



Chapter 1 Network Overview

- Network devices (อุปกรณ์ที่ต่อ internet หรือไม่)
- Network diagrams (รูปที่แสดงภาพทางเครือข่าย เช่น บ้านเรือน)

 - ทำให้เข้าใจโครงสร้างพื้นฐานของเครือข่าย/วิธีการต่อไปนี้
 - + รูปแบบ ① Physical connection port/interface อย่างไร ที่จะต่อไปนี้
 - ② Logical คือ ip

Network protocol - TCP, UDP

- Network addr.
 - IP (logical) L3
 - MAC (Physical) L2
 - Port Number (Service) L4
 - Protocol media
- Components of a network ที่ HH ที่ Network device - end devices ต่อไปนี้

Network Representations



Types of Networks - NH size

- ① small home nw
- ② small office/Home office
- ③ Medium to large Network
 - + LAN → ผู้ดูแลระบบ LAN → ผู้ดูแลนโยบาย网络安全 policy / ร่วมกัน Ex สำนัก ↔ สำนัก
 - + MAN, Wireless LAN, SAN, PAN
- ④ World Wide nw
 - HAN → ผู้ดูแลระบบ
 - Metroplitan
 - Storage
 - Personal

Types of Connection in a LAN

- 1 type (UTP cat 5):
 - ① BH = 100 Mbps
 - ② ยาว 100m (connect hub, repeater, switch)
- 2 type → ① cross → จุดต่อไปนี้เป็นตัวกลาง SW --- hub, pc --- router
- ② HAN connection → จุดต่อไปนี้เป็นตัวกลาง router (female), DCE (command clock rate 56000)

Chapter 2 Basic Router Configuration

Port Address → IANA (Internet Assigned Number Authority)

- 0-1023 : requesting entities "well known ports" destination port
- 1024-49,151 : registered port = published
- 49,152-65535 : dynamic or private port "Randomly generate" source port

Logical Address : IP address (IPv4) ที่ L3

- 5 class A B C D E → reserved (000)
- 96 bit host Multicast Addr. ต้องห้ามซ้ำใน LAN เดียวกัน
- ใช้ .hw / node or com & logical name (domain names) & ip unique

192.168.1 /24 → prefix range

255.255.255.0 → subnet mask

192.168.1.255 → broadcast ip addr.

255.255.255.255 → broadcast NW

Class A: 0	NW	Host	Host	Host	0-127
Class B: 10	NW	Host	Host	Host	128-191
110	NW	Host	Host	Host	192-223
Class C: 1110	NW	Host	Host	Host	224-239 multicast
1111	NW	Host	Host	Host	240-255 experimental
Class E: 1111	NW	Host	Host	Host	

Ex 20: FTP(data), 21:FTP(control), 25: SMTP(Simple mail transfer)
53: DNS(Domain Name Server) [TCP/UDP], 80: WWW(World wide web)
81: Hosts - Name Server.

HTTP

Private addressing → ip. can reuse

→ ต้องห้ามซ้ำใน internet 2 ข้อดังนี้

RFC1918 Internal Addr Range.	CIDR Prefix
10.0.0.0-10.255.255.255	10.0.0.0/8
172.16.0.0-172.16.255.255	172.16.0.0/12
192.168.0.0-192.168.255.255	192.168.0.0/16

Physical Addr.: Mac addr.

- Ethernet: 48bit 7742 = 12 ตัว ค่า 16 → ฟิกเกอร์ 0xXX:XX:XX

- ก่อตั้งโดย IEEE → มีชุด 3 byte (24 bit) code "Organizationally Unique Identifier (OUI)"

