Cs223
ทบทวน LAN Networking

Kasidit Chanchio
Department of Computer Science,
Faculty of Science and Technology,
Thammasat University
1st Semester 2024

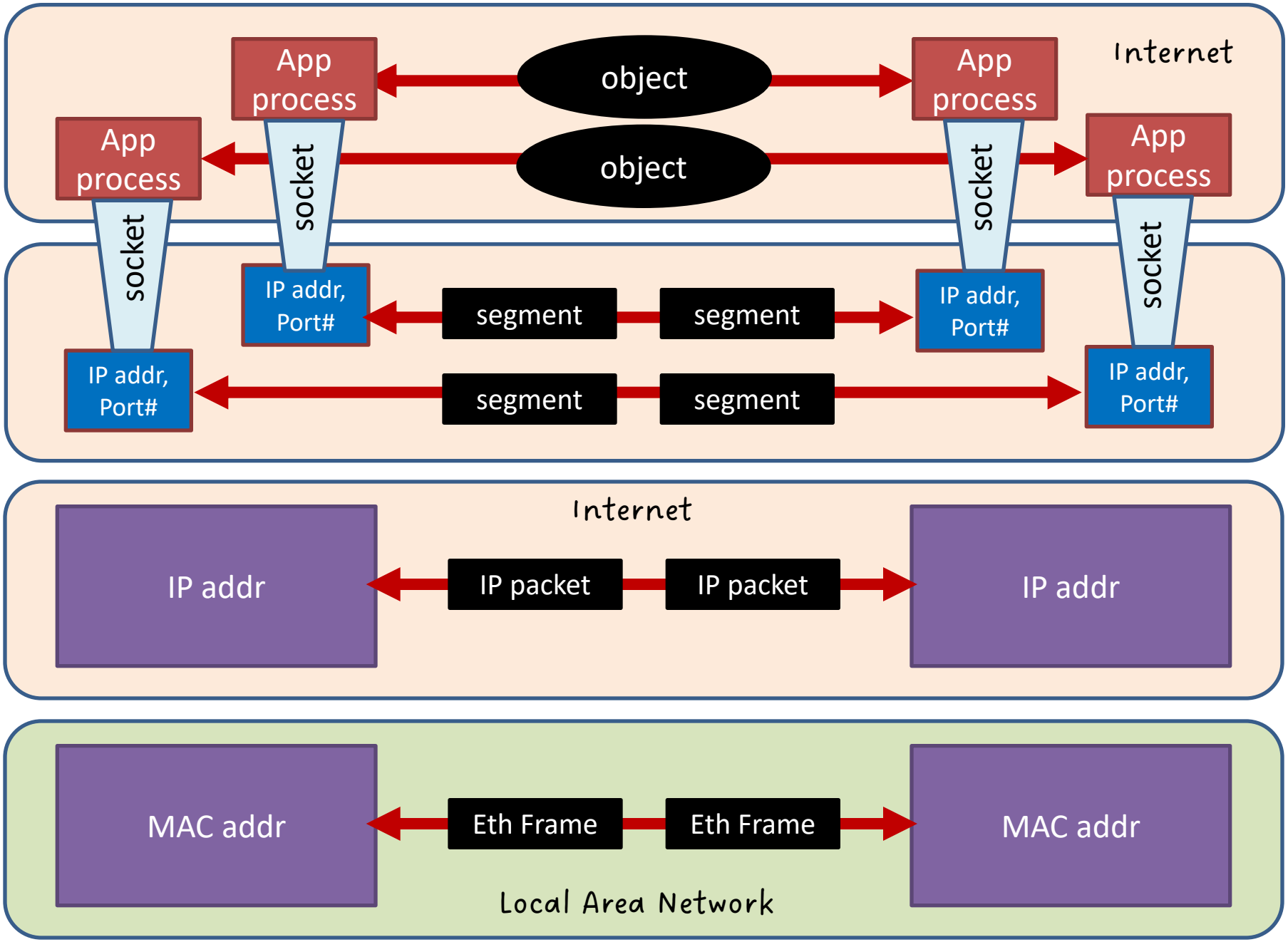
ทบทวน Layer 3 Networking

(IP Layer)

สถาปัตยกรรมแบบเลเยอร์

- การสื่อสารในระบบเครือข่ายประกอบไปด้วย ผู้ส่ง ข้อมูล และผู้รับ
- ใน Internet Protocol Suit มี 5 เลเยอร์ ซึ่งแต่ละอันให้นามธรรมกับตัวตนของทั้งสามส่วนต่างกัน

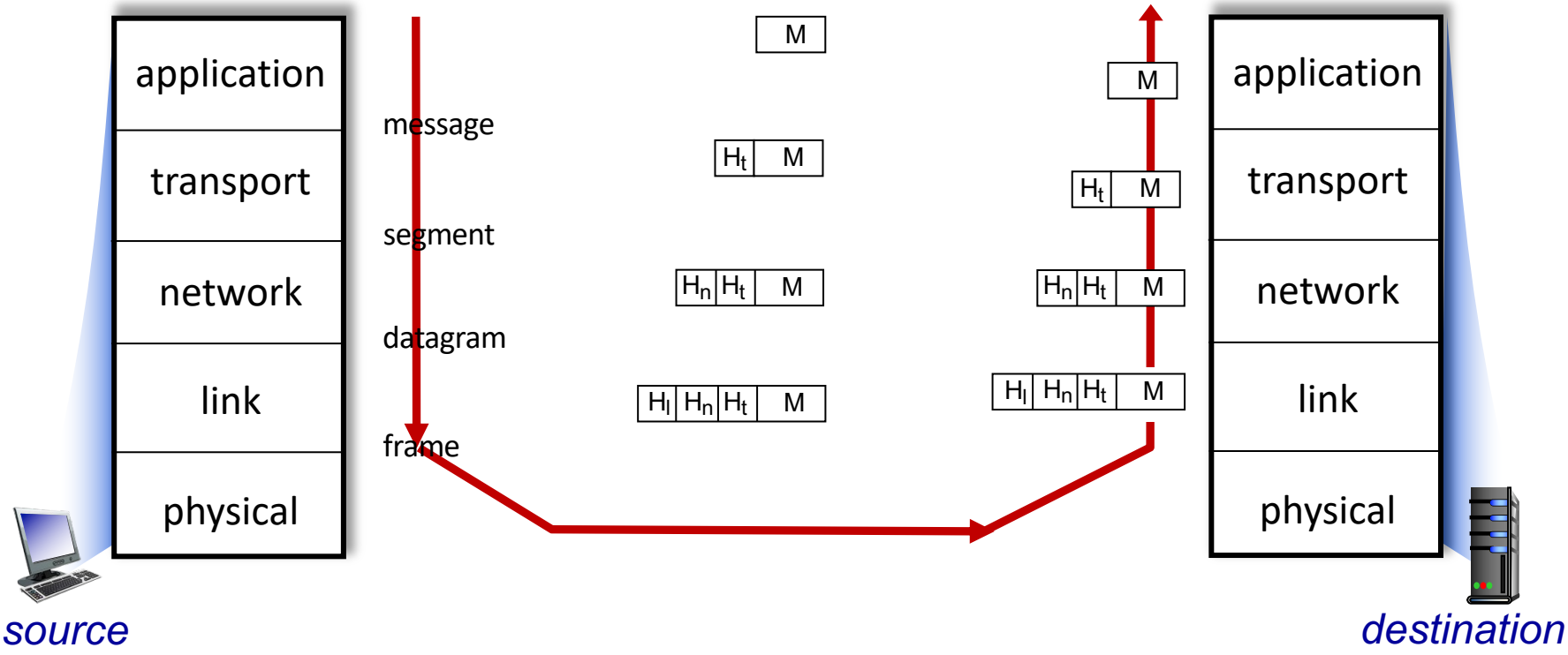
Layer	ผู้ส่ง	ข้อมูล	ผู้รับ
Application	User Process	Objects, Stream	User Process
Transport	Source IP addr, Source Port#	segments	Dest IP addr, Dest Port#
Network	Source IP addr	packet	Dest IP addr
Data Link	Src MAC Addr	Ethernet Frame	Dest Mac Addr
Physical	Source NIC	Cable	Dest NIC


Internet
App process
object
App process
App process
socket
object
socket
App process
socket
socket
IP addr, Port#
segment
segment
IP addr, Port#
IP addr, Port#
segment
segment
IP addr, Port#
Internet
IP addr
IP packet
IP packet
IP addr
MAC addr
Eth Frame
Eth Frame
MAC addr
Local Area Network

ความสัมพันธ์ระหว่างนามธรรมส่วนประกอบ

- Host เครื่องหนึ่งอาจมีหลาย IP ได้: นศ 1 คนมีหลาย Sim มือถือ
- Network Interface Card (NIC) 1 อัน มี IP 1 ค่า: เหมือน Sim มี 1 เบอร์โทร
- NIC 1 อันมี MAC (Media Access Control) address 1 ค่า: เหมือน Sim มี Serial Number ของบริษัทผู้ผลิต
- คู่ (IP addr, Port#) เรียกอีกอย่างว่า end points หรือประตูสู่เน็ต
- App Process หนึ่งอาจมีหลาย end points
- Object หนึ่งอาจถูกแยกเป็นหลาย segments
- 1 segment คือ payload ของ 1 packet
  - Packet ประกอบด้วย header+payload
- 1 packet คือ payload ของ 1 frame
  - Eth Frame ประกอบด้วย Frame header+payload

Services, Layering and Encapsulation



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Rough Message Format

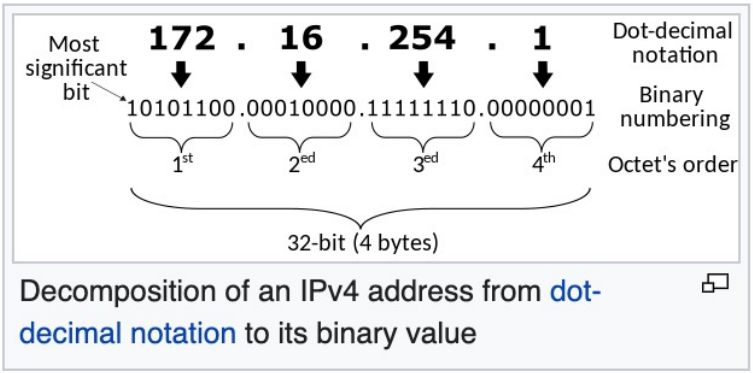
		Hl	Hn	Ht	Payload
Message (Object)	L5				M
Segment	L4			Src Port# Dst Port#	M
Datagram (Packet)	L3		Src IP Dst IP	Src Port# Dst Port#	M
Frame	L2	Src MAC Dst MAC	Src IP Dst IP	Src Port# Dst Port#	M

IP Address

- เราจะเริ่มต้นจาก นามธรรมที่ให้กับระบบคอมพิวเตอร์แต่ละเครื่องที่ต้องการจะมีตัวตน ในโลกของระบบเครือข่าย

  เรียกว่า Internet Protocol (IP)

  Address



Decomposition of an IPv4 address from dot-decimal notation to its binary value

- IP v4 เป็นค่าตัวเลขนาด 32 bits
  - การบ้าน 1) IP v4 มีค่าได้กี่ค่า
  - การบ้าน 2) Dotted Notation คืออะไรจงแสดงการแปลงค่า IP จาก Binary เป็น Dotted Notation
  - การบ้าน 3) CIDR คืออะไร เกี่ยวข้องกับ IP address อย่างไร
- IP address เป็นนามธรรมที่ unify Network ทั่วโลกเข้าด้วยกันเป็นระบบเดียว

https://en.wikipedia.org/wiki/IP_address#IPv4_addresses

Private IP Address

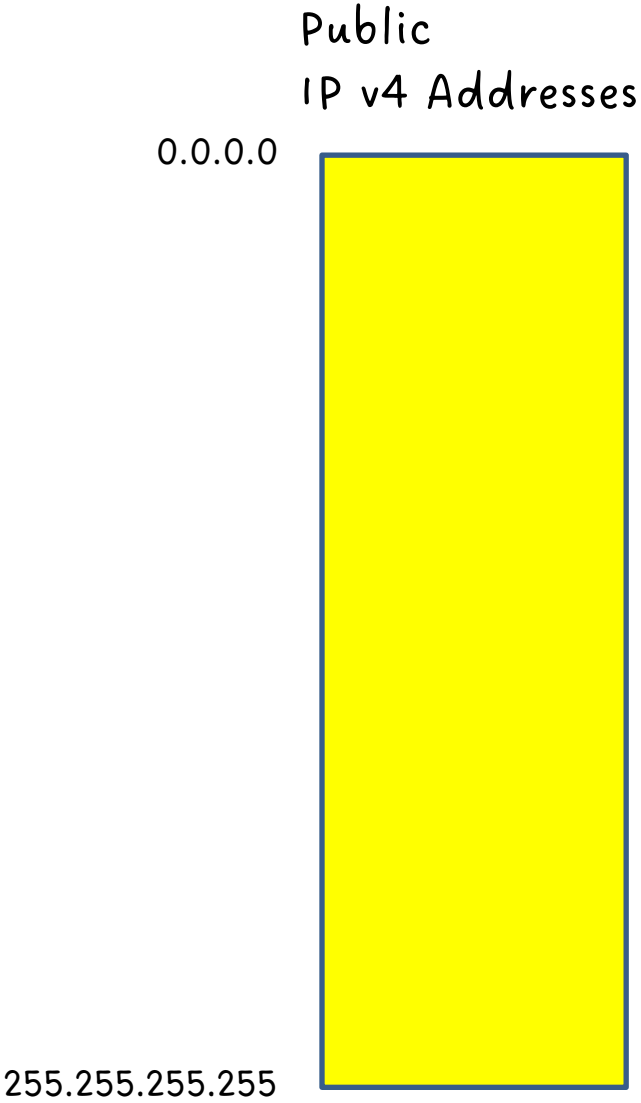
- IP address มี 2 ชนิด ได้แก่ Private IP address and Public IP address
- Private IP address Ranges (RFC 1918)

RFC 1918 name	IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits	*Classful* description[Note 1]
24-bit block	10.0.0.0 – 10.255.255.255	16 777 216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 – 172.31.255.255	1 048 576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 – 192.168.255.255	65 536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

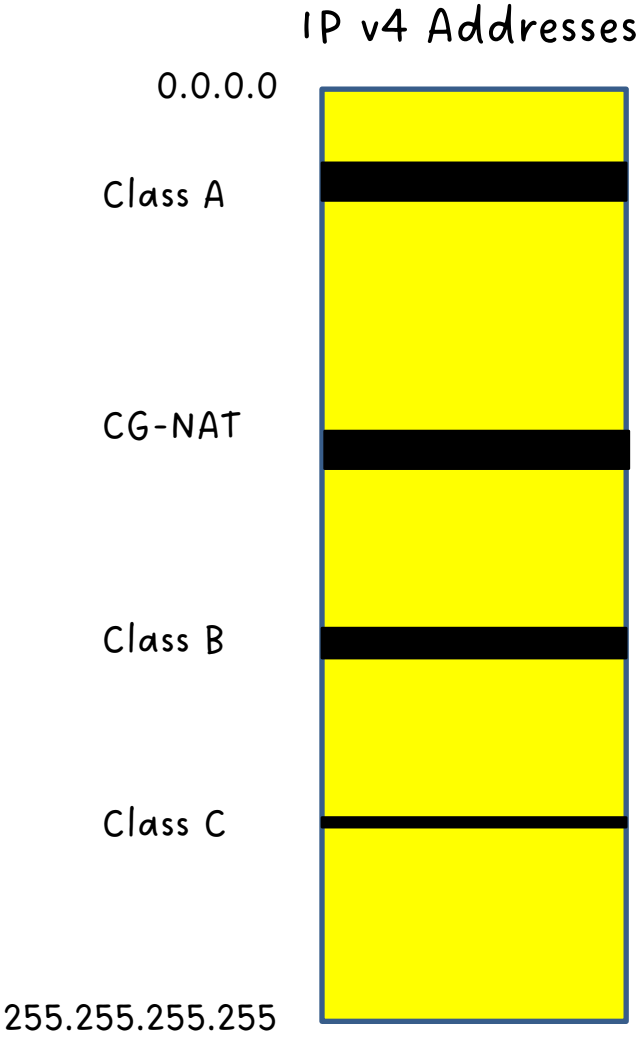
- Carrier-Grade NAT IP range (RFC 6598)
  - 100.64.0.0/10 (100.64.0.0 to 100.127.255.255, netmask 255.192.0.0) ประมาณ 4 ล้าน addresses

