ชื่อ-สกุล นิติพันธ์ เพ็งเลา กระดาษแผ่นที่ 1 รหัสนักศึกษา 59080738

for Staples

Ch1

Component of Network → Hardware, software
- End Device
- Intermediary network device
  - ↳ Network Access Device } ตัวกลางต่างๆ
  - ↳ Internetworking Device
  - ↳ Security Device
- Network Media → สื่อต่างๆ
- * topology diagrams ที่บอกตำแหน่ง NW บอกแบบละเอียดว่า port ไหนต่ออะไร

Type of NW.
- NW size
  - Small Home NW
  - Small Office Remote ผ่านได้
  - M-L NW : 100-k
  - World Wide NW : 100-M
- LAN → ดูแลด้วย Admin คนเดียว
- WAN → หลายคน
- MAN
- SAN
- WLAN
- PAN

Reliable NW
- Fault tolerance
- Scalability
- Security
- Quality of Service

Protocol Model
Reference Model → OSI

Protocol
- App → Host Conf [BOOTP, DHCD]; Email — SMTP, POP, IMAP
- Trans → TCP, UDP
- Internet Ly → IP NAT; IPSup — ICMP; Routing [OSPF, EIGRP]
- NW Access Ly — ARP, PPP, Ethernet, Interface Driver

Intermediary NW Device
- Hub, Repeater → CSMA/CD
- SW, Bridges → Learning / Flooding / Filtering — ไม่ปลอดภัยสุด
- Router — เลือกทางออก

สาย
- CAT5 10/100 Mbps
- CAT5E 10/100/1000 Mbps
- CAT6 1000/10Gbps

NW Diagrams มี 2 type → ① Physical บอก interface เชื่อมกันยังไง (เห็นภาพ) ② Logical บอก IP

Type of Connection in a LAN
ข้อจำกัด (UTP Cat5) : ① BW = 100 Mbps ② ยาว 100 m
2 type ① ตรง ② Cross → ต่ออุปกรณ์เหมือนกันเข้าด้วยกัน SW-hub PC--router
- WLAN Connection → เชื่อมระหว่าง Router
  - ↳ 2 ฝั่ง → DCE (♀) → ต้องมี command clock rate 56000
  - ↳ DTE (♂)
- สาย Console (Rollover Cable) → router ---- PC
  - ⇒ Manage command ต้อง [RJ-45-to-DB-9; Adapter labeled TERMINAL]

Ch2 Basic Router Configuration.

Port Addr กำหนดโดย IANA
- 0-1,023 → well known port — destination port
- 1,024-49,151 → Reg port = Public ทุกคนใช้
- 49152-65535 → Dynamic or Private port "Randomly Generate" source port

Ex FTP : 20 data 21 control; STMP : 25, DNS : 53; HTTP : 80, HOST52 : 81

IPV4 แบ่งเป็น 5 class ใช้ที่ Ly 3
- class A — NW Host H H 0-127
- class B — NW NW H H 128-191
- class C — NW NW NW H 192-223
- class D — 224-239 multicast
- class E — 240-255 experimental

192.168.1/24 prefix range
255.255.255.0 broadcast IP
192.168.1.255 broadcast NW
255.255.255.255 ทุกเครื่องใน NW ได้

Private IP — IP ที่เกิดขึ้นในโลกของ Internet; ช่วยในสามารถใช้งาน internet ได้มากขึ้น

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

Message Delivery
- Unicast ส่งจากต้นทางไปปลายทาง NW เดียวกัน
- Broadcast ส่งหาทุกเครื่อง เช่น DHCP, ARP ใน NW เดียวกัน — broadcast IP 255.255.255.255
- Multicast ส่งหาหลายเครื่อง รับเฉพาะเครื่องที่เปิดรับ service นั้นๆ เช่น CSGO — เริ่มต้นด้วย 01-00-5E-XX-XX-XX

Physical Addr (MAC) เป็นเลขฐาน 16 : 12 ตัว
ก่อตั้ง IEEE → กำหนด 3 byte code "organizationally Unique Identifier (OUI)"
↳ กฎ ① ทุก MAC กำหนดให้ NIC หรือ Ethernet device อื่นๆ ใช้ out 3 byte แรก
② ทุก MAC ที่ out เดียวกันต้องกำหนด unique ที่ 3 byte สุดท้าย

CISCO IOS → function 1) Addressing 2) Interface 3) Routing 4) Managing Resource 5) Security 6) QoS

Router & SW Boost Sq
- ROM 1) POST (Power On Self Test)
- 2) Run boost loader SW mini IOS
- RAM 3) Boost loader does low-LV CPU init
- Flash 4) " — " init the flash file system
- TFTPServer 5) " — " locates & load a default IOS และ run บน RAM

Navigating the IOS → 2 mode
1. User mode → ">"
2. Privileged → "#"
   - ↳ Global Config → "(config)#"
   - ↳ Other " — " → "(config-mode)#"

The command Structure
① Help → ?
② Check → enter
③ Shortcut
④ IOS Examination Command → show...

Setting Basic
① ตั้งชื่อ hostname router(config)# hostname name
② จำกัดการเข้าถึง
③ กำหนด Interface Addr
④ ตรวจสอบ config & ก.เชื่อมต่อ
⑤ Save Config router# copy running config startup-config
- → Banner Msg Router(config)# banner motd # text #
- → Security Device Access :: Enable pass, Enable secret, Console pass, VTY Pass, Encrypt Pass Display

for Staples

③ Addr Device.
1) เลือก Interface to config
- Phy 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)# ipaddress ipaddr subnetmask
" ——— " no shutdown

④ Verify Connectivity → คำสั่งเพิ่มเติม section, include exclude, begin
Router # show running-config
show startup-config
show ip route
show interface
show ip interface
show ip interfacebrief show interfaceแบบสรุป
traceroute
ping
PC > ping
" — " tracert
" — " route ping
" — " nslookup

