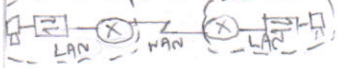
ชื่อ-สกุล นายธติกร อยู่เจริญทรัพย์ กระดาษแผ่นที่ 1 รหัสนักศึกษา 59011196

for Staples

Type of Network

- LAN : home
- WAN : LAN ที่แยกออกจากกัน



Protocols

- Application layer
  - DNS : Name System
  - BOOTP, DHCP : Host Config
  - SMTP, POP, IMAP : Email
  - FTP, TFTP : File Transfer
  - HTTP : Web
- Transport layer
  - UDP, TCP
- Internet layer (Network - Logical Addr.) <IP>
  - IP, NAT
  - ICMP : IP Support
  - OSPF, EIGRP : Routing Protocol
- Network Access layer (Data link, Physical) - Timing, sync bits - Physical addr.)
  - ARP
  - PPP
  - Ethernet
  - Interface Drivers.

LAN : type B :

for Staples

Port Address : (0 - 65,536) destination port

- well-know : (0 - 1023) ← กำหนดโดย IANA
- registered port : (1024 - 49151)
- dynamic/private port : (49152 - 65,535)

#source port → random

Logical Addresses : IPv4 < 5 class >

class A	0 - 127	0 ← High start
class B	128 - 191	10
class C	192 - 223	110
class D	224 - 239	1110
class E	240 - 247	1111

Private addr. CIDR Prefix

- class A : 10.0.0.0 /8 - 10.255.255.255
- class B : 172.16.0.0 /12 - 172.31.255.255
- class C : 192.168.0.0 /16 - 192.168.255.255

Payload

byte 1 → byte 2 → byte 3 → byte 4

Version	IP Header Length	Differentiated Services DSCP / ECN	Total Length	
Identification			Flag	Fragment Offset
Time To Live	Protocol		Header checksum	
Source IP Address				
Destination IP Address				
Option				Padding

MAC address : 48 bit (12 hex) IEEE

Message Delivery :

- Unicast MAC addr.
- Broadcast MAC addr. : เช่น DHCP, ARP (IPv4)
  destination MAC addr = FF-FF-FF-FF-FF-FF
- Multicast MAC addr. :
  มี IP addr ในช่วง 224.0.0.0 - 239.255.255.255
  dest MAC addr เริ่มต้น 01-00-5E-...

Cisco IOS : (Cisco Internetwork OS)

- shell → kernel → hardware

Mode

- User EXEC mode : view only
  limited number of basic monitoring command
- Privileged EXEC mode (enable) : Detail, Debug Test, จัดการไฟล์
- Global Configuration Mode (configure terminal) :

Limiting Access to Device Configurations.

- Banner Message
  - เป็นคำสั่งแสดงผล ที่ถูกดำเนินต่อไปตาม ทำงานอยู่ทั้งหมด
  - ค่าที่ส่งผลออกเมื่อ ทำการ login
  - ส่งผลการใช้ในการ legal notification เพราะจะแสดงถูก connected terminal
- Enable password
- Enable secret
- Console password
- VTY password
- Encrypting Password Display
  หลีกเลี่ยง show password

Function of a Router

- CPU
- OS / Cisco IOS
- Memory
  - RAM - running IOS, configuration File
    - IProuting / ARP table
    - Packet buffer
  - ROM - bootup instruction (non Volatile)
    - Basic diagnostic software
    - Limit IOS
  - NVRAM - startup configuration file
  - Flash - IOS, Other System file

หน้าที่

- detemine best path (routing table)
- Forward packet to dest.
- ใช้ static routes และ dynamic routing

Packet Forwarding Methods.

- Process switching : older packet forward
- Fast switching : common packet forward
- Cisco Expres Forwarding (CEF)
  - most recent, fast, preferred Cisco IOS packet forward

Document Network Addressing

- Device name - Interface - IP addr and subnet mask
- Default gateway

Enable IP on Host

- Statically assign IP addr. : host manually assign
- Dynamically assign IP addr. : assign by (DHCP) sever ใช้ Dynamic Host Configuration Protocol

Switching Packet between Networks.

- Router switching Func.
- Send a packet — ใช้ routing table
- Forward to next hop
- Packet Routing
- Reach to dest — ARP

Best path : "lower metric"

- Dynamic routing protocol
  - RIP ⇒ hop count
  - OSPF ⇒ cumulative bandwidth (source to dest)
  - EIGRP ⇒ bandwidth, delay, load, reliability

ถ้ามี เส้นทาง มากกว่า 1 เส้นทาง และ cost เท่ากันหมด router จะส่ง packet ออกไปทั้ง 2 เส้นทาง เท่ากัน
(AD) Administrative Distance = "trustworthiness"

Routing Table : เป็น file ที่เก็บใน RAM

- Directly connected Rotes
- Remote router
- Network or Next hop Associations

Routing Table source.

- Link local Interface : เพิ่มใน routing table เมื่อ interface is configured
- Directly connected interface : เพิ่มใน routing table เมื่อ interface is configure and active
- Static routes : เพิ่มใน routing table เมื่อ manually configured and the exit interface is active
- Dynamic routing protocol : เพิ่มเมื่อ EIGRP or OSPF ถูก implement และ networks are identified

# Router # sh ip ro
L = local, C = connect, S = static
R = RIP, M = mobile, B = BGP, D = EIGRP

result

D 10.1.1.0/24 [90/2170112] via 209.165.200.226
00:00:05 Serial0/0/0

- 10.1.1.0/24 : dest network
- 90 : AD
- 2170112 : metric to reach remote Net
- D : How the network has learn by the router
- 00:00:05 : elapsed time
- Serial0/0/0 : Interface on the router to reach the dest Net
- 209.165.200.226 : next hop

for Staples

Remote Network Routing Entries.

Dynamic Routing Protocols.