https://en.wikipedia.org/wiki/Private_network

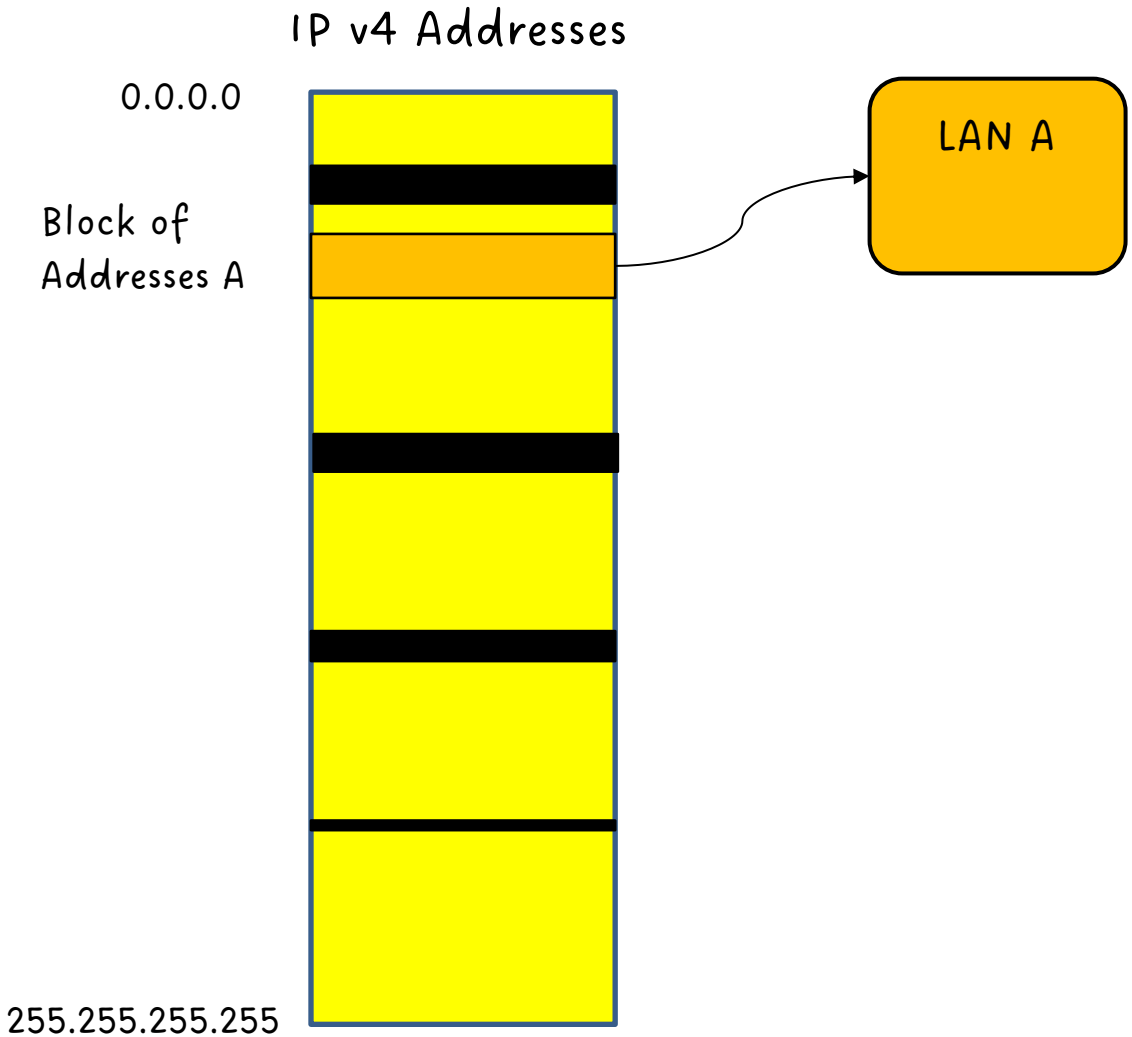
IP Address กับโครงสร้างของอินเตอร์เน็ต

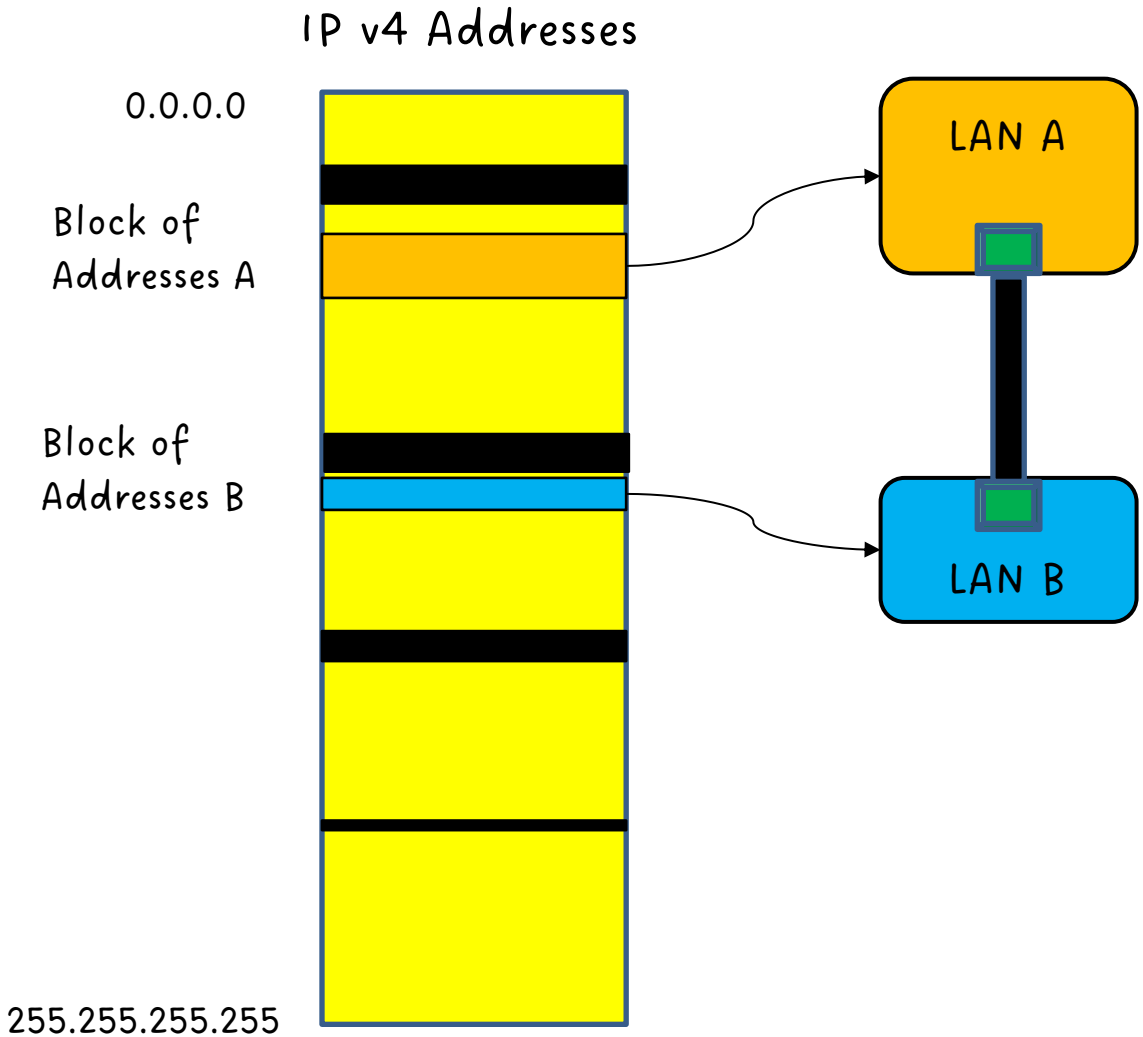


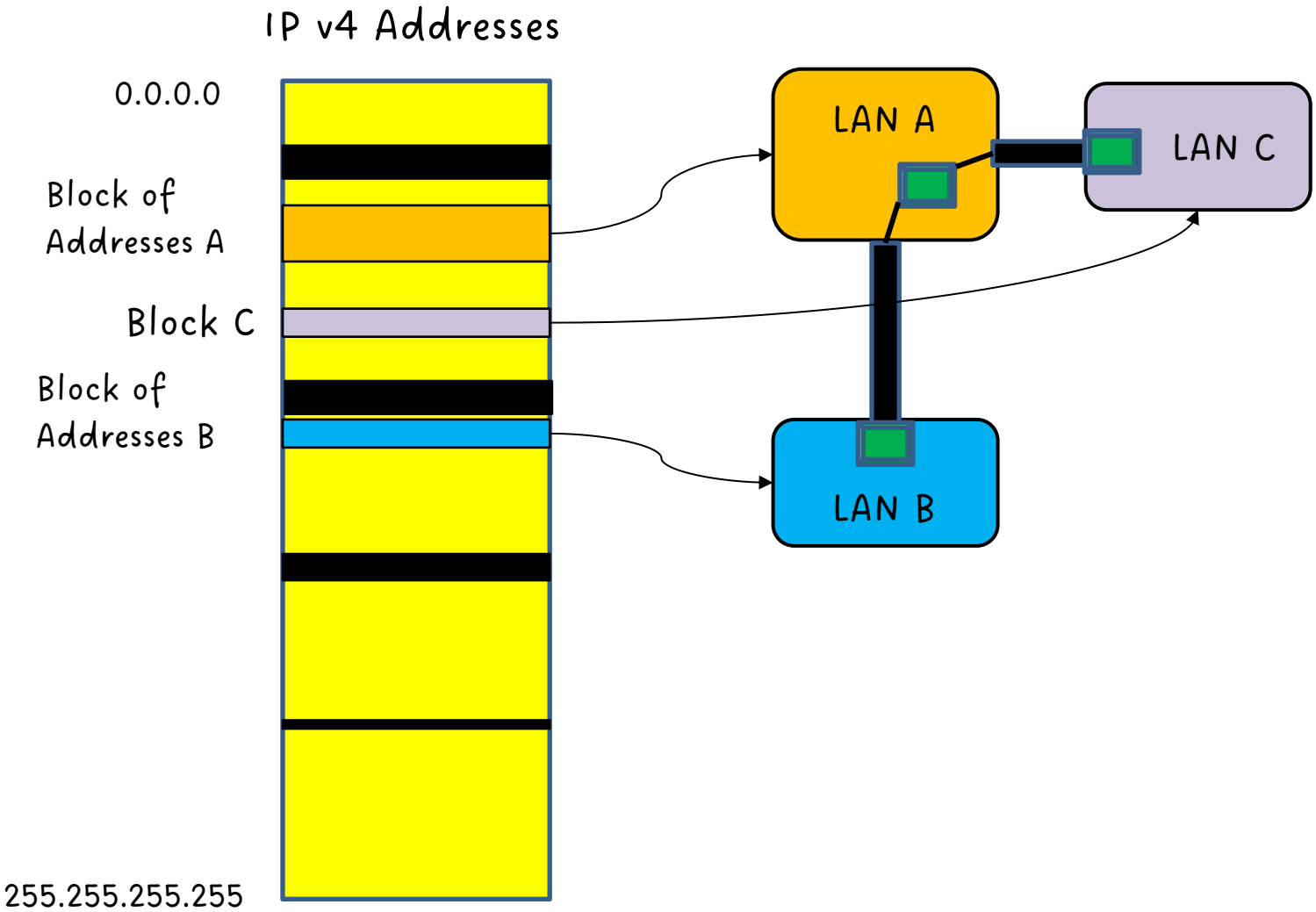
Private IP Address Ranges

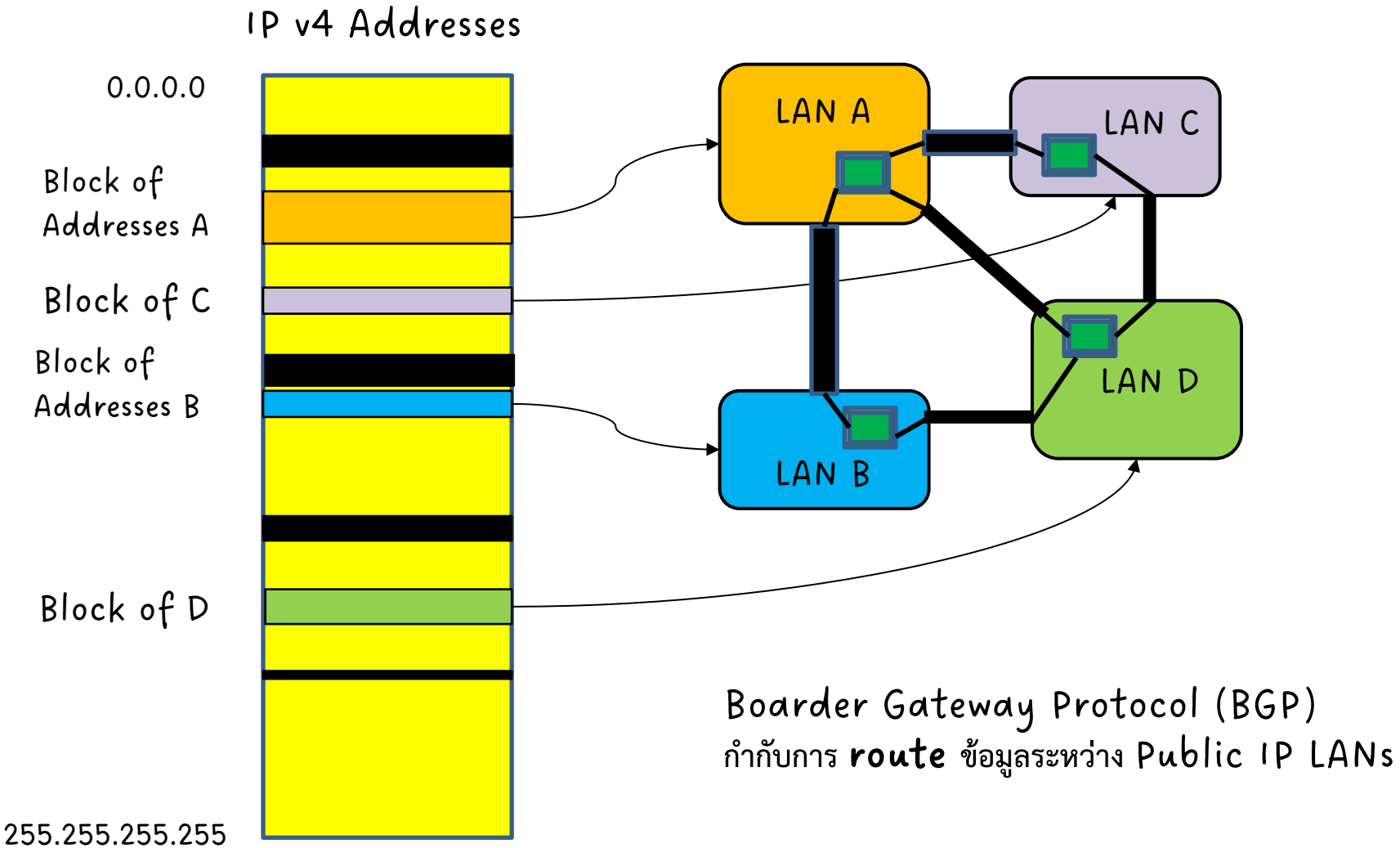


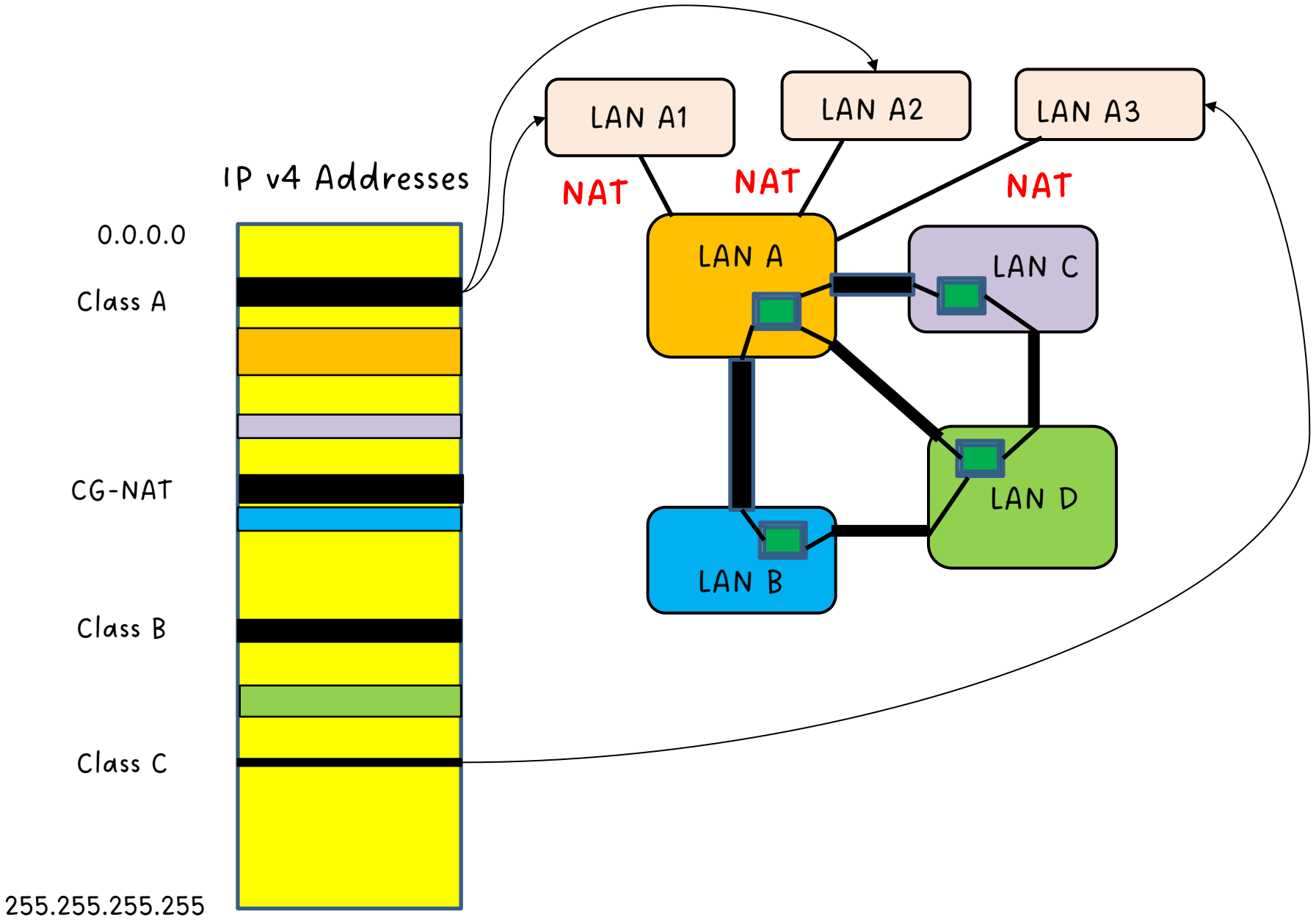
โครงสร้างของอินเตอร์เน็ต

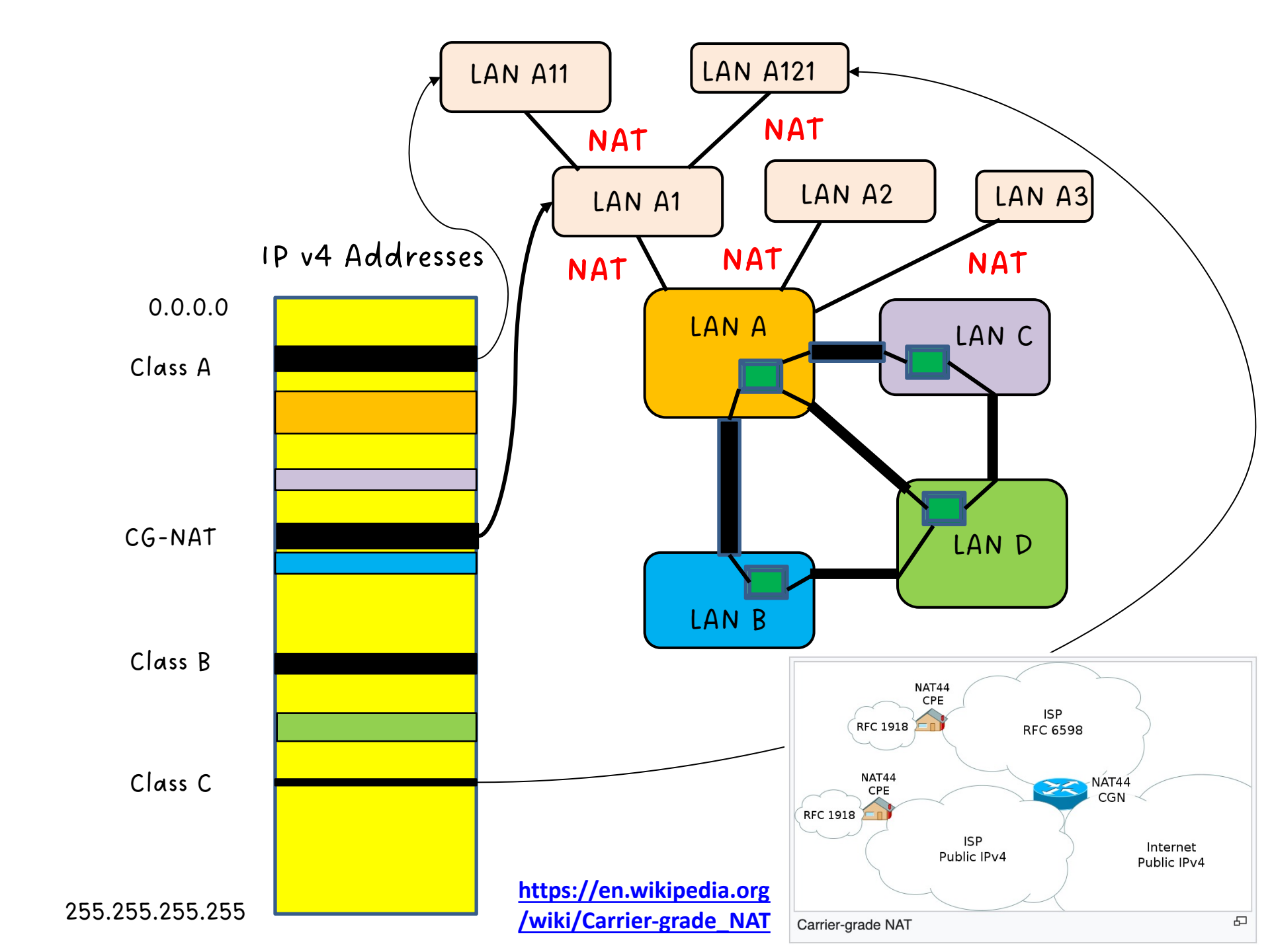



IP v4 Addresses
0.0.0.0
Block of Addresses A
Block of Addresses B
255.255.255.255
LAN A
LAN B


IP v4 Addresses
0.0.0.0
Block of Addresses A
Block C
Block of Addresses B
255.255.255.255
LAN A
LAN C
LAN B


IP v4 Addresses
0.0.0.0
Block of Addresses A
Block of C
Block of Addresses B
Block of D
255.255.255.255
LAN A
LAN C
LAN D
LAN B
Boarder Gateway Protocol (BGP)
กำกับการ route ข้อมูลระหว่าง Public IP LANs


IP v4 Addresses
0.0.0.0
Class A
CG-NAT
Class B
Class C
255.255.255.255
LAN A1
LAN A2
LAN A3
NAT
NAT
NAT
LAN A
LAN C
LAN D
LAN B

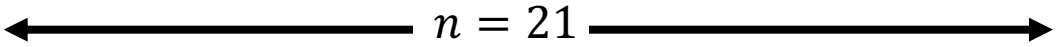

LAN A11
LAN A121
NAT
NAT
LAN A1
LAN A2
LAN A3
NAT
NAT
NAT
LAN A
LAN C
LAN D
LAN B
IP v4 Addresses
0.0.0.0
Class A
CG-NAT
Class B
Class C
255.255.255.255
https://en.wikipedia.org/wiki/Carrier-grade_NAT
NAT44 CPE
RFC 1918
ISP RFC 6598
NAT44 CGN
NAT44 CPE
RFC 1918
ISP Public IPv4
Internet Public IPv4
Carrier-grade NAT

Local Area Network