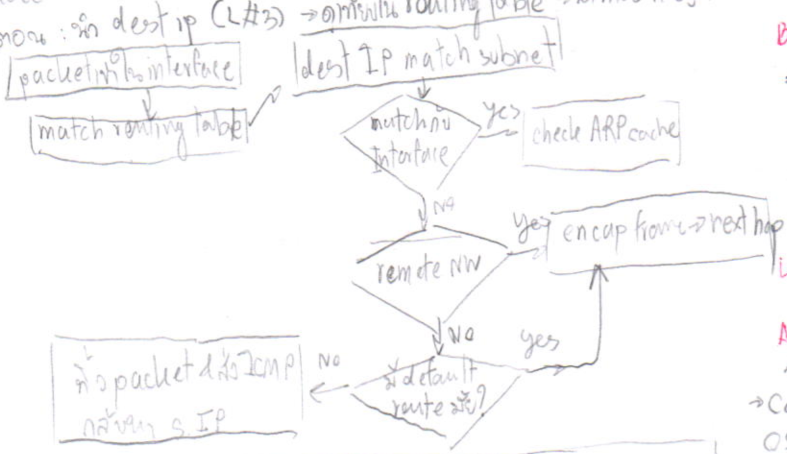
Ch8 Static Routing & Dynamic Routing Protocol

~~Connect Devices~~

- Function of Router → Characteristic
① Topology ⑤ Avalibility
② speed ⑥ Scalability
③ cost ⑦ Reliability
④ security
- Packet Forwarding Methods
① Process switching = ทุก packet ที่เข้า router ↑ process ที่ CPU ↓ ออก interface ไหน?
② Fast switching = มีตัวช่วยทำให้ forward ได้เร็ว ↑
③ Cisco Express Forwarding (CEF) = forward packet ได้เร็วสุด

connect Devices.
▷ Default Gateway → เป็นได้ ① first usable host (.1) ② last usable host (.254)
→ ทางออกเชื่อมไป NW อื่น
▷ Enable IP on a Host :: ① Statically Assigned IP addr
② Dynamically " ——— " → สามารถกำหนด ip ได้เมื่อมี NW มี DHCP

- Sw Packet Between NW
ขั้นตอน : หา dest ip (L#3) → ดูที่ใน routing table → หาทางออกไปดูที่ไหน MAC addr. → ใส่ dest MAC (L#2)



Best Path : lowest metric (cost)
=> Dynamic routing protocol ใช้
① RIP → จำนวน hop
② OSPF → BW มากสุด
③ EIGRP → Bw, delay, load, reliability
Load balancing → กรณีมี 1 เส้นทาง
→ ให้ทุกเส้นทางไปเท่ากัน
Administrative Distance (AD) "trustworthiness"
ระยะห่างจากผู้ดูแลถึง protocol ต่างๆ
→ Connected = 0, Static = 1, Internal EIGRP = 90
OSPF = 110, RIP = 120

- Routing
1) Static Routing
ข้อดี ปลอดภัย, Resource น้อย, ลด routing entity
ข้อเสีย : ลำบากในการขยาย / เปลี่ยนทาง
ใช้กับ NW เล็กๆ, ทางออกเดียว stub NW
4 type ① standard ② default ใช้ตอน ip ไม่ match
③ Summary ④ floating (backup)
Router(config)# ip route nw-addr subnet-mask {ip addr | ext-intf}

The Routing Table

		AD				
D	10.1.1.0/24	[90/2170112]	via 209.165.200.226	00:00:05	, Serial 0/0/0
บอกว่ามาจาก dest ไหน	Dest ที่รู้จัก	cost ของ protocol	Nxt Hop Addr		ออกทางนี้

Classful Addressing → update ตาม class
Classless Inter-Domain Routing
▷ Summarization rip summarize นั่นแหละ
▷ VLSM
Fixed Length Subnet Masking วิธีหา ① prefix ใหม่ - เก่า ได้จำนวน bit ที่เหลือ
② หลังจากหา bit เป็น 1 แล้ว เอาฐาน 10 ไป + ip ที่ตัดสินกัน +1 วนไปเรื่อยๆ

Config : Next-hop option
สมมติ R(config)# interface G 0/0
" ——— "-if)# ip address 172.168.1.0 255.255.255.0 } ทำทุก interface
" ——— " no shutdown
R1(config)# ip route 172.168.1.0 255.255.0 → 172.168.1.2 } ได้ 2 แบบ
หรือ 0/0/0

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

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

ชื่อ-สกุล นิธินันท์ เพ็งเลา กระดาษแผ่นที่ 2 รหัสนักศึกษา 59010734

for Staples

Chapter 4 RIP V.1

fn ของ Dynamic Routing → 1. Share information 2. Update routing 3. best path

Component of Routing Protocol 1. Algorithm หาทางดีที่สุด 2. Routing Protocol msg ที่ติดต่อเพื่อนบ้านและแลกข้อมูล

Purpose of dynamic Routing → 1. Discover remote network 2. ปรับปรุง routing information 3. find Best Path 4. หา Path เพื่อบอกเส้นทาง

classifying

Dynamic Routing → Exterior Gateway Protocols → BGP
Dynamic Routing → Interior Gateway Protocol
- Distance vector
  - RIP → RIPV2
  - IGRP → EIGP
- Linkstate
  - OSPF
  - IS-IS

IGP 1. Distance Vector 1. ใช้ระยะกับทิศทาง 2. incomplete view of NW topology 3. อัพเดทตามคาบ
2. Link State 1. Complete view 2. ไม่อัพเดทรายคาบ

* Convergence กำหนดค่าเมื่อ routing table & state ที่มั่นคง
Metric : ค่าที่ใช้ตัดสินใจเลือกเส้นทาง • Hopcount (RIP) • BW (OSPF) • load • Reliability • Cost • Delay

Administrative Distance (AD) เป็นค่าที่เอาไว้บอก route เฉพาะ (เลือก Protocol)
EIGRP: 90 OSPF: 110 RIP: 120 Connected: 0 Static: 1

Distance Vector Routing Protocol : ลักษณะ 1. Periodic Update 2. Neighbor 3. Brodcast update 4. ทั้ง routing table ต่อการ update.
เกณฑ์ที่ใช้เปรียบเทียบ protocol • Time to convergence • Scalability • Resource Usage • Implementation & maintenance

Network Discovery จะ Learn จาก Router ข้างๆ

Routing table Maintance → RIP Update time (30) Invalid time (180) Hold down timer (180) Flush timer (240)
• Bounded Update: EIGRP อัพเดทแค่ที่มีการเปลี่ยน
• Triggered Update → update เลยไม่รอคาบ
• Random Jiter ใช้ NW เป็น multi acc ของหลายตัวเชื่อมกัน ถ้าเกิดชนกันตอนนี้จะใช้ Random

