ชื่อ-สกุล นาย ศุภวิชญ์ ฉาริจิตสกุล กระดาษแผ่นที่ 1 รหัสนักศึกษา 58[illegible]

for Staples

① Network Overview

• Layer wit TCP/IP & OSI MODEL

7 Application		Application
6 Presentation		
5 Session		
4 Transport	→	Transport
3 NW	→	Internet
2 DataLink		NW Acess
1 Physical		NW access

• Network diagrams = โครงสร้างภาพที่เราดูแล มักเชื่อมต่ออย่างไร
- 2type ① Physical → บอกว่า port / interface ไหน เชื่อมต่ออย่างไร
② Logical → บอก ip
• Network protocol → tcp/UDP, FTP, ARP, SMTP, POP3, IMAP, ICMP
• Component of Network → (AW) → NW device มี 3 type
① end device = หลังจากเป็น ~
② intermediary devices = อยู่ระหว่างอุปกรณ์ เช่น Nw access, Security device
[..] Hub — [ ] switch ⊗ router
③ Network Media = สื่อกลาง เช่น copper, fiber, Optic, Wireless
(SW) → ① switch เลือกทางดี ② router เลือกทางที่ดีที่สุด
• type of NW → size → [1] small home NW ใช้งานตั้งแต่ต่อสายเครื่อง [2] small office / home จากด้านนอก → เข้าด้านใน
[3] Medium to Large Nw → มีการเชื่อมต่อจากตั้งแต่ 100-1000 เครื่อง [4] world Wide Nw เช่น Internet
→ Infrastructure [1] Local Area NW (LAN) = มี 1 กลุ่ม admin ดูแล
[2] Wide Area NW (WAN) - มีหลายกลุ่ม Admin
อื่นๆ MAN (Metropolitan Area NW), Wireless (WLAN), (SAN), PAN)

for Staples

• Reliable NW ① fault Tolerance → หาทางต่อการผิดพลาด ② Scalability → ปรับเปลี่ยนขยายได้ ไม่ส่งผลต่อ user
③ Security → จำกัด or limit การเข้าถึง ④ Quality of Service (QoS) → แต่ละ Service ใช้ไม่เท่ากัน

---

② Basic Router Configuration

• Port Address : กำหนดโดย (Internet Assigned Number Autority : IANA) 0-1023 : พอร์ทที่เรารู้จัก
49,152 - 65536 = Random / 1024 - 49,151 : registerport = ให้ทุกคนใช้
• Logical Address : (IP v4) - 5 Class A, B, C, D, E

Class A :	NW (0)	Host	Host	Host	0-127
class B :	NW (10)	NW	H	H	128-191
Class C :	NW (110)	NW	NW	H	192-223
Class D :	1110				224-239 multicast
Class E :	1111				

for Staples

• Physical Address : MAC
• Ethernet : 48 bit • ก่อตั้งโดย IEEE
• Message Delivery
- Unicast - ส่งจากเครื่องปลายทางเพียงหนึ่ง เครื่องภายในเดียวกัน / Multicast = ส่งจากหลายเครื่อง รับเฉพาะเครื่องที่เปิด service ไว้
- Broadcast - ส่งหาทุกเครื่อง ใน NW เดียวกัน

ชื่อ-สกุล นาย ศุภฤกษ์ อารีรัตน์กุล กระดาษแผ่นที่ 2 รหัสนักศึกษา [illegible]

for Staples

③ Static Routing & Dynamic Routing Protocol

- Functions of Router → Characteristic ① Topology ② Speed ③ cost ④ security ⑤ Availability ⑥ Scalability ⑦ Reliability
  - Packet Forwarding Methods ① Process switching = ทุก packet ที่ส่งเข้า Router
    ② Fast switching = มีตัวช่วย ทำให้ forward ได้เร็วขึ้น ③ Cisco Express Forward = Forward Packet ได้เร็วที่สุด
- Connect Device
  - Default gateway → เป็นได้ 1> first usable host 2> last usable host
    → ทางออกไปเชื่อมกับ NW อื่น
  - Enable IP on a Host : ① Statically Assigned IP address
    ② Dynamically สามารถกำหนด ip ได้
- switching Packet beetween Nw
  ขั้นตอน : หา dest. ip (L#3) ดูเส้นทางใน Routing table → นำออกไป ดูเส้นทาง MAC addr. ได้ dest. MAC (L#2)

for Staples

- Routing
  1> Static Routing → Manual
  ข้อดี : security ใช้ resource น้อยใน process, ลด routing Entry
  ข้อเสีย : ลำบากในการ scalibility สามารถเปลี่ยนเส้นทาง
  ควรใช้เมื่อ : NW ขนาดเล็ก, จำนวน router น้อย, NW มีทางออกเดียว
  4 type : ① standard ② default = ใช้ when dest. ip ไม่ Match
  ③ summary ④ Floating = backup
- Classful Addrssing → update ตาม class
- classless Inter - Domain Routing
  - summarization เงื่อนไข ① อยู่ติดกัน ② ไปทางเดียวกัน
  - ถ้า set ใหม่ ต้องไปใช้ IP เก่าก่อน วิธีทำ ① แปลง ip → ฐาน 2
    ② Group bit ที่เหมือนกันมากสุด

for Staples

- VLSM = ความสามารถในการ กำหนด subnet Mask ที่แตกต่างกันไปให้กับแต่ละ sub NW ต่างๆ

- Dynamic Routing Protocol → Auto
① EGP (Exterior Gateway Routing Protocol) ② IGP (Interior Gateway Routing Protocol)

