

for Staples

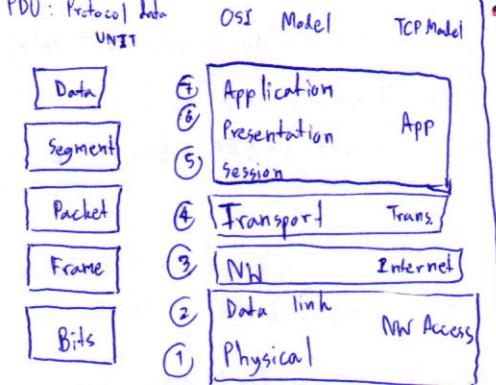
Chapter 1 Network Overview

- Network diagrams = โครงสร้าง NW ก่อกร้าว หรือ แม้กร้าว เชื่อมต่ออย่างไร ?
- 2 type :: ① Physical → ผ่าน port / interface (File Transfer, Email, E-mail, Internet Control Message Protocol) ⇒ ping IP + Command ② Logical → ผ่าน IP
- Network protocol ⇒ TCP / UDP, FTP, ARP, SMTP, POP3, IMAP, ICMP
 - (Address Resolution Protocol) ⇒ map router IP addr. หรือ MAC addr. เป็นอย่างไร
- NW Addr. :: ① IP addr. (Logical addr.) @ L3 ② Mac addr & Physical Addr. @ L2 ③ Port Number (Service addr.) @ L4 (Protocol or media)
- Components of Network → HW → NW device จำแนก 3 type
 - ① end devices = อุปกรณ์สุดท้ายที่เชื่อมต่ออยู่ใน NW (NW Representation)
 - ② intermediary devices = อุปกรณ์ที่เชื่อมต่อ NW access devices, Internetworking devices, Security devices
 - hub, switch, router
 - hub, repeater @ L1 ⇒ จังหวะต้องพัฒนา Collision : QoS CSMA / CD (Carrier Sense Multiple Collision Avoidance)
 - Switch, bridges @ L2 ⇒ Learning / Flooding / Filtering / Forwarding / Aging
 - Routers @ L3 ⇒ Routing
 - ③ network media = สายเคเบิล เช่น Copper, Fibre Optic, Wireless [LAN straight cross WAN]
- Type of Networks → SN
 - ① Switch เครือข่าย local ② router เครือข่าย มีประสิทธิภาพมาก
 - size
 - ① Small home nw ⇒ สำหรับบ้านเดี่ยว ② small office / Home office ⇒ config ตามสถานที่ตั้งของตัวเอง
 - ③ Medium to Large NW ⇒ สำหรับองค์กร 100-1000 ตัวๆ ④ World Wide NW หรือ internet infrastructure
 - ① Local Area NW (LAN) ผู้ดูแล admin อยู่ใน policy/nw อยู่ Ex. ห้องนี้ ↔ สำนักงาน
 - ② Wide Area NW (WAN) ผู้ดูแล admin
 - ⇒ Metropolitan Area NW (MAN), Wireless LAN (WLAN), Storage Area NW (SAN), Personal Area NW (PAN)
- Reliable Network ① fault Tolerance ⇒ มี冗余 ② Scalability ⇒ สามารถเพิ่มขนาดได้ ③ Quality of Service (QoS) ⇒ ให้บริการ QoS ที่ต้องการ

Layer with TCP/IP & OSI Model

- ③ Security ⇒ ต้องการ limit ภัยคุกคาม ④ Quality of Service (QoS) ⇒ ให้บริการ QoS ที่ต้องการ

PDU: Protocol Data Unit

Type of Connection in a LAN

- จังหวะ (UTP cat5) : ① BW = 100 Mbps ② ระยะ 100 m (carrie hub, repeater, switch)
- 2 type :: ① cross ② cross → ต้องต่อสาย (เช่น SN---hub, pc---router)
 - ⇒ DWAN Connection ⇒ ต้องต่อสาย router
 - ↳ 2 สาย ↳ DCE (female) ⇒ รับ command clock rate 56000
 - ↳ DTE (male)
 - ⇒ AUX console (Rollover Cable) ⇒ router : " " ; PC
 - ⇒ manage command
 - RJ-45-to-DB-9 Adapter labeled TERMINA

Chapter 2 Basic Router ConfigurationCisco IOS (Internetwork Operating System)

- function ① Addressing ② Interface ③ Routing

- ④ Managing Resource ⑤ Security ⑥ QoS

Router & Switch Boot Sequence

- ROM ① POST (Power On Self Test) ⇒ Check hardware use
- ② Ram boot loader SW
- ROM ③ Boot loader does low-level CPU initialization mini IOS
- ④ — initializes the flash file system
- ⑤ — locates & loads a default IOS an run in RAM

Port Addr. : หมายเลข (Internet Assigned Number Authority : IANA)

0-1023 : requesting entities "well known ports" destination port

49,152 - 65,535 : dynamic or private port "Randomly generate" source port

1024-19,151 : registered port = public หมายเลข

(Data) 20: FTP, 21: FTP (control), 25: SMTP, 53: DNS, 80: WWW HTTP, 81: HOSTS 2 Name Server

logical Addr. : IP addr. (IPv4) @ L3

- 5 class :: A,B,C,D,E, → reserved (902) หมายความว่า max 902 workstation required

