

ថែរក្រោង

គម្រោងផែនទី 1

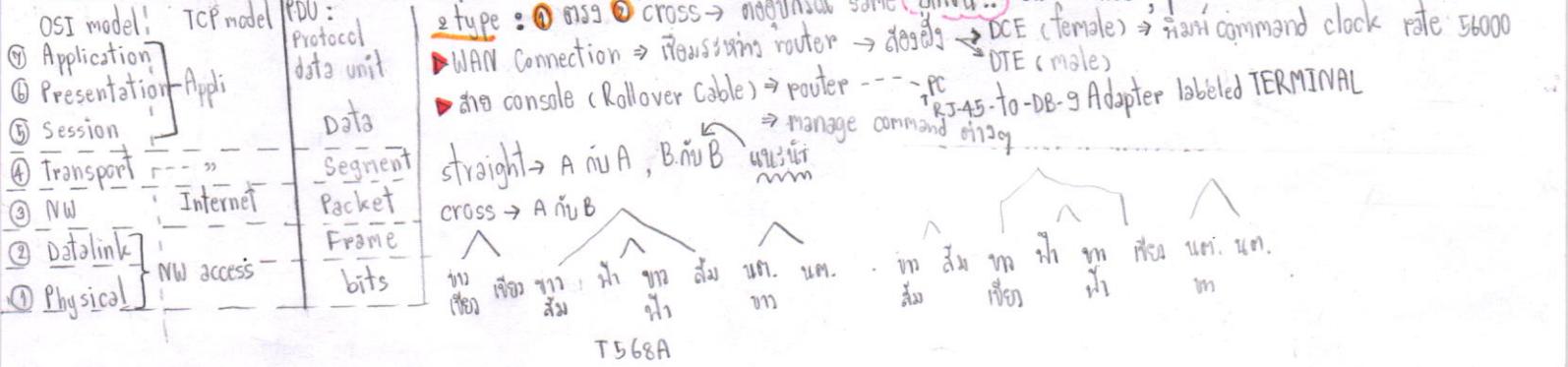
លេខស៊ីគិក 68888888

for Staples

Chapter 1 Network Overview

• Network devices

- Network diagrams = ក្រុងដាក់របស់ network នៅទំនាក់ទំនងមួយទៀតទេ?
- នៅក្នុង ① physical → ឈាន port / interface នៅក្នុងម៉ាស៊ីន
- នៅក្នុង ② logical → ឈាន ip
- Component of NW → HW device នៃ 3 type:
 - Type of NW → SW → ① Switch នៅក្នុងគណន៍
 - នៅក្នុង router នៅក្នុងគណន៍
- size → ① small home nw → ទីតាំងនំពីរ
- ② small office / Home office នៅក្នុងគណន៍
- នៅក្នុង config នៅក្នុងគណន៍
- ③ Medium to Large nw → នៅក្នុងគណន៍ 100 - 1000
- ④ World wide NW → internet
- Reliable NW



for Staples

Chapter 2 Basic Router Config

Internet Assigned Port number authority (IANA) : destination port

0 - 1023: requesting entities "well known ports"

1024 - 49151: registered port = publish "source port"

49152 - 65535: dynamic or private port "Randomly generate"

Ex. 20: FTP (data), 21: FTP (control), 25: SMTP,

53: DNS (domain name server) [TCP/UDP], 80: WWW HTTP,

81: Hosts & Name server

★ Logical Addr.: IP addr. (IPv4) នៃ L.3

- 5 class :: A, B, C, D, E → reserved (709)

Will be host → multicast Addr. → សំណើលើ

គណន៍អាជីវកម្ម, max 999 workstations required

- គឺជាដែន/ node or com → នៃ logical name (domain name)

& ip unique

prefix
192.168.1/24 range

255.255.255.0 → Subnet mask

192.168.1.255 → broadcast ip addr.

255.255.255.255 → broadcast network

↳ និងក្នុងជាដែន នឹងត្រូវ

class A : 0 NW 24 bit Host 0 - 127

class B : 10 NW 16 bit Host 128 - 191

class C : 110 NW 8 bit Host 192 - 223

class D : 1110 24 bit Multicast 224 - 239

class E : 1111 24 bit Experimental 240 - 255

TFTP Server

Flash Ram

ROM

POST

Console

Configuration

Locate and load operating system image

Locate and load configuration file enter setup mode

Perform POST

Load Bootstrap

ROM

Accessing a Cisco IOS Device

- ① Console port ② Telnet ③ secure shell (SSH)
- Terminal Emulation Program :: PUTTY, Tera term, secure CRT, Hyperterminal, OS terminal
- 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 user show
- ③ Hot Keys and Shortcuts
- ④ IOS Examination Commands → show...
- Getting Basic** ① host name → router(config)# hostname name " show ip interface"
- ② banner motd → Router(config)# banner motd # text # show ip interface brief → show interface nw, set?, status?
- Securing Device Access: Enable password/secret, console pass, VTY pass, Encrypting pass display
- ③ interface addressing ④ no shutdown config + n. interface ⑤ save config → router# copy running-config startup-config