การเกิด Routing Loop เกิดจาก NW down แต่ยังส่ง update แล้วจะส่งวนกลับไปมา
เกิด count to infinity เพราะค่า Hop เกิน เลย Set Max ไว้ 16 / ใช้ Split Horizon ส่งไปทางที่ไม่ได้ Learn
→ Split Horizon with poisen reverse ส่งค่านั้น Hop 16 ไปบอกด้วย *
→ เพื่อปกติ ถ้าเป็น Loop พอค่า Time to Live หมดจะ Lost ไปเอง
→ แก้ Routing Loop

→ Network Discover (ทำ Basic Config ก่อน)
3 state ① Cold Start
② Initial Exchange of Routing information
③ Exchange of Routing Information

① set max hop 16 = unreachable ② holddown timer ถ้า down → hold ③ splithorizon ไม่ส่งข้อมูลกลับทางเดิม ④ Routing Poision 1) เกิด down set unreachable 2) ส่ง unreachable ที่ poision ออกไป ให้ int นั้น hop = 16
③ และ ④ ถ้าเกิด unreachable จะ overrule split horizon โดยส่ง ip inf ที่ down
⑥ IP & TTL จะหยุดเมื่อ TTL = 0

	RIPV1	RIPV2	IGRP	EIGRP
speed convergence	slow	slow	slow	fast
scalability	small	small	small	large
Use of VLSM	×	✓	×	✓
Resource Usage	Low	Low	Low	medium
implementation maintance	simple	simple	simple	Complex

RIPV1 AD = 120
คุณสมบัติ classful, DV. metric = hop count • hopcount > 15 unreachable
• update brodcast ทุก 30 s

encapsulated ใน UDP segment ส่ง Source & Dest port 520

Datalink Frame	IP Packet header	Udp Segment Header	RIP msg

0 1 req 2 reply 7 8 15 16 ขอ full routing table 23 24 31

	Command 1 or 2	Version 1	Must be zero
Route Entry	Address family identifier (2 = IP)		Must be zero
	IP Addr dest		
	Must be zero		
	Must be zero		
	Metric (Hop) 1-15 ตัวจาก table +1 ส่งออก		
	Multiple Route entrie upto a max of 25		

• msg มี 2 แบบ
① Request → ขอ routing table → ไป intf ที่ config ไว้เพื่อรับการ update
② Response → ส่ง Info ของ routing table

• Basic RIP Config ① ทำ basic config ② สั่ง router rip + ใส่ NW
• Verification & troubleshooting : show ip conf show ip route ip protocol, debug ip rip
• Passive Command (ไม่อัพเดทที่ไม่ต้องการ) R(config-router)# passive interface intf-type (Fa/0/5) intf-number (0/0, 0/0/0)
• Automatic Summarize ทำเพื่อลดขนาด Routing table
ข้อดี ลดขนาด routing update • single router แสดงแทนให้ภายใน
← multiple route ที่มากในร routing table
ข้อเสีย ไม่ support discontiguous NW (major เหมือนกันแต่ไม่ติดกัน) ถ้าเกิด load balance ได้

boundary Router: Summarize RIP subnet from 1 major NW to another

Processing RIP Update
ดูว่าที่ส่งตัวที่ update ไป (intf) ว่าเป็น classful เดียวกันไหม?
→ ใช่ update subnetwork ex. 172.16.1.0
→ ไม่ใช่ update classful ex 172.16.0.0

Default Route & RIPV1 ทำให้เลือกทางออกใน routing table
ตามเฉพาะแต่ละ protocol → จะออก default route

for Staples

R(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1
default info. originate command → เพื่อ update ไปใน กรณีว่าเชื่อม: static ↔ dynamic
Router ที่อยู่ระหว่าง 2 protocol ← R(config-router)# default-information originate

Chapter 6 RIPV2 & ACL

RIPV1 & RIPV2

classful & classless

not support discontiguous subnet

not support VLSM เพราะไม่ส่ง subnet mask 255.255.255.255

Routing Update → Broadcast

ใช้ Timer ป้องกัน Routing loop ใช้ split horizon or split horizon with posion reverse
ใช้ triggered update maxhop count -15

update nexthop addr.
ใช้ authentication routing
(รับ discontiguous ขาวกันได้)
Routing Update → Multicast

ข้อจำกัดของ RIPV1.
เป็น virtual interface สามารถเพิ่มในrouting ใช้update ออกไปได้
- loopback intf → ping ไป ip virtual intf → reply ได้.
- Null Intf → ใช้ดักคนที่จะเข้ามา channel ที่เราไม่ต้องการ → วิ่งออก

null intf → packet discard เอง → timeout

- static route & null intf → null intf เป็นทางออกของ static route

R(config)# ip route summary-static-route subnet-mask Null 0 (major-nw) → ของ static subnet route

- Route Redistribution → อยากให้ rip รู้จัก static ตัวที่เพิ่มใหม่ โดยส่ง static ไปด้วย : R(config-router)# redistribute static
- Verify & test connectivity : show ip interface brief, ping, traceroute
- RIPV1 ไม่ส่ง subnet classful summarize nw @ major boundaries

ตรวจ routing table debug ip rip (content of routing update) ถ้าเป็น RIPV1 จะไม่ได้รหัส subnetmask ใน nw addr

RIPV2

0	7 8	15 16	23 24	31
command 1 or 2		Ver 2	Must be zero	
Addr family iden (2=IP)			Route tag	
IP				
Subnet				
Nexthop				
Metrics (Hop)				
Multiple Route Entries max 25				

- Config
  - Enabling & Verify RIPV2
  - Config RIP → RIPV1 → รับได้ทั้ง V1 & 2 แต่ส่งได้แค่ V1
    - ↳ RIPV2 → รับ & ส่งได้แค่ V2
  - Auto-summarize & RIPV2 → auto sum route @ major nw boundaries
    - → sum route ของ subnet ที่น้อยกว่า classful subnet
  - disabling Auto-summary : no autosummary เพราะเมื่อนั้น nw topology ต้องเป็น discontiguous

verify show ip route, debug ip rip

- VLSM & CIDR → verify info. ที่ส่งโดย RIPV2. → VLSM : เผยแพร่ nw addr & subnet → CIDR : ใช้ supernetting (bunch ของ contiguous classful nw ที่เป็น addr เหมือน single nw)

