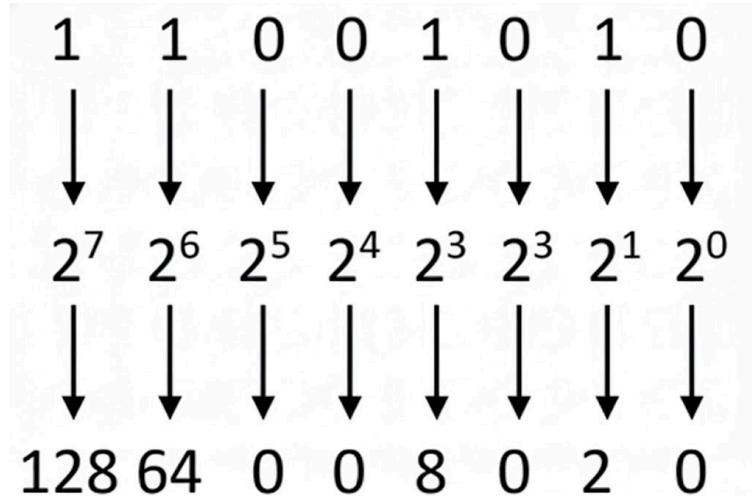


บทที่ 2 IP (Internet Protocol) & Device

2.1 Binary Number

Binary numeral system หรือ ระบบเลขฐานสอง เป็นระบบเลขพื้นฐานทางระบบคอมพิวเตอร์ที่ใช้ตัวเลขเที่ยงสองค่า คือ 0 และ 1 ซึ่งเป็นพื้นฐานสำคัญของระบบคอมพิวเตอร์และระบบเครือข่าย เนื่องจากอุปกรณ์อิเล็กทรอนิกส์สามารถแยกแยะได้เพียงแค่สองสถานะ คือ มีหรือไม่มีสัญญาณไฟฟ้า ระบบเลขฐานสองเลียนสำเนาใช้แทนสถานะตั้งกล่าวได้อย่างเหมาะสม

ในความเป็นจริง ระบบบัญชีในทุกส่วนของคอมพิวเตอร์ ไม่ว่าจะเป็นหน่วยประมวลผลกลาง (Central Processing Unit: CPU), หน่วยความจำ (Memory), ระบบจัดเก็บข้อมูล (Storage Device) รวมถึงอุปกรณ์เครือข่าย เช่น Switch และ Router ข้อมูลทุกชนิดที่ถูกประมวลผลหรือส่งผ่านเครือข่ายเป็นเลขฐานสองทั้งหมด

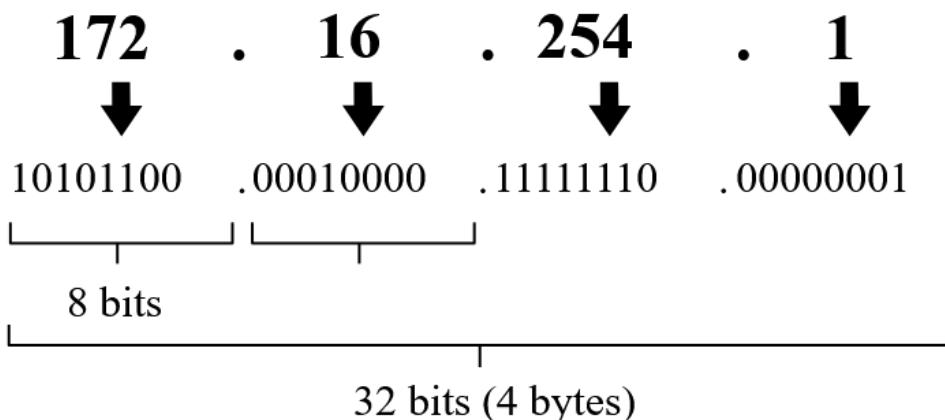


รูปภาพที่ 7 แสดงตัวอย่างของเลข Binary

2.1.1 เลขบิต (bit) และหน่วยข้อมูลในระบบเครือข่าย

ในระบบเลขฐานสอง ตัวเลขแต่ละหลักจะถูกเรียกว่า “บิต (Bit)” เป็นหน่วยข้อมูลที่เล็กที่สุด โดยบิตหนึ่งตำแหน่งสามารถมีค่าได้เพียงแค่ 0 และ 1 เท่านั้น ถ้านำบิตหลาย ๆ ตัวมาเรียงต่อ ๆ กัน จะสามารถนำมาแทนข้อมูลที่ซับซ้อนมากขึ้นได้

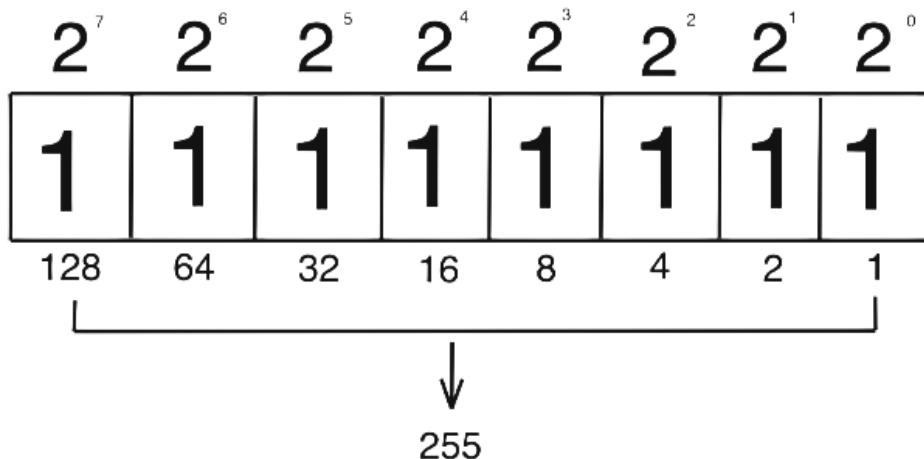
ในระบบเครือข่ายคอมพิวเตอร์ มักใช้กลุ่มของเลขบิตจำนวน 8 บิตร่วมกันจะรวมกันหรือจะเรียกได้ว่าเป็นจำนวน “หนึ่งไบต์ (Byte)” ซึ่งเรียกว่า “อ็อกเตต (Octet)” โดยในหนึ่งอ็อกเตตสามารถแทนค่าตัวเลขในช่วง 0 ถึง 255 ในระบบเลขฐานสิบ เช่น การกำหนดเลขแบบ IPv4 จะใช้จำนวนทั้งหมด 32 บิต จำนวน 4 ไบต์ หรือ 4 อ็อกเตต เป็นต้น



รูปภาพที่ $n + 1$ แสดงตัวอย่างเลข IPv4

2.1.2 ค่าน้ำหนักของบิต (Bit Weight)

