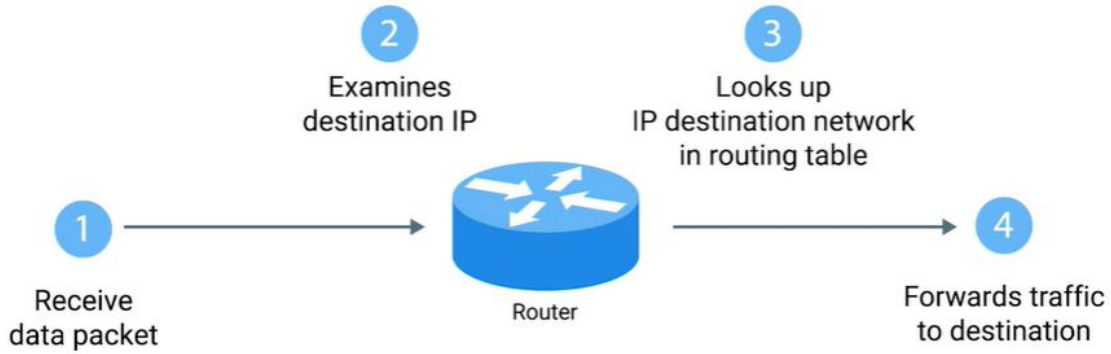
CIDR (Classless Inter-Domain Routing) เป็นวิธีการที่ยืดหยุ่นในการแบ่ง Network ID และ Host ID

- ใช้ Subnet Mask เพื่อที่จะแบ่งขอบเขต (Demarcate) ของ Network
- **Demarcation Point** คือ จุดที่สิ้นสุดของ Network หนึ่ง และเป็นจุดเริ่มต้นของอีก Network หนึ่ง
- CIDR Notation

Routing

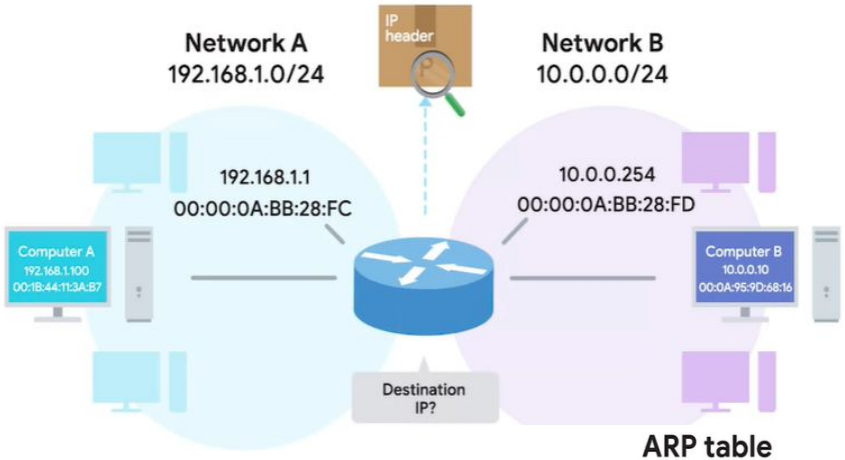
Router คือ อุปกรณ์ที่สามารถวิเคราะห์และส่งต่อ Traffic ไปหาที่อยู่ปลายทาง (Destination IP Address) ได้

วิธีการทำงานของ Router เบื้องต้นมี 4 ขั้นตอน ดังนี้



Routing

ตัวอย่างการ Routing จาก Computer A (192.168.1.100) ไปหา Computer B (10.0.0.10)



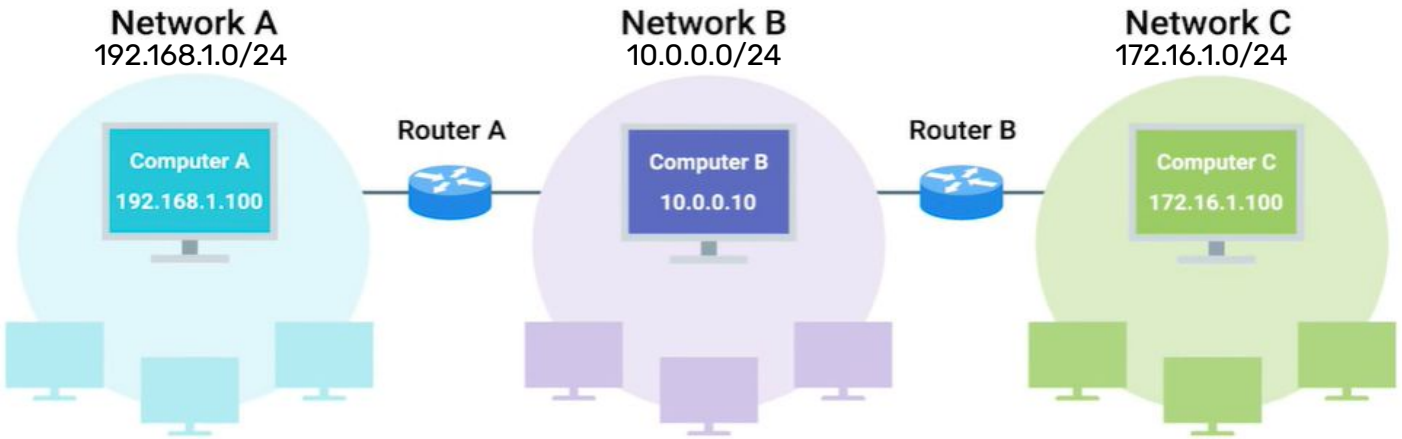
Network name	Network range
A	192.168.1.0/24
B	10.0.0.0/24

ARP table

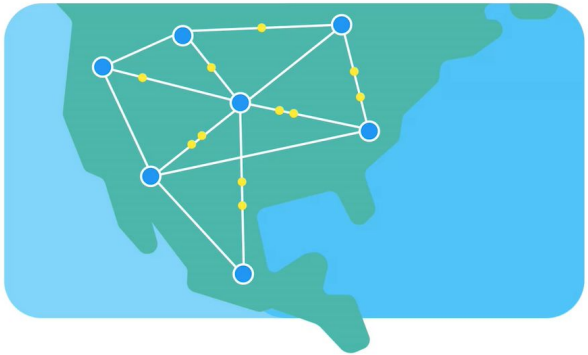
MAC address	IP address
00:1B:44:11:3A:B7	192.168.1.100
00:0A:95:9D:68:16	10.0.0.10

Routing

ตัวอย่างการ Routing จาก Computer A (192.168.1.100) ไปหา Computer C (172.16.1.100)



Routing



Routing Table ประกอบด้วยข้อมูลหลัก 4 อย่าง ดังนี้

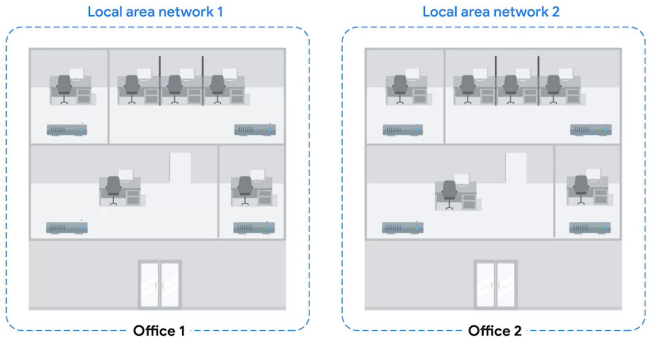
- **Destination Network** คือ Network ID ที่ Router รู้จัก
- **Next Hop** คือ IP Address ของ Router ตัวต่อไปที่ควรจะได้รับข้อมูล เพื่อที่จะส่งต่อไปหา Destination Network ได้
- **Total Hops** คือ จำนวน Hop ทั้งหมดที่ใช้ในการส่งข้อมูลไปหา Destination Network
- **Interface** คือ Interface ที่ Router ต้องส่งต่อข้อมูลเพื่อให้ไปถึง Destination Network

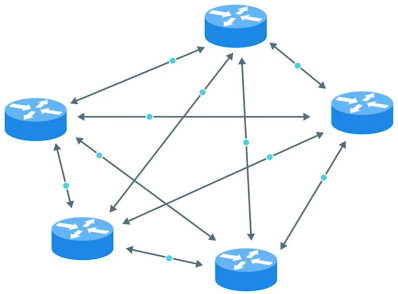
Routing

Routing Protocols เป็น Protocol ที่ Router ใช้ในการสื่อสารกันเพื่ออัพเดท Routing Table โดย Routing Protocols สามารถแบ่งออกเป็น 2 ประเภทใหญ่ ๆ คือ

- **Interior Gateway Protocols**
- **Exterior Gateway Protocols**

Routing





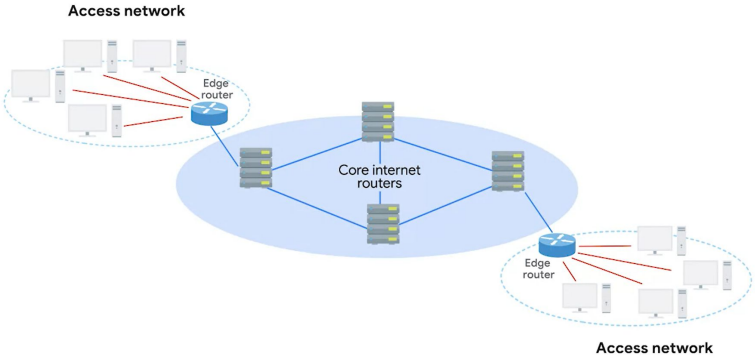
Interior Gateway Protocols ใช้ในการแชร์ข้อมูลภายใน Autonomous System (AS) เดียวกัน

- **AS** คือ กลุ่มของ Networks ที่อยู่ภายใต้การควบคุมดูแลขององค์กรเดียว

Interior Gateway Protocols ถูกแบ่งเป็น 2 ประเภทคือ

- **Distance-vector**: หาจำนวน Hop ที่น้อยที่สุด
- **Link-state**: หาเส้นทางที่ดีที่สุด

Routing



Exterior Gateway Protocols ใช้ในการแชร์ข้อมูลระหว่าง Router ที่อยู่บนขอบ (Edges) ของ AS

- ทำให้แชร์ข้อมูล Routing ข้ามองค์กรได้
- Internet Assigned Numbers Authority (IANA) ทำหน้าที่ในการจัดสรร Autonomous System Number (ASN) ให้กับองค์กรต่าง ๆ เช่น IBM มี ASN คือ AS19604

Routing

IPv4 ไม่เพียงพอสำหรับการใช้งานในปัจจุบันแล้ว

RFC (Request For Comments) ทำหน้าที่ทำให้อินเตอร์เน็ตดำเนินไปอย่างมีมาตรฐาน

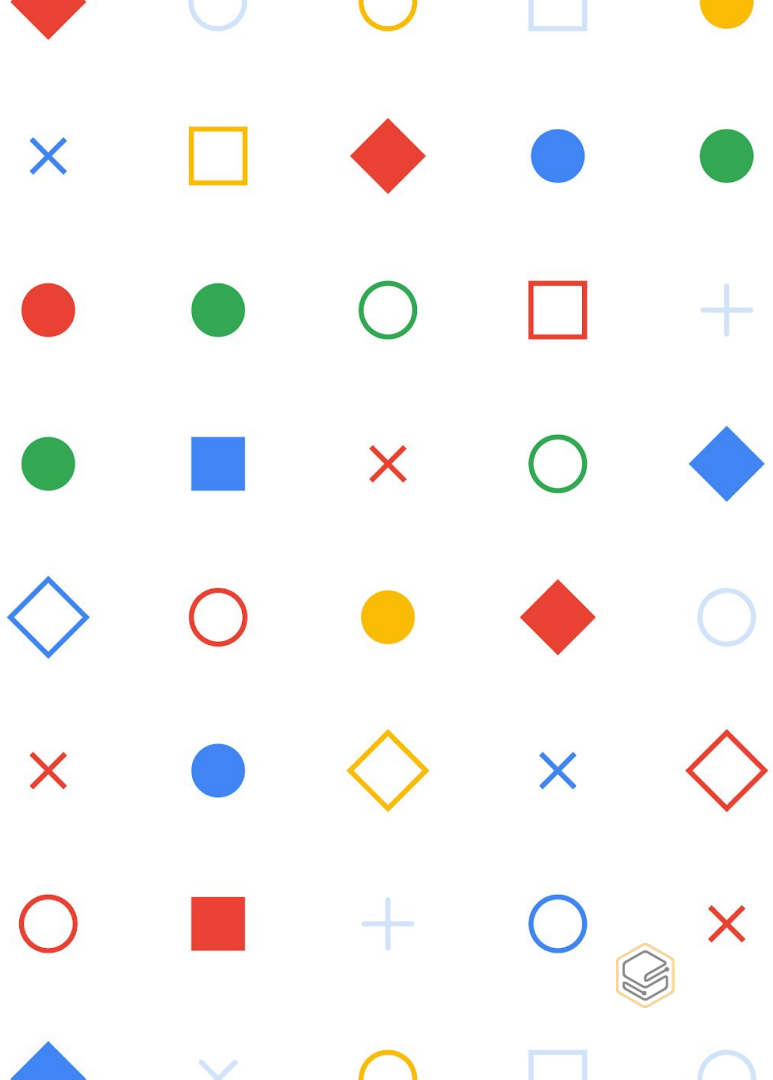
- ในปี 1996 ได้มีการประกาศ RFC1918 เรื่อง Non-routable Address Space

Non-routable Address Space คือ กลุ่มของ IP Addresses ที่ไม่อนุญาตให้ Route โดย Exterior Gateway Protocols

- แต่อนุญาตให้ใช้ใน Internal Network ซึ่งใช้ Interior Gateway Protocols ได้
- **Network Address Translation (NAT)** ช่วยให้คอมพิวเตอร์ที่ใช้ Non-routable Address Space สื่อสารกับเครื่องที่อยู่บน Internet ได้

Week 3

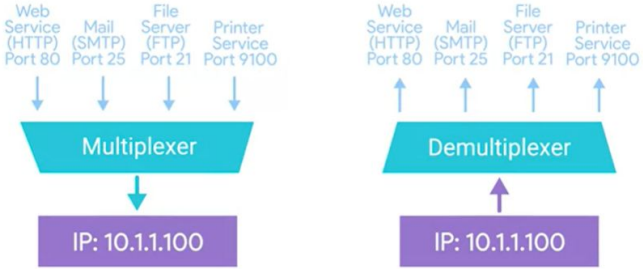
The Transport and Application Layers

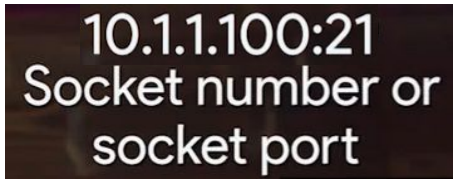


Samart Skills
A Grow with Google PROGRAM

Skooldio

The Transport Layer





Transport Layer ทำหน้าที่จัดเรียงข้อมูล (Sorting) ที่โปรแกรม Client และ Server จะต้องได้รับ และทำให้ข้อมูลถูกส่งไปถึง Application ที่ต้องการได้

- TCP และ UDP
- TCP Segment ซึ่งประกอบด้วย TCP Header และ Payload

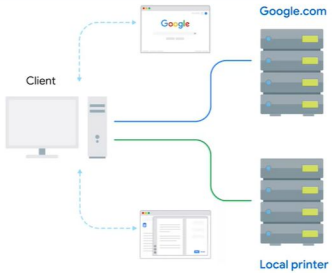
Transport Layer จัดการเรื่อง **Multiplexing และ Demultiplexing** ผ่าน Ports

- Multiplexing คือ การทำให้คอมพิวเตอร์สามารถให้บริการหลาย Services บนเครื่องเดียวกันได้
- Demultiflexing คือ การรับข้อมูลและส่งต่อไปยัง Service ที่ต้องการบนเครื่องคอมพิวเตอร์เดียวกันได้
- Port เป็นเลข 16 bits (0 - 65,535) ที่ถูกใช้ในการส่งข้อมูลไปถึง Service/Application ที่กำลังรันอยู่บนคอมพิวเตอร์ที่เชื่อมต่อกับ Network เช่น FTP ใช้ Port 21, HTTP ใช้ Port 80 เป็นต้น

The Transport Layer

Bit 0			Bit 15 Bit 16	Bit 31
Source port (16)			Destination port (16)	
Sequence number (32)				
Acknowledgment number (32)				
Header Length (4)	empty (6)	Control flags (6)	Window (16)	
Checksum (16)			Urgent (16)	
Options (0 or 16 if any)			Padding	
Data payload (varies)				

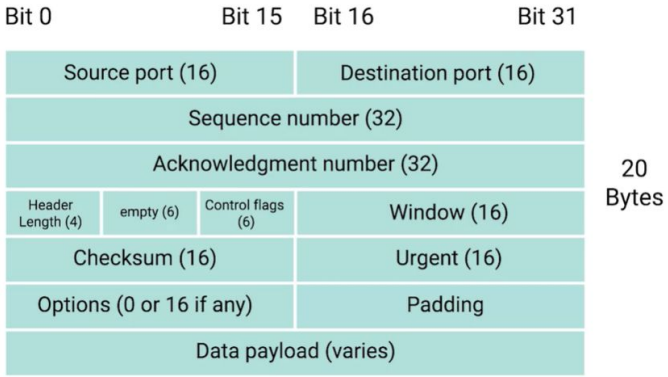
20 Bytes



TCP Header มีความยาว 20 bytes ประกอบด้วยข้อมูลดังนี้

- **Source Port** คือ Port ต้นทางซึ่งถูกเลือกมาจาก Ephemeral Ports (49152 - 65535)
- **Destination Port** คือ Port ของ Service ปลายทางที่ต้องการส่งไปถึง เช่น FTP ใช้ Port 21

The Transport Layer

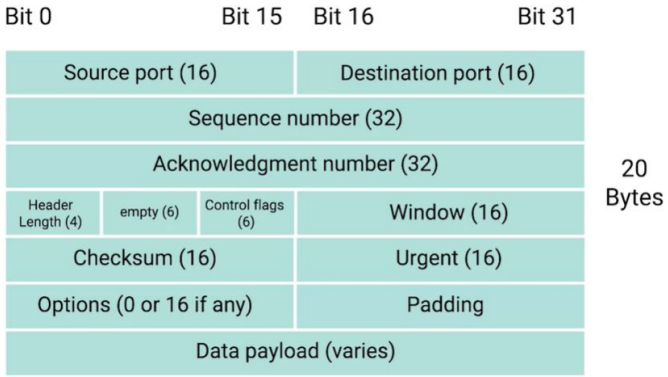


Sequence Number มีความยาว 32 bits ใช้ในการติดตามลำดับ (Sequence) ของ TCP Segments ว่าเป็นลำดับที่ควรจะเป็นหรือไม่

- หากข้อมูลมีขนาดใหญ่ เราจำเป็นต้องแบ่งข้อมูลออกเป็นหลาย ๆ ส่วน (Segment) ก็เลยต้องมีลำดับ

Acknowledgement Number มีความยาว 32 bits ใช้ในการติดตาม Segment ถัดไป

The Transport Layer



Header Length (Data Offset) มีความยาว 4 bits ใช้บอกความยาวของ TCP Header ทำให้รู้ว่าจุดเริ่มต้นของ Payload

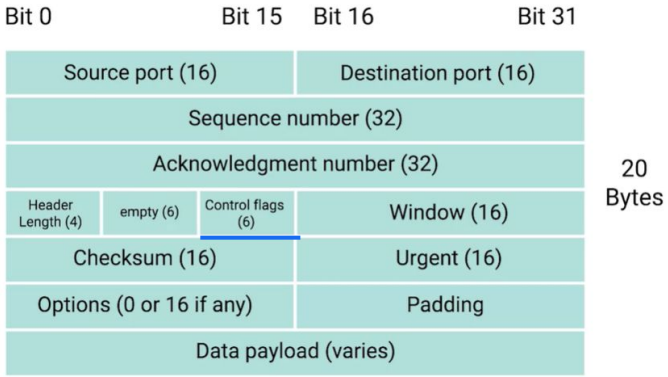
Window มีความยาว 16 bits ใช้ในการบอกช่วงความยาวของ Sequence Number ที่จะถูกส่งก่อนที่จะต้องการ Acknowledgement

Checksum มีความยาว 16 bits ใช้ในการบอกค่า Checksum ของ TCP Segment

Urgent Pointer มีความยาว 16 bits ใช้ในการบอกความเร่งด่วยของ Segment

- ไม่นิยมใช้ในปัจจุบันแล้ว

The Transport Layer



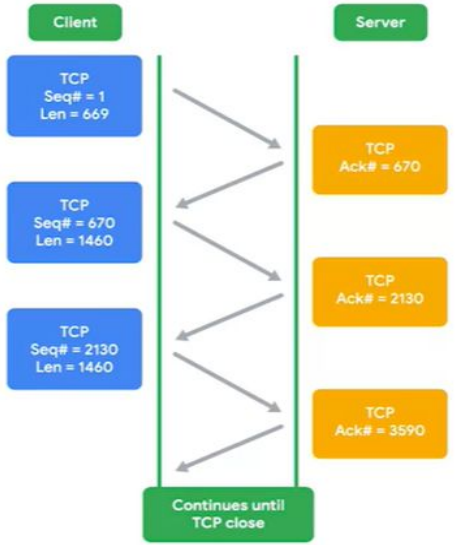
Control Flags มีความยาว 6 bits

- **URG** (Urgent): Segment นี้มีความเร่งด่วนหรือไม่
- **ACK** (Acknowledged): ให้ไปตรวจสอบ Acknowledgement Number
- **PSH** (Push): นำข้อมูลที่ Buffer ไว้ไปเก็บไว้บน Application โดยเร็วที่สุด
- **RST** (Reset): ให้เริ่มต้นส่งข้อมูลใหม่ตั้งแต่แรก อาจเพราะเครื่องผู้รับไม่สามารถ Recover Segment ที่เสียไปแล้วได้
- **SYN** (Synchronize): ใช้เริ่มต้นการเชื่อมต่อ (Establishing Connection) และให้ไปตรวจสอบ Sequence Number
- **FIN** (Finish): ใช้ในการปิดการเชื่อมต่อ