ชื่อ-สกุล ศุภกิตภาญ อารีสิตสกล กระดาษแผ่นที่ ______ รหัสนักศึกษา 58[illegible]253

for Staples

Chapter 4 Distance Vector Routing Protocol RIP ver 1

- Dynamic Routing Protocol
  - of : Routing share ระหว่าง Router · auto update routing table when topology เปลี่ยน (เมื่อมีปัญหา) best path
  - purpose = หา remote nw (nw ที่อยู่ไกล) · ปรับปรุง routing info · เลือก best path ไป dest. nw หาเส้นทาง new best path
  - Component = 1). Algorithm ใช้เพื่อหา routing info & best path
    2). Routing Protocol msg. = ค้นหา neighbor & แลกเปลี่ยน routing info (best path)

	Dynamic routing	vs static routing
ความยุ่งยากในการ config	ขนาด nw (ไม่เพิ่มเติม)	ขนาด nw (เพิ่ม command ทุก router)
required ความรู้ Admin	Advanced (best config basic → ต้องมีความรู้มาก)	ไม่เพิ่มเติม (กำหนดเส้นทาง เองโดย command
Topology change	ปรับ Auto	admin config ใหม่ทั้งหมด
Scaling	เหมาะ simple & complex (router ที่ไม่ใช่ Directly ไม่ต้องทำไร)	เหมาะ simple topologies
Security	น้อยกว่า	มากกว่า
Resource usage	ใช้ CPU, Mem (เก็บ Routing info), Link bandwith	No เพิ่มเติม
Predictability	Router ตาม current Topology	Route → dest.nw เดิมตลอด

- Classifying Routing Protocol

for Staples

- RP
  - ภายใน (AS) Interior Gateway Protocol (IGP)
    - Distance Vector P.
      - ประมาณ vector (distance, Direction)
      - incomplete view ของ nw topology
      - Periodic update
      - RIP (Routing Info P.) → RIP V.2
      - IGRP (Interior Gate way Routing P.) → EIGRP (Enhanced Interior Gateway Routing P.)
    - Link - state P.
      - Complete nw topology (เก็บข้อมูล)
      - Update ไม่ใช่ Periodic
      - (open Shortest Path first) OSPF
      - IsIS (Intermediate System) to Intermediate system
  - (ภายนอก AS) Exterior Gateway Protocol (EGP)
    - BGP (Border Gateway Protocol)
    - Autonomous System (AS) เป็นกลุ่มของ Router ภายใต้การควบคุมของ single Authority (กลุ่ม policy or ผู้ดูแล)

- 2 type
1) Classful routing P. → update ตาม class ไม่ส่ง subnet mask ใน routing update
2) classless → ส่ง subnet mask ใน routing update

- Convergence : ถูกกำหนด เมื่อ Routing table ของ routing ทั้งหมด มีสถานะ ตรงกัน (ไม่เปลี่ยนแปลง)
  - ↳ 2 type : slower : RIP & IGRP, Fastere (มีการ update เมื่อเกิดการเปลี่ยนแปลง) >1. EIGP & OSPF
- Routing Protocol Mectrics
  - Metric : ค่าที่ใช้ในการคิด/วัด ในการไป dest. nw → เลือก best path ไหน เช่น Hop content, BW, Cost, Delay, Load, ค่าเชื่อถือ Reliability
  - Load balancing : nw มีเส้นทาง >1 ที่ Metric เท่ากัน → และจะทำการใช้งานแต่ละเส้นเท่าๆ กัน
- Administrative Distance of a Router (AD) → ใช้เลือก Protocol ในการ Routing
  วัตถุประสงค์ : ค่าตัวเลข ที่แสดงสิทธิ์หรือของ particular ละเอียด route
- Distance Vector Routing Protocol Ex. RIP, IGRP, EIGRP
  - Distance vector Technology ต้องรู้ 2 สิ่งนี้ คือ ① vector or direction การที่จะไปทางไหน ② Distance to final dest (cost)
  - ลักษณะทั่วไป : Preridic (ตามช่วงเวลา) update neighbor (⊗ ใกล้เคียง), broad cast (255.255.255.255) update, เอา routing table all ไป update
  - ——— ของ Routing Protocol : ลักษณะที่ใช้ในแต่ละ device ต้องรู้ ① Time to convergene → เวลาที่เป็น steady state ของ routing table ทั้งหมด (การเปลี่ยนแปลงแล้ว)
    ② Scalability ขยายมากสุดเท่าไร ③ Resource usage ④ Implementation & maintenance
- NW Discovery (ค้นพบ) (ต้อง Basic config ก่อน)

for Staples

  - 3 stage ① Cold State : Router Initial start up
    ② Initial Exchange of Routing info. ทำการแลกเปลี่ยน
    ③ Exchange of Routing Info → update (เพิ่ม hop content) routing info
- Routing Table Maintenance
  - Periodic update : RIP update timer (default 30s) → ของ router อื่นๆ ว่ายังอยู่ไหม
    Invalid time (info ที่ lost) (default 180),
    Hold down timer (ได้ down → hold ไว้ใช่ไหม, up ตอนไหน) (default 180), Flush (ทิ้ง), timer (default 240)

- Bounded (ขอบเขต) Update: EIGRP → update แค่เปลี่ยนแปลงที่
- Triggered Update → update ไม่รอ periodic time
- Random Jitter → ใช้ใน nw ที่เป็น multiple acess router หลายตัว เชื่อมต่อกัน → ถ้าเกิด update ชนกันตรงนี้ ไม่ใช้ Random

ปัญหา standard DV. ① Rotiy Loops เกิดเมื่อ info ในการ down จะถูกลืมออกจาก table → ส่งทำให้ neighbor จะส่งมา update
↳ แก้ปัญหา: ① set max hop = 16 hop = 16 → if hop = 16 → unreachable (มัน down ไปแล้ว)
② hold down timer (ถ้า intf down → hold)
③ split Horizon Rule → ไม่ส่งข้อมูลซ้ำเลกกลับไป ยังขา intf ที่ได้รับมา update มา
④ Route Poisioning → ① เกิด down set unreachable ② ส่ง unreachable (ตัวบ) poision ออกไป
⑤ ③ with ④ → ถ้าเกิด unreachable จะ over rule split horizon โดยส่ง ip intf ที่ down (hop = 16)
⑥ IP TTL (time to live) เกิดการวน update กม จะหยุดเมื่อ TTL = 0

