

## Chapter 1 : Network Overview

- Network device
  - ↳ End device : PC, Printer, Laptop
  - ↳ Intermedia Network Device : Switch, Router, Hub
  - Network media : Fiber Optic, UTP, Coaxial, RJ-45
- Network Protocol
  - ↳ protocol ที่มีการต่อ
  - Address - physical (MAC-Datalink)
  - logical (IP-Network)
  - Special (Port-transport)
- Network Type
  - LAN : small and single admin
  - WAN :
- Reliable Network
  - Fault tolerance - กรณีมีความเสียหายของเครื่อง
  - Scalability - สามารถขยาย NW ได้
  - Security
    - GoS - ให้ความสำคัญกับ Service Quality

แบบ - จุดต่อสายคู่ - Crossover  
 1 - switch-Hub, Router-PC  
 2 - จุดต่อสาย straight

Logical Diagram จุดต่อ

เข้ากัน NW ด้วยตัว test connect

Physical Diagram จุดต่อจริง

จุดต่อจริง, สาย

OSI

Application	DNS 6007 HTTP
Presentation	PHP CP SMTE
Session	POP IMAP
transport	TCP UDP
segment	IP NAT DCEP
Packet	OSPF EIGRP
Network	FTP TFTP
frame	ARP PPP
Data	Ethernet
physical	Interface Adapter

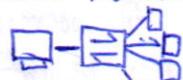
port number
 

- 0-1023 well known
- 1024-49151 registered
- 49152-65535 private/Rand

 private IP - reserve 192.168.0.100-1023

- IPv4 - Class Unique
 

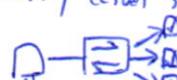
A	NW.H.H.H	0	0-127	126	NW/H	private IP
A	NW.NW.H.H	1.0	128-191	192	16.77M	10.0.0.0/8
B	NW.NW.NW.H	11.0	192-223	2M	65.535	102.16.0.0/12
C	multicast	111.0	224-239	N/A	254	192.168.0.0/16
D					N/A	192.168.0.1/0/16
- Mac Address → Physical Address - identify actual source/dest



Unicast จุดต่อจุดเดียว



Broadcast - จุดต่อทั้งหมด  
Broadcast IP/MAC



Multicast - จุดต่อกลุ่ม  
224.0.0.0-239.255.255.255

- Cisco IOS

Access - console, telnet, SSH, AUX

Mode - User mode >

- privilege mode # → Global config : (config) #

Structure - prompt, command, space, keyword/Argument

method ตั้งชื่อ hostname name

ใน privilege → enable

ใน global config user

line console 0

password kontrol

login exit

ใน global config user

in global - # configure terminal

password privilege - ตั้งชื่อ password cisco

- telnet enable secret class

interface # interface type slot/subslot/port

ip (config-if) # ip address subnet mask

## Chapter 3: static routing and Dynamic Routing Protocol

- Routing คือ packet ที่ต้องผ่านทางใด

↳ Routing Table - ตาราง Von Richten

- คือชุด column

- คือจุด final dest

- Routing → Choose Best Path

- Encap packet นำต่อ header ที่ต้องการ

- 1. Static Routing

2. Dynamic Routing protocol

- Forwarding 1. Process switching ผ่านชั้น hardware packet ที่มี

2. fast switching - ผ่านชั้น hardware ที่forward ไวๆ

3. CEF - lookup, trigger และ forward

\* ต้องรู้ ip, packet ที่ client มีแล้ว และ default gateway ที่ต้องผ่าน NW ที่อยู่

192.168.1.31  
ess.255.255.0



192.168.1.X

255.255.255.0

Router

- CPU

- OS - Cisco IOS

- Memory, Storage Flash  
HDD

↳ ที่ NW ต้องการที่ต้องการ gateway

optional) 192.168.1.254

NW ID: 192.168.1.0

Broadcast: 192.168.1.255

\* default gateway ไม่ต้องตั้ง NW ที่ต้องผ่าน NW ที่อยู่

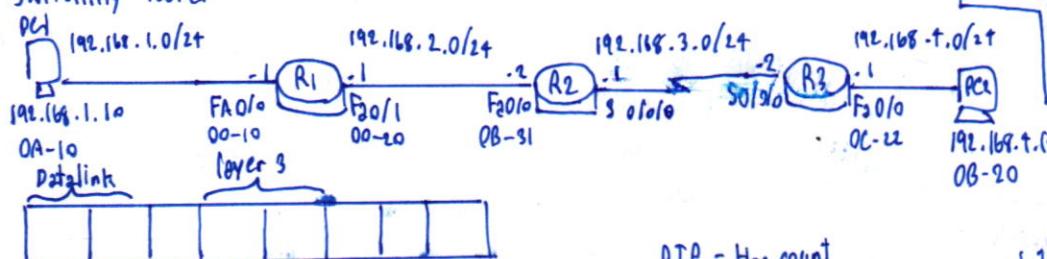
(optional) 192.168.1.0 NW ที่ต้องผ่าน NW ที่อยู่



• Document Network Addressing  
 Device name  
 Interface  
 IP address  
 Subnet mask  
 Default gateway  
 ผู้ดูแลระบบตรวจสอบสถานะเครือข่าย  
 ตรวจสอบและแสดง controller type slot/port

- Enable IP
  1. Statically : manual - กำหนด IP, subnet และ internet profile  
 Identify NW resource, NW อย่างไร
  2. Dynamically : auto - ใช้ DHCP กำหนด