Chapter 3 Static Routing & Dynamic Routing Protocol

Functions of Router → Characteristic:

- ① Topology ② Speed ③ Cost ④ Security ⑤ Availability
- ⑥ Scalability ⑦ Reliability
- Packets Forwarding Methods ① Process switching = packet ผ่านใน router 3 process CPU 3 open interface ไหน?
- ② Fast Switching = ดูใน buffer แล้ว forward ทันที
- ③ Cisco Express Forwarding (CEF) = forward packet ตามลักษณะ

Connect Devices

- Default gateway → ผู้ให้ ① first usable host (1) OSPF = 110, RIP = 120
- last usable host (.254) → ผู้ให้ 255.255.255.254 nw ไหน
- Enable IP on Host: ① Statically Assigned IP Addr. ② Dynamically Assigned IP Addr.
- can ไม่ได้ ip ให้ ผู้ให้ nw 3 DHCP (Dynamic Host Configuration Protocol)

The Routing Table

D	10.1.1.0/24	loopback0	via 209.165.200.226	00:00:05	Serial 0/0/0
---	-------------	-----------	---------------------	----------	--------------

Legend: D = Direct, L = Link, C = Connected, E = EIGRP, R = RIP

D Identifies how the nw was learned by the router

10.1.1.0/24 destination nw ที่สัก

in dest. ip (L*3) → ผู้ให้ routing table [90] administrative distance (trustworthiness) of the route source.

in mac address table MAC Addr. → dest. MAC (L*2)

the metric to reach the remote nw.

Patch Determination

Packet ผ่าน Interface
↓
match routing table
↓
dest. IP match subnet

match nw interface? y → check ARP cache
remote nw? y → encaps frame → next hop
default router? y → encaps frame → next hop
default router? n → packet & ICMP
n → n/w s. IP

match nw interface? y → encaps frame → next hop
remote nw? y → encaps frame → next hop
default router? n → encaps frame → next hop
default router? n → packet & ICMP
n → n/w s. IP

Routing ① Static Routing → manual
目的: security, resource utilization, process, and routing entry
特點: สำหรับ un. scalability, can't handle many routes
形式: "Stub NW"
4 type ① Standard ② Default = ให้ dest. ip บัง match
③ Summary ④ Floating = backup

Router * traceroute
Router * ping

PC > ping
→ " traceroute
→ " route ping
→ " nslookup

→ 192.168.1.0 subnet nw = nw ip & subnet mask
→ broadcast nw = ทั้งหมดใน subnet
host ที่ subnet nw คือ 192.168.1.255
Ex. = 192.168.1.255

Router(config)* ip route nwaddr. subnet_mask
{ ip-addr. 1 exit_intf }

Config: Next-hop Option

Router(config)* interface G0/0
R(config-if)* ip address 192.168.1.0 255.255.255.0
" " no shutdown } basic set min
R1(config)* ip route 192.168.1.0 255.255.255.0 interface G0/0:R.
nw 192.168.1.2 S 0/0/0
nw 2

Dynamic Routing Protocol → auto

① EGP (Exterior Gateway Routing Protocol) :: BGP
② IGP (Interior) :: RIP, OSPF, EIGRP, IS-IS
→ (Interior System to Intermediate System)

Classful Addressing → update entire class

Classless Inter-Domain Routing

summarization: ผู้ให้: ① อยู่ติดกัน
② ไม่ต้องเดินทาง
→ ตั้ง set ไว้ 255.0.0.0 no ip imiou
→ 255.255.255.255
② Group bit ที่ same กันทั้งสอง

VLSM

Fixed Length Subnet Masking
→ ① Prefix 1 หรือ Prefix 0
= จำนวน bit ที่ต้องมี 0 หรือ 1
→ ไม่ต้อง bit ที่ 1 ห้ามที่ phru 10/1
+ ip เริ่มต้น กับ + 1
→ จำนวน 1 หรือ 0

Chapter 4' Distance Vector Routing Protocol RIP v.1**► Dynamic Routing Protocol**

- **fn:** share info between router - auto update routing table when topology changes (เมื่อมีปัญหา) • แก้ best path
- **purpose:** แก้ remote nw (nw ห้องห้องใน) • ปรับปรุง routing info • เลือก best path ไป dest. nw • ค้นหา new best path ถ้า path
- **component:**
 - Algorithm:** ให้เพื่อนบ้าน routing info. & best path
 - Routing protocol msg.:** สำหรับเพื่อนบ้าน neighbor & แนะนำ路由 routing info. (best path)

