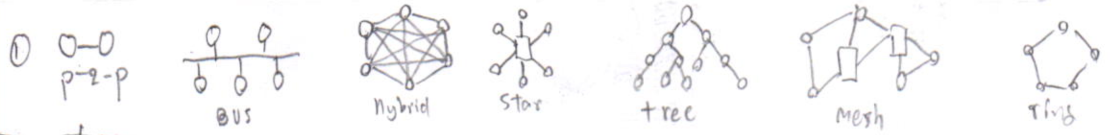
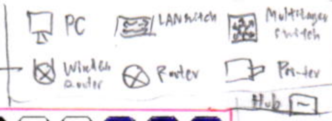


network topology



Layer TCP/IP

ชื่อ-สกุล มุฮัมหมัด ริดวาน อัดดิน กระดาษแผ่นที่ 1 รหัสนักศึกษา 59011098

MAC Address IEEE

for Staples

	Hostconfig	Email	File Transfer	Web
App, Present, Session → App	DNS / BOOTP DHCP	SMTP POP IMAP	FTP TFTP	HTTP
Transport → Transport	UDP	TCP		
Network → Internet	IP NAT	IP Support ICMP	OSPF	Route hop EIGRP
DataLink, Physical → Network Access	ARP	PPP	Ethernet	Interface Driver

ชนิด LAN ②

ง จ ฉ ฟ ห ส A

K & V ฟ ห ฮ ห H B

IPv4	High Order bit	
Class A	0	0 - 127
B	10	128 - 191
C	110	192 - 223
D	1110	224 - 239
E	1111	240 - 255

Private	CIDR Prefix
A 10.0.0.0 - 10.255.255.255	/8
B 172.16.0.0 - 172.31.255.255	/12
C 192.168.0.0 - 192.168.255.255	/16

Unicast ส่ง 1 ทาง
Multicast ส่งหลายทาง 01-00-5E-XX-XX-XX
Broadcast ส่งทุกทาง
③

Network overview
Physical → port / Interface ต่อสัมผัสได้
Logical → IP Address

Function of Router
- CPU Execute OS instruction
- RAM store routing table
- ROM Store bootstrap program
- NVRAM Store startup-config / IP / Routing Protocol / Hostname
- Flash Memory Contain OS
- Interface Ethernet / fa / Serial

User EXEC Mode
Router>
Privileged EXEC Mode
Router#
Global Config Mode
Router(config)#
Router(config-if)#

Component
- End Device เช่น PC
- intermediary device เช่น hub / switch / Router
- media เช่น Copper fiber optic, coaxial, wireless

Type
switch / เลือกทางออก Router / เลือกทางที่ดีที่สุด
small home / ไม่กี่เครื่อง small office / config ด้วยตนเอง
medium to large / 100-1000 เครื่อง world wide / Internet

Reliable
1) fault tolerance หากล่มยังมีทางอื่น 2) Scability เพิ่มขยายได้โดยไม่กระทบ user
3) Security รักษาความปลอดภัย 4) Quality of Service แต่ละ service มี quality ≠

ขอ IOS version / Bootstrap version / Model & CPU /
ขนาด RAM แบ่งเป็น 2 ส่วน
ประเภท และจำนวน Interface
ขนาด NVRAM
ขนาด Flash Memory

Router (config) # enable password cisco
Router (config) # hostname GAD
Router (config) # router rip
Router (config) # banner motd # SOME WORD #
Router (config) # line console 0
Router (config) # password cisco
login
exit

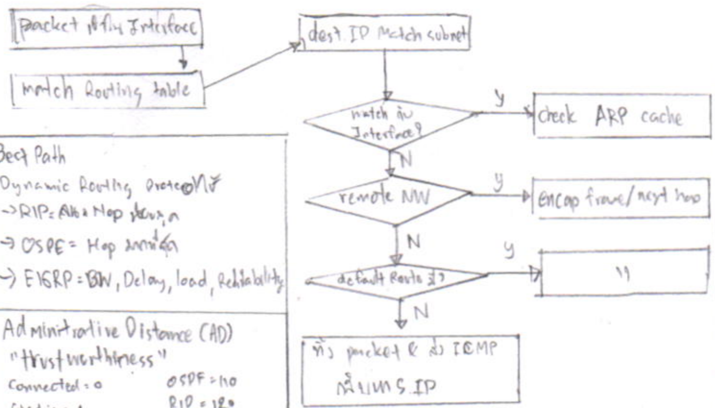
for Staples

console
telnet ②

Router (config) # line vty 0
Router (config) # enable secret cisco
Router # start running-config
Router # copy running-config startup-config } copy ไปใน NVRAM
Router (config) # interface
Router (config-if) # ip address
Router (config-if) # no shutdown
Router (config-if) clock rate 56000 ← for DCE

R(config)# interface fa0/0
R(config)# interface S0/0/0
R(config)# interface Vlan 1

show running-config → ดู config
show startup-config → set ที่ save
show ip route → ดู routing table
show ip interface } show info ของ interface
show interface
show ip interface brief → ดู interface



Best Path
Dynamic Routing Protocol
→ RIP = Hop น้อยสุด
→ OSPF = Hop มากสุด
→ EIGRP = BW, Delay, load, Reliability

Administrative Distance (AD)
"trustworthiness"
Connected = 0 OSPF = 110
Static = 1 RIP = 120
Internal EIGRP = 90

Static - เช่น Network server หรือ printer
Dynamic - DHCP Service ใน Cisco Router

Console ใช้สาย RJ-45-to-DB9
ใช้ Terminal เช่น Tera Term, Putty, Hyperterminal

Characteristic
① Topology ② Speed ③ Cost ④ Security ⑤ Scalability ⑥ Reliability

Default Gateway
first usable Host .1 last usable Host .254
เป็นทางออกของ NW นั้นๆ ที่จะไปยัง Network อื่น

• Routing

① static Routing → Manual
ข้อดี Security, ใช้ Resource น้อยกว่าการ process, ลด routing entry
ข้อเสีย ลำบากในการ Scalibility, ต้องแก้ทุกครั้งที่เปลี่ยนแปลง
ควรจะใช้เมื่อ : NW มีขนาดเล็ก, มี Router น้อย, NW มีทางออกทางเดียว
A type ① standard ① default stub NW
เมื่อ Dest. ip ไม่ตรงกัน
③ Summary ④ Floating back-up

※ ip route nw-address subnet-mask { ip-address | exit inf }

② Dynamic Routing Protocol
1. EGP Exterior Gateway Routing Protocol :: BGP
1. IGP (Interior ⟵ :: RIP, OSPF, EIGRP, IS-IS