ACL ดูคนที่เข้าออก ดูจาก Conversation ดูว่าใครคุยกับใคร

Packet filtering ดู ① dest, source @ L2 ② protocol ที่ใช้ ③ ไปไหน ที่อยู่ → ทำการให้ผ่านหรือ block ไว้

Operation → ทำตามลำดับ seq → last statement เป็น implict deny → block → discard

inbound → ⊗ → outbound

Standard IPV4 ACLs vs Extended IPV4 ACL

- check source addr.
- ปกติ permits or denies ทั้งชุด protocol
- number ACL : 1-99 & 1300-1999

- check source & dest addr.
- ปกติ permits or denies เฉพาะ protocol
- number ACL 100-199 & 2000-2699

wildcard → invert subnet mask
- → 0 = match/fix , 1 = ignore ค่าใดก็ได้
- → วิธีหา set ของ ip ① หาจำนวนเลข bit ที่ซ้ำกัน ใส่ wildcard mask ตำแหน่งนั้น = 0 ② ที่เหลือ 1 ถ้าหาไม่ได้ให้แยก pattern ส่วนที่ต่าง สุดท้าย wild card จะเหมือนกัน
- → หา wildcard ของ subnet = 255.255.255.255 - subnetmask
- → keyword → 0.0.0 = match all ใช้ host
  - → 255.255.255.255 = ignore all ใช้ any

- Guildline for (3Ps) → One ACL/protocol = ctrl traffic flow บน intf, ACL จะต้อง define แต่ละ protocol enable บน intf

ACL Creation → one ACL/direction = ctrl traffic direction ที่เวลาบน intf, แยก ACL ctrl in & out bound traffic
- → One ACL/interface = ACL ctrl traffic for an intf, Ex G0/0

※ Extend ACL : @ close source → standard ACL : @ close destination

Config ACLs → standard
- → number
- → ชื่อ

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

Router(config-if)# ip access-group
 { access-list-number | access-list-name
 { in | out }

remove all : no access-list
ถ้าแก้ • no access list num #
 ↳ ส่งใหม่
• no บรรทัด # → บรรทัด # คำสั่ง
ถ้า remove all : no ip access-group
ถ้าแก้ → บรรทัด # คำสั่งใหม่
 ↳ บรรทัดที่จะแทรก

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

ชื่อ-สกุล นิธินันท์ เมืองลา กระดาษแผ่นที่ 3 รหัสนักศึกษา 59010734

for Staples

verify : show ip interface, show access-list
Securing VTY Port → ใช้เฉพาะที่จะให้เข้า
Router (config-line)# access-class access-list-number {in [vrf-also] | out}

Extended : filter source/dest addr., protocol, port number
access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operater operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name] [estabilished]

ทำเหมือนเหมือน standard มีทั้ง number ทั้ง name
-debug-output : debug ip packet ACL-number

Chapter 6 OSPF & DHCP

Link-state Routing Protocol เป็น protocol ที่ต้อง map nw topology ก่อนจากนั้นหา shortest path first

เหมาะกับ
- nw ใหญ่
- fast convergence
- admin มีความรู้ความเข้าใจ

ขั้นตอนการ update
1. Learn info ของ Link
2. Say hello neighbor
3. เอา Info มาสร้าง Link state packet
4. router flood LSP to all neighbors → รับแล้วเก็บลง db
5. router เอา all LSP เก็บใน db (รูปแบบ tree) + Adding OSPF → routing table

ข้อดี
1. สร้าง topology map สามารถหา shortest path
2. fast convergence ข้อมูลที่เปลี่ยนแปลง
3. LSP ส่งเฉพาะข้อมูลที่เปลี่ยน แล้วคำนวณ shortest
4. hierarchical design (nw ใหญ่จะทำ) → ลด resouce เพราะแลกข้อมูลแค่ใน area

ข้อเสีย
1. ใช้ memory ในการเก็บ Linkstate เยอะ
2. ใช้ CPU ในการคำนวณ
3. ตอนส่ง LSP ใช้ BW เยอะ

for Staples

☆ OSPF Protocol (AD = 110)
3 Table
1. Neighbor show ip ospf neighbor
2. Topology (ทั้ง map) show ip ospf database
3. Routing (มี shortest path)

• msg Encapsulating OSPF MSG : MAC Addr Dest Multicast : 01-00-5E-00-00-05 or 01-00-5E-00-00-06
Protocol field = 89

type OSPF Packet : 01 Hello → ทุก 10 s (default : multiaccess & point to point nw), ทุก 30 s (default : non-broadcast multiaccess (NBMA) nw), cisco default 4 times (40s)
: 02 Db Description (DBD) → synchronization db info
: 03 Link-state Request (LSR) → request link-state
: 04 Link-state Update (LSU) → send update link-state
: 05 Link-state Acknowledgment (LS Ack) → ตอบกลับได้เลย

• operation : สร้างการเชื่อมต่อ (1) Down state (เริ่มต้น) (2) init state (ส่ง Hello) → (3) Two-way state (ตอบกลับ Hello) → Exstate state → Exchange state → Loading state → Full state (update ข้อมูลเรียบร้อย)

• Config Single-Area OSPF v2 router ospf process-id → 1-65,535, เป็น locally significant
R(config-router)# router-id 1.1.1.1 ถ้าไม่ set สามารถใช้ loop back, active interface ip สูงสุด

for Staples

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

- OSPF cost ขึ้น BW ต่างกัน (default ref 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

ต้องการปรับค่า cost เปลี่ยนที่ ref BW.
fa = 100
G = 1000
10 G = 10000

เปลี่ยนที่ BW : R(config-if)# bandwidth 64 (EIGRP & OSPF สามารถใช้ได้)

เปลี่ยนที่ cost: ~ ip ospf cost 15625 .

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

more config R(config)# ip route 0.0.0.0 0.0.0.0 loopback ~ ~
router ospf process-id
R(config-router) # default-information originate

DHCP (Dynamic host Configuration Protocol แจก ip

method ① Manual Allocation : Admin กำหนดเอง
② Automation Allocation : DHCPv4 auto assign addr. จาก pool & ไม่มี lease (เช่า) time
③ Dynamic Allocation : ใครเปิดขึ้นมาจะได้ ip ไปมี lease-time ถ้าหมด lease time ต้อง re ip ใหม่

config R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9 (ไม่แจก ip ไว้)
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1 สร้าง pool
(dhcp-config)# network 192.168.10.0 255.255.255.0 กพ ที่จะแจก
default-router 192.168.10.1
dns-server 192.168.11.5
end.