Dynamic Routing**vs: Static routing**

a. ผู้ดูแล config

& แก้ไข nw (same โหมด)

Required by admin

Advanced (bec. config basic)

Topology change

เปลี่ยน auto

Scaling

ระหว่าง simple & complex (router ที่ไม่ติดต่อ direct ไม่ต้องคำนึง)

Security

ข้อบกพร่อง

Resource usage

ใช้ CPU, mem (เก็บ routing info.), link bandwidth

Predictability

Route & current topology

► Classifying Routing Protocols**DRP****Interior Gateway Protocol (IGP)****Distance Vector P.****Exterior Gateway Protocol (EGP)****Link State P.****BGP (Border Gateway Protocol)**

- **distance vector [distance, direction]** • complete nw topology (เก็บของทุกๆ อย่าง)
- incomplete . แก้ nw topology • update ไม่ต่อเนื่อง periodic
- periodic update (ทำงานเรื่อยๆ) (Open Shortest Path First) OSPF IS-IS (Intermediate System to Intermediate System) (แก้ policy or ผ่านตัวกลาง)

RIP (Routing Info. P.) IGRP (interior Gateway Routing P.)

RIP v.2

EIGRP (Enhanced Interior Gateway Routing P.)

▪ 2 type

① classful routing P. → update ตาม class ทำให้ subnet mask ไม่ routing update

② classless routing p. → แก้ subnet mask ให้ routing update

▪ **Convergence :** ต้องรอต่อ when routing table ของ all router ที่ดีกว่าเดิม (ไม่เปลี่ยนแปลง)

↳ 2 type : Slower (RIP & IGRP), Faster (quick. update when ต่อต่อเปลี่ยนแปลง) : EIGRP & OSPF

► Routing Protocol Metrics▪ **Metric :** ค่าที่ใช้ในการคำนวณ best path ของ nw ex. Hop count, BW, cost, Delay, Load, Reliability▪ **Load balancing :** nw มากกว่า 1 ต้อง metric ต่ำกว่า → เส้นทางที่ดีกว่า ไม่ใช่แค่เส้นทางเดียว กัน**► Administrative Distance of a Router (AD) ⇒ แก้เลือก protocol ในการ routing**▪ **สำคัญประการที่ 1 :** ก่อนจะเลือกที่จะใช้ ต้องให้ความรู้ particular (เฉพาะ) route

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

► NW Discovery (พื้นที่) (ทำ basic configuration)

⇒ 3 stage ① Co. State : Router Initial Start up

② Initial Exchange of Routing info. → กำหนด route ที่ต้องการ

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

► Routing Table Maintenance

→ บน router ต้องมีการรักษาอยู่ไหม?

▪ **Periodic update :** RIP update timer (default 30s), Invalid timer (info เสียหาย) (default 180s)

Hold down timer (ต้อง down → hold ไว้ ไม่ต้อง flush) (default 180s), Flush (ลบ) timer

(default 240s)



• Bounded (วงจร) Update : EIGRP → update จำกัดเวลา

• Triggered Update → update เกิดจาก periodic time

• Random Litter → ไฟล์ nw ที่เป็น multiple access router ต้องห้ามซื้อต่อ กัน → if เกิด update ทุกคนเหมือนกัน : จึงแก้ Random

▷ คุณสมบัติ standard DV. ① Routing Loops เกิดwhen intf ตก down ไม่ถูกอัปเดตใน table → ต้องหา neighbor แจ้งว่า update (จะ)

RIP RIP ↗ ไม่ถูกอัปเดต : ① set max hop = 15 → if hop = 16 → unreachable (ถ้า down ไปแล้ว) update → hop ต้องมากกว่า 16

v.1 v.2 IG EIG RIP RIP ② split Horizon Rule → ไม่ส่งข้อมูล update สำหรับ intf ที่ต้องรับ update แล้ว

speed convergence slow slow slow fast ③ hold down timer (ถ้า intf down → hold) ถ้า intf ที่ hop = 16

scalability - size nw small small small Large ④ Route Positioning → ① เกิด down set unreachable ② ถ้า unreachable ต้อง position บน intf

use of VLSM x ✓ x ✓ ⑤ @with ④ → ถ้าเกิด unreachable ต้อง over rule split horizon กรณี ip intf ที่ down & hop =

Resource usage Low Low Low Medium ⑥ IP & TTL (Time to Live) เหตุการณ์ update บ่อย กรณี when TTL = 0 16)

implementation & sim sim sim complex

maintenance ple ple ple

▷ RIP version 1 AD = 120

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

RIP v.1 Message Format			
Data Link Frame Header	IP Packet Header	UDP Segment Header	RIP Message
command = 1 or 2	version = 1	Must be zero	
Address family identifier (2 = IP)		Must be zero	
IP address (Network address)			
most be zero			
multiple route entries, up to a maximum of 25			