- Exterior Routing Protocols.
  - BGP
- Interior Gateway Routing Protocols.
  - RIP = Routing Information Protocol
  - OSPF = Open shortest Path First
  - EIGRP = Enhanced Interior Gateway Routing Protocol
  - IS-IS = Intermediate System-to-Intermediate System

Static Routes. Application

- ลดจำนวนการหาเส้นทาง
- สร้าง backup route

Type: standard, Default, summary, Floating static route

Router(config)# ip route dest network addr subnet-mask ip-address|exit (next-hop)

Next-Hop option:

- Next-hop route : next-hop → IP address
- Directly Connected static route : next-hop is router exit interface
- Fully specified static route : next-hop IP address และ exit interface

Default Static Route

(match any network addr. / subnet mask)

Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}

CIDR = Classless Inter-Domain Routing

[illegible] ใน internet โดยใช้ Inter Domain Routing

↳ คล้ายๆ summary IP / ไม่มี class A, B, แบ่ง subnet เท่าๆ กัน

VLSM = 1 Network มีการแบ่ง subnet mask แต่ละ subnet มีขนาดไม่เท่ากันได้

ex 192.168.20.0 /24 → /27

จะได้ 8 subnet, 30 host per subnet

Sol 11000000.10101000.00010100.000|00000

Sol1

$2^5 = 32$

$256 \div 32 = 8$ subnet

Sol2

8 subnets 000 : 111

$2^5 = 32$ → $32 - 2 = 30$ / 30 host

Floating Static Routes

- มี AD > AD ของ static route อื่น, หรือ dynamic route
- AD ของ static route สามารถเพิ่มขึ้น เพื่อให้ route เป็นที่น่าพอใจน้อยกว่า static route อื่น, หรือ route ที่เรียนรู้ผ่าน dynamic routing protocol
- จะได้ถูกใช้เมื่อ route ที่ AD ต่ำกว่า active อยู่

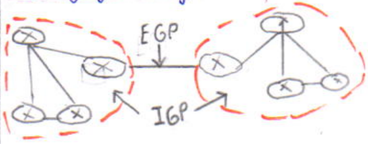
ชื่อ-สกุล นายรุจิกร . อยู่เจริญทรัพย์ กระดาษแผ่นที่ 2 รหัสนักศึกษา

(A)

Dynamic Routing Protocols

- share ข้อมูลระหว่าง router
- update table
- หา best path

* Classifying -Routing Protocol



- IGP : RIP, IGRP, EIGRP, OSPF, IS-IS
- EGP : BGP

classful : Subnet mask "same"

classless : Subnet mask "แตกต่าง"

*Convergence : กำหนดเมื่อ router ทุกตัว ได้ routing table at state of consistency

*Metric : ค่าที่ใช้ใน routing protocol เพื่อตัดสินว่า router ไหนดีกว่ากัน (best path)

ex hopcount, cost, bandwidth

- load balance : เส้นทางที่ cost เท่ากัน จะส่งไปทั้ง 2 เส้นทาง

*Administrative Distance of route (AD)

: ค่าที่เจาะจงแต่ละ router (น้อย, ดี)

Distance Vector Routing Protocols

ex : RIP, IGRP, EIGRP

ต้องรู้ 2 อย่าง : -distance to destination
-direction, traffic ที่ควรไป

หน้าที่ : -periodic update, neighbors. routing table ทั้งหมดส่ง routing-update

- เหตุที่ใช้ในการเปรียบเทียบ routing protocol ex: resource usage, time to convergence.

Network Discovery

1) Router initial start up
2) Initial Exchange of routing informa.
3) Exchange router imformation

Routing Table Maintenance

Periodic update : RIP
Bounded update : EIGRP
Triggered Update
Random Jitter

Routing Loops (unreachable)

- RIP : กำหนด infenity ที่ 16 hops.
- Holddown Timer : ไม่ต้องการเปลี่ยนข้อมูล ใน table ถ้ามี router down

- split horizon rule : router ไม่ควร advertise network ผ่าน interface จากที่ที่ update come.
- route poisioning : ใช้ในการ mask router as unreachable ใน routing update ที่ส่งไปให้ router อื่นๆ
- Split horizon with poison reserse : เมื่อส่ง update ไปยัง specific interface, กำหนด network that were learned on that interface as unreachable
- IP & TTL (time to live) : 8 bit field ใน IP header โดย limit จำนวนของ hop ที่ packet can traverse (สำรวจ) ผ่าน network ก่อนที่จะถูก discarded

RIP version 1 (AD:120)

: classful, metric = hop count, hop > 15 => unreachable, update เป็น boadcast ทุก 30 sec.

สีส้ม = V2

Data link Frame header	IP Packet header	UDP segment Header	RIP Message (512 byte, up to 25 rout

Command = 1 or 2	version = 1 2	Must be zero	header
Address family identifier (2 = IP)		must be zero	route tag
IP Address (Network Address)			Route Entry
subnet mask		Must be zero	
next hop		Must be zero	
Metric (Hops)			
Multiple route entries, up to maximum of 25			

Message :

1.) request : ส่งเมื่อ startup by each RIP enabled interface request all RIP enabled neighbors to send router table

2.) responce : message sent to requesting router containing routing table

Classful : ไม่ส่ง subnet mask ไปใน routing update

```
R1 (config) # router rip
R1 (config-router) # network 192.168.1.0
        :
debug ip rip
```

Passive interface command : หลีกเลี่ยง router ออกจาก ส่ง update ไปยัง interface

```
R1 (config) # router rip
R2 (config-router) # passive-interface
                FastEthernet 0/0
```

Automatic Summarization

- Boundary Routers. : RIP automa. summarize classful network, summarize RIP subnet จาก 1 major network ไปยัง another
- Sending RIP update : automatic summarization to reduce size of routing table

single route are used to represent multiple routes. which result in faster lookup in the routing table.

ไม่ support discontiguous network

R2 (config-router) # default-information originate

↳ propagate default routes.

เพิ่มเติม จากบทที่ (D: Dynamic, S: Static)

เปรียบเทียบ Dynamic and static routing

1.) Configuration Complexity
D: ไม่ขึ้นอยู่กับ network size
S: เพิ่มขึ้นตาม network size

2.) Required administrator knowledge
D: advanced knowledge required
S: no extra know...