- หมาย NW/node or COM ⇒ ให้ logical name (domain names) & ip unique

Physical Addr. : MAC addr.- Ethernet : 48 bit $\text{addr} = 12 \text{ in } \text{hex} \rightarrow 0x\text{XXXXXXXX}$

- มาตรฐาน IEEE ⇒ ต้อง 3 byte (24 bit) code "Organizationally Unique Identifier (OUI)"

→ 2 byte → ① ที่ 1 MAC ที่รักษาไว้ NIC หรือ Ethernet device อยู่ → 96 OUI 3 byte หรือ

② ที่ 2 MAC ที่ same OUI แต่ต้อง unique ใน 3 byte อย่างไร

for Staples

Message Delivery

- Unicast = หมายความว่าส่งไปยังหนึ่งเดียว ที่ NW ต้องมีที่อยู่

- Broadcast = หมายความว่าส่งไปยังทุกคน ที่ NW ต้องมีที่อยู่

→ broadcast ip/rw = 255.255.255.255 = FF-FF-FF-FF-FF-FF

- Multicast = หมายความว่าส่งไปยังกลุ่ม & ที่ NW ต้องมีที่อยู่

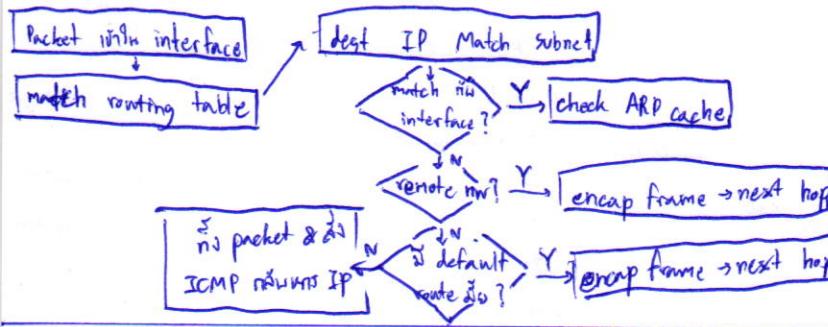
→ หมายเลข 01-00-5E-xx-xx-xx



- Accessing a Cisco IOS Device
 - ① Console port
 - ② Telnet
 - ③ Secure Shell (SSH)
 - ④ Aux Port
 - ↳ Terminal Emulation Program :: PuTTY, Tera Term, SecureCRT, Hyperterminal, OS X Terminal
- Navigating the IOS → 2 mode :: ① user > ② privileged (enable) *
- The Command Structure
 - ① Context Sensitive Help :: ?
 - ② Command Syntax Check = enter > show interface no
 - ③ Hot keys and shortcut
 - ④ IOS Examination Commands → show ...
- Getting Basic
 - ① ~~no~~ to host name
 - ② ~~no~~ interface addressing
 - ③ ~~no~~ interface address
 - ④ ~~no~~ config + n. reboot
 - ⑤ ~~no~~ save config
 - ⑥ ~~no~~ copy running-config startup-config
 - ⑦ ~~no~~ banner msg. Router(config) > banner motd > text
 - ⑧ ~~no~~ Securing Device Access :: Enable password / secret, console pass, VTY Pass, ~~no~~ Encrypting Pass display
- ③ Addressing Devices
 - 1) from 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
- ④ Verify Connectivity → configuration section, include, exclude, begin
 - Router > show running-config → get config details
 - show startup-config → get set config details
 - show ip route → get routing table
 - show interface
 - show ip interface brief → show info on interface only
 - traceroute
 - ping
 - PC > ping
 - tracert
 - route ping
 - nslookup
- ▷ Best Path: lowest metric (cost)
 - Dynamic routing protocol #
 - ① Routing Information Protocol (RIP) = HW. hop
 - ② Open shortest path first (OSPF) = BW aware, A
 - ③ Enhanced Interior Gateway Routing Protocol (EIGRP) = BW, delay, load, reliability

Chapter 3 Static Routing & Dynamic Routing Protocol

- Functions of Router → Characteristics :: ① Topology ② Speed ③ Cost ④ Security ⑤ Availability ⑥ Scalability ⑦ Reliability
 - ▷ Packet Forwarding Methods ① Process switching = in packet $\xrightarrow{\text{CPU}}$ router \rightarrow process @ CPU → on interface True?
- Connect Devices
 - ▷ Default gateway → hub ① first usable host (0.1) ② last usable host (0.254)
 - maximum NW 254
 - ▷ Enable IP on a HOST :: ① statically assigned IP addr. (Dynamic Host Configuration)
- Switching Packet between NW ② Dynamically → can assign ip to when nw is DHC Protocol
- Process :: in dest ip (L3) \rightarrow in routing table \rightarrow in mac table, \rightarrow MAC addr. \rightarrow dest MAC (L2)
- Path Determination



