ชื่อ-สกุล น.ส.เพชาย พิรานนท์ กระดาษแผ่นที่ 1 รหัสนักศึกษา 88888888

for Staples

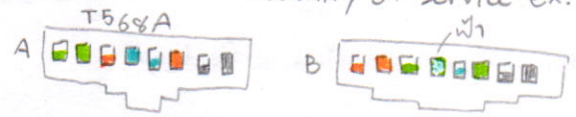
CHAP1: Network Overview

- NW devices → end devices → ไม่มี device อื่นหลังจากมัน
  - intermediary devices
- NW diagrams → ดูว่า NW เชื่อมต่อยังไง
  - physical NW diagram → อะไรอยู่ห้องไหน
  - logical diagram → ต่อ device กับ NW ไหน
- NW protocol → ข้อกำหนดมาตรฐานที่ใช้เพื่อสื่อสารระหว่าง computer
  - ex. ARP ใช้หา MAC addr จาก IP addr
  - NW addr มี 3 ประเภทคือ IP / MAC / port address
- Components of a NW → end devices
  - intermediary devices → NW access devices
    - Internetworking devices
    - security devices
  - NW media → wireless
    - copper → UTP, STP, coaxial
    - fiber optic
- Reliable NW → fault tolerance = redundance ex. หากเส้นหลักใช้ไม่ได้ก็ยังมีเส้นสำรองมารองรับ
  - scalability → เพิ่มการใช้งานได้โดยไม่กระทบ user เดิม
  - security → จำกัดได้ว่าใครเข้าถึงส่วนไหน
  - Quality of service ex. steaming ต้องใช้ quality สูงกว่า email

Application
Presentation PDU
Session → data
Transport → segment
Network → packet
Datalink → frame
Physical → bits

สาย cross
อุปกรณ์เหมือนกัน
PC ↔ router
sw ↔ hub

for Staples



Straight-Through cable → BB
crossover cable → AB

CHAP2: Basic Router Configuration

Ports → 0-123 → The internet assigned numbers authority (IANA) → well-known port
↳ destination port
→ 1024-49151 → registered port numbers
→ 49,152-65,535 → dynamic or private port number

IP class	high order bits	num of bit NW addr
A	0	8
B	10	16
C	110	24
D	1110	28

→ multicast
ตัวสุดท้ายแต่ละ NW คือ broadcast NW / ตัวแรกคือ NW ID
255.255.255.255 คือ broadcast address
E คือ experimental
IP มี 32 bits (IPv4)

private addressing → เอามา reuse ใช้งานได้ ≠ public IP → IP ที่อยู่บนโลกของ internet
↳ ex มี 1 IP อยากใช้หลายเครื่อง

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

Primary mode { user → router
Privileged → router# → enable mode

Global configulation mode
↳ router(config)#
submodes
router(config-if)#

MAC address → 12 hexadecimal digits
↳ broadcast MAC address = FF-FF-FF-FF-FF-FF
↳ multicast → MAC addr begins with 01-00-5E

Router & SW Boot Sequence
- POST (power on self test) → check HW
- run boot loader SW
- boot loader does low-level CPU initialization
- boot loader initializes the flash filesystem → ในสลอตข้อมูลมาไว้บน RAM
- boot loader locates and loads a default IOS (image) into memory and hands control of the switch over to the IOS

for Staples

Getting Basic

1. hostnames → configuring hostname
2. Limiting access to device configurations
   - → banner msg
   - → securing device access – enable password / secret, console passw, VTY (telnet) passw, encrypting psw display
3. addressing devices
   - → select an itf to configure
   - → set the IP address of an interface
4. verifying connectivity
5. saving configurations

CHAP3: Static routing & Dynamic Routing Protocol

R1# show ip route

Router components

- CPU
- RAM → contains the running copy of config file, stores the routing table
  - → vollatile
- ROM → stores the router's bootstrap, diagnostic SW when router is powerup → non-vollatile
- NVRAM → stores startup configuration
- Flash memory → contains OS (cisco IOS)
- Interfaces → serial, ethernet/fast ethernet, management interfaces