บิตแต่ละตำแหน่งในระบบเลขฐานสองมีค่าน้ำหนักที่แตกต่างกัน โดยค่าของบิตจะเพิ่มขึ้นตามเลขยกกำลังของเลขสองจากขวาไปซ้ายโดยเริ่มจากตำแหน่งที่ 0 ฝั่งขวาไปจนถึงตำแหน่งที่ 7 ฝั่งซ้าย สำหรับเลขอ็อกเตตหนึ่งชุดที่มี 8 บิต ค่าน้ำหนักสามารถแสดงได้ ดังนี้



รูปภาพที่ $n + 2$ แสดงเลขอ็อกเตตจำนวนหนึ่งชุด

เมื่อตำแหน่งบิตใดมีค่าเป็น 1 จะหมายถึงค่าน้ำหนักนั้นจะถูกนำมาคำนวณค่าของเลขฐานสิบ แต่หากบิตตำแหน่งใดค่าเป็น 0 จะไม่ถูกนับรวมมาคำนวณด้วย

2.1.3 การแปลงเลขฐานสิบเป็นเลขฐานสอง

การแปลงเลขฐานสิบเป็นเลขฐานสองสามารถทำได้โดยการพิจารณาว่าค่าของเลขฐานสิบนั้นสามารถคำนวณได้จากค่าน้ำหนักของเลขบิตตำแหน่งได้บ้างในเลขฐานสอง

ตัวอย่างเช่น เลขฐานสิบ 192 สามารถแยกได้เป็น $128 + 64$ จากตำแหน่งที่ 7 และ 6 จำกัด 6 จำกัด 7 จึงได้เป็น 192 พอดี

ดังนั้น ตำแหน่งเลขฐานสองก็จะเป็น 11000000 เมื่อลองนำมาคิดดูอย่างละเอียด เราสามารถใช้วิธีการหารสั้นกับตัวเลขฐานสิบและนำหารด้วยเลข 2 ตามตัวอย่างก็คือเลข 192 เป็นตัวตั้งนำมาหารกับเลข 2 ที่เป็นตัวหาร ก็จะนำเศษที่ได้จากการหารสั้นแต่ละครั้งนำมาประกอบเศษจำนวนสุดท้ายໄล่ขึ้นมาจนถึงเศษที่ทำการหารสั้นครั้งแรก ก็จะได้เป็นเลขฐานสองจำนวน 8 บิตพอดี ดังรูป

2	192	----- 0
2	96	----- 0
2	48	----- 0
2	24	----- 0
2	12	----- 0
2	6	----- 0
2	3	----- 1
	1	

$$\therefore 192_{10} = 11000000_2$$

รูปภาพที่ ก + 3 แสดงการหารสิ้นเพื่อแปลงเลขฐานสิบเป็นฐานสอง
การแปลงตัวเลขจะมีความสำคัญในการทำความเข้าใจโครงสร้างของหมายเลข IP และ Subnet Mask ในระบบเครือข่าย

2.1.4 การแปลงเลขฐานสองเป็นเลขฐานสิบ

ในทางกลับกัน การแปลงเลขฐานสองเป็นเลขฐานสิบสามารถทำได้โดยการนำค่าหนักของบิตที่มีค่าเป็น 1 มาบวกกัน ตัวอย่างเช่น 11000000 นำบิตค่าที่เป็น 1 อายุที่ตัวแทนงที่ 7 และ 6 และนำเลขทั้งสองตัวนี้บวกกันแล้วจะได้ผลลัพธ์ 2 เป็นฐานและยกกำลังตามตำแหน่งของเลขบิต ที่คือ 2 ยกกำลัง 7 และ 2 ยกกำลัง 6 และแล้วลังจากนั้นก็จะทำการคำนวณหาเลขยกกำลัง ที่จะได้เป็น 128 นำมารวมกับ 64 ที่จะได้เป็น 192 ดังรูป

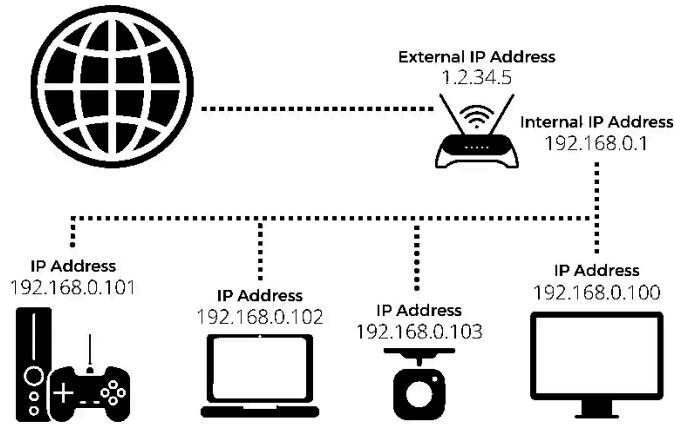
1	1	0	0	0	0	0	0
↓	↓	↓	↓	↓	↓	↓	↓
2^7	2^6	2^5	2^4	3^3	3^3	2^2	2^0
↓	↓	↓	↓	↓	↓	↓	↓
128	64	0	0	0	0	0	0

รูปภาพที่ ก + 4 แสดงการแปลงเลขจากฐานสองเป็นฐานสิบ

ในระบบเครือข่าย การแปลงรูปแบบนี้สามารถช่วยให้สามารถตรวจสอบค่าหมายเลข IP หรือ Subnet Mask ที่แสดงอยู่ในเลขฐานสิบได้อย่างถูกต้อง

2.2 IP Address (Internet Protocol Address)

IP Address หรือ Internet Protocol Address คือ หมายเลขประจำตัวที่ระบุอุปกรณ์แต่ละชิ้นที่เชื่อมต่อกับแต่ละอุปกรณ์ในเครือข่ายคอมพิวเตอร์ หน้าที่หลักคือการระบุตำแหน่งต้นทางและปลายทางของข้อมูล เพื่อให้อุปกรณ์ส่งข้อมูลผ่านเครือข่ายไปยังปลายทางที่ถูกต้องได้ หากไม่มี IP Address ให้กับอุปกรณ์ อุปกรณ์จะไม่สามารถส่งข้อมูลผ่านเครือข่ายได้

