ชื่อ-สกุล นาย อมาเดช ขมฤทธิ์มิตร กระดาษแผ่นที่ 1 รหัสนักศึกษา 59000591

for Staples

Chapter 1 Network Overview

- Network diagrams = โครงสร้าง nw ที่เราดูแลมีการเชื่อมต่ออย่างไร?
  - 2type ∴ ① Physical → บอกว่า port / interface ไหน เชื่อมต่อกันอย่างไร @ ตำแหน่ง (เน้นnw) ② Logical → บอก ip
- Network protocol → TCP/UDP, FTP, ARP, SMTP, POP3, IMAP, ICMP (internet control message protocol) → ping เป็นใน comm (mail, email)
  (File Transfer protocol) → รับ-ส่ง file ระหว่าง client กับ sever (Addr Resolution Protocol) → map ระหว่าง IP Addr กับ MAC Addr เป็นไป
  - NW Addr ∴ ① IP Addr. (Logical addr) @L3 ② MAC Addr (Physical Addr) @L2 protocol α ตาม media ③ Port Number (service Addr) @L4
- Components of Networks → HW → NW device มี 3 type
  ① end devices = ที่นั่งจากมันเป็นคน
  ② intermediary devices = อยู่ระหว่างอุปกรณ์ เช่น NW access devices, Internetworking devices, security devices (nw representation: hub, switch, router)
  - hub repeater @L1 → ส่งพร้อมกันเกิด collision ∴ ใช้ CSMA / CD (Carrier Sense Mutiple) when เจอ collision ก็หยุดส่ง
  - switch, bridges @L2 → Learning / flooding / filtering / Forwarding / Aging
  - Router @L3 → Routing
  ③ network media = สื่อกลาง เช่น copper, fibre optic, wireless LAN — straight, cross wan Z
- Types of Networks → sw → ① switch เลือกทางออก ② Router เลือกไปทางดีที่สุด
  → size → ① small home nw → วงใช้งานด้านนอกอย่างเดียว ② small office/home office → config จากด้านนอกมาด้านใน ③ Medium to Large NW → มีการต่อต่อภายใน 100–1000 เครื่อง ④ world wide Nw เช่น internet
  → infrastructure ทั่วไป ① Local Area NW (LAN) → มีกลุ่ม admin ดูแล policy / nw ต่าง ๆ ② Wide Area NW (WAN) → มีหลายกลุ่ม Admin Ex สาขา ↔ สำนักงาน
  อื่นๆ ∴ Metropolitan Area NW (MAN), wireless LAN (WLAN), storage Area NW (SAN), Personal Area NW (PAN)
- Reliable Network ① fault Tolerance → ทนต่อความผิดพลาด ② Scalability → สามารถปรับเปลี่ยนขนาดได้ โดยไม่ส่งผลต่อ user เดิม ③ Security → จำกัด or limit การเข้าถึง ④ Quality of Service (Qos) → แต่ละ services จะมี quality ไม่เท่ากัน
- layer with TCP/IP & OSI model

PDU: Protocol data Unit		OSI model	TCP Model
data	⑦	Application	Application
	⑥	Presentation	
	⑤	session	
segment	④	Transport	Transport
Packet	③	Nw	Internet
Frame	②	Data link	Nw Access
Bits	①	Physical	

- Type of Connection in a LAN
  ข้อจำกัด (UTP cat 5) : ① Bw = 100 Mps ② ยาว 100 m (can ต่อ hup reapeater, switch)
  2type : ① ตรง ② cross → ต่ออุปกรณ์ same ยกเว้น sw --- hub, pc --- router
  WAN Connection เชื่อมระหว่าง Router
  ↳ 2 ฝั่ง → DCE (female) → พิม command clock rate 56000
  ↳ DTE (male)
  สาย console (Rollover Cable) → router ---- pc

Chapter 2 Basic Router Configuration

- Port Address @L4 : กำหนดโดย (Internet Assigned Number Anthority : IANA)
  0–1023 : requesting entities "well known ports" destination port
  1024–49151 : registered port = publish ให้คนใช้
  49152–65535 : dynamic or private port "Random generate" source port
  Ex. 20 : FTP (data), 21 : FTP control, 25 : SMTP (simple mail transfer), 53 : DNS (domain name server) TCP/UDP, 80 www
- Logical Address IP address (IPv4) @L3
  - 5 class ∴ ABCDE → reserved (ของ) แตกต่างที่จำนวน max ของ workstation required
    ใช้กับ host → multicast Addr → ส่งไปให้ทุกเครื่องในวง LAN เดียวกัน
  - แต่ละ NW / node or com → มี logical name (domain name) & ip unique

class							
A	0	nw	host	host	host	24 bit	0–127
B	10	nw	nw	host	host	16 bit	128–191
C	110				host	8 bit	192–223
D	1110						224–239 multicast
E	1111						240–255 experimental

Private Addressing → ip com เรา ใช้ภายในได้ – ช่วยให้ can ใช้งาน internet ได้มากๆ

class	RFC 1918 internal Addr Range	CIDR Prefix
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.16.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

- Physical Address : MAC Address
  - Ethernet : 48 bit ฐาน 2 = 12 ตัว ฐาน 16 → เขียนแบบ 0x ฐาน 16
  - ตัวควบคุม IEEE → กำหนด 3 byte (24 bit) code "organizationally Unique Identifier (OUI)"
    → 2 กฎ ① ทุก MAC ที่กำหนดให้ NIC หรือ Ethernet device อื่นๆ → ใช้ OUI ที่ 3 byte แรก ② ทุก MAC ที่ same OUI ต้องกำหนด unique ที่ 3 byte สุดท้าย
- message Delivery
  - unicast → ส่งโดยตรง NW เดียวกัน
  - Broadcast → ส่งหาทุกเครื่อง NW เดียวกัน
  - Multicast → ส่งหาหลายเครื่อง ที่เปิด service ไว้
- Cisco IOS (Internetwork operating system)
  - function ① Addressing ② interface ③ Routing ④ Managing Resouce ⑤ security ⑥ Qos
  - Router & Switch Boot sequence
    ROM ① Post (Power on self test) เช็ค HW พร้อมมั้ย
    ② Run Boot loader sw
    ROM ③ Boot loader does low-level CPU initialization
    Flash ④ intialize the flash file system

TFTP servers ⑤ —— locates & load a default IOS

- Accessing a Cisco IOS Devise

① Console port ② Telnet ③ Secure shell (SSH) ④ Aux Port

- Navigating the IOS → 2 mode ∴ ① user ">" ② privileged (enable) "#"
  - 2.1 Global configuration Mode "(config)#"
  - 2.2 Other " "(config-mode)#"

- The Command Structure

① context sensitive Help : "?"
② Command Syntax Check = enter หลัง show ว่าได้ หรือ ผิด
③ Hot Keys and Short cuts
④ IOS Examination Command → show....

router# copy running-config startup-config

- Getting Basic ① ตั้งชื่อ host name ② กำหนดรหัสผ่าน ③ กำหนด interface addressing ④ ตรวจสอบ config + ทดสอบการเชื่อมต่อ ⑤ save config

router(config)# hostname
- Banner msg. Router(Config)# banner motd text
- Securing Device Access ∴ Enable password / secrect, console pass, VTY pass

③ Addressing Devices

1) เลือก interface to config
- Physical interface / loopback interface
  Router(config)# interface type port
  ──────────── type slot/port
  ──────────── type slot/subslot/port
- switch virtual interface (SVIs)
  switch config)# interface vlan number

2) set ip addr.
router config-if)# ip address ip-address subnet-mask
──────────── no shutdown