ยกเลิก no service dhcp

verify show running-config | section dhcp
show ip dhcp binding
show ip dhcp server statistics

config DHCP client (แจก ip ให้ Client) : int : ip address dhcp
ดู sh.

ชื่อ-สกุล นิธินนท์ เพียเลา กระดาษแผ่นที่ 4 รหัสนักศึกษา 88888888

for Staples

Chapter 7 Basic SW Addr Resolution Protocol

☆ LAN Design → Borderless sw nw design มีกฎทั่วไป → • Hierarchical • Modularity • Resiliency • Flexibility

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

① Core ⇒ อุปกรณ์ที่รองรับ BW ↑ ทำให้มี speed ก.เชื่อมต่อ ↑ } Ly 3 Support, [Gig/10Gig Ethernet]
② Distribution ⇒ ก.เชื่อมต่อระหว่าง ① & ②, Security Policy/Access Ctr { Redundant components ⇒ มันคลาดสิ้นทางไป
③ Access ⇒ ติดต่อ end Device, Port Security, VLAN, [Fa/Gig Ethernet] 100M, Power of Ethernet รองรับ ไม่ก็ได้.

Link aggregation ทำให้ BW ↑ Quality of service (QoS)

• เพิ่มความสามารถในการใช้งานให้ได้ LAN BW และ ประสิทธิภาพ สูงสุด.

• ก และการวาง Server ① Enterpirse S. → ติดตั้งที่ Main Distribution Faculty : Core → ทางผ่านไปข้างนอกที่ใกล้กับข้าง

② workshop S. → ติดตั้งที่ Intermediate D.F. : Distribution → เชื่อมระหว่าง cross กับ access ที่ใกล้กันจ.

VCC (Vertical cross-connect) optical Fiber MDF↔IDF

HCC (Horizontal ——) UTP: Distribution ↔ Access

• Collision detection issue ปัญหาการตรวจจับการชน

• Segmentation issue ปัญหาการแบ่งส่วน → ทำให้มีปัญหาการใช้งาน nw มีประสิทธิภาพที่ดีขึ้น

• Broadcast Domain Issue → ใน nw เกิดตลอด เช่น Broadcast หา MAC Addr ดังนั้น Broadcast nw ควรมีขนาดเล็ก

• Segmentation เป็น process split single collision domain → smaller collision domain ลดจน. Collision บน LAN segment ∴ L#2 device ใช้ร่วม bridge sw

• Broadcast domain รับหมดทุก port แต่ router (Ly3) เป็นตัว filter /segment broadcast ไม่ให้กระจายตัวออกจากมัน

☆ SW Enviroment
◦ SW Operation ① Learning รับ frame ทำ SW จะเรียนว่า Source MAC Addr ต่อกับ Port ไหน + reset Aging

② Aging อายุขัยของ MAC Addr. ถ้าหมดก็ทิ้ง

③ Flooding ส่ง frame ออกทุก port ของ sw เมื่อ frame เป็น 1) brodcast 2) multicast 3) unknow unicast → กรณี dest ไม่อยู่ table

④ Forwarding กรณีพบใน table

⑤ Filtering ทำได้รับ frame ไป dest จาก port ที่ไปทาง dest (source & dest มา interface เดียวกัน) จะ filter ทิ้ง

• SW methods ① store & forward SW ⇒ Check CRC ว่า error ไหม, auto buffer

② Cut-Through SW ⇒ check เฉพาะบางส่วน (dest, source อย่างน้อย 12 byte แรก) 10 ms, No FCS & auto Buffer

↳ 2 mode 1) fast forward ~12 byte 2) fragment-Free ~64 byte ชนหยุด ไม่ส่ง

for Staples

• SW domain ① Collision domains → domain ที่เกิดการชนตรวจสอบส่งพร้อมกัน "ดู SW เป็นตัวแบ่ง"

② Broadcast domains → domain ที่ส่ง broadcast อยู่ domain เดียวกันจะได้รับ "ดู router เป็นตัวแบ่ง" VLAN ↗

☆ Basic Config & Concept → เหมือน router เลย

• SW Boot Seq → เหมือน Router • Preparing of Basic SW Management SW ไม่มี loopback กำหนดเป็น SVI (SW Virtual Intf)

• Config Port → ① Full ② Half (ต้องกันส่งรับเหมือนกัน) แต่ intf duplex full → speed 100 ถ้า intf duplex auto speed auto mdix auto

→ Auto MDIX ปกติ SW จะเชื่อมกันด้วย cross-over แต่ต้องเปลี่ยนเป็นสายตรง

SW security Security Remote Access ⇒ SSH (Secure shell) TCP port 22, Telnet : TCP port 23 } ccna line vty 0 15

↳ Config: ip domain-name ชื่อ → # crypto key generate rsa → # username admin pass

→ -line) # transport input ssh → -line) # login local [verify ssh : show ip ssh, show ssh]

SW port security → กำหนดให้ MAC Addr ไหนเข้าออกไม่ได้ → switchport mode access

Secure MAC Addr → ① Static :: S(config-if)# switchport port-security mac-address MAC

② Dynamic : S(config-if) # switchport port-security mac-address sticky → Learn frame ที่วิ่งมา ก่อน record ไว้

เพิ่มเติมจำนวน MAC : # swiport port-secur maximum MAX

Violation mode : ① protect ② restrict ③ shutdown (default) — security violation เกิด — mode

↳ verify show port-security int fa0/0 เก็บว่าเกิดอะไรบ้าง
show port-security address

Addr resolution Protocol (ARP) ARP cache เก็บ MAC Addr ที่ map หาทางไป dest (ถ้าข้างนอกต้องรู้ MAC Gateway)

IPV4 : Classless : Variable Length Subnet Masking (VLSM) แบ่งทุก nw ไม่เท่ากัน → ของชิ้นใหญ่เล็ก

Fixed: เท่ากันหมด

chapter 8 LAN Redundancy & Spaning tree Protocol (STP)