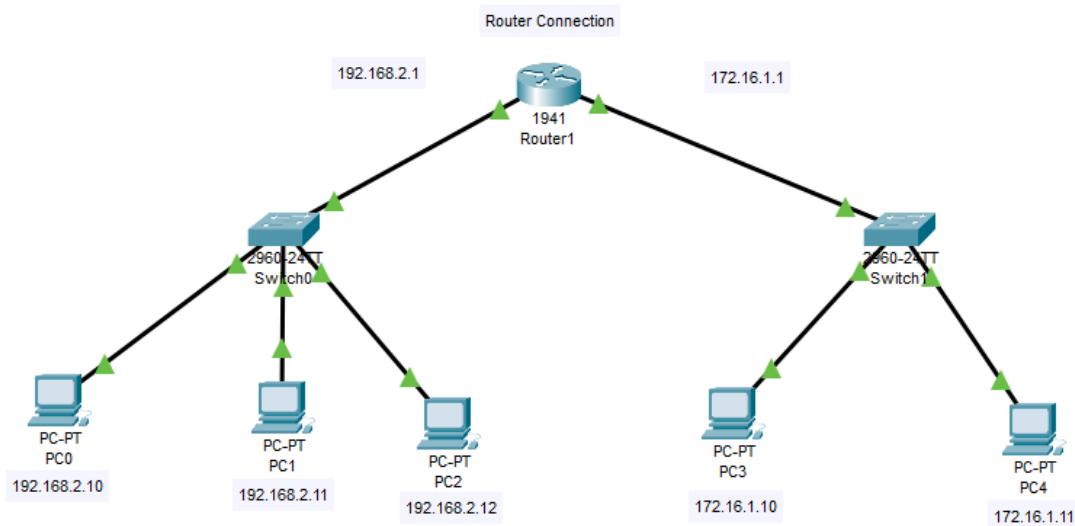


รูปภาพที่ n + 5 แสดง IP Address ต่าง ๆ ของอุปกรณ์ในเครือข่าย

2.2.1 หน้าที่และความสำคัญของ IP Address

IP Address ทำหน้าที่เหมือนกับ “พีซู” ของอุปกรณ์ในระบบเครือข่าย โดยอุปกรณ์เครือข่าย เช่น Router จะใช้ IP Address ในการตัดสินใจเลือกเส้นทางในการส่งข้อมูลไปยังปลายทางที่เหมาะสม การกำหนด IP Address ที่ถูกต้องจะมีความสำคัญอย่างยิ่งกับประสิทธิภาพและความถูกต้องของการสื่อสารในเครือข่าย

ในการปฏิบัติ IP Address จะถูกใช้งานร่วมกับ Subnet Mask เพื่อแยกอุปกรณ์เดียวกัน และอุปกรณ์เดียวกัน



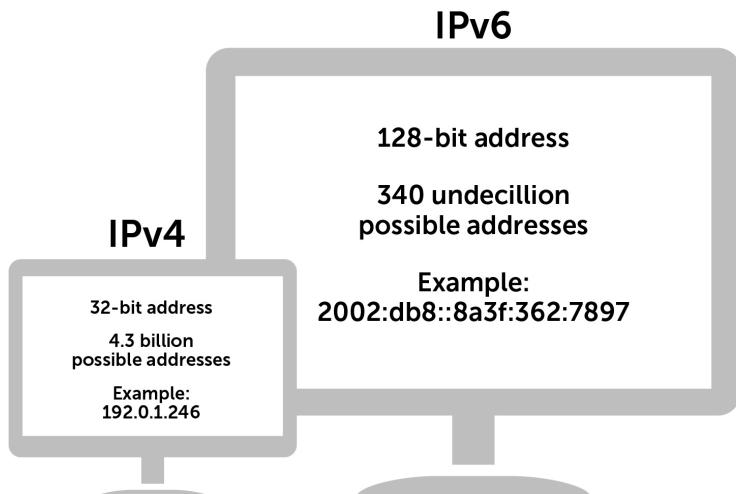
รูปภาพที่ n + 6 แสดงตัวอย่าง Network Topology ที่มีการใช้ IP Address ร่วมด้วย

2.2.2 ประเภทของ IP Address

IP Address สามารถแบ่งออกเป็น 2 ประเภทหลัก ๆ ได้แก่

1. IPv4 (Internet Protocol Version 4)
2. IPv6 (Internet Protocol Version 6)

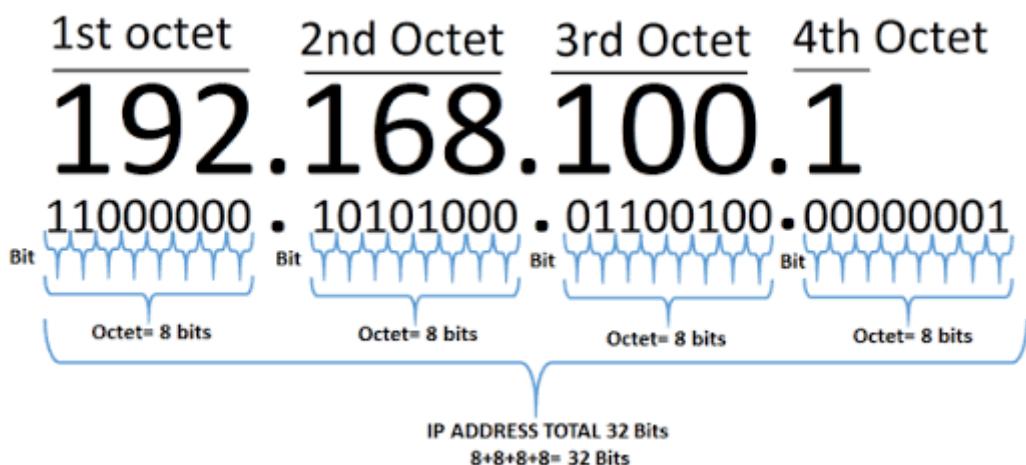
โดย IPv4 และ IPv6 ทั้งสองอย่างมีจุดประสงค์และหน้าที่ตามที่ได้อธิบายไป แต่ว่าทั้งสองตัวนี้จะแตกต่างกันหลัก ๆ ตรงที่จำนวน IP และขนาดที่แตกต่างกัน โดยในปัจจุบัน IPv4 ยังคงถูกใช้งานอย่างแพร่หลาย แต่ว่าด้วยยุคสมัยที่ผ่านไป การใช้งานก็เพิ่มมากยิ่งขึ้น ทำให้ IPv4 ที่มีจำนวน 2 ยกกำลัง 32 ตามจำนวนบิตทั้งหมดใน 4 อ็อกเตต ก็จะเป็นจำนวน 4,294,967,296 ที่ไม่罕กันกำลังจะไม่พอใช้ในปัจจุบัน เลยทำให้ต้องมีการสร้าง IPv6 ขึ้นมาเพื่อแก้ไขการใช้งานที่ไม่เพียงพอของ IPv4 ทั้งในปัจจุบันและอนาคต และแก้หน้าที่อื่น ๆ ที่ IPv4 ยังคงบกพร่องอยู่



รูปภาพที่ n + 7 แสดงความแตกต่างของ IPv4 Address และ IPv6 Address

2.2.3 IPv4 Address

IPv4 เป็นรูปแบบของ IP Address ที่มีความยาวทั้งหมด 32 บิต โดยแบ่งออกเป็น 4 ส่วน แต่ละส่วนจะมีขนาด 8 บิต หรือ 1 อ็อกเตต ซึ่งแสดงอยู่ในค่าของเลขฐาน 10 และถูกคั่นด้วยเครื่องหมายจุด(.) โดยที่อุปกรณ์เครือข่ายจะทำการประมวลผลเลข IP เป็นรูปแบบเลขฐานสองเสมอ แม้ว่าผู้ใช้งานจะเห็นเป็นรูปแบบของเลขฐานสิบก็ตาม