3.) Topology change
D: auto adapt to Topology change
S: ต้องใช้ administrator ช่วย

4.) scalling
D: เหมาะกับ simple & complex topology
S: เหมาะกับ simple topology

5.) Security D: less, S: more security

6.) Resource usage
D: ใช้ CPU, memory, link bandwidth
S: no extra resource needed

7.) Predictability
D: route ขึ้นอยู่กับ topology ปัจจุบัน
S: route to destination เหมือนเดิมตลอด

Dynamic Routing Protocol

- Interior Gateway Protocol (IGP)
  - Distance Vector Protocol → RIPV1, IGRP, EIGRP, RIPV2
  - Linked stated Protocol { -OSPF -IS-IS
- Exterior Gateway Protocol (EGP) → BGP

AD

connected	0	Internal EIGRP	90	External EIGRP	170
static	1	IGRP	100	Internal BGP	200
EIGRP summary route	5	OSPF	110		
External BGP	20	IS-IS	115		

	RIPv1	RIPv2	IGRP	EIGRP
Speed of Convergence	slow	slow	slow	fast
Scalability-size nw.	small	small	small	small
Use of VLSM	X	✓	X	✓
Resource usage	Low	Low	Low	Medium
Implement & maintain	Simple	Simple	Simple	Complex

RIP version 2 ⑤

RIPv1 vs RIPv2

- RIPv1 :- classful distance vector routing protocol
  - :- ไม่ support discontiguous subnets, VLSM
  - :- ไม่ส่ง subnet mask ใน routing update
  - :- routing update ใช้ broadcast
- RIPv2 :- เป็น version 1
  - next hop address is include in update
  - running update are multicast
  - มี authentication ได้ (secure)

เหมือนกันทั้ง RIPv1 และ RIPv2

- timer → prevent routing loop
- มี split horizon แต่ split horizon with poison
- มี triggered update
- max hop count : 15

CIDR (Classless Inter-domain Routing)

- update include subnet mask
- support VLSM, route summarization

RIPv1 Limitation

- Loopback interface
- Null Interface
- static route and null interface
- Route redistribution : ใช้ไม่ได้ static route
- Verifying and Testing Connectivity
  ↳ sh ip interf brief, ping, traceroute

- ไม่ส่ง subnet ID update
- summarizes network at major network boundaries
- ไม่ support VLSM, CIDR

Configuring RIPv2 (Frame ตัวอย่างมีมาให้)

show ip protocol ⇒ ตรวจสอบ RIPv2

- automatically summarize route ที่ major network boundaries และ summarize route ด้วย subnet mask ในคลาส classful subnet mask

no auto-summary ใช้ auto-summary ของ v2

VLSM & CIDR

- verify RIPv2 ↘ automatic summarization turn off
- ถ้า VLSM IP addressing scheme ↗ use classless
- CIDR use supernetting

Verifying & Troubleshooting RIPv2

step : 1) check status of all link
2) check cabling
3) check IP address & subnet mask config
4) remove unneeded configuration command

examine : version (v2), Network statement, automatic summarization

authen : ป้องกัน invalid routing update, ข้อมูล routing updates are encrypted

Access Control List block all traffic

- last statement ของ ACL จะมี "implicit deny"

Standard IPv4 ACL (ดูแค่ source destination) (block IP)

- check source address
- permit/deny entry protocol suite

access-list 10 permit 192.168.30.0 0.0.0.255
(1-99) or (1300-1999) wild card

Extended ACL (ดูทั้ง source)

- check source and destination address
- permit/deny specific protocol

access-list 103 permit 192.168.30.0 0.0.0.255 any eq 80
(100-199) or (2000-2699)

Wildcard Mask in ACL

- 255.255.255.255 - subnet mask

ex ip address = 192.168.16.0
Wildcard mask = 0.0.15.255
result = 192.168.16.0 to 192.168.31.255

Guideline for ACL creation

- ใช้ ACL ที่ firewall
- config ที่ border router

The three Ps :
1) 1 ACL per protocol
2) 1 ACL per direction
3) 1 ACL per interface

Best Practice : 1) ACL security 2) descript of ACL do 3) text editor to create edit and save ACLs
4) Test ACL on dev network

Configure Standard IPv4 ACLs

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

ex R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
R1(config)# access-list 1 deny any
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in

VTY port → secure standard ACL
ssh 192.168.10.1

Configure Extended IPv4 ACLs

config เหมือน standard

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

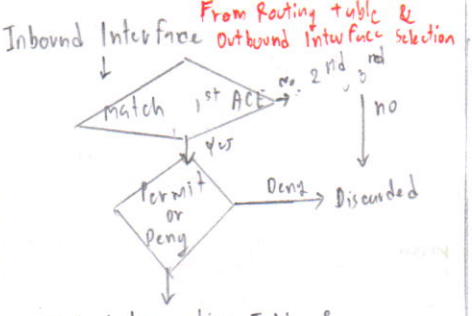
format : access-list access-list-number {deny|permit|remark} protocol source [source-wildcard] [operator operand] [port port-number or name] destination [destination-wildcard] [operator operand] [port port-number or name] [established]

ex R1(config)# ip access-list extended Browsing
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config...)# exit

Limiting Debug Output

- to verify and troubleshoot network operation
- easy to view debug

ex R1# debug ip packet 101



ชื่อ-สกุล นายรุจิกร อยู่เจริญทรัพย์ กระดาษแผ่นที่ 3 รหัสนักศึกษา 88888888

for Staples

OSPF (Popular standard based routing protocol)

Link-state Routing Protocol:
- complete map of network topology
- ใช้ link_state information เพื่อสร้าง topology map และ select best path to all destination
- = ส่วนมากใช้ใน large network
- ต้อง fast convergence
- ผู้ใช้ต้องมีความรู้ในการ implement
- ใช้ Dijkstra's algorithm refer to shortest path first (SPF)
- accumulated cost

Link-state Update step:
- Each router learn own links
- Exchange Hello packet กับ link-state router อื่นๆ
- Building the link-state Packet (LSP)
- Flooding LSP & Building Database
- Building the SPF Tree, add OSPF route to routing Table

ข้อดี: - หา shortest path
- flooding of LSP achieves faster convergence
- LSP จะส่งเมื่อ topology changed

for Staples

ข้อเสีย: - ใช้ memory เพิ่มในการรักษา link-state database and SPF tree
- คำนวณ SPF algorithm ใช้ CPU เพิ่ม

OSPF (AD: 110)

sh ip ospf neighbor
sh ip ospf database

OSPF Message

- IPv4 header Fields.