- คือระบบเครือข่ายพื้นฐานที่สุดในอินเตอร์เน็ต
- ประกอบไปด้วย
  - router gateway คือคอมพิวเตอร์ ที่มีหลาย NICs
    - มี NIC หนึ่งที่เชื่อมต่อกับเครือข่ายภายใน และอีกอันเชื่อมต่อภายนอก
  - อุปกรณ์ส่งข้อมูล คือ Hub และ Switch (ใช้ Bridge protocol)
  - คอมพิวเตอร์ที่เชื่อมต่อกับ Hub และ Switch
- คอมพิวเตอร์ใน LAN เดียวกันจะแชร์ IP address Block เดียวกัน เรียกอีกอย่างว่า Subnet
- IP address ของ Subnet อาจเป็น Public หรือ Private IP Address ก็ได้

Classless Inter-Domain Routing

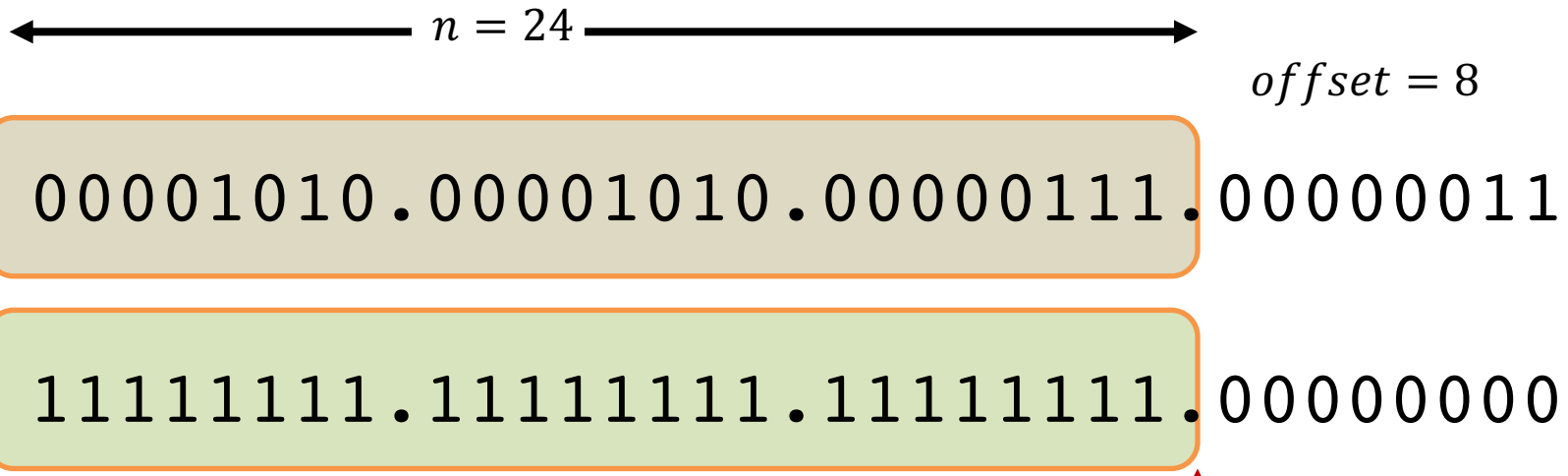
- คือวิธีการจัดสรรค่า IP address และการ Route IP packets
- มีรูปแบบคือ **a.b.c.d/N** ซึ่ง $0 \leq n \leq 32$
- เป็นการแบ่งค่า IP address ออกเป็น สองส่วน
- ส่วนแรกคือ Network Address (หรือหมายเลข Subnet) คือ N bit นับตั้งแต่ Most Significant Bit
- ส่วนที่สองคือ Offset ของเครื่องภายใน Network Address (หรือ subnet)



$offset = 11$

aaaaaaaa.bbbbbbbb.ccccccccc.ddddddddd

Subnet ของ LAN



- CIDR ของ IP address ข้างบนคือ 10.10.7.3/24
- Subnet Address คือ 10.10.7.0
- IP Address คือ 10.10.7.3
- Netmask คือ 255.255.255.0

Subnet ของ LAN

$offset = 16$

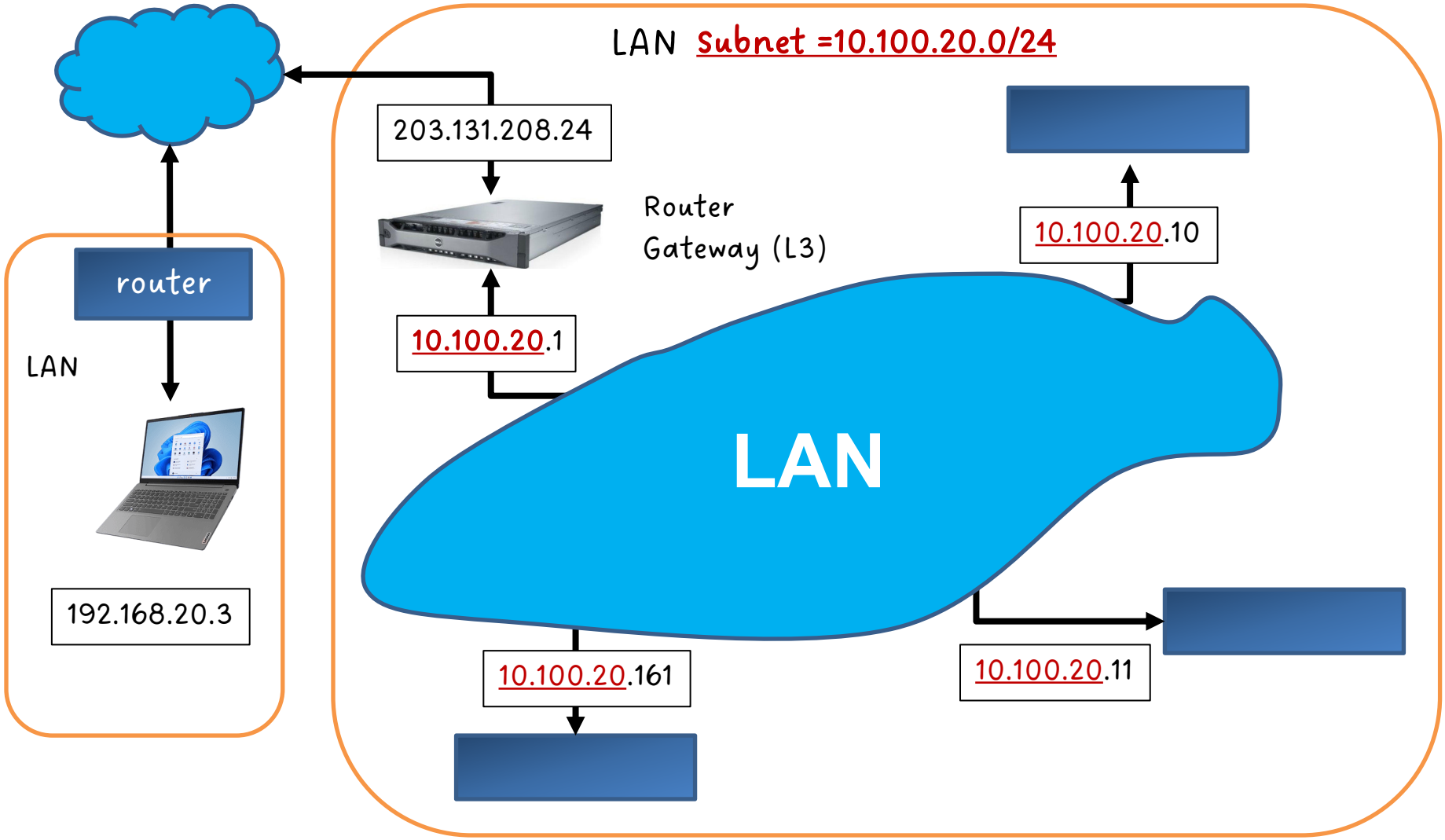
10101100.00001000.00000000.00000011

11111111.11111111.00000000.00000000

- CIDR ของ IP address ข้างบนคือ 171.16.0.3/16
- Subnet Address คือ 172.16.0.0
- IP Address คือ 172.16.0.3
- Netmask คือ 255.255.0.0