• Classful Addressing → update ตาม class
• Classless Inter-Domain Routing
① summarization
ยังไม่ไป อยู่ติดกัน, ไม่มีทางลัดกัน
• VLSM
① Fix Length Subnet Masking
② prefix ใหม่ - prefix เก่า = จำนวน bit ที่เพิ่ม
③ เพิ่มทุกที่ bit เป็น 1 แล้วนำตำแหน่ง 10 ไป + ip เพิ่มทีละ +1 ทางขวาไปเรื่อยๆ

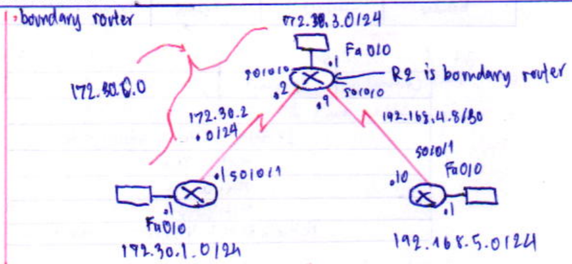
for Staples

801 22

ชื่อ-สกุล มุฮัมหมัด ฮัซซาน ฮัลดีน กระดาษแผ่นที่ 02 รหัสนักศึกษา 59888098

for Staples

Chapter 4 Distance vector Routing RIP v1



▷ Dynamic Routing Protocol

☐ fn: share info ระหว่าง Router • auto update routing table เมื่อ topology เปลี่ยน เมื่อมีปัญหา • หา best path

☐ purpose: หา remote nw (nw ที่อยู่ห่างไกล) • ปรับปรุง routing info. • เลือก best path ไป dest. nw. • สามารถหา new best path ถ้า path มีปัญหาไม่ว่างยาวๆ

☐ Component: ① Algorithm: ใช้เพื่อสะดวก routing info & best path.
② Routing protocol msg.: สำหรับหา neighbor & แลกเปลี่ยน routing info. (best path)

☐	Dynamic Routing	VS	Static Routing
ความซับซ้อนในการ config	∝ ขนาด nw (เท่าเดิม)		∝ ขนาด nw (เพิ่ม command ทุก router)
Required ความรู้ admin	Advance (เพราะ basic config → nw ใหญ่ + ซับซ้อน อาจมีปัญหา		ไม่มีเพิ่มเติม (กำหนดเส้นทางเองโดย command)
Topology change	ปรับ auto		admin config ใหม่ ทั้งหมด
Scaling	เหมาะสำหรับ simple & complex (router ที่ไม่ได้ directly ไปต่อกันก็ได้)		เหมาะสำหรับ simple topologies
Security	น้อยกว่า		มากกว่า
Resource usage	ใช้ CPU, mem (เก็บ routing info), link bandwidth		ไม่มีเพิ่มเติม
Predictability	Routing ∝ current topology		Route → dest. ทางเดิมตลอด

▶ Classifying Routing Protocol

DRP
- (ภายใน AS) Interior Gateway Protocol (IGP)
  - Distance Vector P.
    - • ประกอบด้วย vector [distance, direction]
    - • incomplete view ของ nw topology
    - • periodic update (ระยะเวลาซ้ำๆ)
    - RIP (Routing Info P.) → RIP V.2
    - IGRP (Interior Gateway Routing P.) → EIGRP (Enhanced Interior Gateway Routing P.)
  - Link-State P.
    - • Complete nw topology (เห็นภาพทั้งหมด)
    - • update ไม่ใช่ periodic
    - OSPF (Open Shortest Path First)
    - IS-IS (Intermediate System to Intermediate System)
- (ระหว่าง AS) Exterior Gateway Protocol (EGP)
  - BGP (Border Gateway Protocol)
    - • Autonomous System (AS) เป็นกลุ่มของ Router ที่อยู่ภายใต้การควบคุมของ Single Authority (1 กลุ่ม policy เดียวกัน)

for Staples

☐ 2 Type
① Classful routing P. → update ตาม class ไม่ส่ง Subnet mask ใน routing update
② Classless → ส่ง Subnet mask ใน routing update

☐ Convergence: ถูกกำหนดเมื่อ routing table ของ router ทั้งหมด มีสถานะเดียวกัน (ไม่เปลี่ยนแปลง) } 2 type: slower: RIP & IGRP, Faster (เมื่อข้อมูลเปลี่ยนแปลงเกิดการเปลี่ยนแปลงเร็ว): EIGP & OSPF

▶ Routing Protocol Metric

☐ Metric: ค่าที่ใช้ในการคิด/หาในการไป Dest. NW จะเลือก best path ใหม่ เช่น Hop count, BW, Cost, Delay, Load, Realiability

☐ Load balancing: nw มีเส้นทาง > 1 ที่มี metric เท่ากัน → เฉลี่ยให้การใช้งานแต่ละเส้นทางเท่าๆ กัน

▶ Administrative Distance of Router (AD) ใช้เลือก protocol ในการ Routing ซึ่งถูกประเมินค่าตัวเลขที่เหมาะสมที่สุดของ (ความเชื่อถือ) particular 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	100	115	170	200

▶ Distance Vector routing protocol Ex. RIP, IGRP, EIGRP

☐ Distance Vector Technology ต้องรู้สองสิ่งมาใช้คือ ① Vector or Direction, ทราบการเปลี่ยนแปลงที่ถูกต้อง ② Distance to final Dest. (cost)

☐ ลักษณะทั่วไป: peridic (ตามเวลา) update, neighbor (ⓧใกล้เคียง), broadcast (255.255.255.255) update, เอา routing table all ไป update

☐ ลักษณะที่ดีของ Routing Protocol เกณฑ์ที่ใช้วัดว่า ดีหรือไม่ ① Time to Convergence → เวลาที่เข้าสู่ steady state ของ Routing table ที่เกิดการปรับปรุงแล้ว ② scability ขนาดของที่สุดเท่าไร ③ Resource usage ④ Implementation & maintenance

	RIP V1	RIP V2	IGRP	EIGRP
speed convergence	slow	slow	slow	fast
scability size-nw	small	small	small	large
use of VLSM	✗	✓	✗	✓
Resource usage	Low	Low	Low	Medium
implemention & maintanence	Simple	Simple	Simple	Complex

▷ มี 3 stage 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 อื่นต่อไปเท่าไร

▷ 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 240)