Issue with Ly 1 Redundancy ① MAC Addr instability → MAC ไม่เสถียร เปลี่ยนแปลงบ่อย ② Broadcast Storm วนส่งไม่หยุด

③ Multiframe transmission → start: unknow unicast → ทำให้ dest ได้รับ หลาย frame แต่ source ส่ง 1 frame

☆ STP → หา block port → block ไม่ให้เกิด traffic เพื่อแก้ปัญหา

สิ่งที่ใช้เปรียบเทียบ ① BPDU Flag (priority น้อยสุด) ② BID น้อยสุด ③ Path cost ④ Sender's BID ⑤ Sender Port

for Staples

ขั้นตอน: ① หา Root Bidge → priority min Rule 1RB/1nw, 1RP/1RB, 1DP/segment

② หา path cost ทั้งหมด ③ หา root port → port cost min → อีกฝั่งจะเป็น DP

④ ส่วน Segment path cost เท่ากัน → ดู BID min เป็น DP อีกฝั่งเป็น block port

Config วิธีที่ 1 : S1(config)# spanning-tree VLAN 1 root primary วิธีที่ 2 : spaning-tree VLAN 1 priority 24576 ตั้งให้น้อย

อันรอง root Bridge ใช้อีกอันเป็น Secondary → show spanning-tree

แบบ Extended System ID : B. priority (2 byte) → B. priority (4 bit) (per VLAN0 + Extended Sys ID (VLAN) (12 bit) + MAC Addr (6 byte) ∴ BID = 8 byte

- PVST+ (พัฒนามาจาก IEEE 802.1D STP) เมื่อทำ load balancing โดยแยก root / vlan   show spaning-tree active
- Rapid PVST+ → หา Alternate port ไม่ใช่ block เลย ส่งข้อมูลได้บางส่วน
  - ต้องทำ set Edge Port @ port of a router : -if)# spaning-tree portfast
  - linktype → port ที่เชื่อมระหว่าง sw ต่อกันเป็น point-to-point

if)# spaning-tree bpduguard enable → Port ที่ต่อออกไปให้ BPDU ไปด้วย

→ config : S1(config)# spaning-tree mode rapid-pvst → #int ทำ p-to-p

spaning-tree link-type point-to-point ทำ clear → clear spaning-tree detected protocol

Protocol	Std	Resource	Conver	Tree cal
STP	802.1D	L	slow	All VLAN
PVST+	cisco	H	S	Per VLAN
RSTP	802.1w	M	F	All VLAN
Rapid PVST	cisco	VH	F	Per VLAN
MSTP	802.1S cis	M/H	F	Per Inst

Chapter 9 VLAN & Inter VLAN

ข้อดี secure ↑, ลด cost, ผลงาน ↑, broadcast domain เล็ก ↓, จัดการงาน

VLAN แบ่งแยกที่ L2 ให้คุยได้แค่ VLAN เดียวกัน   show vlan brief

in multi sw Environment → trunk ใช้ carry ได้มากกว่า 1 Vlan/port

- Tagging Ethernet Frames (IEEE 802.1Q)

Dest MAC	Src MAC	Tag	Type/Length	Data	FCS

↳ Tag ส่งผ่าน trunk

- Assignment : VLAN number → 1-1005 เก็บ config @ vlan.dat (flash)
  ↳ 1006-4096 → เก็บใน NVRAM

assign port   swi mode acc
swi acc vlan_

Inter vlan ใช้ subIntf

Chapter 10 VTP (VLAN trunking Protocol)

ช่วย Manage VLAN

	Server	Client	Transparent
Source VTP Msg	✓	✓	✗
Listen VTP Msg	✓	✓	✗
Create VLAN	✓	✗	✓
Remember VLAN	✓	✗	✓

VTP (msg : ISL or IEEE 802.1Q) ก. Manage sw VTP เป็นการ manage ใน domain

Operation : การ update VTP จะใช้เลข. revision number 32 bit (0-4294927295) เชื่อค่าที่สูง

↳ 3 mode

1. Server → remove rename VLAN ได้
2. Client → รับข้อมูล VTP มา process, ส่ง VTP msg ออกทุก trunk
3. Transparent → สามารถสร้าง, remove, rename แต่ในเครื่องมันเองเท่านั้นผ่าน

Config ลงแบบ → 1) sw cisco 2) มี trunk ระหว่าง sw 3) ตั้ว domain 4) มี 3 mode

① global config → vtp version 2 } ตั้ง mode   show vtp status/counters

② VLAN config → v2-mode
↳ เลือก mode ที่จะเปลี่ยนไม่ต้องสั่งทำ mode

Pruning → manage ให้ traffic ที่ใช้งานใน interface น้อย ↓ โดย config ที่ intf ต่างๆ เพื่อ remove ข้อมูลที่ไม่ได้ใช้

s(vlan) # vtp pruning → เข้า intf → s(config-if)# swi trunk pruning vlan remove vlan-num

NAT แปลง private ip ↔ public ip

Terminology 4 type ① Inside local Addr ③ Inside global Addr
② Outside local Addr ④ outside global Addr

Class	
A	10.0.0.0/8
B	172.16.0.0/12
C	192.168.0.0/16

กำหนด

① static   ip nat inside source static local-ip global-ip

② Dynamic สร้าง pool   ip nat pool ชื่อ start-ip end-ip { netmask subnet | prefix-length }
↳ set ACL → ip nat inside source list ACLNum pool ชื่อ overload (PAT)

③ PAT (Port Addr Translation) → port ที่กำหนดร่วมกับ nw addr. (map : many ↔ 1)

↳ Config ① NAT ② Inside ③ outside

Config อีกวิธีของ PAT (single Addr) ①.① สร้าง ACL ①.② ip nat inside source list ACL-Num interface f0/0 overload

show ip nat translation.