- R (config)* interface G 0/0
- if* ip address 172.16.1.0 255.255.255.0
- no shutdown
- R1 (config)* ip route 172.16.1.0 255.255.255.0 172.16.1.2 mask 1 255.255.255.252 s0/0/0 255.255.255.252
- ② Dynamic Routing Protocol → auto
- ③ EGP (Exterior Gateway Routing Protocol) :: BGP
- ④ IGP (Interior :: RIP, OSPF, EIGRP, IS-IS)

- ③ Summary ④ Floating = break up
 - Router (config)* ip route nw -addr. subnet-mask ip-addr. [exit-interface]
 - ▷ Classful Addressing \rightarrow update own class
 - ▷ Classless Inter-Domain Routing
 - ▷ Summarization = Router : 0.0.0.0/8 \rightarrow 172.16.0.0/16
 - ▷ Fixed Length Subnet Masking :: ① prefix mask - prefix in 128bit
 - ② 11111111.11111111.11111111.11111111

for Staples

Chapter 4 Distance Vector Routing Protocol RIP Ver 1

■ Dynamic Routing Protocol

▫️ share info routers, auto update routing table when topology change (เมือง), in best path
 ▫️ purpose : remote nw (nw ไม่ใช่เรา), นำ路 routing info, ทาง best path ไป dest. nw, can in new best path in path list

▫️ component : ① Algorithm : ถือว่า routing info & best path

② Routing protocol msg. : บันทึก neighbor & รับ routing info. (best path)

▫️ ผู้กำหนด config

Reqired a.3 admin

Topology Change

Scaling

Security

Resource usage

Predictability

■ Classifying Routing protocols

(config AS)

DRP

(switch AS)

Interior Gateway Protocol (IGP)

Distance Vector P.

- ️ Demand Vector [distance, direction]
- ️ incomplete view ของ nw topology
- ️ periodic update (เรียบ)

RIP (Routing Info.P.)

for Staples

RIP V.2

IGRP (Interior Gateway)

Routing P.

Link-State P.

- ️ Complete nw topology (มีอยู่ทั้งหมด)
- ️ update มาก periodic

(Open Shortest) Path First

OSPF

IS-IS (Intermediate System)

Exterior Gateway Protocol (EGP)

Border Gateway Protocol (BGP)

- ️ Autonomous system (AS) ผู้ดูแล router เอง มี authority ของ nw single authority
- ️ 1 นโยบาย or กฎชาติ

EIGRP (Enhanced Interior Gateway Routing P.)

▫️ 2 type

① Classful routing P. → update แม่ class ที่มี subnetmask ใหม่ routing update

② Classless routing P. → ใหม่ subnetmask ใหม่ routing update

▫️ Convergence : ต้องรอ when routing table ของ all router ต้องเท่ากัน (เมืองต้องเท่ากัน)

▫️ 2 type : slower : RIP & IGRP, Faster (ใหม่ update when information เปลี่ยนแปลงตัวต่อตัว) : EIGRP & OSPF

▫️ Routing Protocol Metrics

▫️ Metric : ระยะทาง/m กม. ถึง dest. NW ที่เป็น best path ตาม rule Hop count, BW, Cost, Delay, load, Reliability

▫️ Load balancing : nw จำนวนมาก > 1 ตัว metric ใหม่ → ต้องการ 2 ตัว metric ใหม่ ให้มีความต่างกัน

▫️ Administrative Distance of a Router (AD) → กำหนด protocol ใหม่ routing

▫️ หมายเหตุ : หมายความว่า กำหนด route ของ particular (เฉพาะ) route,

Route Source	Connected	Static	Internal EIGRP	OSPF	RIP
AD	0	1	90	110	120

EIGRP	External BGP	IGRP	IS-IS	External EIGRP	Internal BGP
Summary route					

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

▫️ Distance Vector Technology ได้ 2 ข้อดีคือ ① Vector or direction, ไม่ต้องรู้ topology ทั้งหมด ② Distance to final dest. (cost)

▫️ ข้อเสีย : periodic update, neighbor (เพื่อน), broadcast (255.255.255.255) update, ให้ routing table ทั้งหมด update

▫️ " เวลา Routing Protocol : ต้องเช็ค DV ใหม่ๆ ? ④ Time to convergence → ต้องให้ steady state ของ routing table นั้นๆ แต่ต้องใช้เวลา

▫️ Scalability ของระบบ ③ Resource usage ④ Implementation & maintenance

▫️ NW Discovery (ค้นหา) (ใน basic config ใหม่)

▫️ 3 stage ① Cold State : Router Initial Start up

② Initial Exchange of Routing info. สำหรับการ exchange ใหม่ๆ

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

+ ณ ตอน ต้องรู้อะไรบ้าง?

for Staples

■ Routing Table Maintenance

▫️ Periodic update : RIP update timer (default 90s), Invalid timer (info. ไม่ถูก) (default 180s)