Routers choose best paths [determine the best path to send packets, forward packets toward their destination

Packet forwarding methods
- process switching → all process in CPU
- fast switching → some process in CPU, use fast-switching cache to store next hop info
- Cisco Express forwarding → all mechanism → fastest

Default Gateway → first / last usable host

• Path determination
- Best Path: lowest metric
  - └ dynamic routing protocols use
    - RIP → hop count
    - Open Shortest Path First → cumulative BW
- Load Balancing → ใช้ทุกเส้นทางให้ balance กัน
- administrative Distance → ยิ่งใกล้ (น้อย) ยิ่งน่าเชื่อถือ

D 10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, serial0/0/0

dest NW — ad — จำนวน hop — next hop addr — ต้องมีอย่างน้อย 1 อัน

- C → Directly connected
- L → Link Local

Static routing
- เร็ว → ไม่ต้องคำนวณเส้นทาง → ประหยัด resource ในการ process
- รู้ทิศทางแน่นอน → security
- เปลี่ยนเส้นทางไม่ได้, scalability ลำบาก
- Standard Static route → route ไป 1 NW ใช้ 1 cmd
- default Static route → ถ้าไม่ match ให้ไป default
- summary static route → รวมเมื่อไปทางเดียวกัน
- floating static route → ทำเป็น backup

Router(config)#ip route networkaddr subnetmask {ipaddr | exititf} → iproute cmd

Router(config)#ip route 0.0.0.0 0.0.0.0 {ipaddr | exititf} → default static route

Static Routing CIDR → ยกเลิกอันเก่าทั้งหมดแล้วรวมเป็นอันเดียว

CHAP4: Distance Vector Routing Protocols RIP v.1

- Dynamic Routing Protocol
  - function
    - Dynamically share info between routers
    - Automatically update routing table when topology change
    - Determine best path
  - purpose
    - Discover remote NW, choosing the best path for destination
    - Maintaining up-to-date routing info
    - Find new best path if current path is no longer available
  - component → algorithm & routing protocol message
- Classifying Routing Protocol

Dynamic Routing Protocol
- Interior Gateway Protocol (IGP)
  - Distance Vector Protocols
    - RIP → RIP v.2
    - IGRP → EIGRP
  - Link-State Protocols
    - OSPF
    - IS-IS
- Exterior Gateway Protocol (EGP)
  - BGP

  - IGP
    - Distance vector → periodic updates, router are advertised as vector of distance & direction
    - Link state → not periodic, complete view of NW topology is created
  - Classifying Routing Protocols
    - Classful routing protocols → do not send subnet mask in routing update → NW ที่ mask เท่ากัน (จำนวน)
    - Classless routing protocols → do send subnet mask in routing update → NW size ไม่เท่ากัน
  - Convergence → เป็นเมื่อทุก router รู้ว่ามี NW เปลี่ยน → state of consistency
- Routing Protocols Metrics
  - Metric → ค่าที่ routing protocol เอาไว้ตัดสินใจว่า routes ไหนดีกว่า
  - Load balance → เลือกได้มากกว่า 1 เส้นทาง
- Distance Vector Routing Protocols
  - characteristic of distance vector protocol
    - periodic updates
    - neighbors
    - broadcast updates → 255.255.255.255
    - entire routing table is included with routing update
  - Routing protocol characteristics
    - Criteria used to compare routing protocols includes 1) time to convergence 2) scalability 3) resource usage 4) implementation & maintenance

class A:	NW	H	H	H
	1.0.0.0 - 126.255.255.255			
class B:	NW	NW	H	H
	128.0.0.0 - 191.255.255.255			
class C:	NW	NW	NW	H
	192.0.0.0 - 223.255.255.255			