	RIPv1	RIPv2	IGRP	EIGRP
speed convergance	slow	slow	slow	slow
scalabity - ขนาด nw	small	small	small	Large
use of VLSM	×	✓	×	✓
Resorce usage	low	low	low	Medium
implementations maintenance	simple	simple	sim	complex

- RIP version 1 AD = 120
- คุณสมบัติ = - Classful, DV = metric - hop count = hopcount > 15 unreachable - update broadcast ทุกๆ 30s
encapsolated เบรคุใน UDP segment ด้วย source & dest port = 520
- Msg มี 2 type = ① Request → ส่ง Routing table → ไป intf ที่ config ไว้ เพื่อรอรับการ update
② Responce → ส่ง info. ของ routing table
- ip address = แบ่งตาม class A, B, C
- Basic RIP v1 config ① ทำ basic Config ② สั่ง router rip + ส่งสั่ง nw
R1 (config) # router rip
R1 (config-router) # network nw ip ที่ต่อตรงกับ MS
- Verification (ตรวจสอบ) & Troubleshooting (จัดการปัญหา): show running-config or ip route or ip prob cds, debug ip rip
- passive intf command (ไม่ update intf ที่ไม่สนใจ) R (config-router) # passive-interface intf-type (Fo/0/0) intf-number (0/0...)
- Automate Summarization: RIP Auto summarize classful หนวดเพื่อลด size routing table
  - ข้อดี = ลด size routing update - single router หลายหลายๆ แทนการมี multiple route เยอะมากใน routing table
  - ข้อเสีย = ไม่ support discontiguous nw (Major nw เดียวกัน แต่ไม่อยู่ติดกัน) → อาจจะเกิด load balancing ได้
- boundary Routers: summarize RIP subnet from 1 major nw to another
- Processing RIP update = ดูที่จะส่งไป update ไป (intf) ว่าเป็น classful เดียวกันไหม → y: update subnet nw เช่น 172.16.1.0
↳ N: update classful เช่น 172.16.0.0
- default route & RIP v1 ถ้าไม่ลงตอนออกใน routing table (อาจจะเพราะคนละ protocol) → จะลง default route
R (config) # Ip route 0.0.0.0 0.0.0.0 S0/0/1
default info. originate command → เมื่อ update ให้ rip รับเชื่อง, static → dynamic
Router ต้องอยู่ระหว่าง 2 protocol — R (config-router) # default-information originate

Chapter 5 RIP version 2 & Access control Lists

Summarization (Prefix Aggregation) ← route

RIP v1	VS	RIP v2
classful (ไม่ส่ง subnet mask, ไม่ support CIDR		Classless (update subnet mask, support variable Length subnet Masking (VLSM), support update next hop addr.
not support discontigous subnet		ใช้ Authentication routing (รองรับ discontiguous บอกว่า)
not support VLSM เพราะไม่ส่ง subnet mask (255.255.255.255)		
routing update → broadcast		routing update → multicast

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

- ข้อจำกัดของ RIP v1

เป็น virtual interface สามารถที่ให้ routing ให้ update ออกไปได้
- loopback intf → ping ได้ → ip virtual intf → reply ได้
- Null intf → ใช้ทิ้งกลนส่วนเกินจาก channel ที่เราไม่ต้องการ → ถ้ง null intf → packet discard ของ → timeout
- static route & null intf → null intf จะรับหน้าที่เป็นทางออกของ static route
R (config) # ip route summary-static-route subnet-mask Null 0
(major-nw) → ของ static super net route

ชื่อ-สกุล ศุภกิตณ์ ยาริสุตสกุล กระดาษแผ่นที่ 3 รหัสนักศึกษา 58[illegible]

for Staples

· Route redistribution (จัดสรร) → อยากให้ rip รู้จัก static ต้องทำเพื่อให้ rip ส่ง static ไปด้วย : R(config-router)# redistribute static

· Verify & Test Connectivity : Show ip interface brief, ping (เจอ ! ได้, . ไม่ได้, . = time out), tracroute

· RIP v_1 = classful, ไม่ส่ง subnet mask, summarize nw @ major nw boundaries, if nw เป็น discontiguous & RIP v_1 config convergence จะไม่ไปถึง

· ตรวจ routing table debug ip rip (content of routing update), ถ้าเป็น RIP v_1 จะไม่ส่ง subnet mask รวมใน nw addr

▶ RIP v_2

show ip protocols

● Config · Enable & verify (ตรวจสอบ) RIP v_2

· config RIP → RIP v_1 → สามารถรับได้ทั้ง v_1 & v_2 แต่ส่งได้แค่ v_1

→ RIP v_2 → สามารถรับ & ส่งได้แค่ v_2

· Auto-Summary & RIP v_2 → Auto sum route @ major nw boundaries

→ sum route ตาม subnet mask ที่น้อยกว่า classful subnet mask

· disabling Auto-Summary : no auto-summary เพราะเมื่อเป็น nw topology อาจเป็น discontiguous

● VLSM & CIDR → verify info. ที่ sent by RIP v_2 debug ip rip

→ VLSM → เผยแพร่ nw addr. & subnet mask

→ CIDR → ใช้ supernetting (= bunch ของ contiguous classful nw ที่เป็น addr. เหมือน single nw)

→ verify show ip route, debug ip rip

● Access Control List = ควบคุม traffic เข้า ออก → ตรวจสอบ → check → source → dest ผ่านไหม?

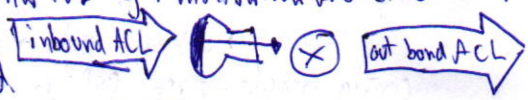
→ ทำ อะไร (เช่น FTP) ผ่านไหม?