### • Switching Packet



R1# show ip route | begin gateway  
 Gateway of last resort is not set  
 172.16.0.9/16 is variably subnetted, 5 subnets, 2 routes  
 C 172.16.1.0/24 [1/0] via 172.16.2.2  
 C 172.16.2.0/24 [1/0] is directly connected, Serial0/0/0  
 L 172.16.2.1/32 is directly connected, Serial0/0/0  
 C 172.16.3.0/24 " " G0/0/0  
 L 172.16.3.1/32 " " G0/0/0  
 S 192.16.1.0/24 [1/0] via 172.16.2.2  
 S 192.16.2.0/24 [1/0] via 172.16.2.2

### • Path Determination - cost - metric

Link local interface  
 show ip route  
 Directly connected interface  
 static route  
 Dynamic routing protocol

RIP - Hop count

OSPF - BW

Load Balancing → ทดแทน, คำนวณ cost ใหม่

Administrative Distance - กำหนด Admin ตัวเอง

ISP

new คำนวณใหม่

(คำนวณ cost แล้ว Add to router)

Problem @ 192.168.1.0 [2/1 120/1]

EIGRP @ " [90/128/5] ✓ คำนวณ AD แล้ว AD ใหม่คำนวณ cost ใหม่

connected @ 192.168.10.0/24 is directly connected Gigabit Ethernet 0/0/0  
 Link local @ 192.168.10.1/32 " "

dest NW how it's connected interface dest router

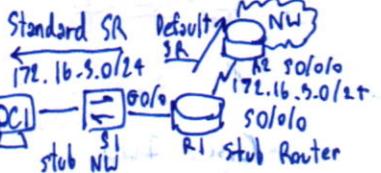
### • Static Route

- connected to specify NW

summarize คำนวณ routing ตัวเอง

create a backup route

คำนวณ sub NW ที่ต้องการตั้งค่า



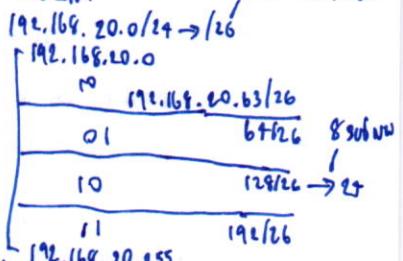
summarize คำนวณเอง

### • CIDR

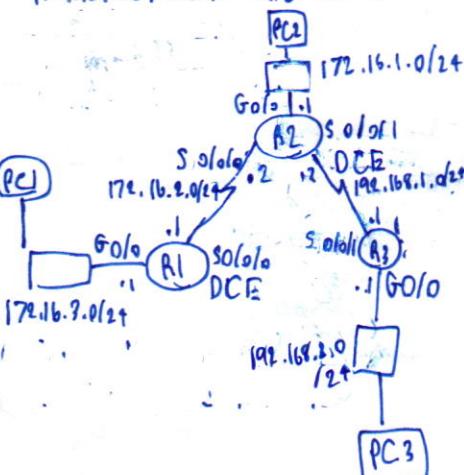
- A. 192.168.0.0/23
- B. 192.168.0.0/23
- C. 192.168.0.0/23
- D. 192.168.0.0/23

Overhead  
 classful update ✗  
 classless update ✓

### • VLSM



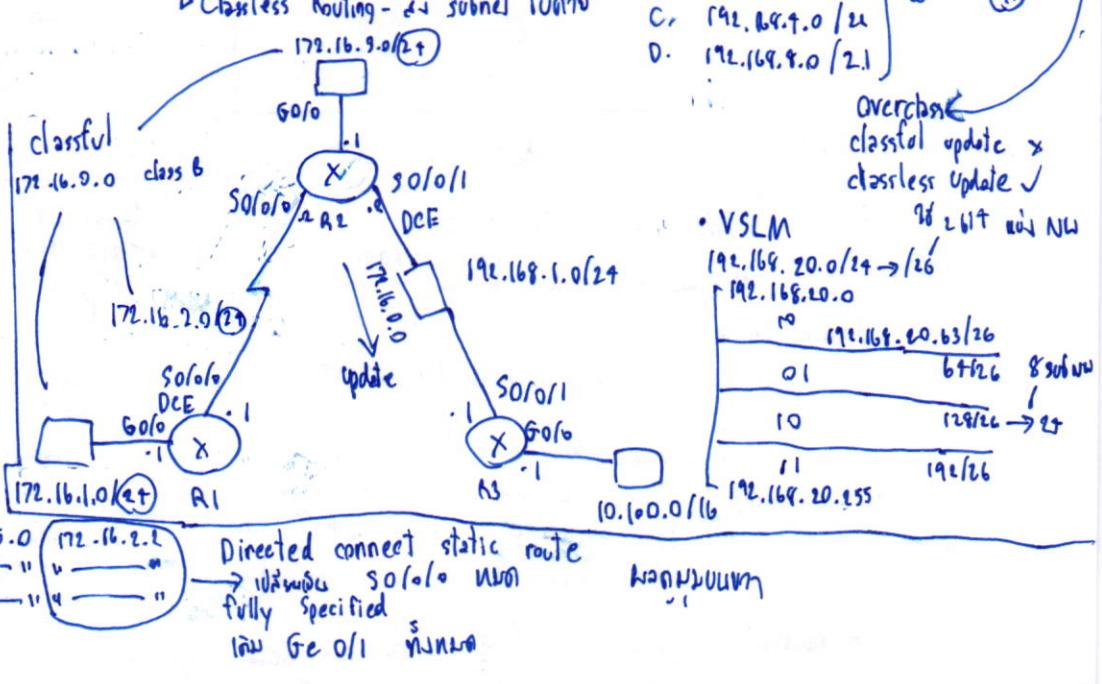
1. how NW learned by router
2. dest NW
3. AD (Admin distance)
4. metric to reach the remote NW



