

for Staples

Chapter 1 : Network Overview

- Network Devices
 - End Device : PC, Printer, Laptop
 - Intermedia Network Device : Switch, Router, Hub, AC
 - Network Media : Fiber Optic, UTP, Coaxial, RJ-45
- Network Protocol
 - Protocol ที่ใช้ในการสื่อสารกันระหว่างเครือข่าย กันไป
 - Address / Physical (MAC - DataLink)
 - Logical (IP - Network)
 - Special (Port - Transport)
- Network Type
 - LAN : small and single admin
 - WAN
 - Fault Tolerance - การ冗余เพื่อความปลอดภัย
 - Scalability - สามารถเพิ่ม/ลด NW ได้
 - Security - Limit Access ทาง物理层
 - QoS - ให้ความสำคัญ Service ที่ใช้งานอยู่
 - 物理层 - คือการเชื่อมต่ออีกฝั่ง - Crossover
物理层ต่อตัวเอง - Straight

NW Design ↗
Diagram VS Topology ↗
subset

- Physical Diagram - แผนผังที่แสดงโครงสร้าง NW จริงๆ
- Logical Diagram - แผนผังที่แสดงโครงสร้าง NW จริงๆ สำหรับการทดสอบ

OSI Model

	Application
(Data)	Presentation
(Segment)	Session
(Packet)	Transport
(Frame)	Network
(Bits)	Data Link
	Physical

TCP/IP Protocol

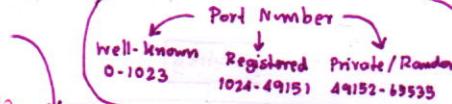
DNS
BOOTP DHCP
SMTP POP IMAP
FTP TFTP HTTP
TCP UDP
IP NAT ICMP OSPF EIGRP
ARP PPP Ethernet Driver

Chapter 2: Basic Router Configuration

การตั้งค่า config ของ router ตามที่ต้องการในแต่ละกรณี.

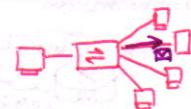
- IPv4 - Class → Unique [ตัวอักษร]

	NW	Hosts	Private IP
A :	N.H.H.H	0 - 127	126 16.8M 255.0.0.0 10.0.0.0/8
B :	N.N.H.H	128 - 191	16.4K 65.5K 255.255.0.0 172.16.0.0/12
C :	N.N.N.H	192 - 223	2M 254 255.255.255.0 192.168.0.0/16
D :	Multicast	192-224-239	N/A N/A

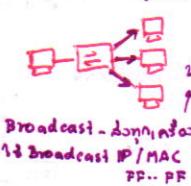
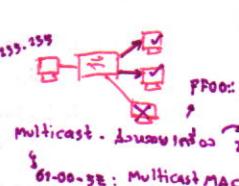
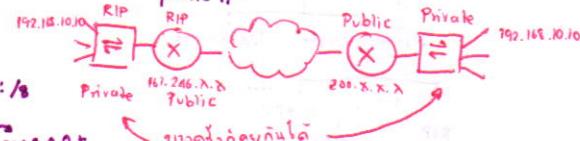


- MAC Address → Physical Address - identify actual source and dest.

for Staples



Unicast - ข้อมูลเดียวต่อตัว

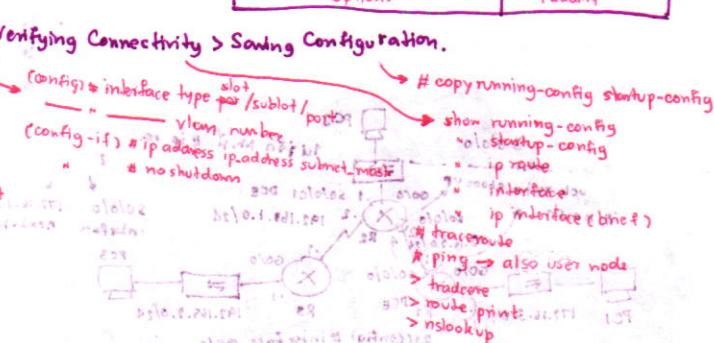
Broadcast - ข้อมูลเดียวต่อทุกคน
1. Broadcast IP/MAC
PF..PFMulticast - ข้อมูลเดียวต่อทุกคน
224.0.0.0+
61-00-5E: Multicast MAC

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
TTL	Protocol		Header Checksum
Source Address			
Destination Address			
Options			Padding

(config)# hostname CE7

```

(config)# banner motd $ . $  # privilege
          # enable password Ccna
          # enable secret class 1n privilege.
# User mode # line console 0 / line vty 0-n telnet
          # login
          # exit
          # password km1
          # enable password-encryption
  
```

**Chapter 3: Static Routing & Dynamic Routing Protocol**

- Routing → นำสิ่งที่ package ไปสู่จุดหมายปลายทาง

→ 3. Routing Table - รายการของทุกๆ อย่าง

- เก็บไว้ column

- บอกว่า final destination.

- Routing → Choose BEST Path

- Encap packet นำสิ่งที่ header ที่ต้องการไป

1. Static Routing

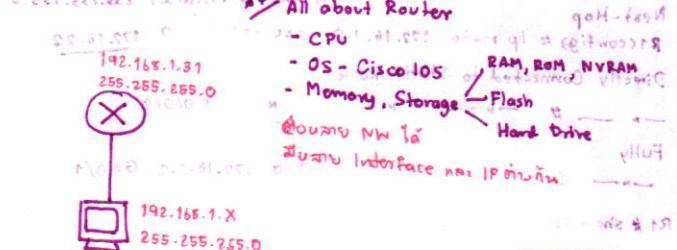
2. Dynamic Routing Protocol

- Forwarding 1. Process Switching - นำสิ่งที่ต้องการไปยัง packet ที่ถูก

2. Fast Switching - นำสิ่งที่ต้องการไปยัง packet ที่ถูก

3. CEF - lookup, trigger แล้ว forward อนาคต

- * ต้องมีค่า IP, subnet ที่ client ทุกตัว ไม่ default gateway information ที่ต้องติดต่อ NW ด้วย



CPU : 1.1.1.1 192.168.1.1

RAM, ROM, VRAM

Memory, Storage

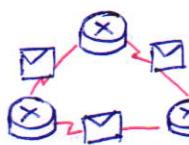
Flash

Hard Drive

Interface

IP ที่ต้องการ

for Staples

Distance Vector Routing Protocol

Function - not Information ระหว่าง router

- update routing table เมื่อ topology change
- ค้น best path ไป destination

Components - Algorithm, Routing Protocol Message.