→ คุม conversation

· packet filtering ดู ① dest, source @ L2 ② protocol อะไร ③ ไป nw ไหน → พิจารณาผ่าน หรือ block ไหม?

· operation → ทำงาน เป็น sequence statement

→ last statement เป็น implicit deny → block → discard



for Staples

· standard IPv4 ACLs VS Extended IPv4 ACLS

Standard IPv4 ACLs:

- check source addr.
- ปกติ permit or denies 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 addr.
- ปกติ permit or denies specific เฉพาะ protocol

access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80

- number ACL 100-199 & 2000-2699

● wild card → invert ของ subnet mask

→ 0 = match / fix, 1 = ignore / อะไรก็ได้

→ กำหนด set ของ ip ① หาคู่ที่เหมือนกัน ของ bit ที่ซ้ำกัน ใส่ wild card mask ตรงนั้น = 0

② bit ที่ไม่ซ้ำใส่ 0

if ถ้าไม่ได้ให้ลองหา pattern or / and ล้วน คือ ทุกตัว wild card = 1 เหมือนกัน

→ หา wild card ของ subnet = 255.255.255.255 - subnet mask

→ key word → 0.0.0.0 = match all ใช้ host * access list 4 permit host 192.168.10.10

→ 255.255.255.255 = ignore all ใช้ any *

permit any

· Guideline for (3Ps) → one ACL / Protocol = ctrl traffic flow บน intf, ACL ต้อง define แต่ละ protocol enable on intf

ACL creation → one ACL / direction = ctrl traffic in 1 direction at time on intf, แยก ACL ctrl in & out bond traffic

→ one ACL / interface = ACL traffic ของ intf, เช่น G 0/0

· where → Extend ACL : @ close source → standard ACL : @ close destination

· Config ACLs → standard → number * Access-list access-list-number deny | permit | remark source [source-wildcard] [log]

access-list num. permit any

ถ้า remove all : no access-list

ถ้า แก้ (I) no access list num * → ลบไม่ได้

(II) no บรรทัด * → บรรทัด *, ลำดับ

→ in intf → ip access-group { access-list-number | Access-lis-name } { in | out }

ถ้า remove all = no ip access-group

ถ้า แก้ → บรรทัด & ลำดับใหม่

· verify : show ip interface, show access-lists

· security VTY port → อนุญาตให้ผ่านเฉพาะ permit เฉพาะเครือข่ายที่ใช้ได้

* access-class access-list-number { in [vrf-also] | out }

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

for Staples

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

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

ที่เหลือ same standard
ใช้ทั้ง number & name
- debug - output : debug ip packet ACL-number

Chapter 6 OSPF & DHCP

▶ Link-state Routing Protocol = เป็น protocol ที่สร้าง complete map ของ topology ขึ้นมา → หา shortest path first (SPF) (ใช้ dijkstra)
เหมาะกับ: ① Large nw, ② Fast convergence ③ admin ควรมีความรู้
ขั้นตอน update ① learn info. ของ link ② ส่ง hello neighbor ③ เอา info มาสร้าง Link-state Packet (LSP)
④ router flood LSP to all neighbors → ได้รับแล้วเก็บลง db ⑤ router เอา LSP เก็บใน db (รูปแบบ tree) → adding OSPF = router table
ข้อดี: ① สร้าง topology map com หา shortest part ② fast convergence ③ LSP sent only when change topology (ไม่ส่งข้อมูล) → คำนวณ shortest path ④ hierachical design (NW ใหญ่ แบ่ง resource เพราะ หา ข้อมูล แค่ใน area)
ข้อเสีย: ① ใช้ mem ในการเก็บ All Link-state เยอะ ② ใช้ CPU ในการคำนวณ ③ ตอนส่ง LSP ครั้งแรก ใช้ BW มาก

▶ OSPF AD 116

L stable : ① neighbor show ip ospf neighbor ② Topology (สร้าง map) show ip ospf database ③ Routing (ได้ shortest path)
message → Encapsulation : MAC Dest. = multicast : 01-00-5E-00-00-05 or 01-00-5E-00-00-06
Protocol field = 89
→ type OSPF Packet : 01 Hello → ทุกๆ 10 s (default = multiaccess & point nw), ทุกๆ 30 s (default = non-broadcast)
: 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) → ตอบกลับว่าได้แล้ว

Operation : สร้าง nb ที่ติดต่อ ① Down state (เริ่มต้น) → ② Init State (ได้รับ hello) ③ two-way state (ตอบกลับ hello) (Exstart state)
→ exchange state → loading state → Full state (รวมกันแล้ว update ของแต่ละ router)

config single-Area OSPF v2 router ospf process-id → 1-65535, เป็น locally significant
R(config-router) * router-id ① 1.1.1.1 → ถ้าไม่ set จะใช้ ② loop back, ③ active interface, ip สูงสุด ตามลำดับ ① ไป ③
router ospf process-id
network network-address wildcard-mask area area-id

OSPF cost → ใช้ BW คำนวณ [Default reference BW = 10^8]

cost = $\frac{10^8 \text{ bps}}{\text{intf BW bps}}$
→ 10 Gb ethernet = 100×10^8 → cost = 1
Gb ~ = 10×10^8 → ~ = 1
Fast ~ = 10^8 → ~ = 1
Serial ~ = 1.544×10^6 → ~ = 64

→ ต้องการ เปลี่ยนค่า cost
→ เปลี่ยนค่า ref BW Auto-cost reference-bandwidth bandwidth_mbps
- Fast Ethernet Auto-cost reference-bandwidth 100
- Gigabit Ethernet 1000
- 10 Gigabit Ethe 10000
→ เปลี่ยนค่า BW = R(config-if)# bandwidth 64 (EIGRP & OSPF ใช้ได้)
* ip ospf cost 1062 s

verify OSPF show ip ospf neighbor, show ip protocol, show ip ospf interface brief, show ip ospf
more config * ip route 0.0.0.0 0.0.0.0 loopback N
* router ospf process-id
* default-information originate