- NW discovery → 1) cold start 2) initial exchange routing info → เพิ่ม hop count 3) exchange of routing info
- Routing Table maintainance
  - Periodic update → defalt(30), invalid(180), holddown(180), flush(240) → ของ RIP
- Routing Loops
  - set maximum → 16 hops
  - holddown timers
  - split horizon rule → ไม่ส่ง NW กลับไปทาง intf ที่ได้รับมา
  - route poisoning → down แล้ว set เป็น unreachable + ส่ง poison ให้ router อื่น
  - split horizon with poison reverse → ส่งตัวที่ down ให้ intf ที่ได้รับมาด้วย
  - IP & TTL → packet ตัวนอยู่จะหายไปเมื่อ TTL = 0
- RIP version 1
  - class full, metric = hop count, hop count > 15 is unreachable, update every 30 sec
  - request msg
    - sent out on start up by each RIP enable intf
    - request all RIP enabled neighbors to send routing table
  - respond msg - msg send to requesting router containing routing table
  - default AD is "120"
- Basic RIPv1 Configuration

```
R1(config)# router rip
R1(config-router)#network 192.168.1.0
R1(config-router)# network 192.168.2.0
```

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

  - passive interface → prevent a router from sending updates through an interface
- Automatic summarization
  - ถ้า routing update แล้ว intf ที่ได้รับเป็น NW เดียวกัน → ใช้ subnet mask
  - ถ้า routing update แล้ว intf ที่ได้รับเป็นคนละ NW → ใช้ classful subnet mask
  - ลดขนาด routing table แต่ใช้กับ discontiguous ไม่ได้ (NW เดียวกันที่ไม่อยู่ติดกัน)
- Default route & RIPv.1

```
R2(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/1
```

CHAP5: RIP version 2 Access Control Lists

- RIP version 2
  - classless distance vector routing Protocol → support VLSM & route summarization
  - next hop address is included in updates
  - routing updates are ~~broadcast~~ multicast
  - the use of authentication is an option
- Configuraing RIP v.2
  - ▸ message formats

bit 0	7 | 8	15 | 16	23 | 24	31	
command = 1 or 2	version = 1, = 2	Must be zero			v 1
Route Entry: Address family identifier (2 = IP)		Must be zero	Route Tag		v 2
IP address (Network Address)					
Must be zero	Subnet Mask				
Must be zero	Next hop				
Metric (Hops)					
Multiple Route Entries, up to a maximum of 25					

  - ▸ disseminate a static route from one router to another

```
R2(config-router)# redistribute static
R1# show ip protocols → check version
R1(config)# router rip
R1(config-router)# version 2
```

- VLSM & CIDR → when using RIP v2 with auto-summary turned off
  - NW use VLSM IP when use classless routing protocol
  - CIDR uses supernetting (bunch of continuous classful NW that is addressed as a single NW
- Access control List
  - the last statement of ACL is implicit deny
  - ▸ Standard ACLs - check source address (1 to 99) and (1300 and 1999)

    close to dest - permits or denies entire protocol suit

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

  - ▸ Extended ACLs - check source and destination address (100 to 199) and (2000 to 2699)

    close to source - permits or denies specific protocols

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

- Wildcard Mask in ACL → ต้องรู้จักเอาไปคำนวณ เช่น 192.168.1.65 0.0.0.62
  - host: 192.168.10.10 0.0.0.0
  - any: 192.168.10.10 255.255.255.255

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255 | 192.168.10.10 0.0.0.0
R1(config)# access-list 1 permit any                      | host 192.168.10.10
R1(config)# interface g0/0
R1(config-if)# ip access-group 1 in
R1# show access-lists / R1# show running-config | include access-list 1
```

- Structure of an Extended IPv4 ACL
  - ▸ Extened ACLs can filter on - Source address, Destination address, Protocol, Port numbers

```
R1(config)# access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23      > เขียนอันเดียวกัน
R1(config)# access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet  >
```

  - ▸ Filtering Traffic with Extened ACLs → มี NW, wildcard 2 ชุด