Chapter 3 Static Routing & Dynamic Routing Protocol

- function of Router → Characteristic ∴ ① topology ② Speed ③ Cost ④ Security ⑤ Availability ⑥ scalability ⑦ Reliability
- Packet forwarding Methods ① Process Switching = ทุก packet ที่วิ่งเข้า Router ไป process ด้วย cpu ไป ออก interface ไหน?
② fast switching ส่งต่อข้อมูลที่ให้ forward ได้เร็วขึ้น ③ Cisco Express forwarding (CEF) - forward packet ได้เร็วสุด
- Connect Devices
  - Default gateway → เป็นได้ ① first usable host (.1) ② last usable host (.254)
    → ทางออกเชื่อมไป nw อื่น
  - Enable IP on a Host ① statically Assigned IP addr.
    ② Dynamically ──────── → com กำหนด ip ได้ when nw มี DHCP (Dynamic Host Config Protocol)
- Switching Packet between NW
ขั้นตอน ∴ หา dest ip (L#3) → ดูเทียบใน routing table → หาทางออกไปดูเทียบหา MAC Addr → ใส่ dest MAC (L#2)
- Path Determination

packet เข้ามา interface → match routing table → dest. IP match subnet → match กับ interface? —Y→ Check ARP cache; N → remote nw? —Y→ encap frame → next hop; N → มี default route มั้ย —Y→ encap frame → next hop; N → ทิ้ง packet & ส่ง ICMP กลับบอก . IP

- Best Path : lowest metric (cost)
→ Dynamic routing protocol ที่ใช้
① Routing Information Protocol (RIP) - นับ hop
② Open shortest Path first (OSPF) BW มากน้อย
③ Enhanced Interior Gateway Routing Protocol (EIGRP) = BW, delay, load, reliability
- Load balancing กรณีมี > 1 เส้นทาง
- Administrative Distance (AD) "trustworthiness" → ใช้ทุกเส้นทางที่มี เท่ากัน (ค่าความน่าเชื่อถือ)
  - ระยะห่างจากผู้ดูแลตัว protocol ต่างๆ
  → connected = 0, static = 1, Internal EIGRP = 90, OSPF = 110, RIP = 120

- The Routing Table

D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0

ได้มาจาก ... exit

- Routing

① static Routing → manual
ข้อดี : security, ใช้ resource น้อยในการ process, ลด routing entry
ข้อเสีย : ขยายไม่ได้ scalability, config ผิดพลาดง่าย
ควรใช้ when : nw ขนาดเล็ก มี. router น้อย, nw มีทางออกทางเดียว "stub nw"
4 type : ① standard ② Default = ใช้ when dest ip ไม่ match
③ Summary ④ floating = backup
Router (config)# ip route nw-addr. subnet-mask {ip-addr | exit-intf}

config : next-hop option
ตัวอย่าง R(config)# ~~ip route 0.0.0.0 0.0.0.0 {ip-addr | exit-intf}~~
────-if)# ip address 172.16.1.0 255.255.255.0 — Basic set กำหนด interface ให้ Router
no shutdown
R1 (config)# ip route 172.16.1.0 255.255.255.0 → 172.16.1.2 · แบบ 1 / S0/0/0 แบบ 2

set default static route
Router (config)# ip route 0.0.0.0 0.0.0.0 {ip-addr | exit-intf}

- Classful Addressing → update ตาม class
- Classless Inter-Domain Routing
  - summarization เงื่อนไข : ① ต่อเนื่องกัน ② ไปทางเดียวกัน
  ถ้า set ไม่ระวัง ตรวจ ip เก่าก่อน วิธีทำ ① แปลง ip → ฐาน 2
  ② Group bit ที่ same กัน
- VLSM
- Fixed length Subnet Masking
วิธีทำ ① Prefix ใหม่ - Prefix เก่า = จน. bit เปลี่ยน
② เปลี่ยนจาก bit ที่เป็น 1 หลังสุดเป็นฐาน 10 ได้ + ip เริ่มต้นบวกกับ +1 ทำไปเรื่อยๆ

② Dynamic Routing Protocol → auto
- 2.1 EGP (Exterior Gateway Routing Protocol) BGP
- 2.2 IGP (Interior ──────────) RIP, OSPF EIGRP, IS-IS
  - intermediate system to intermediate system

ชื่อ-สกุล นาย อมรเดช บุญฤทธิ์มิตร กระดาษแผ่นที่ 2 รหัสนักศึกษา 59011611

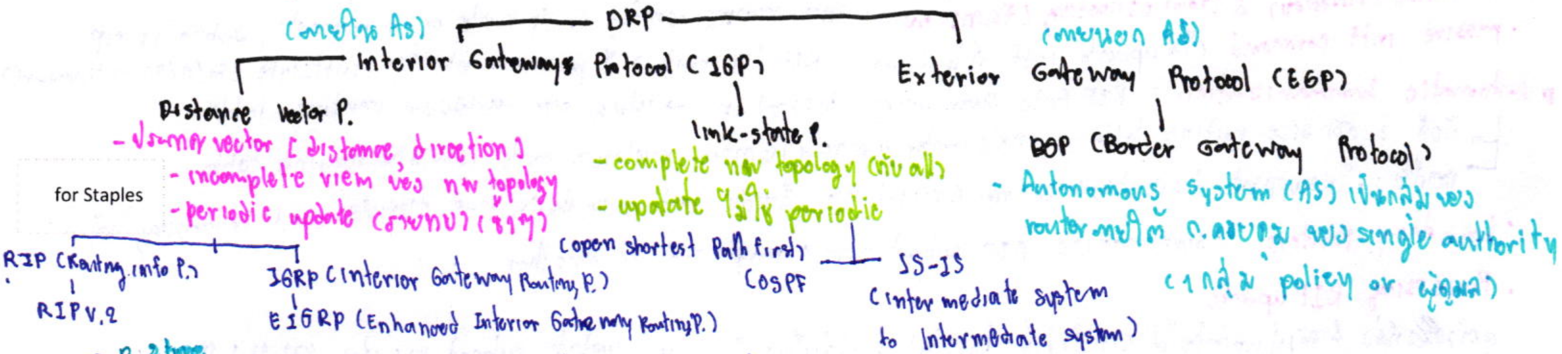
for Staples

Chapter 4 Distance Vector Routing Protocol RIP ver 1

- Dynamic Routing Protocol
  - f : share info ระหว่าง router • auto update routing table when topology เปลี่ยน (เมื่อมีปัญหา) • หา best path
  - purpose : หา remote nw (nw ใกล้เคียง) • ปรับปรุง routing info • เลือก best path ไป dest. nw can หา new best path ถ้า path ไม่ว่าง
  - component : ① Algorithm : ใช้เพื่อคำนวณ routing & best Path
    ② Routing protocol msg : สำหรับหา neighbor & แลกเปลี่ยน routing info (best path)

	Dynamic routing	vs Static routing
ความยุ่งยากในการ config	∝ ขนาด nw (same เดิม)	∝ ขนาด nw (เพิ่ม command ทุก router)
Required ความรู้ admin	Advanced (bcc. config basic → nw ใหม่ + ข้อมูลต่างมีเพิ่ม)	No เพิ่มเติม (กำหนดเส้นทางเอง ใช้ command)
Topology change	ปรับ auto	admin config ใหม่ all
Scaling	เหมาะ sample & complex (router ที่ไม่ได้ directly ไม่เท่า)	เหมาะ simple topologies
Security	น้อยกว่า	มากกว่า
Resource usage	ใช้ cpu, mem (เก็บ routing info), link bandwith	No เพิ่มเติม
Predictability	Route ตาม current topology	Route → dest. ทางเดิมตลอด