• Bounded (ขอบเขต) Update: EIGRP → update เฉพาะที่เปลี่ยน

• Trigger Update → Update เลยไม่รอ periodic time

• Random Jitter → ใช้ใน nw ที่เป็น multiple access router หลายตัว เชื่อมต่อกัน → if เกิด update พร้อมกัน ∴ จึงใช้ Random

▷ ปัญหา Standard DV ① Routing Loops เกิดเมื่อ interface ไหน down จะถูกลบออกจาก table → ค่าที่ได้จาก neighbor จะกลับมา update (วน update → hop เพิ่มขึ้นถึง ∞)

for Staples

วิธีแก้ปัญหา: ① set max hop = 15 → if hop = 16 → unreachable (เป็น down ไปแล้ว)
② holddown timer (ถ้า interface down → hold)
③ Split Horizon rule → ไม่ส่งข้อมูล update กลับไปทาง interface ที่ได้รับ update มา
④ Route Poisioning → ① เกิด down set unreachable ② ส่ง unreachable ที่เป็น poison ออกไป ใน inf นั้น hop = 16
⑤ ③ with ④ → ถ้าเกิด unreachable จะ over rule split โดยส่ง ip interface ที่ down (hop = 16)
⑥ IP & TTL (Time to Live) เกิดการวน update but(แต่) จะหยุดเมื่อ TTL = 0

▷ RIP V1 AD=120

□ คุณสมบัติ : • classful, DV • metric = hop count • hop count > 15 unreachable • update broadcast ทุก 30 s

→ Encapsulated (บรรจุ) ใน UDP Segment ~~ทั้ง~~ Source & Dest. Port 520 (Transport Layer)

RIP V1 Format Message

Data Link Frame header	IP Packet Header	UDP Message header	RIP Message (512 byte: up to 25 route)

request ↖ 1 · 2 ↗ reply · 0 ขอ full routing table

header ←

Bit 0–7	8–15	16–23	24–31
Command 1 or 2	Version=1	Must be Zero	
Address Family Identifier (2=IP)		Must be zero	
IP Address (Network Address) → dest.			
Must be Zero			
Must be Zero			
Metric (hops) → 1-15 ถ้ามาก table+1 → ส่งออก			
Multiple Route Entries, up to maximum of 25			

Route Entry (rows: Address Family Identifier … Metric)

- boundary Routers: summarise RIP subnet from 1 major nw to another
- Processing RIP update
  - ดูว่าที่ส่งและรับ update ใน interface ว่ามี classful เดียวกันไหม!
  - มี : update subnet nw เช่น 172.16.1.0
  - ไม่มี : update classful เช่น 172.16.0.0

□ msg มี 2 type ① Request → ส่ง routing table → ส่ง interface ที่ config ไว้เพื่อรอการตอบ
② Response → ส่ง info จาก Routing table

□ ip address พร้อมกับ class A,B,C

□ Basic RIP v1 config ① ทำ basic routing config
② ส่ง router rip R1(config)# router rip
R1(config-router)# network (nw ที่ต่อกับเราโดยตรง)

□ Verification (ตรวจสอบ) & troubleshooting (แก้ไขปัญหา): show running-config / ip route / ip protocol, debug ip rip

- passive interface command (ไม่ update interface ที่ไม่จำเป็น)
  R(config-router)# passive-interface interface-type(Fa/G/S) interface-number(0/0, 0/0/0)

□ Automatic Summarization : RIP Auto Summarise classful nw → เพื่อลด size ของ routing table
ข้อดี ลด size ของ routing update • single router แทนหลายๆ multiple route เร็วมากใน routing table
ข้อเสีย ไม่ support discontiguous network (Major network เดียวกัน แต่ไม่ได้อยู่ติดกัน) อาจทำ load balance ไม่ได้

□ Default route & Rip V1 ถ้าไม่พบทางออกใน routing table (อาจจะเพราะไม่รู้จัก protocol) → จะออก 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 V2 & ACL (Access Control Lists)

RIP V1	RIP V2	
classful (ไม่ส่ง subnet mask, ไม่ support CIDR)	Classless (update subnet mask, support variable length Subnet mask (VLSM), support route summarisation (Prefix Aggregation))	ใช้ timer ป้องกัน routing loop
ไม่ support discontiguous subnet	update next hop address	ใช้ split horizon or split horizon with poison reverse
ไม่ support VLSM เพราะไม่ส่ง subnet mask 255.255.255.255	ใช้ Authentication routing (รองรับ discontiguous เครือข่าย)	ใช้ triggered update
routing update => broadcast	Routing update → multicast	max hop count = 15

ข้อจำกัด ของ Rip V1
เป็น virtual Interface สามารถ เพิ่มใน routing ได้ update ออกไปได้

loopback interface → ping ไป → ip virtual interface → reply ได้
null interface → ใช้ส่งต่อแพ็กเก็ต channel ที่เราไม่ต้องการ → ส่งออก null → packet discard ไป → timeout
static route & null intf → null interface จะเป็นหน้าที่เป็นทางออก ของ static route
R(config)# ip route summary-static-route subnet-mask Null0
(major nw) → ของ static supernet route

- Route redistribution (กระจาย) → อยากให้ rip รู้จัก static ต้องเพิ่มใหม่ (ให้ rip ส่ง static ไปด้วย) : R(config-router)# redistribution static
- Verify & test Connectivity : show ip interface brief, ping (ผล: ! = ได้, U = ไม่ได้, . = timeout), trace route
- RIP V1 : classful, ไม่ส่ง subnet mask, summarise network ที่ major network boundaries, ถ้า network เป็น discontiguous & Rip V1 config convergent จะไม่เกิด
- ตรวจ Routing table debug ip rip (content of routing update) ถ้าเป็น rip V1 จะไม่มี subnet mask รวมกับ network address

▷ RIP V2

Command 1 or 2	Version=2	Must be Zero
Address family Identifier (2=IP)		Route tag
IP Address (Network Address)		
Subnet Mask		
Next hop		
Metric (Hop)		
Multiple route entries, up to maximum of 25		

☒ Config
- Enabling & verify RIP V2
- Config RIP → RIP V1 → สามารถรับได้ทั้ง V1 และ V2 แต่ส่งได้แค่ V1
  RIP V2 → สามารถรับและส่งได้แค่ V2
- Auto-summary & RIP V2 → auto sum route ที่ major network boundaries
  → sum route ด้วย subnet mask ที่น้อยกว่า classful subnet mask เพราะเมื่อ ใน network topology ต้องเป็น discontiguous
- disabling auto-summary (no auto-summary)

□ VLSM & CIDR → verify info. ที่ส่งโดย RIP V2 (debug ip rip)
→ VLSM → เห็นทั้ง network address & subnet mask
→ CIDR → ใช้ supernetting (= bunch of contiguous classful network ที่เป็น Address เหมือน single network)
→ verify (show ip route, debug ip rip)

▷ Access Control List → ควบคุมการเข้าออก → ตรวจสอบ → check → source → dest ผ่านไหม?
→ ดูจาก conversation → ทำอย่างนี้ (เช่น FTP) ผ่านไหม?