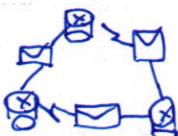
### • Network Addressing

▷ Classful Routing - คำนวณ class ตัวเอง

▷ Classless Routing - คำนวณ subnet ตัวเอง



## Distance Vector Routing Protocol



Function - วิธี Information between router

- update routing table when topology change
- find best path to destination

Purpose - remote NW

- Maintain up to date

- หาเส้นทางที่ดีที่สุด

- ไม่สามารถจัดการได้โดยอัตโนมัติ

Components - Algorithm, Routing Protocol Message

### • Interior Gateway Protocol

- Distance Vector - distance & direction
- incomplete topology
- periodic update
- complete NW topology
- not periodic update

### • Classifying Routing Protocol

#### - Classful

- แบ่ง class ตาม subnet mask ของ class

- ระบุ NW ผ่าน mask ที่แน่นอน

- ระบุ subnet mask ที่แน่นอนใน routing table

#### - classless

- ระบุ VLSM ผ่าน mask ที่กำหนดเอง class

\* Convergence - State of NW ที่มีความเปลี่ยนแปลง down จะต้องมี update routing table ใน router ต่อๆ ไป

à AN Connected o

Metric - วิธีการคำนวณ destination NW ที่ Best Path

Hop count - RIP

Load Balancing - คำนวณ cost ของ NW แล้วเลือกที่ดีที่สุด

Bandwidth - OSPF

Administrative Distance - ตัวตั้ง protocol ในการ routing มาก

• Distance Vector - router ที่ distance ไม่ vector/direction

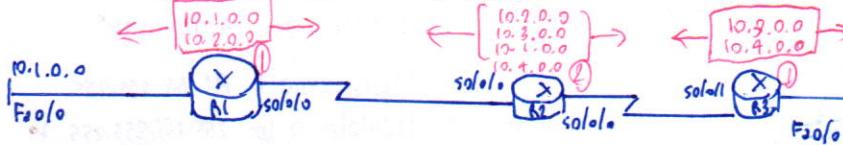
- characteristic - periodic update, neighbors, broadcast update, entire routing table

• NW Discover

1. Router Initial start up

2. Initial Exchange

3. Exchange of Routing Information



Network	Interface	Hop
10.1.0.0	F0/0	0
10.2.0.0	S0/0	1
10.3.0.0	S0/0	1
10.4.0.0	S0/0	2

Network	Interface	Hop
10.2.0.0	S0/0	0
10.3.0.0	S0/0	1
10.4.0.0	S0/0	1
10.9.0.0	S0/0	1

Network Interface Hop

### Periodic Time Update

#### • Timed Update Timer

Default : 30s

Invalid : 180s (ถ้าไม่ได้รับข้อมูล)

Hold down : 180s (ถ้าไม่ได้รับข้อมูล Invalid)

Flush : 270s (จะลบ掉 invalid)

#### • Bound update : EIGRP

จะรับข้อมูล update ของตัวเอง

• Triggered → รีบคืนสู่ตัวเอง

• Random Jitter → Multiple Access

• RIP Problems ① Routing Loops ไม่สามารถ NW down ที่ interface ใดๆ ก็ได้ packet จะวนloop  
ตั้ง Hop Count to infinite [Ex R3: F0/0 → S0/0]

Solution : Setting a maximum hop counts → 10 hop = Unreachable  
: Hold down Timer → Hold 5ms down ที่จะ update ต่อไป down

② Split Horizon Rule หลักการ NW ออกเดินทาง interface ที่ไม่รวม update ณ

10.9.0.0	1	10.2.0.0	1
10.0.0.0	2	10.1.0.0	2

③ Route poisoning นำ NW down → set unreachable → 2x poison update

④ Split horizon and poison reverse - ①+②+③

⑤ IP & TTL - ที่ TTL ที่ packet ผ่านมา อย่างไรก็ drop นั้น

R1(config)# router rip

R1(config-router)# network 22NW

R1# show ip route

**RIP v1** Characteristic - Classful, distance vector → not send subnet mask

R 192.168.8.0/27 [120/2] via 192.168.2.2

192.168.2.0/24  
Hop Address

update subnet n' info ไม่แน่นอน

- metric คือ hop count

- hop count > 15 = unreachable

- broadcast deny 30s

- can auto summarize

passive interface → ไม่ interface ที่ต้องการ

R(config-router) # passive-interface

inf-type  
inf-area

**Rule** 1. Routing Update Interface receive on same NW

- subnet apply to network on routing table

2. if different NW

- Classful subnet mask applied to the NW in routing update

Automatic summarization → RIP ที่ auto summarization ให้สรุป routing table → faster lookup

not support

discontinuous network (NW ไม่ติดต่อกันทั่วทั้งสองฝ่าย)

Default route - packet ที่ไม่ระบุ address จะไปที่ routing table ที่มี default route

display timer  
by RIP

# ip route 0.0.0.0 0.0.0.0 [inf-type] → # default-information originate → # show ip protocol



## RIPv2

- classful - update learns address
- $\nexists$  sup disjoint subnet
- $\exists$  VLSM + CIDR
- $\exists$  subnet mask in routing table
- update via broadcast

## RIPv2

- classless - update via subnet
  - enhance V1 feature
- $\exists$  Next Hop address in update
- update via multicast
- $\exists$  authentication
- $\exists$  sup VLSM + Route Sum + Auto sum
  - auto boundary - major class NW result sum 7 of summarization

## Similar (R2)

- $\nexists$  routing loop detector
- $\nexists$  split Horizon, poison reverse
- $\nexists$  trigger update
- Max Hop count = 15