- Classifying Routing Protocols



- 2 type
  ① Classful routing P. → update ตาม class ไม่ส่ง subnet mask ใน routing update
  ② classless ——— → ส่ง subnet mask ใน routing update
- convergence : กำหนด when routing table ของ all router มีสถานะคงที่ไม่เปลี่ยนแปลง)
  ↳ 2 type : slower : RIP & IGRP , faster (มีการ update when เกิดการเปลี่ยนแปลงดี >) : EIGP & OSPF

- Routing Protocol Metrics
  - Metric : ค่าที่ใช้ในการเลือก (หาทางไป dest. nw จะเลือก best path ไหน เช่น Hop count, Bw, cost, Delay, load, Reliability)
  - Load balancing : nw มีเส้นทาง >1 ที่มี metric เท่ากัน → เฉลี่ยให้การใช้งานแต่ละเส้นทางเท่าๆ กัน

- Administrative Distance of a Router (AD) → ใช้เลือก protocol ในการ routing
  - วัตถุประสงค์ : ค่าตัวเลขที่เจาะจงลักษณะพิเศษของ particular (เฉพาะ) route

Route source	Connected	Static	Internal EIGRP	OSPF	RIP	EIGRP summary route	External BGP	IGRP	IS-IS	External EIGRP	Internal BGP
AD	0	1	90	110	120	5	20	10	115	170	200

- Distance Vector Routing Protocol Ex. RIP, IGRP, EIGRP
  - Distance vector Technology ต้องรู้ 2 สิ่งมาใช้ตัด ① Vector or direction, การแลกเปลี่ยนควรดูคอบคลุม ② Distance to final dest (cost)
  - ลักษณะทั่วไป : periodic (ครบรอบเช่นเดิม) update, neighbor (ตัวใกล้เคียง), broad cost (255.255.255.255) update, เอา routing table all update
  - ——— ของ Routing Protocol : เกณฑ์ที่ใช้ check ว่า DV ดีไหมดี? ① Time to convergence → เวลาที่เข้า steady state ของ routing table ที่เกิดการเปลี่ยนแปลงแล้ว ② scalability ขยายมากสุดเท่าไร ③ Resource usage ④ Implementation & maintenance

- network Discovery (ค้นพบ) (ทำ basic config ก่อน)
  มี 3 state ① Cold State : Router Initial start up
  ② Initial Exchange of Routing info → ทำการแลกเปลี่ยน
  ③ Exchange of Routing info → update (เพิ่ม hop count) routing info
  → บอก Router อีกตัวว่าห่างเท่าไร

for Staples

- Routing Table Maintenance
  - Periodic update : RIP update timer (default 30s), Invalid timer (info เริ่ม lost) (default 180)
  Holddown timer (ถ้า down → hold ไว้ไม่ว่า up หรือไม่) (default 180), flush (ทิ้ง) timer (default 200)

- Bounded (ขอบเขต) Update : EIGRP → update แค่ที่เปลี่ยน
- Triggered Update → update เลยไม่รอ periodic time
- Random Jitter → ใช้ใน nw ที่เป็น multiple acess router หลายตัวเชื่อมต่อกัน → if เกิด update พร้อมกันทุกครั้ง ∴ จึงใช้ Random

▶ ปัญหา standard DV. ① Routing Loops เกิดwhen intf ใน down แล้วถูกลบออกจาก table → ค่าเก่าใน neighbor ส่งกลับมา update (จน update hop เพิ่ม)
└ แก้ปัญหา ① set max hop = 15 → if hop = 16 → unreachable (ส่ง down ไปแล้ว)
② holddown timer (ถ้า intf down → hold)
③ split Horizon Rule → ไม่ส่งข้อมูล update กลับไปทาง intf ที่ได้รับ update มา, ใช้ intf นั้น hop = 16
④ Route Poisoning → ① เกิด down set unreachable ② ส่ง unreachable ที่เป็น posion ออกไป
⑤ ③ with ④ → ถ้าเกิด unreachable → over rule split horizon โดยส่ง ip intf ที่ down (hop = 16)
⑥ IP & TTL (Time to Live) เกิดการ update but จะหยุด when TTL = 0

	RIPv1	RIPv2	IGRP	EIGRP
speed convergence	slow	slow	slow	fast
scalability - size nw	small	small	small	Large
use of VLSM	x	✓	x	✓
Resource usage	Low	Low	Low	Medium
implementations & maintanance	simple	simple	simple	complex

▶ RIP version 1 AD = 120
- คุณสมบัติ : classful, DV = metric = hop count • hop count > 15 unreachable • update broadcast ทุก 30s
- msg มี 2 type ① Request → ~~ขอ routing table~~ → ส่ง routing table → ไป intf ที่ config ไว้เพื่อรอรับการ update
② Responce → ส่ง info ของ routing table
- ip addr. แบ่งตาม class A, B, C
- Basic RIPv1 config ① ทำ basic config ② สั่ง router rip R1 (config) # router rip
+ ต่อด้วย nw R1 (config) # network nw ip ที่ต้องการรู้จัก
- verification (การตรวจสอบ) & troubleshooting (จัดการปัญหา) : show running-config or ip route or ip protocols, debug ip rip
  - passive intf command (ไม่ update intf ที่ไม่ต่อออก) R(config-router) # passive-interface intf_type (fa0/0/s) intf_number (0,
- Automatic summarization : RIP Auto summarizes classful nw → เพื่อลด size ~~จาก~~ routing table
└ ข้อดี : ลด size routing table • single router แทนกลุ่มที่มาจาก multiple route เยอะมากใน routing table
└ ข้อเสีย : - ไม่ support discontiguous nw (major nw เดียวกัน but ไม่อยู่ติดกัน) → อาจจะเกิด load balancing ได้
  - boundary Routers : summarize RIP subnet from 1 major nw to another
  - Processing RIP update
  ดูตัวที่ส่ง & ตัวที่ update ไป (intf) ว่ามี classful เดียวกันไหม ? → Y : update subnet nw เช่น 172.16.1.0
  └ N : update classful เช่น 172.16.0.0
- default route & RIPv1 ถ้าไม่เจอทางออกใน routing table (อาจ bec. ต่าง Protocol) → ออก default route
  R (config) # ip route 0.0.0.0 0.0.0.0 s0/0/1
  default info. originate command → เพื่อ update ไปใน rip ว่าเชื่อม : static → dynamic
  Router ที่อยู่ระหว่าง 2 protocol ← R(config-router) # default-information originate

Chapter 5 RIP version 2 & Access Control Lists

RIPv1	vs RIPv2
classful (ไม่ส่ง subnet mask), ไม่ support CIDR	Classless (update subnet mask, support Variable Length Subnet Masking (VLSM), support Route summarization (Prefix Aggregation)
not support discontiguous subnet	update next hop addr.
not support VLSM bec. ไม่ส่ง subnet mask (255.255.255.255)	ใช้ authentication routing (รองรับ discontiguous ขาวกอล)
routing update → broadcast	Routing update → multicast

ใช้ timer ป้องกัน routing loop
ใช้ split horizon or split horizon with posion reverse
ใช้ triggered update
max hop count = 15

- ข้อจำกัดของ RIPv1
เป็น virtual interface สามารถเพิ่มใน routing ได้ แต่ update ออกไปได้
- Loopback intf → Ping ไป → ip virtual intf → reply ได้
- Null intf → ใช้ตัดคนที่จะมาทาง chanel ที่เราไม่ต้องการ → วิ่งออก null intf → packet discard เอง → time out
- static route & null intf → null intf จะเป็นตัวที่เป็นทางออกของ static route
  R (config) # ip route summary-static-route subnet-mask Null0
  (major-nw) → ของ static supernet route

ชื่อ-สกุล นาย สมภพ บุญทำมิตร กระดาษแผ่นที่ 3 รหัสนักศึกษา [redacted]

• Route redistribution (ขัดตรง) → อยากให้ rip รู้จัก static ตัวที่เพิ่มใหม่โดย rip ส่ง static ไปด้วย : R(config-router)# redistribute static

• Verify & Test Connectivity : Show ip interface brief , ping (ผล : ! = ได้ U = ไม่ได้ . = timeout , trace route

• RIPv1 : Classfull, ไม่ส่ง subnet mask, summarize nw @ major nw boundaries, if nw เป็น discountiguous & RIPv1 config convergence จะมาไม่ถึง

• ตรวจ Routing table debug ip rip (content of routing update, ถ้าเป็น RIPv1 จะไม่ใส่ subnet mask รวมใน nw addr.