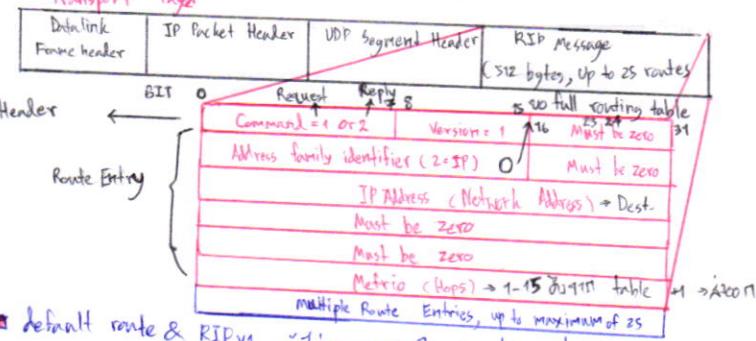
▫️ Hold down timer (ต้อง down → hold 10 วินาที ไม่ติดต่อ) (default 180s), Flush (ลบ) timer (default 240s)



- Bounded convergence Update: EIGRP → update 10-15ms
- Triggered Update → update every 30 seconds
- Random Jitter → If two routers have multiple access routers, randomization → if no update triggered: Random
- Down standard DV:** ① Routing Loops too when ~~intf~~ link down กรณีต้องการตัด link ที่ไม่ใช่ interface ให้ตัด掉 link ที่ไม่ใช่ interface แทน
- RIPv1 RIPv2 IGRP EIGRP
- spec convergence slow slow slow fast
- scalability - size nw small small small large
- use of VLSM X ✓ X ✓
- Resource usage low low low medium
- implementation & maintenance simple simple simple complex

RIP Version 1 AD = 120

- Properties:
 - Classful, DV = metric + hop count
 - hop count > 15 unreachable
 - update broadcast every 30s
 - encapsulated in UDP segment over source & dest port 520
 - Transport layer



- default route & RIPV1 maintains routing table (original route protocol) → 200 default route
 - R(config)* ip route 0.0.0.0 0.0.0.0 5.0.0.1
 - default info originate command → into update ที่ Au rip ที่ Au
 - R(config-router)* default-information originate [static ↔ dynamic]

Msg 2 type

- ① Request → to routing table
 - Tel intf config ที่ Au config n. update
- ② Response → to info. var routing table
- ipaddr. ไม่สามารถ class A,B,C
- Basic RIPv1 Config ③ in basic config

④ ที่ Au router rip R1(Config)* router rip

- + ที่ Au RIP + R1(Config)* router rip
- Verification & trouble shooting (troubleshooting):
 - passive intf command (ที่ Au update intf fib)
- Automatic Summarization: RIP Auto Summarizes classful nw → ไม่สามารถ size routing table; sum size routing table, single router ไม่สามารถ support multiple route table
 - โดยที่ Au support discontiguous nw (Major nw แต่ minor แต่ ไม่ต่อเนื่อง) → origin load balancing
 - boundary Routers: summarize RIP subnet from 1 major nw other
 - Processing RSP update กรณี & กรณี update Tel intf ที่ Au classful ไม่สามารถ

→ Y: update subnet nw ที่ Au 172.16.10
→ N: update classful nw ที่ Au 172.16.0.0

Chapter 5 | RIP Version 2 & Access Control Lists

RIP v1	VS	RIP v2
Classful (ไม่ support subnet mask, ไม่ support VLSM)	not support contiguous subnet	Classless (update subnet mask, support Variable Length Subnet Masking (VLSM), Support Route summarization)
not support VLSM b/c ที่ Au sub net mask (255.255.255.255)		
routing update + broadcast		Routing Update → Multicast
98 timer จารึก routing table		
98 split horizon or split horizon with poison reverse		
98 triggered update		
max hop count = 15		

configuration RIPV1

- ที่ Au virtual interface กรณี config รันติง กรณี update control
 - loop back intf → ping Tel → ip virtual intf → reply กรณี
 - Null intf → กรณีที่ Au ต้องการ null intf → กรณี null intf → packet discard กรณี timeout
 - static route & null intf → null intf กรณีที่ Au มี static route

R(config)* ip route summary-static-route subnet-mask Null 0



for Staples

- Route redistribution (ตัวต่อตัว) \rightarrow overfix rip ถ้า static ต้องตั้งให้同 ip หรือ static ให้ static | Reconfig router & redistribute static
- Verify & Test Connectivity : show ip interface brief, ping (wait, timeout, = timeout), traceroute
- RIPV1 : classful, แบ่ง subnet mask, summarize network @ major network boundaries, if network is contiguous & RIPV1 config
- routing table : debug ip rip , ดูว่า RIPV1 จะตัด subnet mask ออกใน network address convergence ต้องต่อ

▪ RIPv2

- Config
 - Enabling & verify RIPv2
 - Config RIP \rightarrow RIPv1 \rightarrow config V1 & V2 but ต้องไม่ V1
 - \rightarrow RIPv2 \rightarrow can sum & distribute V2
 - Auto-Summary & RIPv2 \rightarrow auto sum route @ major network boundaries
 - \rightarrow sum route คือ subnet mask ที่อยู่ใน classful subnet mask
 - disabling Auto-Summary : no auto-summary b.c. when the network topology is contiguous
- VLSM & CIDR
 - verify info. ที่ sent by RIPv2
 - VLSM \rightarrow ระบุ network address & subnet mask
 - CIDR \rightarrow 95 supernetting (= bunch up contiguous classful network into a single network)
 - \rightarrow Verify

▪ Access Control List = รากฐานของ ACL \rightarrow ตรวจสอบ \rightarrow check source \rightarrow dest หรือไม่?