## RIPv1 Limitation

- \* Null - Virtual Interface
  - $\nexists$  ping  $\nexists$  routing table

### \* Null Interface config \*

```
R2(config)# ip route 192.168.0.0 255.255.0.0 Null 0
```

Route Summarization

### \* $\nexists$ auto summarization \*

$\nexists$  R2(config-router) # no auto-summary  $\rightarrow$   $\nexists$  RIPv1 distribution NW entry via: (192.168.0.0/0 config)

## Access Control List

- Packet filtering : Filter traffic to/from
- operation - always implicit deny - deny any  $\rightarrow$   $\nexists$  configuration

### Standard

- block or allow block user
- check only source address
- permit or deny entire protocol suite
- (1 to 99) and (100 to 199)

### Extend

- iron block
- check source and dest (option)
- permit or deny specific protocol suite
- (10 to 199) and (2000 to 2699)

### Ex mru Wildcard Mask

1. 192.168.1.65, 67, 69..., 187

Sol:	65	0100 0000
	67	0100 0011
	69	0100 0101
:		
	127	0111 1111
		01xx xxxx
		0011 1110
WC:		0.0.0.001111e

2. 192.168.64.x - 192.168.191.x  
(x is odd)

Sol:	192.168.01000000.X
	192.168.01111111.X
	192.168.64.1 0.0.63.254 -①
	192.168.10000000.X
	192.168.10111111.X
	192.168.128.1 0.0.63.254 -②

### wildcard mask

- inverse of subnet mask

Ex 192.168.1.0 255.255.255.0

WC 192.168.1.0 0.0.0.255 —any  
0.0.0.0  $\rightarrow$  mask  $\nexists$

192.168.xxx xxxx - xxxx xxxx xx

$\rightarrow$  192.168.1.0 = 192.168.1.255

192.168.255.0 = 192.168.255.255

- Calculate  $\rightarrow$  192.168.255.255 in
  - auñsu subnet lñsu (invert from WC)

Apply ACC lñsu + protocol / 1 ACL  
\* 2nnm + 81ñ lñsu + n: 4, 8, 12...  
ACC lñsu + compile policy lñsu

## ACL Creation - စာမျက်နှာ

1. One ACL / protocol  $\rightarrow$  control traffic flow on an interface  $\rightarrow$  define for each protocol
2. One ACL / direction  $\rightarrow$  control traffic in one direction  $\rightarrow$  inbound/outbound
3. One ACL / interface  $\rightarrow$  control traffic for an interface

- Extended  $\rightarrow$  2nd ACL lñsu source
- Standard  $\rightarrow$  lñsu lñsu dest

Create name

# ip address-list

[standard | extend]

name

# ip access-group name [in|out]

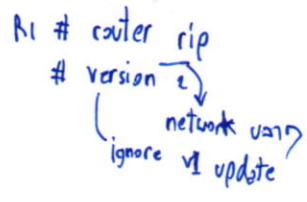
\* configure no access-list lñsu no yas. ACL lñsu number lñsu lñsu list

router(config) # access-list access-list\_number deny|permit|remark source [source wildcard] [log]

Ex # access-list 1 permit ip 192.168.0.0 0.0.0.255  
access-list 2 deny any

\* apply to interface : ip access-group 1 in  $\leftarrow$  into router

Router(config-if) # ip access-group access-list\_num name in|out



for Staples

ACL

- secure VTY port for telnet or SSH  
router(config-line)#access-class access-list-number {in[vrf-v1] | out}
  - Extended ACL → like Standard

- Apply Extended ACL to interface

```
R1(config)# access-list num permit tcp source wildcard any eq 80 - port  
R1(config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443 - example  
R1(config)# access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established  
R1(config)# interface g0/0  
R1(config-if)# ip access-group 103 in  
R1(config-if)# ip access-group 104 out
```

- filter traffic with extended ACLs

```
Ricconfig)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255 eq tftp,tftp-data  
" _____" permit ip any any  
interface g0/1  
ip access-group 101 in
```

Open Shortest Path First aka OSPF

- Link-State Routing Protocol
    - IPv4 → OSPFv2
    - IPv6 → OSPFv3
    - AD → Ilo
    - hierarchical, fast convergence
    - admin have good knowledge
  - Algorithm - Shortest path first (SPF)
  - Update
    - Router learns directly connected networks
      - "saying Hello" to its neighbors on directly connected networks
      - Build a Link-State Packet (LSP) then flood the LSP to all neighbors
      - Use the database to construct a complete map

for Staples

## Link State Content Example

- R1, Ethernet network, 10.1.0.0/16, cost 2
  - R1 → R2 : Serial point-to-point, 10.2.0.0/16 : cost 20
  - R1 → R3 : \_\_\_\_\_ " \_\_\_\_\_ , 10.3.0.0/16 : cost 5
  - R1 → R4 : \_\_\_\_\_ " \_\_\_\_\_ , 10.4.0.0/16 : cost 20

- Feature : Classless, Efficient, Fast Convergence , Scalable , Secure

- Data Structure
  - Adjacency DB → Neighbor Table : show ip ospf neighbor
  - Link - static DB → Topology Table : show ip ospf database
  - Forwarding DB → Routing Table : show ip route

OSPF •  $\downarrow$  - Hello packet

- Database Description packet
  - Link-State Request and Update packets
  - Link-State Acknowledgement packet

- Update ~~1111~~ Multicast : 01-00-5E-XX-XX-XX
- ~~↳~~ Hello Message nn (0s Broadcast LSP n,n 20)

- > Hello Message in Ios Broadcast LSP
- Operation Down state Establish Neighbor + Advertisements

```

graph TD
    Down[Down] --> SSync[Synchronize OSPF]
    Init[Init] --> SSync
    Init --> TwoWay[Two-way]
    TwoWay --> SSync
    TwoWay --> ExStart[ExStart]
    ExStart --> SSync

```

Adjacencies

```

graph TD
    A[Exchange State] --> B[Loading State]
    B --> C[Synchronize DBP]
    style C fill:none,stroke:none
    
```

The diagram illustrates the sequence of states in a process. It starts with 'Exchange State', which leads to 'Loading State'. From 'Loading State', the process moves to 'Synchronize DBP'. The 'Synchronize DBP' state is enclosed in a red bracket on the right side of the diagram.