□ Basic RIPv1 config ① in basic config ② ผ่าน router rip R1(config) # router rip

+ ค้นหา nw R1(config-router) # network nw ip กำหนดมาตั้งแต่

□ Verification(ตรวจสอบ) & trouble shooting (ตัดสินใจ): show running config or ip router or ip protocols, debug ip rip

• passive intf command (ไม่ update intf ที่ไม่ต้อง) R(config-router) # passive interface intf-type (Fa/G/S) intf-number (color, color)

▪ Automatic Summarization : RIP Auto Summarizes classful nw → ทำให้ size routing table

ข้อดี : • ลด size routing update • single router สามารถจัด理 multiple route ลงใน routing table

ข้อเสีย : • ไม่ support discontiguous nw (major nw เดียวกัน but ไม่ติดกัน) → อาจทำให้ load balancing ลำบาก

• boundary Routers : summarize RIP subnet from 1 major nw to another

• processing RIP update

ก่อนที่จะ & ต้อง update ทุก intf ที่ classful เดียวกันไหม? → y : update subnet nw 172.16.1.0

↓ N : update classful intu 172.16.0.0

□ default route & RIPv1 ตัวเลือกของ routing table (อย่าง b/c. enas protocol) → จะเป็น default route

R(config) # ip route 0.0.0.0 0.0.0.0 50/0/1

default info. originate command → ต้อง update ทุก intu rip ให้ เป็น static ↔ dynamic

Router ที่ต้องตั้งเป็น 2 protocol ← R(config-router) # default-information originate

Chapter 5 RIP version 2 & Access Control Lists

classful (ต้อง subnet mask, ไม่ support CIDR) classless (update subnet mask, support Variable length Subnet Masking (VLSM), Support

not support discontiguous subnet Route Summarization (Prefix Aggregation) | update next hop addr.

not support VLSM b/c. ต้อง subnet mask

routing update ⇒ broadcast (255.255.255.255)

| 17 authentication routing (จัดการ discontiguous ทางกรอบ)

| Routing update ⇒ multicast

ก่อนที่จะ routing loop

ก่อนที่จะ split horizon or split horizon with poison reverse

ก่อนที่จะ triggered update

max hop count = 15

ก่อนที่จะ RIP v1

ก่อนที่จะ virtual interface can ทำให้ routing ที่ update แบบที่ได้

• loop back intf → ping → ip virtual intf → reply ให้

• null intf → ไม่ต้องมีช่องทาง channel ที่จะต้องมี → จึงจะ null intf → packet discard 100 → timeout

• static route & null intf → null intf จะรับสูญเสียไม่สามารถ static route

R(config) # ip route summary-static-route subnet-mask Null0

(major-nw) → รอง static supernet route

- Route redistribution (รีดิสทริบูชัน) → ย้าย ip ที่ static ให้เข้ามา (โดย ip ที่ static ไม่ได้): Router(config-router)* redistribute static
- Verify & Test Connectivity: show ip interface brief, ping (ua: ! = 1, u = ไม่ต่อ, . = timeout), trace route
- RIP v1: classful, ไม่ต้อง subnetmask, summarize nw @ major nw boundaries, if nw เป็น discontiguous & RIPv1 config convergence จะไม่ถูก
- ตรวจสอบ routing table debug ip rip (content of routing update), ถ้าเป็น RIPv1 จะไม่ให้ subnet mask ของใน nw addr.

▷ RIP v2

show ip protocols

- config • Enable & verify (ตรวจสอบ RIP v2)

- Config RIP → RIPv1 → ค้นรู้ว่า รองรับ v1 & v2 บุต. ถ้ารองรับ v1
→ RIPv2 → ค้นรู้ว่า รองรับ v2

- Auto-Summary & RIP v2 → auto sum route @ major nw boundaries Entry

→ sum route ต้อง subnetmask ที่น้อยกว่า classful subnet mask

- disabling Auto-Summary : no auto-summary bec. when ที่ nw topology ไม่เป็น discontiguous

- VLSM & CIDR → verify info. ที่ sent by RIPv2 debug ip rip

→ VLSM → เผยแพร่ nw addr. & subnet mask

→ CIDR → ที่ super netting (= bunch ของ contiguous classful nw ที่ต่อ addr. ไม่ใช่ single nw.)

→ verify show ip route, debug ip rip source → dest. คืออะไร?

- ▷ Access Control List = กฎควบคุมการเข้าออก → ตรวจสอบ → check ผ่านหรือไม่ ex. FTP, คุณภาพ? ⇒ กรณี conversation

- Packet Filtering ① dest., source @ L2 ② protocol ③ ที่ nw ไหน, ทำ 3 กรณี control ให้เข้า or block ที่?