□ packet filtering จาก ① dest, source ที่ L2 ② protocol อะไร ③ ไป network ไหน, ทำอะไร → ทำให้ผ่านได้หรือ block ไว้

□ Operation → ทำงาน เป็น sequence statement
→ last statement เป็น implicit deny → block → discard

□ Standard ACLs IPv4
- check source ~~dest~~. address
- ปล่อย permits หรือ deny ทั้งชุด protocol
  access-list 10 permit 192.168.30.0 0.0.0.255
- number ACL : 1-99 & 1300-1999

□ Extended IPv4 ACLs
- check source & destination address.
- ปล่อย permit หรือ deny ตามแต่ละ 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 set ของ ip ① หาตำแหน่งของ bit ที่ซ้ำกัน ใส่ wildcard mask ตำแหน่งนั้น = 0
② bit ที่เหลือใส่ 1
if กรณีต้องการ ลอกแบบ Pattern or/and ส่วน คือ ดูค่าใน wildcard จะเหมือนกัน
→ หา wildcard ของ subnet = 255.255.255.255 - subnet mask
→ keyword → 0.0.0.0 = match all ใช้ host
→ 255.255.255.255 = ignore all ใช้ host

R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0]
R1(config)# access-list 1 permit host 192.168.10.10
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255]
R1(config)# access-list 1 permit any

ชื่อ-สกุล นู้ฮัยนมัด วิจกน อัดดุ้ง กระดาษแผ่นที่ 03 รหัสนักศึกษา 58088098

for Staples

□ Guideline for (3P) → One ACL / Protocol : ctrl traffic flow บน interface, ACL ต้อง define ตาม protocol ให้ enable บน interface

ACL Creation → one ACL / direction = control traffic in 1 direction at time on any Interface, หาก ACL control in & out bond traffic

→ One ACL / Interface = ACL ctrl traffic for an interface, Ex 0010

• Where → Extend ACL : ที่ Close source → Standard ACL : ที่ close destination

□ Config ACLs → Standard

เลือก เพบบ ที่ปรับแต่งอัน หลังจาก คำสั่ง permit/deny ใหม่

→ number : Router(config)# access-list access-list-number deny | permit | remark source [source-wildcard] [log]

remove all : no access-list ถ้าแก้ (I) no access-list num# → ทั้งหมด access-list num# permit any

(II) no ของหัว# → ของหัว# ถึงทั้ง

→ ใน int : Router(config-if) ip config-group { access-list-number | access-list-name } { in | out }

Router(config)# ip access-list [standard | extended] name

remove all : no ip access-group ถ้าแก้ → ของหัว# ถึงใหม่ → ของหัวทั้งหมด

□ Verify : show ip interface, show access-lists

□ Securing VTY port → อย่าให้คนนอกเข้า permit หมายเฉพาะที่อนุญาตให้เข้า Router(config-line)# access-class access-list-number {in [vrf-also] | out}

→ Extense : filter : source / dest. Addr, protocol, port number ที่เหลือเหมือน standard ได้ทั้งแบบ Number & name

- debug-output : debug ip packet ACL-Number

Chapter 6 OSPF & DHCP

▷ Link-state Routing Protocol = เป็น protocol ที่สร้าง complete map (มี info ทั้งหมด) ของ network topology ที่คำนวณ shortest path first (SPF) โดย dijkstra

เหมาะกับ : ① large network ② fast convergence ③ admin ควรมีความรู้ที่ดี

ขั้นตอนการทำงาน : 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 เอาทั้งหมดของ LSP มาสร้าง Database ในรูปแบบของ tree + Adding OSPF → routing table

ข้อดี : ① สร้าง topology map ของตัวเอง shortest path ② fast convergent เพียงแค่ flood ③ LSP sent only when change topology (ไม่ต้องส่งข้อมูลทั้งหมด) → คำนวณ shortest path) ④ hierachical design (network ในรูปแบบ) → ลด resource เพราะแบ่งข้อมูลเป็น Area

ข้อเสีย : ① ใช้ memory ในการเก็บ link-state ทั้งหมด ② ใช้ cpu ในการคำนวณ ③ ตอนส่ง LSP ครั้งแรก จะใช้ Bandwidth เยอะมาก

▷ OSPF AD = 110

↳ Table : ① neighbor show ip ospf neighbor ② Topology (แผนที่map) show ip ospf database ③ Routing (มี shortest path)

for Staples

message → Encapsulating : MAC Dest. = Multicast : 01-00-5E-00-00-05 หรือ 01-00-5E-00-00-06 Protocol field = 89

→ type OSPF Packet : 01 Hello ทุก 10 s (default : multi access & point to point nw), ทุก 30s (default : non-broadcast multiple-access (NBMA) nw), Cisco default 4 times (40s)

: 02 Db Description (DBD) → Synchronousation db info

: 03 Link-state Request (LSR) → request link-state

: 04 " Update (LSU) → send update link-state

: 05 " Acknowledgement (LSAck) → ยืนยันกลับได้รับ

Operation ; สร้างการเชื่อมต่อ ① Down state (เริ่มต้น) → ② Init state (เริ่ม Hello) → ③ two way state (ตอบกลับ Hello) → Exstate state → Exchange state → Loading state → Full state (ระหว่าง router update ข้อมูลเรียบร้อย)

config Single-Area OSPF V2 (router ospf process-id → 1-65,535, เป็น local significant

R(config-router)# router-id 1.1.1.1 → ถ้าไม่ set สามารถใช้ loop back, active interface ip สูงสุด โดยควรมี 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]

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

→ 10 Gb E = 100×10^8 → cost 1

→ Gb = 10×10^8 → cost 1

→ F = 10^8 → 1

→ S = 1.544×10^6 → 64

ปรับการเปลี่ยนค่า cost → เปลี่ยนค่า auto-cost reference-bandwidth bandwidth-mbps (F = 100 Gb 1000 10Gb = 10000)

→ เปลี่ยน BW R(config-if)# bandwidth 64 (EIGRP & OSPF สามารถใช้ได้)