The Transport Layer

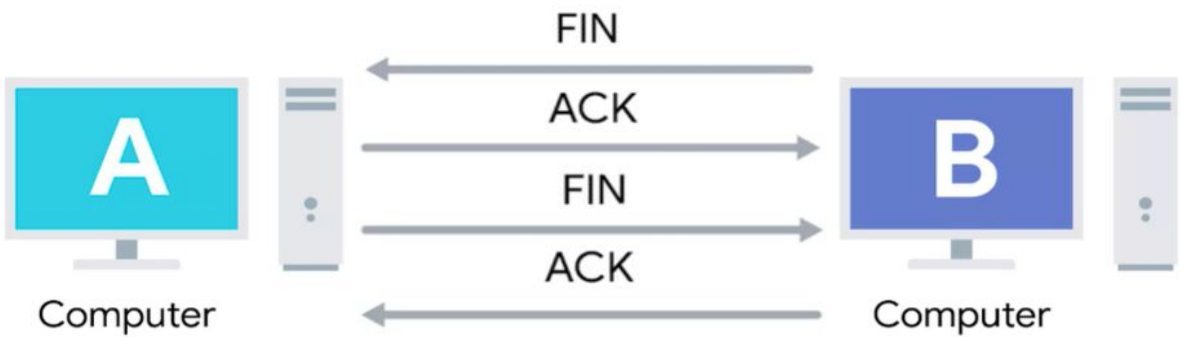
กระบวนการที่ใช้ในการเริ่มต้นการเชื่อมต่อแบบ TCP (TCP Connection Establishment)

จะเรียกว่า **Three-way Handshake**



The Transport Layer

กระบวนการที่ใช้ในการปิดการเชื่อมต่อแบบ TCP (Close Connection) จะเรียกว่า **Four-way Handshake**



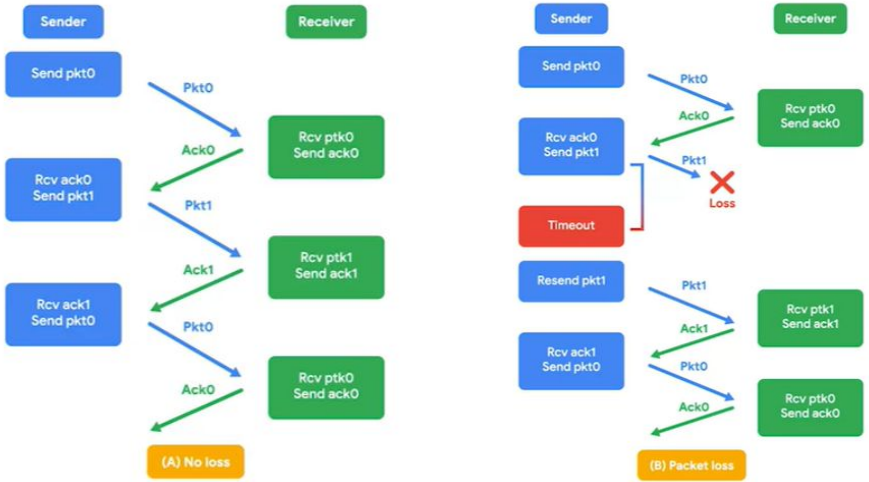
The Transport Layer

Socket States

- **LISTEN:** TCP Socket พร้อมให้บริการและกำลังเปิดรอสำหรับการเชื่อมต่อเข้ามา
- **SYN_SENT:** SYN ได้ถูกส่งไปแล้วแต่การเริ่มต้นการเชื่อมต่อยังไม่เสร็จสิ้น
- **SYN_RECEIVED:** เครื่องที่อยู่ในสถานะ LISTEN ได้รับ SYN แล้ว และได้ส่ง SYN/ACK กลับไปแล้ว
- **ESTABLISHED:** การเชื่อมต่อกำลังทำงานและทั้งสองฝั่งสามารถส่งข้อมูลหากันได้
- **FIN_WAIT:** FIN ได้ถูกส่งไปแล้ว แต่ยังไม่ได้รับ ACK จากอีกฝั่ง
- **CLOSE_WAIT:** การเชื่อมต่อถูกปิดลงบน TCP Layer แต่ Application ยังไม่ปล่อย Socket
- **CLOSED:** การเชื่อมต่อถูกปิดลงอย่างสมบูรณ์

The Transport Layer

Connection-oriented Protocol คือ Protocol ที่ทำการเชื่อมต่อโดยรับรองว่าข้อมูลทั้งหมดจะถูกส่งไปถึงมือผู้รับอย่างครบถ้วนสมบูรณ์ เช่น TCP

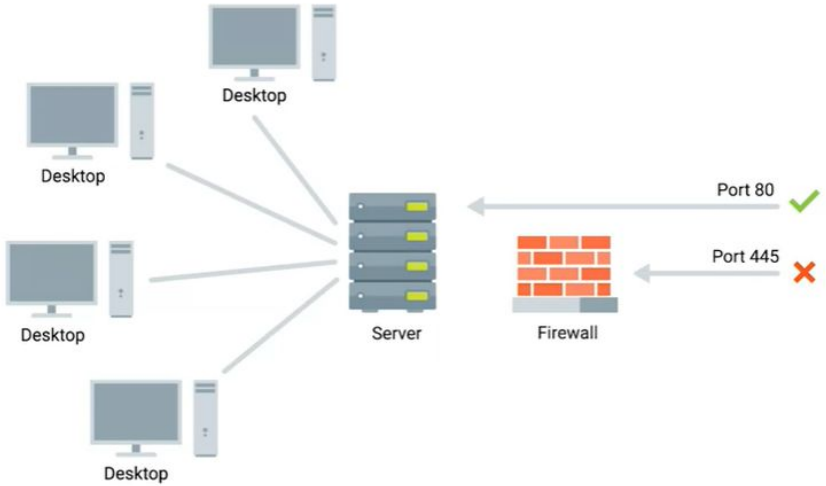


The Transport Layer

Connectionless Protocols คือ Protocol ที่ทำการเชื่อมต่อโดยไม่มีการรับรองว่าข้อมูล เช่น UDP

- ใช้ในการส่งข้อมูลที่ไม่จำเป็นต้องถึงมือผู้รับครบถ้วน เช่น Streaming Video

The Transport Layer



Firewall คือ อุปกรณ์หรือ Software ที่ทำหน้าที่อนุญาตหรือปฏิเสธ Traffic ตามกฎที่ตั้งไว้

- Network-based หรือ Host-based

The Application Layer

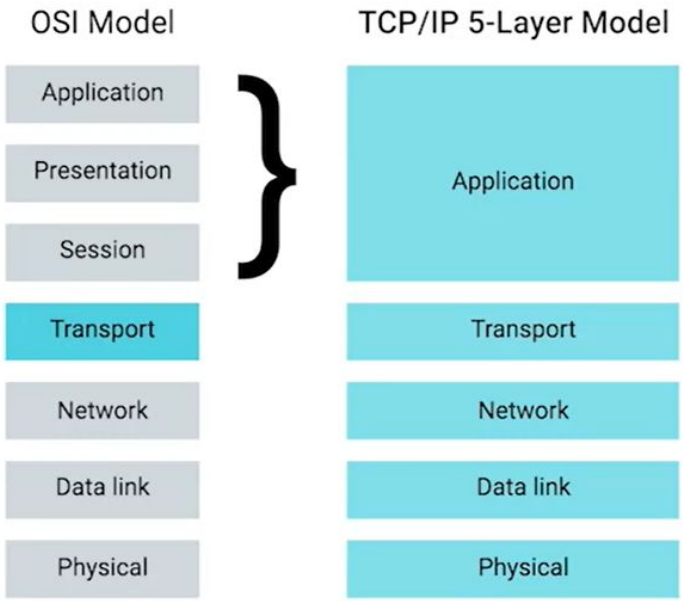
Application Layer ทำหน้าที่จัดการให้ Application บนเครื่องคอมพิวเตอร์ต่าง ๆ สามารถสื่อสารกันได้

- ข้อมูลในชั้นนี้ คือ เนื้อหาที่ Application ต้องการสื่อสารกัน เช่น Web Page, Video หรือ File
- ตัวอย่าง Protocol เช่น HTTP, FTP, DNS, DHCP เป็นต้น

Web Browser และ Web Server จะคุยกันผ่าน Protocol HTTP

- Web Browser เช่น Chrome, Internet Explorer, Safari
- Web Server เช่น Microsoft IIS, Apache, Nginx

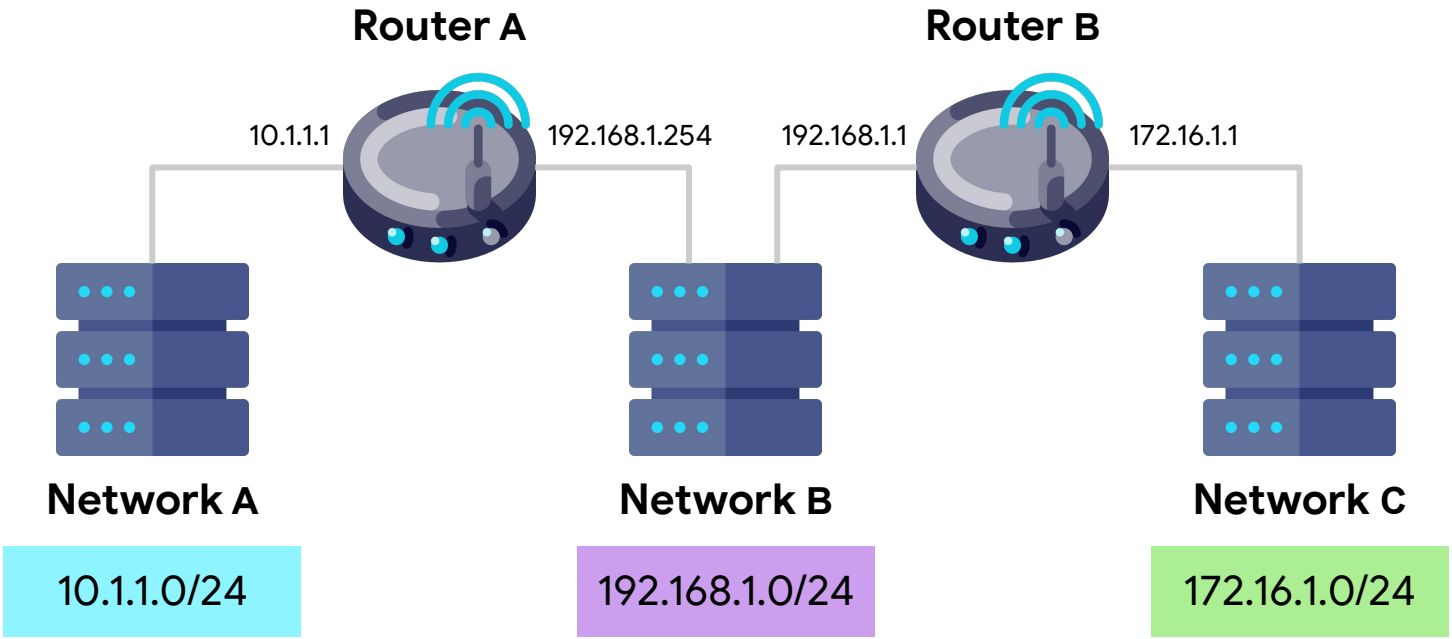
The Application Layer

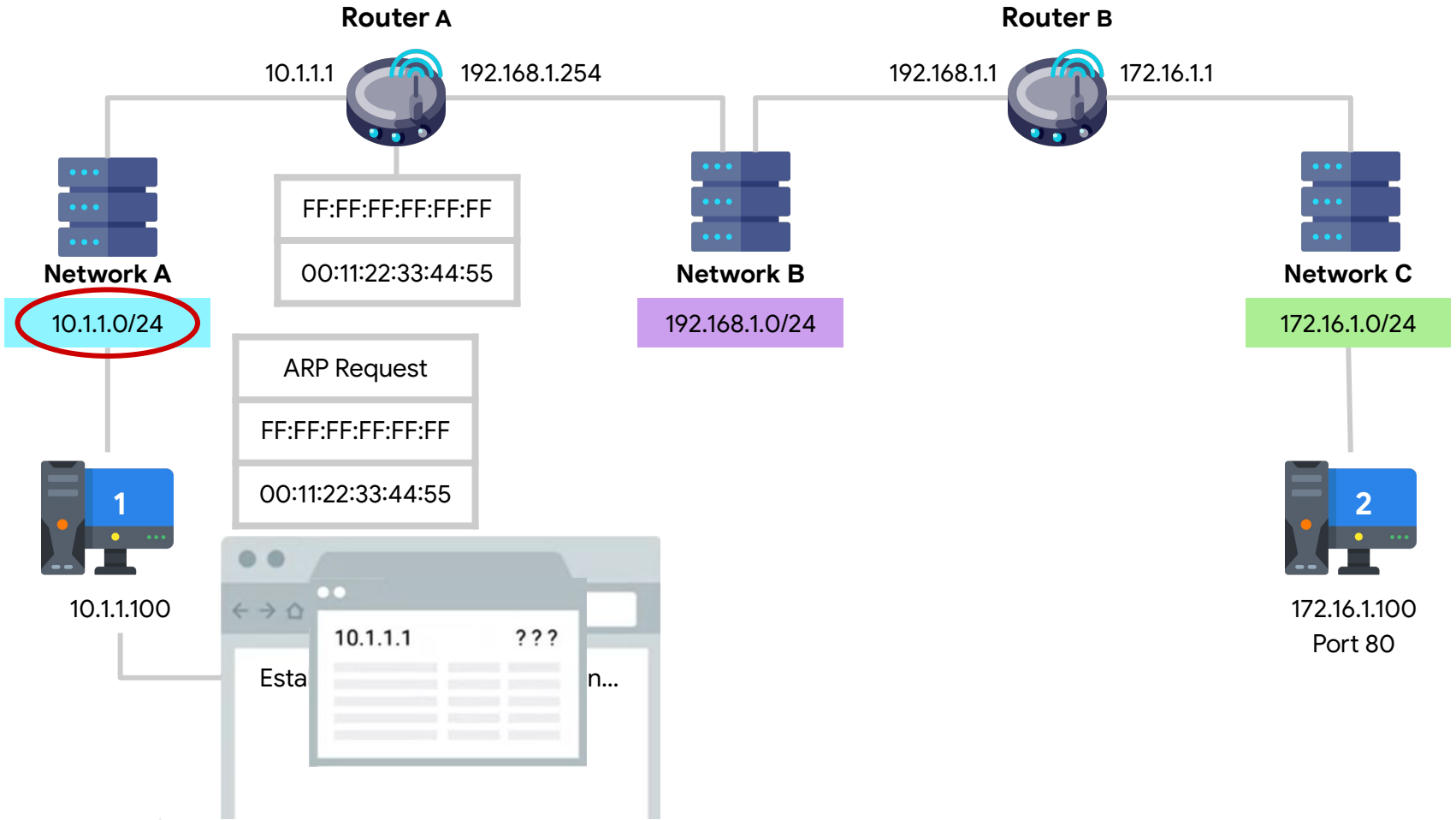


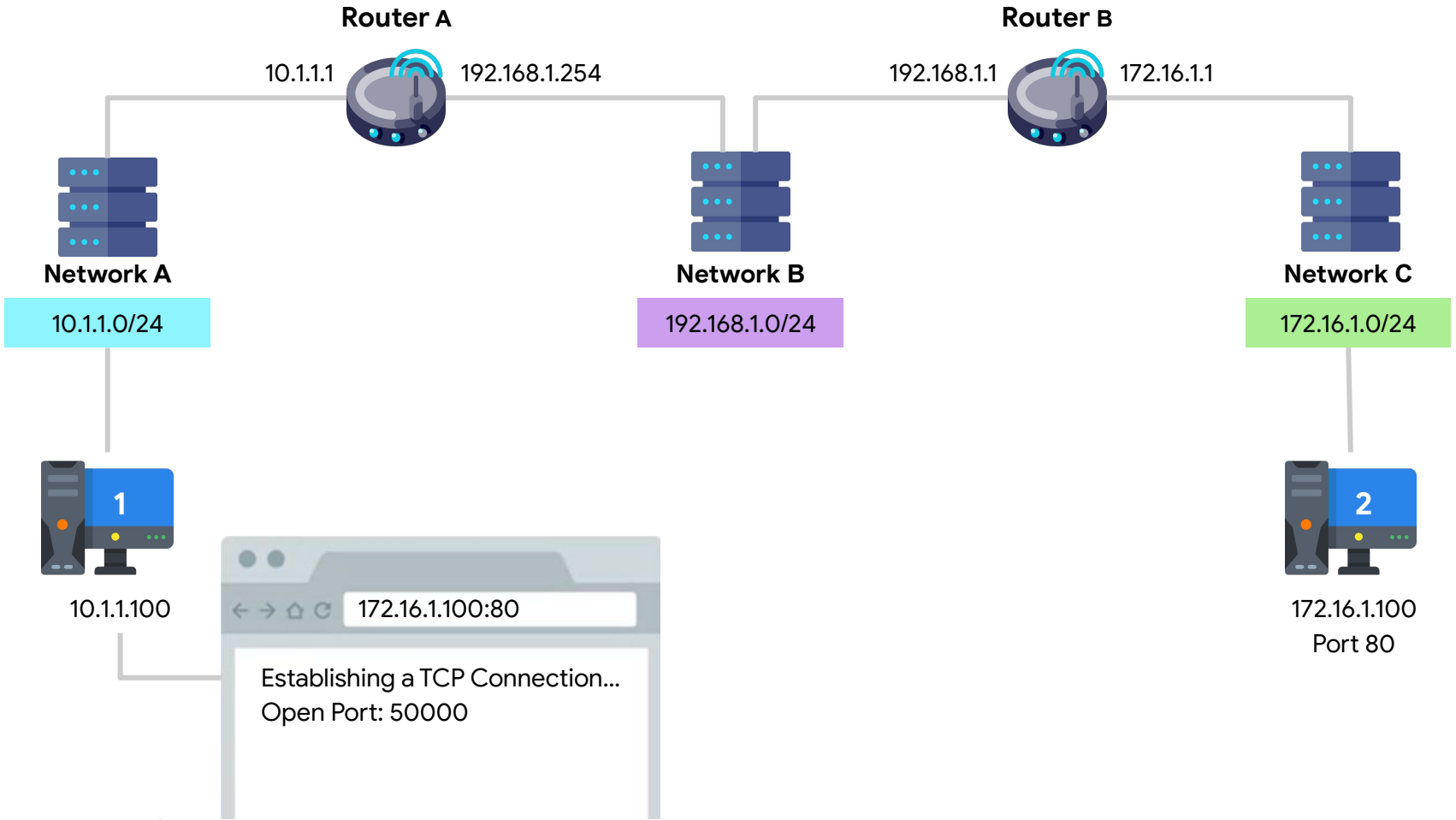
Open Systems Interconnection (OSI) Model