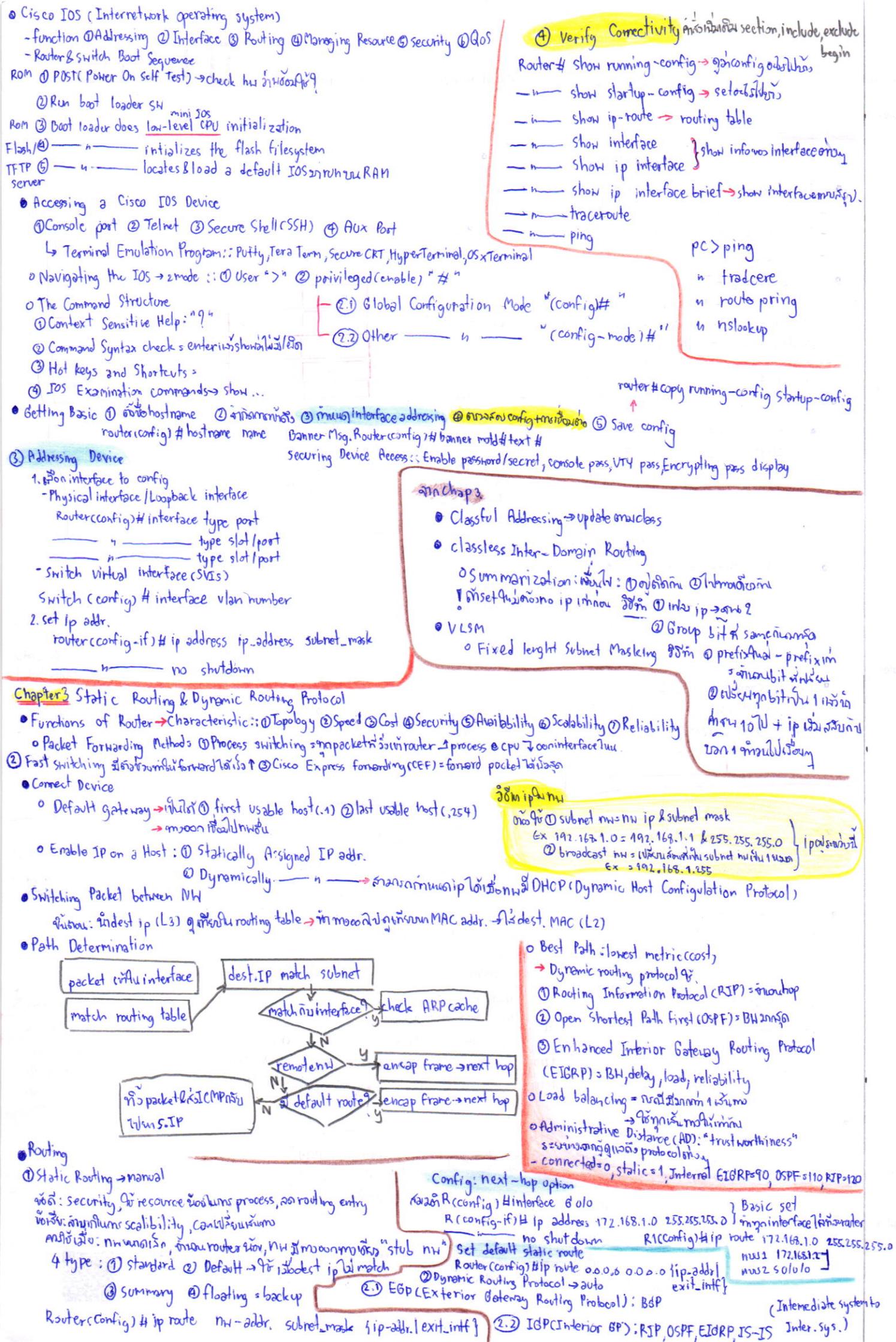
→ 2 ny → 0 ที่ Mac ที่ในชุด NIC ที่ Ethernet device อยู่ → OUI ที่ 3 bytes

② ถ้า Mac ที่ same OUI ต้องมี unique ที่ 3 byte ด้วย

Message delivery

- Unicast → ส่งไปยังผู้รับที่เฉพาะเจาะจงโดยที่ต้องได้รับ
- Broadcast → ส่งไปยังทุกๆ ที่ที่ DHCP, ARP ที่คุณต้องการ → broadcast ip/mask = 255.255.255.255 = FF-FF-FF-FF-FF-FF
- Multicast → ส่งไปยังที่ที่ต้องการ & รับในที่ที่ต้องการที่ service ที่ → ต้องตั้งค่า 01-00-5E-XX-XX-XX