Data link Frame Header	IP Packet Header	OSPF Packet header	OSPF Packet type specific database
MAC addr.	source, dest	router ID, Area ID	0x01-Hello, 0x02-DB descrip, 0x03-LS request, 0x04-LS update, 0x05-LS Ack

Hello packet content

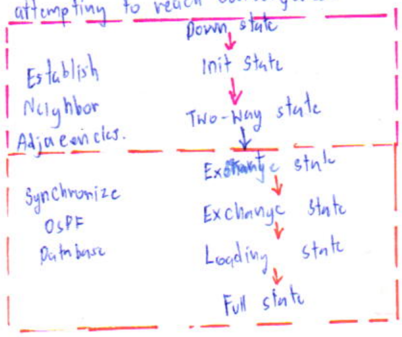
0 7/8 15/16 23/24 31

Version	Type = 1	Packet Length
Router ID		
Area ID		
Checksum	AuType	
Authentication		
Authentication		
Network Mask		
Hello Interval	Option	Router Priority
Dead Interval		
Design Router (DR)		
Backup Designated Router (BDR)		
List of Neighbor(s)		

for Staples

※ Number of adjacencie = n(n-1)/2 (n ← number of router)

OSPF initially connect:
1) สร้าง adjacency with neighbors.
2) แลกเปลี่ยน routing information
3) คำนวณ best path
4) reach convergence
5) OSPF progress through several state while attempting to reach convergence.



Configuring Single-Area OSPFv2

```
# router ospf process-id
ex R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
                  # end

R1(config)# interface loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
                  # end

ex2 R1(config)# router ospf 10
R1(config-router)# network 172.16.1.0 0.0.0.255 area0
```

OSPF cost

cost = reference bandwidth / interface bandwidth
โดยที่ ↗ = 10^8 bps, interface ส่วนมาก = 1.544 Mbps

DHCP (Dynamic Host Configuration Protocol)

provide automatic IP addressing
- subnet mask (IPv4) หรือ prefix length (IPv6)
- Default gateway address
- DNS server address

DHCP: ใช้ difference addr เพื่อ allocation method
- Manual Allocation
- Automatic Allocation
- Dynamic Allocation

DHCPv4 Message Format:

0 7/8 15/16 23/24 31

OP Code	Hardware type	Hardware address length	Hops
Transaction Identifier			
Second - 2 bytes		Flags - 2 bytes	
Client IP addr (CIADDR) - 4 byte			
Your IP addr (YIADDR) - 4			
Server IP addr (SIADDR) - 4			
Gateway IP addr (GIADDR) - 4			
Client Hardware addr (CHADDR) - 16			
Servername (SNAME) - 64			
Boot File name - 128			
DHCP option - variable			

DHCP Discover Message

Ethernet Frame	IP	UDP	DHCPDISCOVER
src MAC: DEST MAC:	IP src: ip dest:	UDP 67	CIDDR: GIDDR: Mask: CHADDR: MAC A

Configuring DHCPv4 Server

setup:
- exclude address from the pool
- set up DHCP pool name
- Configuring specific Task
- กำหนด range of addr, และ subnet mask
- ใช้คำสั่ง default-router แทน default gateway

```
R1(config)# ip dhcp exclude-address 192.168.10.1 192.168.10.4 } ช่วง
~~~~~~~~ # 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
~~~~~~~~ # end
```

verify DHCP
- sh ip dhcp binding
- sh ip dhcp server statistic
- sh running-config | section dhcp

Basic Switch Address Resolution Protocol

LAN - มี single admin ดูแลได้

design: borderless Switched = อนุญาตให้ organization ติดต่อกันทุกๆคน, ทุกที่, ทุกเวลา จะใช้เมื่อ Hierachical, Modularity, Resiliency Flexibility

Access Layer Switch Features: (A) ↷ ทดแทน
Distribution Layer switch Feature: (D) ↷ etc
Core Layer switch Feature: (C) ↷ สำนักงาน

Port security = A
VLANs = A
Fast Ethernet / Gigabit Ethernet = A, D, C
Power over Ethernet (PoE) = A
Link aggregation = A, D, C
Quality of service (QoS) = A, D, C
Layer 3 Support = D, C
High forwarding rate = D, C (very high)
Redundant component = D, C
Security policy / AC control = D

การตัดสินใจเลือก switch:
- Cost: จำนวน และ ค.เร็ว ของ interface
- port density: จำนวน port
- Power: PoE
- Reliability
- Port Speed
- Frame Buffers
- Scalability

To maximize LAN bandwidth และ performance :
- function และ placement ของ sever
- collision detection issue
- segmentation issue
- broadcast domain issue

MDF : Main Distribution Facility
IDF : Intermediate Distribution facility
VCC : Vertical cross-connect
HCC : Horizontal cross-connect

Switch Operation :
- Learning = เก็บ source MAC addr. ที่ส่งเข้ามาใน switch
- Aging = อายุของ MAC addr.
- Flooding = ส่ง Frame ออกทุก Port { unknown unicast, multicast, broadcast }
- Forwarding = ส่งออก port ที่รู้จัก
- Filtering = filter ไม่ให้ผ่าน ดูจาก Forwarding

Transparent Bridge Process - Jeff Doyle:

Receive Frame → learn source addr / refresh aging timer
↓
Is destination boadcast, multicast or unknow? — yes → Flood Packet
— no → Are the source & dest. on same interface? — yes → Filter Packet
— no → Forward unicast to correct port

Frame Forwarding :
- Store-and-Forward Switching
  - check for error (CRC)
  - ดู frame ทั้งหมด → ช้า
- Cut-Through switching
  - No FCS check
  - Fast-forward 12 byte (source, dest. MAC addr.)
  - Fragment-free 64 byte

Collision Domain :
- ทุก port ของ hub belong same collision domain
- ทุก port ของ switch is collision domain on its own

Broadcast Domain :
- ทุก port ของ switch belong same broadcast domain
- ถ้ามี >2 switch ต่อกัน broadcast will be forward to all port of all switch

Switch Boot Sequence :
- Post
- Run boot loader software
- Boot loader does low-level CPU initialization
- Boot loader initializes the flash filesystem
- Boot loader locates and load default IOS OS software image into memory and hands control of switch over IOS

Basic Switch Management.
- IP information (addr, subnet mask, gateway) is to be assigned to switch SVI (switch virtual interface)

SSH Operation : (TCP 22)
- Secure shell (SSH) : encrypted command line, เริ่มแรกใช้ใน UNIX

Switch Port Security : manually configured
- Static secure MAC addr.
switchport port-security mac-address mac-addr
- Dynamic secure MAC addr. : dynamic learned
switchport port-security mac-addr sticky
- sticky secure MAC address. : can be dynamically learned หรือ manually configured