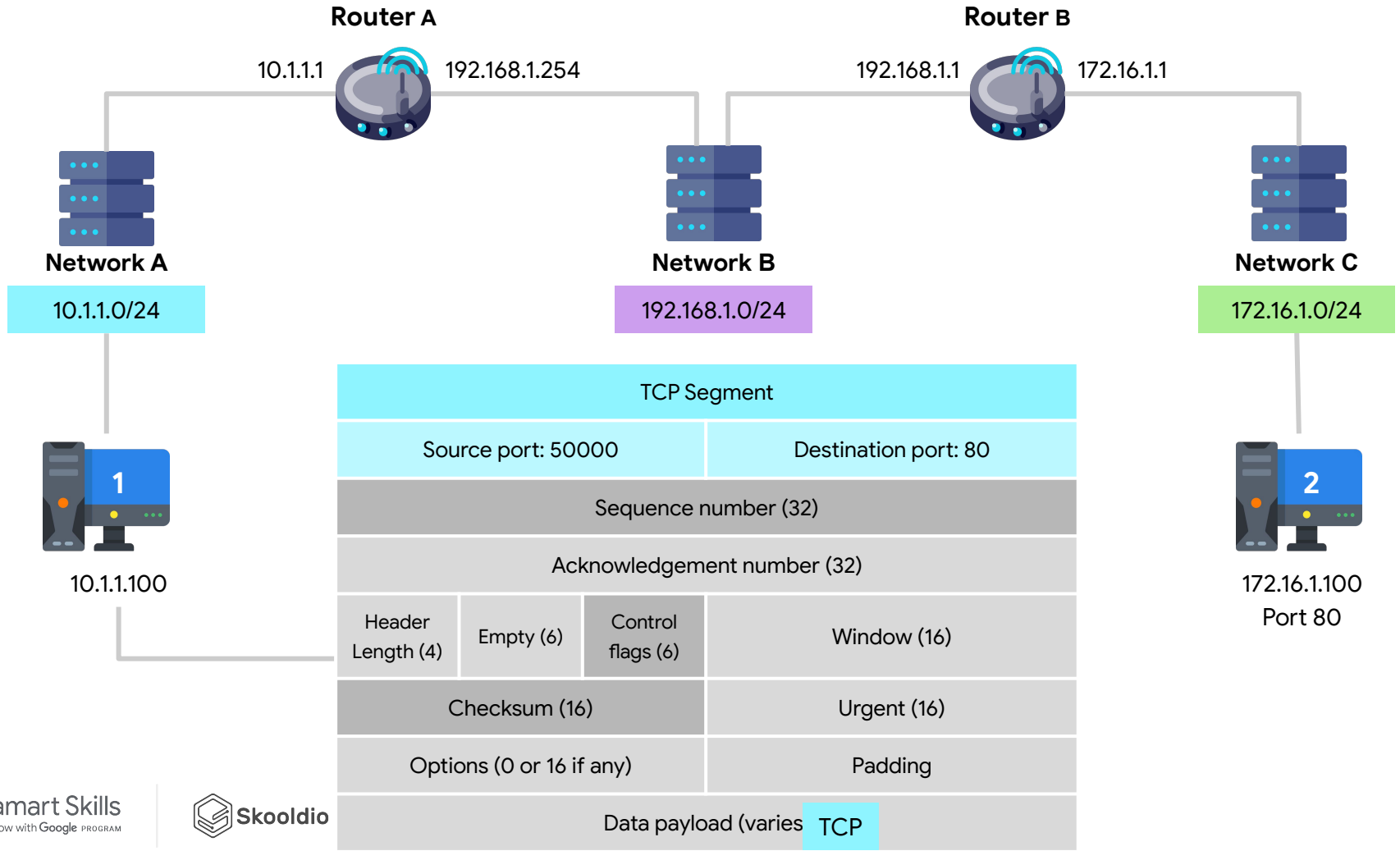
- **Session Layer** ทำหน้าที่เป็นตัวประสานงานระหว่าง Application Layer และ Transport Layer โดยนำข้อมูลของ Application Layer ที่ถูก Decapsulate แล้ว ส่งต่อให้กับ Presentation Layer
- **Presentation Layer** ทำหน้าที่นำข้อมูลมาจัดให้อยู่ในรูปแบบที่ Application สามารถเข้าใจได้

All the Layers Working in Unison



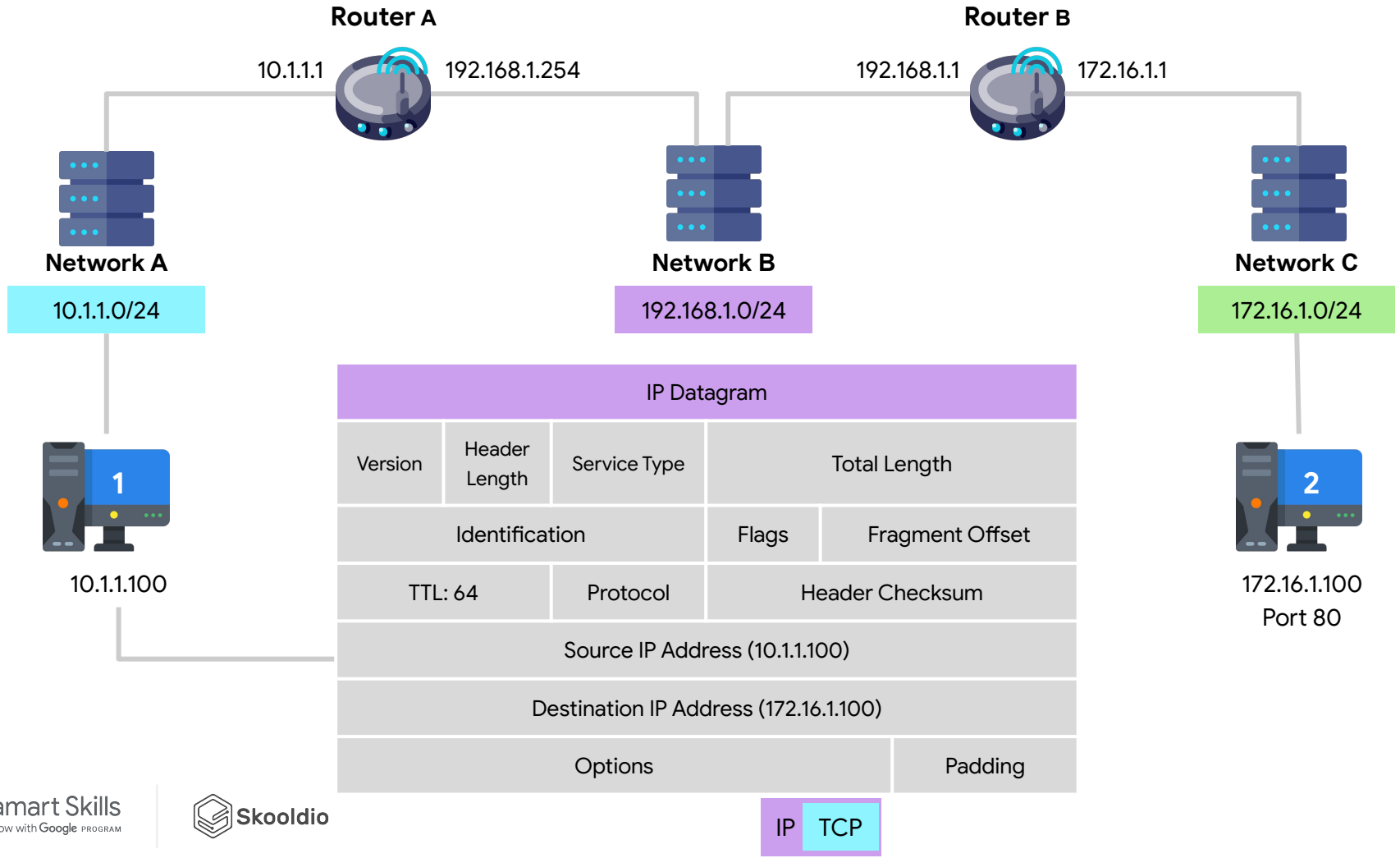

Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
FF:FF:FF:FF:FF:FF
00:11:22:33:44:55
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
ARP Request
FF:FF:FF:FF:FF:FF
00:11:22:33:44:55
1
2
10.1.1.100
172.16.1.100
Port 80
10.1.1.1
???
Esta
n...


Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
1
10.1.1.100
172.16.1.100:80
Establishing a TCP Connection...
Open Port: 50000
2
172.16.1.100
Port 80



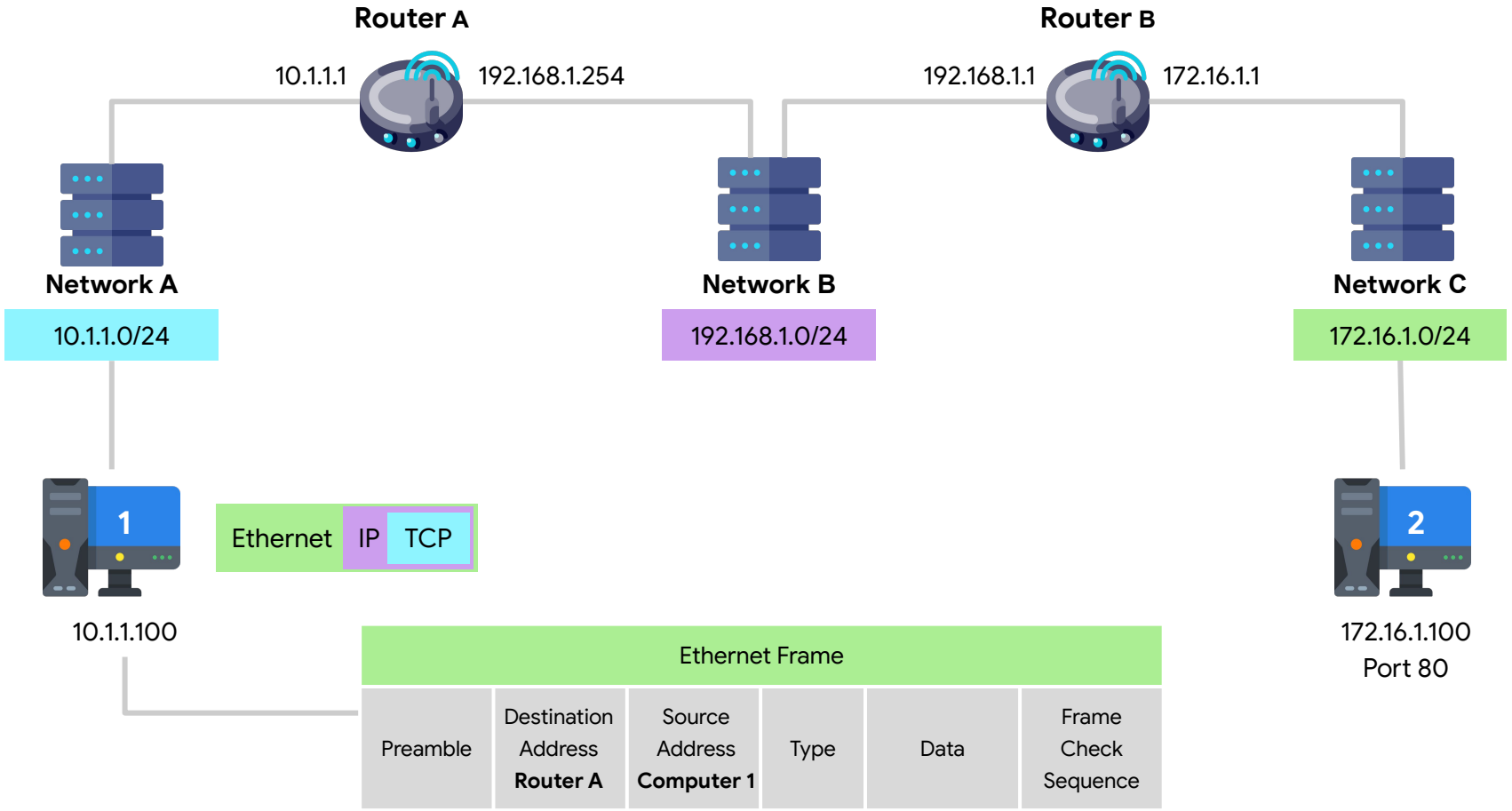
Samart Skills
A Grow with Google PROGRAM

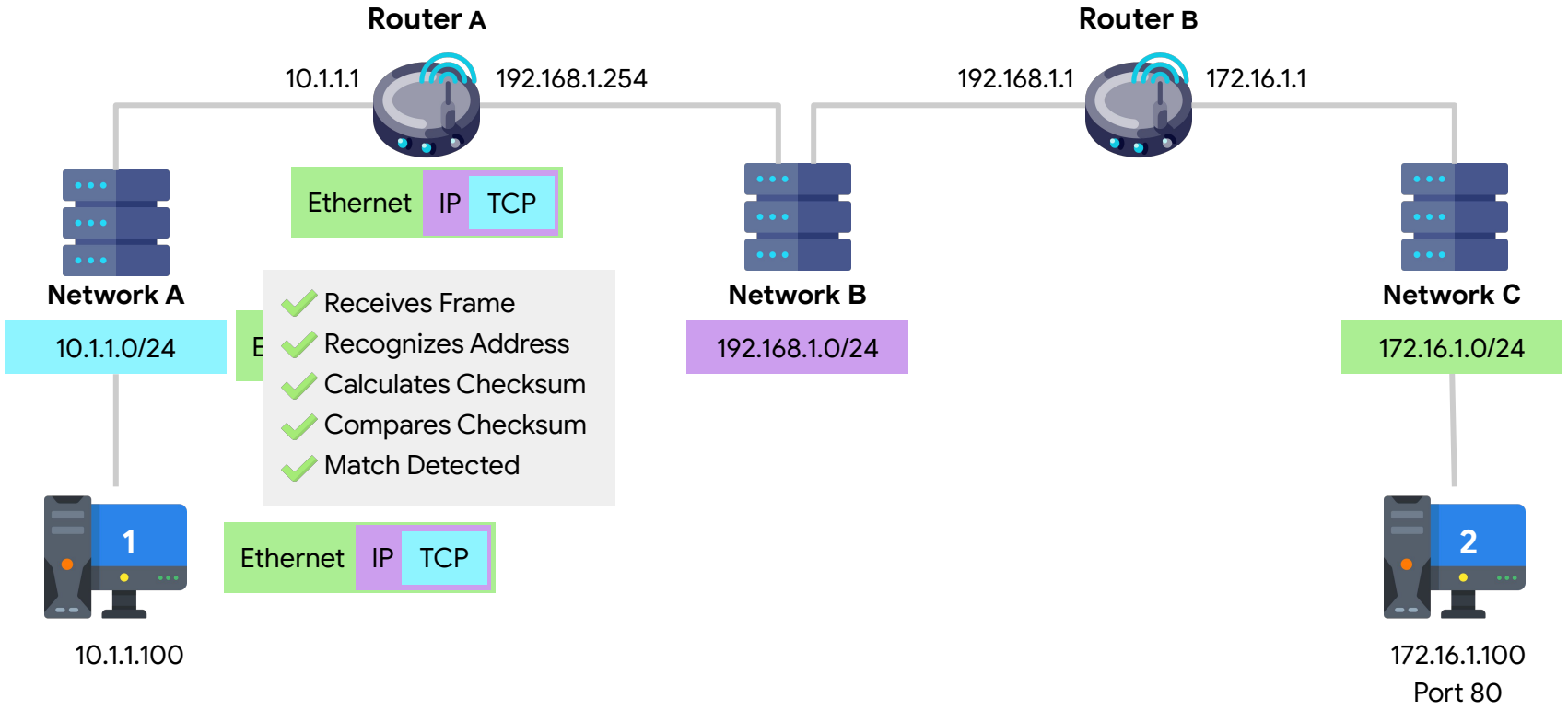
Skooldio

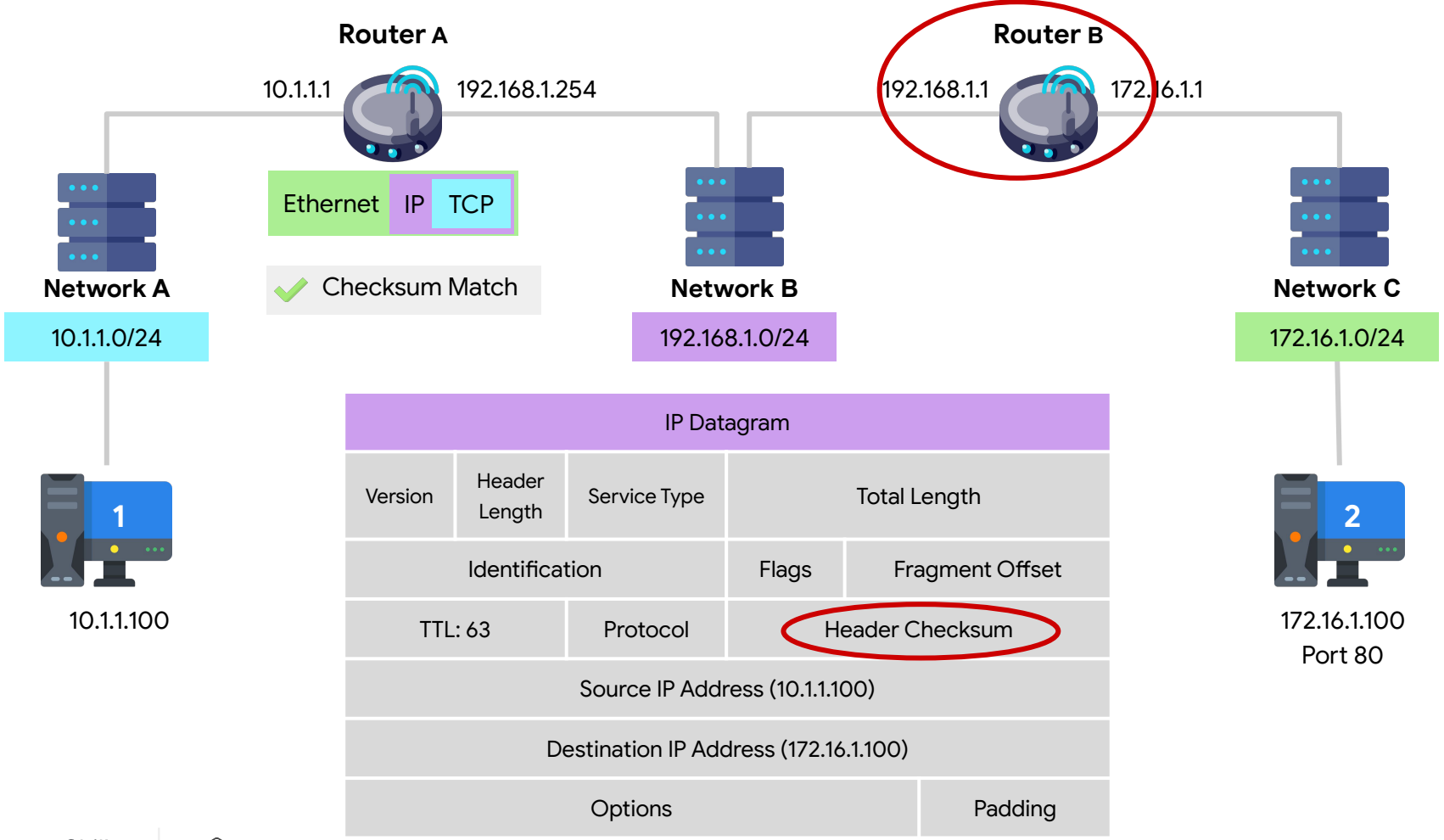


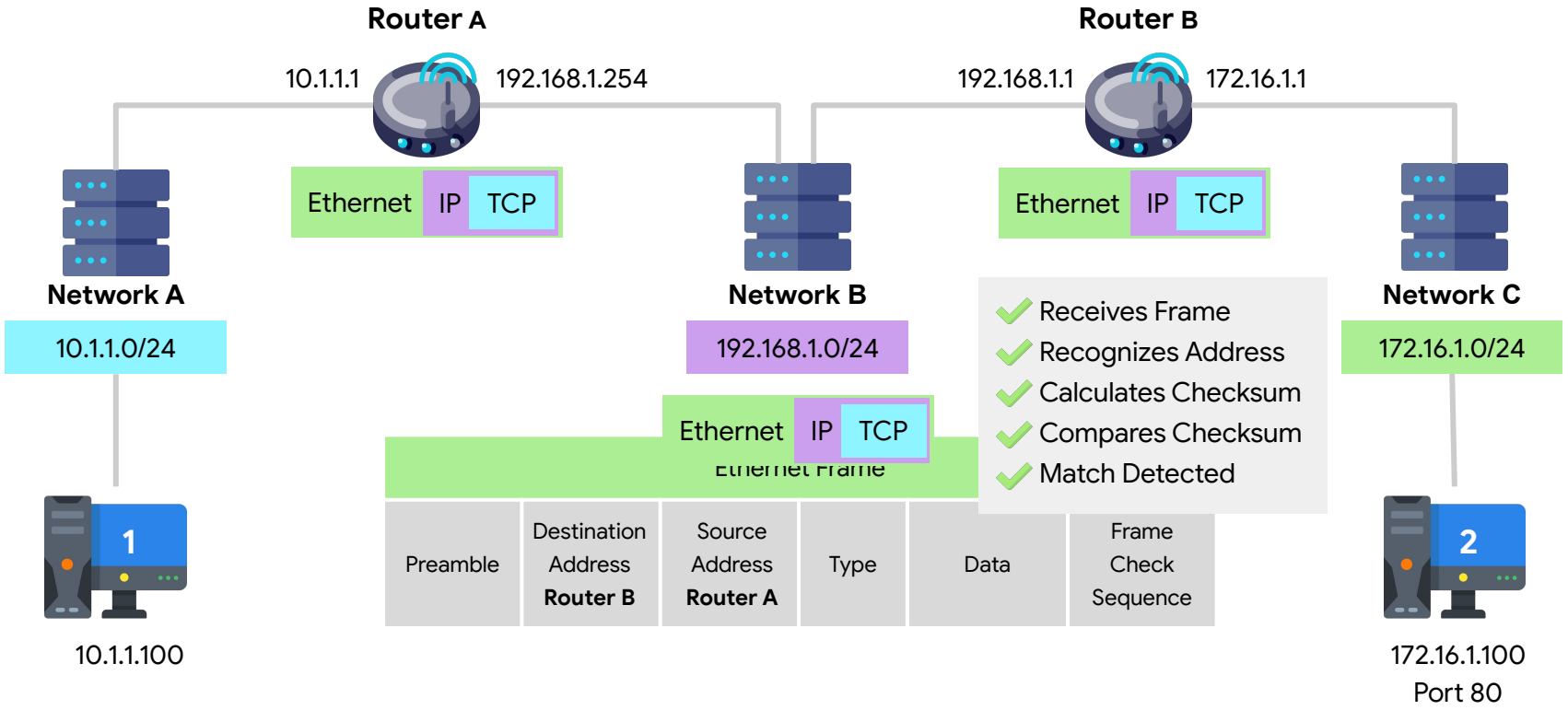
Samart Skills
A Grow with Google PROGRAM