▶ DHCP (dynamic Host Configuration Protocol) → ทำ config ใน host ให้ Auto (เช่น ip, subnet mask, default Gateway)
method ① Manual Allocation : admin assign เอง
② Automatic A~ : DHCPv4 assign addr ใน pool ให้ไม่มี lease time
③ Dynamic A~ : ใครเปิดก่อนจะได้ก่อน ip ไป & less time → ถ้า lease time หมด จะ ip ใหม่

Config * ip dhcp excluded-address 192.168.10.1 192.168.10.9
*
* ip dhcp pool LAN-POOL-1 (ชื่อ pool) 192.168.10.200
* network 192.168.10.0 255.255.255.0 → new ip ที่จะแจก
* default-router 192.168.10.1 → ต้องมี
* dns-server 192.168.11.6 } ไม่มีก็ได้
* domain-name example.com
end

verify
show running-config | section dhcp
show ip dhcp binding
show ip dhcp server statistics
* ขอ ip ให้ client * ip address dhcp
* no shutdown
ถ้าไม่มี
• no service dhcp

ชื่อ-สกุล นาย ศุภกิตติ์ อารีจิตสกุล กระดาษแผ่นที่ 4 รหัสนักศึกษา 58011253

for Staples

Chapter 7 Basic Switch Address Resolution Protocol

▶ LAN Design → Borderless sw nw design : มีกฎทั่วไป :: - Hierachical - Modularity, Resiliency, Flexibility

■ ลักษณะ : ① 3-tier Lan design 1) Core 2) Distribution 3) Access ② 2-tier Lan design 1) Collapsed Core/Distribution 2) Access

Layer sw
1 Core → อุปกรณ์รองรับ BW สูงๆ ทำให้ส่งความเร็วเพิ่มในการเชื่อมต่อ } Layer 3 support, [Gig/10Gig Ethernet]
2 Distribution → เชื่อมระหว่าง 1 & 3, security Policy/Access Ctrl } Redundant component → ส่งหลายเส้นหลายไป
3 Access → ติดต่อ end device, Port Security, VLAN, CFa/Gig Ethernet Power over ethernet รองรับ 1 LAN หรือไม่ก็ได้

} Link aggregation ทำให้ BW device เพิ่ม ↑ Quality of Service (QoS)

■ เพิ่มความสามารถในการใช้ LAN BW, ปสภ. ให้เพิ่ม MAX

.f ตรวจ Server ① Enterprise S. (รองทั้งองค์กร) → ติดตั้ง ② MDF (Main Distribution Facility : Core) หลายไปนอก ที่ทดสอบ
② Work Shop S. (เฉพาะกลุ่ม) → ติดตั้ง ② IDF (Intermediate D. F. : Distribution) → เชื่อม cross กับ access

· Collision detection issue (ปัญหาการตรวจจับการชน)

· Segmentation issue (ปัญหาการแบ่งส่วน) ทำให้หาไม่พบ ปสภ. ขึ้น

· Broadcast domain issue → ใน NW เกิดหลายเส้น Broad cast แบบ MAC addr. ควรจำนวนเล็ก

VCC (vertical cross-connect) : optical Fibre : MDF ↔ IDF
(แนวตั้ง)
HCC (Horizontal) ~~~~) : UTP → Distribution ↔ Access
(แนวนอน)

■ Segmentation เป็น process split single collision domain → smaller collision domain บน LAN segment เช่น bridge, SW

■ Broadcast domain รับมาทุก port not router เป็นการ filter/segment broadcast ไม่ให้กระจายออกจากห้องอื่น

▶ SW Environment

■ SW Operation ① Learning : รับ frame เข้า sw จะเรียน source MAC addr. จากต่อกับ Port ไหน + Reset Aging
② Aging : อายุของ MAC addr. ถ้าหมด → ลบ
③ Flooding : ส่ง frame ออกทุก port ของ sw เมื่อ frame เป็น 1) broadcast 2) Multicast 3) Unknown unicast
กรณีส่งออก { ④ Forwarding : ส่งไป dest. (กรณีพบใน table)
⑤ Filtering :: ถ้าไม่รับ frame ไป dest จาก port ที่เป็นหลายไป dest.

■ SW Method ① Store & forward SW → Check CRC ว่า error ไหม → มี : ทิ้ง → ไม่มี : ส่ง, Auto filter
② Cut-Through SW → Check เฉพาะบางส่วน (dest, source. อย่างน้อย 12 byte แรก) [ข้อมูล], No FCS & Auto-buffer
↳ 2 mode : [1] fast-forward ~ 12 byte [2] Fragment ~ 64 byte (< 64 จึง → ทิ้งได้)

■ SW Domains ① Collision Domains → Domain ที่เกิดการรับ-ส่งข้อมูลที่มาพร้อมกัน → ดูว่า sw มีกี่ port
② Broadcast → Domain ที่ส่ง Broadcast → อยู่ domain เดียวกันจะได้รับ → ดู router มีกี่ port

▶ Basic SW Concept & Configuration

■ Basic SW Config · SW boot sequence = same router
· Preparing of Basic SW Management, sw ไม่มี loopback ทำผ่าน SVI (SW Virtual interface) → VLAN
· Config SW Port → Duplex communication : ① Full ② Half (sw ต่อกันต้องเลือกเหมือนกัน)
เข้า intf → s(config-if)# duplex full → s(config-if)# speed 100 (เปลี่ยน speed)
→ Auto-MDIX : ปกติ sw - เชื่อมกันต้อง Cross-over ต้องเลือกแบบตรงๆ

→ Verify Port Config show int f0/0 / startup-config / running-config / flash / version / history / ip f0/0 / Mac addr table

เข้า intf → s(config-if)# duplex auto → s(config-if)# speed 100 → s(config-if)# mdix auto