```
R1(config)# access-list 101 permit ip any any
```

  - ▸ Creating Named Extended ACLs

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
```

CHAP6: OSPF & DHCP

- Link-State Routing Protocol
  - like having a complete map of the NW topology
  - uses the link-state info to create a topology map and to select the best path to all dest NW
  - best in 1) The NW design is hierarchical, large NW 2) fast convergence 3) admin เก่ง
  - use Digkstra's algorithm to calcucate best path route → accumulated costs along each path to determine the total cost of a route
  - ▸ Link state update
    - Link & Link state → each router learns about it's own links
    - Say Hello → exchanging Hello packets with other link-state routers
    - Building the Link-State Packet (LSP)
    - Flooding the LSP & Building the Link-State DB
    - Building the SPF Tree & Adding OSPF Routes to the Routing Table ; SPF=shortest path first
  - ▸ ข้อดี - แต่ละ router สร้าง topology map มาเอง เพื่อหา shortest path
    - immediate flooding of LSPs achieves faster convergence
    - LSPs ส่งเฉพาะเมื่อ topology มีการเปลี่ยนแปลง และ contain only the info regarding that chang
    - Hierarchical design when implements multiple areas
  - ▸ ข้อด้อย - ใช้ memory เก็บ link-state DB & SPF tree
    - Calculating the SPF algorithm ต้องใช้ CPU
    - ตอนเริ่มส่งใช้ BW เยอะ
  - แบ่ง area แล้วจะใช้ CPU น้อยลง เพราะแต่ละ area มี border router ตัวเดียว
  - AD: OSPF = 110, RIP = 120
- OSPF
  - ▸ OSPF 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 message

Data Link Frame Header	IP Packet Header	OSPF Packet Header	OSPF Packet Type - Specific DB

1) Hello → discovers neighbors and builds adjacencies between them
2) Database Description (DBD) → check for DB synchronization between routers
3) Link-State Request (LSR) → requests specific link-state records from router to router
4) Link-state Update (LSU) → sends specifically requested link-state records
5) Link-state Acknowledgement (LSAs) → Ack the other packet types

  - ▸ OSPF operation
    1) create adjacencies with neighbors
    2) exchange routing info
    3) calculate the best ~~path~~ routes
    4) reach convergence
    5) OSPF progresses through several states while attemping to reach convergence

    - downstate, init state, Two-way state → establish Neighbor adjacencies
    - exstart state, exchange state, loading state → synchronize OSPF DB
    - full state
  - ▸ DR and BDR

    number of adjacencies = $n(n-1)/2$; n = number of router

    DR, BDR เก็บ DB แล้ว router แต่ละตัวจะส่ง LSP ให้ DR router ที่เหลือ
- Configuring Single-Area OSPF v2

  router ospf process-id

  R1(config)# router ospf 10

  R1(config-router)# router-id 1.1.1.1 / R1(config-router)# network 172.16.3.0 0.0.0.3 area0

  R1# clear ip ospf process
- OSPF cost

  cost = reference bandwidth / interface bandwidth ; default (reference) BW = 10^8

  serial (1.544 Mbps) cost = 64, serial (64 kbps) cost = 1562

  ~~default~~ R1# show ip ospf neighbor

- DHCP → dynamic host configuration protocol
  provides automatic IP addressing, available for both IPv4 and IPv6
  - manual allocation
  - automatic allocation
  - dynamic allocation