Chapter 4 : Distance Vector Routing Protocol RIP ver 1

• Dynamic Routing Protocol

- fn: share info ระหว่าง router • auto update routing table when topology เปลี่ยน (เมือง) • in best path
- purpose: remote network (networks) • ป้อน info ของ best path (dest. net) • can know best path ของ network ทางเดียว
- component: 1. Algorithm

	Dynamic routing	Vs Static routing
Protocol configuration	* simple (net config)	* command (net config in router)
Require Admin	Advanced (bec. config basic → may trigger config errors)	No admin (link config mode or command)
Topology change	auto	admin config (full)
Scaling	simple & complex (router ที่ far directly ไม่ต้อง config)	use simple topologies
Security	medium	medium
Resource Usage	CPU, mem (in routing info), link bandwidth	No memory
Predictability	Route ↔ current topology	Route → dest. ทางเดียวแน่นอน

• Classifying Routing Protocol

DRP

(within AS) Interior Gateway Protocol (IGP)

(between AS) Exterior Gateway Protocol (EGP)

- Distance vector P.
- vector (distance, direction)
- incomplete view of network topology
- periodic update (timer) (fixed)

- Link-state P.
- Complete net topology (knows all)
- update based on periodic

BGP (Border Gateway Protocol)

- Autonomous System (AS) ผู้ดูแล router แห่งเดียวใน AS ภายใต้ authority (policy or ดูดูแล)

RIP (Routing Info. P.)

IS-IS (Interior Gateway Routing P.)

RIPV2

EIGRP (Enhanced Interior Gateway Routing P.)

OSPF

IS-IS (Intermediate System to Intermediate System)

• 2 Type

1. Classful Routing P. → update each class ที่ 1 subnet mask & routing update
2. Classless Routing P. → ทั้ง subnet mask & routing update

• Convergence: จุดตัดเวลา When routing table ของ all router ต้องมาพร้อมกัน

↳ 2 type: Slower: RIP & IGRP, Faster (fast update when network เปลี่ยน): EIGRP & OSPF

• Routing Protocol Metrics

- Metric: ค่าที่ใช้ในการคำนวณ path ที่ดีที่สุด. NH 0: in best path ที่มี Hop count, Cost, Delay, load, Reliability
- Load balancing: ทั้ง metric มากกว่า 1 ต้องมี metric ใหม่ๆ → ไม่สามารถคำนวณได้ เนื่องจากมี metric ใหม่

• Administrative Distance of a Router (AD) → ต่อไปนี้ Protocol ไหน Routing

- ต้องการ: ค่า AD ที่ต่ำที่สุด ของ metric ที่ใช้ particular config'd route

Route Source	Connected	Static	Internal EIGRP	OSPF	RIP	EIGRP summary route	External BGP	IS-IS	External EIGRP	Internal BGP
AD	0	1	90	110	120	5	20	100	115	170

• Distance Vector Routing Protocol Ex. RIP, IGRP, EIGRP

- Distance Vector Technology ข้อ 2 ที่สำคัญ 1. Vector or direction, ไม่ต้องรู้ distance ทั้งหมด 2. Distance to final dest (cost)

• ข้อเสีย - periodic (always) update, neighbor (เพื่อนบ้าน), broadcast (255.255.255.255) update, 100% routing table all 70% update

• ข้อดี - DV ต้องติดต่อเพื่อนบ้าน 1. Time to convergence → ใช้เวลานาน แต่ steady state ของ routing table ที่ดีที่สุด

2. Scalability (สามารถขยายตัวได้) 3. Resource Usage 4. Implementation & Maintenance

• NW Discovery (ค้นหา) (in basic config now)