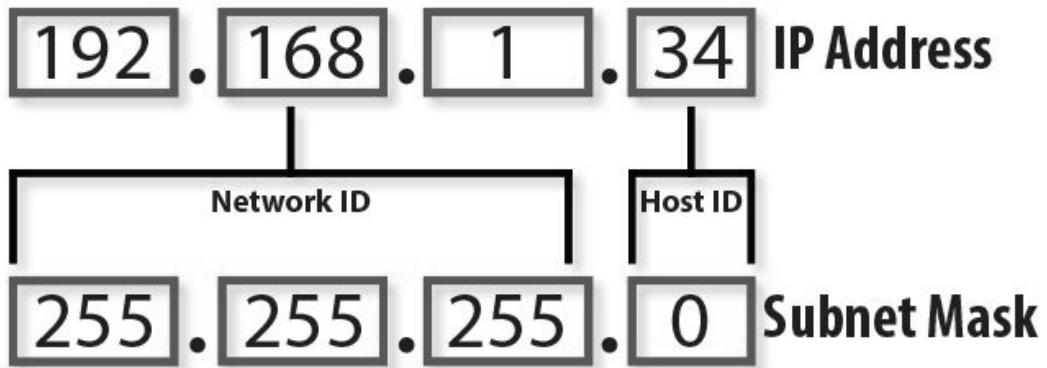
รูปภาพที่ n + 8 แสดงถ้อยคำของ IPv4 Address

2.2.4 โครงสร้าง IPv4 Address

IPv4 Address ประกอบไปด้วย 2 ส่วนหลัก 'ได้แก่'

- Network Address
- Host Address

โดยที่ Network Address ใช้ระบุเครือข่ายที่อุปกรณ์นั้นอยู่ ส่วน Host Address ใช้ระบุหมายเลขของอุปกรณ์ที่อยู่ในเครือข่ายนั้น โดยที่ทั้งสองจะถูกแยกโดยอาศัยค่า Subnet Mask ซึ่งจะกล่าวในบทต่อไป



รูปภาพที่ n + 9 แสดงโครงสร้างของ IPv4 Address

2.2.5 IPv4 Address Classes

IPv4 Address ถูกแบ่งออกเป็นคลาสต่าง ๆ เพื่อกำหนดขนาดของเครือข่าย โดยถูกแบ่งออกเป็น 5 คลาสหลัก มีตัวตั้งแต่คลาส A-E และมีการแบ่งช่วงตาม Public IP และ Private IP ตามรูปภาพ ดังนี้

IPv4 Address Classes and Ranges						
Address Class	Type	Range	Default Subnet Mask	Number of Networks	No of Hosts Per Network	Use
A	Public	1.0.0.0 to 127.0.0.0	255.0.0.0	126	16,777,214	Governments and Large Number of Hosts
	Private	10.0.0.0 to 10.255.255.255				
B	Public	128.0.0.0 to 191.255.255.255	255.255.0.0	16,382	65,534	Medium Companies
	Private	172.16.0.0 to 172.31.255.255				
C	Public	192.0.0.0 to 223.255.255.255	255.255.255.0	2,097,150	254	Small Companies and LANs
	Private	192.168.0.0 to 192.168.255.255				
D	N/A	224.0.0.0 to 239.255.255.255	Not Applicable	N/A	N/A	Reserved for Multicasting
E	N/A	240.0.0.0 to 254.255.255.255	Not Applicable	N/A	N/A	Experimental
Special	Special	127.0.0.1 to 127.255.255.255	N/A	N/A	N/A	Loopback Testing

รูปภาพที่ n + 10 แสดงเกี่ยวกับ IPv4 Classes และการใช้งานเบื้องต้น

1.) Class A

ถูกออกแบบมาเพื่อรองรับเครือข่ายที่มีขนาดใหญ่มาก โดยช่วง Public IPv4 จะเริ่มต้นตั้งแต่ 1.0.0.0 - 127.0.0.0 ในอีกด้านซ้ายจะใช้ระบุ Network Address ส่วนอีก 3 อีกด้านซ้ายจะใช้ระบุ Host Address ทำให้รองรับอุปกรณ์จำนวนมากภายในเครือข่ายนี้

- ค่า Subnet Mask คือ 255.0.0.0
- จำนวน Network ที่เป็นไปได้ คือ 126 เครือข่าย
- จำนวน Host ต่อเครือข่าย คือ 16,777,214 Hosts

Class A เหมาะกับองค์กรขนาดใหญ่ เช่น หน่วยงานระดับประเทศ หรือ ผู้ให้บริการเครือข่ายขนาดใหญ่ อย่างไรก็ตาม การใช้งาน Class A จะทำให้สูญเสียเลข IP จำนวนมาก เนื่องจากเครือข่ายส่วนใหญ่ไม่จำเป็นต้องรองรับโอลิสต์จำนวนมากขนาดนี้

หมายเหตุ: หมายเลข 127.0.0.0 จะถูกสงวนไว้สำหรับ Loopback Address จะไม่ถูกนำมาใช้เป็น IP Address ใน Class A ปกติ

2.) Class B

ถูกออกแบบมาเพื่อรับเครือข่ายขนาดกลาง มีช่วง Public IPv4 ตั้งแต่ 128.0.0.0 - 191.255.255.255 โดย Class B จะใช้สองอ็อกเตตแรกใน
การระบุ Network Address ส่วนอีก 2 อ็อกเตตที่เหลือจะใช้สำหรับ Host Address

- ค่า Subnet Mask คือ 255.255.0.0
- จำนวน Network ที่เป็นไปได้ คือ 16,382 เครือข่าย
- จำนวน Host ต่อเครือข่าย คือ 65,534 Hosts

หมายเหตุ สำหรับองค์กรขนาดกลาง เช่น มหาวิทยาลัย โรงพยาบาล อย่างไรก็ตาม ในหลายกรณี ก็ยังมีจำนวนโอล์ฟ์ที่เกินความจำเป็นอยู่ ทำให้การใช้
IPv4 ยังไม่มีประสิทธิภาพ

3.) Class C

ถูกออกแบบมาเพื่อรับเครือข่ายขนาดเล็ก มีช่วง Public IPv4 ตั้งแต่ 192.0.0.0 - 223.255.255.255 ในสามอ็อกเตตแรกจะใช้ในการระบุ
Network Address และอ็อกเตตสุดท้ายในการระบุ Host Address

- ค่า Subnet Mask คือ 255.255.255.0
- จำนวน Network ที่เป็นไปได้ คือ 2,097,150 เครือข่าย
- จำนวน Host ต่อเครือข่าย คือ 254 Hosts

เป็นคลาสที่ถูกใช้งานมากที่สุดในเครือข่ายแล้ว ๆ เช่น เครือข่ายภายในบ้าน ภายในองค์กรทั่วไป เป็นจากขนาดที่เหมาะสมและจัดการง่าย