Subnet ของ LAN

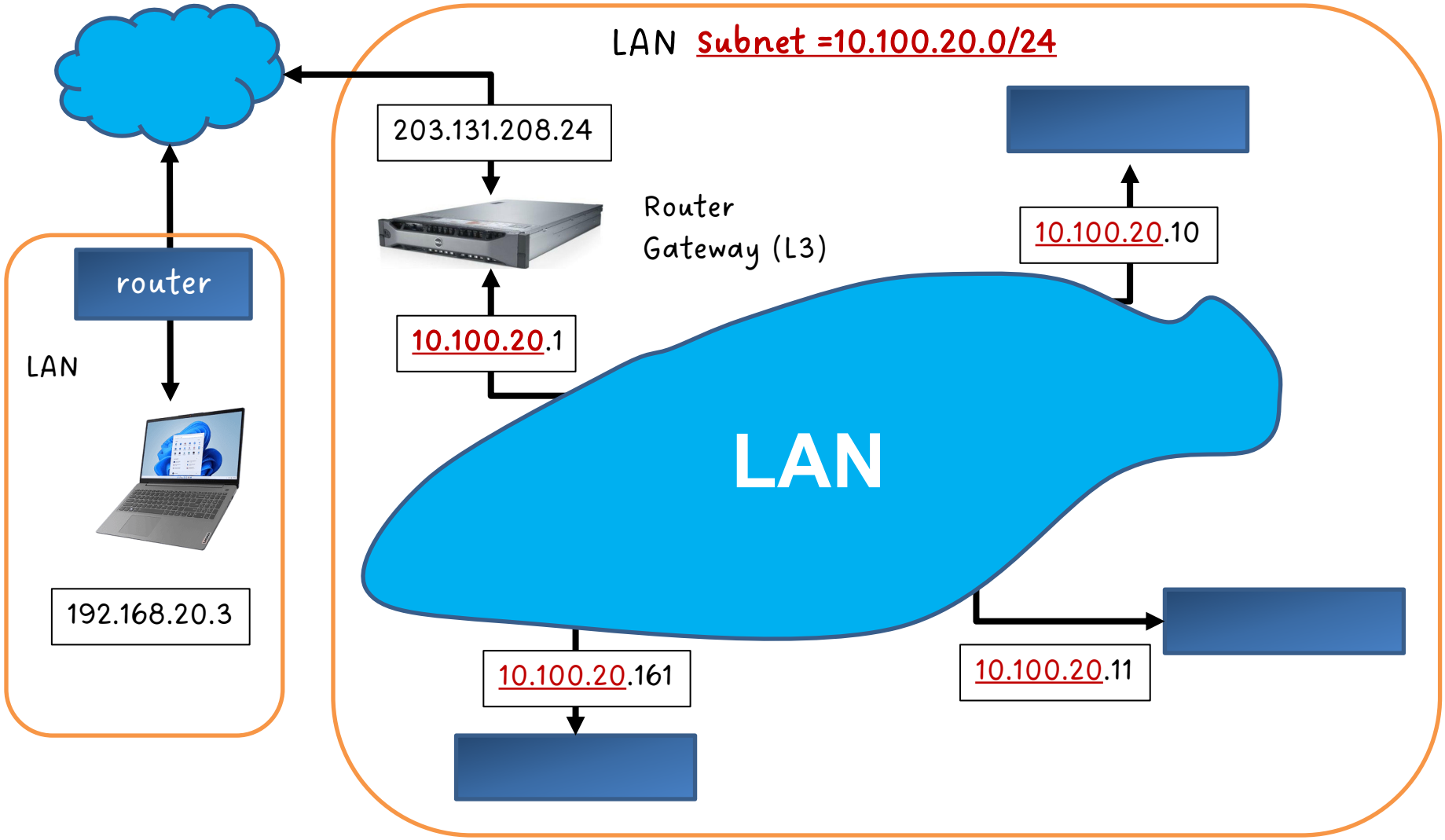
- โดยทั่วไปแล้ว ถ้า N = 31 จะมี offset สองค่า ซึ่งทำให้ Assign IP ได้สองค่าจะเป็น point to point link
- โดยทั่วไปแล้ว ถ้า N = 30 จะมี offset 4 ค่า ซึ่งทำให้ Assign IP offset =1 และ 2 จะเป็น point to point link
- การบ้าน 1) จงระบุว่า Block ของ IP ของ Subnet 192.168.0.0/28 มีกี่ IP address และเป็นตั้งแต่ค่าใด ถึงค่าใด
- การบ้าน 2) จงระบุว่า Block ของ IP ของ Subnet ถัดจาก 192.168.0.0/28 คืออะไร กำหนดให้ Subnet ใหม่มีจำนวน IP เท่ากันกับของ 192.168.0.0/28
- Prefix ของ IP address หมายถึง bit ตั้งแต่ MSB มาจนถึงจำนวน P bits แล้วแต่ผู้ใช้จะกำหนดว่าค่า p เป็นเท่าใด



ราคา Network Switch ลดลงมาก TP-link 5 port 10 Gbps ราคา Lazada = 13000 B
ใช้ CAT6e และ CAT7 Ethernet Cable

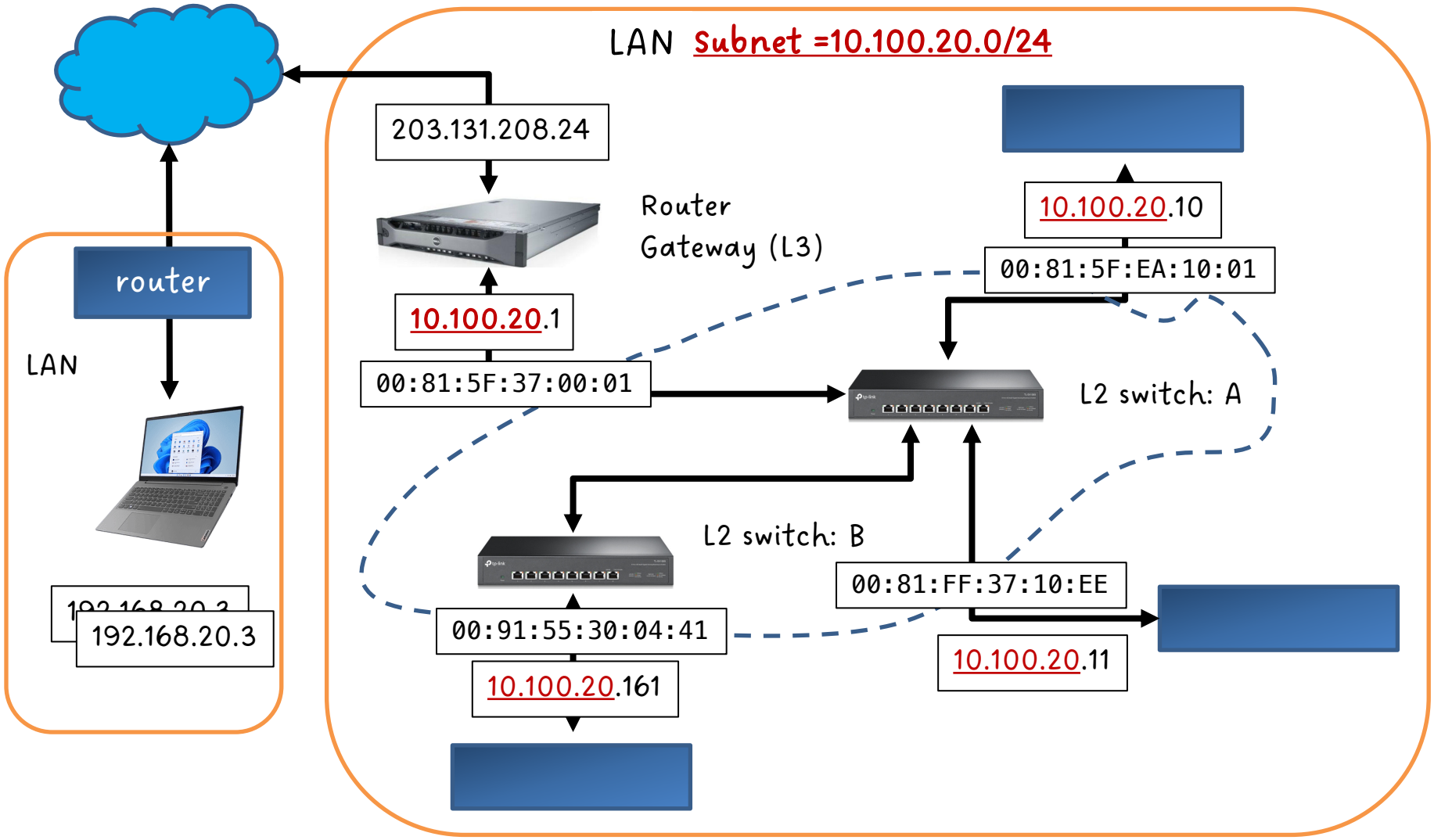
ราคา Network Switch ลดลงมาก TP-link 5 port 10 Gbps ราคา Lazada = 6000 B
ใช้ SPF+ Cable (แปลง digital เป็น แสง ส่งผ่าน fiber optic cable)

ความสัมพันธ์ระหว่าง Layer 3 และ Layer 2 Networking



ราคา Network Switch ลดลงมาก TP-link 5 port 10 Gbps ราคา Lazada = 13000 B
ใช้ CAT6e และ CAT7 Ethernet Cable

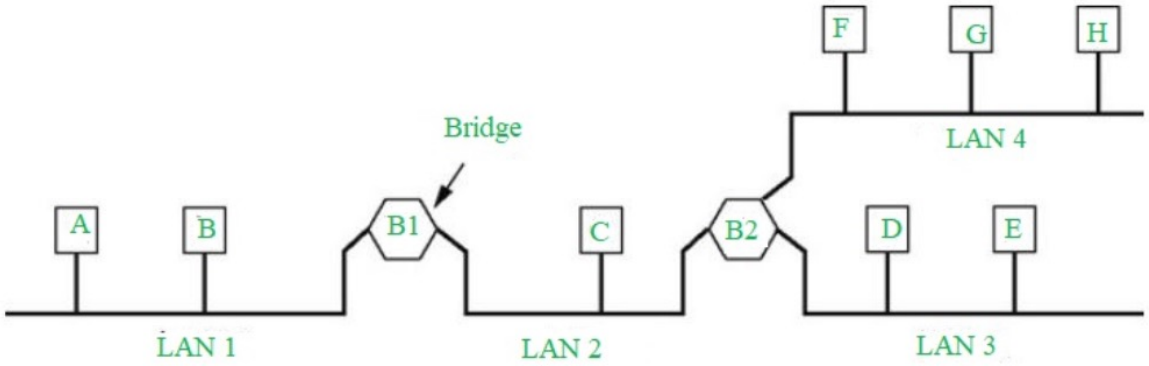
ราคา Network Switch ลดลงมาก TP-link 5 port 10 Gbps ราคา Lazada = 6000 B
ใช้ SPF+ Cable (แปลง digital เป็น แสง ส่งผ่าน fiber optic cable)


LAN Subnet =10.100.20.0/24
203.131.208.24
Router
Gateway (L3)
10.100.20.1
00:81:5F:37:00:01
10.100.20.10
00:81:5F:EA:10:01
L2 switch: A
L2 switch: B
00:91:55:30:04:41
10.100.20.161
00:81:FF:37:10:EE
10.100.20.11
router
LAN
192.168.20.3

Data Link Layer (Layer 2)

- Data Link Layer ประกอบไปด้วยกระบวนการที่กำกับการทำงานของ hardware ที่เชื่อมต่อระบบคอมพิวเตอร์ในระบบเครือข่าย
- การทำงานของกระบวนการดังกล่าวขึ้นอยู่กับลักษณะการเชื่อมต่อของคอมพิวเตอร์ (Network Topology)
  - Linear Network, Bus Network, Star Network, Ring Network, Hybrid Network
- คอมพิวเตอร์ทุกเครื่องจะมีอุปกรณ์ Network Interface Card (NIC) ที่ใช้เชื่อมต่อระบบเครือข่าย และใช้ Media Access Control (MAC) Protocol เพื่อสื่อสารข้อมูล
- แต่ละ NIC จะมี MAC address ที่เป็นเลขที่ไม่ซ้ำกันใน LAN

LAN และ Bridge Device

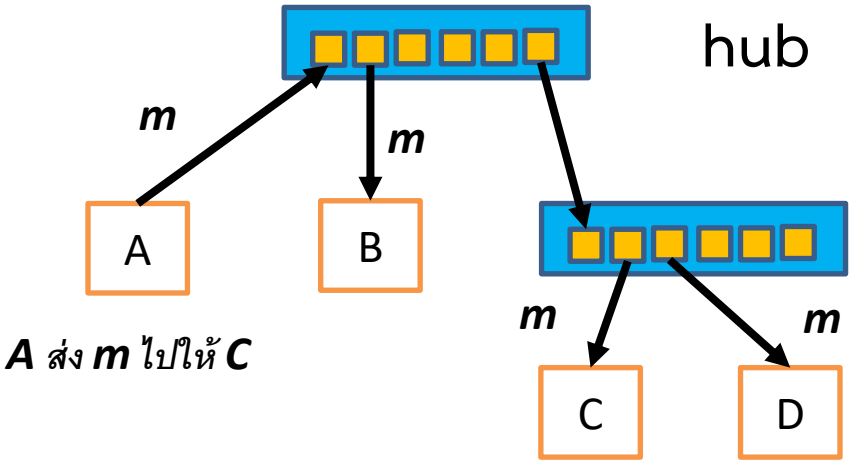


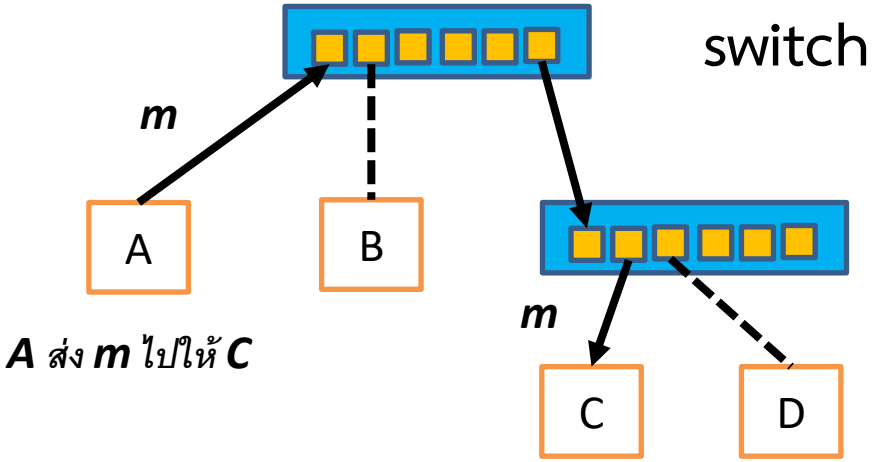
https://www.geeksforgeeks.org/bridges-local-internetworking-device/

- ในอดีต Ethernet Network เชื่อมต่อคอมพิวเตอร์ด้วย Bus Network และเรียกการเชื่อมต่อนี้ว่า LAN
  - ข้อเสียหลักของ Bus คือประสิทธิภาพไม่ดีเมื่อปริมาณ network traffic สูง
- Bridge คืออุปกรณ์เชื่อมต่อ LAN เข้าด้วยกัน โดยที่มันจะสร้าง Table เพื่อจำ MAC address ของคอมพิวเตอร์ว่ามาจาก Port ไหน
- ในอดีต Bridge มีจำนวน port จำกัด (2 ถึง 4 ports) ดังในภาพ

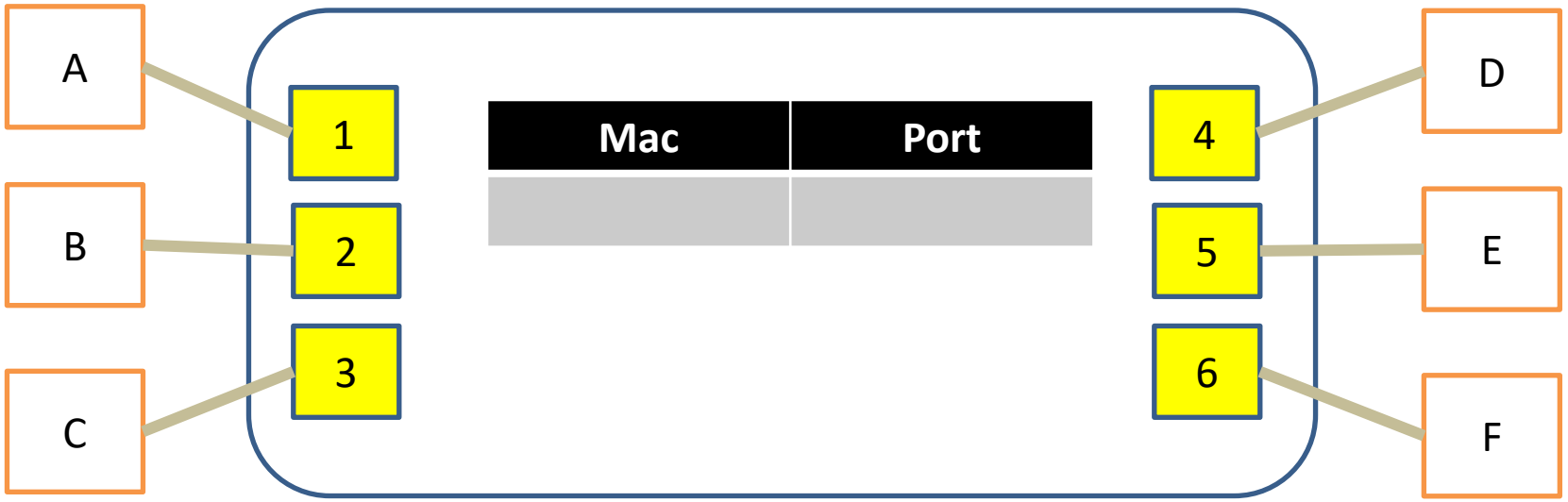
Hub v.s. Brdge v.s. Switch

- Hub เรียกอีกอย่างว่า repeater เป็นอุปกรณ์ที่มีหลาย ports และจะนำข้อมูลที่รับจาก port หนึ่งส่งต่อออกทุก ports (ยกเว้น port ที่รับเข้ามา)
- Bridge มีจำนวน port จำกัด
- Switch คือ bridge ที่มีจำนวน port มากกว่า 2 ports (multiport bridge)
  - Hub ประสิทธิภาพไม่ดีเมื่อมี traffic มาก
  - Bridge ไม่ใช้สำหรับเชื่อมต่อคอม