Purpose - remote NW

- Maintain up-to-date
- ค้น best path
- ไม่ต้องมี information จำนวนมาก

• Interior Gateway Protocol

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

• Classifying Routing Protocol

- Classful = ใช้ class ในการ update ของ class
 - แบ่ง NW ออก mask มาก
 - แบ่ง subnet mask ทำ routing update
- classless - แบ่ง NW ตาม掩码 (without class)

* Convergence - State ของ NW จะมีผลต่อการคำนวณ path down → ต้องคำนึง update routing table ที่ router ต้องรู้

- router ต้องรู้ information ของ NW ที่มีเพื่อคำนวณ route

Metric - วิธีการคำนวณ route destination NW ที่ Best Path < Hop Count - RIP

Load Balancing - คำนึงถึง cost ของ 2 กรณี cost ของ NW ต้องเท่ากัน 1 เส้นทาง

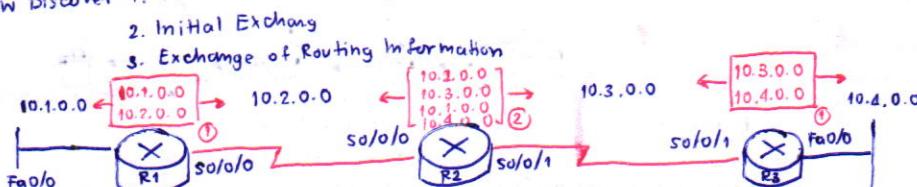
Administrative Distance - ใช้ protocol แล้ว add ให้ routing 1 เท่านั้น

• Distance Vector - router ที่ distance 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



in AD กี่ครั้ง	Connected	0
Static	1	
EIGRP	5	
Ext BGP	20	
Int EIGRP	90	
IGRP	180	
OSPF	110	
RIP	120	
IS-IS	115	
Ext EIGRP	170	
Int BGP	200	

Periodic Time Update

• RIP Update Timer

Default : 30s

Invalid : 180s (ใช้เวลาเดียว Rudolf Bellman)

Holddown : 180s (ใช้เวลาเดียว Invalid ด้วย)

Flush : 240s (เคลียร์ทั้งหมด 240s)

• Bound update : EIGRP

จะอัปเดตข้อมูลใน update ของตัวเอง

• Triggered → ถ้าเกิดมี change

• Random Jitter → Multiple Access

for Staples

Network	Interface	Hop
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

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

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

• RIP Problems

- ① Routing Loops กรณีที่ NW down ที่ต้องการ interface ที่ไม่ได้ packet วนloop
 - Hop Count to Infinite [Ex: R3: Fa0/0 → S0/0/1]

→ Setting a maximum hop counts → 16 hops = unreachable

→ Hold down timer → Hold กรณีที่ NW down ต้อง update ที่ต้อง down อยู่

② Split Horizon Rule กรณีที่ NW ต้องการ interface ที่ต้อง update ที่ต้อง update ที่ต้อง

③ Route Poisoning กรณี NW down → set unreachable → Poison Update

④ Split horizon and poison reverse - ③ + ③

⑤ IP & TTL - กรณี packet ของตัวเอง 0 ต้อง drop it's

10.3.0.0	1	10.2.0.0	1
10.4.0.0	2	10.1.0.0	2

RIPv1

Characteristic - classful, distance vector → not send subnet mask

- metric as hop count
- hop count > 15 = unreachable
- broadcast every 30s
- can Auto Summarize

Rule 1. Routing Update in Interface received on

some NW

- Subnet Mask applied to the NW on the routing update.

2. if different NW

- Classful subnet mask applied to the NW in routing update.

update subnet!

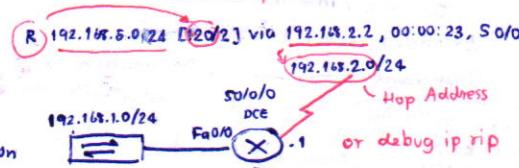
networks

RIP config know how

R1(config)# router rip

R1(config-router)# network [xx NN]

R1# show ip route



Passive Interface → กรณี interface ที่ไม่ต้องการ broadcast

R(config-router)# passive-interface int-type int-no

Automatic Summarization → RIP จะ auto summarize บน routing table → faster lookup

ไม่ support discontiguous network (NW ใน class ต้องติดต่อกัน)

[router ต้อง advertise major network address]



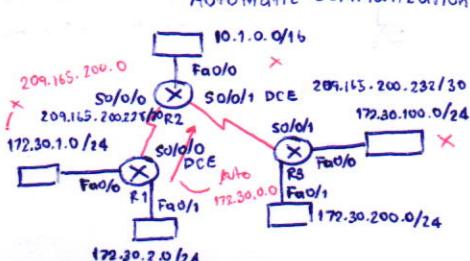
Default Route - packet ที่ไม่ได้ Address ที่มีใน routing table มี default route

ip route 0.0.0.0 0.0.0.0 [int-type]

default-information originate → redistribute default route

through rip ๐๖

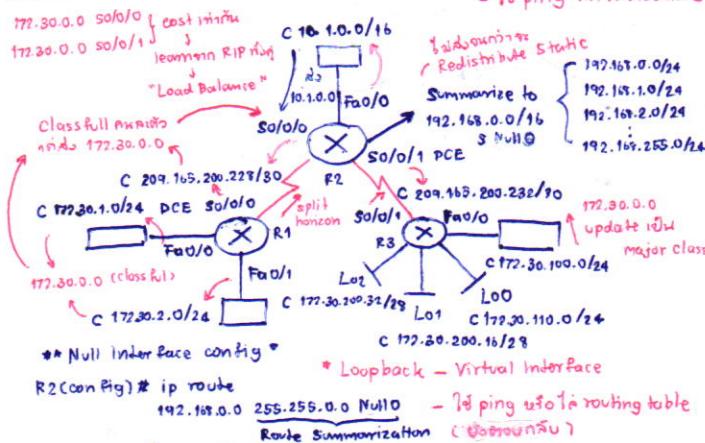
show ip protocols → display timer by RIP



RIPv1

- classful - update 1A/W7 address
- ไม่ support discontiguous subnet
- ไม่ support VLSM (except case) + CIDR
- ไม่ support subnet mask in routing update
- update news broadcast

RIPv1 Limitation



Access Control List

- Packet Filtering : Filter ที่ต้องไม่ต้องคำนึงถึง statement ใดๆ
- Operation - always implicit deny - deny any → ไม่มีทุกอย่าง (deny everything)

Standard

- block หรือ block user
- check only source address
- permit กรณี entire protocol suite (ทั้งหมด)
- (1 to 99) and (1300 and 1999)

Extended

- 既能 block
- check source and destination (ทั้งสอง)
- permit/deny specific protocol suite (บาง protocol บางๆ)
- (100 to 199) and (2000 to 2699)

