ชื่อ-สกุล [illegible] [illegible] กระดาษแผ่นที่ 1 รหัสนักศึกษา 88888888

for Staples

Layer					
Application	Name System: DNS	Host config: BOOTP, DHCP	Email: SMTP, POP, IMAP	File Tran: FTP, TFTP	Web: HTTP
Transport	UDP	TCP			
Internet	IP, NAT	IP support: ICMP	Routing Protocol: OSPF, EIGRP		
Network Access	ARP	PPP	Ethernet	Interface drivers	

Port (0-65535)
- 0-1023 reg. entities
- 1024-49151 register port
- 49152-65535 dynamic/private

IPv4 < first octet >
- Class A ~> 00000000 - 01111111 (0-127)
- Class B ~> 10000000 - 10111111 (128-191)
- Class C ~> 11000000 - 11011111 (192-223)
- Class D ~> 11100000 - 11101111 (224-239) (multicast)

Private IP
- /8 Class A ~> 10.0.0.0 ~ 10.255.255.255
- /16 Class B ~> 172.16.0.0 ~ 172.31.255.255
- /24 Class C ~> 192.168.0.0 ~ 192.168.255.255

MAC addr.
- 48-bit (binary), 12 (hex) digits
- assign OUI as the first 3 bytes (24 bits) if all MAC addr. have the same OUI then assign a unique value in the last 3 bytes

Unicast MAC
- 1-1 Transmission
- des. IP must be in the IP packet header & des. MAC must be in the Ethernet frame header

Broadcast MAC
- Ex. DHCP, ARP
- des. IPv4 addr. (all 1 in host) ← local network
- MAC : FF-FF-FF-FF-FF-FF

Multicast MAC
- allow a source device to send a packet to a group of devices
- Devices in a multicast group assign a multicast IP in range of [Class D] (IPv6 : begin with FF00/8)
- MAC : begin with 01-00-5E in (hex)

Floating Static Routes
- this. admin distance > admin distance of another static Route / dynamic route
- this. admin distance can be incresed to make the route less desirable than another static route or learned through a dynamic routing
- this. can take over when the preferred route is lost (traffic can be sent)

CIDR : Classless Inter-Domain Routing
→ จัดสรรและรวมกลุ่มตำแหน่งบน internet โดยใช้ Inter Domain Routing
(คล้าย summary IP / ไม่มี class A,B,C,... แบ่ง subnet เท่าๆกัน)

Routing table (Store in RAM)
- Directly Connect Routes
- Remote Routes
- Network / Next hop Association

Config IPv4 static Routes
- next hop can be identified by an IP addr, exit interface.
- Next hop route : only next hop IP addr. is specified.
- Directly connected static route : router exit interface
- Fully specified static route : both

Router(config)# ip route dest_network addr. subnet mask ip addr / exit (next hop)

for Staples

for Staples

Routers utilize the following mem.

MEM	Volatile / non-Volatile	Stores
RAM	volatile	running IOS running Config. file IP routing & ARP tables Packet buffer
ROM	non-Volatile	Boot up instruction Basic diag. Software Limited IOS
NVRAM	non-Volatile	Start up config. file
Flash	non-Volatile	IOS, Other system file

Router boot-up process → power-on self test

1. ROM POST Perform POST
2. ROM Bootstrap Load Bootstrap
3. Flash — CISCO Internetwork OS — Locate & Load OS
4. TFTP server
5. NVRAM — Configuration — locate & load config. file / enter setup mode
6. TFTP server
7. Console

Console Access
- Cable: RJ-45-to-DB-9
- Programs: PuTTY, tera term, ...

Path Determination
- Best Path: lowest metric
- dynamic routing use
  - Routing Information Protocol (RIP): hop count
  - Open shortest Path First (OSPF): cost based on cumulative bandwidth from source to des.
  - Enhanced Interior Gateway Routing Protocol (EIGRP): bandwidth, delay, load, reliability
- Load Balance
  - If 2 or more path to a des. with equal cost metrics → use both paths equally

Static Route often use to
- Connect to a specific network
- Provide a Gateway of last Resort for a stub network
- Reduce # routes advertising
- Create back-up route

Packet forwarding methods
- Process switching: old
- Fast switching: use a fast-sw. cache to store hop information
- Cisco Express Forwarding (CEF): fastest table entries is not packet-triggered but change-triggered