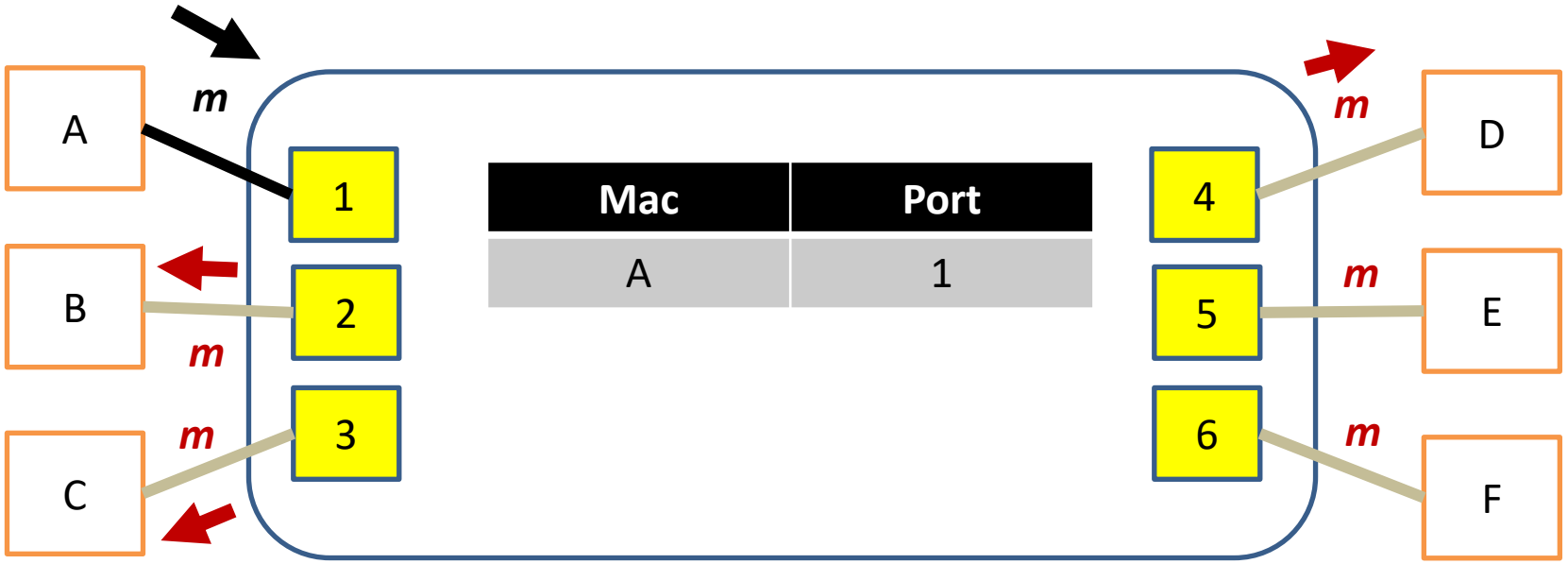


Switch: S



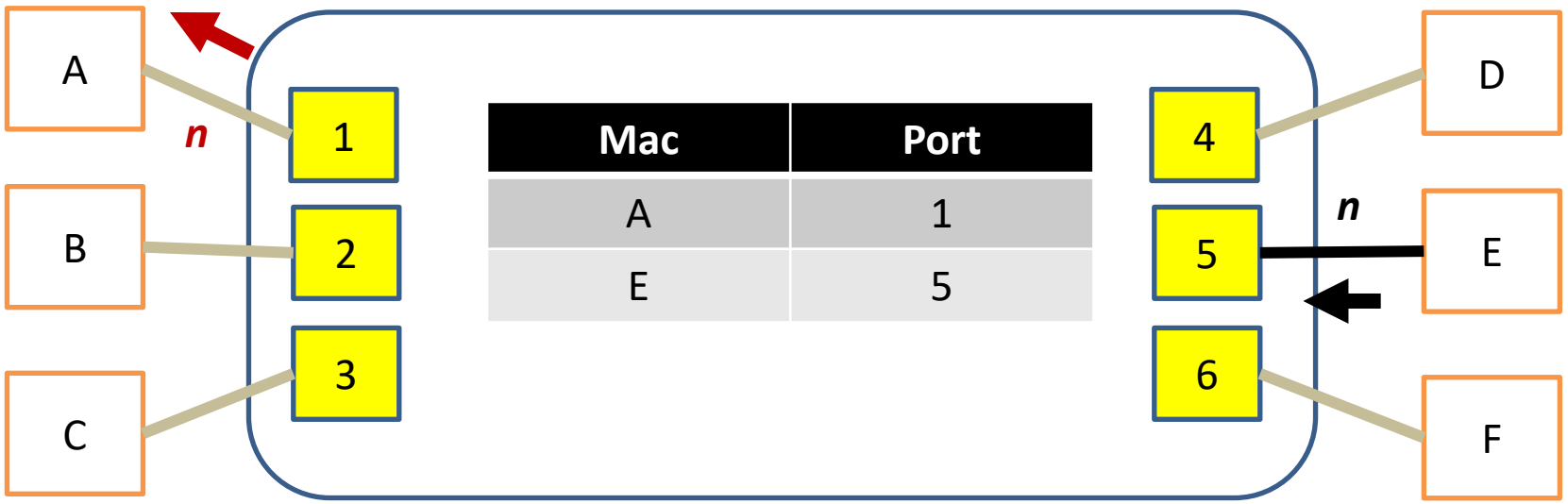
- กำหนดให้ A, B, ..., F เป็นค่า MAC address ของ NIC ของคอมพิวเตอร์ที่เชื่อมต่อ switch ที่ port# 1 ถึง 6 ของ Switch ”S”

Switch: S



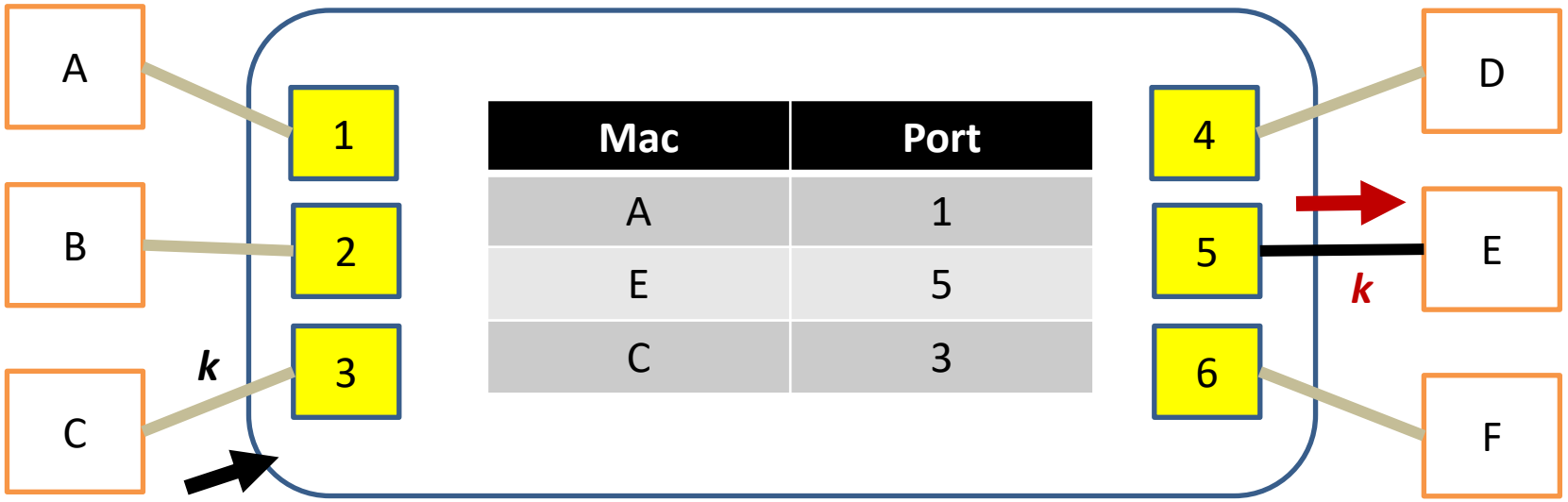
- MAC A ส่ง m ให้ E ซึ่ง Switch S จะรับ m เข้ามาทาง port 1 และจำไว้ในตาราง
- Bridge protocol จะหาในตารางว่า MAC อยู่ที่ port ไหน ถ้าไม่เจอมันจะ Flood (ส่งออก) ทุก Port ที่ไม่มีข้อมูลการ mapping ในตาราง

Switch: S



- ต่อมาเมื่อ E ส่ง n ตอบกลับ A Switch S ก็จะดูในตารางและพบว่า MAC A อยู่ที่ Port 1 และจะ Forward ข้อมูลออกที่ port 1 และ
- เก็บค่า MAC E และ port 5 ไว้ในตาราง

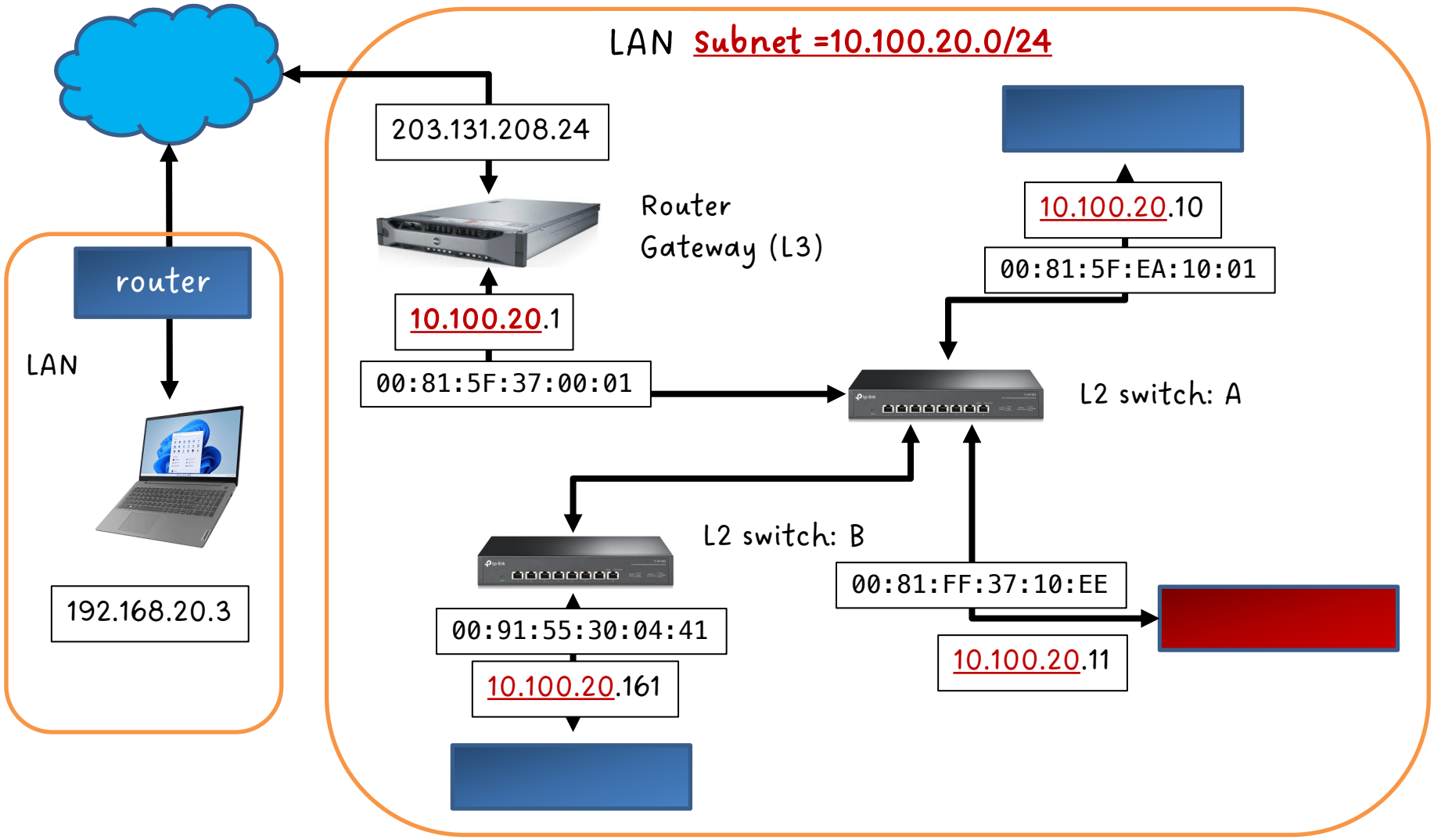
Switch: S



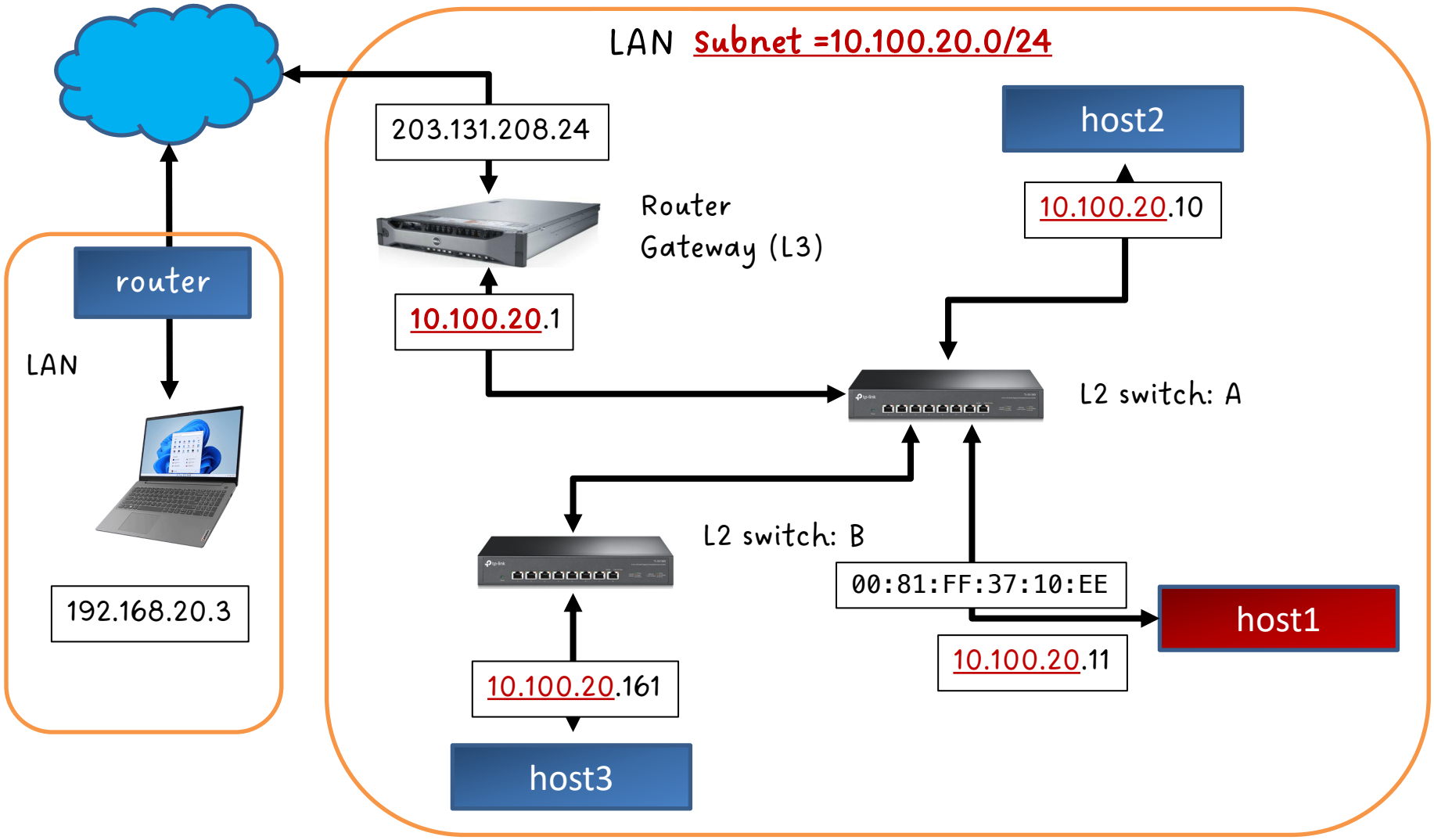
- ต่อมาเมื่อ C ส่ง k ให้ E Switch S ก็จะดูในตารางและพบว่า MAC E อยู่ที่ Port 5 และจะ Forward ข้อมูลออกที่ port 5 และ
- เก็บค่า MAC C และ port 3 ไว้ในตาราง
- Port สามารถเชื่อมกับ switch อื่นได้ ในกรณีนี้ค่า MAC หลายค่า สามารถถูก Map ไปที่ port เดียวกันได้