Ex. match Wildcard Mask

1. 192.168.1.65, -67, -69,..., -127

Soh	.65 :	0100 0001
	.67 :	0100 0011
	.69 :	0100 0101
	:	:
	.127 :	0111 1111
		01XX XXX1
		0011 1110

WC: 0.0.0.0.0011110

Ans 192.168.1.65 0.0.0.62

2. 192.168.64.x - 192.168.191.x

Cx is odd	- 例 2 บวกกัน
Soh	192.168.01000000.X
	192.168.01000001.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

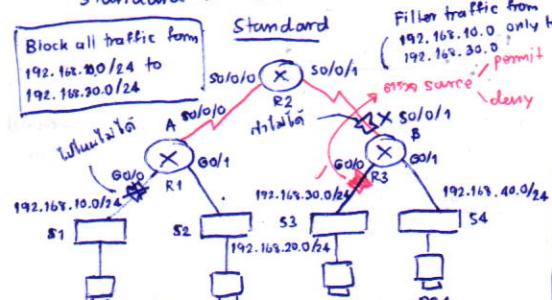
• ACL Creation - สร้าง policy 什么样的

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

- Extended → ไม่ Source

Standard → ไม่ Destination

Filter traffic from 192.168.10.0/24 to all dest reach by R3



Block all traffic from 192.168.10.0/24 to 192.168.30.0/24

Standard

source

deny

permit

destination

Block all FTP and Telnet traffic from 192.168.11.0/24 to 192.168.20.0/24

Extended

source

deny

permit

destination

Examine all traffic before exiting R1 so/0/0

Examine traffic only from 192.168.11.0/24

closest to dest

so/0/1

so/0/0

so/0/1

so/0/0

so/0/1

so/0/0

so/0/1

so/0/0

Create name

ip access-list [standard | extended]

name

ip access-group [in | out]

exit190

Standard IP access list 1

10 deny 192.168.10.10 (8 matches)

20 permit 192.168.0.0 , wc 0.0.255.255

• Configure * no access-list ไม่มี access list ที่ไม่มี number ที่มีชื่อใน list

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

Ex #access-list 1 permit ip 192.168.10.0 0.0.0.255

access-list 2 deny any ← deny all

• Apply to Interface : ip access-group 1 in ← into router.

Router(config-if)# ip access-group 1 in

RIPv2

- classless - update netmask subnet

- enhancement of RIPV1's feature

- at Next hop address to update

- update news multicast

- at authentication

- support VLSM + Route Summarization + Auto summary

- no routing loops ด้วย timers

- แบ่ง split horizon ว่า poison reverse

- triggered updates

- Max hop count = 15

- auto boundary - major class nw must sum to sum

Routing Table

R1

C 172.30.1.0/24 Fa0/0

C 172.30.2.0/24 Fa0/1

C 209.165.200.228/30 Fa0/0

R 10.0.0.0/8 So0/0

R 209.165.200.232/30 So0/0

R2

C 10.1.0.0/16 Fa0/0

C 209.165.200.228/30 Fa0/0

C 209.165.200.232/30 Fa0/0

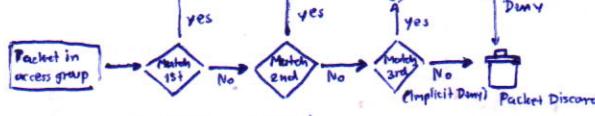
R 192.168.0.0/16 Null0

R 172.30.0.0/16 So0/0

(config) R1 initializel R1 So0/0/1

```
R1 (config) # router rip
(config-router) # network 209.165.200.0
               # network 172.20.0.0
[ERIP]# learn [ip]
R1 (config-router) # version 2
RIP v2 → ignore vt update
```

Packet config



Wildcard Mask

- Inverse of Subnet Mask

Ex 192.168.1.0 255.255.255.0

WC 192.168.1.0 0.0.0.255

match → Fix bit ← not match any

0.0.0.0 → mask 0000

255.255.255.255 → 1's mask 11111111

if IP 192.168.1.1 .00000001

WC 0.0.0.255 .11111111

Result 192.168.1.0 .00000000

192.168.0.00000000

→ 192.168.1.0 - 192.168.1.255

192.168.255.0 - 192.168.255.255

* Calculate → 100 255.255.256.255 คิดตัว subnet 1 คิม

(invert from WC)

* no access-list ไม่มี access list ที่ไม่มี number ที่มีชื่อใน list

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

Ex #access-list 1 permit ip 192.168.10.0 0.0.0.255

access-list 2 deny any ← deny all

• Apply to Interface : ip access-group 1 in ← into router.

Router(config-if)# ip access-group 1 in

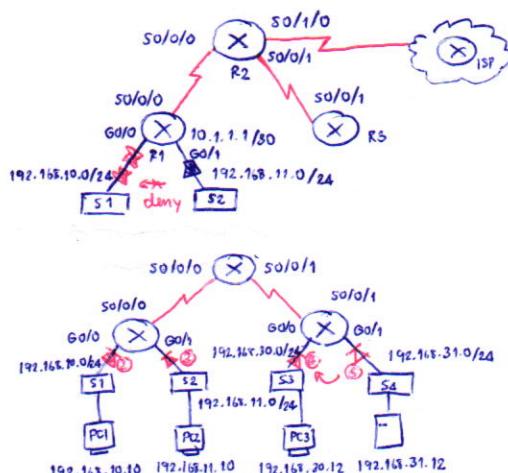
for Staples

Access Control List (cont)

- Secure VTY Port for Telnet or SSH

Router (config-line) # access-class access-list-number {in [vrf-also]} out

- Extended ACL - ริมูนิชัน Standard



- Apply Extended ACL to Interface

R1 (config)# access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80

—> # —> n n n —> n 443

—> # —> 104 * * * deny 192.168.10.0 0.0.0.255 established

R1 (config)# interface go/0

R1 (config-if)# ip access-group 103 in

—> # ip access-group 104 out

- Filter traffic with Extended ACL

R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 80

—> # access-list 101 permit ip any any

—> # interface go/1

R1(config-if)# ip access-group 101 in

R2(config)# ip access-list extended 101 → ดูใน access list ที่ debug

- Troubleshooting

1) 192.168.10.10 no connect w/ 192.168.30.12 —> ล็อก 10 กับ 20 ต่อ 30 oun
10 permit tcp 192.168.10.0 0.0.0.255 any eq telnet (12 match(es))
20 deny tcp 192.168.10.0 0.0.0.255 any

2) 192.168.10.0/24 cannot use TFTP to connect 192.168.30.0/24
30 permit tcp 192.168.10.0 any

3) 192.168.11.0/24 can use Telnet to connect 192.168.30.0/24 but shouldn't be allowed.
10 deny tcp any any eq telnet

4) 192.168.30.12 able Telnet to connect 192.168.31.12 but shouldn't allow.
10 deny tcp host 192.168.30.12 any eq telnet

5) 192.168.30.12 able Telnet to connect 192.168.31.12 — security not allow

- จัดบล็อกใน S3 block ที่มีปัญหา.

for Staples

Open Shortest Path First

- Link-State Routing Protocol - ดูการคำนวณทาง NW ที่ topology

[Link State Distance Vector ที่รู้ว่าคนติด neighbour routers อยู่]

IPv4 → OSPFv2

IPv6 → OSPF v3

AD → 110

- hierarchical, fast convergence

- admin have good knowledge

- Algorithm → Shortest path first (SPF)

- Update - Router learns directly connected networks.