~ # ip ospf cost 15625

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

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 → เพื่อให้มีการส่ง default route update ไปใน ospf

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

method ① Manual Allocation : Admin assign เอง

for Staples

② Automatic Allocation : DHCPv4 auto assign address จาก pool และไม่มี lease time

③ Dynamic Allocation : ใส่ระยะเวลาที่จะใช้ ip ไว้ มี lease time → ถ้าหมด least time ก็ต้องขอ ip ใหม่

verify

show running-config | section dhcp

show ip dhcp binding

show ip dhcp server statistics

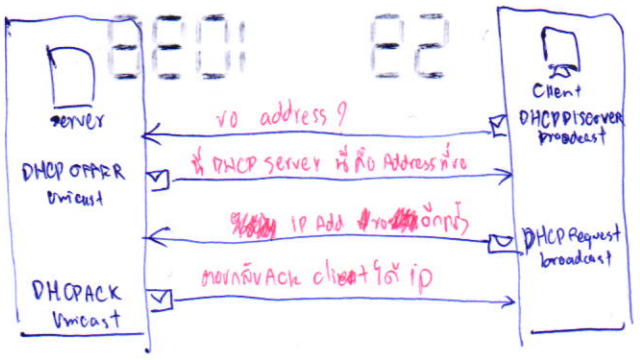
• PC ipconfig /all

debug same extended

config DHCP client → if)# ip address dhcp

if)# no shutdown

Operation



Config R(config)* ip dchp exclude-address 192.168.10.1 192.168.10.9
192.168.10.254

R(config)* ip dchp pool LAN-POOL-1

R(dhcp-config)* network 192.168.10.0 255.255.255.0
* default-router 192.168.10.1
* dns-server 192.168.11.5
* domain-name example.com
* end

• To disable dhcp no service dhcp

ถ้า ip ไม่ขึ้น → cmd → ipconfig /release → ipconfig /renew
→ หรือ set ip ในเครื่องเป็น dhcp หรือ static

ชื่อ-สกุล มุฮัมหมัด ริฎวาน อัลดีน กระดาษแผ่นที่ 4 รหัสนักศึกษา 69010098

for Staples

Chapter 7 Basic Switch Address Resolution Protocol

เปลี่ยน software → switches

▷ LAN Design → Borderless software network design : มีกฎทั่วไป :: - Hierarchical, - Modularity, - Resiliency, - flexibility

☐ ลักษณะ : ① 3-tier LAN Design ประกอบด้วย 1) Core 2) Distribution 3) Access ② 2-Tier LAN Design ประกอบด้วย 1) Collapsed Core/Distribution 2) Access

จุด Layer เป็น SW
- [1] Core → อุปกรณ์ที่รองรับ Bandwidth สูงๆ → ทำให้มี speed สูงขึ้นการเชื่อมต่อ Network } Layer 3 support, [Gig / 10 Gig Ethernet] } Redundant Components ⇒ สำรองเมื่อเสีย
- [2] Distribution → เชื่อมระหว่าง [1] & [3], Security Policy / Access control
- [3] Access ⇒ ต่อไปยัง end service, Port security, VLAN, [Fa(100m) / Gig Ethernet], Power over Ethernet (PoE) รองรับ 1 LAN หรือ ไม่ (1 LAN, 1 power line) ก็ได้

} Link Aggression → ทำให้ Bandwidth ให้ device เพิ่มขึ้น; Quality of Service (QoS)

■ เพิ่มความสามารถในการใช้ได้ LAN Bandwidth และประสิทธิภาพให้เต็มที่

- ตำแหน่งการวาง server ① Enterprise S. (รวมทั้งองค์กร) → ต้องตั้งที่ MDF (Main Distribution Facility : Core) ⇒ การผ่านไปข้างนอก ที่ใกล้กับมัน
  ② Workshop S. (เฉพาะกลุ่ม) → ต้องตั้งที่ IDF (Intermediate Distribution Facility : Distribution) ⇒ เชื่อมระหว่าง cross กับ access ที่ใกล้กับมัน

VCC (Vertical cross-connect) : optical fiber :→ MDF ↔ IDF
HCC (Horizontal cross-connect) : UTP → Distribution ↔ Access

- Collision detection issue (ปัญหาการตรวจจับการชน)
- Segmentation issue (ปัญหาการแบ่งส่วน) → ทำให้มีปัญหาการใช้งาน Network มีประสิทธิภาพที่ดีขึ้น
- Broadcast Domain Issue ⇒ ใน Network ต้องตลอด เช่น Broadcast หา MAC Address :: broadcast Network ควรมีขนาดเล็ก

■ Segmentation คือ process split single collision domain → smaller collision domain ลดจำนวน collision บน LAN segment :: L#2 device ไม่ใช่เป็น Bridges, Software

■ Broadcast domain ขึ้นหยุดที่ port ของ router L#3 ที่จะ filter segment broadcast ไม่ให้กระจายออกไปที่อื่น

▷ Software Environment

■ Software Operation
① Learning อ่านว่า frame เข้า Software หลังเรียนรู้ MAC Address ที่ต่อกับ port ไหน + reset Aging
② Aging อายุของ MAC. Address → ถ้าหมดเวลาให้ทิ้ง
③ Flooding ส่ง Frame ออกทุก Port ของ Software เมื่อ frame เป็น 1) Broadcast, 2) Multicast, 3) Unknow unicast (กรณีที่ Dest. ไม่อยู่ใน Routing table)
④ Forwarding ส่งไป Dest. (กรณีพบใน Routing table)
⑤ Filtering ไม่ส่ง frame ไป Dest. จาก port ที่เป็นทางไป Dest. (Source & Dest. บน Interface เดียวกัน) จะทำการ filter ทิ้ง

■ Software Method ① Store & Forwarding Software ⇒ Check CRC ว่า error ไหม → ถ้ามีก็ทิ้ง → ไม่มีก็ส่ง, auto buffer
② Cut-Through Software ⇒ Check เฉพาะบางส่วน (dest., source อย่างน้อย 12 byte แรก) [10 ms], No FCS & auto buffer