→ 3 stage 1. Cold Stage: Router Initial start up

2. Initial Exchange of Routing info. → รับส่ง info ทางเครือข่าย.

3. Exchange of Routing info. → update (จำนวน hop count) routing info.

→ 2nd router ที่ต้องการ info

Network intf Hop

10.2.0.0 solo/0 0

10.3.0.0 solo/0 0

10.1.0.0 solo/0 1

10.4.0.0 solo/0 1

• Routing table Maintenance

- Periodic update: RIP update timer (default 30s), invalid timer (info is lost, default 180), hold down timer (down → hold down ไว้ 180 sec) (default 180), flush (清空) timer (default 240)

• Bounded (bounded) Update: EIGRP → update แค่部分 info

• Triggered Update: → update เวลาใดๆ periodic time

• Random Jitter → กรณี NW ที่เป็น multiple access router บางที (switches) → if info update มากเกินไป

∴ จึงมี Random



- जब standard DV. 1. Routing Loops कीजिए जब intf नीचे down हो तो unrouteable \rightarrow एकीन्ही neighbor कीजिए update (जूँ update)
 - \hookrightarrow हीपरमेट्रिक : ① set max hop = 15 → if hop > 16 → unreachable (जूँही नीचे)
 - ② hold down timer (जूँ intf down \rightarrow hold)
 - ③ split Horizon Rule → जूँही नीचे update कीजिए intf कीजिए update तो $\neg \exists$ intf जूँही hop = 16
 - ④ Route Poisoning → 1. intf down set unreachable 2. unreachable कीजिए poison entry
 - ⑤ ③ with ④ \rightarrow जूँही unreachable जूँही over rule split horizon लागू करें ip intf down (hop = 16)
 - ⑥ IP & TTL (Time to Live) लागू करें \Leftrightarrow update but जूँही when TTL = 0.

	RIP v1	RIP v2	IGRP	EIGRP
speed convergence	slow	slow	fast	fast
scalability - size nw	small	small	small	large
use of VLSM	x	v	x	v
Resource usage	low	low	low	medium
implementation & maintenance	Simple	Simple	Simple	Complex

- RIP Version 1 AD = 120
 - जूँहीजूँही : classful DV • metric = hop count • hop count > 15 unreachable • update broadcast

गोलगोला लागू करेंगे।

- msg of 2 type
 1. Request \rightarrow routing table, \rightarrow intf की config लाइसेंस
 2. Response \rightarrow info, no routing update
- ip addr. लाइसेंस class A, B, C

- Basic RIPV1 Config
 1. in basic config
 2. सेट router rip R1(config) # router rip + नेटवर्क R1(config-router) # network nn ip जूँहीजूँही
- Verification & troubleshooting (जूँहीजूँही) : show running-config or ip route or ip protocols, debug ip rip
 - passive intf command (उपर्युक्त intf को ms) R1(config-router) # passive-interface intf-type(fa/g/s) intf-number (col0, col1, col2)
- Automatic Summarization : RIP Auto Summarizes classful nw \rightarrow 1 जूँहीजूँही size routing table
 - जूँहीजूँही size routing update • single router लाइसेंस in multiple route 1 जूँहीजूँही routing table
 - जूँहीजूँही: doesn't support discontiguous nw (major nw लाइसेंस but 2 minor subnets) \rightarrow 0 जूँहीजूँही load balancing लाइ
 - boundary Routers: summarize RIP subnet from 1 major nw to another
 - Processing RIP update
 - जूँहीजूँही & जूँहीजूँही update [intf] लाइसेंस classful लाइसेंस? \rightarrow y: update subnet nw 172.16.1.0
 - जूँहीजूँही & जूँहीजूँही update [intf] लाइसेंस classful लाइसेंस? \rightarrow N: update classful nw 172.16.0.0
- default route & RIPV1 (जूँहीजूँही) in basic config routing table command (bec. no protocol) \rightarrow 0 जूँहीजूँही default route
 - R1(config) # ip route 0.0.0.0 0.0.0.0 s0/0/1
 - default info originate command \rightarrow 0 जूँहीजूँही update [intf] (पृष्ठा) : static \rightarrow dynamic
 - Router लाइसेंस 2 protocol \rightarrow R1(config-router) # default-information originate