- "Saying Hello" to its neighbours 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.

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-State DB → Topology Table : show ip ospf database
- Forwarding DB → Routing Table : show ip route

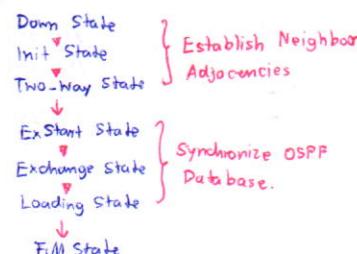
OSPF

- ds - Hello Packet

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

- Update info Multicast : 01-00-5E-XX-XX-XX
- ds Hello Message on 10S Broadcast LSP ที่ 30S

- Operation



- Process 1. 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

Area

- Single Area - Area 0

- Multiarea - Area 0 as backbone area

for Staples

- ผู้รับ Adjacency ที่ไม่ packet วน router ไม่สามารถเห็น

IP ของตัวเอง DR + BDR

PR → ต้อง packet แล้ว broadcast ให้ตัวอื่น ที่ต้องการที่จะรับข้อมูล

BDR → Available if PR failed

* passive-interface : ไม่ให้เก็บ routing update ที่ interface ที่

process-id = int process ที่เป็น OSPF (1-65535)

* ต้องการ router ต้องต่อ

* บน NW ต้องต่อ 1 เท่านั้น ต้องไม่ต่อ [ไม่ต่อที่ต้องกันไปต่อที่อื่น]

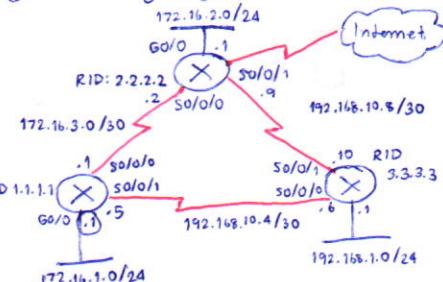
router-id - id ของ router ที่จะ check process ที่ router ที่ id นั้น

- 78 บนตัวที่ต้องกัน router ต้องนี้

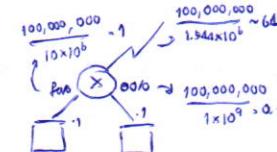
* ต้องต่อ loopback / active ip address แนะนำ



OSPF Configuring



```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
* 0:0:0:1 - 0:0:0:1 Interface 0:0:0:1 on R1
R1(config-router)# network 172.16.1.1 0.0.0.0 area 0
R1(config-router)# passive-interface GigabitEthernet 0/0
```



Cost = reference bandwidth / interface bandwidth * ref. bandwidth = 10^8
~~auto-cost ref-bandwidth bandwidth_mbps~~

- Default Internet Bandwidth = bandwidth of interface + cost (default 1.544 Mb/s)
- Default Route ip route 0.0.0.0 0.0.0.0 loopback 0
- Redistributing redistribute? → გადაიცემ rip უნივერსალურ კუნძულში

Dynamic Host Configuration Protocol

- Protocol განვითარებული მანეჯმენტი IP Address + Subnet Mask / Default Gateway / DNS (both IPv4 and IPv6)
- Methods
 - Manual Allocation - set lease Control Panel / cmd
 - Automatic Allocation - Fix IP ან განკარგვა
 - Dynamic Allocation - მომ იპ იმ პოლ განვითარებული server.
- Operation
 - DHCPDISCOVER - Client და request სამსახური DHCP server → Broadcast
 - DHCPOFFER - Server და Assigned IP Address გვიათ Client → Unicast
 - DHCPREQUEST - Accept IP Address გვიათ Server → Broadcast [ზოგადი გერეტი სისტემის მიერთო]
 - DHCPACK - Server და ACK გვიათ Client → Unicast
- Command ინიციალიზაცია - ipconfig /renew → მიმღები IP Address იმ DHCP
 - ipconfig /release → უნიკალური IP Address უკვე უკვე მიმღები

* no service dhcp - უკვე DHCP

Configure DHCPv4 Server

- Exclude address from the pool - უკვე მიმღები უკვე უკვე მიმღები IP Address ; Server, Default Gateway
- Setup DHCP Pool name