- \Rightarrow open conversation
- \Rightarrow ก่อจราจร (เช่น FTP) หรือไม่?

▪ Packet filtering \rightarrow ที่ dest, source @ L2 @ protocol mts ③ ที่ network mts \rightarrow ไม่อนุญาตหรือ block ที่?

* Operation \rightarrow กำหนด sequence statement

\rightarrow last statement คือ implicit deny \rightarrow block \rightarrow discard

▪ Standard IPv4 ACLS vs Extended IPv4 ACLS

- | Standard IPv4 ACLS | vs | Extended IPv4 ACLS |
|---------------------------------|----|------------------------------------|
| - Check source addr. | | - Check source & destination addr. |
| - อนุญาตหรือปฏิเสธ โปรโตคอล | | - อนุญาตหรือปฏิเสธ โปรโตคอลเฉพาะ |
| - number ACL : 1-99 & 1300-1999 | | - Number ACL 100-199 & 2000-2699 |

* Wild card \rightarrow invert your subnet mask

\rightarrow 0⁰ match/fixed, 1¹ ignore/offset

\rightarrow กำหนด set ของ ip ① ไม่ต้องมี bit ใดๆ ก็ได้ที่ Wildcard mask นั้นๆ \rightarrow 0

(match range) ② bit ใดๆ ก็ได้ 1

\rightarrow ณ Wild card ของ subnet = 255.255.255.255 \rightarrow subnetmask

\rightarrow keyword \rightarrow 0.0.0.0 = match all ที่ Host

\rightarrow 255.255.255.255 = ignore all ที่ any

* Guideline for (3ps) \rightarrow one ACL / protocol \rightarrow ctrl traffic flow on intf, ACL ต้อง define โปรโตคอล enable on intf

ACL creation \rightarrow one ACL / direction \rightarrow ctrl traffic in + direction at time on an intf, 1ACL ctrl in & out bound traffic

\rightarrow one ACL / interface \rightarrow ACL ctrl traffic for an intf, Ex. Goto

* where \rightarrow Extend ACL : @ close source \rightarrow standard ACL ; @ close destination

* Config ACLs \rightarrow standard

\downarrow number

\downarrow ๐๐

- verify

- securing VTY port \rightarrow overrule number permit 192.168.1.1 ๗๗๗

\rightarrow Extended : filter : source/dest. addr., protocol, port number.

for Staples



Chapter 6 OSPF & DHCP

→ [info.all](#)

for dijkstra

- Link-state Routing Protocol : վերաբերությունը հաջող է complete map այս NW topology իւնո՞ւ → մոտավոր քայլություն (SPF) ալգорիթմուն
մասին ① large nw, ② fast convergence ③ administration է
 - իւնո՞ւ update ① learn info. աջ լինք ② say hello neighbors ③ լուր այս լինքուն Link-state Packet (LSP)
④ router flood LSP լուր այս լինքուն ⑤ router լուր այս լինքուն db (լուր տեսք)
 - իւնո՞ւ ① հայտնի տոպոլոգիա մաքս կառն շատ քայլություն (3) LSP սեն այն առանձին տոպոլոգիա
+ adding OSPF → routing table
② հայտնի տոպոլոգիա մաքս կառն շատ քայլություն (3) LSP սեն այն առանձին տոպոլոգիա
(գույքը հայտնի է → այս տարրը կառն շատ քայլություն) ④ hierarchical design (NW partition) → սեր ռեսուրս եօն, բաժանություն Area
իւնո՞ւ ① զայր պահանջուն այս լինք-ստաց ② զայր CPU պահանջուն ③ մուշ է LSP մաք 98 BW այս 77

OSPF (ADL 110)

- ↳ 3 table : ① Neighbor [show ip ospf neighbor] ② Topology (map) [show ip ospf database] ③ Routing (shortest path) [show ip route]

Message → Encapsulating : MAC Dest. + Multicast : 09-00-SE-00-00-05 or 09-00-SE-00-00-06

Protocol field = 89

- type OSPF Packet :
 - : 01 Hello → m/m ras (default : multiaccess & point-to-point m/m), m/m so s.
 - : 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) → receive - T/T 29

operation: សំណើនាំ ① Down state (ចុះឱ្យ) → ② Init state (ចុះឱ្យ hello) → ③ Two-way state (មួយដៃ hello)
 → Exist state → Exchange state → Loading state → Full state (រាយការពីរបាល update ឬចុះឱ្យសំណើនាំ)

Config Single-Area OSPF v2 [router ospf] process-id → 1-65,535, DU locally significant

R(config-router) > router-id 1.1.1.1 → 它会 set config 为 loopback, active interface ip 地址 but 然后 global 地址