- Operation → ทำงานใน sequence statement

→ last statement ที่ไม่ implicit deny → block → discard

command	Version=2	Must be zero
Address family type (2=IP)	Router Tag	
IP address (NW address)		
Subnet Mask		
Next Hop		
Metric (Hops)		

Multiple Route Entries, up to a maximum of 25

▷ Standard IPv4 ACLs

vs. Extendend IPv4 ACLs

- check source addr.

- check source & destination addr.

- กำหนด permits or denies ที่ๆ 1 protocol

- กำหนด permits or denies specific (เฉพาะ) protocol

access-list 10 permit 192.168.30.0 0.0.0.255

access-list 103 permit top 192.168.30.0 0.0.0.255 ang eq 80

- number ACL : 1-99 & 1300-1999

- Number ACL 100-199 & 2000-2699

- wild card → invert ของ subnetmask 1 → 0 = match/fix, 1 = ignore / ยกเว้น

→ รีเซ็ต set ของ ip ① หาก ส่วนที่ 160 bit ที่ต้องนับ ให้ wild card mask 011...011 = 0 ② bit ที่ต้องนับ = 1
(match range) if ตรง ก็ permit ไม่ตรง pattern or/and ถ้า ก็ deny wild card ที่ same กัน

→ in wild card ของ subnet = 255.255.255.255 - subnet mask

→ keyword → 0.0.0.0 = match all หรือ host

→ 255.255.255.255 = ignore all หรือ any

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

- Guideline for (3Ps) → One ACL/protocol = ctrl traffic flow ที่ intf, ACL ไม่ define ว่า protocol enable on intf

- ACL creation → One ACL/direction = ctrl traffic in 1 direction at time on an intf, ใช้ ACL ctrl in & out bound traffic

→ One ACL/interface = ACL ctrl traffic for an intf, Ex. G 0/0

• where → Extend ACL: @ close source → Standard ACL: @ close destination

- ▷ Config ACLs → Standard Router(config)* access-list num กำหนด กำหนด

แล้วกัน 1 แบบ

→ number

deny | permit |* mark | comment |
source [source-wild card] [log]

→ in intf

Router(config-if)* ip access-group num * permit any

{ access-list-number | access-list-name }

{ in | out }

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

• remove all : no access-list

• ลบไป ① no access list num * → ลบไป

• ลบไป ② no บรรทัด * → บรรทัด * ลบไป

• ลบไป → บรรทัด * ลบไป

• ลบไป → บรรทัด * ลบไป

• บรรทัดที่ 4 กด C

- ▷ Verify: show ip interface, show access-lists

- ▷ Securing Vty port → กำหนดให้ user ต้อง input permit ที่เราต้องการ ให้เข้า

Router(config-line)* access-class access-list-number

{ in [vrf-also] | out }

- Extended : filter : source/dest. addr., Protocol, port number



Chapter 9 Basic Switch Address Resolution Protocol

- LAN Design ⇒ Borderless sw nw design : มีภารกิจไป :: - Hierarchical, - Modularity, - Resiliency, - Flexibility
- 2 ลักษณะ : ① 3-Tier LAN Design ปกติ :: 1) Core 2) Distribution 3) Access ② 2-Tier ปกติ :: 1) Collapsed Core/Distribution 2) Access
 - 1 Core → บริการต่อรอง BW ด้วย → ทำให้ speed ↑ ใน เน็ตเวิร์ก nw? Layer 3 Support, [Gig / 10 Gig Ethernet] Link aggregation
 - 2 Distribution → ผู้จัดการห้อง [1 & 2], security Policy / Access Ctrl [Redundant components] → มีความเสี่ยงต่ำกว่า { ทำให้ BW device เพิ่ม↑ } สำหรับ SW
 - 3 Access → ต่อไปยัง end device, Port Security, VLAN, [PoE / Gig Ethernet], Power over Ethernet สามารถ or ไม่ได้ Quality of Service (QoS)
- เพื่อ A. can ใช้ LAN BW & ปรับสัดส่วนให้ max 1 LAN ↗ 1 LAN, 1 power line กันบันดาล
- f & n. ทาง Server ① Enterprise S. (ระบบห้องครัว) ⇒ ติดต่อ MDF (Main Distribution Facility : Core) ⇒ มองเห็นไปเรื่อยๆ ที่ไหน
 - ② Workshop S. (โรงงานผลิต) ⇒ ติดต่อ @ IDF (Intermediate D. F. : Distribution) ⇒ มองเห็น cross กัน access ที่ไหนก็ได้ที่ไหน
- Collision detection issue (ปัญหา กระแทก กัน ทุกที่)
- Segmentation issue (ปัญหา แบ่งส่วน) ⇒ ทำให้ปัญหา ก. ไฟล์ nw จัดการยากหักดิบ HCC (Horizontal ~) : UTP ⇒ Distribution ↔ Access
- Broadcast domain issue ⇒ ใน nw ที่เดียวจะมี broadcast in MAC addr. :: broadcast NW ควรจัดแบ่งເຊີ້ມ
- Segmentation คือ process split single collision domain → smaller collision domain ยกตัวอย่าง LAN segment :: L2 device ที่มี SW, bridges
- Broadcast domain รับจากตู้ port but. router (L3) ไม่รับ filter/segment broadcast ไม่ได้ กด รายการออก จากตัวบันดาล