- Configuring Specific Tasks - define range of addresses and subnet mask. - Use default-router cmd.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9 → ip range მიმღები
R1(config)# ip dhcp excluded-address 192.168.10.254 → გენერიკული default gateway
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
    # domain-name example.com } optional
    # end
```

- Verify DHCP - show running-config | section dhcp
 - show ip dhcp binding
 - show ip dhcp sever statistics

PC → ipconfig /all

Relay:

ip helper-address
→ უკვე router broadcast
უკვე ip მიმღები

next Config DHCP ის გერეტი გვიათ NW
 R1(config)# interface go/1
 R1(config-if)# ip address dhcp
 # no shutdown

Troubleshooting

- Resolve Conflicts
- Verify physical connectivity
- Test with a static IPv4 address
- Verify switch port configuration
- Test from the same subnet or VLAN

IPv4 → Classless Inter-Domain Routing (CIDR)

- Fixed Length Subnet Masking - ყოველი სუბნეტი ერთგული
- Variable Length Subnet Masking - ყოველი სუბნეტი განსაზღვრული

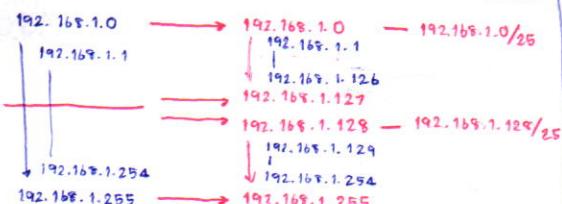
Subnet Planning

Network 161.246.6.0 /23

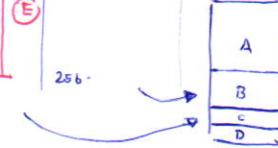
- IP Address 161.246.6.0
- 161.246.6.1
- ...
- IP Address 161.246.6.255
- 161.246.7.0
- 161.246.7.1
- ...
- IP Address 161.246.7.255

Network	Res. 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	255.255.255.224
E	31	62	161.246.7.192	255.255.255.192

範例 192.168.1.0 /24 → /25 * /24 → 128 → 4 bit → 16 ბიტი



Subnet Mask
/31 255.255.255.254 Not Valid
/30 255.255.255.252
/29 255.255.255.248
/28 255.255.255.240
/27 255.255.255.224
/26 255.255.255.192
/25 255.255.255.128
/24 255.255.255.0
/23 255.255.254.0
/22 255.255.252.0
:
/16 255.255.0.0
/15 255.254.0.0
:
/9 255.128.0.0
/8 255.0.0.0



Basic Switch Network

- LAN Design - based on Admin and Policy

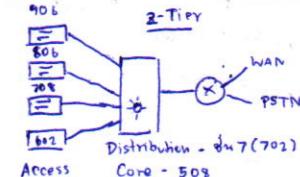
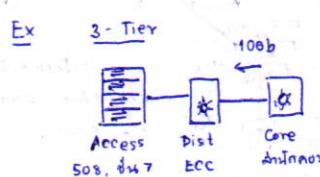
- Borderless switch network design - Hierarchical - รูปแบบเดียวกัน
 - Modularity - ยืดหยุ่น
 - Resiliency
 - Flexibility

3-Tier: Core — Distribution — Access

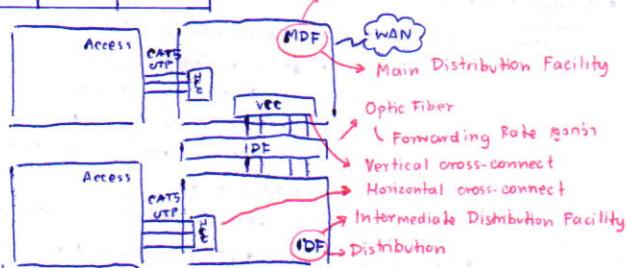
2-Tier: Collapsed — Access
(Core + Distribution)

กรณี Tier ไม่มีใน Overlapped หรืออยู่ด้วยกัน

Port	Port Security	VLANs	Fa/Gig	POE	Link Aggregation	QoS	Layer 3 Support	Forwarding Rate	Redundant Component
Access	✓	✓	✓	✓	✓	✓	-	Medium	-
Distribution	ACL	-	10Gb	-	✓	✓	✓	High	✓
Core	-	-	10Gb	-	✓	✓	✓	Very High	✓



- POE: Power over Ethernet จ่ายไฟผ่านสาย
- Fa/Gig : BW ที่ support Link Aggregation = 2Gb Link ที่ support BW มากที่สุดที่ Redundant = 1Gb per switch ต่อ



- Maximize LAN bandwidth
 - Placement of Servers
 - Workgroup
 - Collision detection issues → ไม่ใช้ใน LAN แต่ใน domain เท่านั้น
 - Segmentation issues
 - Broadcast domain issues

1 port of MAC Address ต้องมีอยู่ 1 MAC Address ต่อ 1 port

Switch Operation

- Learning - พอ switch รับเข้ามาที่ port จะ **table** ที่ Port No. และ **MAC Address** plus learn ถูกต้อง frame ที่ switch
- Aging - พอ switch ไม่ได้ receive ไม่ได้ frame ที่ source ที่ต้องการมาเรียบร้อยๆ หรือ drop ต้องลบตัวนั้น out ของ table
- Flooding - พอ switch ไม่รู้ table ไม่รู้ Source MAC Address ที่
- Unknown Unicast MAC 2. Broadcast MAC 3. Multicast MAC
- Forwarding - พอ switch รู้ว่า frame ที่ต้องการจะไปที่ Dest. Port ที่อยู่ใน Port number (store-and-forward in Table)
- Filtering - พอ switch รู้ว่า Source Address ที่ port ไหน จึงไม่ส่ง

Transparent Bridge Process

Flood Packet

↑ yes

Filter Packet

↑ yes

- Receive Frame → Learn source → BC, MC, Unknown UC → Source/Dest same Inf → Forward unicast to correct port
No → Forward unknown to all ports

Forwarding Methods

Store-and-forward → 16B CRC ถ้า Error ถือ U store และ forward

Cut-Through → Switch ตัดหัวของ frame - match MAC Table → ส่งเลย

→ No FCS check

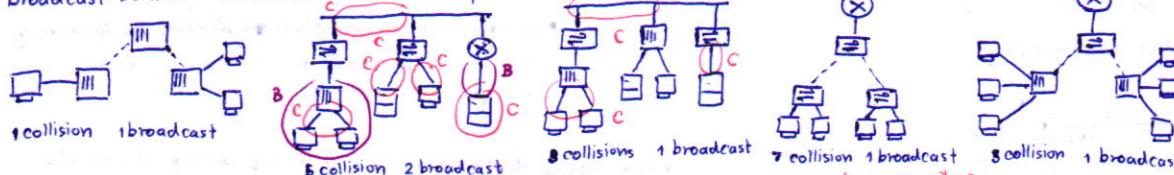
→ No Auto Buffer

Fast-forward ~ 12 B

Fragment-free ~ 64 B

↑ ต้องการ collision less

↑ บน CSMA/CD - if ณ คุณต้อง 64 B

Collision Domain - ไม่สามารถ Auto ต่อที่เดียวกันได้Broadcast Domain - ไม่สามารถ broadcast packet ที่ NW ต่อBasic Switch Configuration

- IP information (address, subnet, gateway) assigned to switch SVI (also Remoting)

```
S1# conf ter
S1(config)# int vlan 99
S1(config-if)# ip address 172.17.99.11 255.255.255.0
S1(config-if)# no sh
S1(config-if)# exit
S1(config)# ip default-gateway 172.17.99.1
```

- Duplex Communication → s1s config 100 duplex full ก็ได้