Router ospf process-id
network network-address wildcard-mask area area-id

OSPF cost \rightarrow 95 BW minmt [default reference BW = 10^8]

$$\text{cost} = \frac{10^3 \text{ lps}}{\text{Gb}} \quad \boxed{10 \text{ Gb Ethernet} = 100 \times 10^3 \rightarrow \text{cost} = 1}$$

$$\text{inf BW lops} \xrightarrow{\quad \rightarrow \text{Ob} \quad \text{or} \quad = 10 \times 10^8 \quad \rightarrow \quad \text{or} \quad = 1} \\ \xrightarrow{\quad \rightarrow \text{Fast} \quad \text{or} \quad = 10^8 \quad \text{or} \quad = 1}$$

$$\rightarrow \text{processing cost} \quad \xrightarrow{\text{Serial}} x = 1.544 \times 10^4 \rightarrow n = 64$$

→ plausibel ref Bh

→ maximum BW = R(config-if) × bandwidth 64 (EIGRP & OSPF can 98%)

→ 沒有設定 cost: → ip ospf cost 15625

Verify ospf [show ip ospf neighbor, show ip protocol, show ip ospf interface brief, show ip ospf]

DHCP (Dynamic Host Configuration Protocol) for config a host via auto (give ip, subnet mask, default gateway)

- ## ① Manual Allocation : admin assign 10J

- ② Automatic Allocation : DHCP will auto assign addr. from pool & bind lease time

- ③ Dynamic Allocation : 分配する時間 ip が lease time → 経過 lease time の間で ip が失われる。

Chapter 7 : Basic Switch Address Resolution Protocol

► LAN Design → Borderless sw nw design : ingress :: - Hierarchical, - Modularity, - Resiliency, - Flexibility

* Collision detection issue (碰撞検出問題)

▪ Segmentation issue (ចំណាំ ឬ ឈើកិច្ច) → រាយការណ៍ នូវការបង្កើត

• Broadcast frames issue: \rightarrow no information broadcast on MAC Addr. :: broadcast NW information

- Segmentation is process split single collision domain \rightarrow smaller collision domain on LAN segment = LAN device group

- Broadcast domain: Swiching port but. router (L3) filter/filter/segment broadcast traffic to other ports

► SW Environment

- SW Operation
 - ① Learning :: if frame \rightarrow SW \Rightarrow MAC Addr. \rightarrow store port link resct Aging
 - ② Aging :: $\text{age} \geq 300$ MAC Addr. \rightarrow if $\text{MAC} \rightarrow \text{null}$
 - ③ Flooding :: if frame coming port was SW when frame \rightarrow 1) broad cast, 2) multicast, 3) unknown unicast
 - ④ Forwarding :: to dest. (with w/f table)
 - ⑤ Filtering :: if to SW frame \rightarrow 1) dest. on port \neq source dest. (source & dest. with same interface)
 - ⑥ Store & forward SW \rightarrow check CRC \rightarrow error \rightarrow drop \rightarrow filter \rightarrow auto buffer
 - ⑦ Cut-Through SW \rightarrow Check transmission (dest., source bytes < 12 byte max) [to MS], No FCS & auto buffer
 - ↳ 2 mode :: ① fast-forward ~ 12 byte ② Fragment-free ~ 64 byte :: $< 64 = \text{MS} \rightarrow \text{drop} \rightarrow \text{MS}$
 - SW Domains
 - ① Collision Domains \Rightarrow domain \neq no. of stations \Rightarrow no. of stations ≤ 2 \Rightarrow SW "switch"
 - ② Broadcast \Rightarrow domain \neq broadcast \Rightarrow one domain \neq broadcast \Rightarrow router "switch"

▷ Basic SW Concept & Configuration

- Basic SW Config • SW Boot Sequence = same Router
 - Preparing of Basic SW Management : SW lädt Loopback ; initialisiert SVI (SW Virtual Interface) \rightarrow VLAN
 - Config SW Port \rightarrow Duplex Communication : ① Full ② Half (SW initialisiert same Pin)
Nur in Intf \Rightarrow sc config-if \Rightarrow duplex full \Rightarrow sc config-if \Rightarrow speed far (Wählt speed)
 - Auto - MDIX : zählt SW als Full-Duplex cross-over und übernimmt diese in der Intf \Rightarrow sc config-if \Rightarrow duplex auto \Rightarrow sc config-if \Rightarrow speed auto \Rightarrow sc config-if \Rightarrow mdix auto
 - SW Security : Security Remote Access \rightarrow SSM (Secure Shell) TCP port 22 Telnet : TCP port 23

Security : Security Remote Access → ssh (Secure Shell) TCP port 22, Telnet : TCP port 23
Config : `sec(config)* ip domain-name rto` → `crypto key generate rsa` → `username admin pass c0ntr0l` → `line vty 0 15`
`line` → `transport input ssh - linc` → `login local` [Verify SSH : show ip ssh, show ssh]

▪ SW Port security → minho policy iñgū MAC Addr. Tumon /oon fu -1-1

`S(config-if) > switchport mode access > switch port port-security > permit 1 dot1q`

Secure MAC Addr. → ① Static :: $s(config-if) \otimes$ switchport port-security mac-address [MAC-ADD] /
② dynamic :: $s(config-if) \otimes$ switchport port-security max-age [time]