Address Resolution Protocol
- Mapping IP to MAC addr.
- destination Outside the Local Networks.
- Removing Addr. Mapping

cmd : > arp -a

ARP request :
Dest addr = FFFF. FFFF. FFFF
OPCODE = 0x0001

ARP reply
OPCODE : 0x0002

IPv4 — classful / classless

Classless Inter-Domain Routing
- Fixed Length Subnet Masking

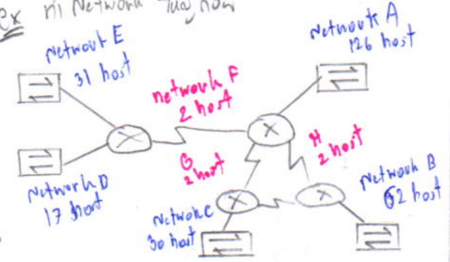
ex 192.168.1.0 /24 → /27

Sol 192.168.1.0
⋮
192.168.1.255

Sol 11..1.11..1.11..1.111 00000
เพิ่มมา 3 bit
$2^3 = 8$, ส่วน จาก 256
$256 / 8 = 32$
network ละ 32 host #

- Varible Length Subnet masking

ex หา Network ใหญ่ก่อน



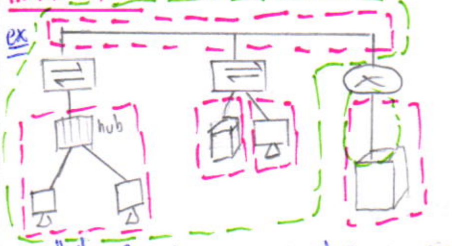
Network	Req Host	Max Host	subnetwork	Subnet mask
A	126	128-2 126	161.246.6.0-.127	.128
B	62	64-2 62	.128-.191	192
C	30	32-2 2	.7.0-.31	.224
D	17	32-2 36	.7.32-.63	.224
E	31	64-2 62	.192-.255	.192
F	2	4-2= 2	.7.64-.67	.252
G	2	4-2= 2	.7.68-.71	$\frac{256}{x} = 4$ → .252
H	2	4-2= 2	.7.72-.75	.252
I	2	4-2= 2	.7.76-.79	.252

หา Subnet ของ E

Sol ต้องแบ่ง 256 ได้ 64
$256 / 4 = 64$ ∴ $= 4 = 2^2 = 2$ bit
11..1.11..1.11..1.11000000 (192) #

เพิ่มเติม จาก บทที่

ex



Collision Domain = 5, Broadcast Domain = 2

Configure switch : ต้องเปลี่ยนชื่อ switch ก่อน

S1(config)# interface vlan 99
S1(config-if)# ip address 172.17.99.11 255.255.0.0
______# no shutdown
______# end

Default Gateway :
S1(config)# ip default-gateway 172.17.99.1
______# end

Config Static secure MAC addr. :
S1(config-if)# switchport mode access
______# switchport port-security
______# switchport port-security mac-address MAC-ADD (static) / sticky (Dynamic)

Security violation mode :

Violation Mode	Forward Traffic	Send Syslog message	Display error message	Increase Violation Counter	shut down Port
Protect	x	x	x	x	x
Restrict	x	✓	x	✓	x
shutdown	x	x	x	✓	✓

ชื่อ-สกุล นายรจิกร อยู่เจริญทรัพย์ กระดาษแผ่นที่ 4 รหัสนักศึกษา 59011196

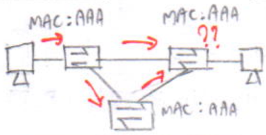
LAN Redundancy : เมื่อเกิด loop → sw ได้รับ MAC addr. ของอุปกรณ์เดียวกันเข้ามาหลายทาง sw เรียนรู้ MAC ผิด จึงทำงานผิดพลาด

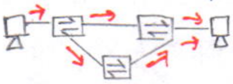
ปัญหา Layer 1 redundancy :

1.) ความไม่แน่นอนของ MAC database

2.) Broadcast storms - flood broadcast ออกทุกพอร์ต

3.) Multiple frame transmission - เครื่องปลายทางได้รับ frame ซ้ำ



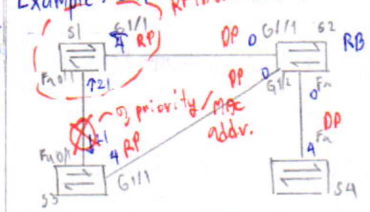


Spanning Tree Protocol : เปลี่ยนสถานะของ port หนึ่งให้เป็น blocking ไว้

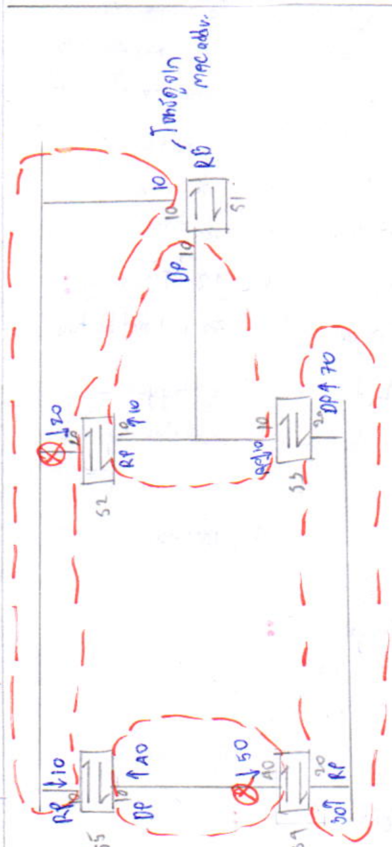
Spanning Tree algorithm :

- STP เชื่อม path ที่ block แล้วจะไม่เกิด loop
- Port is considered blocked เมื่อ user data ถูกปิดกั้น จากการเข้าหรือการออก จาก port นั้น
- Physical path still exist เพื่อ provide redundancy แต่ว่า path จะถูกปิดใช้งานเพื่อหลีกเลี่ยง loop
- ถ้า path จำเป็นต้องชดเชย สำหรับ network cable STP จะ recalculate path และ unblock port ที่จำเป็น to be active.