■ Software Domain ① Collision Domains ⇒ domain ที่เกิดการชนกันของข้อมูลบนสายพร้อมกัน " ดูที่ Software ในแต่ละ port "
② Broadcast ⇒ domain ที่ส่ง Broadcast → อยู่ domain เดียวกันจะได้รับ " ดูที่ Router ในแต่ละ port "

for Staples

▷ Basic Sw Concept & Config

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

☐ Basic Sw Config
- SW Boot Sequence = same router
- Preparing of Basic SW management : SW ไม่มี loopback เพราะจะเป็นกำหนด SVI (Software Virtual Interface) → Vlan
- Config Software Port → Duplex Communication : ① Full ② Half (SW ที่ต่อกันต้องเลือกเหมือนกัน)
  เข้าที่ intf → S(config-if) # duplex full → S(config-if) # speed 100 (เปลี่ยน speed)
  → Auto-MDIX : ถ้าต่อ software จะเชื่อมกันด้วย Cross-over หรือต้องการเปลี่ยนเป็นตรงๆ
  เข้าที่ intf → S(config-if) # duplex auto → S(config-if) # speed auto → S(config-if) # mdix auto

→ Verify Port Config
Show int f0/0, / startup-config, / running-config, / flash, / version, / history, / ip f0/0, / mac-address-table

☐ SW Security : Security Remote Access → SSH (Secure Shell) TCP port 22, telnet : TCP port 23
(change host name)

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

☐ SW Port Security → กำหนด policy ให้ MAC Address ไหนเข้า/ออกได้-ไม่ได้
S(config-if) # switchport mode access → # switch port-security → เลือกมา 1 ประเภท

Secure MAC Address → ① Static :: S(config-if) # switch port-security mac-address MAC-ADD
② Dynamic :: S(config-if) # switch port-security mac-address sticky → learn frame ที่วิ่งผ่านก่อน → record ไว้

การเพิ่มจำนวน MAC : # switchport ~~port-~~security maximum MAX

Violation mode : ① protect :: security violation protect mode
② restrict :: security violation restrict mode ⇒ ส่งไปเก็บข้อมูลโรงเกิดขึ้นแล้ว
③ shutdown :: security violation shutdown mode → default mode

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

Security Violation mode included : Protect, Restrict, and Shutdown.

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shut down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

for Staples

☐ Address Resolution Protocol (ARP) : ARP Cache เก็บ MAC Address ไว้ map จากการไปหา dest. (ถ้าไปทางข้างนอกต้องรู้ MAC gateway)

IPv4 : Classless [ต่อ P.1-2] : - Variable Length Subnet Masking [VLSM] : แบ่งจุด Network ไม่เท่ากัน :→ เริ่มจากอันใหญ่ → เล็ก
- Fixed ~ : แบ่งจุด Network เท่ากัน

Chapter 8 LAN Redundancy & Spanning Tree Protocol (STP)

▷ Issue with Layer 1 Redundancy :: ① MAC Address instability → MAC Addr. table จะไม่เสถียร เพราะเปลี่ยนแปลงบ่อย ② Broadcast storms → วนส่งไปทั่วไม่หยุด ③ Multiple frame transmission → start: unknown unicast → ทำให้ dest. ได้รับหลาย frame ทั้งที่ source ส่ง 1 frame

▷ STP → ทำหน้าที่ block port → block → ไม่ให้เกิด traffic วน เมื่อเกิดปัญหา

□ ขั้นตอน : ① หา Root Bridge = เลข Priority min Rule: [1] 1RB/1 Nw [2] 1 RP/1RB [3] 1 DP/segment
ส่ง BPDU (Bridge Protocol Data Unit) ↳ ส่ง RB & source [802.1D]
② หา path cost all ③ หา Root port → path cost min → อีกฝั่งจะเป็น Designated Port
④ ส่วน segment ที่มี path cost เท่ากัน → ดู BID min เป็น designated port → อีกฝั่งเป็น block port

ถ้าค่าใช้เปรียบเทียบ ① BPDU flag (*priority ต่ำสุด)
② BID น้อยสุด
③ Path cost <
④ Sender's BID <
⑤ Sender's Port <

□ Config : วิธีที่ I : S1 (config)# spanning-tree VLAN 1 root primary วิธีที่ II : S3 (config)# spanning-tree VLAN 1 priority 24576 (เพิ่มไปเรื่อยๆ)
(if S1, S2 เป็น RB) S2 (config)# spanning-tree VLAN 1 root secondary [verify] show spanning-tree]

□ หา Extended System ID : B. Priority (2 byte) = B. Priority (per VLAN) (4 bit) + Extended System ID (VLAN) (12 bit) + MAC Address (6 byte) : BID = 8 byte

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

Protocol	Standard	Resource Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s Cisco	Medium or High	Fast	Per Instance

• Rapid PVST+ → มี Alternate port (คือให้ block ไม่ได้ สามารถส่งข้อมูลได้บางส่วน)
↳ ทำการ set Edge Port @ port ที่ต่อ Host, router : -if)# spanning-tree portfast
↳ link type : port ที่เชื่อมระหว่าง software ต้องเป็น point to point : -if spanning-tree bpduguard enable → port ที่ไม่ต้องการให้ BPDU ไปด้วย
⇒ Config : S1 (config)# spanning-tree mode rapid-pvst → # int ที่ point-to-point → # spanning-tree link-type point-to-point

Chapter 9 VLAN & Inter VLAN

▷ VLAN = การ partition (แบ่งแยก: อย่างนะ: network แต่ broadcast domain เดียวกัน) Layer 2 ด้วย software จะ: ทำการจัดกลุ่มใน VLAN เดียวกัน

(*1) ถ้าทำ : เติม no หน้า → ไม่ได้ลบ ที่แยกทำ. no vlan num

□ ข้อดี : - security ดีขึ้น, - ลด cost, ประสิทธิภาพดีขึ้น, - broadcast domain เล็กลง, - มีประสิทธิภาพด้าน IT, - จัดการประยุกต์ง่าย [verify : show vlan breif]

□ in a Multi-switches Environment

• VLAN Trunk : set ที่ intf ที่เชื่อมต่อระหว่าง Switches ที่มี VLAN → can carry ข้อมูลได้มากกว่า 1 VLAN | สร้าง : I S (config)# vlan vlan_num → vlan)# name (ชื่อ)
II S # vlan database → (vlan)# vlan num name ชื่อ

• assign port ให้ vlan : เข้า intf → -if)# switchport mode access → # switchport access vlan num (*1)

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

- Verify : show vlan name ชื่อ, show vlan summary, show int vlan num

• Config : เข้า intf → -if)# switchport mode trunk [verify : show int f0/0 switchport]

• Tagging Ethernet Frames (IEEE 802.1q) : Ethernet Frame → | Dest MAC | Source MAC | Tag | Type/Length | Data | FCS | → Tag ที่ใส่กลุ่ม vlan เมื่อส่งผ่าน Trunk

▷ Inter-VLAN Routing → router set เป็น trunk โดยใช้หลักการ "sub Interface"