↓  
Full State

## • Summary I. Link' n Link-State

2. Say Hello
  3. Building the Link-State Packet
  4. Flooding LSP & Building Database
  5. Building the SPF Tree & Routing table

5 - រាយការ Adjacency និង packet នៃ router ដូចជាមួយន្តោះ នៅពេលផ្ទៀងផ្ទាត់  
DR + BDR  
• passive-interface និង ផ្តល់ routing update នៃ interface នេះ

- process-id - ID process ໃຫຍ່ນີ້ OSPF (1-65535)
  - ໜ້າມໆ 100 router ແກ່ຕົວ

router-id - id van router die check process in router via id zijn

- ໃຊ້ router ဆານ
- ລັບໃຫຍ່ loopback/active ip address ນາງຄົດ



## Configure Single-Area OSPFv2

R1(config)# router ospf 10

R1(config-router)# network 172.10.1.0 0.0.0.255 area 0

Cost = reference bandwidth / interface bandwidth

auto\_cost : reference-bandwidth bandwidth\_mbps

• Default internet Bandwidth - bandwidth of interface 700 cost will be 1 - default 1.544 mb/s

• Default Route ip route 0.0.0.0 0.0.0.0 loopback 0

• Redistribution → ဆានសាយ rip 10 OSPF រួចឱ្យ rip 10

## Dynamic Host Configuration Protocol

• Protocol ដែលផ្តល់លម្អិតនៃការពារ IP address នៃ Subnet Mask / Default gateway / DNS (both IPv4, IPv6)

• Methods 1. Manual Allocation - set នៅលើ Control Panel / cmd

2. Automatic Allocation - Fix IP នៅលើលាប

3. Dynamic Allocation - នៅលើ IP ពី pool ដែលផ្តល់លម្អិត server

• Operator 1. DHCP DISCOVER - Client ស្ថិត request ទៅ DHCP server → Broadcast

2. DHCP OFFER - Server ស្ថិត Assigned IP Address នៅលើ Client → Unicast

3. DHCP REQUEST - Accept IP Address នៅលើ Server → Broadcast [ទទួលបានការស្វែងរកដែលត្រូវការបញ្ជី]

4. DHCP ACK - Server ស្ថិត ACK នៅលើ Client → Unicast

• Command តាមឯណា - ipconfig/renew → ទូទៅ IP Address នៃ DHCP

- ipconfig/release → សុំលើ IP Address ដែឡូលូ

• Configure DHCPv4 Server

- Exclude address from the pool - សិទ្ធិ IP ដែលត្រូវបាន - សិទ្ធិ IP ដែលត្រូវបាន IP address; server, Default gateway

- Setup DHCP Pool name

- Configure Specific Tasks - define range of address and subnet mask - Use default-router cmd

R1(config)# ip dhcp exclude-address 192.168.10.1 192.168.10.9 → ip range និងលាប

R1(config)# ip dhcp exclude-address 192.168.10.254 → និង default gateway

ip helper-address  
→ ទូទៅ router broadcast  
192.168.10.1 និង

R1(config)# ip dhcp pool LAN-POOL-1

R1(dhcp-config)# network 192.168.10.0 255.255.255.0

|| " " " " default-router 192.168.10.1

|| " " " " dns-server 192.168.11.5 { optional }

|| " " " " domain-name example.com }

|| " " " " end

- Verify DHCP - show running-config | section dhcp

- show ip dhcp binding

- show ip dhcp server statistic

PC → ipconfig /all

IPv4 → Classless inter-domain routing (CIDR)

- Fixed range Subnet Masking - នៃ NW នាយកដី

- Variable range Subnet Masking - ទូទៅ NW និង subnet លូហូរ

\* NS5 Config DHCP ទៅ Router នូវ Broadcast ទៅ NW

R1(config)# interface g0/1

R1(config-if)# ip address dhcp

|| " " " " no shutdown

### Trouble shooting

1. Resolve conflicts

2. Verifying physical connectivity

3. Test with a static IPv4 address

4. Verifying switch port configuration

5. Test from the same subnet of VLAN

## Subnet Planning

\* Network 161.246.6.0/23

- IP address 161.246.6.0

- " " " 161.246.6.1

- " " " 161.246.6.255

- " " " 161.246.7.0

- " " " 161.246.7.1

- " " " 161.246.7.254

Network	Netw. Host	Max Host	Subnetwork	Subnet/mask
A	126	126	161.246.6.0	255.255.255.128
B	62	62	161.246.6.128	255.255.255.192
C	30	30	161.246.7.0	255.255.255.224
D	17	30	161.246.7.32	224
E	31	62	161.246.7.192	192

161.246.6.X 161.246.7.X

0

127

128

191

192

255

256

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

192

224

196

255

31

32

63

128

## Basic Switch Network

- LAN Design - based on Admins and Policy
- Borderless switch network design

- Hierarchical (ลิ้นชัก)
- Modularity (โครงสร้าง)
- Resiliency
- Flexibility

3-Tier : Core - distribution - Access  
2-Tier : Collapsed - Access

Info: Tier ที่มีการซ้อนกัน overlapping (ลิ้นชัก)