Switchport port-security mac-ad
maximum MAC : switchport port-security maximum [MAX]

Violation mode: C protect :: security violation protect mode

② restrict :: security violation restrict mode \Rightarrow չունեցածքային պահանջ

E Verify : show port-security int ~~no~~ fa 0/0 , show port-security address

§ 8. Adv. Resolution Protocol (ARP): ARP Cache ifu MAC Addr. To map unroute dest (if Unroutable, MAC gateway)

IPV4 : Classless [no P.1→2] ; - Variable Length Subnet Masking (VLSM) ; \downarrow no nw [limit] ; \rightarrow more sub

$Q_{\text{out}} \rightarrow \mathbb{R}^n$



Chapter 8 LAN Redundancy & Spanning Tree Protocol (STP)

Chapter 9 VLANs & Inter-VLAN

- ▷ VLAN: partition (隔离: 分为 hw or broadcast domain 域) Layer 2 由 SW 实现的。VLAN 有三个属性
 - 优点: - security, - cost, - 带宽↑, - broadcast domain ↓, - 独立 QoS, 独立 L3
 - in a Multi-SW Environment.
 - VLAN Trunk: set in intf 属性是实现 SW 间 VLAN → Can carry data to >1 VLAN
 - ② config: intf → if & switchport mode trunk [verify: show intf folo switch port] Native (base) VLAN 由 in intf tag & writing to intf
 - Tagging Ethernet Frames (IEEE 802.1q): Ethernet Frame → Dest MAC | Src MAC | Tag | Type/Length | Data | FCS → Tag 表示 VLAN
 - ▷ Assignment: VLAN number → 1-4095 in config @ vlan Int (In flash)
 - ⇒ 1006-4096 in config @ running-config (In NVRAM)
 - ① -> I s* config & vlan vlan-num → vlan & name to when 在 trunk
 - II s* vlan database → (vlan) name to vlan num
 - ② Assign port to VLAN: intf → if & switchport mode access & switchport access vlan num (if int: 100 no num + 1 to num)
 - Verify: show vlan name to, show vlan summary, show int vlan num
 - ▷ Inter-VLAN Routing → routing set in trunk Tagged "sub interface"
 - ▷ config: ① set basic routing (set ip address, no shutdown)

Chapter 10 VTP (Virtual Trunking Protocol) → Manages VLAN & NAT (NLR, Inter-VLAN)

- ▷ VTP [Msg = ISL or IEEE 802.1Q] → n. Manage svr VTP svr & n. Manage Trunk domain
 - Operation : - n. update VTP version revision number 32 bits (0-4294927295) inform svr >
 - ↳ Mode : ① Server → create, remove, rename VLAN name in domain ②
 - ② Client → Joining VTP svr process, ↳ VTP msg on port trunk
 - ③ Transparent → can SVR, remove, rename VLAN name, build domain
 - ④ Config : 2 ways ฝ่ายเดียว : 1) svr Cisco 2) svr trunk management svr 3) svr domain 4) svr mode
 - ⑤ in global configuration S(config) → vtp version 2 → vtp domain \$0 → vtp password pass → vtp mode server / mode svr
 - ⑥ in VLAN configuration S(vlan) → vtp v2-mode [Verify : show vtp status / counters] → vtp server / client
 - ▷ Pruning → manage Trunk traffic interface interface ที่อยู่ใน config in interface msg, no remove VLAN Trunk ID
 - ▷ NAT → n. private ip ↔ publish / real ip S(config-if) → switchport trunk pruning VLAN ID VLAN name

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 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

- ④ Inside global Addr. ④ Outside global Addr. \rightarrow same ip
 type: ④ static : mhusanios [map: 110] \rightarrow Re config \Rightarrow ip not inside source static local-ip global-ip
 ④ Dynamic : \$pool 100 global/Real ip [map: 111 many \Rightarrow 1] : real Yuki's IP 111.111.111.111
 ④ PAT (Port Address Translation) \rightarrow port mhusanios NW addr. [map: many \Rightarrow 1]
 config: 3 줄 ④ NAT ④ INSIDE : Re config-if \Rightarrow ip not inside ④ OUTSIDE : Re config-if \Rightarrow ip not outside

Dynamic Routing Protocol

Interior Gateway P.

Distance Vector, Routing P.

RIP

IGRP

RIPv2

EIGRP

Classful

Classless

IPv6

Link State Routing P.

OSPFv2

IS-IS

OSPFv3

IS-IS for IPv6

Exterior Gateway P.