Chapter 5 RIP version 2 & Access Control Lists

RIP v1	VS	RIP v2
classful (जूँहीजूँही subnet mask, जूँहीजूँही support CIDR)		classless (update subnet mask, support variable length Subnet Masking)
not support discontiguous subnet		support Route Summarization
not support VLSM (जूँहीजूँही subnet mask (255.255.255.255))		Prefix Aggregation (जूँहीजूँही authentication routing (जूँहीजूँही discontiguous subnets))
routing update \rightarrow broadcast		Routing update \rightarrow multicast

जूँहीजूँही routing loop
 जूँहीजूँही split horizon or split horizon with poison reverse
 जूँहीजूँही triggered update
 max hop count = 15

- जूँहीजूँही RIP v1
 - जूँहीजूँही virtual interface
 - जूँहीजूँही routing update
 - जूँहीजूँही
 - {
 - loopback intf \rightarrow ping [intf] \rightarrow ip virtual intf \rightarrow reply [intf]
 - Null intf \rightarrow जूँहीजूँही channel लाइसेंस \rightarrow जूँहीजूँही null intf \rightarrow packet discarded \rightarrow timeout
 - Static route & null intf \rightarrow null intf लाइसेंस नहीं मानता तो static route
- R1(config) # ip route summary-static route subnet-mask Null0
 (major-nw) \rightarrow no static supernet route

for Staples

- Route redistribution → config rip & static (ตั้งค่าrip & static ให้เป็น static) ; Router(config-router) # redistribute static
 - Verify & Test Connectivity: show ip interface brief, ping (use !=loopback, =time out), trace route
 - RIPV1: classful, ไม่ต้อง subnet mask, summarize network @ major nw boundaries, if network discontiguous & RIPV1 config convergence ยาก
 - Routing table debug ip rip (content of routing update), กรณี RIPV1 ไม่มี subnet mask จะสัมภารณ์ addr.
 - RIP V2 → show ip protocols
 - Config - Enabling & verify (configuration) RIPV2
 - Config RIP → RIP v1 → can't do V1 & V2 but. ต้องตั้ง V1 → RIP V2 → can't do & ต้องตั้ง V2
 - Auto-Summary & RIPV2 → auto sum route @ major nw boundaries
 - sum route ต้อง subnet mask ไม่ใช่ classful subnet mask
 - disabling Auto-Summary: no auto-summary because network topology ไม่ใช่ discontiguous
 - VLSM & CIDR → verify info. ที่ sent by RIP V2 debug ip rip
 - VLSM → เผื่อนที่ new addr. & subnet mask
 - CIDR → supernetting (= bunch of contiguous classful network into single net)
 - verify show ip route, debug ip rip
 - Access control List = Any user mention → ตรวจสอบ → check [source → dest. หรือไม่?]
 - Packet filtering ① dest, source @ L2 ② protocol no. ③ 192.168.1.1, 192.168.1.2 } → ไม่ว่าจะ permit or block ทั้ง 2
 - Operation → ไม่ระบุ sequence statement
 - last statement ที่ implicit deny → block → discard
 - Standard IPv4 ACLs
 - check source addr.
 - ไม่ permits or denies specific protocol
 - access-list 10 permit 192.168.30.0 0.0.0.255
 - number ACL: 1-99 & 1300-1999
 - Extended IPv4 ACLs
 - VS
 - check source & destination addr.
 - ไม่ permits or denies specific (more) protocol
 - access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80.
 - Number ACL 100-199 & 2000-2699.
 - Wild Card → invert subnet mask
 - 0 = match / fix, 1 = ignore/only 1 bit
 - 255.255.255.255 = match all subnet mask 0 = 0
 - if not specified 255.255.255.255 Pattern or/and กรณี same ว่า wild card & same นั้น
 - in wildcard no subnet = 255.255.255.255 - subnet mask
 - keyword → 0.0.0.0 = match all หรือ host → R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0 host 192.168.10.10 0.0.0.0 255.255.255.255
 - 255.255.255.255 = ignore all หรือ any → R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0 any 0.0.0.0 255.255.255.255
 - Guideline for (3P) → one ACL / protocol > ctrl traffic flow zu intf, ACL ที่ define โน้ต protocol enable on intf
 - ACL creation → one ACL / direction : ctrl traffic in 1 direction at time on an intf, run ACL ctrl in/out bound traffic
 - one ACL / interface = ACL ctrl traffic for an intf, Ex G0/0.
 - Where → Extend ACL: @ close source → standard ACL : @ close destination.
 - Config ACLs → standard
 - number Router(config)# access-list access-list-number
 - deny | permit | remark → comment
 - source [source-wildcard] [log]
 - in intf Router(config-if)# ip access-group {access-list-number | access-list-name} {in|out}
 - to Router(config)# ip access-list [standard | extended] name
 - Verify: show ip interface, show access-lists
 - Securing VTY port → config user permit 192.168.1.10 0.0.0.0
 - Router(config-line)# access-class access-list-number {in[vrf-all] | out}