► SW Environment

- SW Operation ① Learning :: รับ frame ที่มี SW จะเรียนรู้ Source MAC addr. ที่เดินทาง port ไหน + reset Aging
- ② Aging :: ลบ MAC addr. "if ไม่ต่อ" → ถ้า dest. ไม่ต้องใน table
- ③ Flooding :: ถ้า frame เดินทาง port ของ SW when frame คือ 1) broadcast, 2) multicast, 3) unknown unicast
- ④ Forwarding :: ถ้า dest. ไม่ต้องใน table
- ⑤ Filtering :: if ไม่รู้ frame ไม่ dest. บน port ที่เดินทาง dest. (source & dest. ไม่ same interface) จะต้อง filter ที่
- SW Methods :: ① Store & Forward SW ⇒ check CRC ในการ error ตรวจ → ถ้า ถูก → ไม่ส่ง → ดึง, auto buffer (รอเพิ่ม frame)
- ② Cut-Through SW ⇒ check ระยะทางส่วน (dest, source อยู่ห่างกัน 12 byte แรก) [10 ms], No FCS & auto buffer
 - 2 mode : ① fast-forward ~12 byte ② Fragment-free ~ 64 byte :: < 64 = ทุก → ไม่ต้อง → ไม่ต้อง
- SW Domains :: ① Collision Domains ⇒ domain ที่เกิดกันใน กลุ่มที่ต้องห้ามเชื่อมต่อกัน "ก. ณ ที่ เป็นตัวต่อต่อ"
- ② Broadcast ~ ⇒ domain ที่ต้อง broadcast → ถ้า domain ต้องกันจะได้รับ "ก. ณ router เป็นตัวต่อต่อ"

► Basic SW Concept & Configuration

- Basic Sw Config • SW Boot Sequence = same router
 - Preparing of Basic SW Management : SW ต้อง loopback :: กำหนดเป็น SVI (SW Virtual Interface) ⇒ VLAN
 - Config SW Port → Duplex Communication : ① Full ② Half (SW ที่ต้องกันต้องเลือก same กัน)
 - ตั้ง config intf → s(config-if)* duplex full → s(config-if)* speed 100 (เปลี่ยน speed)
 - Auto-MDIX : กำหนดจะต้องกันต้อง cross-over but. มองไปยังสายต่อ
 - ตั้ง config intf → s(config-if)* duplex auto → s(config-if)* speed auto → s(config-if)* mdix auto

► SW security : Security Remote Access → SSH (Secure Shell) TCP port 22 , Telnet : TCP port 23

Config : s(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 ให้ MAC Addr. ให้เข้า/ออกได้ - ไม่ได้

S(config-if)* switchport mode access → * switchport port-security ... → เลือก 1 ไปร่วมงาน

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 ที่วิ่งกัน → record ไว้
กรณีเข้ามาใหม่ MAC : * switchport port-security maximum MAX

Violation mode ① protect :: security violation protect mode

② restrict :: security violation restrict mode ⇒ จำกัดจำนวนการเข้าต่อเข้าบันดาล

③ shutdown :: security violation shutdown mode ⇒ shutdown

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

► Addr. Resolution Protocol < ARP > : ARP Cache ให้ MAC addr. ไว้ map ไป dest. (if ไม่พูดชื่อต้องรู้ MAC gate-

IPV4 : classless (ip p.1-2) : - Variable Length Subnet Masking (VLSM) : แบ่งกัน nw ให้ร่วมกัน : ⇒ เดือนกันร่วมกัน

- Fixed ~ : แบ่งกัน nw ไม่ร่วมกัน

ไม่ร่วมกัน → ลาก



way)

Chapter 8 LAN Redundancy & Spanning Tree Protocol (STP)

Issue with L1 Redundancy :: ① MAC Addr. instability \Rightarrow MAC Addr. table ຈຳກັດຕິບັງບໍ່ເປົ້າຍັນແປງຂອງ frame

② Broadcast storms \Rightarrow ວຸກສະບັບທີ່ຈຳກັດຕິບັງບໍ່ເປົ້າຍັນແປງຂອງ frame ③ Multiple frame transmission \Rightarrow start: unknown unicast \rightarrow in 1st dest. ໂດຍຮັບຫາໄດ້ frame but. source ດັວຍ