Example : STP RP เทียบระยะทาง 4 และ 21



S1	32764	000A00111111
S2	24577 - RB	2 ... 2
S3	32769	3 ... 3
S4	32769	4 ... 4
Priority		MAC addr



STP Operation :

*

- 1 Root Bridge / Network
- 1 Root Port / Non-Root Bridge
- 1 DP / Segment (designated port)

- Root Bridge :

Bridge Priority	Extended System ID	MAC Addr.
4 bits	12 bits	48 bits.

- ดูที่ Priority ถ้าน้อยสุด → RB
  ถ้าเท่ากัน ดูที่ MAC addr น้อยสุด

Link Speed	Cost (IEEE) (IEEE แบบใหม่)	Cost (IEEE แบบเก่า)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

Extended System ID 2 bytes 6 bytes

Bridge Priority	MAC Addr.
4 bits 12 bits	48 bits.

Bridge Priority	Extended System ID	MAC Addr

Protocol	Resource Needed	Convergence	Tree Calculation
STP	Low	Slow	All VLANs
PVST+	High	Slow	per VLANs
RSTP	Medium	fast	All VLANs
Rapid PVST+	Very high	fast	Per VLANs
MSTP	Med - high	fast	Per Instance

PVST + :

- can run independent IEEE 802.1D STP
- สำหรับแต่ละ VLAN ใน network
  Optimum load balance can result
- 1 STP สำหรับแต่ละ VLAN แลกกับการ considerable waste of CPU cycle สำหรับทุก sw ใน NW

Port State

Processes	Block	Listen	Learn	Forward	Disable
Process received BPDUs	✓	✓	✓	✓	X
Forward data frame received on interface	X	X	X	✓	X
Forward data frame switched from another interface	X	X	X	✓	X
Learn MAC addr	X	X	✓	✓	X

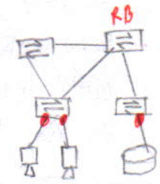
Extended System ID : เหมือนกับ Root Bridge

Rapid PVST+ :

- RSTP prevent layer 2 loop ใน sw
- RSTP run ในแต่ละ VLAN
- RSTP support new port type
- ไม่มี blocking port ใน RSTP define port state เป็น discarding, learning or forwarding
- RSTP keep same BPDU format as IEEE 802.1D

Edge Ports :

- ไม่มี sw ที่ต่อกับมัน
- เปลี่ยนแปลงทันทีและ forward ไป
- แม้ทำเหมือนกับ port config



Link Types : can determine ว่า port can immediately transition to forwarding state. Edge port / point-to-point connection แบ่งกัน สำหรับ rapid transition to forwarding

Spanning Tree Configuration :

```
S1(config) : spanning-tree VLAN 1 root primary
S2(...) : " ——————— " secondary
S3(...) : " ——————→ priority 24576
S3# show spanning-tree
S(config) : int fa 0/1
S(config-if) : spanning-tree portfast
———→ : spanning-tree bpduguard enable
```

First-Hop Redundancy Protocols :

ความสามารถของ network ในการ dynamic recovery จาก failure ของอุปกรณ์ ที่เป็น default gateway

- HSRP :
  - group of router - one active, one standby
  - virtual IP and MAC ถูก shared ระหว่าง 2 router
  - ใน group stand by
- GLBP : Gateway Load Balancing Protocol
  automatic selection และการใช้ multiple available พร้อมกัน to automatic failover ระหว่าง those gateways.

VLANs : (Virtual LAN)

- is a logical partition of layer 2
- each VLAN is broadcast domain/มี IP network ของตัวเอง
- VLANs แยกออกจากกัน ต้องต่อผ่าน router
- ไม่ถูกแบ่งโดยใช้ sw

ประโยชน์ของ VLANs :

- Improved security
- Reduce cost
- Better Performance
- Smaller Broadcast Domain
- IT Efficiency
- Management Efficiency

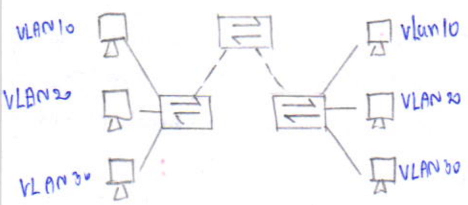
Type of VLANs :

VLAN 1 can't renamed/delete

- Native VLAN
- All ports assigned to VLAN 1 to forward data by default

VLAN Trunks.

- carries more than one VLAN
- โดยปกติ จะเชื่อมระหว่าง sw ด้วยกัน same-VLAN device can สื่อสารกันได้ ถึงแม้ว่า physically connected to different sw
- VLAN trunk is not associated (ตลอด) to any VLAN. Neither is the trunk port used to establish the trunk link



F0/1-5 are 802.1Q trunk, native VLAN 99
F0/11-17 => VLAN 10, Faculty/staff - 172.17.10.0/24
F0/18-24 => VLAN 20, Student - 172.17.20.0/24
F0/6-10 => VLAN 30, Guest - 172.17.30.0/24

Controlling Broadcast Domain with VLANs :

- limit the reach of broadcast frames.
- VLAN is broadcast domain of its own
- broadcast frame ที่ถูกส่งจาก device ใน specific VLANs จะถูก forwarded ใน VLAN นั้นเท่านั้น
- uni/multi cast frame are forwarded within originating VLAN

Tagging Ethernet Frame for VLAN Identification :

Ethernet Frame

Dst MAC	Src MAC	Type/length	Data	FCS

802.1Q Frame

Dst MAC	Src MAC	Tag	Type/Length	Data	FCS.

Ethernet Type (0x8100)	Pri	C	VLAN Identifier
2 byte	3 bit	1 bit	12 bit

- Frame tagging ใช้ส่ง multiple VLAN frame ผ่าน trunk link
- SW will tag frame to identify ว่า VLAN เป็นของอะไร
- Protocol ที่กำหนด structure ของ tagging header added to the frame
- sw will add VLAN tag to frame ก่อนที่จะ placing them into trunk link และลบ tag ก่อน forwarding frame ผ่าน non-trunk port

frame can transverse (ข้าม) any number of sw via trunk link และ still be forward within the correct VLAN at the destination

Native VLAN และ 802.1Q Tagging :

- frame ที่เป็นของ native VLAN will not be tag
- frame that is received untagged will remain and place in native VLAN when forward

ถ้าไม่มี port ที่ associated กับ native VLAN และ no other trunk link, untagged frame will be dropped

VLAN Assignment :