Document Network Addr.
- Device names
- Interfaces
- IP addr & subnet mask
- Default gateways

Summary Routes
- Route aggregation, the process of advertising a contiguous set of addr. as a single addr with shorter subnet
- CIDR: Ignore the limitation of classful boundaries
- reduce # entries in routing up dates & lowers # entries in local routing table

(AD) Administrative Distance = "trustworthiness"

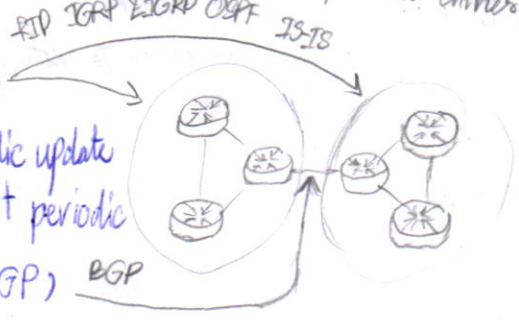
Type: standard, default, summary, Floating static route

Dynamic Routing Protocol

- dynamic share information
- Automatically update routing table
- determine best path

	dynamic routing	static routing
configuration complexity	independent of the network size	Increase with network size
require admin. knowledge	advanced knowledge required	no required
Topology change	automatically adopt	admin required
Scaling	simple/complex topo.	simple topo.
Security	less secure	more secure
Resource usage	use CPU, mem, link bw.	no needed
Predictability	route depend on the current topo.	always the same route(s)

Classifying Routing Protocol



- Interior Gateway Protocol (IGP)
  - distance vector . periodic update
  - Link state . updates aren't periodic
- Exterior Gateway Protocol (EGP)
- Classful routing Protocols . Do not send subnet mask in routing updates
- Classless . Do send subnet mask, support VLSM
- Convergence is defined as all routers' routing tables are at stable state
- Load balance . distribute packets among multiple same cost paths

Distance Vector Protocols

- Characteristic
  - Periodic updates
  - neighbors
  - Broadcast updates
  - Entire routing table
- Criteria used to compare routing protocols
  - Time to convergence
  - Scalability
  - resource usage
  - Implementation & maintenance

Routing Loop

- setting a Maximum
  - RIP (16 hops) → if infinite, mark as "(unreachable)"
- Prevent with Holddown timers
- Split Horizon Rule
  - router should not advertise a network through the interface from which the update come
- Route Poisoning
  - mark the route as unreachable in a routing update that is sent to other routers
- IP & TTL - Limit hops (8 bits field in IP header)

Comparing RIPv1 & RIPv2 Message format

Bit 0 7 8 15 16 23 24 31

Command = 1 OR 2 | Version = 1 | Must be zero

Route entry:
- Address family identifier (2=IP) | Must be zero
- IP Address (Network Address)
- Must be zero
- Must be zero
- Metric (HOPS)

Multiple route entries, up to a maximum of 25

Version 2

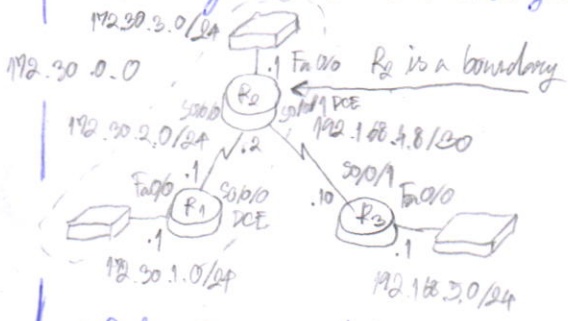
Route entry: replace must be zero by
- route Tag
- subnet mask
- next hop

Routing table Maintenance

- Periodic update: RIP update timer (default 30)
  - IOS 3 additional timer for RIP
    - Invalid (default 180)
    - Holddown (default 180)
    - Flush (default 240)
- Bounded update: EIGRP
- Triggered update
- Random Jitter

RIP v1

- Characteristic
  - Classful, Distance Vector
  - Metric = hop count
  - hop count > 15 (unreachable)
  - Boardcast update every 30s
- RIP Message (512 Bytes, upto 25 routes)
  - Header
    - Command field
    - Version field
    - Must be 0
  - Route Entry
    - Address family Identifier
    - IP address (A, B, C)
    - Metric
- RIP Operand
  - req
  - res
- Boundary Router - automatically summarize RIP subnets



CIDR uses Supernetting

- Supernetting is a branch of contiguous classful networks that is addressed as a single network