for Staples

Chapter 7 Basic Switch Address Resolution

► LAN Design → Borderless SW NW design : ไม่มีบอร์เดอร์ - Hierarchical, - Modularity, - Resiliency, - flexibility

□ 2 ระดับ = ① 3-Tier LAN Design 1) Core 2) Distribution 3) Access ② 2-Tier LAN Design 1) Core 2) Distribution 1) Collapsed/Distribution 2) Access

① Core → ผู้ให้บริการ BH ทั่วไป → ต้องมี speed ที่สูงและต่อเน็ตทั่วโลก. } Layers Support, Gig / 10Gig Ethernet } Link aggregation

② Distribution → ผู้ให้บริการ INTERNET & Security Policy / Access Ctrl } Redundant components → สำรองตัวเอง } ให้เกิด BH device มากขึ้น

③ Access → ต่อสู่ end device, Port Security, VLAN [FDDI/Gig Ethernet], Power over Ethernet, Quality of service (QoS)

□ แนวคิดของสถาปัตยกรรม LAN BH & QoS ที่สำคัญ

• ftr & mgmt Server ① Enterprise S. (ฐานข้อมูล) → ตั้งต้น @ [MDF (Main Distribution Facility : Core) → มีเครือข่ายทั่วโลก] ที่สำคัญที่สุด.

② Workshop S. (ห้องเรียน) → ตั้งต้น @ [IDF (Intermediate D. F.: Distribution) → มีเครือข่าย cross-layer access] ที่สำคัญที่สุด

• Collision detection issue (ปัญหาการตรวจสอบชนกัน)

• Segmentation issue (ปัญหาการแบ่ง局域网) → ต้องมีป้องกันการส่งข้อมูลที่ไม่ต้องการ, ที่ไม่ถูกต้อง

• Broadcast domain issue → ทุก LAN ต้องมี broadcast in MAC addr. ∵ broadcast NWP ที่ไม่ต้องการ

□ Segmentation ผ่าน process split single collision domain → smaller collision domain ลดลง collision บน LAN segment : L# 2 device หรือ bridge, SW

□ Broadcast domain รับในตัวบุญ port but, router (L4) ไม่รับ filter/segment broadcast ที่ผ่านมาต้องตัดออก

► SW Environmental

□ SW Operation ① Learning : ข้อมูล frame ใน SW จะบันทึก Source MAC addr. ตาม Port และ reset aging

② Aging : ของ MAC addr. → ไม่ต้อง → ไม่ต้อง

→ non dest. Table

③ Flooding : ข้อมูล frame ไม่สามารถ找到 dest. When frame คือ 1) broadcast, 2) multicast, 3) unknown unicast

④ Forwarding : 送到 dest. (มีผลลัพธ์)

⑤ Filtering : if ไม่ได้ frame ที่ dest. import ที่ไม่ใช่ dest. & source & dest. 2 interface) ⇒ ไม่ต้อง filter

for Staples

□ SW Methods : ① Store & Forward SW → check CRC header → ถ้าผิด → 丢弃 ; ถ้าถูก, auto buffer

② Cut-Through SW → check CRC header (dest, source & size of byte 16ms), No FCS & auto buffer