4.) Class D

ถูกออกแบบมาเพื่อใช้งานแบบ Multicast โดยมีช่วง IPv4 ตั้งแต่ 224.0.0.0 - 239.255.255.255 โดยที่คลาสนี้ได้ถูกออกแบบมาเพื่อระบุ
Network หรือ Host Address แบบปกติ โดยมีเพื่อส่งข้อมูลจากต้นทางไปปลายทางหลาย ๆ ที่ในเวลาเดียวกัน เช่น การถ่ายทอดสด หรือ group
call เป็นต้น

- ไม่มี Subnet Mask แบบมาตรฐาน
- ไม่สามารถกำหนดให้กับอุปกรณ์ทั่วไปได้

การใช้งาน multicast จะช่วยลดปริมาณ Traffic ในเครือข่าย เนื่องจากส่งข้อมูลไปครั้งเดียวและกระจายไปหาผู้รับได้หลายราย

5.) Class E

ถูกสร้างไว้สำหรับการทำวิจัยหรือการทดลอง โดยมีช่วง IPv4 ตั้งแต่ 240.0.0.0 - 255.255.255.255 โดยคลาสนี้จะไม่ถูกนำมาใช้งานปกติได้
อุปกรณ์ส่วนใหญ่จะไม่รองรับ IPv4 ในช่วงนี้

6.) Special class

IP Address ในช่วงนี้เรียกว่า Loopback Address เพื่อใช้ในการทดสอบการทำงานของระบบเครือข่ายภายในเครื่องเดียวกัน ช่วงหมายเลข IP
ตั้งแต่ 127.0.0.0 ถึง 127.255.255.255 ถูกจัดเป็น Special IP Address ที่ส่วนใหญ่ใช้สำหรับการใช้งานเฉพาะ ไม่ถูกนำมาใช้เป็นหมายเลข IP
สำหรับเครือข่ายหรือโอล์ฟ์ทั่วไป แม้ว่าตามโครงสร้างเดิมจะอยู่ในช่วงของ Class A ก็ตาม โดยไม่เกี่ยวข้องกับอุปกรณ์เครือข่ายภายนอก เช่น
Switch หรือ Router เช่น การตรวจสอบว่า Service ทำงานอยู่หรือไม่

อย่างไรก็ตาม ในสมัยนี้การแบ่ง Class ถูกใช้งานน้อยลง และถูกแทนที่ด้วยการใช้งานแบบ Classless หรือ CIDR เพื่อความยืดหยุ่นที่มากกว่าการ
ใช้แบบ Class

2.2.6 Private/Public IPv4 Address

IPv4 สามารถแยกตามลักษณะการใช้งานได้ 2 ประเภท คือ

1.) Public IP Address

เป็น IP Address ที่ใช้งานบนเครือข่ายอินเทอร์เน็ตโดยตรงที่ได้รับมาจากผู้ให้บริการอินเทอร์เน็ต (ISP) เช่น True, 3BB, AIS โดยที่ต้องมีเลข IP ที่ไม่
ซ้ำกันกับอุปกรณ์อื่น ๆ บนโลกอินเทอร์เน็ต เราจะได้ Public IP มาเลขเดียวจากผู้ให้บริการอินเทอร์เน็ต ทำให้เครื่องที่ออกเน็ตสามารถติดต่อได้
แค่เครื่องเดียว ทำให้เกิด Private IP ขึ้นมา

2.) Private IP Address

เป็น IP ภายในเครือข่ายส่วนบุคคล ไม่สามารถออกอินเทอร์เน็ตได้โดยตรง โดย Private IP ก็จะมีช่วงคลาสเหมือนกับ Public IP โดยจะมีคลาสแบ่งได้เป็น 3 คลาส ดังนี้

1.) Class A

จะมีช่วงตั้งแต่ 10.0.0.0 - 10.255.255.255

2.) Class B

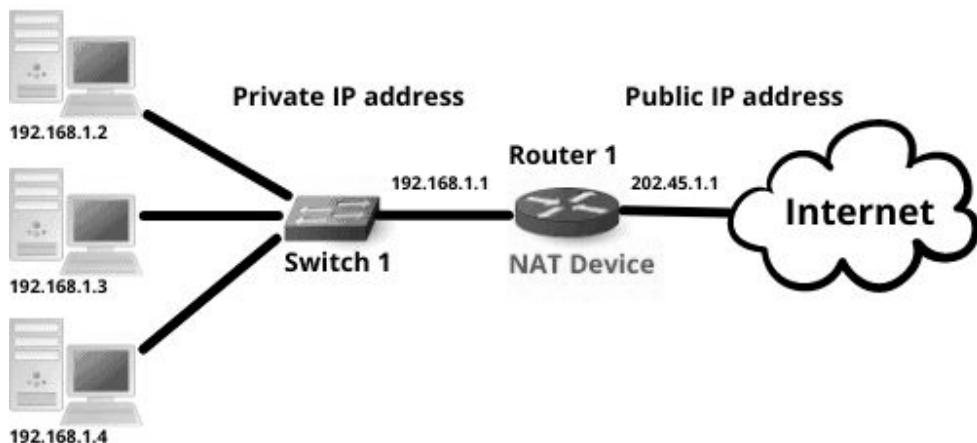
จะมีช่วงตั้งแต่ 172.16.0.0 - 172.31.255.255

3.) Class C

จะมีช่วงตั้งแต่ 192.168.0.0 - 192.168.255.255

โดย Subnet Mask ก็จะมีตามช่วงคลาสเหมือนที่ได้อธิบายไปก่อนหน้านี้ โดยเลข Private IP จะนิยมใช้กับองค์กรและเครือข่ายภายในบ้าน โดยถ้าต้องการที่อยากจะออกอินเทอร์เน็ต จะต้องใช้งานร่วมกับเทคโนโลยีที่เรียกว่า Network Address Translation (NAT) โดยส่งข้อมูลไปที่ Router ส่วนตัวเพื่อแปลงเลข Private IP ของเราเป็นเลข Public IP ที่เราได้รับมาจากผู้ให้บริการอินเทอร์เน็ต (ISP) เพื่อออกอินเทอร์เน็ต

Network Address Translation



รูปภาพที่ n + 11 แสดงเกี่ยวกับการใช้งาน Private/Public IPv4 Address รวมถึงการใช้ NAT

2.2.7 IPv6 Address

IPv6 ถูกพัฒนามาเพื่อแก้ไขปัญหาการขาดแคลนหมายเลข IPv4 โดยที่มีความยาวทั้งหมด 128 บิต และมีการแบ่งทั้งหมด 8 ชุด ชุดละ 16 บิต แต่ละชุดถูกคั่นด้วยเครื่องหมายทวิภาค (:) และถูกแสดงในรูปแบบเลขฐานสิบหก (Hexadecimal)