▶ RIPv2

■ config
- Enabling & verify (ตรวจสอบ) RIPv2 → show ip protocols
- Config RIP → RIPv1 → can รับได้ทั้ง v1 & v2 but ส่งได้แค่ v1
  → RIPv2 → can รับได้ & ส่ง แค่ v2
- Auto-Summary & RIPv2 → auto sum route @ major nw boundaries
  → sum route ด้วย subnet mask ที่น้อยกว่า classful subnet mask
- disabling Auto-Summary : no auto-summary bec. when ใน nw topology ต้องเป็น discontiguous

RIPv2 Route Entry:

0	7 8	15 16	23 24	31
Command = 1 or 2	version = 2	Must be zero		
Address family identifier			Route tag	
Subnet Mask				
Next hop				
Metric (Hops)				

Multiple Route Entries, up to a maximum of 25

■ VLSM & CIDR → verify info ที่ sent by RIPv2 debug ip rip
  → VLSM → เผยแพร่ nw addr. & subnet mask
  → CIDR → ใช้ supernetting (= bunch ของ contiguous classful nw ที่เป็น addr. เหมือน single nw)
  → verify show ip route , debug ip rip

▶ Access control List = ควบคุมทางเข้าออก → ตรวจสอบ → check → source → dest ผ่านไหม ?
  → อย่าก Conversation → ทำอย่างนั้น (เช่น FTP) ผ่านไหม ?

■ Packet filtering : ① dest, source @L2 ② protocol ที่ใช้ ③ ไปทาง nw ไหน, ที่ไร } → ทำตรวจนี้ให้ผ่าน or block ไว้ ?

■ Operation → ทำงานเป็น sequence statement
  → Last statement เป็น implicit deny → block → discard

■ Standard IPv4 ACLs vs Extendend IPv4 ACLs

Standard:
- check sourse addr.
- ปกติ permits or denines ทั้งชุด protocol
access-list 10 permit 192.168.30.0 0.0.0.255
- number ACL : 1-99 & 1300-1999

Extendend:
- Check sourse & destination addr.
- ปกติ permits or denines specific (เฉพาะ) protocol
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
- Number ACL 100-199 & 2000-2699

■ wildcard → invert ของ subnet mask
  → 0 = match / fix , 1 = ignore / อะไรก็ได้
  → วิธีหา จาก set ของ ip (match range) ① นำความสัมพันธ์ 1 bit ที่ซ้ำกันใส่ wildcard mask ตำแหน่งนั้น = 0
  ② bit ที่เหลือใส่ 1
  if กรณีคิดไม่ได้ ลองหา Pattern or / and ผ่านคิด ดูท้าย wildcard จะ same กัน
  → หา wild card ของ subnet = 255.255.255.255 - subnet mask
  → keyword → 0.0.0.0 = match all ใช้ host
  → 255.255.255.255 = ignore all ใช้ any

■ Guideline for ACL creation (3P,) → One ACL / Protocol = ctrl traffic flow บน intf, ACL ต้อง define แต่ละ protocol enable on intf
  → one ACL / direction = ctrl trafic in directional time on an intf, แยก ACL ctrl in & out bound traffic.
  → one ACL / interface = ACL ctrl traffic for an intf, Ex G 0/0

- where → Extend ACL : @ close sourse → standard ACL : @ close destination

■ Config ACLs → Standard
  → number Router(config)# access-list access-list-number (num ที่ต้องการสร้าง) deny | permit | remark sourse [wildcard][log]
  ถ้า remove all : no access-list
  ถ้าแก้ ① no access list num # → สั่งใหม่
  ② no บรรทัด # → บรรทัด # ค่าสั่ง
  → in intf Router(config-if)# ip access-group { access-list-number | access-list-name } { in | out }
  ถ้า remove all : no ip access-group
  → ซื่อ ถ้าแก้ → บรรทัด # ค่าสั่งใหม่ → บรรทัดแรก

■ verify : show ip interface , show access-list.

■ securing VTY port : อยากให้คนนอกเข้าได้ permit เฉพาะที่เราต้องการให้เข้า Router(config-line)# access-class access-list-number { in [vrf-also] | out }

→ Extended : filter : sourse / dest addr , Protocol , port number

standard : 0-99, 1300-1999 Extended : 100-199, 2000-2699

access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operator operand]
port port-number or name | destination [destination-wildcard]
[operator operand] [port port_number or name] [established]

ที่เหลือ same standard มีได้ทั้งแบบ number & name
- debug_output : debug ip packet ACL-number

Chapter 6 OSPF & DHCP

▸ Link-state Routing Protocol • เป็น Protocol ที่ต้องสร้าง Complete map ของ nw topology (→มี info all) ขึ้นก่อน → หา shortest path first (SPF) (↑ โดย dijksta)

เหมาะกับ ① large nw, ② fast convergence ③ admin ควรมีความรู้ดี

ขั้นตอน update ① learn info ของ link ② say hello neighbor ③ เอา info มาสร้าง Link-state Packet (LSP)
④ router flood LSP to all neighbors → ได้รับแล้วเก็บลง db ⑤ router เอา all LSP เก็บใน db (รูปแบบ tree) + Adding OSPF → routing table

ข้อดี ① สร้าง topology map ตามหา shortest part ② fast convergence ข้อมูลที่เปลี่ยน ③ LSP sent only when change topology → คำนวณ shortest path ④ hierarchical design (ทพ.ในหน่วยย่อย) → ลด resource bec. แลกข้อมูลแค่ใน area

ข้อเสีย ① ใช้ mem ในการเก็บ all link-state เยอะ ② ใช้ cpu ในการคำนวณ ③ ตอนส่ง LSP ตอนแรกใช้ BW มาก

▸ OSPF AD<110
↳ 3 Table : ① Neighbor show ip ospf neighbor ② topology (ทั้ง map) show ip ospf database ③ Routing (มี shortest path)

message → Encapsulation : MAC Dest = Multicast : 01-00-5E-00-00-05 or 01-00-5E-00-00-06
Protocol field = 89
→ type OSPF Packet : 01 Hello → ทุก 10s (default : multiaccess & point to point nw), ทุก 30s (default : non-broadcast multiaccess (NBMA) nw) cisco default 4 time (40s)
: 02 Db Description (DBD) → synchronization db info
: 03 Link-State Request (LSR) → request link-state
: 04 ⟼ update (LSU) → send update link-state
: 05 ⟼ Acknowledgment (LSAck) → ตอบกลับได้แล้ว

operation : สร้างการเชื่อมต่อ ① Down State (เริ่มต้น) → ② init state (เริ่มส่ง hello) → ③ Two-way State (ตอบกลับ hello) → Exstate Stack → Exchange state → leading state → full state (ระหว่าง router update ข้อมูลเรียบร้อย)

config Single-Area OSPFv2 router ospf process-id → 1-65,535 , เป็น locally significant
R(config-router)# router-id 1.1.1.1 → ① ถ้าไม่ set จะใช้ ② loop back , ③ active interface ip สูงสุด but ต้องมี ① ไม่ก็ ②
router ospf process-id
network network-address wildcard-mask area area-id

OSPF cost → ใช้ BW คำนวณ (default reference BW = 10^8)