Address Resolution Protocol

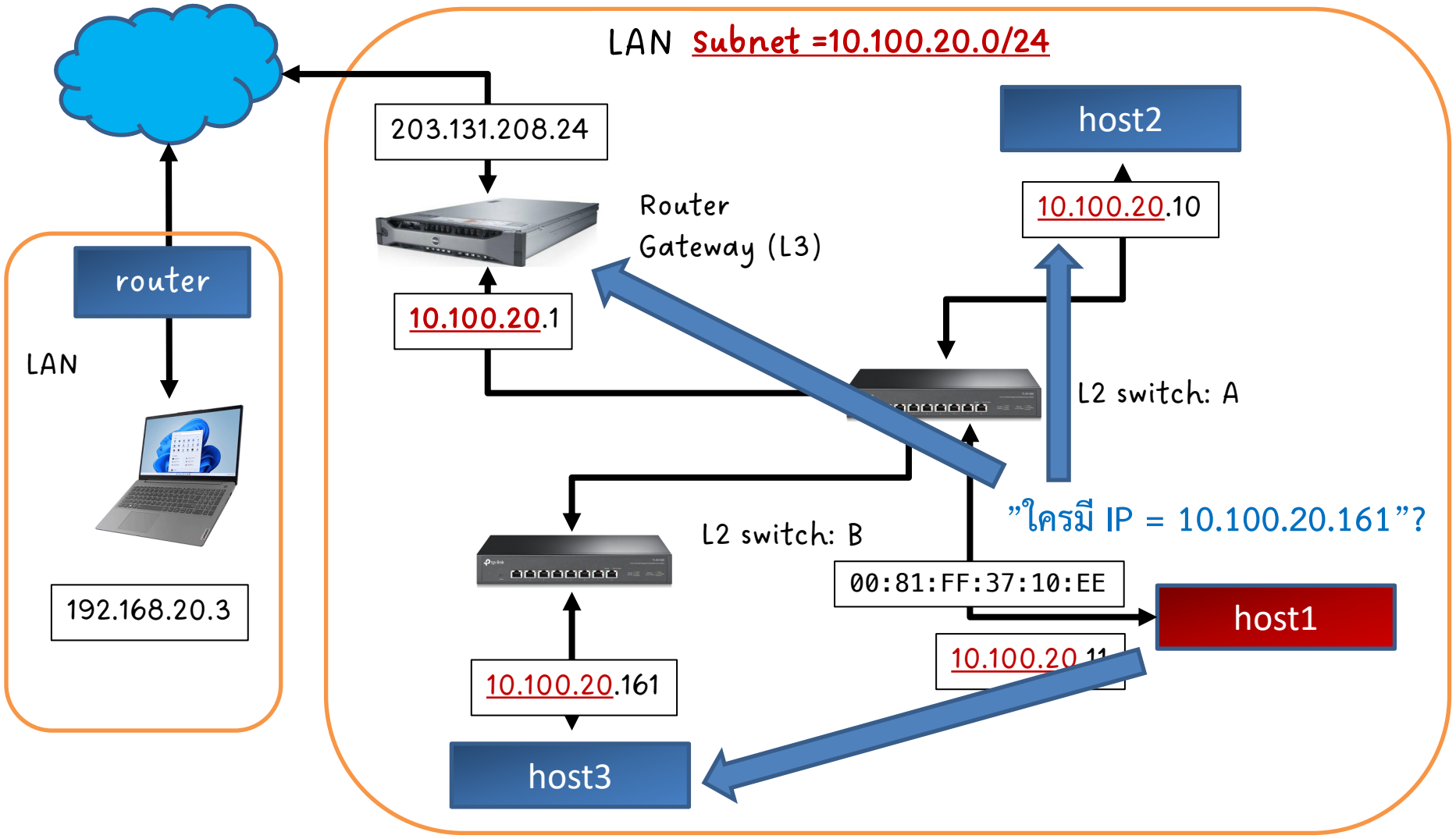
- ในขณะที่เราใช้ Domain Name Systems (DNS) ใน Application Layer (Layer 5) เพื่อแปลง domain name เช่น www.tu.ac.th ให้เป็น IP address เพื่อใช้ในการสื่อสารระดับ Transport Layer (Layer 3) และ Network Layer (Layer 3)
- เราจะใช้ Address Resolution Protocol (ARP) ในระดับ Data Link Layer (Layer 2) เพื่อแปลง IP address ให้เป็น MAC Address ซึ่งเป็น header ของ frame ข้อมูลใน Layer 2



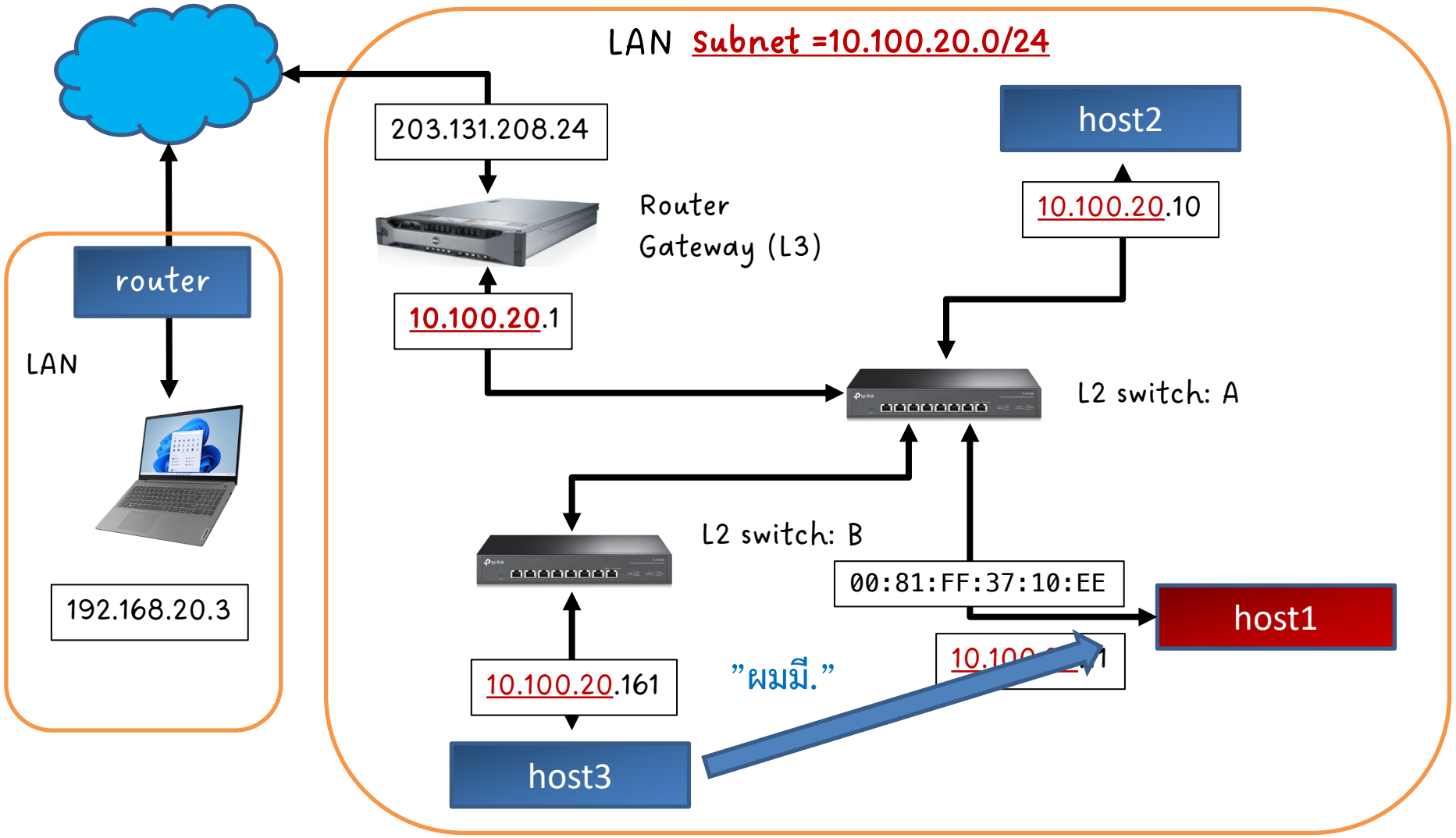
- ทุกเครื่องมี MAC Address



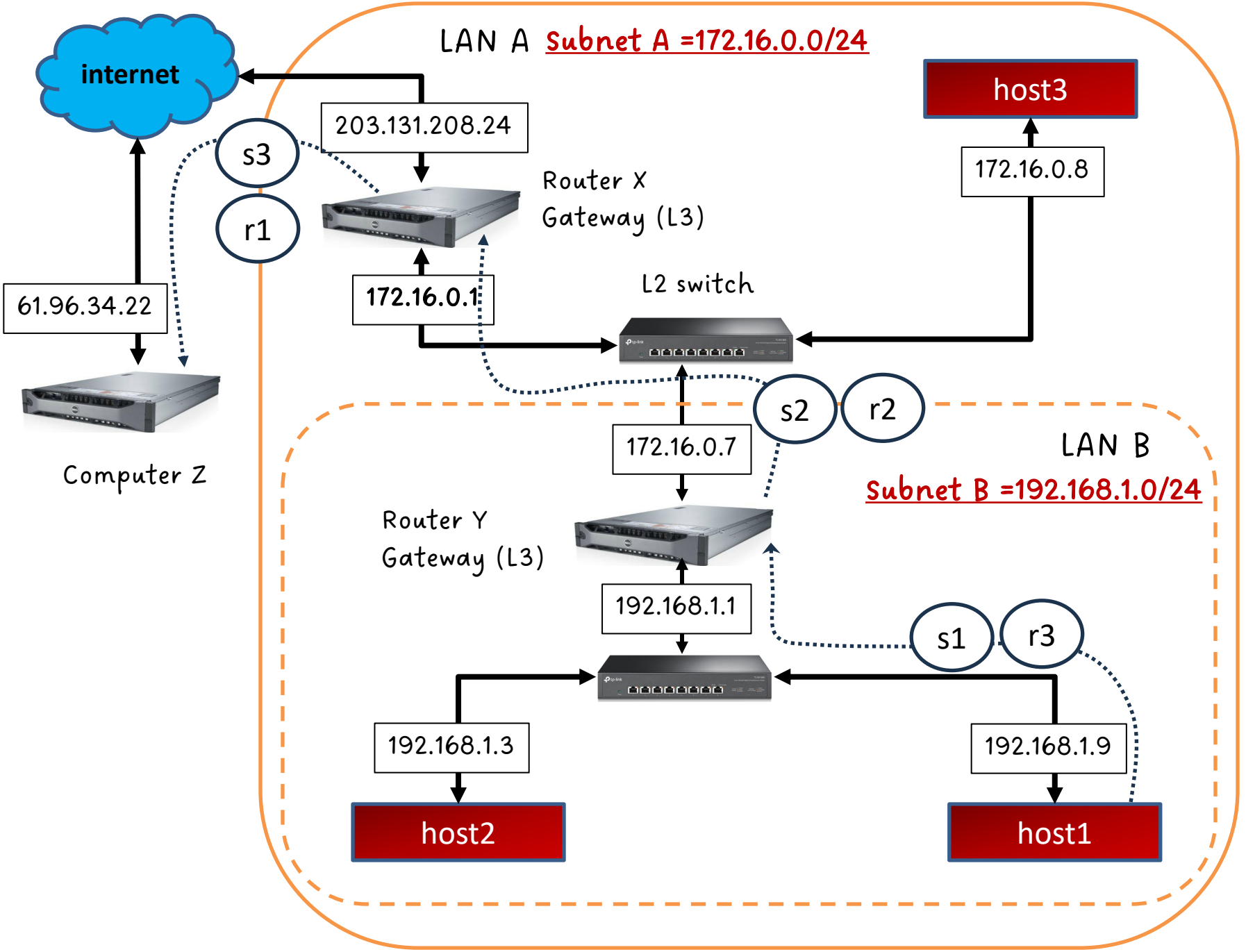
- host1 จะส่ง frame ให้ host3
- host1 รู้จัก MAC Address ของตนเอง ไม่รู้จัก MAC ของเครื่อง host3
- host1 รู้แต่ IP ของ host3



- host1 จะใช้ ARP protocol เพื่อหา MAC ของ 10.100.20.161
- Host1 broadcast frame คำถามให้ทุกเครื่อง "ใครมี IP 10.100.20.161"



- เครื่อง host3 จะตอบกลับเครื่องเดียว
- host1 จะจำค่า mac ของ 10.100.20.161ไว้
- switch A และ B จะบันทึกข้อมูลว่า MAC ของ host1 และ host3 อยู่ที่ port ใด


LAN A Subnet A =172.16.0.0/24
internet
203.131.208.24
s3
r1
Router X
Gateway (L3)
host3
172.16.0.8
61.96.34.22
172.16.0.1
L2 switch
Computer Z
s2
r2
172.16.0.7
LAN B
Subnet B =192.168.1.0/24
Router Y
Gateway (L3)
192.168.1.1
s1
r3
192.168.1.3
192.168.1.9
host2
host1

กลับมาที่การเชื่อมต่อระหว่าง LAN กับ Internet ใน Layer 3

NAT

- เป็นวิธีการที่ทำให้ IPv4 ยังคงเป็น IP หลักบนระบบอินเตอร์เน็ตอยู่ได้ เพราะมันอนุญาตให้องค์กรสร้าง LAN และ LAN ของ LAN โดยที่แต่ละ LAN มีโลกของ IP address ของตนเอง
- ใน Lab เราใช้ Public IP ค่าเดียวก็เพียงพอที่จะทำให้เครื่องทุกเครื่องในระบบ LAN สื่อสารกับคอมพิวเตอร์เครื่องอื่นๆบนอินเตอร์เน็ตได้
- โปรเซสบนคอมพิวเตอร์ใน LAN ทำตัวเป็น TCP Client ติดต่อกับ TCP Server บนอินเตอร์เน็ตได้
- มี SNAT และ DNAT **(การบ้าน)**

SNAT

- เนื่องจาก Header ของ TCP/IP packet จะประกอบไปด้วย
  - (Source IP, Source Port#, Dest IP, Dest Port#)
- กระบวนการ SNAT จึงใช้ประโยชน์จาก คู่ Pair ของ IP และ Port นั้น
- โดยที่ router จะแปลงค่า Source IP address ของ Packet ให้เป็น IP address ของ router และ port number ใหม่
- router จะจำไว้ว่า Source IP และ Source port ใหม่ Map เข้ากับ Original IP กับ port number เดิม
- เมื่อมีข้อความ TCP ส่งกลับมาให้ Source IP ใหม่และ Source port ใหม่ router ก็จะแปลงกลับให้เป็น Original IP กับ Original port number