□ SW Security : Security Remote Access → SSH (Secure Shell) TCP port 22, telnet port 23
s(config-if)#

□ SW Port Security - กำหนด policy ว่าให้ Mac Addr ไหนเข้า/ออก
s(config-if)# switchport mode access → # switchport port-security → เลือก 1 ประเภท
Secure MAC Addr → ① Static :: s(config-if)# switchport port-security mac-address MAC ADD
② Dynamic :: s(config-if)# switchport port-security mac-address sticky
กรณีเพิ่มจำนวน MAC. # switchport port-security maximum MAX
Violation Mode : ① Protect :: Security violation protect Mode
② restrict :: Security violation restrict Mode → ส่งไปเตือนว่ามีการละเมิด
③ shutdown :: ~~~~ shutdown Mode → default

for Staples

for Staples

Gate way

□ Addr Resolution Protocol (ARP) : ARP cache เก็บ Mac Addr ไว้ Map หาปลาย dest. (ถ้าไม่ทราบต้องหา MAC)

IPv4 : classless : Variable length Subnet Masking (VLSM) : แบ่งตามความต้องการ เลือกจากขนาดใหญ่ → เล็ก
- Fixed ~ แบ่งทุก nw เท่ากัน

นาย ศุภกิตติ์ อารีจิตสกุล แผ่นที่ 5 58011257

Chapter 8 LAN Redundancy & Spanning Tree Protocol (STP)

▷ Issue with Layer 1 Redundancy :: ① MAC addr instability → MAC addr table จะไม่เสถียร เพราะได้รับจากหลายพอร์ต ② Broadcast storms → วนส่งไปเรื่อยๆ ③ Multiple frame transmission → Start : Unknown unicast → หาไม่เจอ dest. ได้รับหลาย frame [เพราะ source ส่ง 1 frame]

▷ STP → ลูกหลาย ขาด block port → block มัน → ไม่ให้เกิด traffic ซ้ำ เมื่อเกิดลูป

□ ขั้นตอน : ① หา Root Bridge ≥ เลข priority น้อย | Rule : [1] 1 RB/1 NW [2] 1 RP/1 RB [3] DP/segment |

ดูจาก BPDU ② หา path cost all · ③ หา Root port → path cost น้อย → อีกฝั่งจะเป็น Designated Port

(Bridge protocol data Unit) ③ ส่วน segment ที่ path cost เท่ากัน → ดู BID น้อย เป็น Designated port → อีกฝั่งเป็น block port

↳ ใช้ RB ที่ Source [802.1D]

ลำดับที่ใช้ตัดสิน
1 BPDU flag 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

(ถ้า S1, S2 เป็น RB) S2(config)# ⟶ secondary [verify : show spanning-tree]

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

• PVST + (พัฒนาจาก IEEE 802.1D STP) → เพื่อ workload balancing โดยแยก root/VLan [verify : show spanning-tree active]

• Rapid PVST+ → มี Alternate port (ไม่ได้ block ไปเลย สำหรับเปลี่ยนเมื่อลูปเกิดปัญหา)

↳ หากจะ set Edge Port @ port ต่อ host, router : #. spanning-tree portfast

↳ link type : port ที่เชื่อมระหว่าง SW ต้องเป็น point-to-point

- if #. spanning-tree bpduguard enable → port นี้ไม่ควรรับ BPDU ในห้อง

→ Config : S1(config)# spanning-tree mode rapid-pvst → # int ทุกtop # spanning-tree link-type point to point

[ทำ clear all : clear spanning-tree detected-protocol]

Protocol	Standard	Resource	Convergence	Treecal
STP	802.1D	low	slow	All VLANs
PVST+	Cisco	High	slow	Per VLAN
RSTP	802.1w	Me	Fast	all VLANs
Rapid PVST+	Cisco	very H	Fast	Per VLAN
MSTP	802.1s Cisco	Me or H	Fast	Per instance

Chapter 9 VLANs & Inter VLAN

▷ VLAN = การ partition [แบ่งแยก : อยู่ภายใน NW or broadcast domain ที่ Layer 2 ใน SW เดียวกันคนละกลุ่มอยู่ได้ ใน VLAN เดียวกัน

□ ข้อดี : - security ดีขึ้น, - ลด cost, - ประสิทธิภาพ ↑, - broadcast domain เล็กลง, - ประสิทธิภาพ ด้าน IT, จัดการ ง่าย. [verify : show VLAN brief]

□ in a Multi-SW Environment

• VLAN Trunk : set ที่ intf ที่เชื่อมต่อระหว่าง SW ทั้ง VLAN → can carry ข้อมูลได้ > 1 VLAN

↳ config : เข้า intf → if)# switchport mode trunk [verify : show int f0/0 switchport]

• Tagging Ethernet Frame (IEEE 802.1q) : Ethernet Frame → | Dest MAC | Src MAC | Tag | Type/length | Data | FCS | → Tag จะบอกข้อมูล VLAN ส่งผ่าน Trunk

Native (base) VLAN ไม่ต้องมี tag, untag → ส่งผ่าน intf ได้ไม่ติด

□ Assignment : VLAN number → 1-1005 เก็บ config @ vlan.dat (ใน Flash)

⇒ 1006-4094 เก็บ config @ running-config (ใน NVRAM)

สร้าง : I S(config)# vlan vlan_num → vlan# NAME

II S# vlan database → (vlan)# vlan name ...

assign port ให้ vlan : เข้า intf → -if)#. switchport mode access → # switchport access vlan

• verify : show vlan name ..., show vlan summary show int vlan num

▷ Inter-VLAN Routing → router set เป็น trunk โดยใช้หลัก "sub interface"

□ Config : ① set basic routing (set ip address, no shutdown) [verify : show vlan, show ip route, show running]

② R(config)# interface g0/0.10 ~ VLAN → -subif)# encapsulation dot1q → #. ip-address ip subnet-mask