□ config : ① set basic routing (set ip add, no shutdown)
② R(config)# interface g0/0.10 → VLAN → -subif)# encapsulation dot1Q 10 → # ip address ip subnet-mask [verify : show vlan, show ip route, show running-config]

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

▷ VTP [msg : ISL or IEEE 802.1Q] → การจัดการ switches VTP ที่เป็นสมาชิกภายใน domain

□ Operation : - ตรวจสอบ VTP ที่ใช้ revision number 32 bit (0 - 4294927295) เพื่อดูว่าข้อมูล

↳ 3 mode : ① Server → สามารถสร้าง, remove, rename VLAN ทุกตัวใน domain ยกเว้น③
② Client → รับข้อมูล VTP มา process, ส่ง VTP msg ออกทาง Trunk
③ Transparent → สามารถสร้าง, remove, rename แต่ใช้เฉพาะตัวเอง, เป็นแค่ทางผ่าน

Feature	Server	Client	Transparent
Source VTP Message	Yes	Yes	No
Listen to VTP Message	Yes	Yes	No
Create VLANs	Yes	No	Yes
Remember VLAN	Yes	No	Yes

*Local significant only

□ Config : 2 แบบ สิ่งที่ต้องมี : 1) SW cisco 2) มี trunk เชื่อมระหว่าง switches 3) ตั้ง domain 4) มี 3 mode

① in global configuration S (config)# vtp version 2 → # vtp domain ชื่อ → # vtp password รหัสผ่าน → # vtp mode server | mode อื่น
② in VLAN configuration S(vlan) # vtp v2-mode ↗ [verify : show vtp status / counters] ↘ # vtp server | client | transparent

□ Pruning → จัดการไม่ให้ traffic ที่ไม่จำเป็นไป interface ที่ไม่จำเป็น โดย config ที่ interface ต่างๆ เพื่อ remove ข้อมูลที่ไม่ใช้
S(vlan)# vtp pruning → เข้า interface → S(config-if)# switchport trunk pruning vlan remove vlan-num

Private Internet address are defined in RFC 1918 :

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

▷ NAT → แปลง private ip ↔ public/real ip

□ Terminology : 4 type : ① Inside local Address (private ip) ② Outside local Address
③ Inside global Address ④ Outside global Address } → เพิ่มเติม

□ Type : ① Static : กำหนดตายตัว [map : 1↔1] → ① R(config)# ip nat inside source static local-ip global-ip
② Dynamic : มี pool ของ Global / Real ip [map : many↔1] : real ไม่ผูกติดกับใคร
③ PAT (Port Address Translation) → port ที่ต่อร่วมกับ network address [map : many↔1] }
(1.1) ip nat pool ชื่อ start-ip end-ip {netmask netmask | prefix-length}
(1.2) set ACL (1.3) ip nat inside source list ACL-num pool ชื่อ overload [pool เหมือน 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 Address) (1.1) สร้าง ACL (1.2) ip nat inside source list ACL-NUM interface f0/0 overload
□ verify : show ip nat translation

ชื่อ-สกุล บุญมนิต รุ้งทพ ชัยอนันต์ กระดาษแผ่นที่ 5 รหัสนักศึกษา [illegible]

for Staples

Chapter 11 EIGRP IPv6 Routing

Dynamic Routing Protocol → Interior Gateway P. / Exterior Gateway P.

Interior Gateway P. → Distance Vector Routing P. / Link State Routing P.

	Distance Vector Routing P.		Link State Routing P.		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGPv4 for IPv6

▷ EIGRP (Enhance IGRP)

□ Characteristics (ลักษณะเฉพาะ)

• Basic features △ cisco-proprietary (ใช้เฉพาะ protocol ของ cisco) เปิดใช้ใน 1992
⊕ สร้าง classless version of IGRP ⊕ ทำงานได้ดีกับ Network หลาย protocol, เหมาะกับ ที่ใช้งาน cisco router เป็นหลัก

✓ Dual (Diffusing Update Algorithm) = การันตี loop-free & backup path ทั้งหมดจาก routing domain → หา best path
(การทำงาน ≈ OSPF เรื่อง router) → ทำให้ routing ทำงาน very fast convergent (มี convergent time < ของ OSPF) รวมทั้งหา backup path (ทำให้ทำงานเร็วขึ้น → ถ้า link down จะเลือก path ใน backup ขึ้นมาแทน)

✓ Establishing Neighbor = เชื่อมความสัมพันธ์กับ direcly connected EIGRP routers
Adjancercies = Adjacencies are used to track the status of these neighbor

✓ Realiable Transport Protocol = RTP provides dilivery of EIGRP Packets to neighbors.
- RTP and neighbor adjacencies are used by dual (DUAL) (ในการ Maintain)

✓ Partial and bounded = update เฉพาะส่วนที่มีการเปลี่ยน รวมไปถึงการ อัพเดตไปในเฉพาะส่วนที่มีการเปลี่ยน ∴ update ลดลงจาก RIP (update ทั้ง routing ตลอดเวลาไม่ว่าจะ down หรือไม่)

✓ Equal and Unequal cost = ช่วยให้ admin ดูแลระบบ เพื่อกระจายการรับข้อมูลในเราเตอร์ให้ดีขึ้น (ถ้า cost ≠ แต่ทำ load balance ได้)
Load balancing

△ ใช้ protocol-dependent modules (PDMs) เพื่อรองรับ protocol ที่หลากหลาย เช่น IPv4, IPv6, legacy protocol IPX and Apple Talk
→ เก็บ shortest path and backup shortest path (เก็บ topology ≈ OSPF ≠) EIGRP เลือก Successor ผ่าน Dual

△ PDMs รับผิดชอบ:
⊖ maintain EIGRP neighbor and topology table (Neighbor Table → สร้าง Topology Table → ใส่ routing table เพื่อ routing
⊖ คำนวณ metric ที่ใช้ DUAL ⊖ เชื่อมต่อ DUAL และ routing table
⊖ implement filtering and success 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 ที่ส่งของ EIGRP

△ ไม่ได้ทั้งหมดของ RTP Packet จะส่งได้น่าเชื่อถือ (msg ≈ OSPF)
⊖ Realiable packet require explicit (ชัดเจน) ack จาก dest. ⊖ update query reply
⊖ Unreliable packet do not require ack จาก dest. ⊖ Hello, Ack

(protocol 88 ใน transport layer)

△ รองรับ authentication (no encrypt routing update) แต่ ไม่ recommend (เป็นเรื่องของเรา) (authen ≈ RIPv2, OSPF)