► STP \Rightarrow ອົດມາງວິທີ: ທີ່ block port \rightarrow block ຕົວ \rightarrow ຫີ້ໃຫ້ເພື່ອ traffic ຕັ້ງເຫັນທີ່ປັບປຸງ

▪ function: ① ທີ່ Root Bridge = 1st priority min Rule: ① 1 RB / 1 NW ② 1 RP / 1 RB ③ 1 DP / segment

④ BPDU ⑤ in path cost all ⑥ in Root Port \rightarrow path cost min \rightarrow ສັກເຊີງຈະເປັນ Designated Port

(Bridge Protocol Data Units) ⑦ ດັວຍ segment ສະໜັບ path cost ຕັ້ງກັນ \rightarrow 1st BID min ເປັນ designated port \rightarrow ສັກເຊີງໃໝ່ block port

L \rightarrow 1st RB & source E802.1D

■ Config: ວິທີ I: s1(config)* spanning-tree VLAN 1 root primary ວິທີ II: s2(config)* spanning-tree VLAN 1 priority 24576

(if s1, s2 ໃນ RB) s2(config)* spanning-tree VLAN 1 root secondary (verify: show spanning-tree) (ເພີ້ມໃຫ້ກາງ)

■ ຂະໜາດ Extended System ID : B. Priority \rightarrow B. Priority (per VLAN + Extended Sys ID (VLAN) + MAC Addr. \therefore BID = 8 byte

• PVST+ (ຜົນການ IEEE 802.1D STP) \rightarrow ແກ້ວມຳ load balancing ໂດຍຮັບ root/vlan

[Verify: show spanning-tree active]

• Rapid PVST+ \rightarrow in Alternate port (ໃໝ່ໃໝ່ block ໄທໃຊ້ can return ຕ້ອງຈະໄດ້ໃໝ່ປາກສ່ວນ)

↳ min. set Edge Port @ port ນີ້ host, router :- if * spanning-tree port fast

↳ link type : port ຖ້າມີມາຮ່າງ SW ຖ້າມີມາ point-to-point

- if * spanning-tree bpdu-guard enable \rightarrow port ໃຫ້ເນັດໃໝ່ BPDU ໄທໄດ້ \rightarrow clear all: clear spanning-tree detected-protocol

\rightarrow config : s1(config)* spanning-tree mode rapid-pvst \rightarrow * int in p-t-p * spanning-tree link-type point-to-point

Chapter 9 VLANs & Inter VLAN

▷ VLAN = in partition (ພູມພາຍ: ອົບມານ ນຸ້ນ ນຸ້ນ or broadcast domain ກົດ Layer 2 ໃຫ້ SW ແລະ ຖ້າມ. ຕິດຕະຫຼາດໄດ້ດັ່ງນີ້ VLAN ເຊິ່ງກຳນົດ

▪ ໜຶດ: - security ຕື່ອັນ, - link cost, - ປັກ. ຕື່ອັນ, - broadcast domain ລັດ, - ປັກ. ດົນ IT, ຈົດ. ປັກ. [Verify: show vlan brief]

■ in a Multi-SW Environment

• VLAN Trunk : set in intf ຖ້າມີມາຮ່າງ SW ທີ່ຈະ VLAN \rightarrow can carry ທີ່ຈະໄດ້ > 1 VLAN Tag & Untag \rightarrow ຊັ້ນ intf tag

③ ↳ config : in intf \rightarrow - if * switchport mode trunk [Verify: show int tag 0 switchport] (ຮັບຈຳນວນ)

Native (base) VLAN

when switch Trunk

③ Tagging Ethernet Frames (IEEE 802.1q) : Ethernet Frame \rightarrow Dest. MAC Src. MAC Tag Type/Length Data | FCS \rightarrow Tag ໃຫ້ສັດຄວາມ VLAN

■ Assignment : VLAN number \rightarrow 1-1005 ໃຫ້ config @ vlan.dat (ໃໝ່flash) ① ສັບສົນ: I S(config)* vlan vlan-num \rightarrow vlan* name ໜີ້.

→ 1006-4096 ໃຫ້ config ທີ່ @ running-config (ໃໝ່ NVRam) II S* vlan database \rightarrow (vlan*)* name ໜີ້

② - assign port ໃຫ້ vlan : in intf \rightarrow - if * switchport mode access \rightarrow * switchport access vlan num (if in: ໃຫ້ no num + num)

- verify: show vlan name ໜີ້, show vlan summary, show int vlan num (if in: no vlan num)

► Inter-VLAN Routing \rightarrow router set in trunk (ໃໝ່ໃໝ່ມານ "sub interface")

■ Config : ① set basic routing (set ip address, no shutdown)

② R(config)* interface g0/0.10 \rightarrow VLAN \rightarrow - subif * encapsulation dot1q 10 \rightarrow ip address ip subnet-mask