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

▷ VTP [msg : ISL or IEEE 802.1Q] → การ Manage SW VTP จะเป็นการ manage ใน domain

□ Operation : การ update VTP ด้วย version number 32 bits (0-4294967295) เพื่อดูล่าสุด

↳ 3 Mode ① server → can สร้าง, remove, rename, VLAN ทุกตัวใน domain เดียวกัน

② Client → รับข้อมูล VTP มา process ส่ง VTP msg ออกทุก trunk

③ Transparent → can สร้าง, remove, rename ได้แค่ตัวเอง เป็นแบบ local

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

□ Config : 2 แบบ ต้องใช้ 1) SW Cisco 2) มี Trunk เชื่อมระหว่าง SW ต้องอยู่ domain เดียวกัน 3 mode [NAT แปลง private ip → public (real ip)]

① In global configuration S(config)# vtp version → # vtp domain ชื่อ → # vtp password pass → # vtp mode server mode อื่น

② In VLAN con ~ S(VLAN)# vtp v2-mode ↗ [verify : show vtp status/counters] ↘ #. vtp server | Client | transparent

□ Pruning → Manage ให้ traffic ส่งไปเฉพาะใน interface ที่ต้องการ โดย config ที่ interface ที่ไม่ต้องการให้ส่ง VLAN

NAT □ Terminology 4 type ① Inside local Addr. (Private ip) ② outside local Addr. ③ Inside global Addr. ④ outside global addr.

□ type : ① static : กำหนดตายตัว (map : 1 ต่อ 1) → ① R(config)#. ip nat inside source static local-ip global-ip

② Dynamic : มี pool ของ Global / Real ip (map : ตัวหนึ่ง ⇔ 1 ตัว แต่เปลี่ยนไปเรื่อยๆ) 1.1 # ip nat pool ชื่อ start-ip map-ip

③ PAT (Port Addr. Translation) → port ทำหน้าที่แยกข้อมูลสำหรับ NW addr. (map แบบ 1 ↔ 1) 1.2 set ACL 1.3 ip nat inside source list

□ config 3 ส่วน ① NAT ② INSIDE : R(config-if)#. ip nat inside ③ Outside : R(config-if)# ip nat outside

config อีกรูปแบบ PAT (single addr.) 1.1 สร้าง ACL 1.2 ip nat inside list ACL-num interface f0/0 overload

□ verify : show ip nat translations

ชื่อ-สกุล ศุภวิทย์ อารีจิตสกุล กระดาษแผ่นที่ 5 รหัสนักศึกษา 58088253

for Staples

Chapter 11 EIGRP IPv6 & Routing.

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

IPv6	VS	IPv4
128 bit		32 bit
base 16		base 10

	Distance Vector Routing P.		Link State Routing		Path Vector EGP
Classful	RIP	IGRP			EGP
classless	RIP v2	EIGRP	OSPF v2	IS-IS	BGP v4
IPv6	RIPng	EIGRP for IPv6	OSPF v3	IS-IS for IPv6	BGP v4 for IPv6

▸ EIGRP (Enhanced IGRP)

□ Characteristics (ลักษณะประจำตัว)

◦ Basic features ▵ cisco-propertietary (ใช้งานเฉพาะ Protocol ของ cisco) เปิดใช้ 1992

⊕ สร้าง classless version of IGRP ⊕ ทางเลือกที่เหมาะสมที่สุดสำหรับ หลายๆ protocol, เหมาะกับเครือข่ายที่สร้างบน cisco router เป็นหลัก

• DUAL (Diffusing Update Algorithm) = การันตี loop-free & backup ทั่วทั้ง routing domain → หา best path

→ ทำให้ routing ทำงาน very fast convergent (มี convergent time < ของ OSPF) รวมทั้ง Back up Path ทำให้เร็วขึ้น → ถ้า link down เลือก Path ใน Backup ได้เลย

▾ Establishing Neighbor = เชื่อมความสัมพันธ์กับ directly connected EIGRP routers.

▾ Reliable Transport Protocol = RTP provide delivery of EIGRP protect to neighbor

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

▾ Partial and Bounded. - Update เฉพาะส่วนที่มีการเปลี่ยนแปลง รวมทั้ง update ไปให้เฉพาะที่มีการเปลี่ยนแปลง

▫ Equal and Unequal cost = ทำให้ Admin ดูแลระบบ เพื่อกระจาย traffic รับข้อมูลเครือข่ายได้มากขึ้น

Load Balancing

▵ ใช้ protocol-dependant Modules (PPMs) เพื่อรองรับ protocol ที่แตกต่างกัน เช่น IPv6, IPv4, Legacy Protocol

▵ PDMs รับผิดชอบ - Maintain EIGRP Neighbor and topology table

for Staples

- คำนวณ metric ที่ใช้ DUAL - เชื่อมต่อ DUAL และ routing table
- implement filtering and access list - ทำ redistribution with other routing protocol

▵ RTP is EIGRP transport layer protocol สำหรับ delivery & reception ของ EIGRP packets

▵ ไป = เป็น Msg ที่อยู่ใน Application Layer ใช้ maintain ข้อมูล, msg ต่างๆ ที่แสดง EIGRP

▵ ไม่ใช่ทั้งหมดของ RTP packet จะส่งได้แบบเชื่อถือ (msg ≈ OSPF)

- Reliable packet require explicitc (ชัดเจน) ack จาก dest. - Update, Query, Reply
- Unreliable packet do not require ack จาก dest. - Hello, Ack

▵ รองรับ Authentication (no enrypt routing update)

▵ Packet Type

① Hello → ทำให้ Adjacencies ระหว่าง router 2 ตัวที่เป็น neighbor กัน ② Update → update info dest., update info ของ routing ไป neighbor router

③ Acknowledgement → พอได้รับ การ update ก็ตอบ Ack ④ Query → request info routing จาก neighbor router

⑤ reply → หลังจากได้รับ query ก็ reply.