Standard ACLs

- Check src addr.
- permit/dq entire protocol suite

Extended ACLs

- Check src & des addr
- permit/dq specific protocols

Access Control list (ACL) (can control traffic)

- The last statement of ACL is always an implicit dq (automatically inserted at the end of each ACL) & (It blocks all traffic)

Wild card Masks in ACLs

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	Match all addr.
0	0	0	0	1	1	1	1	Ignore last 4 bits
1	1	1	1	0	0	0	0	Ignore first 4 bits

0 → match
1 → ignore

ACL Best Practices

Guideline	Benefit
Base your ACLs on the security policy the organization	ensure you implement organization security
Use text editor to create, edit and save ACLs	This will help you create library of reusable ACLs

- 2 Rules RIPv1 updates
  - same network → subnet of interface is applied
  - diff network → Classful subnet mask is applied
- RIP Message are encapsulated in UDP src & des port = 520

Similarities Between RIPv1 & RIPv2

- use timers → prevent routing loops
- use split horizon / split horizon with poison reverse
- use triggered update
- Maximum hop count of 15

Calculate Wildcard Masks

- use subtract subnet mask

255.255.255.255 ←
- 255.255.255.240 ← wild card
000.000.000.015

Loopback interface → virtual interface, can be added to routing table
Null int → virtual int., no need configured or created
Static routes & null int. → null int. will serve as the exit int.

RIPv2 → automatically summarize routes at major network boundary & summarize routes with a subnet mask that is smaller than Classful subnet mask

for Staples

Link-state Protocol

- When uses? → network design ที่มีขนาดใหญ่ (large network)
  - → Fast convergence of network is crucial
  - → admins have good knowledge
- all link-state apply dijkstra's algorithm (SPF: Shortest Path First)
- link-state updates
  - each router learns ชื่อและที่อยู่ของ network ของตัวเอง
  - each router ส่ง hello say hello neighbors
  - each router builds a link-state Packet (LSP) containing the state of ลิงก์ของตัวเอง
  - each router ส่ง LSP to all neighbors → store all LSP's received in a db.
  - each router use db to construct a complete map of topology & compute best path

Routing Protocol Classification

- Dynamic routing
  - Interior Gateway (IGPs)
    - Link-state
      - OSPF
      - IS-IS
    - Distance Vector
      - RIPv1 → RIPv2
      - IGRP → EIGRP
  - Exterior Gateway (EGPs)
    - Path-Vector
      - BGP

OSPF

- Message

IPv4 Header Fields

Data link Frame Header	IP Packet Header	OSPF Packet Header	OSPF Packet Type Specific Database

- Cost = reference bandwidth / interface bandwidth (default is 10^8) → auto-cost ref-bw 100

interface type	cost
10 Gigabit Ethernet (10Gbps)	1
Gigabit Ethernet (1Gbps)	1
Fast Ethernet (100 Mbps)	1
Ethernet (10 Mbps)	10
Serial (1544 Mbps) [cisco]	64
Serial (128 kbps)	781
Serial (64 kbps)	1562

When OSPF router is initially connected to a network
- create adjacent w/ neighbors
- exchange routing info.
- Calculate best routes
- Reach convergence

OSPF states

- Down State
- Init State
- Two-Way State

(Establish Neighbors Adjacent)

- ExStart State
- Exchange State
- Loading State

(Synchronize OSPF Database)

- Full State

DHCP (Dynamic Host Configuration Protocol)

- provide automatic IP addressing and other information to clients
  - IP addr.
  - Subnet mask (IPv4) or prefix length (IPv6)
  - Default gateway address
  - DNS server address
- 3 different address allocation
  - Manual : admin assigns a pre-allocated IPv4 addr to client, communicates only IPv4 to device.
  - Automatic : auto assigns a static IPv4 addr permanently to a device, select from pool of available (no rent)
  - Dynamic : dynamic assigns an IPv4 addr. from a pool of addr. for a limited period of time chosen by server. (or rent)

type	Packet name
1	Hello
2	Database Description (DBD)
3	Link-State Request (LSR)
4	Link-State Update (LSU)
5	Link-State Ack (LSAck)

for Staples

for Staples

LAN Design

Borderless Switched Networks

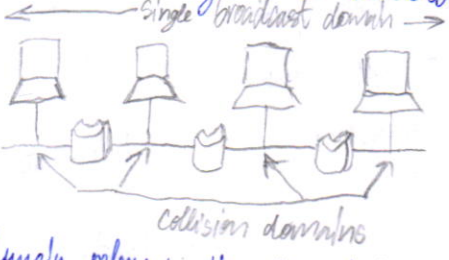
- is a network architecture that allow organizations to connect anyone, securely
- support converged network and changing work patterns
- การใช้งานที่ยืดหยุ่น → ตำแหน่ง
  → ที่ทำงาน
  → อุปกรณ์