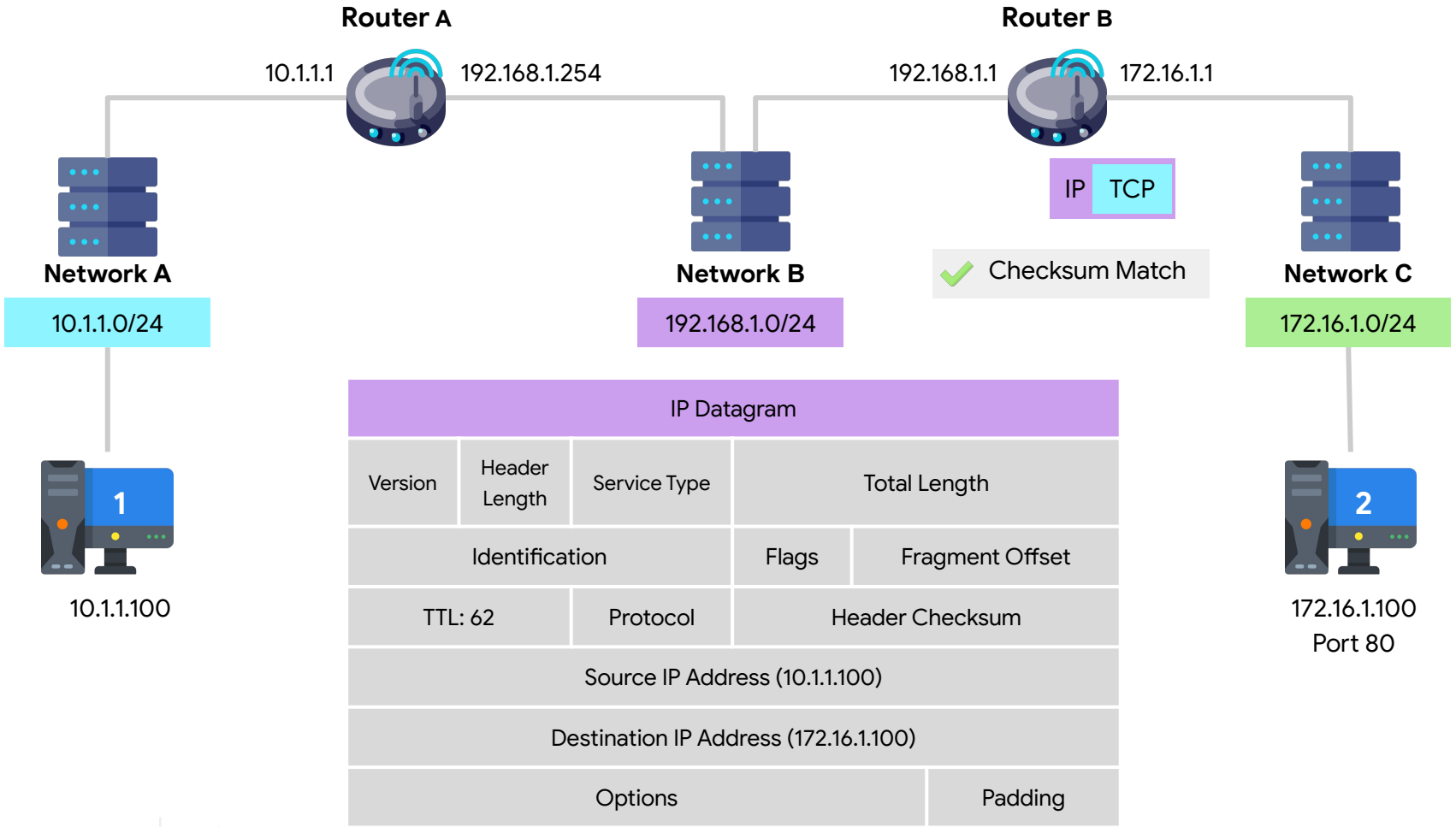
Skooldio

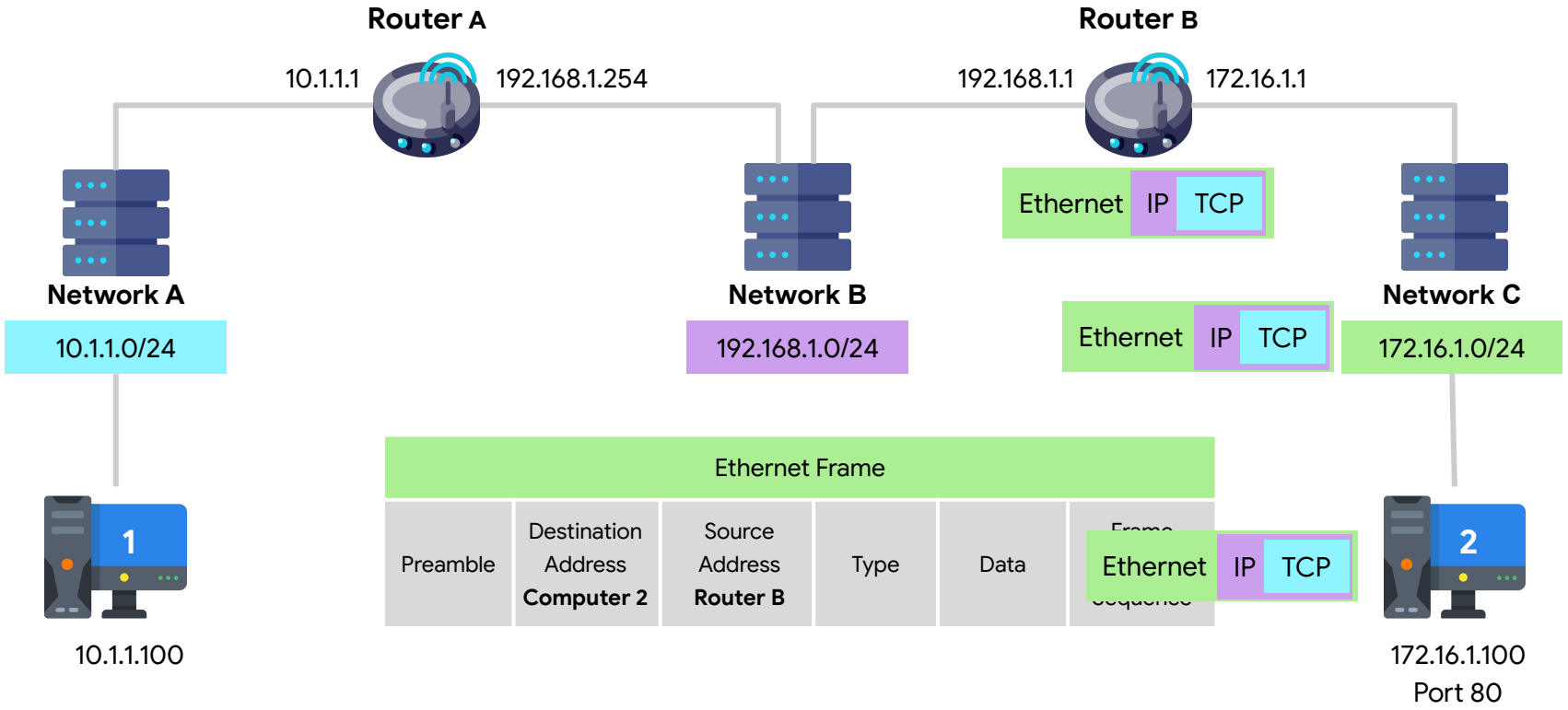

Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
1
Ethernet
IP
TCP
10.1.1.100
2
172.16.1.100
Port 80
Ethernet Frame
Preamble
Destination Address Router A
Source Address Computer 1
Type
Data
Frame Check Sequence
Ethernet
IP
TCP

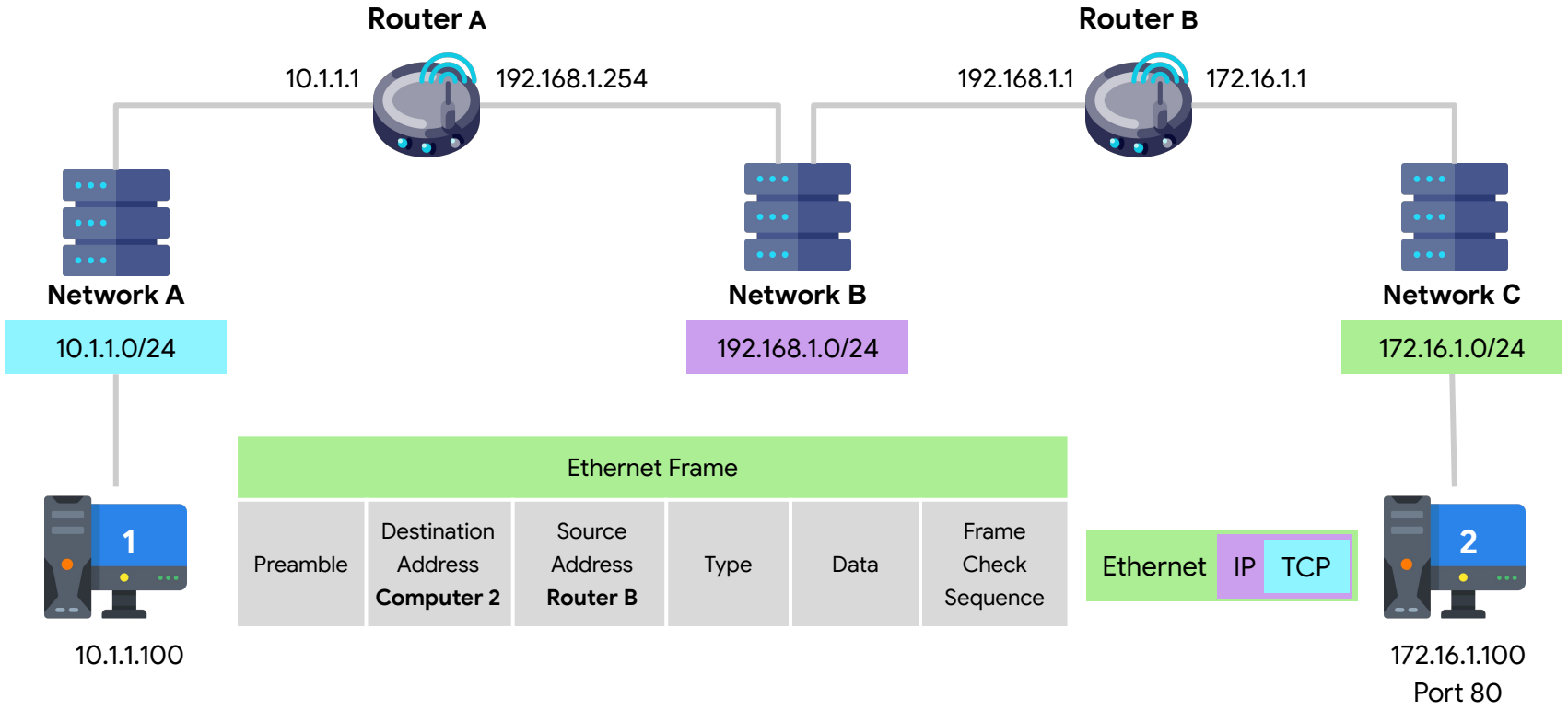

Router A
Router B
10.1.1.1
192.168.1.254
192.168.1.1
172.16.1.1
Ethernet
IP
TCP
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
Receives Frame
Recognizes Address
Calculates Checksum
Compares Checksum
Match Detected
Ethernet
IP
TCP
1
2
10.1.1.100
172.16.1.100
Port 80

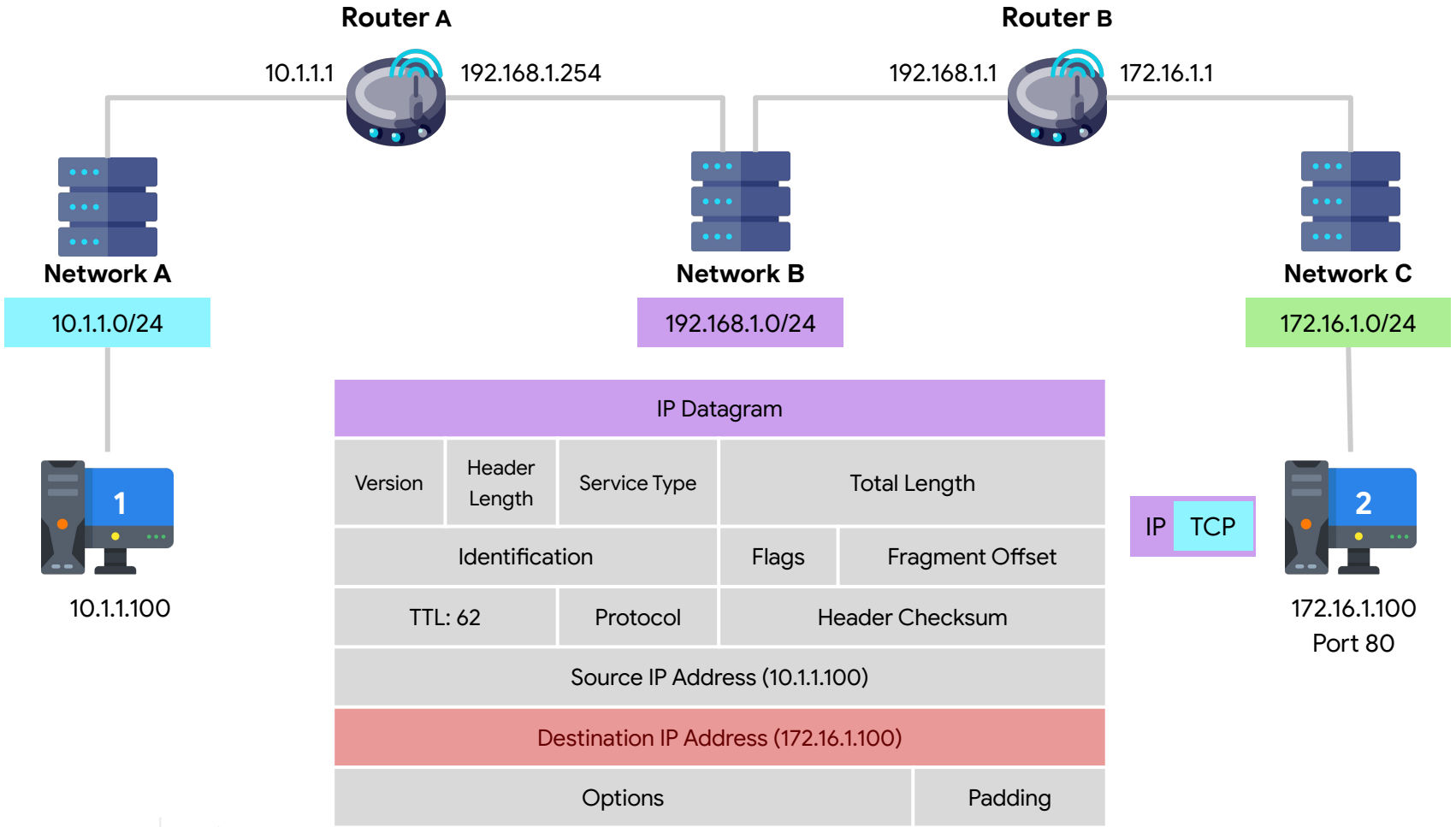

Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Ethernet
IP
TCP
Checksum Match
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
1
10.1.1.100
2
172.16.1.100
Port 80
IP Datagram
Version
Header Length
Service Type
Total Length
Identification
Flags
Fragment Offset
TTL: 63
Protocol
Header Checksum
Source IP Address (10.1.1.100)
Destination IP Address (172.16.1.100)
Options
Padding

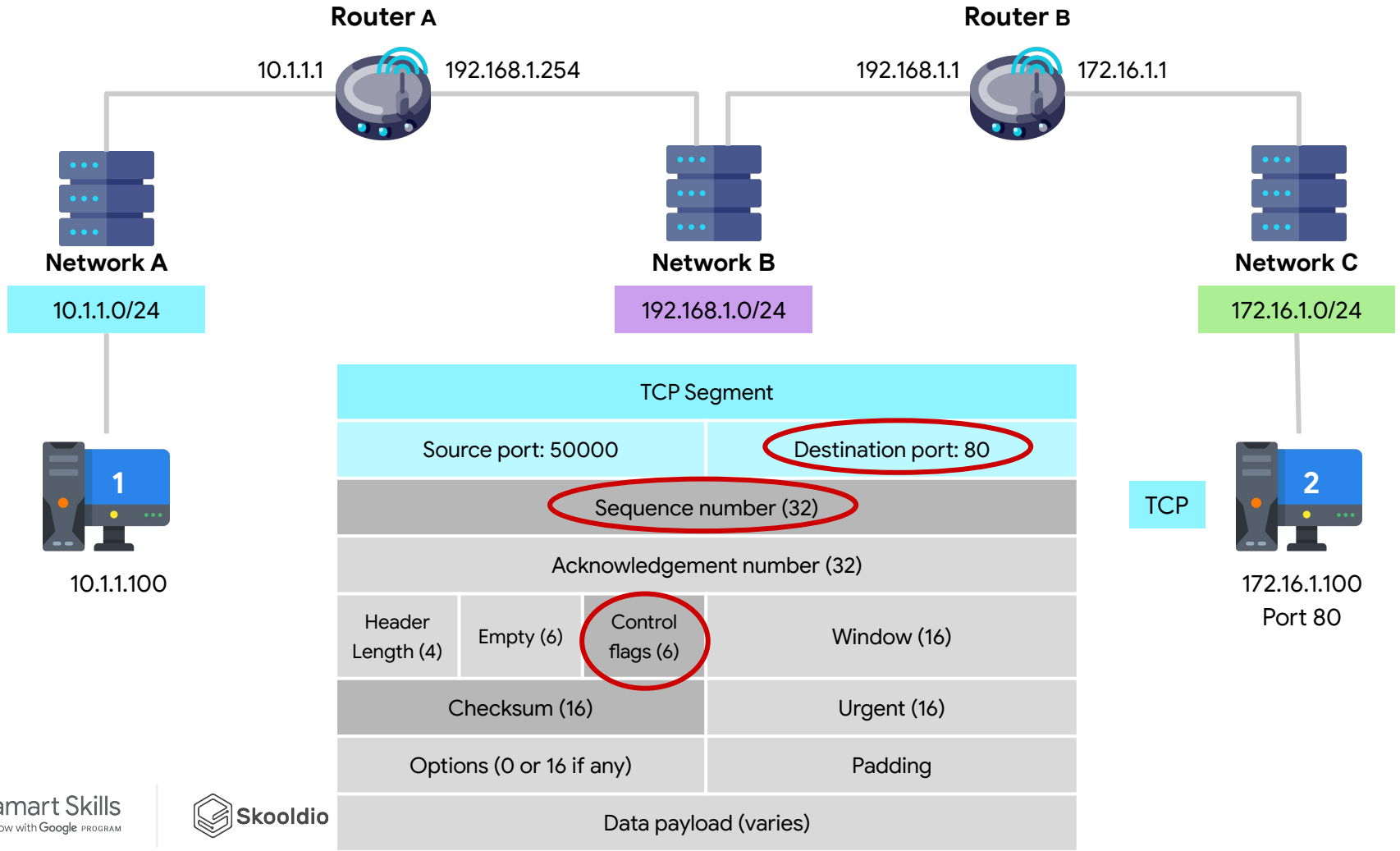

Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Ethernet IP TCP
Ethernet IP TCP
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
Ethernet IP TCP
Ethernet Frame
Preamble
Destination Address Router B
Source Address Router A
Type
Data
Frame Check Sequence
Receives Frame
Recognizes Address
Calculates Checksum
Compares Checksum
Match Detected
1
2
10.1.1.100
172.16.1.100
Port 80


Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
IP
TCP
Checksum Match
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
1
10.1.1.100
2
172.16.1.100
Port 80
IP Datagram
Version
Header Length
Service Type
Total Length
Identification
Flags
Fragment Offset
TTL: 62
Protocol
Header Checksum
Source IP Address (10.1.1.100)
Destination IP Address (172.16.1.100)
Options
Padding


Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
Ethernet IP TCP
Ethernet IP TCP
Ethernet IP TCP
Ethernet Frame
Preamble
Destination Address Computer 2
Source Address Router B
Type
Data
1
2
10.1.1.100
172.16.1.100
Port 80