$cost = \frac{10^8 \text{ bps}}{\text{intf BW bps}}$ →

10 Gb Ethernet	$= 100\times10^8$ → cost	= 1
Gb	$= 10\times10^8$	= 1
fast	$= 10^8$	= 1
Serial	$= 1.544\times10^6$	= 64

→ ต้องการเปลี่ยนค่า cost
→ เปลี่ยนที่ ref BW
- fast Ethernet auto-cost reference-bandwidth 100 F = G = 10G = 1
- Gigabit Ethernet auto-cost reference-bandwidth 1000 F = 10, G = 10G = 1
- 10 Gigabit Ethernet auto-cost reference-bandwidth 10000 F = 100, G = 10, 10G = 1
→ เปลี่ยนที่ BW : R(config-if)# Bandwidth 64 (EIGRP & OSPF จะใช้ได้)
→ เปลี่ยนที่ cost ⟼ ip ospf cost 15625

verify OSPF show ip ospf neighbor, show ip protocol, show ip ospf interface brief, show ip ospf

more config • Redistributing an OSPF Default Route
R(config)# ip route 0.0.0.0 0.0.0.0 Loopback N
R(config)# router ospf process-id
R(config-router)# default-information originate

▸ DHCP (Dynamic Host Configuration Protocol) → ช่วย config ให้ host ได้ auto เช่น ip, subnet mask, default gateway, dns)

method ① Manual Allocation : admin assign เอง
② Automatic Allocation : DHCPv4 auto assign addr จาก pool & ไม่มี lease (เช่า) time
③ Dynamic Allocation : ใครเปิดขึ้นมาก่อนจะได้ ip ไปมี lease time → ถ้าหมด lease time ต้อง re ip ใหม่

config R1(config)# ip dhcp excluded-address → ไม่แจก, ไม่ใช้
R1(config)# ip dhcp pool LAN-POOL-1 สร้าง Pool (ทพ. ip ที่จะแจก)
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1 ต้องมี

verify show running-config | section dhcp
show ip dhcp binding
show ip dhcp server statistics
• On the PC - issue the ipconfig/all command

debug same Extended

to disable dhcp - no service dhcp ยกเลิก

ถ้า ip ไม่ขึ้น → cmd → ip-config/release → ip-config/renew
→ ตั้งกลับก่อน (@ หน้า set ip)

config DHCP client (แจก ip ให้ client) : -if)# ip address dhcp
:-if)# no shutdown

ชื่อ-สกุล นาย ธมรัเดช บุญทานิมิตร กระดาษแผ่นที่ รหัสนักศึกษา [illegible]

for Staples

Chapter 7 Basic Switch Address Resolution Protocol

▷ LAN Design → Borderless sw nw design : ส่วนทั่วไป :- Hierarchical, - Modularity, - Resiliency, - Flexibility

▫ 2 ลักษณะ : ① 3-Tier LAN Design ประกอบด้วย 1) core 2) Distribution 3) Acess ② 2-Tier LAN Design ประกอบด้วย 1) Collapsed Core / Distribution 2) Access

หน้าที่ layer ต่างๆ:
- ① Core → อุปกรณ์ที่รองรับ BW สูงๆ → ทำให้มี speed ที่ในการเชื่อมต่อ NW } layer 3 support, [Gig / 10 Gig Ethernet]
- ② Distribution → เชื่อมระหว่าง ①&② , Security Policy / Access Ctrl } Redundant component → มีหลายเส้นทางไป
- ③ Acess → ต่อต่อ end device , Port Security, VLAN, [Fa/Gig Ethernet], Power over Ethernet รองรับ or ไม่ก็ได้ (1LAN / 1LAN, 1 power line)

} Link aggregation ↳ ทำให้ BW device เพิ่มขึ้น } Quality of service (QoS)

▫ เพิ่มความสามารถในการใช้ได้ LAN BW & ประสิทธิภาพให้ Max

• f^n & การวาง Sever ① Enterprise S. (รวมทั้งองค์กร) → ติดตั้ง @MDF (Main Distribution facility : Core) → ทางผ่านไปข้างนอก ที่ใกล้กับมัน
② Workshop S. (เฉพาะกลุ่ม) → ติดตั้ง @IDF (Intermediate D. F. : Distribution) → เชื่อมระหว่าง cross กับ Access ที่ใกล้กับมัน

VCC (vertical cross-connect): ตั้ง optical fiber → MDF ↔ IDF
HCC (Horizontal ——): ผ่าน UTP → Distribution ↔ Acess

• Collision detection issue (ปัญหาการตรวจจับการชน)
• Segmentation issue (ปัญหาการแบ่งส่วน) → ทำให้ปัญหาการใช้งานทพ มีปลอดภัยขึ้น
• Broadcast domain issue → ใน nw เกิดตลอด เช่น boardcast หา MAC Addr ∴ boardcast nw ควรมีขนาดเล็ก
• segmentation เป็น process split single collision domain → smaller collision domain ลดจำนวน collision ใน LAN segment :: L2 device ใช้เช่น bridge, sw
• Broadcast domain รับหมดทุก Port but router (L3) เป็นตัว filler / segment broadcast ไม่ให้กระจายออกจากตัวมัน

▷ SW Enviroment

▫ SW Operation
① learning : รับframe เข้า sw จะเรียน Source MAC Addr ว่าเชื่อมต่อกับ Port ไหน + reset Aging
② Aging : อายุของ MAC Addr → if หมด → ทิ้ง

กรณีการส่งออก
③ flooding : ส่ง frame ออกทุก Port ของ sw when frame เป็น 1). broad cast, 2) Multicast, 3) unknown unicast (กรณีที่ dest ไม่อยู่ใน table)
④ forwarding : ส่งไป dest (กรณีพบใน table),
⑤ filtering : if ได้รับ frame ไป dest จาก port ที่เป็นทางไป dest (source & dest บน same interface) จะทำการ filter ทิ้งหมด

▫ SW Methods : ① Store & forward SW → check CRC ว่า error ไหม → มี : ทิ้ง → ไม่มี : ส่ง , auto buffer
② Cut-Through SW → Check เฉพาะส่วน (dest, source อย่างน้อย 12 byte แรก) [10 ms], No FCS & auto buffer
↳ 2 mode :: ① fast-forward ~ 12 byte ② fragment-free ~ 64 byte :: < 64 = ชน → แยก → ไม่ส่ง

▷ Basic Sw Concept & Configuration

for Staples

▫ Basic Sw config
• SW Boot sequence : same Router

manage intf : s(config)# interface vlan num
s(config-if)# ip address ip subnet
s(config-if)# no shutdown

default Gateway :
s(config)# ip-default-gateway ip

• Preparing of Basic SW Management : sw ไม่มี loopback ∴ กำหนด SVI (SW virtual interface) → VLAN
• Config SW Port → Duplex commuication : ① full ② Half (sw ที่ต่อกันต้องเลือก same กัน)
เข้าที่ intf → s(config-if)# duplex full → s(config-if)# speed 100 (เปลี่ยน speed)
→ Auto-MDIX ปกติเชื่อมต่อด้วย cross-over but ต้องการเปลี่ยนสายตรง
เข้าที่ intf → s(config-if)# duplex auto → s(config-if)# speed auto → s(config-if)# mdix auto

→ Verify Port config
show info f0/0, /startup-config
running-config / flash / version
history / ip f0/0 / mac-address-table

▫ SW Security : Secuity Remote Access → SSH (Secure shell) TCP Port 22, telnet : TCP port 23

Config : change host name
S_C (config)# ip domain-name ชื่อ → # Crypto key generate rsa → # username admin pass ccna → line vty 0 15 → -line)#
transport input ssh → -line)# login local [Verify SSH : show ip ssh , show ssh]