	Port security	VLAN	Fa/Gig	Poe	Link aggreg.	Gos	Ley 3 sup.	Forward Rate	Redundant component	* PoE : Power over Ethernet จ่ายไฟผ่านสาย
Access	✓	✓	✓	✓	✓	✓	-	Med.	-	* Fa/Gig : BW ที่ = sup.
Distribution	ACL	-	10Gig	-	✓	✓	✓	High.	✓	Link aggreg: 50% link บน BW ของตัวตัวเดียว
Core	-	-	10Gig	-	✓	✓	✓	Very h.	✓	Redundant: 75% บน switch เดียว



- Maximize LAN bandwidth
  - Placement of server < Enterprise - วางตั้งห้องสำนักงาน MDF
  - Workgroup - กลุ่มผู้ใช้งาน group ที่ต้องการใช้งาน กับ IDF หรือชั้น
  - Collision detection issue → มีการคัดลอกใน domain ต่างๆ
  - Segmentation issue
  - Broadcast domain issue

## Switch Operation

1. Learning - ทุก switch ให้เรียนรู้ port ใด = table ใด Port No. ใด; Mac ได้เรียนรู้ frame ที่ switch
2. Aging - ไม่เรียนรู้ learn ทุก table ใด: ลบ frame บน source ที่ไม่สามารถติดตามได้ drop อยู่บ่อยๆ แล้ว learn ใหม่
3. Flooding - ทุก port ของ switch ที่ไม่ได้ source Mac ทุก
  - Unknown Unicast MAC
  - Broadcast MAC
  - Multicast MAC
4. Forwarding - ถ้า frame อยู่ใน dest. port ก็ forward ไป (must have data in table)
5. Filtering - ถ้า frame ไม่มี source Address & port ไม่ได้ใน filter packet

### Transparent Bridge Process

Receive frame → Learn source → BC, MC, Unknown UC → Source/Dest. same int → Forward unicest to correct port

### Forwarding Method

store-and-forward → ตรวจ CRC กรณี Error ไม่พบ store ห้อง No. แล้ว forward

Cut-through → switch ตรวจดู frame - match MAC table - แล้ว

→ No FC5 check Fast forward ~ 12 B 7.5ns collision less

→ No Auto Buffer Fragment-free ~ 64 B CSMA/CD - if ห้องไม่ต้อง collision Broadcast

### Collision Domain: กลุ่มของ帧 ที่ต้องเจอกัน

### Broadcast Domain: กลุ่มที่ broadcast packet ทุก NW ที่มี กำลัง 4

remote, local NW ต้องกัน

remote, gateway ต้องกัน routing

Hub

switch

Router

collision

Broadcast

4 4 1, + ต้อง VLAN

## Basic Switch Configure

- IP information assigned to switch SVI (also routing)

Switch# conf t

int vlan 99

ip address 172.17.99.11 255.255.255.0

no sh

exit

Switch#(config) ip default-gateway 172.17.99.1

- Duplex Command (ต้อง config ให้ duplex ให้ต่อท้าย 2 คำ)

Switch#(config) int fa 0/1

duplex full

speed 100

mdix auto

end

- Security

Switch#(config)# line vty 0 15

Switch#(config-line)# transport input ssh

login local

### Limit MAC Address

- static MAC Address

switch port-security mac-address แม่แบบ MAC

- Dynamic MAC Address → MAC แม่แบบของตัวเอง

switchport port-security mac address sticky

### Violated

Mode	Forward traffic	Send syslog	Display error	Increase violation	Shutdown port
Protect	X	X	X	X	X
Restrict	X	✓	X	✓	X
Shutdown	X	X	X	✓	✓



## Address Resolution Protocol

- MAP IP သို့ MAC Address တော်း IP Windows တွင် ပြန်လည်ပေါ်စေရန် MAC
  - Command : arp -a အဲဒုက္ခု ARP cache EX 10.10.0.3 = 00-0d-56-09-fb-d1
  - ARP Request : - ping (dest) request ၂ = time out
  - ARP Reply : ping reply

LAN Redundancy ensures the design is redundant

- Problem
    1. MAC database instability - MAC table របស់ learning ទូទៅនៃ frame នៃ ផែវិកាបានដោយខ្សោយ
    2. Broadcast storm - Frame ដែលចងចាំពីរុញទូទៅនៃ switch crash (infinite broadcast)
    3. Multi frame transmission - មនុតារ៉ា Dest MAC frame នៃ ឱន្ត switch នៃ Frame ណាត់

**Spanning Tree Protocol** නිර්මාණය කු නිවැරදි වූ මෙහෙයුම් පෙන්වනු ලබයි

- Only one logical path - block port ຢ້າງ  $\Delta$  topology ວິຊາ
  - Bridge Protocol Data Unit (BPDU) ໃກສານ port status ຢູ່ໃຈໃຫ້ loop

- Port Role և Root Bridge - համակառներու (RB) / NW

- Port Role**
    - ↳ Root Bridge -> សោរប្រកួត លាយចំណែក (RB/NW)
    - ផ្តល់ការពកគោរពជាកំណត់ថា មីនុយមិន root -> ផ្តល់ BPDUs នាក់ទៅវា
    - ចូល bridge ID : ដំឡើង
      - Priority → នឹងតួនាទី Priority ធ្វើការ MAC
      - MAC ឱ្យតាម SPT