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9 (เว้นแต่ 1-9)
R1(config)# ip dhcp pool LAN-POOL-1
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config-c
R1(dchp-config)# network 192.168.10.0 255.255.255.0
R1(dchp-config)# default-router 192.168.10.1
R1(dchp-config)# end
R1(config)# no service dhcp
```

ชื่อ-สกุล นายสิงหพงษ์ พีรานนท์ กระดาษแผ่นที่ 4 รหัสนักศึกษา 6908808

for Staples

CHAP 7: BASIC SWITCH ADDRESS RESOLUTION PROTOCOL

- LAN Design → Access Layer (VLAN) > Distribution Layer (access control list) > Core Layer } SW หมดเลย
  - Enterprise servers → Main Distribution Facility (MDF)
  - Workgroup servers → Intermediate Distribution Facility (IDF)
- The switch environment
  - SW operation → learning, aging, flooding, forwarding, filtering
  - SW forwarding methods → Store-and-forward switching → อ่านเต็ม frame แล้ว check CRC
    - Cut-through switching → ดูแค่ S,D addr ของ frame (12 bytes แรก)
      - fast-forward: 12 bytes, fragment-free: 64 bytes
- Switching Domains
  - Collision Domains → แบ่งโดยอุปกรณ์ layer 2 → 1 port is 1 domain
  - Broadcast Domains → ส่ง broadcast ไป แล้วใครได้รับบ้าง → ทุก port ของ SW คือ broadcast dm เดียวกัน
- Switching Port Security
  - Static secure MAC → switchport port-security mac-address mac-address
  - Dynamic secure MAC → switchport port-security mac-address sticky → record frame ที่วิ่งเข้ามาก่อน

swcconfig-if)# SW mo ac

SW ~~mo~~ port-security

switch port port-security → [protect / restrict / shutdown]

→ maximum number

CHAP 8: ~~STP~~ LAN Redundancy & SPANNING TREE PROTOCOL

- Layer 1 Redundancy
  - MAC database instability → MAC โดนเปลี่ยนไปมา → เกิดเมื่อ PC ส่ง broadcast
  - Broadcast Storm → เกิด loop ใน layer 2 เมื่อ PC ส่ง broadcast → TTL ไม่ลดเพราะไม่ผ่าน router
  - Multiple Frame Transmissions → PC ส่ง unicast มา แล้วปลายทางได้รับ frame ซ้ำ
- Spanning Tree Algorithm
  - ① 1RB/NW ② 1 RP / 1 non-RB ③ 1DP/segment
  - Root Bridge → ดู bridge ID (Priority + MAC addr) ที่น้อยที่สุด
  - Path cost → ลาก BPDU ดู RPcost > Bridge Identifier > Port identifier (ของ sender)
  - Extended System ID → ทำ spanning tree per VLAN

Bridge Priority (4 bits) extended System ID (12 bits) MAC address (6 bytes)

- PVST+ → แต่ละ VLAN มี root แยกกัน
- Rapid PVST+ → เปลี่ยน block port เป็น alternate port (ยังรับข้อมูลได้บางส่วน)
  - ใช้ field version 2, ใส่เอา port fast มาคิด STP, link type เป็น point to point
- Spanning Tree configuration
  - S1(config)# spanning-tree VLAN 1 root primary
  - S1(config)# spanning-tree VLAN 1 priority 24576 → เพิ่ม priority เยอะกันไม่ให้เป็น root
  - S1(config)# spanning-tree VLAN 1

CHAP10 (contine)

PAT: Single Address

access-list number permit source
ip nat inside source list number interface num overload
interface num
ip nat inside
interface num
ip nat outside

PAT: Address Pool

ip nat pool name st_ip end-ip {netmask | prefix-len}
access-list num permit source
ip nat inside source list num pool name overload

→ copy

CHAP7 (continue)

Access layer → port security, VLANs, Fa/G, Power over Ethernet (PoE), link aggregation, QoS
Distribute Layer → layer3 support, High Forwarding rate, G/10G, Redundant components, security policies / access control list, link aggregation, QoS
Core Layer → Layer 3 support, very high forwarding rate, G/10G, Redundant components, link aggr, QoS

for Staples

for Staples

CHAP9: VLANs & INTER VLAN

VLAN is a logical partition of layer 2 NW

- Benefit of VLAN
  - Improve security
  - Reduce cost
  - Better Performance
  - Smaller Broadcast Domains
  - IT Efficiency
  - Management Efficiency
- VLAN Trunks → carries more than one VLAN → IEEE802.1q → เพิ่มส่วน tag ใส่ใน frame
- VLAN Assignment - configuration เก็บใน flash → vlan.dat (ไฟล์ชื่อได้) → normal VLAN
  - 1-1005 → normal range / 1006-4096 → extended range
  - configuration เก็บใน running-config → NVRAM
  - VTP ใช้ learn extended VLAN