2001:0DB8:AAAA:1111:0000:0000:0100/64



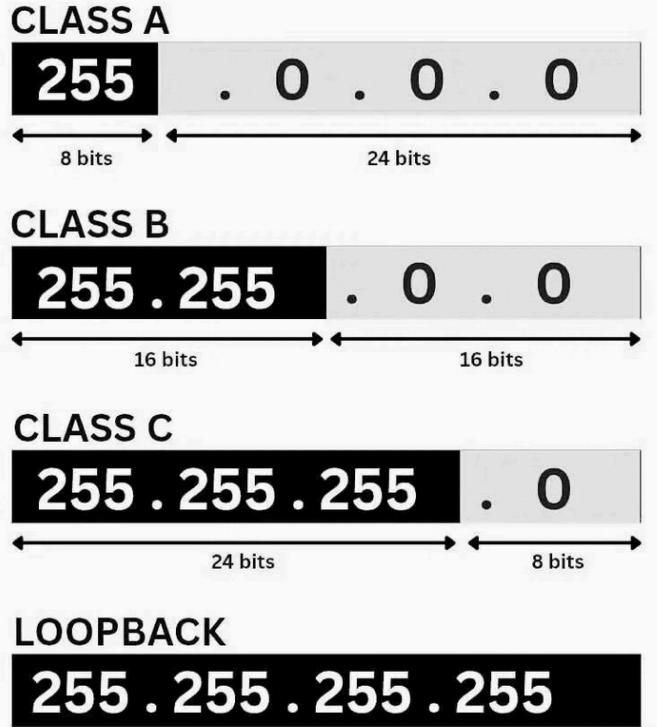
รูปภาพที่ n + 12 แสดงเกี่ยวกับเลข IPv6 Address

IPv6 รองรับ IP ได้มากกว่า IPv4 จำนวนมหาศาล กว่า 2 ยกกำลัง 128 ตามจำนวนบิต หรือ 340 ล้านล้านล้านล้านล้านล้าน (undecillion) ตัวหรือ 3.4×10 ยกกำลัง 38 และถูกออกแบบมาให้มีความปลอดภัยและประสิทธิภาพที่ดียิ่งขึ้น

2.3 Subnet Mask

Subnet Mask เป็นองค์ประกอบสำคัญที่ต้องทำงานร่วมกับ IP Address เพื่อกำหนดขอบเขตของเครือข่าย (Network) และอุปกรณ์ภายใน (Host) ในระบบเครือข่าย แม้ว่าอุปกรณ์จะมี IP Address แต่ก็ตาม หากไม่มี Subnet Mask อุปกรณ์จะไม่สามารถแยกแยะได้ว่าอุปกรณ์ไหนเป็นอุปกรณ์ที่อยู่ในเครือข่ายเดียวกัน และอุปกรณ์ใดจำเป็นต้องส่งข้อมูลผ่าน Router

Subnet Mask จะทำหน้าที่กำหนดค่าส่วนใดของ IP Address เป็น Network Address และส่วนใดเป็น Host Address โดยอาศัยการทำงานของเลขฐานสองและการดำเนินการแบบ AND ที่จะอธิบายหลังจากนี้



รูปภาพที่ n + 13 แสดงเกี่ยวกับ Subnet Mask ของ Private IPv4 Address แต่ละ Class

2.3.1 ความหมายและหน้าที่ของ Subnet Mask

Subnet Mask คือค่าของตัวเลขขนาด 32 บิต แบบเดียวกับ IPv4 Address โดยบิตที่มีค่าเป็น 1 จะถูกใช้แทนส่วนของ Network และส่วนบิตที่มีค่าเป็น 0 จะถูกใช้แทนในส่วนของ Host

ตัวอย่าง Subnet Mask:

Subnet Mask เลขฐาน 10	Subnet Mask เลขฐาน 2
255.255.255.0	11111111.11111111.11111111.00000000

จากตัวอย่างจะเห็นได้ว่า Subnet Mask ที่เป็นเลขฐาน 2 ของ 24 บิตแรกจะเป็น ซึ่งหมายถึงส่วน Network และ 8 บิตสุดท้ายจะเป็น 0 ซึ่งหมายถึงส่วน Host

2.3.2 การดำเนินการ Binary ด้วย AND กับ Subnet Mask

IP Address เพียงอย่างเดียวไม่สามารถบอกได้ว่าเครือข่ายมีขนาดเท่าไหร่ จำเป็นต้องใช้งานร่วมกับ Subnet Mask เพื่อหา Network Address และ Subnet Mask มาทำการคำนวณแบบ **Binary AND** เพื่อหา Network Address

การทำ Binary AND จะช่วยแยกส่วนของ Network Address ออกจาก Host Address โดยบิตที่ตรงกับค่า 1 ใน Subnet Mask จะถูกเก็บไว้เป็นส่วนของเครือข่าย ส่วนบิตที่เป็น 0 จะถูกตัดออก ทำให้ผลลัพธ์เป็น Network Address ของ IP Address นั้น

Network Address ที่ได้นี้จะถูกนำไปใช้ในการส่งข้อมูลไปยังปลายทางสามารถทำได้ภายในเครือข่ายเดียวกัน หรือจำเป็นต้องส่งข้อมูลผ่าน Router ไปยังเครือข่ายอื่น

เมื่ออุปกรณ์ทราบ Network Address ของ IP ปลายทางแล้ว จะนำไปเปรียบเทียบกับ Network Address ของตนเอง หากอยู่ในเครือข่ายเดียวกัน จะสามารถส่งข้อมูลได้โดยตรง แต่หากไม่ตรงกัน ข้อมูลจะถูกส่งไปยัง Default Gateway เพื่อทำการส่งต่อไปยังเครือข่ายอื่น

ตัวอย่าง

IP Address	192.168.1.10
Subnet Mask	255.255.255.0

เมื่อนำมาแปลงเป็นเลขฐานสองและทำการ AND จะได้ผลลัพธ์ดังนี้

	Octet 1	Octet 2	Octet 3	Octet 4
IP Address	11000000	10101000	00000001	00001010
Subnet Mask	11111111	11111111	11111111	00000000
Result	11000000	10101000	00000001	00000000

ผลลัพธ์ที่ได้คือ 192.168.1.0 ที่เป็นเลข Network Address ของ IP Address เลขนี้

อุปกรณ์จะใช้ Network Address นี้เพื่อตรวจสอบว่าอุปกรณ์ปลายทางอยู่ในเครือข่ายเดียวกันหรือไม่ หากอยู่ในเครือข่ายเดียวกัน จะสามารถส่งข้อมูลได้โดยตรง แต่หากอยู่นอกเครือข่าย จะต้องส่งข้อมูลผ่าน Router

2.3.3 CIDR (Classless Inter-Domain Routing)

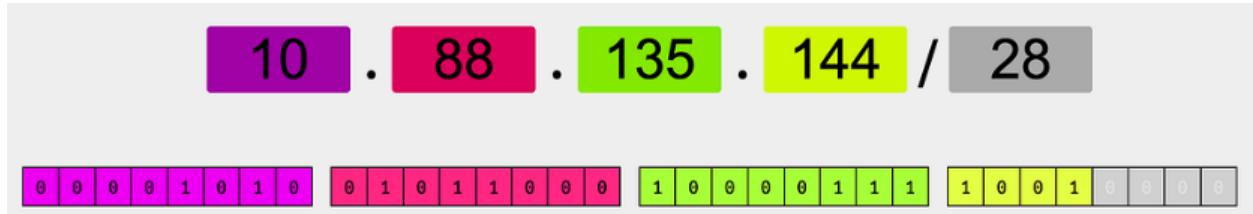
CIDR เป็นแนวคิดการกำหนด IP ที่ไม่จำกัดกับ Class โดยการระบุจำนวนบิตของ Network ด้วยเครื่องหมายทับ (/) ต่อท้าย IP Address