□ IPv6 Routing

◦ Config static route

R(config)# ipv6 route

ใส่ก่อน config อะไรก็ตาม routing ipv6 ipv6 unicast-routing. เพื่อเปิดใช้งาน

▵ verify: show ipv6 route static, show ip route ipv6, show running-config section ipv6 route

▵ Default static IPv6 remote

R(config)# ipv6 route ::/0 | ▵ verify show ipv6 route static

◦ Config EIGRP for IPv6

for Staples

\# ipv6 unicast-routing

\# ipv6 router eigrp

\# eigrp router ip ~~ รูปแบบ IPv4

\# no sh

▵ Network Command → ipv6 eigrp

passive-interface สามารถใช้ได้ global config save ด้วย

▵ verify: show ipv6 eigrp neighbors, show ipv6 protocols, show ipv6 route

ศุภวิดาญ์ อารีจิตสกุล รหัสนักศึกษา 58011257

RIP [Dynamic] ต้องกำหนด version ที่ต้องการใช้งาน ใช้ distance vector ในการหาเส้นทาง โดยพิจารณา hop และแลกเปลี่ยนเราเตอร์ เทเบิล กับเราเตอร์เพื่อนบ้าน การส่งข้อมูลแบบ broadcast ทำให้ traffic เปลือง ข้อเสียเรื่อง convergence time และใช้เวลานาน next hop สูงสุด 15 ตัว ง่ายแก่การคอนฟิก.

OSPF (Open Shortest path first) [Dynamic] กำหนด process id, wildcard, area ใช้อัลกอริทึม Shortest path first ในการคำนวณเส้นทาง พิจารณาจาก bandwidth ทำความรู้จักเพื่อนบ้านโดย hello ส่งการอัปเดตสถานะของลิงค์ไปให้เพื่อนบ้านและให้เพื่อนบ้านสร้างแผนภาพรวมและคำนวณเส้นทางเอง โดยไม่ส่งเราเตอร์เทเบิลไปให้เพื่อนบ้าน

EIGRP [Dynamic] ต้องกำหนด Autonomous number และ wildcard ทำความรู้จักเพื่อนบ้านด้วย hello และทำอัปเดตเฉพาะส่วนที่เปลี่ยนแปลงไปให้เพื่อนบ้าน เมื่อมีการเปลี่ยนแปลงจะเปลี่ยนเฉพาะในส่วน topology table ซึ่งจะมีรายละเอียดของเส้นทางนั้นๆ เช่น subnet ของปลายทาง ค่า cost ซึ่งข้อมูลเหล่านี้เป็นเส้นทางสำรองที่อาจไม่ใช่ทางหลักใช้การไม่ได้ จะสามารถนำข้อมูลใน topology table มาใช้งานได้ทันที ทำให้ convergence time น้อยมาก

VLAN [ไม่ใช่ protocols!] (virtual Local Area Network) การแบ่งแยก VLAN เป็นการแยก broadcast Domain ออกจากกัน หรือเป็นการแบ่งกลุ่มของ NW ออกจากกัน การแยกอาจแบ่งเป็นแผนก, หน้าที่การทำงาน, หน่วยงานย่อย

ประโยชน์ของ VLAN
- จำกัดการแพร่กระจายของ broadcast traffic ไม่ให้ส่งผลกระทบต่อประสิทธิภาพโดยรวมของ NW
- สร้างกลไกลควบคุมความปลอดภัยได้ง่ายขึ้น เช่น การใช้ access list control บนอุปกรณ์ Layer 3 และลดความเสี่ยงเรื่องการดักจับข้อมูล (sniffing)
- รองรับการขยาย NW ที่จะเพิ่มขึ้นในอนาคตได้ง่าย เนื่องจากสามารถแบ่ง Subnet

STATIC เป็น routing Protocol ที่กำหนดค่าแบบคงที่เข้าไปในตัว Router เพื่อบอกให้ Router ทราบว่าต้องส่ง packet ไปยัง Subnet Addr. ต่างๆ จะต้องส่งไปหา Router ตัวถัดไป (Next Hop Addr.) ตัวไหน หรือจะให้ Router ส่งออกไปทาง Interface ใด

VTP (VLAN Trunk Protocol) เป็นโปรโตคอลที่ช่วยลดขั้นตอนในการจัดการ VLAN ของสวิตช์ในระบบเครือข่าย โดยทำให้มันสามารถทำการเปลี่ยนแปลงการตั้งค่า VLAN ต่างๆ บนอุปกรณ์กลางเพียงที่เดียว ไม่ต้องไปทำการตั้งค่าบนสวิตช์ทุกๆ ตัว ซึ่งทำให้การจัดการ VLAN บนระบบเครือข่ายมีความสะดวกมากขึ้น

IPv6 Addressing: 128 bit แบ่งเป็น 8 ส่วน [1 ส่วนมี 2 byte = 16 bit] → represent base 16 ทุกๆ 4 bit แก้ปัญหา ip มีจำนวนจำกัด (privat ip, NAT) ใช้ใน IoT ได้

NAT การแปลง IP Addr. ของเครือข่ายภายใน ให้เป็น IP addr. NAT ให้ประโยชน์มาก เช่น สามารถใช้ไอพีแอดเดรสใดก็ได้ขึ้นมาเองได้ (เป็น IP ที่ไม่ต้องจดทะเบียนบนอินเทอร์เน็ต) เพียงแค่ใช้ไอพี Addrs ในบริการอินเทอร์เน็ตมากพอ อีกทั้งยังสามารถซ่อน IP ภายในเครือข่ายได้ ทำให้มีความปลอดภัย ★ การทำ NAT จะเป็นการแปลง private IP ให้เป็น IP ที่สามารถใช้บนอินเทอร์เน็ตได้ หรือเราเรียกว่า Registered IP (Firewall ใช้ 65,535 port) (สำหรับ Server 1024 ports) ดังนั้นจะมี ports คงเหลือ 64,511