↳ 2 mode : ① fast-forward ~ 12 byte ② Fragment-free ~ 64 byte : < 64 byte → 丢弃 → ไม่ถูก

□ SW Domains : ① Collision Domains → domain ที่ต้องการต่อสื่อมสารกันต้องมี "QoS" ที่ต้องมี

② Broadcast ~ → domain ที่ broadcast → อยู่ domain ใดก็ตามที่ต้อง "QoS" ที่ต้องมี

↳ manage intf; # config 1 # interface VLAN num | default gateway; # config 1 # ip address ip subnet | same of scanning # ip subnet

► Basic SW Concept & Configuration

□ Basic SW Config : SW Boot Sequence = Same router router (scanning) & no shutdown

→ Verify Port Config • Preparing of Basic SW Management : SW ต้องloopback ∵ interface SVI (SW virtual interface) → VLAN

show int f0/0, startup-config • Config SW Port → Duplex Communication : ① Full ② Half (SW ต้องต่อตัวกันเป็นตัวต่อตัว)

running-config / flash / version (intf intf → s(config-if) # duplex full → s(config-if) # speed 100 (Niche speed))

/history, ip f0/0, /mac-address-table → Auto - MDIX : ปลั๊ก SW ต้องต่อ cross-over แต่ต้องต่อตัวกันเป็นตัวต่อตัว

↳ intf intf → s(config-if) # duplex auto → s(config-if) # speed auto → s(config-if) # mdix auto

□ SW Security : Security Remote Access → ssh (secure shell) TCP port 22, telnet : TCP port 23

Config : S - C (config) # ip domain-name to → # crypto key generate rsa → # username admin pass cisco → line vty 0 15

→ -line) # transport input ssh → -line) # login local [Verify SSH : show ip ssh, show ssh]

□ SW Port Security → กำหนด policy กำหนด MAC address, limit 1000 ต่อ 1 ตัวแล้ว

s(config-if) # switchport mode access → # switchport port-security → เริ่มต้น 1 ตัวแล้ว.

Secure MAC addr. → ① static : s(config-if) # switchport port-security mac-address MAC-ADD

② dynamic : s(config-if) # switchport port-security mac-address sticky → learn from neighbor → record to

maximum MAC : # switchport port-security maximum MAX

Violation mode : ① protect : security violation protect mode

② restrict : security violation restrict mode → จำกัดการเข้าสู่เมืองต่อไป

③ shutdown : security violation shutdown mode → default

[Verify : show port security int fa0/0, show port-security address]

□ Addr. Resolution Protocol (ARP) : ARP Cache, IP/MAC addr. & Map ที่เก็บ MAC gateway (if 1 ตัวต่อตัว ก็จะ MAC gateway)

IPV4: Classless [site Pt-2] : - Variable length Subnet Masking (VLSM) : ระบุขนาดที่ต้องการ : ต้องต่อตัวกันเป็นตัวต่อตัว

- fixed ~ : ระบุขนาดที่ต้องการ



Chapter 8 LAN Redundancy & Spanning Tree Protocol (STP)

- Issue with Layer 1 Redundancy ① Mac addr. instability → Mac addr. table will keep being updated.
- Broadcast storms → ② unknown unicast → multiple frame transmission → start: unknown unicast → includes lots of network frames but source is 1 frame
- STP → prevents: unblock port → block port → ③ no loops traffic in network
- Priority: ① in Root Bridge = low priority min Rule: ④ 1 RB / 1 mw ⑤ 1 RP / 1 RB ⑥ 1 DP / segment
q in BPDU ⑦ in path cost all ⑧ in Root port → path cost min → designated best port
Bridge protocol data unit ⑨ in segment in path cost min → q BID min if the designated port is the best block port
Low RB & Source (802.1D)