ตัวอย่าง

IP Address	192.168.1.0/24
------------	----------------

หมายความว่า 24 บิตแรกเป็นส่วนของ Network และ 8 บิตหลังเป็นส่วนของ Host

การทำ CIDR สามารถทำให้กำหนดขนาดเครือข่ายได้แบบยืดหยุ่น และลดการสูญเสียหมายเลข IP แบบไม่จำเป็นได้ และสามารถทำให้เข้าใจว่า IP Address น้อยใน Subnet เลขที่เท่าไหร่ จากการสังเกตตัวเลขชั้งหลังที่ต่อท้าย ทำให้เข้าใจมากกว่าการอ่านเลขบิตมากขึ้น



รูปภาพที่ n + 14 แสดงตัวอย่างของเลข IPv4 Address ชุดหนึ่งที่มีการใช้ CIDR ร่วมด้วย

2.3.4 Subnetting

Subnetting คือกระบวนการแบ่งเครือข่ายขนาดใหญ่ออกเป็นเครือข่ายขนาดย่อยหลาย ๆ เครือข่าย โดยการเพิ่มจำนวนบิตของ Subnet Mask ในส่วน Host เพื่อใช้เป็น Subnet

โดยการที่ Subnetting ทำไปเพื่อลดปริมาณการ Broadcast ภายใน Network และเพิ่มความปลอดภัย รวมถึงการบริหารเครือข่ายได้มากขึ้น แล้วใช้เลข IP ได้อย่างมีประสิทธิภาพ

2.3.5 Network Address และ Broadcast Address

ในแต่ละ Subnet จะมีหมายเลข IP ที่ถูกสรุนไว้เป็นพิเศษเพื่อใช้เป็น Network Address และ Broadcast Address โดยที่ Network Address จะเป็นเลขตัวเลขของ Subnet (Host บิตทั้งหมดเป็น 0) และ Boardcasr Address จะเป็นหมายเลขสุดท้ายของ Subnet (Host บิตทั้งหมดเป็น 1)

ตัวอย่าง Subnet

Network Address	192.168.1.0
Broadcast Address	192.168.1.255

หมายเลขอ้างอิงสามารถใช้เป็นเลขไอสต์เต็ม

2.4 Network Device

หลังจากที่ได้ศึกษาโครงสร้างของ IP Address, Subnet Mask และการคำนวณ Network Address ด้วย Binary AND แล้ว ขั้นตอนถัดไปที่สำคัญคือการทำความเข้าใจ อุปกรณ์เครือข่าย (Network Devices) ซึ่งเป็นตัวกลางในการรับ-ส่งข้อมูลระหว่างอุปกรณ์ภายในเครือข่ายและระหว่างเครือข่ายที่ต่างกัน

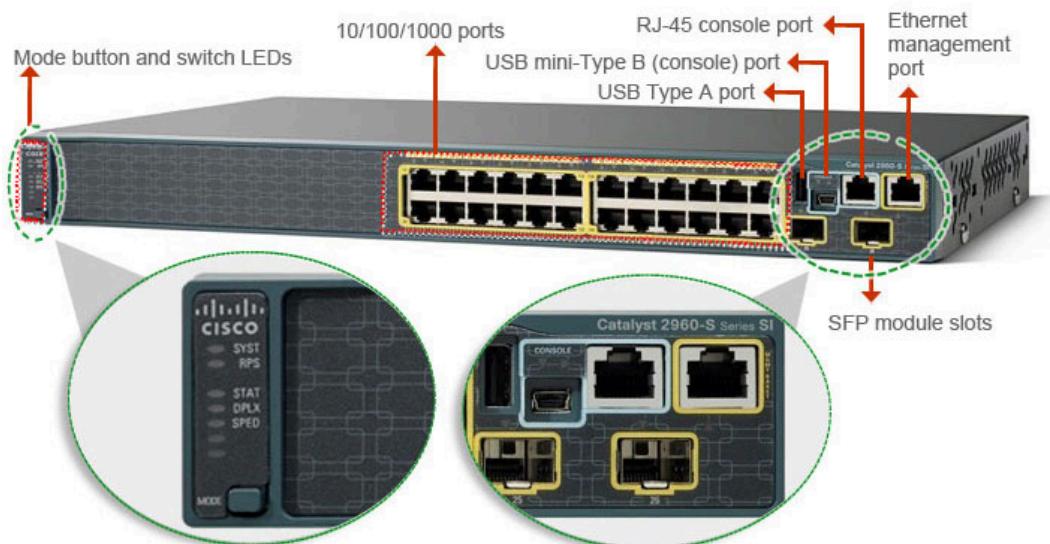
อุปกรณ์เครือข่ายแต่ละประเภทจะทำงานอยู่บน OSI Model คละ Layer และมีหน้าที่แตกต่างกันอย่างชัดเจน โดยในบทนี้จะกล่าวถึงอุปกรณ์หลัก 3 ส่วน ได้แก่

1. Switch
2. Router
3. Network Interface
4. LAN Cable

2.4.1 Switch

Switch คือ อุปกรณ์เครือข่ายที่ใช้เพื่อต่ออุปกรณ์หลายตัวภายใน Local Area Network (LAN) เข้าด้วยกัน โดยมีหน้าที่รับ-ส่งข้อมูลไปยังปลายทางที่ถูกต้องภายในเครือข่ายเดียวกัน

Switch ทำงานหลัก ๆ อยู่ที่ OSI Layer 2 (Data Link Layer)



รูปภาพที่ n + 15 แสดงเกี่ยวกับ Switch ของ Cisco และระบุถึง Ports ต่าง ๆ ของ Switch

หลักการทำงานของ Switch

Switch จะเก็บ MAC Address ของแต่ละอุปกรณ์ ซึ่งจะเป็นตัวในการตัดสินใจส่งข้อมูล โดยภายใน Switch จะมีตารางที่เก็บข้อมูลต่าง ๆ ของ MAC Address เรียกว่า “MAC Address Table” ซึ่งทำการเก็บข้อมูลเฟรม (Frame) ต่าง ๆ ที่ผ่าน Port ต่าง ๆ ในอุปกรณ์ ซึ่งมีรูปแบบการส่งได้หลายวิธี ได้แก่

- Broadcast (ส่งทุก Ports)
- Multicast (ส่งหลาย Ports)
- Unicast (ส่ง 1 Port แบบระบุปลายทาง)