Source Computer

Src IP	S Port	Dst IP	D port
10.100.20.3	1234	69.13.23.2	80

LAN

Router GW

INTERNET

Source Computer

LAN

Router GW

Src IP	S Port	Dst IP	D port
10.100.20.3	1234	69.13.23.2	80

INTERNET

Source Computer

LAN

Router GW

Mapping Table

New Src IP	New S Port	Ori Src IP	Ori S port
203.131.208.24	5678	10.100.20.3	1234

convert Source IP, S Port

Src IP	S Port	Dst IP	D port
203.131.208.24	5678	69.13.23.2	80

ส่งออก

INTERNET

Source Computer

LAN

Router GW

Mapping Table

New Src IP	New S Port	Ori Src IP	Ori S port
203.131.208.24	5678	10.100.20.3	1234

convert Source IP, S Port

Src IP	S Port	Dst IP	D port
69.13.23.2	80	203.131.208.24	5678

รับเข้า

INTERNET

Source Computer

LAN

Src IP	S Port	Dst IP	D port
69.13.23.2	80	10.100.20.3	1234

Router GW

INTERNET

Source Computer

LAN

Src IP	S Port	Dst IP	D port
69.13.23.2	80	10.100.20.3	1234

Router GW

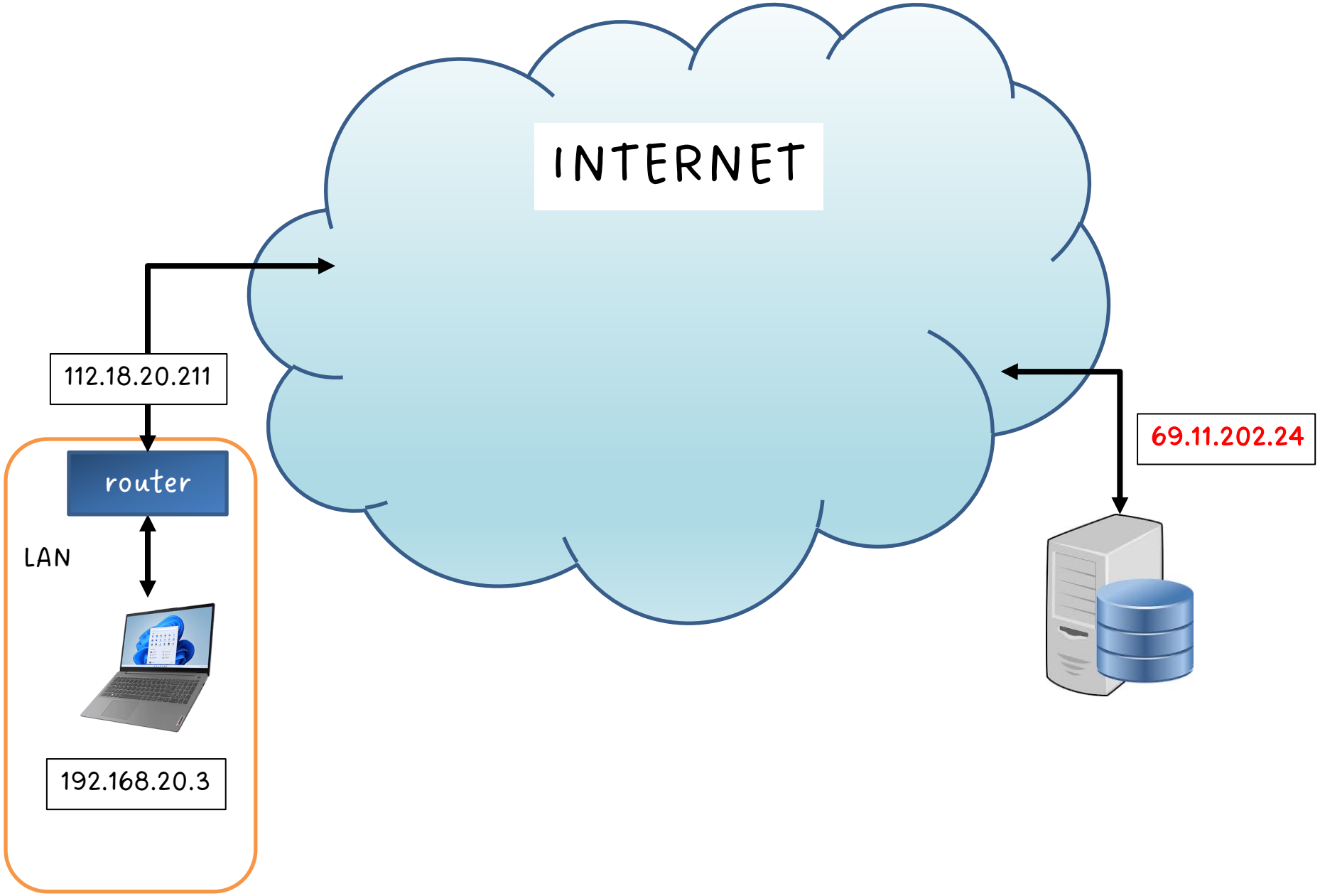
INTERNET

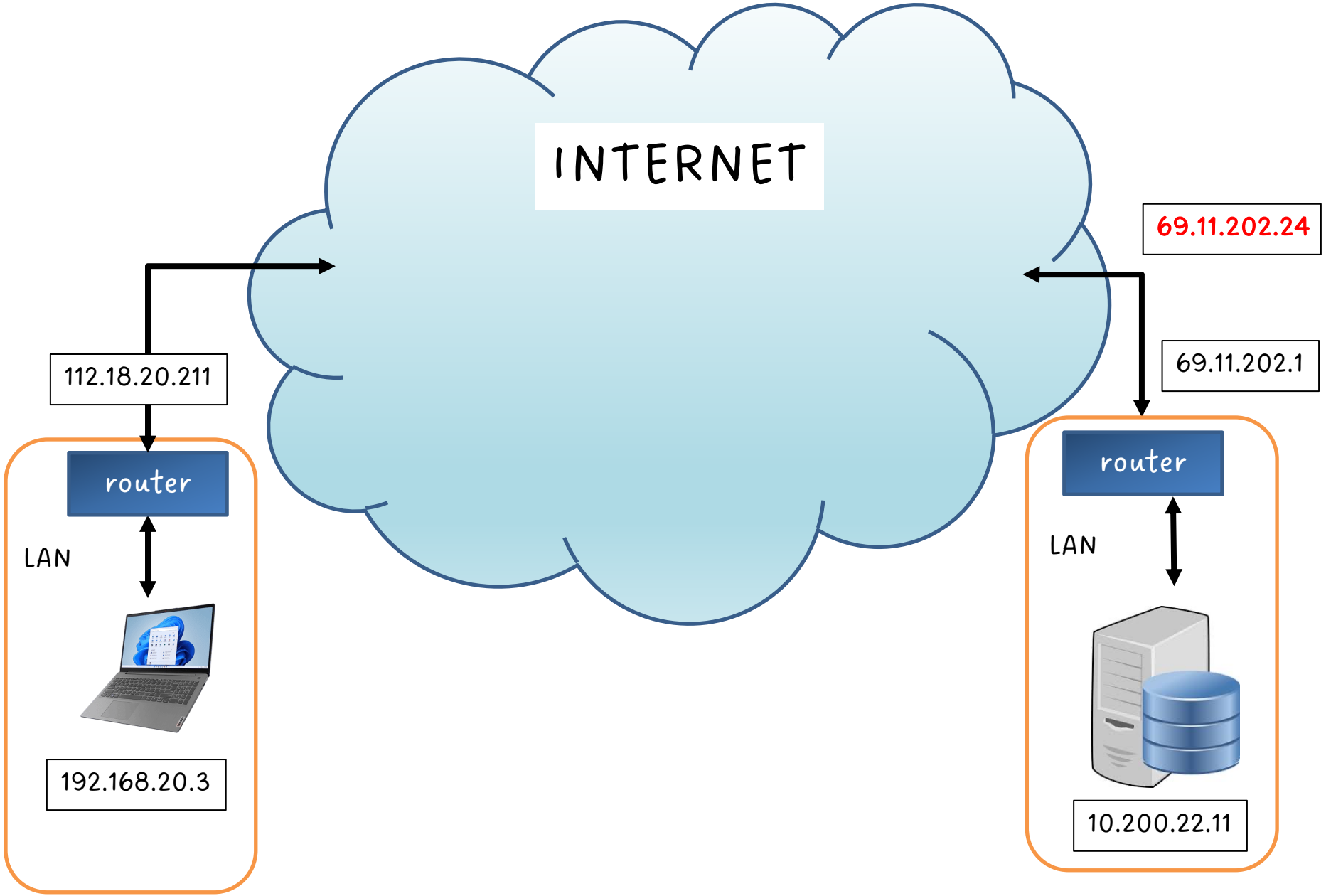
INTERNET

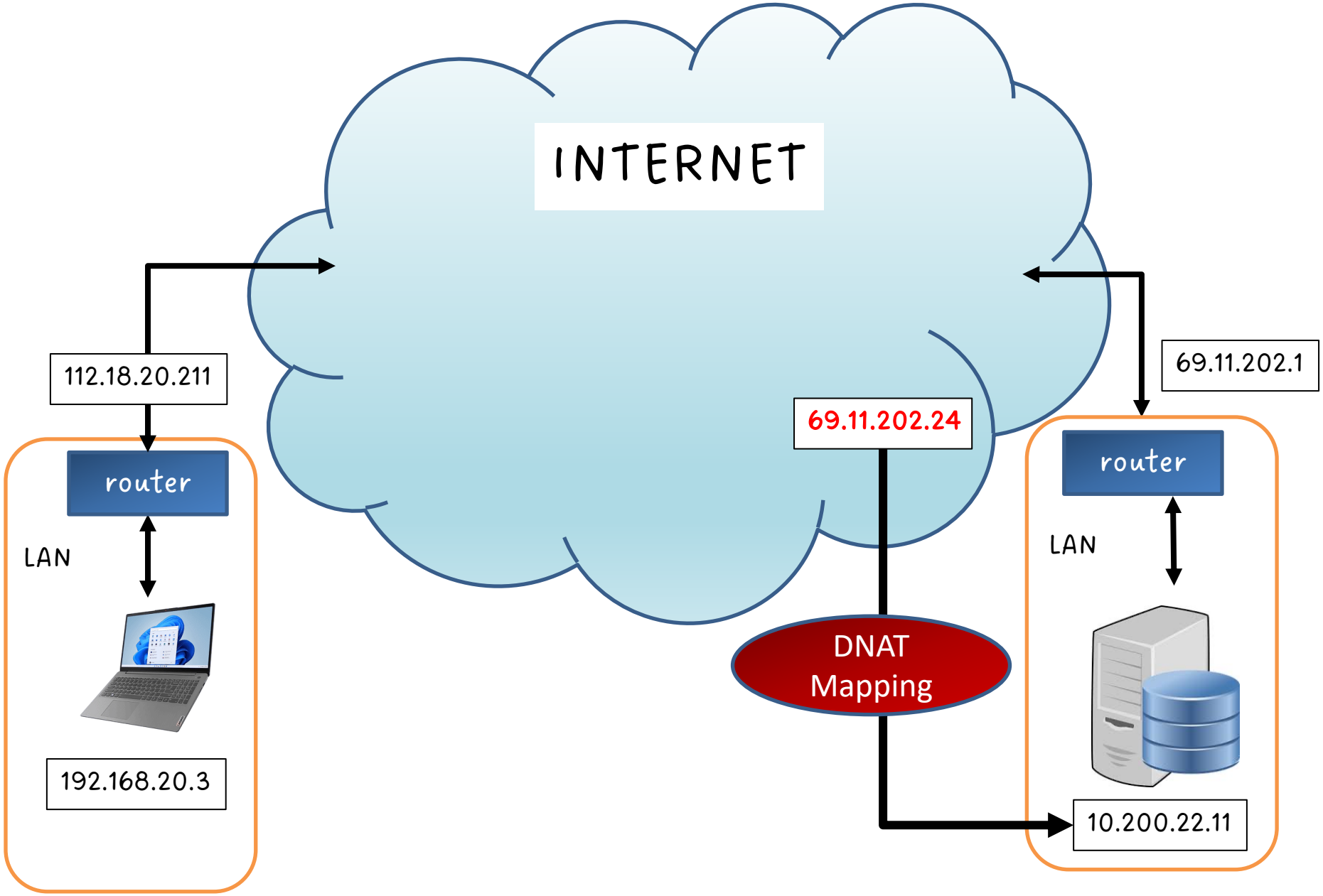
LAN A

การบ้าน

- จงเขียนรายงานว่า NAT คืออะไร มีความสำคัญอย่างไรต่อระบบ INTERNET
- SNAT คืออะไร จงอธิบายการทำงานของ SNAT
- DNAT คืออะไร จงอธิบายการทำงานของ DNAT


INTERNET
112.18.20.211
router
LAN
192.168.20.3
69.11.202.24


INTERNET
69.11.202.24
112.18.20.211
69.11.202.1
router
LAN
router
LAN
192.168.20.3
10.200.22.11


INTERNET
112.18.20.211
router
LAN
192.168.20.3
69.11.202.24
DNAT
Mapping
69.11.202.1
router
LAN
10.200.22.11

Router GW

รับเข้า

INTERNET

Src IP	S port	Dest IP	D Port
112.18.20.211	5678	69.13.23.24	80

Mapping Table

Public IP	Private IP
69.11.202.24	10.200.22.11

convert DEST IP

Src IP	S port	Dest IP	D Port
112.18.20.211	5678	10.200.22.11	80

Src IP	S port	Dest IP	D Port
112.18.20.211	5678	10.200.22.11	80

Destination Computer

Router GW

ตอบกลับ

INTERNET

Src IP	S port	Dest IP	D Port
69.11.202.24	80	112.18.20.211	5678

Mapping Table

Public IP	Private IP
69.11.202.24	10.200.22.11

convert DEST IP

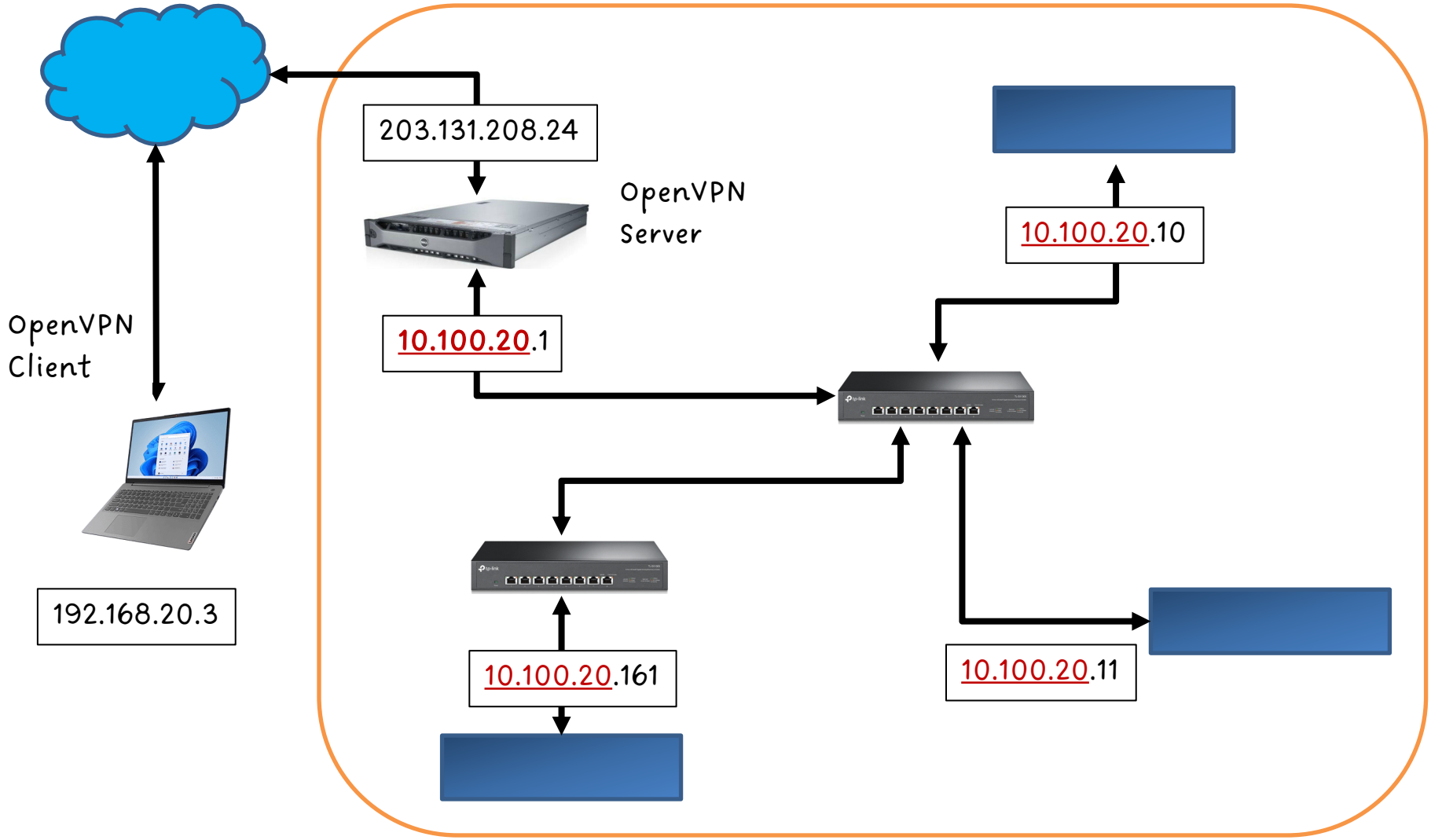
Src IP	S Port	Dest IP	D port
10.200.22.11	80	112.18.20.211	5678