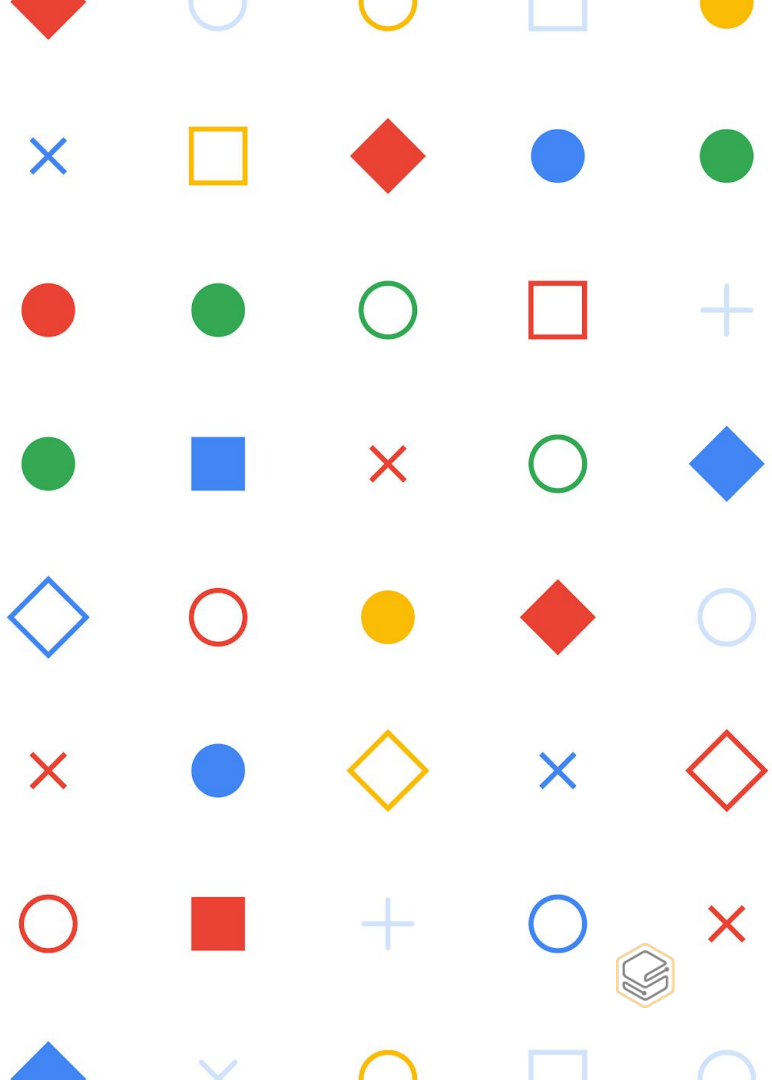

Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
Ethernet Frame
Preamble
Destination Address Computer 2
Source Address Router B
Type
Data
Frame Check Sequence
Ethernet
IP
TCP
1
2
10.1.1.100
172.16.1.100
Port 80


Router A
10.1.1.1
192.168.1.254
Router B
192.168.1.1
172.16.1.1
Network A
10.1.1.0/24
Network B
192.168.1.0/24
Network C
172.16.1.0/24
1
10.1.1.100
2
172.16.1.100
Port 80
IP
TCP
IP Datagram
Version
Header Length
Service Type
Total Length
Identification
Flags
Fragment Offset
TTL: 62
Protocol
Header Checksum
Source IP Address (10.1.1.100)
Destination IP Address (172.16.1.100)
Options
Padding



Week 4

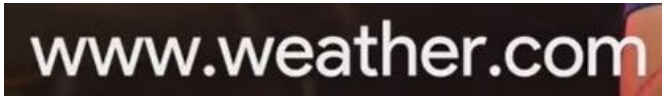
Networking Services

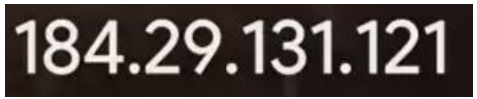


Samart Skills
A Grow with Google PROGRAM

Skooldio

Name Resolution





Domain Name System (DNS) คือ ระบบที่ทำหน้าที่ Name Resolution คือการจับคู่ระหว่างชื่อ (Domain Name) กับ IP Addresses

- DNS จะใช้ UDP Port 53 ในการสื่อสาร

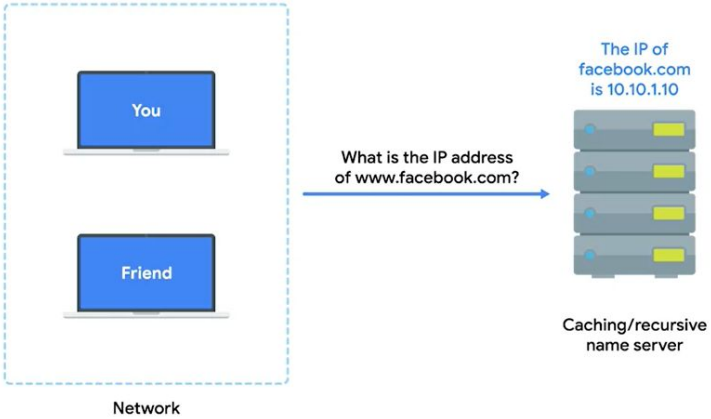
ประโยชน์:

- ง่ายต่อการจำ Address
- ง่ายในการจับคู่เมื่อต้องการเปลี่ยน IP Address เป็นอันใหม่

DNS Server แบ่งออกเป็น 5 ประเภทคือ

- Caching Name Servers
- Recursive Name Servers
- Root Name Servers
- TLD Name Servers
- Authoritative Name Servers

Name Resolution



Caching Name Servers ทำหน้าที่เก็บค่าของ Name-IP Address ไว้ระยะเวลาหนึ่ง

- Time To Live (TTL) เป็นระยะเวลา (วินาที) ที่จะเก็บค่า Cache เอาไว้ ก่อนที่จะทิ้งและร้องขอ Full DNS/Recursive Resolution ใหม่

Recursive Name Server ทำหน้าที่ในการร้องขอ Full DNS/Recursive Resolution

- ส่วนใหญ่แล้ว Caching Name Server มักทำหน้าที่เป็น Recursive Name Server ด้วย
- Caching and Recursive Name Servers มักให้บริการโดย Internet Service Provider (ISP) หรือ Local Network

Name Resolution

Root Name Servers ทำหน้าที่ในการจับคู่ Name-IP Address ให้ไปหา TLD Name Server ต่อไปได้

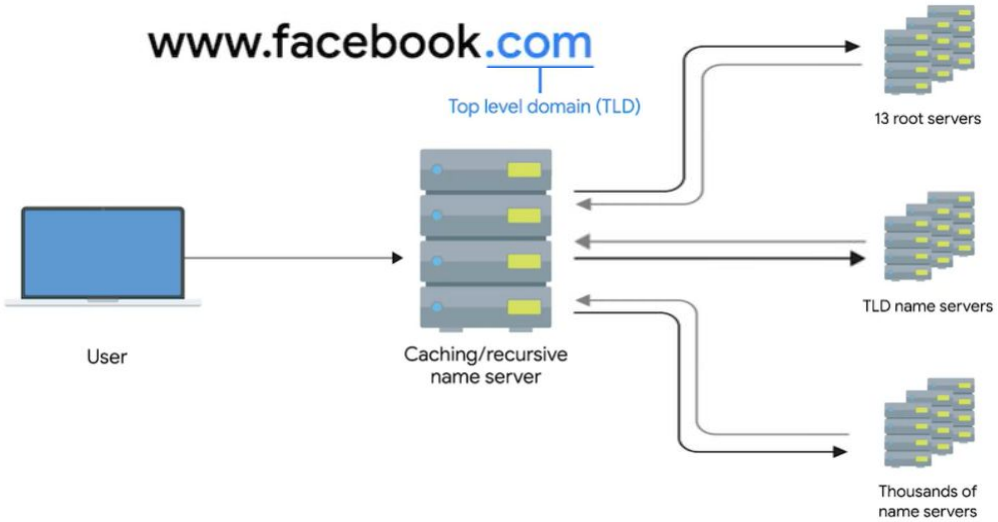
- ในอดีตมีทั้งหมด 13 เครื่องกระจายอยู่ตามพื้นที่ต่าง ๆ ทั่วโลก
- Anycast เป็นวิธีการที่ทำให้หนึ่ง IP Address ถูกแชร์กับหลาย ๆ อุปกรณ์ได้
    - **Anycast** เป็นเทคนิคที่ใช้ในการหาเส้นทางไปหาอุปกรณ์ปลายทาง (Destination) ที่แตกต่างกันขึ้นกับปัจจัยต่าง ๆ เช่น สถานที่ (Location), ความหนาแน่นของ Traffic (Congestion) เป็นต้น

TLD (Top-Level Domain) Name Servers ทำหน้าที่ในการจับคู่ Name-IP Address ให้ไปหา Authoritative Name Servers

Authoritative Name Servers ทำหน้าที่ในการจับคู่ Name-IP Address ของ Domain Name นั้น ๆ

Name Resolution

Full Recursive Resolution จะเกิดขึ้นเมื่อ Name Servers นั้นไม่มีข้อมูลของ Name-IP Address



Name Resolution in Practice

DNS Record Types

- **A Record**: จับคู่ Name-IPv4 Address
  - หนึ่งชื่อสามารถมีหลาย IP Address ได้ ซึ่งจะทำให้เราสามารถทำ DNS Round Robin ได้ เป็นการ Balance Traffic ไม่ให้หนักที่ IP Address หนึ่ง
  - **Round Robin** เป็นเทคนิคในการวนไปตามรายการที่มีตามลำดับ เมื่อครบตามรายการจะวนกลับไปเริ่มต้นที่ลำดับแรกของรายการ
- **AAAA (Quad A) Record**: จับคู่ Name-IPv6 Address

Name Resolution in Practice

CNAME Record: Redirect Traffic จาก Domain Name หนึ่งไปยังอีก Domain Name หนึ่ง

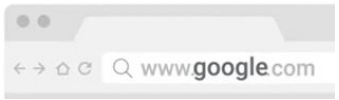
- ตัวอย่าง: microsoft.com ถูก Redirect ไปที่ www.microsoft.com
- ช่วยให้ง่ายในการเปลี่ยน IP Address ในภายหลัง

MX Record: ใช้เพื่อให้ส่ง Email ไปหา Mail Server ที่ถูกต้อง

SRV Record: ใช้ในการบอกค่า Parameters ต่าง ๆ ของ Service เช่น Protocol และ Port ที่ใช้

TXT Record: ใช้ในการบอกข้อมูลเพิ่มเติม

Name Resolution in Practice



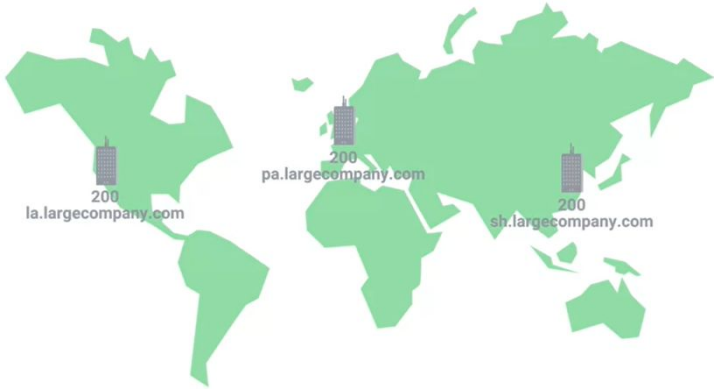
Domain Name ประกอบด้วย 3 ส่วนคือ

- **Top Level Domain** (TLD): เช่น .com, .net, .edu, .cn, .th, .museum, .pizza, etc.
  - The Internet Corporation for Assigned Names and Numbers (ICANN) ทำหน้าที่จัดการเกี่ยวกับ TLD Names
- **Domain**: บอกถึงจุดสิ้นสุดในการควบคุมจาก TLD Name Server และเริ่มต้นการควบคุมโดย Authoritative Name Server
  - **Registrar** ทำหน้าที่ในการจดทะเบียน Domain Name
- **Subdomain** หรือ Hostname เป็น Domain ย่อยภายใต้องค์กรเดียวกัน ซึ่งสามารถรองรับ Subdomain ได้ถึง 127 levels

Fully Qualified Domain Name (FQDN) คือ ชื่อเต็มที่รวมทั้ง 3 ส่วนเข้าด้วยกัน

- แต่ละส่วนจะมีความยาวตัวอักษรได้แค่ 63 ตัวเท่านั้น และหนึ่ง FQDN จะมีความยาวตัวอักษรได้สูงสุดที่ 255 ตัว

Name Resolution in Practice



Authoritative DNS จะรับผิดชอบสำหรับ DNS Zone ที่ระบุไว้สำหรับตัวมันเท่านั้น

- Root DNS Root Zone
- TLD DNS TLD Zone
- Authoritative DNS Its Zone

DNS Zone ทำให้สามารถควบคุม Multiple Levels ของ Domain หนึ่งได้ง่าย

- ตัวอย่าง: แทนที่จะมี 1 Zone สำหรับ 600 ชื่อ เราสามารถแยกออกเป็น 3 Zones เพื่อให้ง่ายในการควบคุม (รวมทั้งหมดจะมี 4 Zones)

Name Resolution in Practice

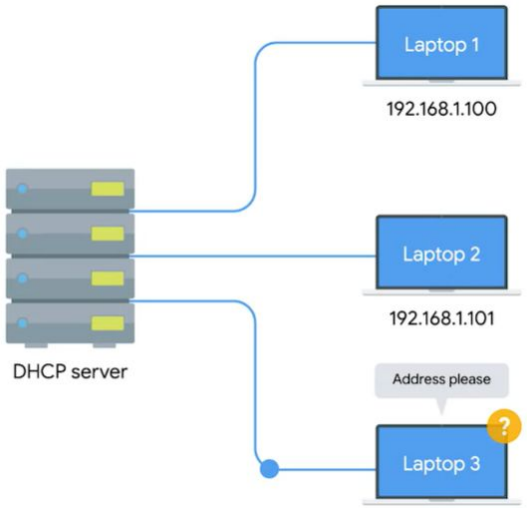
Zone Files ใช้ในการปรับแต่งค่าเกี่ยวกับ DNS Zone

- SOA (Start Of Authority) Record: ใช้ในการประกาศชื่อ Zone และ Name Server ที่มีอำนาจหน้าที่รับผิดชอบ (Authoritative) สำหรับ Zone นั้น
- NS Record: บอกเกี่ยวกับ Name Servers อื่น ๆ ที่อาจจะรับผิดชอบสำหรับ Zone นั้น
    - เผื่อว่า Name Server หนึ่งใช้งานไม่ได้ จะได้มีตัวสำรอง

Reverse Lookup Zone Files อนุญาตให้ DNS สามารถจับคู่กลับจาก IP Address มาเป็น FQDN ได้

- PTR (Pointer) Record: จับคู่ IP Address-Name

Dynamic Host Configuration Protocol



Dynamic Host Configuration Protocol (DHCP) ใช้ในการจัดสรรค่า Network Setting ต่าง ๆ ให้คอมพิวเตอร์อย่างอัตโนมัติ ซึ่งหลัก ๆ จะมีอยู่ 4 ค่า คือ

- IP Address
- Subnet Mask
- Gateway
- Name Server

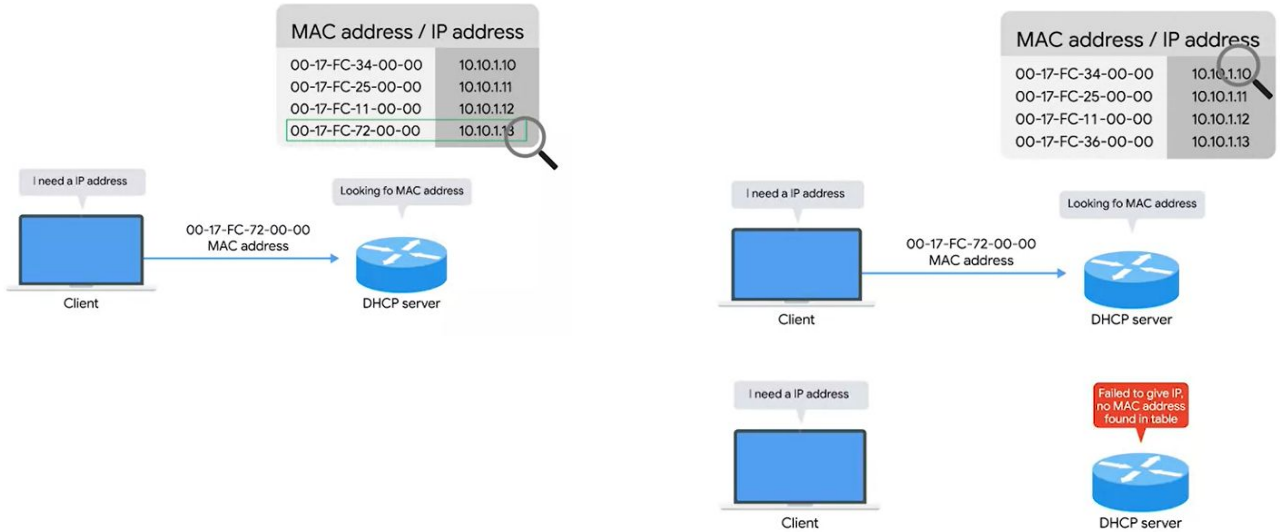
นอกจากนี้ DHCP ยังสามารถจัดสรรค่า NTP Server ได้

- NTP (Network Time Protocol) ทำให้อุปกรณ์ต่าง ๆ ใน Network มีเวลาตรงกัน (Synchronized)

สำหรับ Servers หรือ Network Devices ควรใช้ Static IP Address (Manually)

Dynamic Host Configuration Protocol

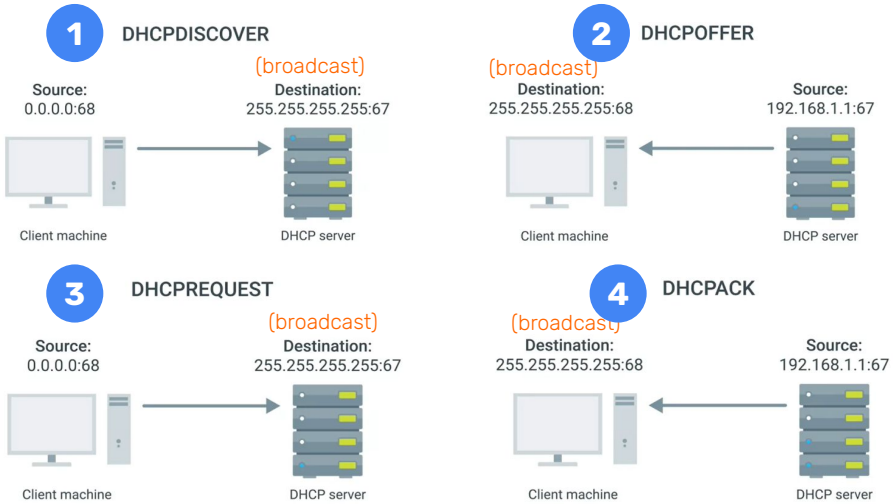
3. **Fixed Allocation คือ** การแจก IP Address แบบเฉพาะเจาะจงสำหรับ MAC Address ที่เชื่อมต่อเข้ามา โดยต้องมีการจับคู่ MAC Address และ IP ไว้ล่วงหน้า



Dynamic Host Configuration Protocol

DHCP ใช้ Port UDP 67 และ 68 ในการทำงาน

DHCP Discovery Process คือ กระบวนการทำงานเพื่อให้อุปกรณ์หนึ่งได้รับค่า Network Settings ซึ่งมีทั้งหมด 4 ขั้นตอนดังนี้

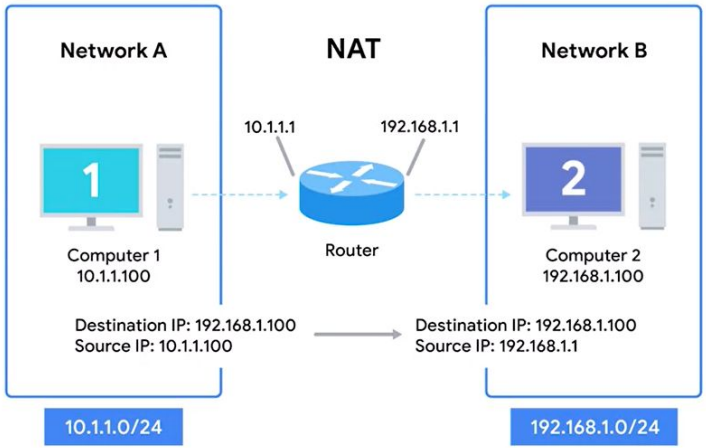


Dynamic Host Configuration Protocol

DHCP Lease คือ ค่า Network Settings ที่ DHCP แจกให้ โดยจะมีอายุการใช้งานกำกับไว้

- หาก Lease หมดอายุ DHCP Client จะทำ DHCP Discovery Process ใหม่อีกครั้งเพื่อให้ได้ค่า Lease ใหม่

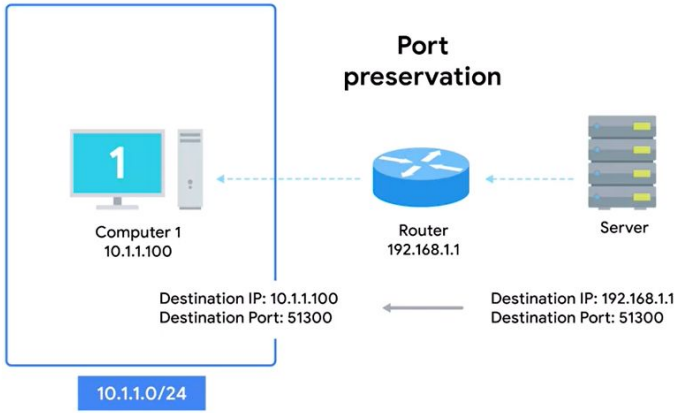
Network Address Translation



Network Address Translation (NAT) คือเทคนิคในการแปลง IP Address หนึ่งไปเป็นอีก IP Address หนึ่ง