Creating a VLAN.

```
S1(config)# vlan vlan_id
~~~~~~~~~~~# name vlan_name
```

Assign Port To VLAN :

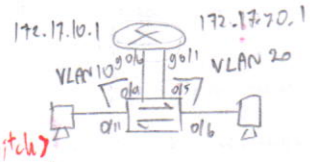
```
S1(config)# int fa0/18
S1(config-if)# switchport mod access
~~~~~~~~~~~# ~~~~~~ access vlan 20

S1# show vlan brief
```

Config Trunk Links :

```
S(config)# int fa0/1
S(config-if)# switchport mode trunk
~~~~~~~~~~~# ~~~~~~ trunk native vlan 99
```

Inter-VLAN Routing Operation :

เป็น process สำหรับ forwarding network traffic จาก one VLAN to another using router



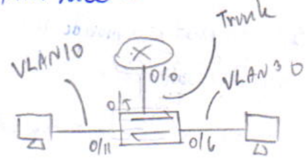
<switch>

```
S1(config)# vlan 10
S1(config-vlan)# vlan 20
~~~~~~~~~~~# int fa0/11
S1(config-if)# sw acc vlan 10
~~~~~~~~~~~# int fa0/4
~~~~~~~~~~~# sw acc vlan 10
```

<Router>

```
R1(config)# int g0/0
R1(config-if)# ip addr 172.17.10.1 255...
~~~~~~~~~~~# no sh
```

Subinterface :




```
R1(config)# int g0/0.10
R1(config-subif)# encapsulation dot1q 10
~~~~~~~~~~~# ip addr 172.17.10.1 255.255...
~~~~~~~~~~~# int g0/0.30
~~~~~~~~~~~# ip addr 172.17.30.1 255.2..
R1(config)# interface g0/0
R1(config-if)# no sh
```

ชื่อ-สกุล นายสิทธิ์ อยู่เจริญทรัพย์ กระดาษแผ่นที่ 5 รหัสนักศึกษา [illegible]

or Staples

VTP & NAT

VTP: VLAN Trunking Protocol

VTP เป็น message protocol ที่ใช้ trunk frame ในการจัดการ ทั้งการเพิ่ม, การลบ และการเปลี่ยนชื่อของ VLAN บน single domain โดยจะส่งผ่าน trunk link ไปยังอุปกรณ์อื่นๆ

* ควรกำหนด VTP ก่อนสร้าง VLAN

VTP: อนุญาตให้ VLAN configuration เพื่อการ maintain ภายใน administrative domain

ใน Cisco switch, VTP จะทำงานและมีการตั้งค่าเริ่มต้นไว้แล้ว

VTP Operation: VTP advertisements จะถูกส่งออกทาง trunk connection ทุกทาง

- เลข 32 bit → ชี้ให้เห็น the particular revision ของ VTP Configuration
- เลข Configuration revision มีตั้งแต่ 0 ถึง 4,294,927,295 และวนกลับมา 0
- VTP แต่ละตัวจะ track revision number ของตนเอง โดย VTP packet ประกอบด้วยเลข VTP conf ของผู้ส่ง
- โดยเลขเป็นการบอกว่า version ไหนใหม่กว่ากัน
- ถ้า switch ได้รับ VTP advertisement ผ่านทาง trunk link มันจะทำการ inherit VTP domain name และ Configuration revision num.
- ถ้ามี configuration revision number น้อยกว่า (ver. เก่า) จะ ignores.

Feature	Sever	Client	Transparent
Source VTP Message	/	/	×
Listen to VTP Mesi.	/	/	×
Create VLAN	/	×	/
Remember VLAN	/	×	/

- VTP servers สามารถสร้าง, แก้ไข, ลบ VLAN และทำการบันทึก VLAN configuration info ใน Catalyst NVRAM และส่ง VTP message ออกทาง all trunk ports.
- VTP Client ไม่สามารถสร้าง, แก้ไข, ลบ VLAN หน้าที่หลักของ VTP Client คือ process VLAN change และส่ง VTP message ออกทุก all trunk port
  - โดย VTP Client จะ maintain full list of VLAN ใน VTP domain แต่จะไม่เก็บ info ใน NVRAM
  - การเปลี่ยนแปลงต่างๆ ต้องได้รับจาก VTP Sever
- VTP transparent mode:
  - forward VTP advertisement แต่จะ ignore information contained ใน message
  - transparent switch จะไม่ได้รับการ modify database เมื่อได้รับการ update

VTP Configuration

- global Configulation mode
- VLAN Configulation mode: ใช้งานได้โดยคำสั่ง vlan database ใน privileged EXEC command

1.) กำหนด Version Number
2.) Choose the domain
3.) Choose the VTP mode
4.) Password protect the domain

(VLAN configulation mode)

1.) กำหนด Version

```
sw# vlan database
sw (vlan) # vtp v2-mode
```

มี 2 version โดย version 1 และ 2 ไม่เข้ากันต่อกัน ทำงานแยกกัน โดย version 2 รองรับ Token Ring VLANs.

2.) กำหนด Domain & Password

```
sw (vlan) # vtp domain cisco
sw (vlan) # vtp password mypass
```

เมื่อเพิ่ม password จะเป็นการจัดการ domain ใน secure mode, same password ต้อง config ทุก switch ใน management domain เพื่อให้ secure mode

3.) กำหนด VTP mode

```
sw (vlan) # vtp sever
```

— การเพิ่ม switch ไปยัง VTP Domain ที่มีอยู่แล้ว

1. Clear the conf
2. Clear VTP file
3. Power cycle the switch
4. conf VTP mod and domain
5. password protect domain

* ใช้การเพิ่มเครื่อง เพื่อเพิ่ม new sw into an existing domain

```
delete vlan.dat
erase startup-config
```

VTP Pruning: เพิ่ม network bandwidth และ use by ลดความไม่จำเป็นของการ flooding of traffic เช่น broadcast, multicast, unknow และ flooded unicast packet, ซึ่งโดยปกติ VTP pruning จะ disabled ไว้

NAT

NAT Characteristics:

IPv4 Private Address Space:

- Network private addr. อยู่ภายใต้ RFC 1918 โดยออกแบบเพื่อใช้ภายในองค์กรหรือ site เท่านั้น
- Private addr are not route by Internet router
- NAT เป็น process ในการ translation

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

- NAT มีอยู่ด้วยกันหลายประเภท addr ;
  - Inside local addr.
  - Inside global addr.
  - Outside local addr.
  - Outside global addr.