```
S1(config)# vlan 1
S1(config-vlan)# name NWLab
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 1
```

```
S1(config)#interface fa0/2
S1(config-if)# switchport mode trunk
S1(config-if)#switchport trunk vlan 1
```

- Inter VLAN

```
R1(config)# interface fa0/0.10
R1(config-subif)# encapsulation dot1q 10
                  # ip address 192.168.1.254 255.255.255.0
R1(config)# int fa0/0
R1(config-if)# no shutdown
```

CHAP 10: VTP & NAT

- VLAN Trunking Protocol → manage the addition, deletion, renaming of VLANs on a single domain
  - *before creating VLANs must first set up a VTP management domain

Feature	Server	Client	Transparent
Source VTP Messages	✓	✓	X
Listen to VTP Messages	✓	✓	X
Create VLANs	✓	X	✓*
Remember VLANs	✓	X	✓*

→ การผ่านของ VTP

* คำเฉพาะตัวสัน ไม่เกี่ยวกับ domain

- VTP configuration → global mode / VLAN mode
  - determine the version number > choose domain > choose VTP mode > password protect domain

```
SW(config)#vtp version 2
SW(config)# vtp domain cisco
SW(config)# vtp password class
SW(config)# vtp mode server

SW # show vtp status
```

```
SW# vlan database
SW(vlan)# vtp v2-mode
SW(vlan)# vtp domain cisco
SW(vlan)# vtp password class
SW(vlan)# vtp server
```

- VTP Pruning → remove VLAN ที่ไม่ได้ใช้งาน

```
SW(vlan)# vtp pruning
SW(config)#int fa0/3
SW(config-if)# switchport trunk pruning vlan remove 20
```

- NAT (Network address translation) → between private & public IP
  - Stub NW: มีทางออกทางเดียว
  - A: 10.0.0.0/8, B: 172.16.0.0/12, C: 192.168.0.0/16 → private IP
  - 4 types of address → Inside local, Inside global, Outside Local, Outside global
  - Static NAT → assign เอง, ใช้ access ตรงๆ มีอย่างเรา, one-to-one: ใช้ real IP เท่า IP ที่ต้องการ
  - Dynamic NAT → มี pool ของ global per real IP → many to one
  - Port Address Translation NAT (PAT) → มี port เพิ่มเข้ามา ex. 206.x.x.x:11

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)# int S0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config)# int S0/0/1
R2(config-if)# ip address 209.165.200.225 255.255.255.224
R2(config-if)# ip nat outside
Static!!
```

```
# ip nat pool name st-ip end-ip
  {netmask | prefix-lenght}
# access-list number permit source
# ip nat inside source list number
  pool name
# int number
# ip nat inside
# int number
# ip nat outside   Dynamic!
```

CHAP11: EIGRP + IPv6 & Routing

EIGRP

- EIGRP Characteristics → EIGRP was created as a classless v. of IGRP
  - use DUAL as routing algorithm → guarantees loop free and backup path
  - establish neighbor adjacencies → direct connect EIGRP routers
  - Reliable Transport Protocol
  - Partial and ~~Balance~~ Bounded updates → update เฉพาะส่วนที่เปลี่ยน
  - Equal and Unequal ~~load~~ cost Load Balancing

EIGRP multicast for
IPv4 → 224.0.0.10
IPv6 → FF02::A

- uses protocol-dependent modules (PDMs) to support different protocols
- PDMs [maintaining EIGRP neighbor and topology table → แต่ละ protocol แยก table กัน
  computing the metric using DUAL
- RTP → reliable (update, query, reply) unreliable (hello, ACK) packets
  ↳not require ACK ↳ EIGRP Packet Type
- supports authentication