```
S1(config)# int fa 0/1
```

```
S1(config-if)# duplex full
```

```
S1---# speed 100
```

```
S1---# media auto
```

```
switchport mode access
```

```
S1---# end
```

```
S1# show mac-address-table
```

- Security Remote Access → SSH Operation

```
s1(config)# line vty 0 15
s1(config-line)# transport input ssh
s1(config-line)# login local
```

Limit MAC Address

- Static MAC address

switchport port-security mac-address static MAC

- Dynamic MAC Address → MAC ที่ได้รับอนุญาตจะเปลี่ยน

switchport port-security mac-address dynamic

- Sticky MAC Address

MAC ที่อยู่ใน table จะถูก running

MAC ต้องตั้งให้เป็น unblock

↓

↓

↓

↓

↓

↓

↓

↓

↓

Violated

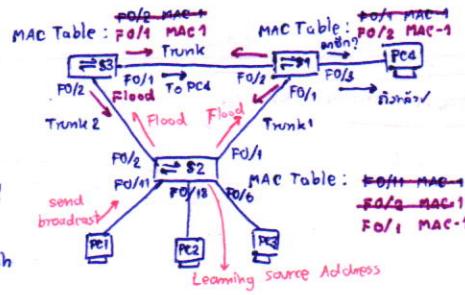
Mode	Forward Traffic	Send Syslog	Display Error	Increase Violation	Shutdown Port
Protect	X	X	X	X	X
Restrict	X	✓	X	✓	X
Shutdown	X	X	X	✓	✓

switchport security violation mode.

Address Resolution Protocol

- Map IP with MAC Address និង IP អាជីវកម្មសំគាល់របច្ឆុទ នៃការពារតាមលក្ខណៈ MAC
 - Command : `arp -a` ដើរកិច្ច ARP CACHE Ex 10.10.0.3 = 00-0d-56-09-fb-d1
 - ARP Request - ping (dest) request -> timeout
ARP Reply - ping reply

* ចំណាំរបៀបទាញឱ្យមែនក្នុង ARP Cache មាន

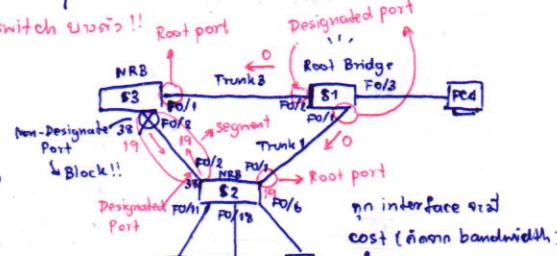


LAN Redundancy means ms Design in Redundant

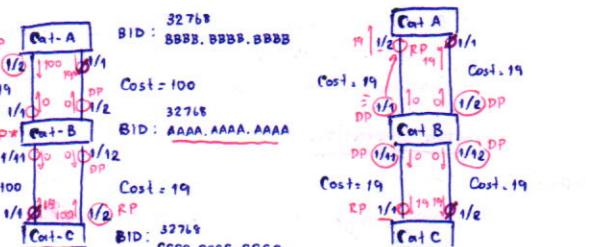
- Problem 1. MAC database instability - MAC Table នៃ learning បានឈរ frame ទាំងអស់ទៅក្រោម
 - 2. Broadcast Storm - Frame ដែលចូលទៅឱ្យផ្តល់ទៅលាស់លើ switch ធ្លាប់ក្រុមហ៊ុន (infinity broadcast)
 - 3. Multiframe Transmission - សម្រាប់ Dest តើ Frame នៃវីដីo switch ដែល Frame រាយ

Spanning Tree Protocol

- Only one logical path - block port ໃບ ເພີ້ນທີ່ໃຫ້ topology ເພີ້ນ
 - Bridge Protocol Data Unit (BPDU) ໃຫ້ຄໍານວນ port status ລາຍເຖິດ loop.
 - Port Role**
 - Root Bridge - ສັງເກດສັບອັນ ໄນກ່ອນ "RB/NW"
 - ຮັບໂຄງກູມກ່າວຄະດີວ່າຕ້າງໆແປນ root - ໂດຍ BPDU ນາຍຸງອຳນວຍ
 - ອຸປະກອນ, Bridge ID : ໂົມທີ່ຊັດ
 - Priority → ເລີນ MAC ນາມຊົນ
 - MAC Address - ໃຫ້ຄໍານວນ SPT
 - Root Port - 1 RP / Non RB
 - ສັງເກດ ດໍາລື ນາຍຸງອຳນວຍ 1 root port ຕົວ 1 ຕັ້ງ
 - Designated Port - 1 DSN / Segment (ສານ LAN 1 ແລ້ວ) - non root port
 - Non-Designated Port - 1 Block port ທີ່ມີເນື້ອ

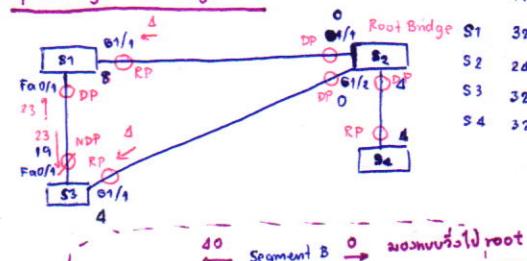


- Path Cost - Cumulative Path Cost
station root
 - 1st in BPDU (learn from root bridge)

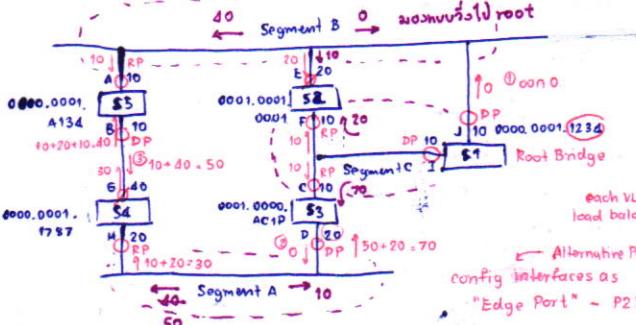


*² an cost minn \rightarrow "Bridge ID"
an Bridge Sender minn \rightarrow "Source Port ID" an BPDU

Spanning Tree Algorithm



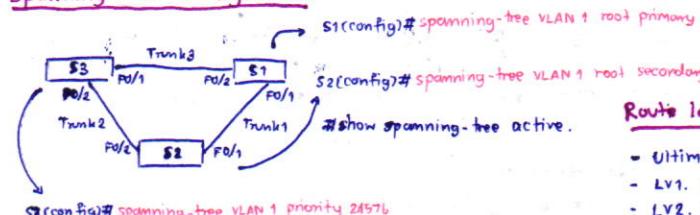
Priority	MAC Address	Cost=19
769	000A001111 * RP	DP 1/1 0/0 0/0 P
577	—> 22222	RP* Cost= B
769	—> 53333	DP 1/1 0/0 0/0 P
769	—> 44444	Cost=100



SPT Characteristic

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High		Per VLAN
RSTP	802.1W	Medium		All VLANs
Rapid PVST+	Cisco	Very High	Fast	Per VLAN
MSTP	802.1S Cisco	Medium or High		Per Instance

Spanning Tree Configuration



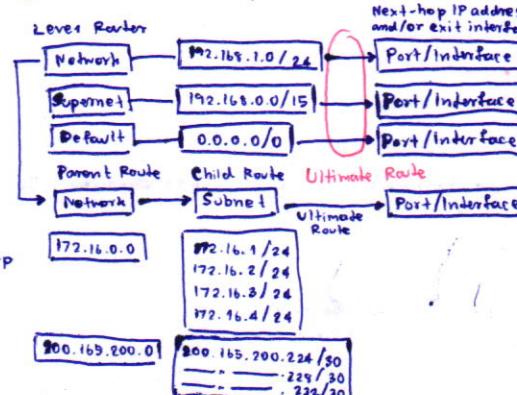
- PVST + Load Balancing : ~~multiple~~ VLAN
 - S1 (config)# spanning-tree vlan 10 priority 4096
 - S3 (config)# — — — vlam 20 — — 4096
 - Rapid PVST+ ; support RSTP on per-VLAN basis
 - S1 (config)# Spanning-tree mode rapid-pvst
 - — # interface [inf-id]
 - S1 (config-if)# spanning-tree link-type point-to-point
 - // clear spanning-tree detected-protocols → clear all detected STP
 - Troubleshooting : ~~multiple~~ 3 steps

- portfast - Wann port state von blocking in zu forwarding
bpduguard - sollt port von error-disable in BPDU

Ex # spanning-tree portfast
————— bpduguard disable

Route lookup Hierarchy - รูปที่แสดง route lookup routing เป็นรูปต่อๆ กัน

- Ultimate Route - next hop
 - LV1. NW Route, Supernet Route, Default Route
 - LV2. Parent Route (Group in LV1. Route)



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

Chapter 9 VLANs & Inter-VLAN

- VLANs (Virtual LAN)** - เครือข่ายภายใน Physical เดียวกัน แต่เป็น Logical ต่างๆ
 - แต่ละ VLAN เป็น broadcast domain & IP 子网

Benefits

- Improve Security
- Reduce Cost - ใช้ปั๊บต่อตัวเอง switch แทนตัว [Up to NW Topo Scale]
- Better Performance
- Smaller Broadcast Domain - Segment broadcast noise VLAN
- IT Efficiency
- Management Efficiency

* show vlan - show โครงสร้าง switch ของ VLAN ที่อยู่ใน switch

Trunk - ไฟล์ switch ให้ VLAN เดียวกันผ่านตัว switch ต่อไปได้ (ไม่ต้อง SPT ในการเดินทาง VLAN)

- IEEE802.1q - แต่ละ VLAN ทำ Link Layer (จะมี VLAN ID ใน port) \rightarrow Track frame ของ VLAN ที่มีความต้องการ tag \rightarrow frame - VLAN ID
- config as trunk ที่ port ไม่ว่ากี่บิตก็ได้ต่อ 1 VLAN
- switch flood ของ VLAN ที่ trunk ที่ broadcast Flood all

Native VLAN

- config temp as Native \rightarrow ทุก VLAN ที่ Native / Temp
- กรณี Native VLAN - จะต้องมี tag แต่ละ VLAN ที่ VLAN 105

Assignment

- Catalyst 2960, 3560 รองรับ 4,000 VLAN (1-1005) - Extended 1006-4096
- เก็บไว้ใน flash : vlan.dat ใน NVRAM
- * จัด VLAN ต้อง same - ทุก interface ที่ต้องเก็บใน flash
 - membership ต้อง same - ไม่สนใจ

Summary

1. สร้าง VLAN
2. Assign port ที่มี membership ของ VLAN
3. หา trunk link.

Inter-VLAN

- แม่板ต้อง trunk ระหว่าง switch และ router เพื่อให้ทั้ง VLAN ภายนอก (นักเรียนภายนอก NW)

* ก็ตต์ config trunk ที่ port ณ router ต้อง

Sub-Interface Configuring!