▫ SW Port security → กำหนด policy ว่าให้ MAC Addr ไหนเข้า / ออก ได้ - ไม่ได้
s(config-if)# Switchport mode access → # switch port port-security → เลือกมา 1 ประเภท
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 frame ที่วิ่งเข้ามาก่อน record ได้
กรณีเพิ่มจำนวน MAC : # switchport port-security maximum MAX

Violation mode : ① protect : security violation protect mode
② restrict : security violation restrict mode → ส่งไปเก็บว่ามีอะไรเกิดขึ้นบ้าง
③ shutdown : security violation shutdown mode → default
[verify : show port-security int fa0/0, show port-security Address]

security violation modes

mode	forwards traffic	sends syslog message	Display Error massage	increases violation counter	shut Down Port
Protect	x	x	x	x	x
Restrict	x	✓	x	✓	x
shutdown	x	x	x	✓	✓

▫ Addr. Resolution Protocol (ARP) : ARP Cache เก็บ MAC Addr ไว้ Map เส้นทางไป dest (if ไปข้างนอกต้องรู้ MAC gateway)

IPv4 : Classless (ต่อ P1.-2) : - Variable length subnet Masking (VLSM) แบ่งทุก ทพ ไม่เท่ากัน → เลือกของชิ้นใหญ่-เล็ก
- fixed ~ : แบ่งทุก ทพ เท่ากัน

for Staples

Chapter 8 LAN Redundancy & Spanning Tree Protocol (STP)

▷ Issue with layer 1 Redundancy : ① MAC Addr. instability → MAC Addr table จะไม่เสถียร bec. เปลี่ยนแปลงบ่อย
② Broadcast storms → ส่งต่อไปทั่วไม่หยุด ③ Multiple frame transmission → start : unknown unicast → ทำให้ dest ได้รับหลาย frame but. source ส่ง 1 frame

▷ STP → อุดมการณ์ : นำ block port → block สาย → ไม่ให้เกิด traffic ขึ้น เพื่อแก้ปัญหา

□ ขั้นตอน ① หา Root Bridge → เลข priority min Rule : ① 1 RB/1 nw ② 1 RP/1 RB ③ 1 DP/segment
ดูที่ BPDU ② หา Path cost all ③ หา Root Port → Path cost min → อีกฝั่งจะเป็น Designated Port
(Bridge protocol data unit) ④ ถ้าใน segment มี path cost เท่ากัน → ดู BID min เป็น designated port อีกฝั่งเป็น BLOCK Port
↳ มี RB & source [802.1D]

สิ่งที่ใช้เปรียบเทียบ
① BPDU flag (*priority น้อยสุด)
② BID น้อยสุด
③ Path Cost <
④ Sender's BID <
⑤ Sender's Port <

□ config : วิธีที่ 1 : S1(config)# spanning-tree VLAN 1 root primary วิธีที่ 2 : S3(config)# spanning-tree VLAN 1 priority 24576 (เพิ่มทีละมาก)
(if S1, S2 เป็น RB) S2(config)# spanning-tree VLAN 1 root secondary (verify : show spanning-tree)

□ แบบ Extended System ID : B. Priority (2 byte) → B. Priority (per VLAN) (4 bit) + Extended Sys ID (VLAN) (12 bit) + MAC Addr (6 byte) ∴ BID = 8 byte

• PVST+ (พัฒนามาจาก IEEE 802.1D STP) → เพื่อทำ load balancing โดยแยก root / vlan
[Verify : show spanning-tree active]

• Rapid PVST+ → หา Alternate port (ไม่ให้ block ไปเลย com รับส่งข้อมูลได้บางส่วน)
↳ ทำการ set Edge Port @ Port ต่อ host, router : -if)# spanning-tree portfast
↳ Link type : port ที่เชื่อมระหว่าง sw ต้องเป็น point-to-point
-if)# spanning-tree bpduguard enable → Port นี้ไม่ต้องการให้ BPDU ไปเล่น
- config : S1(config)# spanning-tree mode rapid-pvst → # int ที่ p-to-p → # spanning-tree link-type point-to-point

Protocol	Standard	Resources needed	Convergence	Tree calculation
STP	802.1D	Low	slow	All VLANs
PVST	Cisco	High	slow	Per VLANs
RSTP	802.1W	Medium	fast	All
Rapid PVST	Cisco	Very high	fast	Per
MSTP	802.1S Cisco	Medium of High	fast	Per

ถ้า clear all : clear spanning-tree detected-protocol

Chaper 9 VLANs & Inter VLAN

▷ VLAN ทำ Partition (แบ่งแยก : อยู่คนละ nw or broadcast domain กัน) layer 2 เช่น sw และทำการติดต่อได้แค่ใน VLAN เดียวกัน
□ ข้อดี : - security ดีขึ้น, - ลด cost - ปลอดภัยขึ้น - broadcast domain เล็กลง - ปลอดภัยด้าน IT, จัดการง่ายขึ้น [verify : show vlan brief]
□ ~~VLAN~~ in a Multi-SW Environment
• VLAN Trunk set ที่ intf ที่เชื่อมต่อระหว่าง sw ที่มี VLAN → can carry ข้อมูลได้ > 1 VLAN
③ ↳ config : เข้า intf → -if)# switch mode trunk [verify : show int f0/0 switchport]
• Tagging Ethernet frames (IEEE 802.1Q) : Ethernet frame →

Dest MAC	Src MAC	tag	Type / Length	Data	FCS

→ Tag ทำให้ส่ง VLAN ถูก when ส่งผ่าน Trunk

Native (base) VLAN
ไม่ทำการ tag & untag → ส่งผ่าน intf ได้เลย

□ ~~Tagging Assignment~~ Assignment : VLAN number → 1-1005 เก็บ config @ vlan.dat (ใน flash)
→ 1006-4094 เก็บ config @ running-config (ใน NVRAM)
① สร้าง ① S(config)# vlan vlan-num → (vlan)# name ชื่อ
② S# vlan database → (vlan)# vlan num name ชื่อ
② assign port ให้ vlan : เข้า intf → -if)# switchport mode access → # switchport access vlan num (if ลบ : เติม no หน้า ไม่ใส่ num)
(if ลบทั้ง : no vlan num)
- verify show vlan name ชื่อ, show vlan summary, show int vlan num

▷ Inter-VLAN Routing → router set เป็น trunk โดยใช้เทคนิค "sub interface"
② config ① set basic routing (set ip address, no shutdown)
② R(config)# interface g0/0.10 → vlan → -subif)# encapsulation dot1q 10 → # ip address ip subnet-mask

Chapter 10 VTP (VLAN Trunking Protocol) → ช่วย manage VLAN & NAT (NW Addr Translation)

▷ VTP [ใช้กับ : ISL or IEEE 802.1Q] → การ manage sw VTP จะเป็นการ manage ใน domain
□ operation : การ update VTP จะใช้เลข revision number 32 bit (0-4294967295) เชื่อค่าที่สูง >
↳ 3 mode : ① Server → can, สร้าง, remove, rename VLAN ทุกตัวใน domain ยกเว้น ③
② Client → รับข้อมูล VTP and Process, ส่ง VTP msg ออกทุก trunk
③ Transparent → can สร้าง, remove, rename แต่ในตัวมัน, เป็นแค่ทางผ่าน

Feature	Server	Client	Transparent
Source VTP msg	✓	✓	✗
Listen to VTP msg	✓	✓	✗
Create VLANs	✓	✗	✓
Remember VLANs	✓	✗	✓