2. Root Port - 1 RP/Non RB

- ყველა port გთის დანართს 1 rootport ში 1 switch

3. Designated Port - 1 DSN/ Seg

- ited Port - 78 block port minimo

3. Designated Port - 1 DSN/Segment (within LAN) - non root port

4. Non-Designated Port - It blocks port minors.

## 5. Alternate / Back up part

\*in cost inning, Bridge ID

\* in Bridge sender initia @ source port ID  
in BDPU

## SPT Characteristic

Protocol	Standard	Resource Needed	Convergence	Tree Calculation
STP	802.1D	LOW	slow	All VLAN
PVST	CISCO	HIGH	slow	Per VLAN
RSTP	802.1W	MED	fast	All
RAPID PVST+	CISCO	Very high	fast	Per
MSTP	802.1S Cisco	MED or HIGH	fast	Per

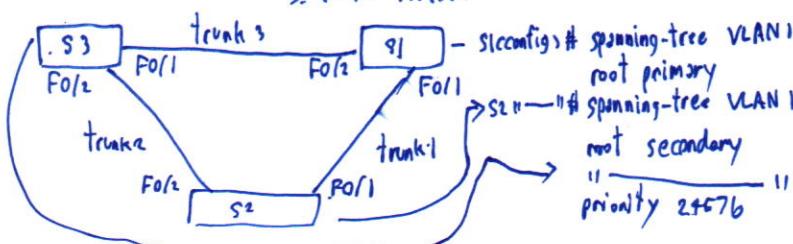
- port fast - یعنی port state من blocking نباشد
- bridgeguard - یعنی port نباشد error - disable شود بـ BPDPU

EX # spanning-tree port fast

# !! —> bdp guard disable

## Spanning tree Config

- PVST + Load Balancing : စိတ်အား VLAN
    - SLC(config)# spanning-tree vlan 10 priority 4096
    - S3C(config)# 11 -----, vlan 20 " 4096
  - Rapid PVST + : support RSTP on per-VLAN basis
    - SLC(config)# spanning-tree mode rapid-pvst
    - " ---" # int (interface-id)
    - " ---"-if) # spanning-tree link-type point-to-point
    - clear spanning-tree detected-protocols → clear all detected STP
  - Troubleshooting - မှာ track ရန်
    - remove redundant when failure
    - Problem 1. Default gateway limitation
    - 2. Router Redundancy
    - 3. Router failover



route lookup hierarchy - ჩვეულებურ lookup routing მიზანისას

- Ultimate Route - next hop

- LVL1 NW Route, Supernet Route, Default route

- LVL2 Parent Route (Group in LVL1, Route)

Level Router

Network → 192.168.1.0/24 → Port / Int  
 Network → 192.168.0.0/15 → Port / Int  
 Network → 0.0.0.0/0 → Port / Int

Next Hop IP and/or exit int

Parent Route → Child Route  
 Child Route → Subnet → Port / Int  
 Subnet: 172.16.1 / 24, 172.16.2 / 24, 172.16.3 / 24, 172.16.4 / 24

Ultimate route

  - Best Match
  - L1. Ultimate
  - forward
  - L1 Parent
  - examine child route (subnet)
  - L2 Child
  - forward
  - Not Match in L2
  - search L1 supernet / default route
  - Not Match any
  - Drop

172.16.0.0

200.165.200.0

200.165.200.24 / 30

200.165.200.25 / 30

200.165.200.26 / 30

Chapter 9 VLANs & InterVLAN

**VLANs (Virtual LAN)** - แบ่งช่องทาง Physical เดียวเป็น เน็ตเวิร์ก: logic คือ - วิธีการแบ่งเน็ตเวิร์ก叫 VLAN

- Benefit**
- Improve Security
  - Reduce cost (ไม่ต้องซื้อรุ่นละเมิด)
  - Better Performance
  - Smaller Broadcast Domain
  - IT Efficiency
  - Management Efficiency

Trunk

- จัดให้ switch ทุก VLAN ต่อเข้ากัน ผ่านทาง switch ภายนอกต่อตัวเป็นตัวกลาง
- VLAN tagging - ตรวจสอบว่าอยู่ใน VLAN ไหนใน Link ต่อไป
- config as trunk ทุก port ต้องอยู่ใน VLAN เดียวกัน
- switch flood หมายความว่า VLAN ใด trunk ใด broadcast Flood all

Native VLAN - config temp as Native

- ถ้าต้องการ Native - ต้องมีตัว tag

Assignment - Catalyst 2960, 3560 รองรับ 9000 VLAN (1-1005) - Extend 1006-1016  
- เก็บใน flash : vlan.dat ใน NVRAM

Summary 1. สร้าง VLAN

2. assign port ให้ member ของ VLAN

3. ตั้ง trunk link

InterVLAN - ยังต้อง trunk ระหว่าง switch กับ router ที่อยู่ต่อไป VLAN ต่างๆ

Chapter 10

**VTP** - จัดการ VLAN - เพื่อ, ลบ, แก้ไข ของ domain เดียว

- ใช้งานกับ Cisco Switch เท่านั้น

**Benefit** - consistently maintain VLAN access a common admin domain

- VTP is running and has certain default already config

Operation 1. Manage VLAN ต้องผ่าน trunk อันเดียว

- Parameter VTP config revision no. - 32 bit

- switch จะทำงานตาม domain ที่ config

	source VTP msg	Listen to VTP msg	Create and remember VLAN
server	✓	✓	✓
client	✓	✓	✗
transparent	✗	✗	✓

Configuration ต้อง manage VLAN via trunk, ต้องเดียว domain

• 2 mode, VLAN db  
conf t

Verify - show vtp status

VTP Pruning - ลด bandwidth ที่ต้องส่ง trunk

L > on traffic

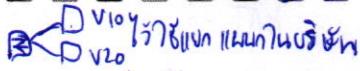
- Default - disable

- on config

(vlan db) - VTP pruning

(conf t) - int (int.id)