```
R1(config)# interface int-id.subif some num as vlan-id
R1(config-subif)# encapsulation dot1q vlan-id
      # description vlan vlan-id
      # ip address ip-address subnet-mask
      # exit
R1(config)# interface intid
      # no shutdown
```

Chapter 10 : VTP + NAT

- * **VTP** - ใช้ในการ管理 VLAN - ใหม่, 旧, ไม่แนบทรร. ลงใน Domain เดียวกัน
 - Cisco Proprietary ที่ทำงานกับ Cisco Switch ไม่ต้องมาต่อ

Benefit

- Consistently maintain VLAN across a common administrative domain
- VTP is running and has certain defaults already configured

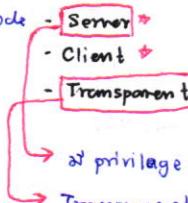
Operation

→ Manage VLAN ต้องต่อตัวกับ trunk ต้อง

- Parameter: VTP configuration revision number - 32-bit, 0-4294927295 (increment by version 1)

- Switch activation domain ที่ต้อง config ให้

- ที่ต้องมี 3 mode



→ privilege สามารถ modify, add VLAN + config ให้กับ

→ Transparent : forward VTP message to other switch.

- Configuration** - ต้อง manage VLAN via trunk \rightarrow ต้องมี Domain \rightarrow ต้องมี VLAN domain เดียวกัน

- ต้อง 2 mode **Global**

VLAN

- Access VLAN \rightarrow VLAN database (EXEC privilege)

Global Configuration

Switch# conf t

Switch(config)# vtp version 2

----- # vtp mode [server/client/transparent]

----- # vtp domain *domain-name*

----- # vtp password *domain-password*

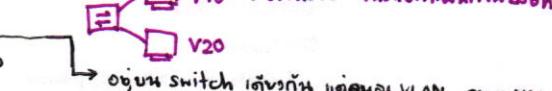
Switch# vlan database

Switch(vlan)# vtp v2-mode

----- # vtp [server/client/transparent]

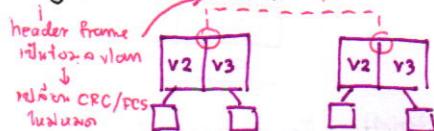
----- # vtp domain *domain-name*

----- # vtp password *domain-password*

VLAN Configuration

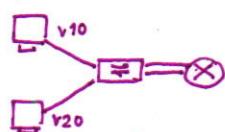
Native VLAN (VLAN1) คือ default ทุก port อยู่ใน VLAN 1
ใน port ที่ switch อยู่ใน membership
ใน VLAN เดียวกัน (port based)

PHYSICAL PORTS อยู่ใน NW เดียวกัน \rightarrow VLAN เดียวกัน



Config