ชื่อ-สกุล นิธินนท์ เพ็งเลา กระดาษแผ่นที่ 5 รหัสนักศึกษา [illegible]

for Staples

Chapter 11 EIGRP IPV6 & Routing

Dynamic Routing Protocol
- Interior Gate way P.
  - Distance Vector Routing P.
  - LinkState Routing P
- Exterior Gateway P.
  - Path Vector

	Distance Vector		Link State		Path Vector
Classful	RIP	IGRP			EGP
Classless	RIPV2	EIGRP	OSPFv2	IS-IS	BGPV4
IPv6	RIPng	EIGRP for V6	OSPFV3	IS-IS for IPv6	BGPV4 for IPv6

EIGRP (Enhanced IGRP)

ลักษณะประจำตัว

Basic feature ใช้เฉพาะกับ cisco เปิดให้ใช้ใน 1992

⊕ สร้าง classless version of IGRP ⊕ ทางเลือกที่เหมาะสมสำหรับ nw หลาย Protocol, ขนาดใหญ่ ที่สร้างขึ้นบน Cisco Router

- Dual (Diffusing Update Algorithm) = การันตี loop-free & backup path ทั้งหมดของ Routing Domain → หา Best Path
  → ทำให้ Routing ทำงาน very fast convergent (มี convergent time < OSPF) รวมทั้งมี back up path ทำให้ทำงานเร็วๆ) → if link down เลือก path ใน backup ที่มีมาเลย
- (การทำงาน ≈ OSPF เชื่อม Router)
- Establishing Neighbor Adjacencies = เชื่อม ค. สัมพันธ์กับ directly connected EIGRP router
  = Adjacencies are used to track the status of these neighbors
- Reliable Transport Protocol = RTP provides delivery of EIGRP packets to neighbors
  = RTP and neighbor adjacencies are used by dual (ในการ maintain) — Update ทั้ง Routing ตลอดถ้าไม่มีอะไร down ไหม
- Partial and Bounded = Update เฉพาะส่วนที่มีการเปลี่ยนแปลงจริงๆ update ในเฉพาะส่วนที่มีการป. ∴ update < RIP
- Equal & Unequal Cost (OSPF, RIPv2) — ช่วยให้ admin ดูแลระบบเมื่อกระจาย ก. รับข้อมูลในเครือข่ายได้ดีขึ้น

Load Balancing L> ค่า cost ≠ but ทำเป็น load balance ได้

△ มี protocol-dependent modules (PDMs) เพื่อรองรับ protocol ที่แตกต่างกันเช่น IPV4, IPv6, legacy protocol IPX and AppleTalk

△ PDM รับผิดชอบ

⊖ Maintain EIGRP neighbor and topology table (Neighbor Table → ผ่าน dual สร้าง Topology Table → ใส่ routing table เป็น routing EIGRP) เลือก successor

เก็บทั้ง topology ≈ OSPF ≠ → เก็บ shortest path กับ backup shorten

⊖ คำนวณ metric ที่ใช้ Dual ⊖ เชื่อมต่อ Dual และ Routing table

⊖ implement filtering and ACL ⊖ ทำ redistribution with other routing protocol

△ RTP is EIGRP Transport Ly protocol สำหรับ delivery & reception ของ EIGRP packets
= เป็น msg ที่อยู่ใน application layer ที่ maintain ข้อมูล, msg ต่างๆ ที่ส่งของ EIGRP

△ ไม่ใช่ทั้งหมดของ RTP Packet จะส่งได้น่าเชื่อถือ (msg ≈ OSPF)

⊖ Reliable packet require explicit (ชัดเจน) ack จาก dest. ⊖ Update, Query, Reply

⊖ Unreliable packet do not require ack จาก dest ⊖ Hello, ack

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

Packet Type Routing update or queries EIGRP multicast IPv4 01-00-5E-00-00-0A 224.0.0.10, IPv6: FF02::A
ข้อมูล IGRP multicast 224.0.0.4
RIP v1 brodcast 255.255.255.255

① Hello → ทำให้ adjacencies ระหว่าง router 2 ตัวที่เป็น neighbor กัน ไม่ต้องรอ responce, ส่ง unreliably

② Update → update info ของ dest update info ของ routing ไปให้ neighbor router

③ Acknowledgement → พอได้รับการ update ก็ตอบ ack

④ Query → request info. routing จาก neighbor router } เวลาต้องการ info ของ routing เพิ่มก็ query ไปกับ router ข้างๆ แล้ว reply ตอบกับว่ามีหรือไม่มี

⑤ Reply → หลังได้รับ query ก็ reply

Implement EIGRP for IPv4

Autonomous System (AS) is a collection of nw ภายใต้ ก. ดูแลของ single authority (อ้างอิง RFC 1930)

L> AS number → ใช้ exchange routes between AS
→ managed by IANA & assigned by RIRs to ISPs, Internet Backbone providers, and institution ต่อ. สถาบันอื่น
→ 16 bit : 0-65535 → since 2007, 32 bit : over 4 billion

sh ip eigrp neighbors
sh ip protocols
sh ip route

for Staples

conf → router EIGRP ___
eigrp router-id → ถ้าไม่กำหนดจะใช้ loopback intf → IPv4 addr ที่สูงสุดที่ active
network ___ [wildcard]

มีก็ได้ passive-interface type number [default] → ไม่ให้ส่งแพ็กเกจไป intf ไหน

Operation

Initial Route Discovery ① R1 say hello กับ neighbor router ② R2 อาจจะส่ง hello or update กลับมา ③ R1 ตอบ Ack & update info ④ ใช้ Dual คำนวณ best route & update routing table

- Metric BW [lowest], Delay [สะสม], Reliability [worst], load [worst] ดูค่า value : show interface

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

Default Composite Formula

$$metric = [K1*bw + K3*delay]*256 = \left[\left(\frac{1{,}000{,}000}{bw}\right)+\left(\frac{\text{sum of delay}}{10}\right)\right]\times 256$$

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

R(config-router)# metric weight tos k1 k2 k3 k4 k5 -set bw: ที่ intf bandwidth kilobits-bw-value

Dual and the Topology Table (ใช้ FSM ในการเลือกเส้นทาง) show ip eigrp topology [all-link], show ip route

+ Successor(s) [router ที่ไป dest สั้นสุด] neighbor router ที่จะเลือกทางไป dest ที่มีค่า metric น้อยสุด
+ Feasible successor (FS) (ต้องใช้ FC Feasible condition) = Backup path (เส้นทางสำรอง)
+ Reported Distance (RD) [distance ที่ neighbor ตัวอื่นๆ report distance มาให้เรา] = "advertised distance"
+ Feasible Distance (FD) (distance ที่ไปทาง 3) คือ distance ที่คำนวณไปหา dest ทั้งหมด ทางที่สั้น → dest * cost เท่ากับ "มองจาก hop lowest → dest" ที่ค่า cost