▸ EIGRP messages
- destination multicast: 01-00-5E-00-00-0A (EIGRP frame)
- IP packet header dest: 224.0.0.10 → protocol 88

▸ Configure EIGRP for IPv4
- An Autonomous System (AS) is a collection of networks under the control of a single authori
- AS number ใช้เพื่อ exchange routes between AS (16 bits → 0-65535) แต่ปัจจุบัน 32 bits, managed by IANA ty assigned by RIRs to ISPs

router eigrp AS-# or process ~~number~~ ID

- EIGRP router ID → eigrp router-ID > highest IPv4 add of loopback > highest IPv4 addr
  ↳network NW-num [wildcard]
  passive-interface type number (in config-router)
  R1# show ip eigrp neighbors
- EIGRP Operation
  R1: hello → all, R2: add R1 to neighbor table & update → all & hello → R1,
  R1: update topology table & ACK → R2 & update → R2, ~~R2: ACK → R1~~
  R2: update topology table & ACK → R1, R1: use DUAL to calculate the best path to each destination & update routing table, R2: same as R1

▸ EIGRP metrics
- Bandwidth: lowest BW K1
- Delay: cumulative interface delay K3
- reliability } optional K4, K5
- Load K2

metric = (K1 × BW + K3 × delay) × 256
= [K1 × BW + (K2 × BW)/(256 - load) + K3 × delay] × [K5/(reliability + K4)]

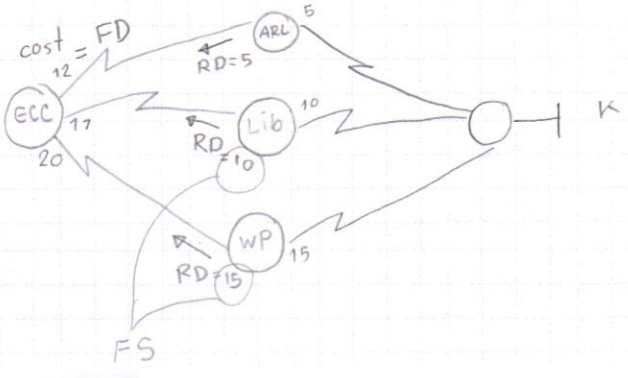
R1(router-config)# metric weights tos k1 k2 k3 k4 k5 (10100)
R1# show interfaces
~~R1# conf~~ R1(config-if)# bandwidth 64

- Delay(μsec) → G(10), Fa(100), T1(20,000)

metric = [(10^7/BW) + (sum of delay/10)] × 256 note. lowest BW

- DUAL (Diffusing Update Algorithm) → provide the best and backup loop-free paths
  - Successor (S) → the least-cost route to dest
  - Feasible Successor (FS) → backup path
    ↳ RD ต้องน้อยกว่า FD ถึงได้เป็น FS
  - Reported Distance (RD) → reported metric from neighbor advertising the route
  - Feasible Distance (FD) → actual metric of a router from the current router
    ↳ "lowest" calculated metric

S → FD → RD → FS!



show ip eigrp topology → FS, S
show ip eigrp topology all-links → all ~~ports~~ paths

- IPv4
  v4 → 32 bits v6 → 128 bits
  v6 → NAT, IoT
  ▸ Migration from IPv4 to IPv6
  - DUAL Stack → run ไปคู่กัน → config v6 เพิ่ม เครื่องไหนมีแค่ 4 ใช้ 4 มีคู่ใช้ 6
  - Tunneling → ตรงกลางเป็น v4 แล้วมีตัว connect
  - Translation

- IPv6
  - x:x:x:x:x:x:x:x
  ▸ Address Types
  - Unicast → Global unicast, Link-local, Unique Local
  - Multicast
  - Anycast