Path Vector

EGP

BGPv4

BGPv4 for IPv6

▷ EIGRP (Enhanced IGRP)

□ Characteristics (คุณสมบัติของ)

• Basic features Δ Cisco-proprietary (proprietary protocol von Cisco)

introduc in 1992

④ รอง classless version of IGRP ④ มีลักษณะเดียวกับ IP routing protocol, ไม่ต้องการรับข้อมูล Cisco router ไปใช้

• DUAL (Diffusing Update Algorithm) \Rightarrow ไม่มี loop-free & back up path ที่อยู่ใน routing domain \rightarrow in best path
(ไม่ต้องคำนึงถึง backup path) \rightarrow ไม่ต้องคำนึงถึง backup path ที่ดีที่สุด

• Establishing Neighbor = สองเครือข่ายที่ต่อตัวกันโดยตรง เช่น two directly connected EIGRP routers

update in routing measurement
link down แล้วตัวเอง• Adjacencies \Rightarrow Adjacencies are used to track the status of these neighbors

• Reliable Transport Protocol = RTP provides delivery of EIGRP packets to neighbors

RTP

• Partial and Bounded

= RTP and neighbor adjacencies are used by DUAL (ไม่ต้อง maintain)

= update ไม่ต้องคำนึงถึง backup path \Rightarrow update < RIP

for Staples

Equal and Unequal Cost = ต้องคำนึงถึง cost ของ route ที่ต้องผ่าน node ใด node จึงจะได้ cost ที่ต่ำที่สุด

~ Load Balancing

 Δ 9 protocol-dependent modules (PDMS) \Rightarrow 9 โมดูล protocol ที่ต้องรู้ protocol ของ IPv4, IPv6, legacy protocol IPX and AppleTalk Δ PDMS ฟังก์ชัน:• maintain EIGRP neighbor and topology table (Neighbor Table \rightarrow สร้าง Topology Table \rightarrow 9 routing table สำหรับ routing)

from topology & OSPF

from shortest path in backup shortest path

EIGRP from successor

• maintain EIGRP neighbor and topology table

• ผ่าน metric ให้ DUAL ที่ต้อง DUAL ไม่ routing table

• implement filtering and access list \Rightarrow in redistribution with other routing protocol Δ RTP is EIGRP neighbor and topology table Δ RTP is EIGRP Transport layer protocol ในการ delivery & reception von EIGRP packets Δ RTP = โปรโตคอล application layer ที่ maintain โหนด, msg ไม่ใช่ RTP Δ ต้องรู้ destination RTP packet ของตัวต่อไป (msg \approx OSPF)• Reliable packet require explicit acknowledgement (ต้อง) ต้อง dest. \Rightarrow update, query, reply• Unreliable packet do not require ack in dest. \Rightarrow Hello, Ack Δ จัดส่ง authentication (no encrypt routing update) ไม่ recommend (ห้าม) (authen & RIPv2, OSPF)

01-00-5E-00-00-0A

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

• 5 types of routing update or queries EIGRP multicast IPv4 : 224.0.0.10, IPv6 : FF02::A

① Hello \rightarrow แจ้ง adjacencies ที่ต้อง router 2 ตัวที่เป็น neighbor ที่มี response, ให้ unreliable② Update \rightarrow Update info. ของ dest., update info von routing table ของ neighbor router③ Acknowledgment \rightarrow ตอบกลับ info. update ที่ได้รับ④ Query \rightarrow request info. routing ของ neighbor router⑤ Reply \rightarrow ตอบ query ที่ได้รับ

■ Implement EIGRP for IPv4

 Δ Autonomous System (AS) is a collection of nw routers under single authority (ดู RFC 1930)↳ AS number \rightarrow 9 ที่ exchange routes between AS

↳ managed by IANA & assigned by RIRs, Internet Backbone providers, and institution

from government

 Δ Configure : Router config * router eigrp AS-*Router config * eigrp router-id \rightarrow ต้องระบุ interface \rightarrow IP address ที่ต้องติดต่อ

" * network nw-number [wildcard-mask]

" * passive-interface type number [default]

Δ Verify show ip eigrp neighbors

show ip protocols, show ip route



▷ Operation

- Initial Route Discovery (一轮)
 - R1 say hello to neighbor router (2) R2 receives hello or update route info.
 - R1 now ack & update info. (4) DUAL finds best route and update routing table
- Metrics: BW [lowest], Delay [highest], Reliability [worst], Load [worst] min value: show interface
- Default Composite Formula:
$$\boxed{\text{Metric} = [K_1 \cdot \text{BW} + K_2 \cdot \text{delay}] * 256}$$

$$= \left[\left(\frac{10,000,000}{\text{BW}} \right) + \left(\frac{\text{sum of delay}}{10} \right) \right] * 256$$
- complete:
$$\left[\frac{K_1 \cdot \text{BW} + (K_2 \cdot \text{BW}) + K_3 \cdot \text{delay}}{(256 - \text{load})} \right] * \left[\frac{K_5}{\text{reliability} + K_4} \right]$$
- R(config-router) set metric weight for K_1, K_2, K_3, K_4, K_5 - set bw: on intf. $\Rightarrow R(\text{config-if})$ bandwidth
 + Successor (S) [router to dest] = neighbor router having min dest min cost
 + Feasible Successor (FS) [2 routers & feasible condition] = Backup path (冗余路径) \Rightarrow neighbor
 + Reported Distance (RD) [distance to neighbor may report distance as 0] = "advertised distance"
 + Feasible Distance (FD) [distance to dest s] = on distance mindest cost
 min cost \Rightarrow dest cost min
 min cost lowest \Rightarrow dest.