- Gateway (Router/Firewall) สามารถเขียนทับ Source IP ของ IP Datagram ขาออกได้ ในขณะที่มีการจำ Original Source IP ไว้ เพื่อจะได้ใช้เขียนทับในการตอบกลับ (Response)
- **IP Masquerading** คือ การซ่อน IP ต้นทางเอาไว้ และใช้ IP ของ Gateway ในการติดต่อ
  - เราสามารถซ่อน IP ของทั้ง Network จากภายนอกได้ โดยใช้เทคนิคที่เรียกว่า **One-to-Many NAT**

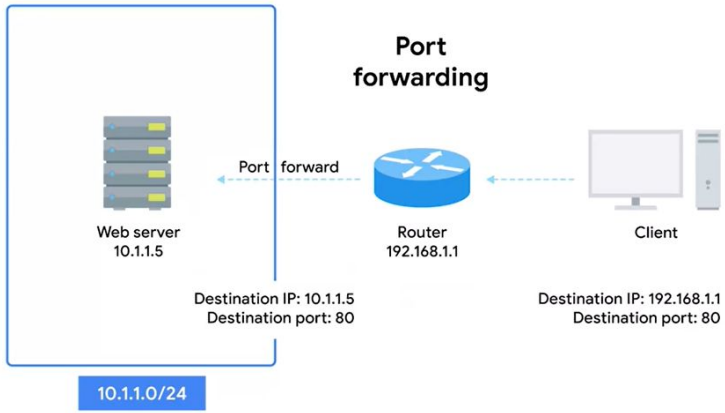
Network Address Translation



Port Preservation เป็นการนำ Source Port ที่ถูกเลือกโดย Client มาเป็น Port เดียวกันกับที่ถูกใช้โดย Router

- ตั้งแต่ตอน NAT ขาออก Router จะบันทึก Source Port ที่ Client ใช้ในการติดต่อเข้ามา และ Router จะใช้ Port นั้นในการส่ง Traffic กลับไปให้ Client เดิมได้

Network Address Translation



Port Forwarding เป็นเทคนิคที่ให้เราระบุ Destination Port เพื่อส่งต่อไปยังอุปกรณ์ที่เราต้องการ

- เทคนิคนี้ทำให้เราซ่อน IP ไว้ได้แต่ยังสามารถให้บริการกับโลกภายนอกและสามารถ Remote Access เข้ามาที่เครื่องใน Internal Network ได้

Network Address Translation

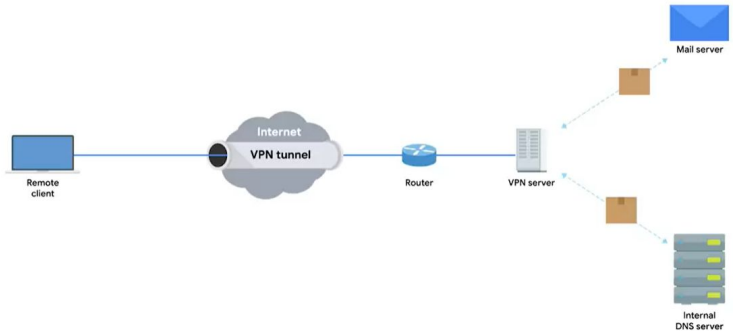
Internet Assigned Numbers Authority (IANA) มีหน้าที่ให้การจัดสรร Address Blocks ให้กับ

5 Regional Internet Registries (RIRs)

- AFRNIC ให้บริการกับ Africa
- ARIN ให้บริการกับ US, Canada และส่วนของ Caribbean
- APNIC ให้บริการกับ Asia, Australia, New Zealand และหมู่เกาะ Pacific
- LACNIC ให้บริการกับ Central and South America และส่วนของ Caribbean ที่ ARIN ไม่ครอบคลุม
- RIPE ให้บริการกับ Europe, Russia, Middle East และส่วนของ Central Asia

IPv4 ไม่เพียงพอต่อการใช้งานแล้ว ทำให้ต้องมี **Non-routable Address Space (RFC1918) และ NAT** มาช่วยแก้ปัญหาเรื่องนี้ก่อนที่ IPv6 จะถูกนำมาใช้อย่างแพร่หลาย

VPNs and Proxies



Virtual Private Network (VPN) เป็นเทคโนโลยีที่ทำให้เราสามารถขยาย Private/Local Network ไปให้กับคอมพิวเตอร์ที่ไม่ได้อยู่ใน Local Network นั้นได้

- VPN ช่วยให้พนักงานสามารถเข้าถึง Network ขององค์กรได้ โดยที่ไม่ต้องนั่งอยู่ที่องค์กร
- VPN เป็น Tunneling Protocol ซึ่งทำให้การสื่อสารมีความปลอดภัยด้วยการเข้ารหัสข้อมูล
- VPN จำเป็นที่จะต้องมีการพิสูจน์ตัวตนอย่างเข้มงวด เพื่อให้มั่นใจว่า VPN จะถูกใช้โดยผู้ที่มีสิทธิ์เท่านั้น
    - **Two-factor Authentication** คือ การพิสูจน์ตัวตนแบบ 2 ปัจจัย ซึ่งโดยมากจะใช้ Password และ OTP

VPNs and Proxies

VPN สามารถทำการเชื่อมต่อแบบ Site-to-Site VPN ได้ ซึ่งจะทำให้สองออฟฟิศที่อยู่ต่างที่กัน รวมเป็น Network เดียวกันได้ผ่าน Tunnel

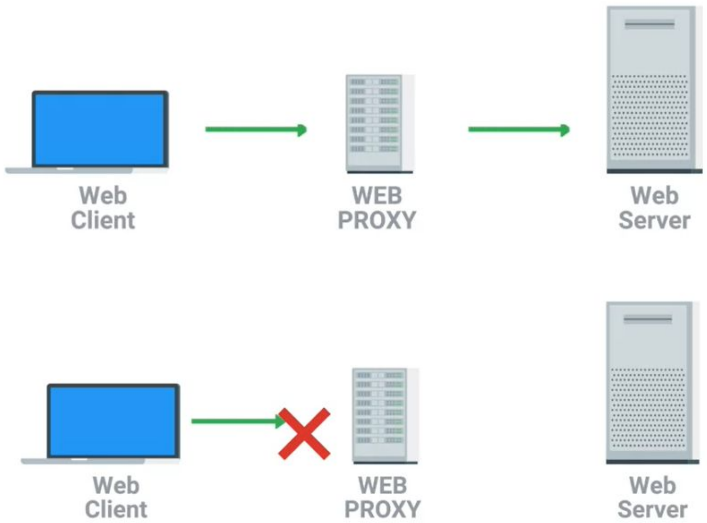
VPNs and Proxies

Proxy เป็นอุปกรณ์ที่ทำหน้าที่เป็นตัวแทนของ Client ในการเข้าถึง Service

ประโยชน์ของ Proxy:

- Anonymity
- Security
- Content Filtering
- Increased Performance

VPNs and Proxies



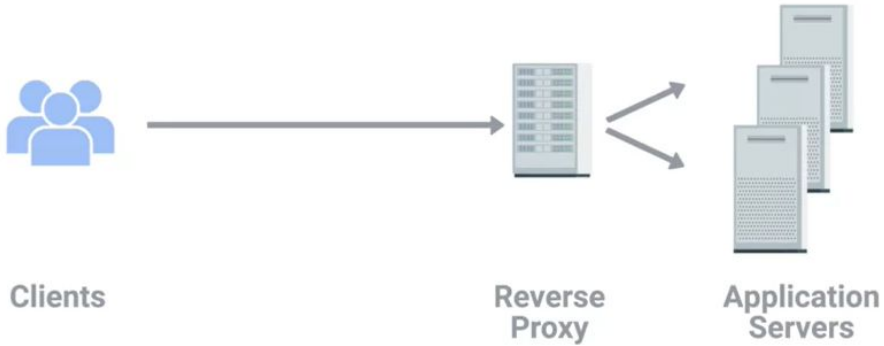
Web Proxy เป็น Proxy ที่ออกแบบมาเพื่อ Web Traffic

- Web Proxy จะจำ (Cache) Web Page ที่ถูกเรียกเอาไว้ หากมี Client อื่นเรียก Web Page เดียวกัน ก็จะสามารถตอบได้เลย
    - ปัจจุบันอินเทอร์เน็ตมีความเร็วเพิ่มขึ้น และเว็บต่าง ๆ ก็เปลี่ยนแปลงไปสำหรับแต่ละผู้ใช้งานมากขึ้น จึงทำให้ Web Proxy ไม่ได้ถูกนำมาใช้ Cache Web Page แล้ว
- Web Proxy สามารถนำมาใช้กรอง (Filtering) การเข้าถึง Website เช่น ห้ามพนักงานใช้ Website Twitter ในช่วงเวลาทำงาน เป็นต้น

VPNs and Proxies

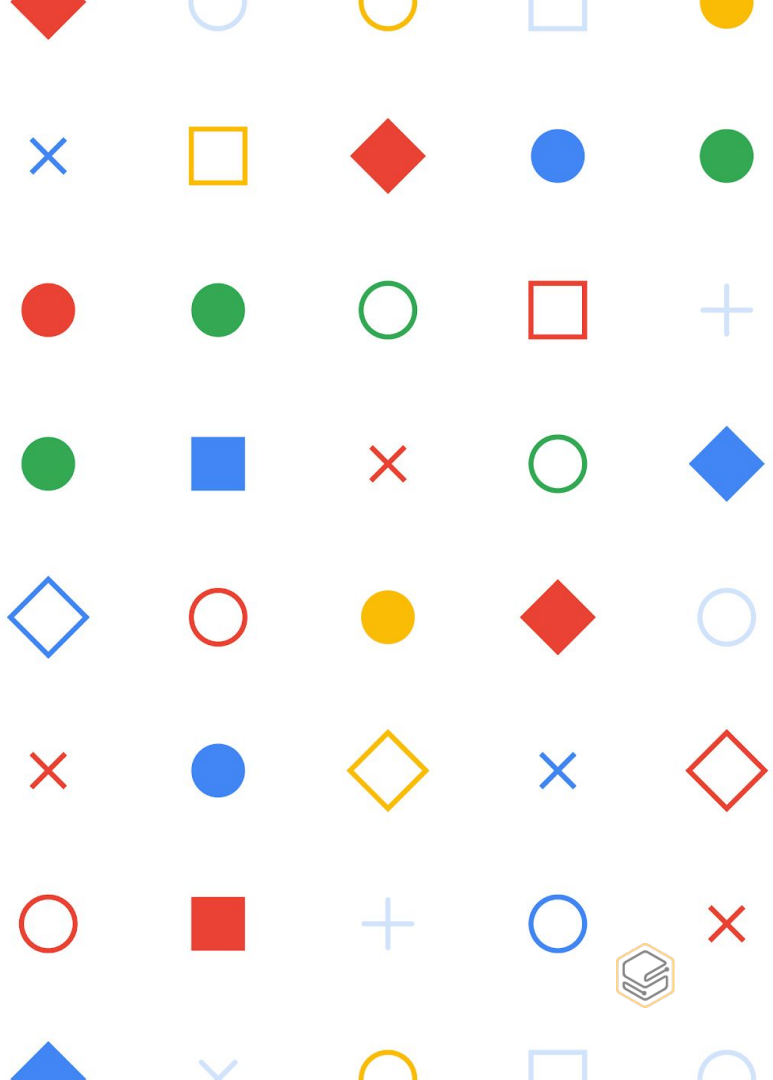
Reverse Proxy เป็น Proxy แบบหนึ่งที่เป็นตัวแทนให้ Client ที่อยู่ภายนอก สามารถเข้าถึง Server ต่าง ๆ ในองค์กรได้

- สามารถทำ Load Balancing ได้



Week 5

Connecting to the Internet



Samart Skills
A Grow with Google PROGRAM

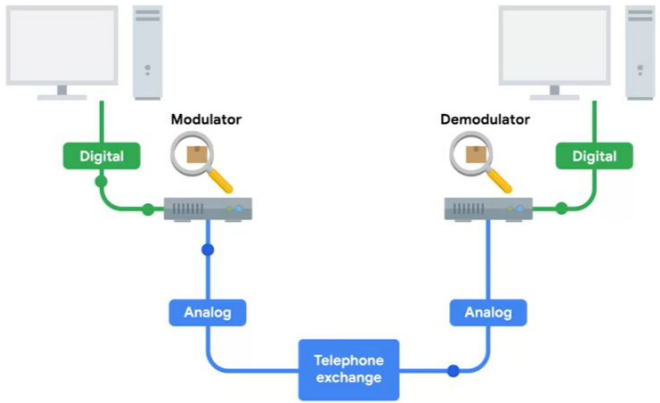
Skooldio

POTS and Dial-up

PSTN (Public Switched Telephone Network) หรือ **POTS** (Plain Old Telephone Service)

เป็นการใช้สายโทรศัพท์ในการรับส่งข้อมูล ทำให้ส่งข้อมูลในระยะไกลได้

POTS and Dial-up



One smartphone photo = 2 Megabytes
2 Megabytes = 16,777,216 bits
16,777,216 bits at 14.4 kilobits/sec = 1165 seconds
1165 seconds = 19.4 minutes

Usenet เป็นวิธีการเชื่อมต่อผ่าน POTS ที่ประสบความสำเร็จเป็นอันแรก และยังคงมีใช้งานอยู่จนมาถึงปัจจุบัน

Dial-up Connection ใช้ POTS เพื่อเชื่อมต่ออินเทอร์เน็ต โดยมีอุปกรณ์ Modem (**Mo**dulator/**Dem**odulator) เป็นตัวเชื่อมต่อ

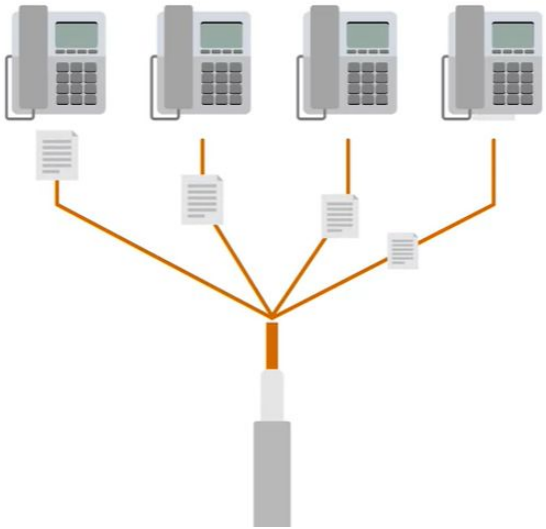
- แปลง Digital ไปเป็น Audible Wavelengths (Analog)
- **Baud Rate (Speed)** คือ วิธีการวัดจำนวน bits ที่สามารถส่งผ่านสายโทรศัพท์ในหนึ่งวินาที (bps)
- ในปีช่วงปี 1990 Dial-up Access มี Baud Rate อยู่ที่ 14.4 kbps

Broadband Connections

Broadband คือ การเชื่อมต่ออินเทอร์เน็ตแบบอื่น ๆ ที่ไม่ใช่แบบ Dial-up

- เป็นการเชื่อมต่อแบบเปิดไว้ตลอดเวลา (Always on) ไม่ต้องต่อเป็นครั้งๆ เหมือน Dial-up
- มีความเร็วสูงกว่า Dial-up มาก

Broadband Connections



T-carrier Technologies คือ เทคโนโลยีที่ใช้ในการส่งการคุยโทรศัพท์ (Phone Call) หลายชุด ผ่านสายโทรศัพท์เส้นเดียว

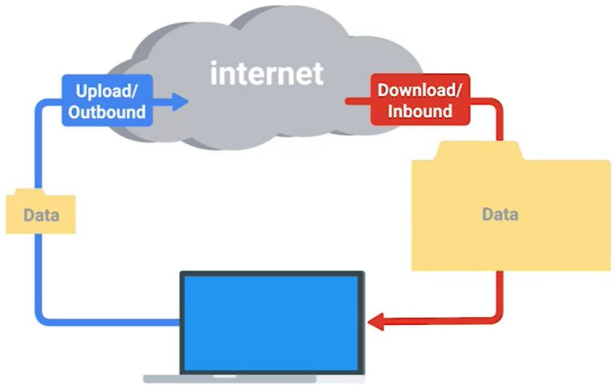
สาย T1 (Transmission System 1)

- เป็นสายทองแดง (Copper) แบบเฉพาะ
- สามารถรองรับได้ 24 Phone Calls
- แต่ละ Phone Call สามารถส่งข้อมูลด้วยความเร็ว 64 kbps
- ดังนั้นสาย T1 หนึ่งเส้น สามารถส่งข้อมูลได้ที่ความเร็ว 1.544 mbps

สาย T3

- รองรับได้เท่ากับสาย T1 28 สาย
- ความเร็ว 44.736 mbps

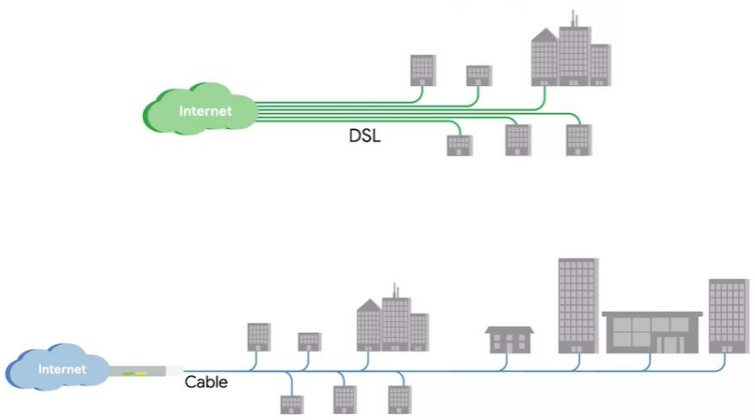
Broadband Connections



Digital Subscriber Line (DSL)

- ใช้สายโทรศัพท์ในการส่งข้อมูล แต่เราสามารถใช้โทรศัพท์ไปพร้อม ๆ กับใช้งานอินเทอร์เน็ตในเวลาเดียวกัน โดยใช้สายชุดเดียวกันได้
- ใช้ Modem แบบเฉพาะที่เรียกว่า **DSLAMs** (Digital Subscriber Line Access Multiplexers)
  - ต่อครั้งเดียวใช้ได้ยาวจนกว่าจะปิดอุปกรณ์ DSLAM (Always on)
  - **ADSL** (Asymmetric DSL) มีความเร็วในการ Download และ Upload ไม่เท่ากัน
  - **SDSL** (Symmetric DSL) มีความเร็วในการ Download และ Upload เท่ากัน โดยมีความเร็ว 1.544 mbps (เท่ากับ T1)
  - **HDSL** (High bit-rate DSL) มีความเร็วมากกว่า 1.544 mbps

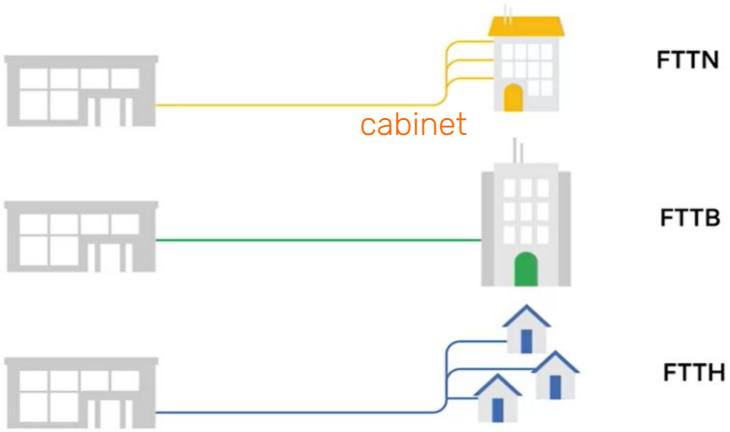
Broadband Connections



Cable Broadband

- TV Broadcast เริ่มต้นโดยใช้เทคโนโลยี Wireless
- ช่วงปี 1990 cable TV Infrastructure มีขนาดพอ ๆ กับ POTS
- ใช้สาย Coaxial ในการส่งข้อมูล
- ถ้าเป็น DSL จะต่อตรงจากบ้านไปหา Central Office (CO) ซึ่งทำให้สามารถรับประกันเรื่องความเร็วได้ เพราะเป็น Point-to-Point หรือเรียกว่า Dedicated Bandwidth
- Cable Broadband เป็นเทคโนโลยีแบบ **Shared Bandwidth** คือ แต่ละบ้านต่อผ่านช่องทางเดียวกันเพื่อไปถึงผู้บริการ ซึ่งอาจทำให้ไม่สามารถรับประกันเรื่องความเร็วได้
- Cable Modem เป็นอุปกรณ์ที่อยู่ที่ฝั่งผู้ใช้งาน ใช้ในการเชื่อมต่อไปที่ **Cable Modem Termination System (CMTS)** ที่อยู่ที่ผู้ให้บริการ