IP.V6 ☆

IPV4 Issue

- แก้ปัญหา IPV4 ไม่พอใช้ IOT assign IP ไม่พอ
- การใช้งานร่วมกัน (coexistence)
  - Migration IPV4 → IPV6 Techniques: ① Dual stack = run ทั้งคู่ if ต้องลงใหม่ ไม่กระทบ user
    ② Tunneling (อยากใช้ IPv6 แต่ core ไม่ support) = เปลี่ยนเฉพาะหัว แต่วิ่งผ่าน V4 same เดิม
    ③ Translation (คล้าย NAT) = IPv6 ⇔ IPv4

IPV6 Addressing 128 bit แบ่ง 8 ส่วน represent base ทุกๆ 4 bit

การออกแบบ

Rule1 Omit Leading 0s = ตัดแต่ละ partition "0" ที่อยู่ด้านหน้าให้ตัดทิ้งไป 000X, 00XX, 0XX (X → 0-F)

Rule2 Omit All 0 segment = แทน Segment ที่มี "0" ติดกันยาวๆ ด้วย "::" ใช้ได้ครั้งเดียว only

Type of IPv6 Address

- IPv6 Addr Type ① unicast: ⊖ Global Unicast (→ 3 bit แรก: "001" or "2000::/3") ⊖ Link Local (→ สร้าง intf ที่อยู่ติดกัน (@ Local เดียวกัน); → ใช้ช่วง FE80::/10 = ใช้งานเข้าได้ค่าภายใน link-local (ใช้ได้เฉพาะใน local)) ⊖ unique Local
  - static config → ipv6 address ip —— → no sh
  - ② multicast
  - ③ Anycast = ส่งได้หลาย device
- △ IPv6 Prefix length = 0-128, most LANs is /64 bec LAN เล็กสุด 64 bit

IPV6 Routing

- static route ipv6 route ____ {ipv6 addr | exit-intf} (next hop, exit)

ใส่ก่อนใช้งาน routing IPv6 ipv6 unicast-routing เพื่อเปิดใช้งาน

verify show ipv6 route static, show ip route ipv6, show running-conf | section ipv6 route

Default static route

ipv6 route ::/0 {ipv6 addr | exit-intf}

- Conf EIGRP
  - เปิด unicast
  - เหมือนๆ กันแต่เดิม ipv6 ข้างหน้า ↗ ตอนสร้าง Eigrp #
  - △ network command ที่ intf ipv6 eigrp AS#
  - แต่ passive intf ต้องอยู่ global conf เหมือนเดิม

verify show ip eigrp neighbor, show ipv6 protocol, show ipv6 route

ชื่อ-สกุล นิติวันท์ เสือเสา กระดาษแผ่นที่ 6 รหัสนักศึกษา 68088084

for Staples

Router

① basic config

show interface } sh info intf
show ip interface }
show ip interface brief ดูเร็วๆ

Dynamic Routing

- RIP → passive intf : R(config-router)# passive-interface intf-type intf number
  - เชื่อม RIP↔static : R(config)# router rip → R(config-router)# {redistribute static | default-information originate}
    ใช้ router ตัวไหน set default route @ Intf ที่เชื่อมกับ 2 protocol อยู่!
- RIP v.2 : R(config)# router rip ⇒ R(config-router)# version 2 ⇒ no auto-summary ⇒ network nw-ip
- EIGRP : R(config)# router eigrp # ⇒ ตัว router-id ⇒ network nw-ip [wildcard-mask]

verify → show ip eigrp neighbors, show ip eigrp topology
metrics : R(config-router)# metric weigth tos k1 k2 k3 k4 k5
set bw. ที่ intf ⇒ R(config-if)# bandwidth kbits-bw-value

OSPF

set bw : ที่ intf ⇒ R(config-if)# bandwidth 64
ip ospf 15625

verify : show ip ospf neighbor, sh ip ospf intf brief, sh ip ospf
อื่นๆ clear ip ospf process
redistribute (OSPF ↔ default route) : R(config)# ip route 0.0.0.0 0.0.0.0 loopback N
router ospf process-id
default-information originate

for Staples

② other

- ACL → ip access-list [standard|extended] name
set ACL : R(config)# access-list ACL-num {permit|deny|remark} source [source|wildcard] [log]
set @ intf → เอาไว้ใน in-out → ip access group {num|name} {in|out}
verify → sh acc list

for Staples

Extended ACL

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

DHCP → exclude → ~~

SWITCH

Config port

in intf => duplex full => speed 100

auto MDIX in intf => S(config-if)# duplex auto => speed auto => mdix auto

Secure Remote Access

+SSH (TCP port 22) : S(config)# ip domain-name cisco.com => crypto key generate rsa =>
username admin password cena => line vty 0 15 => S(config-line)# transport input ssh =>
login local
-verify : show ip ssh, show ssh

+Telnet (TCP port 23)

-switch port security : in intf => S(config-if)# switchport mode acc => swi port-security
+ static secure MAC Addr : => swiport port-secure mac-add MAC-ADD
dynamic ~~ : ~~ sticky
+ MAX MAC Addresses : => ~~ maximum MAX
+ Violation Mode : => ~~ violation {protect|restrict|shutdown} mode
- verify → sh port-security address

(5) STP mvv 1 S(config)# spanning-tree VLAN 1 root {primary|secondary}
mvv 2 S(config)# spanning-tree VLAN 1 priority 24576 (priority ✱)
+verify: sh spanning-tree [active], show running config

☐ Rapid PVST+
+port fast : in intf => S(config-if)# spanning-tree port fast
+BPDU Guard : in intf => S(config-if)# spanning-tree bpduguard mode
+config : S(config)# spanning-tree mode rapid-pvst => in intf => S(config-if)# spanning-tree
+clear STP => S# clear spanning-tree detected protocol link-type point-to-point

NAT sh ip nat statistics
-static ip nat inside source static local ip global ip in intf => ip nat {inside|outside}
-dynamic => ip nat pool name start ip end-ip {netmask netmask|prefix-length prefix}
→ access list ACL num permit source (source-wildcard) => ip nat inside source list ACL-num
in intf ip nat {inside|outside} pool name ✱ overload

/ for pat