- Config: ⑩ I: s1(config) # spanning-tree VLAN 1 root primary ⑪ II: s2(config) # spanning-tree VLAN 1 priority 24576
(if s1, s2) ⑫ S2(config) # spanning-tree VLAN 1 root secondary [Verify: show spanning-tree] 6 byte (IEEE 802.1D)
- Inn Extended System ID: B. priority → B. priority (per VLAN) + Extended Sys ID (VLAN) + MAC addr, ∴ BID=8 byte
 - PVST+ (IEEE 802.1D STP) → ⑬ load balancing based on root / VLAN → [Verify: show spanning-tree active]
 - Rapid PVST+ → in Alternate port (2 bits block bit) → spanning tree port fast
 - max reset Edge port @ port like host, router: -if # spanning tree port fast
 - Link type: port-to-point or point-to-point
 - if # spanning tree bpdu guard enable → port block by bpdu guard
 - Config: s1(config) # spanning-tree mode rapid-pst → # int ip-to-p → H spanning-tree link-type point-to-point

Chapter 9 VLANs & Inter VLAN

- VLAN = in partition VLAN: either in one broadcast domain or broadcast domain in layer 2 like switches (with VLAN interface)
- Mode: - security mode, - access, VLAN ID, - broadcast domain ID, - VLAN name. [Verify: show vlan brief]
- In a multi-SW Environment
 - VLAN-Trunk → Config: int <--> if # switchport mode trunk [Verify: show int folo switchport]
 - ↳ set in int to native mode VLAN → can carry more than 1 VLAN
 - Tagging Ethernet Frames (IEEE 802.1Q): Ethernet Frame →

Dest MAC	Src MAC	Tag	Type/Length	Data	FCS
----------	---------	-----	-------------	------	-----

 → Tag information in LAN header
- Assignment: VLAN number → 1-1005 (in config @ VLAN.dat (flash))
 - ↳ s(config) # vlan vlan-number → VLAN number to name
 - 1006-4096 (in config @ running-config (in NVRAM))
 - ↳ s(config) # vlan database → VLAN number name if no name: no vlan num
- Assign port to VLAN: int <--> if # switchport mode access → # switchport access vlan num (if no num: no num)
 - Verify: show vlan name if, show vlan summary, show int vlan num
- Inter-VLAN Routing → Router set int trunk. Then formula "Sub interface"
 - Config: ① set basic routing (set ip address, no shutdown)
② R(config) # interface g0/0.① → VLAN → subif # encapsulation dot1Q → ip address ip subnet-mask [Verify: show vlan, show ip route, show running config]

Chapter 10 VTP (VLAN Trunking Protocol) → Manage VLAN & NAT (NW addr. Translation)

- VTP (msg: ISL or IEEE 802.1Q) → manages VTP domains
- Operation: msg update VTP revision number 32bit (0-4294927295) (Working)
 - ↳ 3 mode ① server → config, remove, rename VLAN in its domain. ② Client → receives VTP process, sends VTP msg to its trunk.
 - ③ Transparent - config, remove, rename VLAN in its domain, transparent
- Config: ① in global conf. ② in VLAN conf. ③ in trunk ④ in domain ⑤ in 3 mode
 - ① in global conf. s(config) # vtp version 2 → # vtp domain id → # vtp password pass → # vtp mode server/client
 - ② in VLAN conf. s(vlan) # vtp v2-mode [Verify: show vtp status/counters] → # vtp server/client/transparent
 - ③ Pruning → manage traffic in trunk intf → Config in intf only to remove VLAN traffic.
s(vlan) # vtp pruning → in intf → s(config-if) # switchport trunk pruning VLAN remove VLAN-num

DNAT → in local private ip to publish real ip

- Terminology: 4 types ① Inside local Addr. (private ip) ② outside local Addr.
 - ③ Inside global Addr. ④ Outside global Addr. → same ip.
- Type
 - ① static mapping [Map 1w1] → ② R(config) # ip nat inside source static local-ip global-ip | prefix length
 - ② Dynamic [ip pool] vs Global / Real ip [Map: many ↔ 1]: real mac address (1:1) # ip nat pool to start-ip end-ip netmask network
 - ③ PAT (Port Address Translation) → port map in NW add [Map: many ↔ 1] ④ set ACL

http://paperkit.net (1.3) ip nat source list ACL-num pool to overload

(PAT is dynamic)