□ config : 2 แบบ สิ่งสำคัญ 1) SW Cisco 2) มี trunk เชื่อมระหว่าง SW 3) ต้อง domain 4) มี 3 mode
① in global configuration S(config)# vtp version 2 → # vtp domain ชื่อ → # vtp password pass → # vtp mode server mode อื่น
② in VLAN configuration S(vlan)# vtp v2-mode ↗ [verify : show vtp status / counters] ↘ # vtp server | client | transparent
□ Pruning → manage ให้ traffic ที่ใช้งานใน interface น้อยลง โดย config ที่ interface ต่างๆ เพื่อ remove ข้อมูลที่ไม่ได้ใช้
S(vlan)# vtp pruning → เข้า interface → S(config-if)# switchport trunk pruning vlan remove vlan-num

▷ NAT → แปลง Private ip ↔ publish / real ip
□ Terminology : 4 type ① Inside local Addr (private ip) ② Outside local Addr
③ Inside global Addr ④ Outside global Addr → same เดิม

Class	RFC 1918 internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

□ type ① Static กำหนดค่าเอง [map : 1 to 1] ① R(config)# ip nat inside source static local-ip global-ip
② Dynamic มี pool ของ Global / Real ip [map : ตัว many ↔ 1] real ไหนว่างก็ใช้อันนั้น ①.1 # ip nat pool ชื่อ start-ip end-ip {netmask netmask | prefix-length}
③ PAT (Port Addr Translation) → port ที่ต่อแชร์ร่วมกัน NW addr [map : many ↔ 1] ①.2 set ACL ①.3 ip nat inside source list ACL-num pool ชื่อ overload (PAT เพิ่มจาก dynamic)
□ config 3 ส่วน ① NAT ② INSIDE : R(config-if)# ip nat inside ③ outside R(config-if)# ip nat outside
config อีกวิธีของ PAT (single Addr.) ①.1 สร้าง ACL ①.2 ip nat inside source list ACL-num interface f0/0 overload
□ verify : show ip nat translations

ชื่อ-สกุล นาย อมรเดช บุญทปิสิตร กระดาษแผ่นที่ 5 รหัสนักศึกษา [illegible]

for Staples

Chapter 11 EIGRP

→ EIGRP (Enhanced IGRP)

- Characteristics (ลักษณะประจำตัว)
  - Basic features △ Cisco-proprietary (ใช้งานเฉพาะ protocol ของ cisco) เปิดให้ใช้ in 1992
  - ⊕ สร้าง classless version of IGRP ⊕ ทางเลือกที่เหมาะสมสำหรับ nw หลาย protocol, ขนาดใหญ่, ที่สร้างขึ้นบน cisco router

♥ DUAL (Diffusing Update Algorithm) = การันตี loop-free & back up ทั้งหมดของ routing domain → หา best path
→ ทำให้ routing ทำงาน very fast convergent (มี convergent time < ของ OSPF) รวมทั้งมี backup path (ทำให้ทำงานเร็วขึ้น) → if link down จะเลือก path ใน back up ขึ้นมาแทน

(ค.ทำงาน ≈ OSPF เชื่อม router)

♥ Establishing Neighbor Adjacencies = เชื่อมความสัมพันธ์ กับ directly connected EIGRP routers
= Adjacencies are used to track the status of those neighbors

♥ Reliable Transport Protocol · RTP provides ~~delivery~~ delivery of EIGRP packet to neighbors
EIGRP can update = RTP and neighbor adjacencies are used by DUAL (ในการ maintain)

♥ Partial and Bounded - update เฉพาะส่วนที่มีการเปลี่ยนแปลง รวมถึง update ไปให้เฉพาะส่วนที่มีการเปลี่ยนแปลง ∴ update < RIP

update ทั้ง router ตลอดเวลา

♥ Equal and Unequal Cost (OSPF, RIPv2) = ช่วยให้ admin ดูแลระบบ เพื่อกระจายการรับข้อมูลในเครือข่ายได้ดีขึ้น
Load Balancing ↳ ค่า cost ≠ but ทำเป็น load balance ได้

▲ ใช้ protocol-dependant modules (PDMs) เพื่อรองรับ protocol ที่แตกต่างกัน เช่น IPv4, 6

▲ PDMs รับผิดชอบ :
- ⊖ maintain EIGRP neighbor and topology table (Neighbor table → สร้าง topology table → ใส่ routing table)
  (→ เก็บ shortest path กับ backup; เป็น routing)
- ⊖ คำนวณ metric ที่ใช้ DUAL ⊖ เชื่อมต่อ DUAL และ routing table

for Staples

- ⊖ implement filtering and access lists ⊖ ทำ redistribution with other routing protocol

△ RTP is EIGRP transport layer protocol สำหรับ delivery & reception ของ EIGRP packets
= เป็น msg ที่อยู่ใน application layer ใช้ maintain ข้อมูล, msg ต่างๆ ทั้งส่ง ของ EIGRP

△ ไม่ใช่ทั้งหมดของ RTP packet จะส่งได้น่าเชื่อถือ (msg ≈ OSPF)
- ⊕ Reliable packet require explicit (ชัดเจน) ack จาก dest ⊖ Update, Query, Reply
- ⊖ Unreliable packet do not require ack จาก dest ⊖ Hello, Ack

▲ รองรับ authentication (no encrypt routing update) และ is recommend (เป็นที่ยอมรับ) (authen ≈ RIPv2, OSPF)

△ Packet Type routing update or queries EIGRP multicast IPv4 : 224.0.0.10, IPv6 : FF02::A

1. Hello → ที่ใช้ adjacencies ระหว่าง router 2 ตัวที่เป็น neighbor กัน, ไม่ต้องรอ response, ส่ง unreliably
2. Update → update info ของ cost, update info ของ routing ไปให้ neighbor router
3. Acknowledgement → พอได้รับ msg update ก็ตอบ ACK
4. Query → request info routing จาก neighbor router
5. Reply → หลังจากได้รับ query ก็ reply

} เวลาต้องการ info ของ routing เพิ่มก็ query ไปให้กับ router ที่อยู่ข้างๆ แล้ว reply ตอบกลับว่า มีหรือไม่มี

□ Implement EIGRP for IPv4

△ Autonomous system (AS) is a collection of nw ภายใต้การดูแล ของ single authority (อ้างอิง RFC 1930)
↳ AS number → ใช้ exchange router between AS
→ managed by IANA & assigned by RIR to ISP, Internet Backbone providers and institution
→ 16 bit : 0 - 65535 → since 2007 32 bit over 4 billion

△ verify : show ip eigrp neighbors ดูต่อตลอดเวลาปัจจุบัน
show ip protocols
show ip route

for Staples

△ Configure : R(config)# router eigrp AS-# (≈ router-id @ OSPF)

show ip protocols ← R(config-router)# ~~router-id~~ eigrp router-id → ถ้าไม่กำหนด จะใช้ loopback
R(config-router)# ~~nw-number~~ network nw-number [wildcard-mask] → intf → IPv4 addr ที่สูงสุด ที่ active
ถ้าไม่มีใช้
R(config-router)# passive-interface type number [default]: ไม่ให้ update ไปที่ intf ไหน

□ Operation

- Initial Route Discovery (ค้นพบ) ① R1 send hello กับ neighbor ② R2 ตอบกลับส่ง hello or update กลับมา ③ R1 ตอบ ack & update info
④ ใช้ DUAL คำนวณ best route and update routing table

□ metrics : BW (lowest) (k1=1), Delay (ผลรวม) (k3=1), Reliability (worst) (k4=0), Load (worst) (k2=0) ดูค่า value : show interface

Default Composite formula : metric = [k1 * bw + k3 * delay] * 256
= [(10 000 000 / bw) + (sum of delay / 10)] * 256

Complete : = [k1 * bw + (k2 * bw) / (256 - load) + k3 * delay] * [k5 / (reliability + k4)]

- R(config-router)# metric weights tos k1 k2 k3 k4 k5 - set bw : เข้า intf. → R(config-if)# bandwidth kilobits-bw-value