Broadband Connections



Fiber Connection สามารถส่งข้อมูลได้ระยะหลายไมล์ด้วยความเร็วสูง

- สมัยก่อนมีราคาค่อนข้างแพง จึงนิยมใช้ในกลุ่มผู้ให้บริการอินเทอร์เน็ต สำหรับ Core Network
- ในปัจจุบันมีให้ใช้สำหรับกลุ่มผู้ใช้งานทั่วไปแล้วในรูปแบบของ FTTX (Fiber To The X)
  - **FTTN** (Fiber To The Neighborhood)
  - **FTTB** (Fiber To The Building)
  - **FTTH** (Fiber To The Home)
- **Optical Network Terminator (ONT)** เป็นอุปกรณ์ที่ทำหน้าที่แปลง Protocol จาก Fiber ไปเป็น Twisted-pair Copper

FTTP
(Fiber To The Premises)

WANs

WAN (Wide Area Network) คือ Network ที่ครอบคลุมหลาย ๆ พื้นที่

- มักจะต้องใช้บริการอินเทอร์เน็ตกับ ISP เพื่อให้สามารถเชื่อมต่อข้ามพื้นที่ได้ ซึ่งจะทำให้คอมพิวเตอร์ในองค์กรที่อยู่ต่างสาขาเสมือนเชื่อมต่ออยู่ใน Network เดียวกัน
- Demarcation Point คือ จุดสิ้นสุดของ Network ของผู้ใช้บริการและเป็นจุดเริ่มต้นของ ISP Network เช่น ONT เป็น Demarcation Point สำหรับ Fiber Connection
- พื้นที่ระหว่าง Demarcation Point และ ISP Network จะถูกเรียกว่า Local Loop ซึ่งสามารถถูกเชื่อมต่อกันด้วย T-carrier หรือ Fiber Connection
- มีหลาย Data Link Layer Protocols ที่ใช้ในการส่งข้อมูลข้าม WAN ได้

WANs

Point-to-Point (Site-to-Site) VPN คือ การใช้ VPN ทำ Tunnel ผ่านอินเทอร์เน็ตเพื่อเชื่อมต่อกันระหว่างสองพื้นที่

- ไม่ต้องอาศัยการเชื่อมต่อแบบ Dedicated High-speed WAN
- สามารถใช้ Router หรือ Firewall เป็นอุปกรณ์ในการเชื่อมต่อของทั้งสองฝั่ง
- ไม่จำเป็นต้องตั้งค่าการเชื่อมต่อใด ๆ บนเครื่องผู้ใช้งาน

Wireless Networking

Wireless Networking คือ วิธีการเชื่อมต่อ Network โดยไม่ใช้สาย (WiFi)

- IEEE802.11 เป็นมาตรฐานที่กำหนดคุณสมบัติและวิธีการสำหรับอุปกรณ์ต่าง ๆ ในการทำ Wireless Network บางครั้งเราจะเรียกว่า 802.11 Family
  - 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac
  - แต่ละมาตรฐาน 802.11 นั้น จะใช้ Protocol พื้นฐานเหมือนกันแต่จะต่างกันที่ Frequency Band ที่ใช้

Frequency Band คือ ความกว้างของคลื่นความถี่ที่ได้มีการตกลงร่วมกันเพื่อใช้สำหรับการสื่อสารหนึ่ง

- WiFi จะใช้ 2.4 GHz และ 5 GHz
  - 5 GHz จะมีความเร็วสูงกว่า แต่ใช้ได้ในระยะทางที่สั้นกว่า

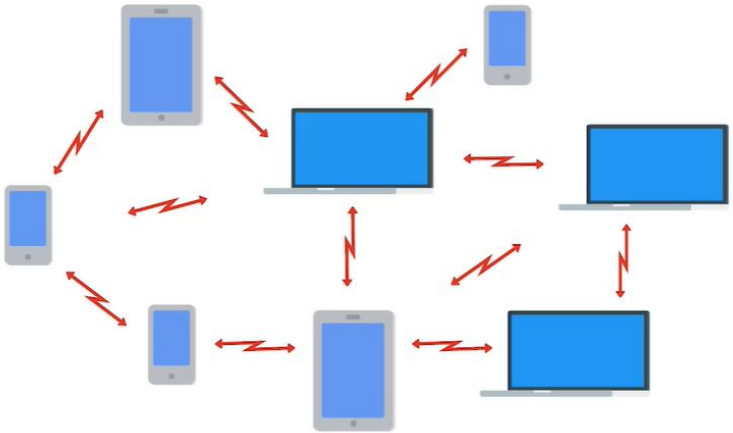
Wireless Networking

802.11 Protocols ทำงานอยู่ทั้งบน Physical Layer และ Data Link Layer

802.11 Frame ประกอบด้วยข้อมูลต่าง ๆ ดังนี้

- **Frame Control:** มีความยาว 16 bits ใช้ในการบอกรายละเอียดเกี่ยวกับ frame นั้นเอง เช่น Version ของ 802.11
- **Duration/ID:** มีความยาว 16 bits ใช้ในการบอกความยาวทั้งหมดของ Frame
- **Address 1-4:** ใช้ในการบอกว่า Access Point ตัวไหนทำหน้าที่รับ Frame
- **Sequence Control:** มีความยาว 16 bits ใช้ในการติดตามลำดับการรับส่ง Frame
- **Frame Check Sequence (FCS):** มีความยาว 32 bits ใช้บอกค่า Checksum

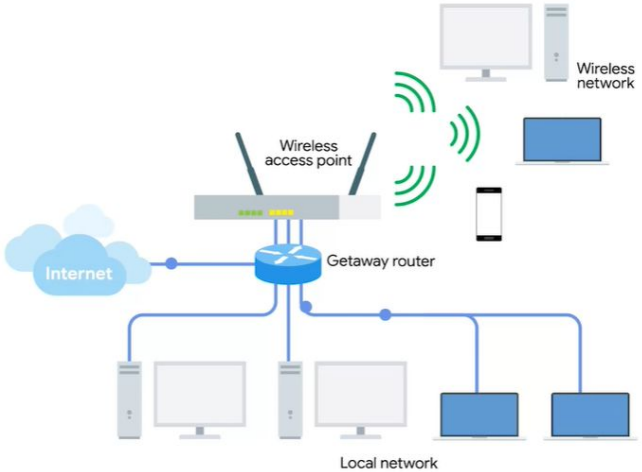
Wireless Networking



Wireless Network Configurations

- **Ad-hoc Network**: อุปกรณ์สื่อสารกันเองโดยตรง
  - นิยมใช้กับ Smartphone ในการส่งข้อมูลหากัน เช่น รูปหรือวีดีโอ เป็นต้น

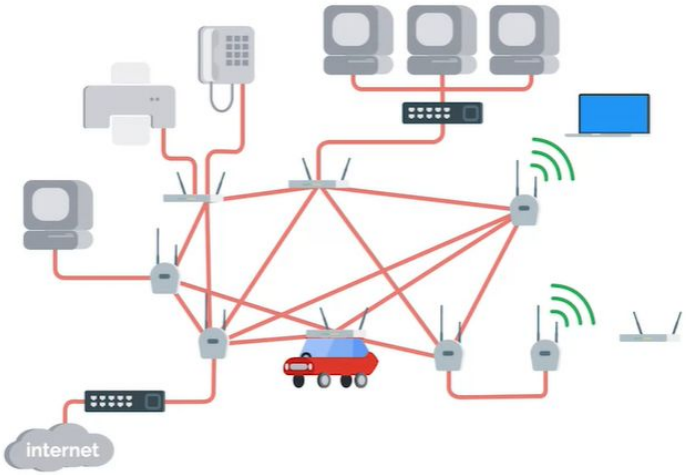
Wireless Networking



Wireless Network Configurations

- **Wireless LAN (WLAN)**: ใช้ Access Point เป็นสะพาน (Bridge) เชื่อมต่อระหว่าง Wireless และ Wired Network
  - อาจใช้ AP หลายตัวในการทำให้ครอบคลุมพื้นที่วงกว้าง
  - อุปกรณ์ที่ต้องการเชื่อมต่อ Wireless Network จะต้องเชื่อมต่อ (Associate) มาที่ AP ซึ่งโดยมากจะเชื่อมต่อตัวที่สัญญาณดีที่สุด
  - AP จะส่ง Traffic ต่อไปที่ Gateway Router เพื่อเชื่อมต่อกับ LAN ทำให้สามารถส่งข้อมูลไปอินเทอร์เน็ตได้

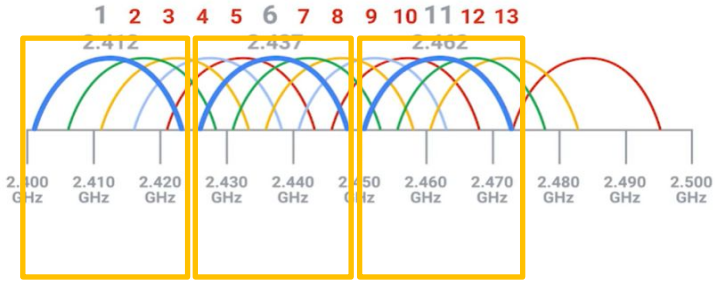
Wireless Networking



Wireless Network Configurations

- **Mesh Network**: ผสมกันระหว่าง Ad-hoc และ WLAN
  - ช่วยเพิ่มระยะทาง (Range) และประสิทธิภาพ (Performance) ของ WLAN

Wireless Networking



Wireless Channels คือ ช่องสัญญาณ ซึ่งเป็นส่วนย่อย ๆ ของ Frequency Band

- ตัวอย่าง: 2.4 GHz band บน 802.11b Wireless Network หมายถึง ความกว้างตั้งแต่ 2.400 GHz ถึง 2.500 GHz โดยประมาณ

  ซึ่งสามารถแบ่งย่อยเป็น Channel ได้ 13 Channels แต่ละ Channel จะมีความกว้าง 22 MHz โดยเริ่มตั้งแต่ 2.412 GHz

  - ช่วยแก้ปัญหา Collision Domain บน Wireless Network
  - การสื่อสารที่มีการทับซ้อน (Overlap) กันของ Channel อาจทำให้เกิด Data Collision ดังนั้นเราจะต้องใช้ Channel ที่ไม่ทับซ้อนกันให้ได้มากที่สุด เช่น 1, 6, 11
  - AP มีความสามารถในการตรวจสอบ Channel ที่หนาแน่นและเปลี่ยนไปใช้ Channel ที่ไม่หนาแน่นให้อัตโนมัติ

Wireless Networking

Wireless Security

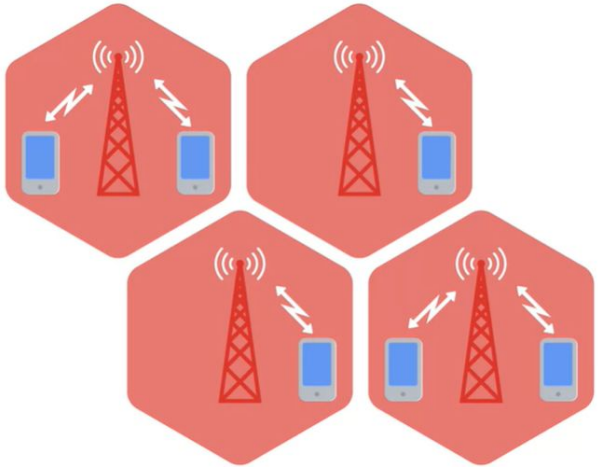
- บน Wireless Network เครื่องที่อยู่ในพื้นที่ครอบคลุมจะสามารถดักจับ Traffic ของเครื่องอื่น ๆ ได้
- **WEP** (Wired Equivalent Privacy) เป็นเทคนิคในการเข้ารหัสข้อมูล (Encryption) เพื่อไม่ให้คนที่ไม่มีสิทธิ์เข้าใจข้อมูลได้
    - แต่ WEP ใช้ Encryption Algorithm อ่อนแอ และใช้ความยาว Key สั้นเกินไป (40 bits) ทำให้ผู้ไม่ประสงค์ดีสามารถถอดรหัสข้อความได้โดยง่าย
- **WPA** (WiFi Protected Access) ถูกคิดค้นมาใช้ทดแทน WEP แบบชั่วคราว ก่อนที่จะมี WPA2
    - ความยาว Key 128 bits
- **WPA2** เป็น Wireless Security ที่ใช้ในปัจจุบันและยังมีความปลอดภัยอยู่
    - ความยาว Key 256 bits

Wireless Networking

Wireless Security

- **MAC Filtering** เป็นอีกวิธีที่ช่วยป้องกัน Wireless Network โดย AP จะอนุญาตให้เฉพาะเครื่องที่มี MAC Addresses ตาม List ที่ตั้งไว้เข้าถึง Network ได้เท่านั้น
    - เช่น ป้องกันไม่ให้พนักงานนำคอมพิวเตอร์ส่วนตัวมาเชื่อมต่อ Wireless Network

Wireless Networking

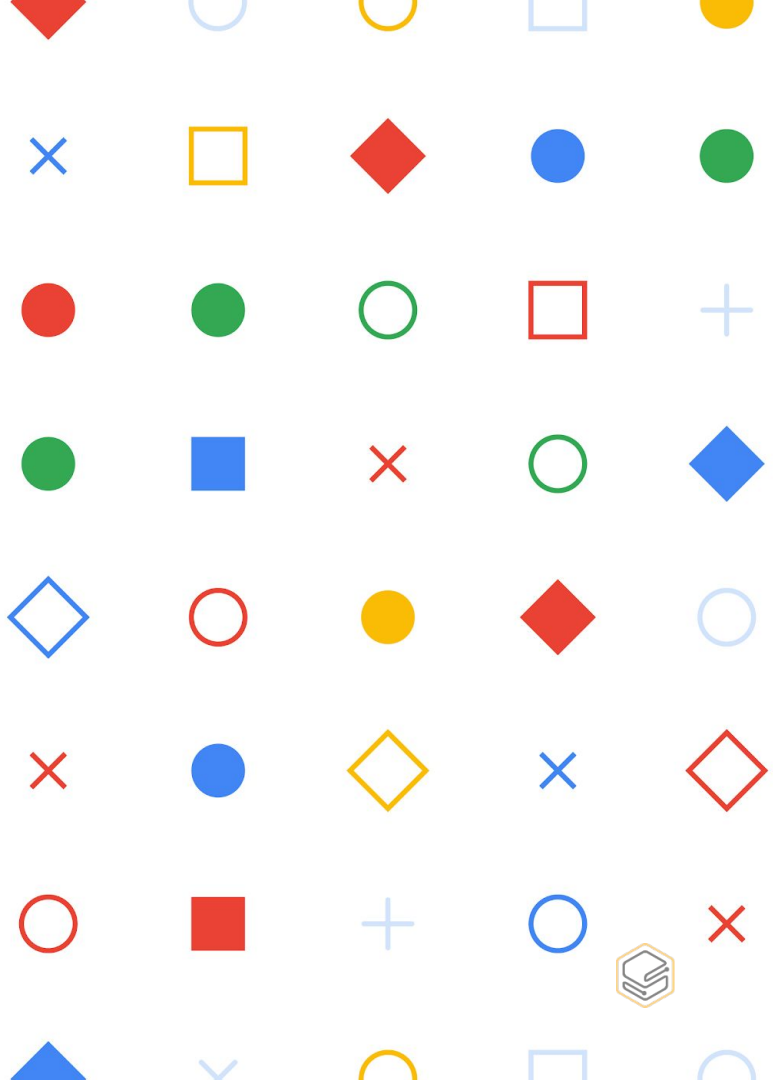


Cellular/Mobile Networking คือ Network ของมือถือ

- ต่างจาก WLAN ตรงที่ใช้ Frequency Band ต่างกันและระยะทางที่ใช้งานจะไกลกว่ามาก อาจจะเป็นหลายกิโลเมตรก็ได้
- Cellular Tower ทำหน้าที่คล้าย AP แต่มีครอบคลุมระยะทางที่ไกลกว่า โดยแต่ละ Cell จะใช้ Frequency Band ที่ไม่ Overlapped กัน

Week 6

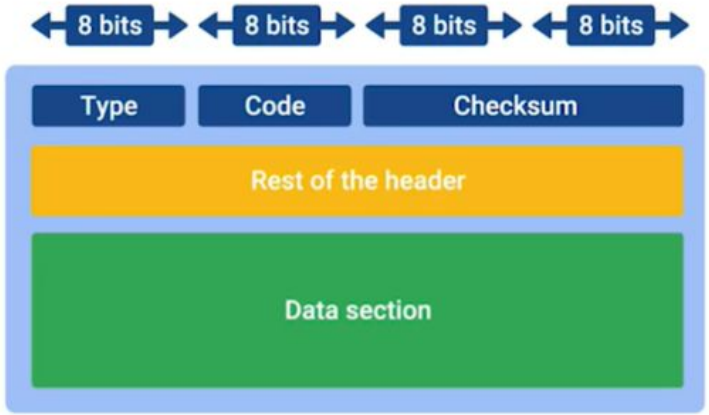
Troubleshooting and the Future of Networking



Samart Skills
A Grow with Google PROGRAM

Skooldio

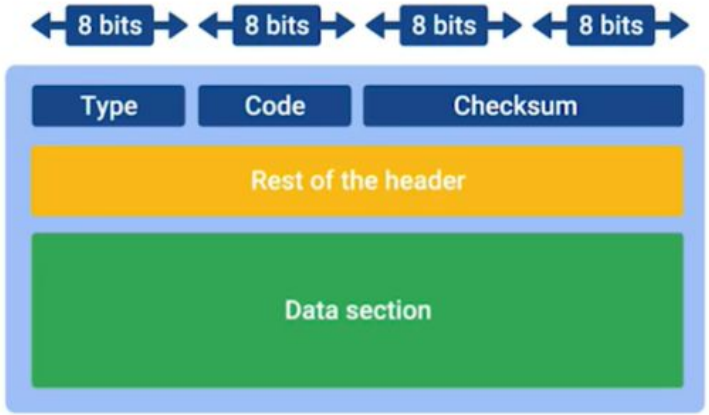
Verifying Connectivity



ICMP (Internet Control Message Protocol) เป็น Protocol ที่มักถูกใช้โดย Router หรือ Remote Host เพื่อที่จะตรวจสอบว่าทำไมการส่งข้อมูลถึงล้มเหลว

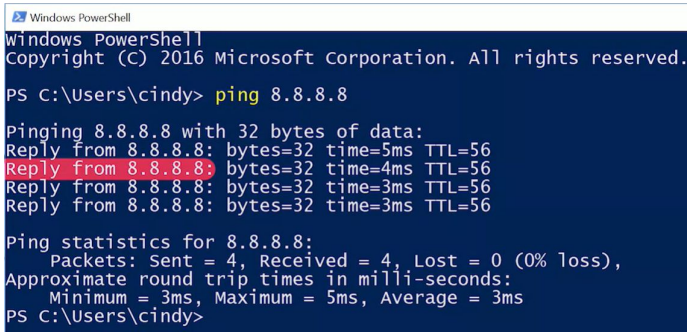
- ICMP อยู่บน Network Layer ประกอบด้วยข้อมูลต่าง ๆ ดังนี้
  - **Type:** มีความยาว 8 bits ใช้ในการบอกประเภทของข้อความที่กำลังถูกส่ง เช่น Destination Unreachable, Time Exceeded
  - **Code:** มีความยาว 8 bits ใช้ในการบอกเหตุผลสำหรับข้อความนั้น เช่น Destination Network Unreachable หรือ Destination Port Unreachable
  - **Checksum:** มีความยาว 16 bits ใช้เก็บค่า Checksum

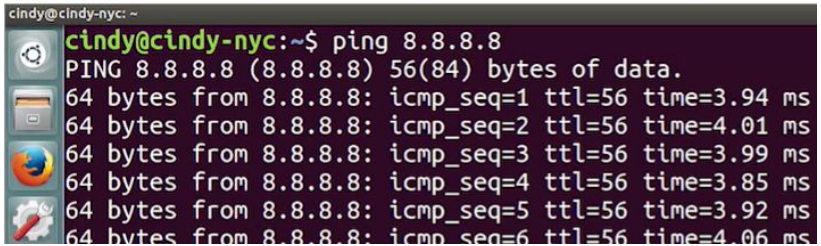
Verifying Connectivity



- **Rest of the Header (Optional):** มีความยาว 32 bits ใช้ในการบอกข้อมูลเพิ่มเติมสำหรับ Type และ Code
- **Data Section (Payload):** เป็นเนื้อหาที่บอกกับผู้รับว่าการส่งไหนที่ทำให้เกิดปัญหา

Verifying Connectivity

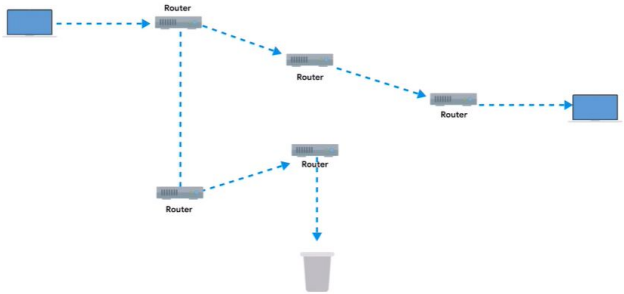


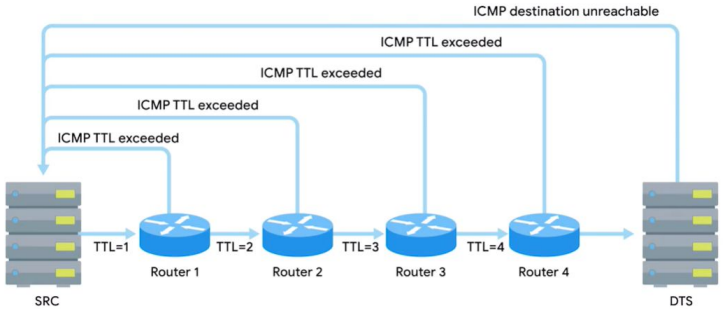


Ping เป็น Software ที่ใช้ในการส่งข้อความ ICMP ประเภทหนึ่ง เรียกว่า Echo Request ซึ่งเป็นการถามไปยังเครื่องปลายทางว่าเปิดอยู่หรือไม่