Static NAT

- uses one-to-one mapping ของ local และ global address
- * static NAT จะมีประโยชน์มาก เมื่อ servers hosted in the inside network
- network admin can SSH to a server in the inside network.

Dynamic NAT

- ใช้ pool ของ public addr. และ assign them on first-come, first-served
- เมื่อ inside device request access to an outside network → dynamic NAT assign available public IPv4 addr. from pool

or Staples

or Staples

PAT (Port Addr. Translation)

- PAT map multiple private IPv4 addr. to single public IPv4 addr. or a few addr.
- PAT ใช้การจับคู่ระหว่าง source port และ source IP addr. to keep track of what traffic belong to what internal client
- also known as NAT overhead
- validate the incoming packet were requested โดยจะเพิ่ม a degree of security to the session

NAT vs PAT

- NAT translate IPv4 addr on a 1:1
- PAT modifies both the addr. and port num
- NAT forwards incoming packet to their inside destination
- PAT มี public exposed IPv4 addr น้อย
- PAT สามารถ translate protocol ที่ไม่ใช้ port number ได้

Pros & Cons of NAT

Pros:
- Converse the legally registered addr. scheme
- Increase the flexibility of connection to the public network
- Provide consistency for internal network addr. schemes.
- Provide network security

Cons.
- Performance (เรื่อง Time) degraded
- End to end func' is degraded
- ——— IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connection can be disrupted

EIGRP (Class, Distance Vector Routing Protocol)

Characteristics.

feature: 1.) Diffusing Update Algorithm (Dual) (ตัวกระจาย)

2.) Establishing Neighbor Adjacencies

3.) Reliable Transport Protocol

4.) Partial and Bounded updates

5.) Equal and Unequal Cost load balance

- Eigrp ใช้ protocol-dependent moudule (PDM) เพื่อ support different protocol

PDM
- maintain eigrp neighbor และ topology table
- คำนวณ metric using DUAL
- เชื่อมต่อ DUAL และ routing table
- กำหนด filtering and access list
- ทำ redistribution กับ other routing protocol

RTP คือ eigrp Transport layer protocol ที่ใช้ส่งเพื่อการส่งและรับของ eigrp packet

EIGRP support authentication and is recommended

- IP EIGRP ขึ้นอยู่กับ 5 type of packet เพื่อ maintain its various table และสร้าง complex relationship กับ neighbor router

1.) Hello
2.) Update
3.) Acknowledgement
4.) Query
5.) Reply

1. Hello packet ใช้เพื่อ discover และ adjacencies with neighbors.
   - always ส่ง unreliably
2.) Update packet ใช้เผยแพร่ routing information when topology change
   - unicast to router ที่ขอ
   - require ack.
3.) Ack packet = "data less"
4,5) Query/Reply packet : used by DUAL when searching for network
   - ร้องขอ ack
   - query = multicast/unicast
   - reply = unicast

Characteristic

- eigrp frame ปลายทาง multicast addr.
  01-00-5E-00-00-0A
- IP packet header ปลายทาง dest IP addr. 224.0.0.10 (protocol 88)
- data portion
  - Packet Header
  - Type/length/Value

- EIGRP for IPv6 is encapsulated ใน IPv6 header multicast addr.

FF02::A

Implement

An Autonomous System (AS) คือ collection ของ network under control of a single authority

- AS number แจกเปลี่ยน route ระหว่าง AS
- AS number จัดการโดย IANA และกำหนดโดย RIRs to ISPs, Internet Backbone provider
- AS num = 16 bit (0-65535) (2007 now 32 bit (>4 ล้าน))

router(config) router eigrp ID

router ใช้ 3 เหตุการณ์ เพื่อกำหนด router ID

1.) ใช้ค่าใน eigrp router_id

2.) ถ้าไม่มีการกำหนด router ID จะเลือก highest IPv4 addr of loopback interface

3.) ถ้าไม่มี loopback Interface จะเลือกจาก highest active IPv4 addr ของ Physical Interface

- EIGRP auto convert a subnet mask to wildcard mask
- Passive Interface แจ้งเลิก EIGRP update out a specified router interf

ชื่อ-สกุล [illegible] กระดาษแผ่นที่ 6 รหัสนักศึกษา

Operation

: eigrp use a composite metric which can base on the following

packet travers route:
1.) Bandwidth — K1
2.) Delay — K3
3.) Reliability — K5
4.) Load — K4

→ Reliability of the Interface as a fraction of 255.

Media	Delay in sec
Gigabit Ethernet	10
Fast Ethernet	100
FDDI	100
16M Token Ring	630
Ethernet	1,000
T1 Serial Default	20000
DS0 (64 kbps)	20000
1024 kbps	20,000
56 kbps.	20000

- กำหนด EIGRP

1.) กำหนด link ของ slowest bandwidth and use that value to calc bandwidth (10^7/bandwidth)

(Bandwidth + Delay) * 256 = Metric

2.) กำหนด delay value สำหรับ each out going interface on the way to dest and add the delay value and divide by 10 (sum of delay / 10)

3.) This composite metric produces a 24-bit value which EIGRP multiple with 256

$$\left[(10^7/\text{bandwidth}) + \frac{(\text{sum of delay})}{10} \right] * 256 = \text{metric}$$

DUAL : term:

- successor
- Feasible Success (FS)
- Reported Distance (RD)
- Feasible Distance (FD)

- The decision process for route compute is done by DUAL Finite state Machine (FSM)

โดย DUAL FSM track all route และใช้ EIGRP metric to select efficient, ... etc.

1.) Successor is router เพื่อนบ้าน ที่มีค่า cost ไปยัง dest น้อยสุด

2.) FD คือ metric ค่าน้อยสุด ที่ไปยัง dest network

3.) FS คือ neighbor with loop-free backup path to the same network as the successor

IPv6

IPv6 vs IPv4
- has large 128-bit addr space
- 340 undecillion addr.
- solve limitation with IPv4
- addr. auto configuration

Why IPv6
- Internet of Thing
- Issue with NAT
- Rapidly increasing Internet population
- Depletion of IPv4

มี 128 bit ทุกๆ 4 bit จะแทนด้วย single hexadecimal digit

IPv6 addr. Type

- Unicast — Global / link-local / Unique Local
- multicast
- Anycast

64 bit	64 bit
Prefix	Interface ID