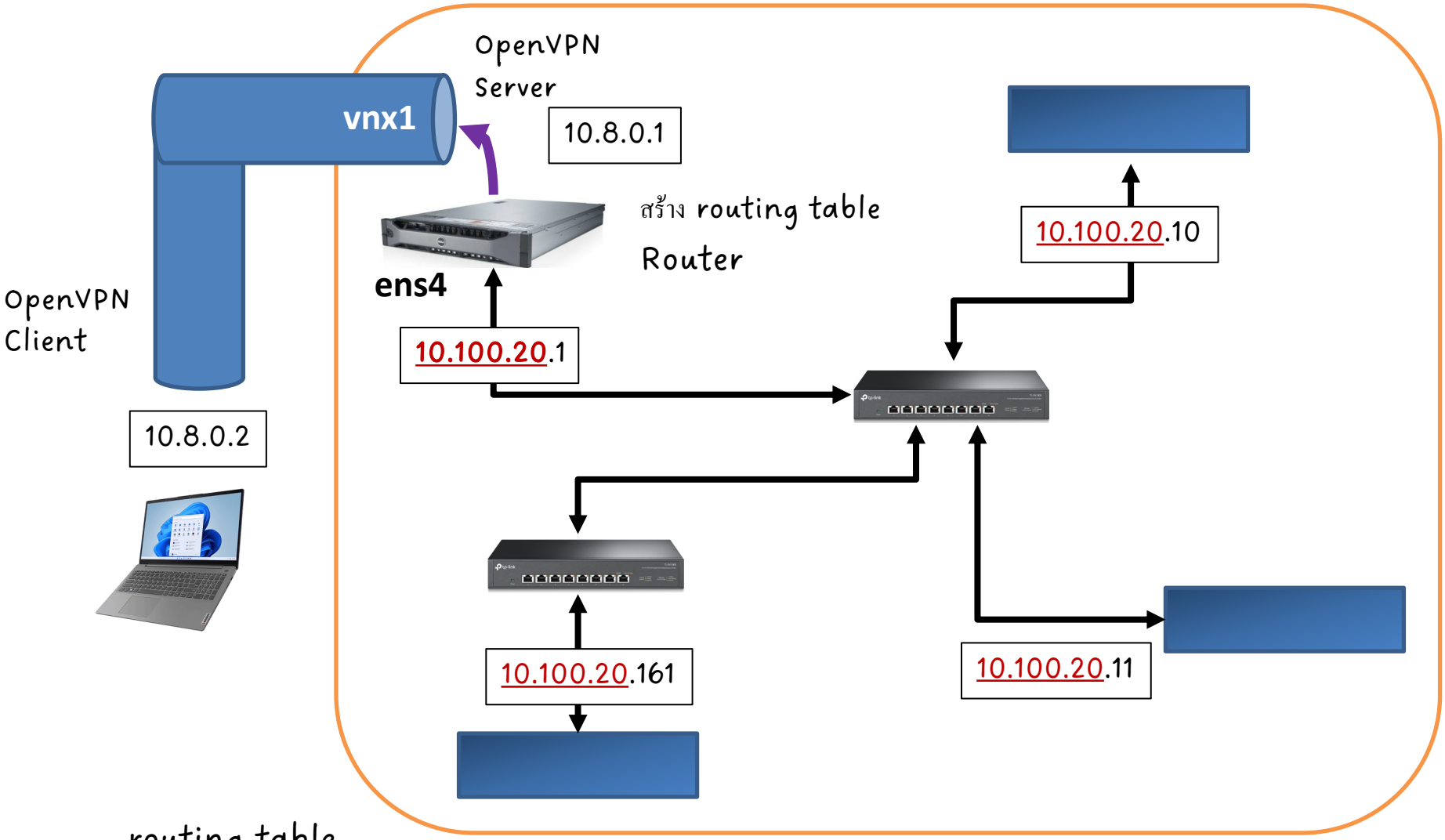
Src IP	S Port	Dest IP	D port
10.200.22.11	80	112.18.20.211	5678

Destination Computer

การเชื่อมต่อขั้นสูง

OpenVPN: การนำเอา TCP/IP (Layer 4) มาจำลองเป็น Layer 2 เพื่อเชื่อมต่อคอมพิวเตอร์เข้าสู่ LAN


203.131.208.24
OpenVPN
Server
10.100.20.10
10.100.20.1
OpenVPN
Client
192.168.20.3
10.100.20.161
10.100.20.11



routing table

Dest IP prefix	ส่งออกทาง port
10.8.0.*	vnx1
10.100.20.*	ens4

OpenVPN อธิบายอย่างง่าย

- OpenVPN จะให้ Kernel ทั้งสองฝั่งสร้าง NIC เสมือนขึ้น เรียกว่า TUN interfaces (เป็นไฟล์ๆหนึ่ง)
- TUN จะรับข้อมูล Internet Packets มาเก็บไว้
- OpenVPN ให้ OpenVPN Client และ Server สร้าง TCP connection
- OpenVPN Client จะอ่านค่าจาก TUN ไฟล์แล้วส่งไปให้ server
- OpenVPN Server รับข้อมูลมาเขียนลง TUN interface
- Server’s Kernel จะรับข้อมูลจาก TUN interface แล้วส่งต่อตามที่กำหนดบน routing table

OpenVPN

คอมพิวเตอร์ของ นศ

Kernel's routing table

prefix	NIC
192.168.20.0/24	eno1
default	eno1

NIC1

eno1

internet

lab gateway

Kernel's routing table

prefix	NIC
10.100.20.0/24	ens4
default	ens3

NIC1

ens3

ens4

NIC2

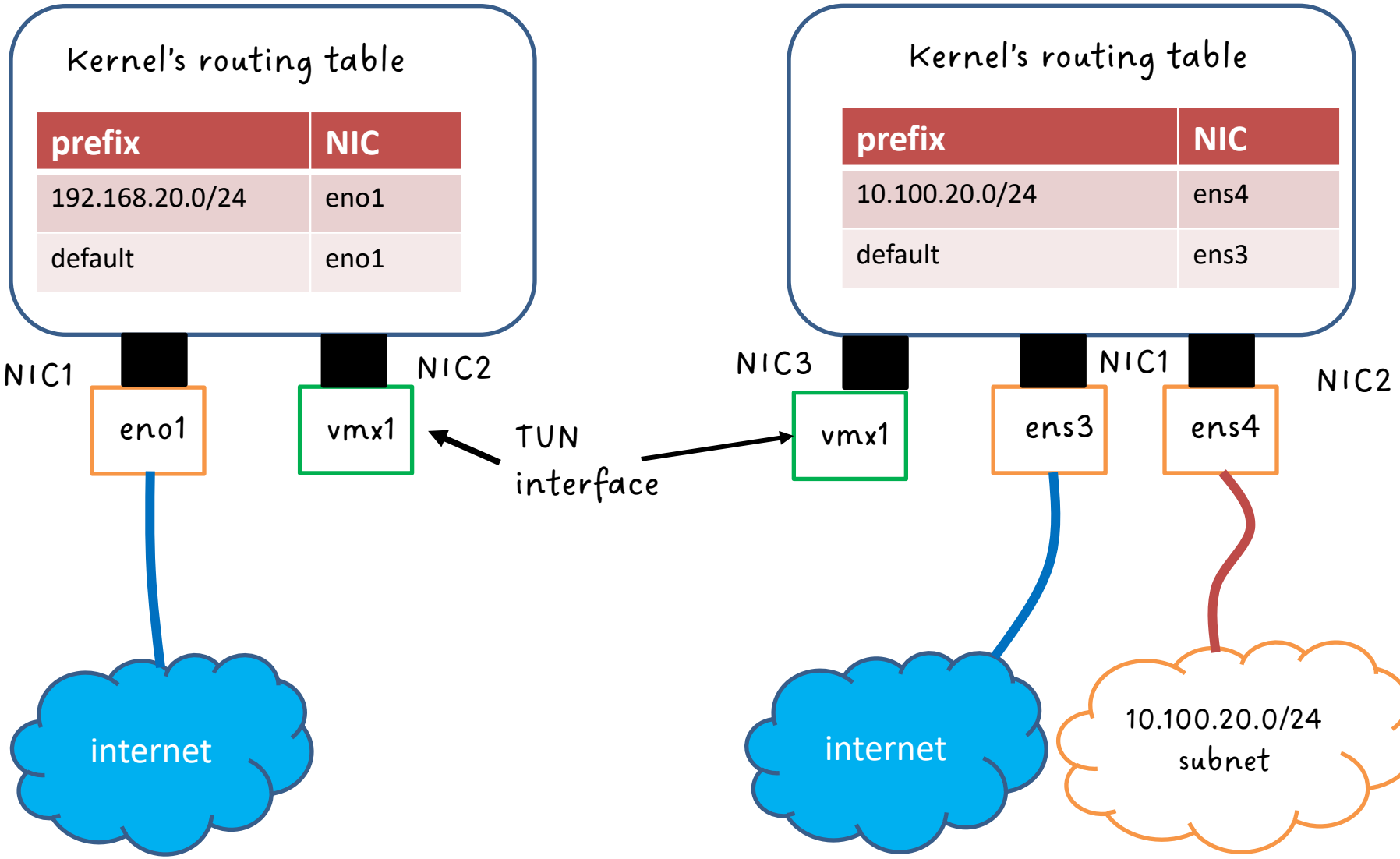
internet

10.100.20.0/24
subnet

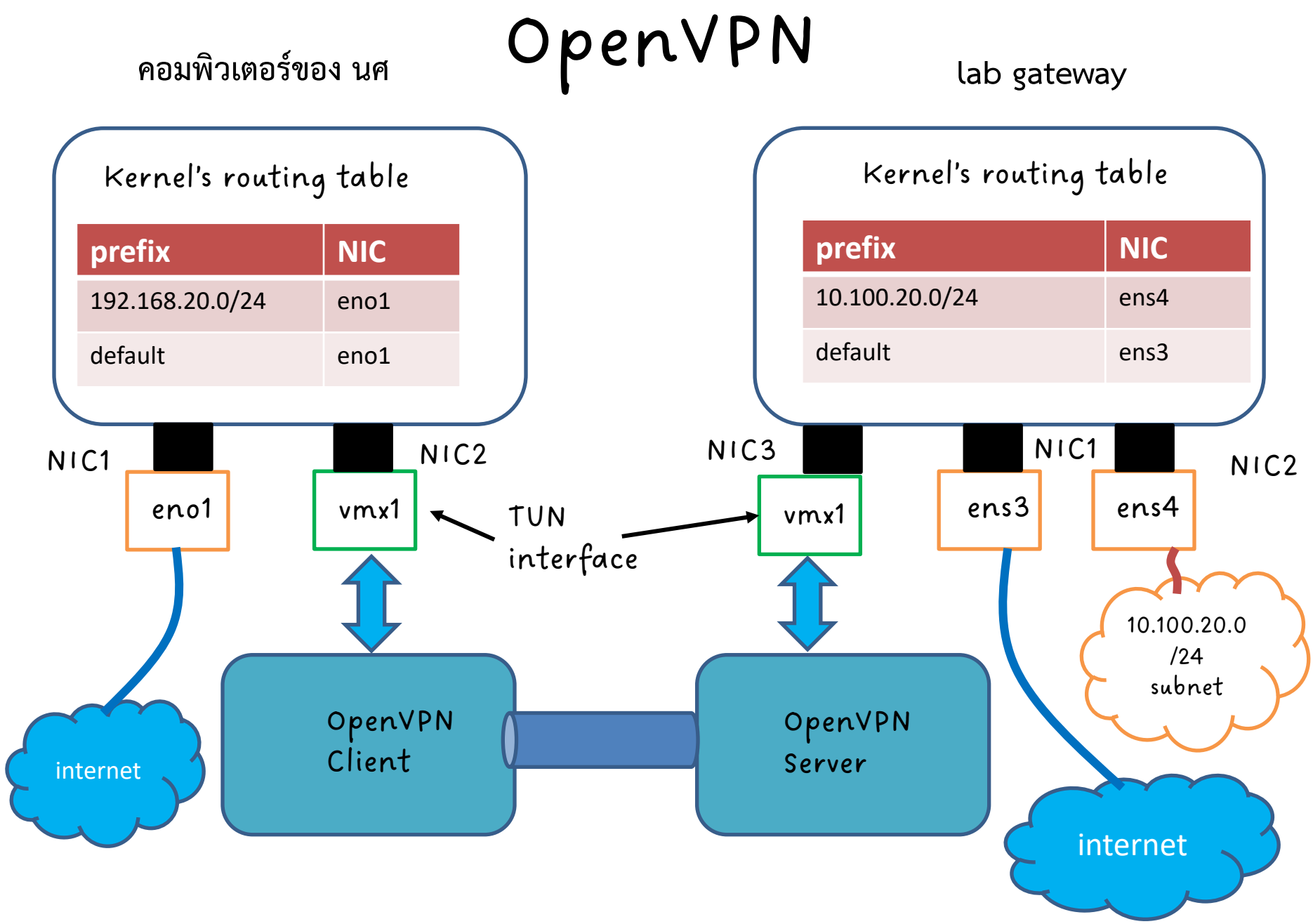
OpenVPN

คอมพิวเตอร์ของ นศ

lab gateway



OpenVPN


คอมพิวเตอร์ของ นศ
lab gateway
Kernel's routing table
prefix
NIC
192.168.20.0/24
eno1
default
eno1
Kernel's routing table
prefix
NIC
10.100.20.0/24
ens4
default
ens3
NIC1
NIC2
NIC3
NIC1
NIC2
eno1
vmx1
TUN
interface
vmx1
ens3
ens4
10.100.20.0
/24
subnet
internet
OpenVPN
Client
OpenVPN
Server
internet

OpenVPN

คอมพิวเตอร์ของ นศ

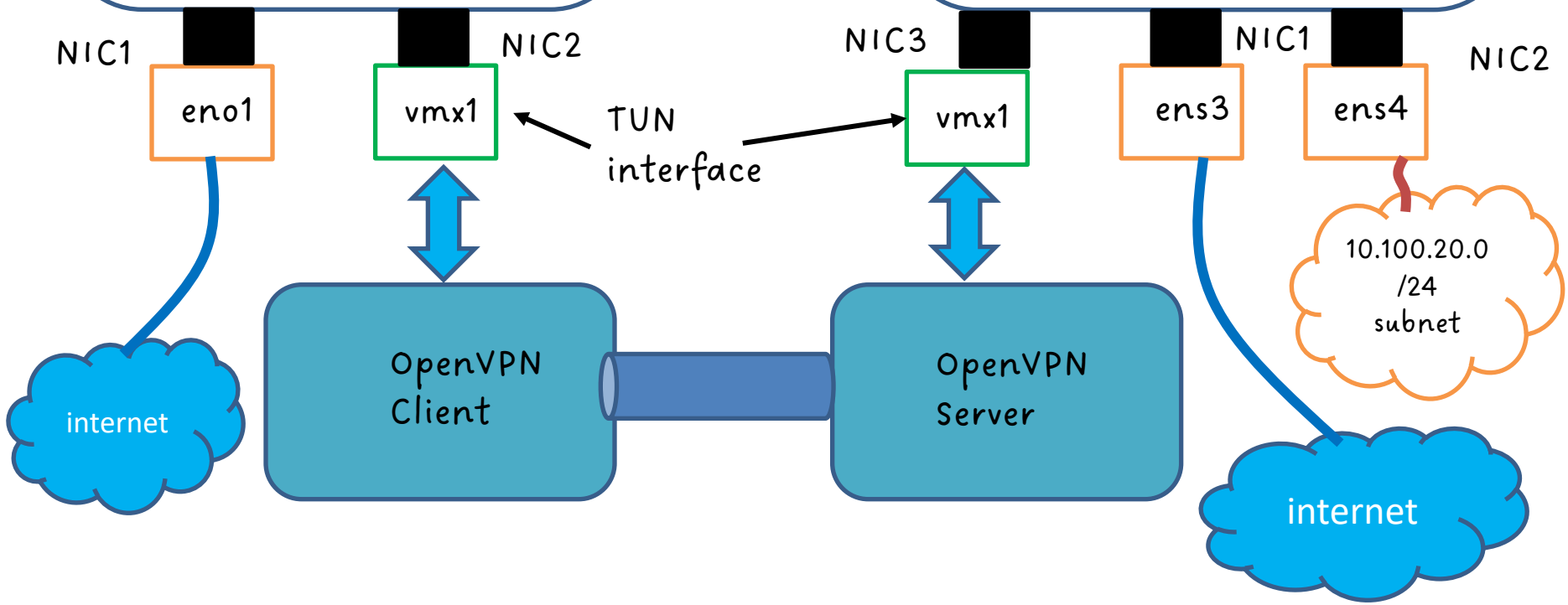
lab gateway

Kernel's routing table

prefix	NIC
192.168.20.0/24	eno1
10.8.0.0/24	vmx1
10.100.20.0/24	vmx1
default	eno1

Kernel's routing table

prefix	NIC
10.100.20.0/24	ens4
10.8.0.0/28	vmx1
default	ens3



สรุป

- ทบทวน IP Address
- ทบทวน Network, LAN
- แนะนำ OpenVPN
- Note: ในปัจจุบัน Network ของ Lab ที่ นศ จะใช้คือ

  Subnet: 172.16.0.0/16

  gateway: 172.16.0.1

Subnet ของ LAN

$offset = 16$

10101100.00001000.00000000.00000011

11111111.11111111.00000000.00000000

- CIDR ของ IP address ข้างบนคือ 171.16.0.3/16
- Subnet Address คือ 172.16.0.0
- IP Address คือ 172.16.0.3
- Netmask คือ 255.255.0.0