○ Packet Type routing update or queries EIGRP multicast IPv4: 224.0.0.10 (01-00-5E-00-00-0A), IPv6

① Hello → ทำให้ adjencencies ระหว่าง router 2 ตัวที่เป็น neighbor กัน, ไม่ต้องตอบ responce, ส่ง unrealiably
② Update → update info. ของ dest, update info ของ routing ไปให้ neighbor router
③ Acknowledgement → พอได้รับการ update ก็ตอบ ACK
④ Query → request info. routing จาก neighbor router
⑤ Reply → หลังจากได้รับ query ก็ reply
} เผื่อต้องการ info ของ routing เพิ่มก็ query ไปถาม router ที่อยู่ข้างๆ หรือ reply ตอบกลับมาว่ามีไหม

□ Implement EIGRP for IPv4

△ Automomous System (AS) is a collection of Network ภายใต้การดูแลของ single Authority (อ้างอิง RFC 1930)
↳ AS Number → ใช้ exchange routes between AS
→ managed by IANA & assigned by RIPs to ISPs, Internet Backbone Providers, and institution (สถาบัน) ที่เชื่อมต่อสถาบันอื่น
→ 16 bit: 0-65535 → since 2007, 32 bit: over 4 milion

△ verify: show ip eigrp neighbor,
show ip protocols,
show ip route

△ Configure: R(config)# router eigrp AS-# (≈ router-id ของ OSPF)
show ip protocol ← R(router-config)# eigrp router-id → ถ้าไม่กำหนดไว้ใช้ loopback interface → IPv4 Address ที่สูงสุดที่ active
R(router-config)# network network-number [wildcard mask] → มีหรือไม่มีก็ได้
R(router-config)# passive-interface type number [default]: ไม่ส่ง update ไปที่ Interface ในระบบ LAN, G, F (ส่วนใหญ่ Serial) (มีหรือไม่มี)

for Staples

for Staples

Operation

- Initial Route Discovery (ค้นหา) ① R1 say Hello กับ Neighbor router ② R2 อาจจะส่ง hello แล้ว update กลับมา ③ R1 ตอบ ACK & update info. ④ ใช้ DUAL คำนวณ best route and update routing table

Metric : BW [lowest], Delay [ระยะ], Reliability [worst], Load [worst] ดูค่า value : show interface

K1=1, K3=1, K4=0, K5=0, K2=0

Default Composite Formula : metric = [K1*bw + K3*delay]*256 = $\left[\left(\frac{10,000,000}{bw}\right) + \left(\frac{\text{sum of delay}}{10}\right)\right] \times 256$

Complete : $= \left[K1*bw + \frac{(K2*bw)}{(256-load)} + K3*delay\right] \times \left[\frac{K5}{reliability + K4}\right]$

- R(config-router)# metric weight tos K1 K2 K3 K4 K5 - set BW : interface → R(config-if)# bandwidth kilobits-bw-value

- DUAL and the topology table (ใช้ FSM (Finite State Machine) ในการเลือกเส้นทาง) → show ip eigrp topology [all link], show ip route
+ Successor(s) [router ไป dest. สั้นสุด] = neighbor router ที่จะเลือกทางไป dest. ที่มีค่า min น้อยที่สุด
+ Feasible Successor (FS) [มีได้ไม่ ∝ Fesible Condition] (if (RD < FD) → FS) = Backup path (เส้นทางสำรอง)
+ Reported Distance (RD) [distance ที่ neighbor ตัวอื่น report distance มาให้เรา] = "advertised distance"
+ Feasible Distance (FD) [distance ไปหา S] = ค่า ~~dest.~~ distance ที่คำนวณไปหา dest. ทาง เป็นค่า cost lowest → dest.

IPv6

IPv4 Issue

- Need for IPv6 → แก้ปัญหา IPv4 มีจำนวนจำกัด (private ip, NAT)
- การใช้งานร่วมกัน (coexistence)
  - Migration IPv4 → IPv6 Techniques :: ① Dual Stack = run ทั้งคู่ ถ้าเปลี่ยนไม่ได้กระทบ user
    ② Tunneling (ออกไปใช้ v6 แต่ care ไม่ support) :: เปลี่ยนตามแต่เรา หลังวิ่งผ่าน v4 เหมือนเดิม
    ③ Translation = (คล้าย NAT) = IPv6 ↔ IPv4

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

- ออกแบบวิธีการเขียนแบบสั้น IPv6

Rule 1 - Omit Leading 0s = ในแต่ละ partition "0" ที่อยู่ด้านหน้าตัดทิ้งไป 000X, 00XX, 0XXX (0-F)

Rule 2 - Omit All 0 segment = แทน segment ที่มี 0 ติดกันยาว ด้วย "::" ใส่ได้ที่เดียว only

Type of IPv6 Address

- IPv6 Address type ① Unicast : ⊖ Global Unicast (→ 3 bit แรก: "001" or "2000::/3") ⊖ Link-local (→ ครั้ง interface ที่อยู่ติดกัน (@local เท่านั้น)) ⊖ Unique Local
  - static config ← ; ↳ ipv6 address ipv6-address/prefix-length → no shutdown
  - Link-local: ↳ ในช่วง FE80::/10 = ใช้งานเข้าได้เฉพาะ link-local (ใช้ได้เฉพาะใน local)
  ② Multicast
  ③ Anycast = ส่งให้หลาย advice
- IPv6 Prefix Length = 0-128, Most LAN is /64 เพราะว่า LAN เล็กสุด 64 bit

IPv6 Routing

- config static route
  R(config)# ipv6 route ipv6-prefix/prefix-length {ipv6-address | exit-interface} → ต้องใส่ (next hop address | exit-interface)
- * ใส่ก่อน config ใช้งาน routing ipv6 = ipv6 unicast routing เพื่อการเปิดใช้งาน
  - verify : show ipv6 route static, show ip route ipv6, show running-config | section ipv6 route
  - Default Static IPv6 route
    R(config)# ipv6 route ::/0 {ipv6-address | exit-interface}
  - verify : show ipv6 route static
- Config EIGRP for IPv6

R(config)# ipv6 unicast-routing

R(config)# ipv6 router eigrp AS-X

R(config-router)# eigrp router ip 0.0.0.0 → รูปแบบ IPv4

R(config-router)# no shutdown

- network command : เข้า interface → ipv6 eigrp AS-X
  แต่ passive-interface ต้องทำใน global config เหมือนเดิม
- verify : show ipv6 eigrp neighbor, show ipv6 protocol, show ipv6 route