ตัวของ Switch จะทำการเลือกเองว่าเฟรมต้องส่งแบบไหน โดยการส่งข้อมูลระหว่าง Switch เรียกว่า “Switching”

และประเภทของ Switch จะมีการแบ่งออก 2 แบบ

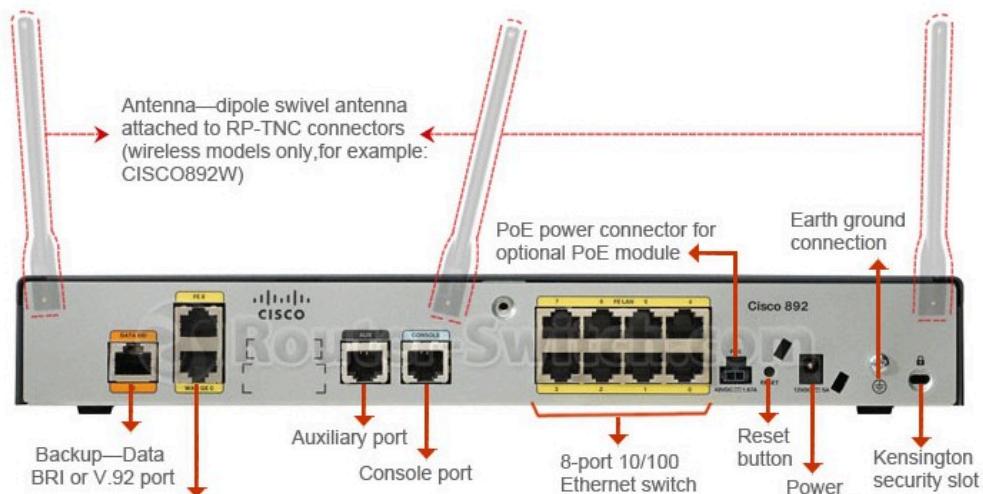
1. Unmanaged Switch - ใช้งานง่าย ไม่มีการตั้งค่า
2. Managed Switch - สามารถตั้งค่า VLAN, Trunk, Port Security ได้

2.4.2 Router

Router คืออุปกรณ์เครือข่ายที่ทำหน้าที่เชื่อมต่อ เครือข่ายตั้งแต่ 2 เครือข่ายขึ้นไป และเป็นตัวตัดสินใจเส้นทางการส่งข้อมูลระหว่างเครือข่าย Router ทำงานหลัก ๆ อยู่ที่ OSI Layer 3 (Network Layer)



รูปภาพที่ n + 16 แสดงเกี่ยวกับ Router ของ Cisco



รูปภาพที่ n + 17 แสดงเกี่ยวกับรายละเอียด Router ของ Cisco รุ่น 800 series

หลักการทำงานของ Router

จะใช้ IP Address ในการส่งข้อมูลและหาเส้นทาง และมีการเป็บข้อมูลไว้ใน Routing Table ไว้ใช้เลือกส่งข้อมูลข้ามเครือข่าย และมีการทำงานขั้นตอน ดังนี้

1. อ่าน Destination IP Address
2. นำ IP Address ไปเปรียบเทียบกับ Routing Table
3. เลือกเส้นทางที่เหมาะสมที่สุด
4. ส่ง Packet ออก Interface ที่กำหนด

Router จะไม่พิจารณา Host Address โดยตรง แต่จะพิจารณา Network Address ด้วย วิธีการหากสอดคล้องตามที่ได้อธิบายไปในหัวข้อก่อนหน้านี้ 2.3.2) ด้วย

2.4.3 Network Interface

Network Interface คือส่วนเข้มต่อระหว่างอุปกรณ์กับเครือข่าย อาจอยู่ในรูปของ

- Network Interface Card (NIC)
- Physical Interface (Ethernet, Fiber)
- Logical Interface (Virtual Interface)

หน้าที่หลัก ๆ ของ Network Interface

- รับ-ส่งข้อมูลเข้าสู่เครือข่าย
- เป็นจุดที่กำหนด IP Address
- เป็นตัวที่แทนอุปกรณ์ใน Network

อุปกรณ์หนึ่งสามารถมีได้มากกว่าหนึ่ง Interface เช่น

- เครื่อง Server ที่มีหลาย Network
- Router ที่มีหลาย Interface

เวลาเชื่อมต่อสาย LAN เข้ากับอุปกรณ์ เราจะต่อเข้ากับ Physical Interface หลัก ๆ อยู่ 2 ชนิด คือ

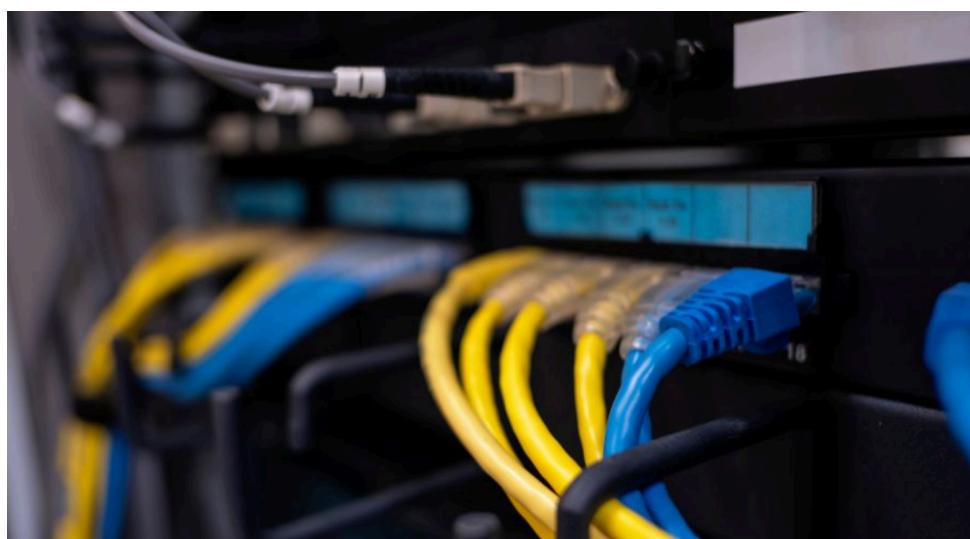
- Fast Ethernet
- Gigabit Ethernet



รูปภาพที่ n + 17 แสดงตัวอย่าง Port ของอุปกรณ์เครือข่าย

2.4.4 LAN Cable

สายแลน (LAN Cable) หรือ UTP (Unshielded Twisted Pair) เป็นสายนำสัญญาณชนิดทองแดงที่นำมาตีเกลียว และหุ้มฉนวน มักใช้ในการต่อคอมพิวเตอร์เข้าด้วยกัน หรือจะเป็นคอมพิวเตอร์กับเครือข่ายอินเทอร์เน็ตที่หลายคนจะคุ้นชื่อกับพอร์ตที่ซื่อว่า RJ45 ที่นิยมใช้กันในปัจจุบัน



รูปภาพที่ n + 17 แสดงสาย LAN