Chapter 10 VTP (VLAN Trunking Protocol) \rightarrow ໃຫ້ manage VLAN & NAT (NW addr. Translation)

▷ VTP [msg: ISL or IEEE 802.1Q] \rightarrow n. manage SW VTP \rightarrow in 1. manage in domain

■ Operation: - n. update VTP \rightarrow revision number 32 bit (0-4294927295) \rightarrow ເກີດກ່າວສັງເກດ \rightarrow

↳ 3 mode: ① Server \rightarrow can add, remove, rename VLAN ນີ້ໃນ domain ເວັ້ນ ②

② Client \rightarrow ຮັບເອົາ VTP ບໍລິສັດ, ດັບ VTP msg ແລ້ວນັກ trunk

③ Transparent \rightarrow can add, remove, rename ນີ້ໃນ domain, ເວັ້ນນັກການ

■ Config: 2 ນີ້ ສັບສົນ: 1) SW cisco 2) ທີ່ trunk ພົມມາຮ່າງ SW 3) ນີ້ domain 4) ທີ່ 3 mode

① in global configuration S(config)* vtp version 2 \rightarrow * vtp domain ໜີ້ \rightarrow * vtp mode server mode ຖ້າມ

② in VLAN configuration S(vlan)* vtp v2-mode \rightarrow [Verify: show vtp status, counters] \rightarrow vtp server/client/transparent

■ Pruning \rightarrow manage ລັດ traffic ຖ້າມີມາໃນ interface ແລ້ວ \rightarrow ໂດຍ config ທີ່ interface ມາ, ແລ້ວ remove ອົບກັດໄລ້ຕີ້ງ parent svlan * vtp pruning \rightarrow ລັດ interface \rightarrow S(config-if)* switchport trunk pruning vlan remove vlan-num

► NAT \rightarrow ລັດ private ip \leftrightarrow publish/real ip

■ Terminology: 4 type ① Inside local Addr. (private ip) ② Outside local Addr.

③ Inside global Addr. ④ Outside global Addr. \rightarrow same domain

■ type: ① Static: ກຳຕົວທີ່ 1:1 [map 1:1] \rightarrow ① R(config)* ip nat inside static local-ip global-ip

② Dynamic: ສັບສົນ Global/real ip [map: ຖື່ມ many \rightarrow 1]: real \rightarrow [ip range \rightarrow 1:1] (1.1)

③ PAT (Port Addr. Translation) \rightarrow port ນີ້ໃນ ລັດ private nw addr. (map: many \rightarrow 1) (1.2)

■ Config : 3 ດັວຍ ① NAT ② Inside : R(config-if)* ip nat inside

③ outside : R(config-if)* ip nat outside

Operation

- Initial Route Discovery (初步发现)
 - R1 say Hello แก่ neighbor router
 - R2 ยังไม่ได้ Hello or Update ทาง
 - R1 ให้ ACK & update info.
 - DUAL คำนวณ best route และ update routing table

- Metric : BW [lowest], Delay [highest], Reliability [worst], Load [worst]
 - Default Composite Formula: metric = $[k_1 * BW + k_3 * delay] + 256$

$$= \left[\frac{(10,000,000)}{BW} + \left(\frac{\text{sum of Delay}}{10} \right) \right] * 256$$

$$\text{Complete: } = \left[k_1 * BW + \frac{(k_2 * BW) + k_3 * Delay}{(256 - load)} \right] * \frac{k_5}{\text{Reliability} + k_4}$$

- R(config+router) กำหนด metric weights ต่อ k1 k2 k3 k4 k5 - set bw:ใน int. → R(config-if) กำหนด bandwidth kilobits-bw-value

DUAL and the topology Table

- (Finite State Machine) บน เส้นทางที่มี → sh ip eigrp topology [all-link], sh ip route
- + Successor(s) [router ที่ไป dest. ดีที่สุด] = neighbor router ที่ไป dest. ดีที่สุด min cost
- + Feasible Successor (FS) [ถ้า cost < FD] = Backup Path (เส้นทางสำรอง)
- + Reported Distance (RD) [Distance ที่ neighbor รายงาน report distance กันไป dest.] = "advertised distance" กรณี cost มากกว่า dest. cost iniplus "?" ก็จะถูก skip
- + Feasible Distance (FD) [Distance ที่กัน S] = An distance ที่คุณต้องไป dest. น้อยที่สุด cost lowest → dest.

▷ IPv6

▷ IPv4 ISSUE

△ Need for IPv6 → ไม่พอ IP 地址 จำกัด (private IP, NAT), จำกัด IoT ต่อ

△ ไม่สามารถ共存 (coexistence)

- Migration IPv4 → IPv6 Techniques

IPv6	IPv4
128 bit	32 bit
base 16	base 10