```
switch# vlan database
switch(vlan)# vlan vlan-id name vlan-name
switch(config)# interface int-id
      # switchport mode access
      # switchport access vlan vlan-id
* if trunk: switchport mode trunk.
```



* ต้อง Router ที่ต้อง trunk interface ที่ subif

Hierarchy - Ultimate Route

- LV1 - Subnets lookup routing
 - NW Route
 - Supernet Route
 - Default Route
- LV2 - Parent Router

→ ต้องมี route ที่ switch ต้องรู้ด้วย

→ ต้องมี route ที่ switch ต้องรู้ด้วย

for Staples Configuring PAT - a.k.a NAT overloading

```

Router(config)# ip nat pool name start-ip end-ip netmask subnet-mask | prefix length prefix-length
---# access-lists ac-number permit source-nw source-wildcard
---# ip nat inside source list ac-number pool name overload
---# interface type number
Router(config-if)# ip nat inside
---# interface type number
---# ip nat outside

-Single Address-
Router(config)# access-list ac-number permit source-nw source-wildcard
---# ip nat inside source list ac-num interface type number overload

```

Interface ต้องเป็น public

Chapter 11 EIGRP

• EIGRP - Enhanced IGRP ใช้หลักการเดียวกับ OSPF

- Features
 - Diffusing Update Algorithm (DUAL) Dual routing algorithm
 - Establishing Neighbour Adjacencies Guarantee loop-free in backup path.
 - Reliable Transport Protocol Relationship w/ Directly connected routers
 - Partial and Bounded updates Use adjacency to track neighbors's status.
 - Load Balancing - Cost balancing กับ Load Balancing ต่อ
- 7. PDM (Protocol-Dependent Modules) ไม่ Support สาม protocol ต่อๆ กัน

↳ Maintain neighbor and topology table

Computing metric using DUAL

Interfacing DUAL and routing table

Implementing filtering and ACL

Performing redistribution w/ other routing protocol

Neighbor Table: Next-Hop Router → Interface

Topology Table: Destination → Successor

→ 2 → Feasible Successor

Routing Table: Destination → Successor

- 7. RTP ดูแลรับ packet : Update, Query, Reply, Hello, ACK

- Authentication support

- Message ไปยัง Destination Multicast Address : 01-00-5E-00-00-0A

Hello ไป router ที่ NW + ข้อมูล topology

Update 보내 routing information ไป destination - update ผ่าน ACK ตอบกลับ packet

Query ต่อตัวมีเพื่อนบ้าน neighbor - update ถ้า NW down

Reply ตอบ Query คืน

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

- 7. กำหนดเส้นทาง route ที่ AS ต่อๆ กัน

- Config : Router(config)# router eigrp **AS*** NOT Autonomous System!!

แต่ PROCESS ID of routing domain

Router(config-router)# eigrp router-id **router-id** ต้อง Criteria ที่ router-id > loopback > highest IPv4

(Optional) Router(config-router)# network network-number wildcard-mask

Router(config-router)# passive-interface type number [default] ไม่รับการ send update

- Verify : show ip eigrp neighbors

• Operation 1. Router 1 ริบส์ Hello Packet ให้ neighbor router ที่มีความสัมพันธ์ EIGRP ที่จะทำการ update

2. Router R2 ได้ Hello Packet ที่ R1 หล่อส่ง R1 นำ R2 นำ neighbor table หล่อส์ Hello ให้ R1
และ Update Packet ให้ตัวเอง

3. R1 update neighbor table ให้ R2 หล่อส์ update ให้ topology table

4. ลง topology

5. R1 ให้ ACK ให้ R2 หล่อส์ update ให้ R2 หล่อส์ update ให้ R2 : advertise route

6. R2 ให้ ACK ให้ R1

7. R1 นำ DUAL คำนวณ metric ของ route ต่อๆ กัน : metric + next hop , R2 คำนวณ ของ route ต่อๆ กัน

* EIGRP update packet use reliable delivery.

for Staples

• Metric - ใจค่า cost ที่ต้องห้าม - Bandwidth: lowest BW = ลักษณะต่ำสุด [ต่างกับ OSPF ที่เป็น cumulative]

- Delay: Cumulative interface delay - ลักษณะต่ำสุด

- Reliability, Load

- Config : Router(config-router)# metric weights tos k1 k2 k3 k4 k5

- Bandwidth : Router(config-if)# bandwidth kilobits bandwidth-value

- Delay - อัตราการลดเวลาของ packet หลักที่ source



Default
K1 (Bandwidth) = 1
K2 (Load) = 0
K3 (Delay) = 1
K4 (Reliability) = 0
K5 = 0

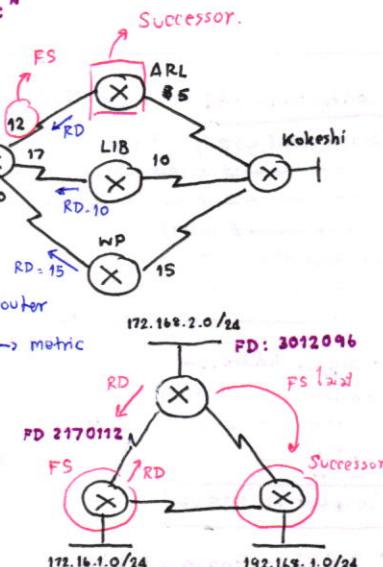
Metric Calculating

- Bandwidth ($10,000,000 / \text{bandwidth}$)
- Delay (Sum of Delay / 10) $\rightarrow (\text{Bandwidth} + \text{Delay}) \times 256 = \text{"Metric"}$

DUAL Topology Table - Term

- Successor(s): ที่ส่ง forward ไปยัง neighbour นั้น cost ต่ำกว่า

- Feasible Successor (FS) - Backup Paths
 - คือทางสำรองที่ดีกว่าในTopology Tab.
 - $\text{RD} < \text{FD}$: if True $\rightarrow \text{FS} //$
- Reported Distance (RD) - Advertised Distance
 - ที่ report บน Neighbor Router
- Feasible Distance (FD) - ณ cost ของตัวเอง \rightarrow metric
- Operator - ณ FS นั้น S อยู่ใน Topology Table
 - ต้อง update บน routing
- D 192.168.1.0/24 [90/3012096] via 192.168.10.10,
00:12:32, Serial0/0/1
- Feasible Distance
- Successor



- Verify: show ip eigrp topology
- boot Display or show (cost/RD)
 - Only Successor \rightarrow IP routing table
 - Passive State \rightarrow Stable State and available for use
 - Active State \rightarrow Recomputed by DUAL

- Successor fail, no FSS
 - DUAL \rightarrow active state, active query if neighbor for a new successor.

* Special commands.

- Redistribute (OSPF - static) -- classless redistribute connected subnets
- Redistribute (OSPF - RIP)


```
router rip
redistribute ospf process_id metric metric-no.
router ospf
redistribute rip subnets.
```
- RIP + Static


```
default-information originate.
```