□ DUAL and the Topology table (ใช้ FSM (finite state Machine) ในการเลือกเส้นทาง) → show ip eigrp topology [all-link],
+ Successor (S) (router ที่ไป dest สั้นสุด) = neighbor router ที่ส่งออกทางไป dest ที่มีค่า metric น้อยสุด show ip route
+ Feasible Successor (FS) (มีได้ในเงื่อนไข feasible condition) = Back up path เส้นทางสำรอง มี cost เท่ากัน
+ Reported Distance (RD) (distance ที่ neighbor ตัวอื่น report distance มาให้เรา) = "advertised distance" จากตัวมัน → dest
+ Feasible Distance (FD) (distance ที่ไปทาง S) ค่า distance ที่คำนวณไปยัง dest ทั้งหมด เป็นค่า cost lowest → dest

IPv6

□ IPv4 Issue

- Need for IPv6 → แก้ปัญหา ip มีจำนวนจำกัด (private ip, NAT) ใช้ใน IOT ได้
- หาวิธีการร่วมกัน (coexistence)
  - Migration IPv4 → IPv6 techniques : ① Dual Stack = run ทั้งคู่ if ฟังก์ชันไม่ได้ไม่กระทบ user same เดิม
  ② Tunneling (อยากใช้ v6 but core ไม่ support = เปลี่ยนเฉพาะเรา เลยวิ่งผ่าน V4
  ③ Translation (คล้าย NAT) = IPv6 ↔ IPv4

□ IPv6 Addressing : 128 bit แบ่ง 8 ส่วน (1 ส่วน มี 2 byte = 16 bit) → represent base 16 ทุก 4 bit
- ออกแบบวิธีการกำหนดค่า IPv6

Rule 1 Omit leading 0s ในแต่ละ partition "0" ที่อยู่ข้างหน้าไม่ต้องก็ได้ 000x (00-F), 00xx, 0xxx
Rule 2 Omit All 0 segment แทน segment ที่มี "0" ติดกันหลายตัว "::" ใช้ได้ที่เดียว only

□ Type of IPv6 Address

- IPv6 Address Type ① Unicast ⊖ Global Unicast ⊖ Link-local ⊖ Unique local
② Multicast
③ Anycast ส่งได้หลาย device

ชื่อ-สกุล นาย อมรเทพ บุญทนพิตร กระดาษแผ่นที่ 6 รหัสนักศึกษา 59080508

for Staples

Config

Router

① basic configuration

เข้า intf (เช่น gig, fa) → R(config-if)# ip address ip-addr subnet-mast → R(config-if)# no shutdown

เข้า intf (serial ฝั่ง DCE) → ~ → R(config-if)# clock rate 56000 → ~

② protocol

- static routing

next hop addr exit interface

เข้า intf → R(config-if)# ip route nw-ip subnet-mask {ip addr | exit-intf}

4 default route ~ # ip route 0.0.0.0 0.0.0.0 {ip addr | exit-intf}

- Dynamic routing
  - Interior Gateway P.
    - Distance Vector Routing P.
      - RIP : R(config)# router rip → R(config-router)# network nw-ip

passive intf : R(config-router)# passive-interface intf-type intf-number

เชื่อม RIP↔static : R(config)# router rip → R(config-router)# {redistribute static | default-information originate}

โดย router ที่ต้อง set default @ intf ที่เชื่อมระหว่าง 2 protocol ด้วย!

- RIPv2 : R(config)# route rip → R(config-router)# version 2 → no auto-summary → network nw-ip
- EIGRP : R(config)# route eigrp AS-# → R(config-route)# eigrp router-id-network nw-ip (wildcard-na)

passive intf : R(config-router)# passive-interface intf type intf-number

metrics : R(config-router)# metric weights tos k1 k2 k3 k4 k5

- set bw : เข้า intf → R(config-if)# bandwidth kbits-bw-value

- Link state Routing P.
  - OSPF

1-65,535

: R(config)# router ospf process-id → -router)# router-id 1.1.1.1 → network nw-ip wild card-mask area area-id

set bw : เข้า intf → R(config-if)# bandwidth 64

set cost: ip ospf cost 15625

passive intf : R(config-router)# passive-interface intf-type intf-number

redistribute (OSPF↔default route) : R(config)# ip route 0.0.0.0 0.0.0.0 loop back N

router ospf process-id

→ R(config-router)# default-information originate

redistribute (ospf↔อื่นๆ) : R(config)# router ospf process-id → R(config-router)# redistribute ?

③ อื่นๆ

for Staples

- ACL if สร้าง Name : R(config)# ip access-list [standard | extended] name

set ACL : R(config)# access-list ACL-num {permit | deny | remark} source (source-wildcard) (log)

set @ intf : เข้า intf → R(config-if)# ip access-group {ACL-num | ACL-name} {in | out}

for Staples

- Securing VTP with standard IPv4 ACL : R(config-line)# access-class ACL-num
- Extended IPv4 ACL :

R(config)# access-list ACL-Num {deny | permit | remark} protocol | source [source-wildcard] [operator operand] destination [dest-wildcard] [operator operand] [port port-num or name] [established]

- DHCP : R(config)# ip dhcp excluded-address ip-addr-start ip-addr-end
  R(config)# ip dhcp excluded-address ip-addr
  ip dhcp pool LAN-POOL-1
  R(dhcp-config)# network nw-ip subnet-mask
  default-router ip-address-gateway

Switch

① basic configuration
- management intf : S(config)# interface vlan N → S(config-if)# ip address ip-addr subnet-mask
  no shutdown
- default gateway : S(config)# ip default-gateway ip

② Configure switch port
- duplex communication : 내가 intf → S(config-if)# duplex full → speed 100
- auto-MDIX : 내가 intf → S(config-if)# duplex auto → speed auto → mdix auto
- security Remote Access
  + SSH (TCP port 22) : S(config)# ip domain-name cisco.com → crypto key generate rsa
    → username admin password cona → line vty 0 15 → S(config-line)# transport input ssh
    → login local
  + telnet (TCP port 23)
- switch Port security : 내가 intf → S(config-if)# switchport mode access → switch port-security
  + static secure MAC addr. : switchport port-security mac-address MAC-ADD
  + dynamic : switchport port-security mac-address stiky
  + max MAC Address : switchport port-security maximum MAX
  + violation mode : switchport port-security violation {protect | restrict | shutdown} mode

③ STP : 내가 1 S(config)# spanning-tree VLAN 1 root {primary | secondary}
내가 2 S(config)# spanning-tree VLAN 1 priority 24576 → 작을수록 priority 높
- Rapid Pvst +
  + Portfast : 내가 intf → S(config-if)# spanning-tree portfast
  + BPDU Guard : 내가 intf → S(config-if)# Spanning-tree bpduguard mode
  + Config : S(config)# spanning-tree mode rapid-pvst → 내가 intf → S(config-if)# Spanning-tree link-type point-to-point

④ VLAN 1. set VTP mode : S(config)# vtp version 2 → vtp mode {server|client|transparent} → vtp domain name → vtp password pass
2. set trunk : 내가 intf → S(config-if)# switchport mode trunk
3. 원하는 VLAN 에 server : S(config)# vlan num → name name
4. assign intf 내가 intf → S(config)# switchport mode access → switchport access vlan num
5. set inter-VLAN : R(config)# int fa0/0.10 → description vlan 10 → encapsulation dot1q 10 → ip address ip subnet

⑤ NAT
- static : R(config)# ip nat inside source static local-ip global-ip → 내가 intf → S(config-if)# ip nat {inside | outside}
- dynamic : R(config)# ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix}
→ access-list ACL-num permit source (source-wildcard) → ip nat inside source list ACL-num pool name
→ 내가 intf → S(config-if)# ip nat {inside | outside}