- switchport trunk pruning VLAN remove VLAN id



วิธีการใช้ VLAN ในการตั้งค่า



- NAT - Network Address Translation

- ຖានលាង IP រួម TP និង reuse ឬបាន private ទែរង
- NAT → ផ្តល់លាង IP ចាប់ពី pub ឬបាន private

- Characteristic - Terminology - Inside NW : Device w/ private IP  
- Outside NW : NW number

- Type of address
    - 1. Inside Local Address
    - 2. Inside Global Address
    - 3. Outside Local
    - 4. Outside Global

- Type of NAT

- static NAT
    - map private IP to pub new fixed-IP
    - server In inside or access from outside
    - SSH to

- ## ◦ Dynamic NAT

- Public can map multi-IP to private
  - map by one-to-many, run by one-to-one
  - inside local → in glo

- PAT - Port Address translation

- map IP-port into IP-IP မြန်မာစွဲတော့်တော့်
  - map multiple private IPv4 to single pub IP
  - dynamic NAT overload

## Benefit and disadvantage

## Benefit

- conserve the legally registered address
  - မြန်မာ flexible တိညိုင်ပေါ်မှုပါ ပုံမှန် NW
  - အမျိုးသုတေသနများ အတွက် internal NW addresses
  - NW security

disadvantage

- Downgrade Performance end-to-end function
  - End to End IP traceability lost
  - IP tunnel ဆောင်ရွက်မှု
  - Initiating TCP connection စွမ်းပေါ်မှု

## Config

- Static NAT
    - (conf t) - ip not inside source static
    - int (int types) → inside int
    - ip not inside
    - exit
    - int (types) → outside int
    - ip not outside

### - Dynamic NAT

- (conf t) - ip nat pool name start-ip end-ip  
          netmask subnet | prefix-length re-length

  - access list number permit source-Nw source-wildcard
  - ip nat inside source list number (access list) pool name
  - int c-types
  - ip nat inside
  - int c-types
  - ip nat outside

for Staples

Configuring PAT (NAT Overload)

- Router (conf t) - ip nat pool name start-ip end-ip netmask subnet-mask | prefix-length length
- access-list ac-num permit source-NW source-wildcard
  - ip NAT inside source list ac-num pool name overload
  - int (type)
  - ip NAT inside
  - int (type)
  - ip NAT outside
- Single Address → -
- ip NAT inside source list ac-num int (type) overload

Chapter 11 EIGRP

- EIGRP - Enhanced IGRP (Algorithm OSPF)

- Feature
  - Diffusing Update Algo
  - Establishing Neighbor
  - Reliable transport Protocol
  - Partial and Bound Update
  - Load Balancing
- PDM (Protocol-Dependent Module) support many protocol

↳ Maintain neighbor and topology table

Computing metric using DUAL

Interface DUAL and Routing table

Implementing Filtering and ACE

Performing redistribution w/ other routing protocol

Neigh Table : Next-Hop Router → Int

Topology Table : Dest1 → successor

Dest2 → Feasible Successor

Routing Table : Dest1 → successor

Hello in router to Nbr for topology

Update to routing info to dest.

ACK neighbor packet

Query neighbor about neighbor

Reply from query neighbor

- If RTP จัดส่ง packet : Update : every, Query, Reply, Hello, ACK

- Authentication support

- Message to Destination Multicast address : 01-00-5E00-00-0A

- Configuration - Autonomous System (AS) - Group of AS ที่ทำงานร่วมกัน [16 bit : 0-65535]

- ระบุตัวเอง route ที่ AS ของตัว

- Verify : show ip eigrp neighbors

- Operation 1. Router R1 ที่ส่ง Hello Packet ที่ routers ที่อยู่ในเครือข่าย EIGRP ที่ต้องการ update

2. Router R2 ที่收到 Hello Packet ที่ R1 ทั้งหมด R1 ใน neighbors table ที่ส่ง Hello ให้ R1 จะ send Update Packet ที่ต่อไป

3. R1 Update Neighbors table ที่ R2 ที่ต่อไป update ลง topology table

4. คำนวณ topology

5. R1 นำ ACK ที่ R2 ที่ต่อไป update ที่ต้องลง update ที่ R2 : advertise route

6. R2 นำ ACK ที่ R1

7. R1 นำ DUAL (คำนวณ topology) : metric + next hop, R2 นำ DUAL คำนวณ topology

- Metric - ตัวค่า cost ประกอบ Bandwidth ; lowest BW

- Delay : Cumulative

- Reliability : Load

- Config: Router (conf t) - metric weight das k1 k2 k3 k4 k5

- Bandwidth : Router (conf\_int) bandwidth kilobits

- Delay

for Staples



- Metric Calculating
  - Bandwidth (bandwidth / bandwidth)  $\rightarrow$   $(BW + D) \times 256 = \text{Metric}$
  - Delay (sum of Delay / 10)
- DUAL Topology Table - Term - successors: ien forward 10 neighbor it cost 100%  
 - Feasible Successor (FS) - Backup Path  
 - ~~Successors originate from topology tab~~  
 -  $BDC < FD$ : if true  $\rightarrow$  FS  
 - Reported Distance (RD) - Advertised Distance  
 - ~~On report from Neigh Router~~  
 - Feasible Dist (FD) -  $\text{In cost } \frac{\text{original cost}}{\text{metric}}$   
 - Operation -  $\text{on FS in s aninlu topology table}$   
 - ~~aninlu update in routing~~  
 - Verify: show ip eigrp topology  
 - Successor fail, no FS  
 DUAL  $\rightarrow$  active state, active query  
 it neighbor for a new successor

#### • Special command

- Redist (OSPF-static) - classless redistribute connected subnets
- RIP + static default - information originate