- ถ้าเครื่องปลายทางเปิดอยู่และสามารถสื่อสารผ่าน Network ได้ เครื่องนั้นจะตอบ ICMP Echo Reply กลับไปหาผู้ส่ง
- **Syntax:** ping [IP/FQDN]

Verifying Connectivity

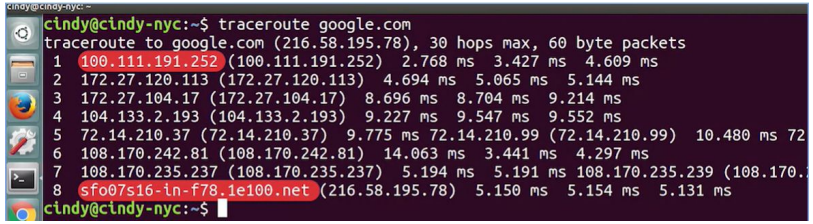


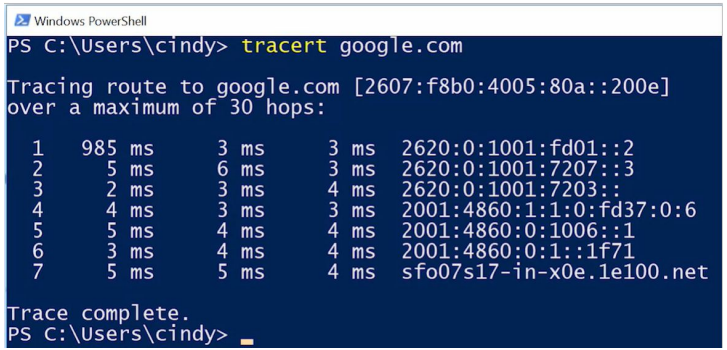


Traceroute เป็น Software ที่ใช้ตรวจสอบเส้นทางระหว่างสองอุปกรณ์ และบอกข้อมูลเกี่ยวกับแต่ละ Hop ตลอดเส้นทางนั้น

- TTL ถูกใช้มาช่วยในการตรวจสอบเส้นทาง
  - เมื่อ TTL มีค่าเป็น “0” Packet จะถูกทิ้งและข้อความ ICMP Time Exceeded จะถูกส่งกลับไปหาเครื่องต้นทาง
  - Traceroute จะ Set TTL เป็น “1” สำหรับ Packet แรก และเพิ่มขึ้นที่ละหนึ่งสำหรับ Packet ถัดไป

Verifying Connectivity





Traceroute

- Linux และ MacOS: Traceroute จะใช้ UDP ส่งไปที่เลข Port สูง ๆ
  - **MTR** เป็นอีกหนึ่ง Software ที่ใช้ในการทำ Traceroute
- Windows: โดยปกติจะใช้ Software ชื่อ “**Tracert**” ซึ่งจะใช้ ICMP Echo Request ในการทำ Traceroute
  - **Pathping** เป็นอีกหนึ่ง Software ที่ใช้ในการทำ Traceroute

Verifying Connectivity

Test Port Connectivity เป็นการตรวจสอบว่า Port ปลายทางเปิดอยู่หรือไม่

- เป็นการตรวจสอบบน Transport Layer

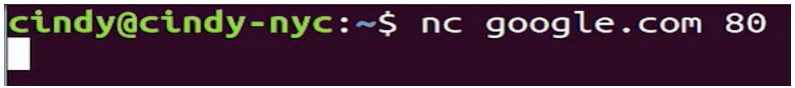
Linux และ MacOS: Netcat

- Syntax: nc [OPTIONS] [IP/FQDN] [PORT]
- OPTIONS:
  - -z : status of a port (สถานะของ port)
  - -v : verbose เป็นการแสดงรายละเอียด

Verifying Connectivity

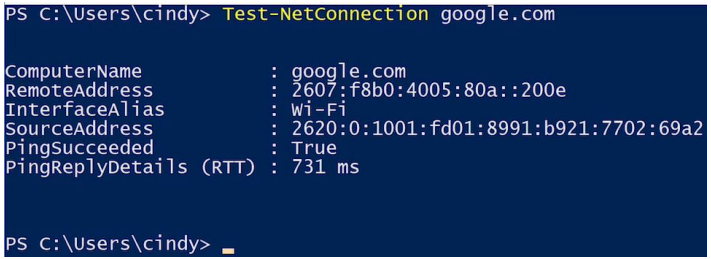
Linux และ MacOS: Netcat

- ตัวอย่าง: การใช้ Netcat ทดสอบว่า Port 80 บนเครื่อง google.com เปิดอยู่หรือไม่
  - ถ้าไม่เปิด Netcat จะปิดตัวเองออก
  - ถ้าเปิด จะมี Cursor รอให้เราใส่ข้อมูลเพิ่มเติมต่อได้



- ตัวอย่าง: การใช้ Netcat โดยบอกสถานะของ Port และแสดงรายละเอียด

Verifying Connectivity



Windows: Test-NetConnection

- Syntax: Test-NetConnection [IP/FQDN] -Port [PORT]
  - ถ้าไม่ระบุ PORT จะใช้ ICMP Echo Request ในการทดสอบคล้ายกับ Ping
- ตัวอย่าง: การใช้ Test-NetConnection ทดสอบเครื่อง google.com โดยไม่ระบุ Port

Verifying Connectivity

```
PS C:\Users\thana> Test-NetConnection google.com -Port 80


ComputerName     : google.com
RemoteAddress    : 142.250.199.14
RemotePort       : 80
InterfaceAlias   : Ethernet
SourceAddress    : 192.168.1.107
TcpTestSucceeded : True
```

```
PS C:\Users\thana> Test-NetConnection google.com -Port 81
WARNING: TCP connect to (172.217.26.78 : 81) failed


ComputerName            : google.com
RemoteAddress           : 172.217.26.78
RemotePort              : 81
InterfaceAlias          : Ethernet
SourceAddress           : 192.168.1.107
PingSucceeded           : True
PingReplyDetails (RTT) : 26 ms
TcpTestSucceeded        : False
```

Windows: Test-NetConnection

- ตัวอย่าง: การใช้ Test-NetConnection ทดสอบว่า Port 80 บนเครื่อง google.com เปิดอยู่หรือไม่

Digging into DNS

```
cindy@cindy-nyc:~$ nslookup twitter.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   twitter.com
Address: 104.244.42.193
Name:   twitter.com
Address: 104.244.42.65
```

nslookup เป็น Software ที่ใช้ในการถาม DNS Server เพื่อให้ช่วยตอบ Name-IP Address

- Syntax: nslookup [FQDN]
- ตัวอย่าง: nslookup เพื่อถาม IP Address ของ twitter.com

Digging into DNS

```
cindy@cindy-nyc:~$ nslookup
>
```

nslookup

- หากไม่ใส่ FQDN จะเป็นการเปิด Interactive Mode

```
cindy@cindy-nyc:~$ nslookup
> coursera.org
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   coursera.org
Address: 54.192.146.230
Name:   coursera.org
Address: 54.192.146.18
Name:   coursera.org
Address: 54.192.146.32
Name:   coursera.org
Address: 54.192.146.150
Name:   coursera.org
Address: 54.192.146.234
Name:   coursera.org
Address: 54.192.146.188
Name:   coursera.org
Address: 54.192.146.67
Name:   coursera.org
Address: 54.192.146.4
```

```
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
>
```

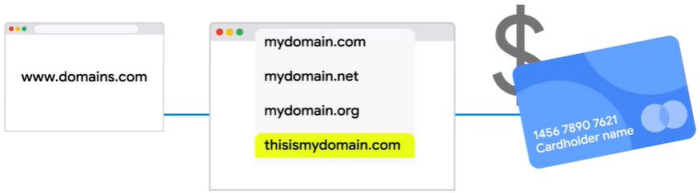
```
> set type=MX
> google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.

Authoritative answers can be found from:
>
```

Digging into DNS

Public DNS Servers เป็น DNS Server ที่เปิดให้ใครก็ได้มาเรียกใช้บริการโดยไม่เสียค่าใช้จ่าย

- สามารถใช้ในการ Troubleshoot ในกรณีที่ DNS Server ขององค์กรเกิดปัญหา
- Google Public DNS IP Address: 8.8.8.8 และ 8.8.4.4
- Public DNS ส่วนใหญ่จะใช้เทคนิค Anycast

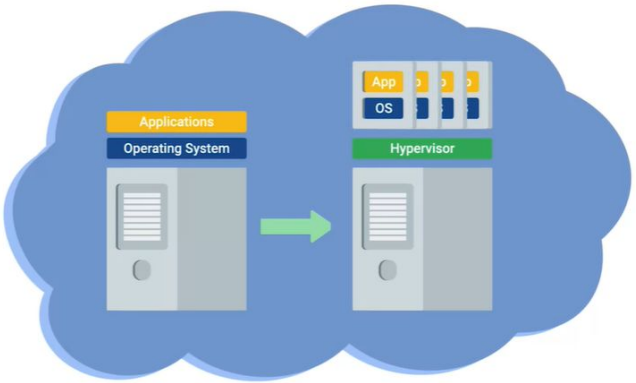
Digging into DNS



Domain Registrar เป็นหน่วยงานที่ทำหน้าที่ในการจัดสรร Domain Name ให้กับองค์กรและบุคคล เช่น Network Solutions Inc., GoDaddy

- Domain Name ต้องไม่ซ้ำกัน
- เราสามารถโอน Domain Name ที่ลงทะเบียนกับ Registrar เจ้าหนึ่งไว้แล้ว ไปให้ Registrar อีกเจ้าหนึ่งได้ แต่จะต้องพิสูจน์ความเป็นเจ้าของ Domain Name นั้นก่อน โดยการใช้ TXT Record
- Domain Name ที่ลงทะเบียนไว้จะมีอายุการใช้งาน หากหมดอายุแล้ว คนอื่น ๆ จะสามารถลงทะเบียน Domain Name นั้นได้

The Cloud



Cloud Computing คือ เทคนิคที่ทำให้ Resources คอมพิวเตอร์สามารถแชร์กันได้ และให้ผู้ใช้งานจำนวนมากใช้งาน Resources ตามที่ต้องการได้

- เทคโนโลยีที่สำคัญที่อยู่เบื้องหลัง Cloud Computing คือ Hardware Virtualization

Virtualization คือ การทำให้เครื่องคอมพิวเตอร์หนึ่งเครื่อง (Host) สามารถมีเครื่องเสมือนได้หลาย ๆ เครื่อง (Guest)

- Hypervisor คือ Software ที่ใช้ในการรันและจัดการเครื่องเสมือน (Virtual Machine) โดยทำตัวเป็นผู้จัดการในการติดต่อ Hardware จริง

The Cloud

Public Cloud คือ Cloud ที่ให้บริการโดยบริษัทอื่น

Private Cloud คือ Cloud ที่ใช้กันภายในองค์กรเท่านั้น

- โดยปกติบริษัทจะเป็นเจ้าของ Hardware และถูกติดตั้งอยู่ในสถานที่ของบริษัท

Hybrid Cloud คือ Cloud ที่ใช้ทั้ง Public Cloud และ Private Cloud ผสมกัน

- อาจจะใช้ Private Cloud สำหรับข้อมูลที่เป็นความลับขององค์กร และใช้ Public Cloud สำหรับข้อมูลที่เปิดเผยได้

The Cloud

Cloud Services

- **Infrastructure as a Service (IaaS):** ให้บริการเครื่อง Servers และ Network เช่น Amazon EC2, Linode, Microsoft Azure, Google Compute Engine
    - ผู้ใช้บริการเป็นผู้รับผิดชอบ OS, Applications และข้อมูล

The Cloud

Cloud Services

- **Platform as a Service (PaaS):** ให้บริการ Platform ในการพัฒนางานต่าง ๆ เช่น Web, Application
  - Heroku, Microsoft Azure, Google App Engine
  - ผู้ใช้บริการเป็นผู้รับผิดชอบ Applications และข้อมูล

The Cloud

Cloud Services

- **Software as a Service (SaaS):** ให้บริการ Software เช่น Microsoft Office 365, Google G Suite
  - ผู้ใช้บริการเป็นผู้รับผิดชอบข้อมูล

The Cloud

Cloud Storage คือ Cloud ที่ให้บริการพื้นที่จัดเก็บข้อมูล ซึ่งจะทำให้ข้อมูลของเรามีความปลอดภัย (Security) เข้าถึงได้ง่าย (Accessibility) และพร้อมใช้งานอยู่เสมอ (Availability)

- สามารถใช้ในการ Backup ข้อมูลได้ทั้งสำหรับคอมพิวเตอร์และ Smartphone

IPv6

IPv4 (32 bits) รองรับได้ทั้งหมด 4.2 พันล้าน IPs ซึ่งไม่เพียงพอแล้วในปัจจุบัน

IPv6 มีความยาว 128 bits รองรับได้ทั้งหมดเท่ากับตัวเลข 39 หลัก

340,282,366,920,938,463,463,374,607,431,768,211,456

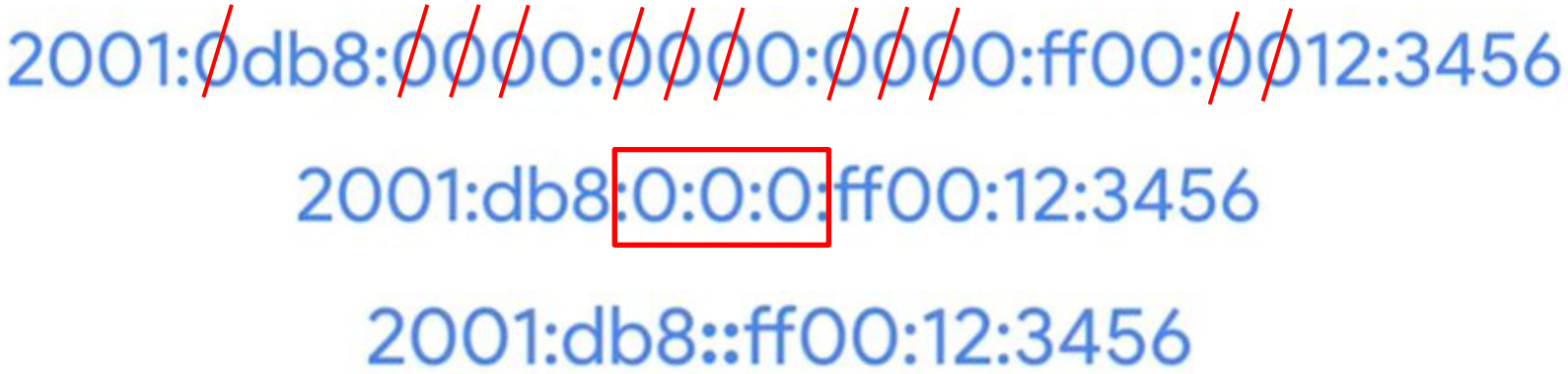
IPv6 ประกอบด้วยเลข Hex 4 หลัก จำนวน 8 ชุด

2001:0db8:0000:0000:0000:ff00:0012:345

IPv6

มีกฎ 2 ข้อที่ทำให้เรายน่ความยาว IPv6 ให้สั้นลงได้

- สามารถลบเลข 0 ที่นำอยู่ข้างหน้า (Leading Zeros) ในแต่ละชุดได้ เช่น 0001 □ 1
- ชุดของ 0 ที่อยู่ติดกัน สามารถใช้ “:” สองตัวแทนได้ เช่น :0:0:0: □ ::
    - แต่สามารถทำได้ครั้งเดียวเท่านั้นสำหรับหนึ่ง IPv6



IPv6

Reserved IPs ของ IPv6

- **Loopback Address**

0000:0000:0000:0000:0000:0000:0000:0001

::1

- **Multicast IP** เริ่มต้นด้วย FF00::
- **Education Purposes** เริ่มต้นด้วย 2001:0db8
- **Link-local Unicast Address** เริ่มต้นด้วย FE80::
    - Link-local Unicast Address ใช้สำหรับอุปกรณ์ที่ใช้ IPv6 ในการรับ Network Settings ต่าง ๆ คล้ายกับ DHCP แต่จะใช้วิธีนำ MAC Address 48 bits ของเครื่องนั้นมาคำนวณเพื่อให้ได้ Unique Address 64 bits แล้วนำไปใส่ในส่วนของ Host ID

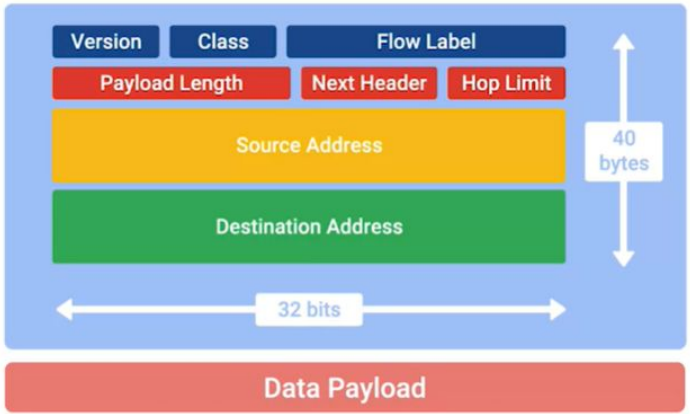
IPv6

Network ID และ Host ID

- หนึ่ง IPv6 Network รองรับ Host ได้ถึง 2^{64}

- ไม่จำเป็นต้องทำ Subnetting
- แต่บางครั้งเพื่อให้ง่ายในการบริหารจัดการ Network เราสามารถทำ Subnetting ได้โดยใช้ CIDR Notation เหมือนกับที่ทำกับ IPv4

IPv6



IPv6 header ประกอบไปด้วยข้อมูลต่าง ๆ ดังนี้

- **Version:** ความยาว 4 bits ใช้ในการบอก IP Version
- **Traffic Class:** ความยาว 8 bits ใช้ในการบอกประเภท ของ Traffic ที่อยู่ใน IP Datagram
- **Flow Label:** ความยาว 20 bits ใช่ร่วมกับ Traffic Class สำหรับ Router ในการตัดสินใจเกี่ยวกับ QoS ของ Datagram นั้น
- **Payload Length:** ความยาว 16 bits ใช้ในการบอกความยาวของ Payload
- **Next Header:** ความยาว 8 bits ใช้ในการบอกประเภทของ Header ของ Datagram อันถัดไป
- **Hop Limit:** ความยาว 8 bits ทำหน้าที่เหมือน TTL บน IPv4
- **Source and Destination Address:** ความยาว 128 bits

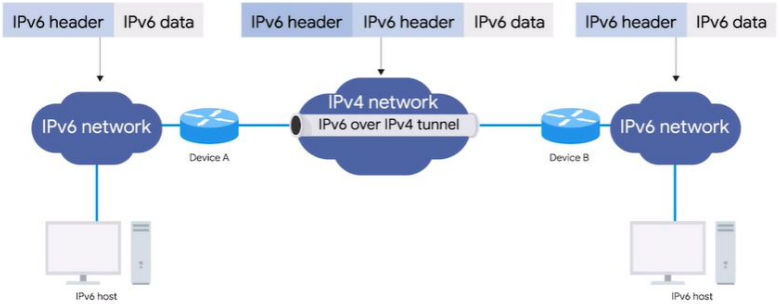
IPv6

IPv4 Mapped Address Space คือ เทคนิคที่ทำให้ IPv4 สามารถใช้ใน Network ที่ใช้ IPv6 ได้

- IPv6 ที่ขึ้นต้นด้วย “0” จำนวน 80 ตัวแล้วตามด้วย “1” จำนวน 16 ตัว เลข 32 bits หลังจากนั้นก็คือ IPv4

192.168.1.1 = 0:0:0:0:0:ffff:d1ad:35a7

IPv6



IPv6 Tunnel คือ เทคนิคที่ทำให้ IPv6 สามารถใช้ใน Network ที่ใช้ IPv4 ได้

- ต้องมี IPv6 Tunnel Server ติดตั้งทั้งสองฝั่งของการเชื่อมต่อ
- Server ฝั่งส่งจะนำ IPv6 Traffic มา Encapsulate ลงใน IPv4 Datagram และส่งผ่าน IPv4 Network ส่วน Server ฝั่งรับจะ Decapsulate จาก IPv4 กลับมาเป็น IPv6 Traffic
- **IPv6 Tunnel Broker** คือ บริษัทที่รับทำหน้าที่ IPv6 Tunneling ให้กับองค์กร เพื่อที่องค์กรจะได้ไม่ต้องซื้ออุปกรณ์เพิ่มเติมสำหรับเรื่องนี้