Consideration when selecting switch Equipment

- Cost : depend on number and speed of interface
- Port density
- Power
- Reliability
- Port Speed : speed of network connection
- Frame Buffers : may be congested port
- Scalability

Segmentation is the process of splitting a single collision domain into smaller domain

- create smaller domains reduce the number of collision on a LAN segment
- Layer 2 device (bridge/switch) can be use



Broadcast domain refers to the set of devices that receive a broadcast data frame originating from any device within that set

- consume resource & available Bw of the host
- Layer 2 devices (bridge/switch) reduce the size of collision domain but don't reduce the size of broadcast domain
- Router reduce collision domain & broadcast domain @ Layer 3

3 tier LAN Design

Switched environment

Operation

aging → Learning
→ Programs growing old
→ Flooding
→ Forwarding
→ Filtering

Transparent Bridge Process (Jeff Doyle)

Receive frame
↓
Learn src addr. / refresh aging timer
↓
Is the des. a broadcast, multicast or unknown unicast?
No ↓ Yes → Flood Packet
Are the src and des on the same interface
No ↓ Yes → Filter Packet
Forward unicast to correct port

Frame Forwarding

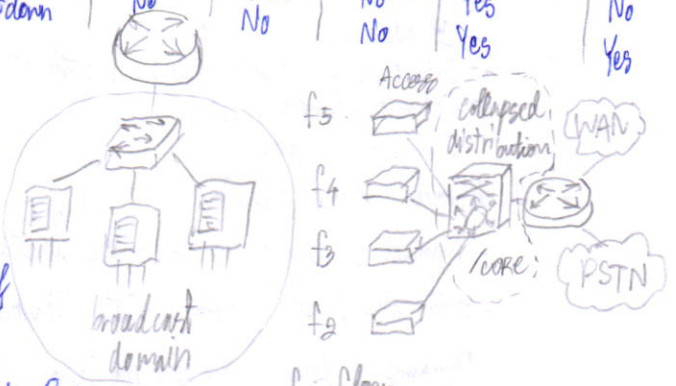
→ Store-and-Forward Switching (slow)
- check for errors (FCS Check)
- automatic buffering → CRC

→ Cut-Through Switching
- start forward in 10 ms
- No FCS check, No automatic buffering
- Fast-forward ≈ 12 bytes
- Fragment-free ≈ 64 bytes

SSH uses TCP port 22, Telnet uses TCP port 23

Security Violation Modes

Violation mode	Forwards traffic	Sends syslog	Displays error	Increments Violation counter	Shuts port
protect	No	No	No	No	No
restrict	No	Yes	No	Yes	No
shutdown	No	No	No	Yes	Yes



ชื่อ-สกุล ธนกร อัจฉริยะ กระดาษแผ่นที่ 4 รหัสนักศึกษา 68011999

for Staples

Spanning Tree Algorithm

- only 1 logical path between all dis.
- block port when user data is prevented from entering / leaving that port
- physical paths still exist to provide redundancy (but disabled)
- If switch failure, STP recalculates the paths

STP Operation

- Root Bridge

Bridge Priority	Extended System ID	MAC Address
4 bits	12 bits	48 bits

Field	Byte length
Protocol ID = 0x0000	2
Protocol version ID = 0x02	1
BPDU Type = 0x02	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello time	2
Forward Delay	2

Rapid PVST+

- prevent layer 2 loops in a switched network environment.
- independent instance of RSTP runs for each VLAN
- no blocking ports. RSTP define port states (discard, learn, forward)
- RSTP keeps the same BPDU format as IEEE 802.1D except version (2), flag (8 bits)

RSTP BPDU (V.2)

Field	Bit
Topology Change	0
Proposal	1
Port Role	2-3
Unknown Port	00
Alternate / Backup	01
Root Port	10
Designated Port	11
Learning	4
Forwarding	5
Agreement	6
Topology Change	7
Acknowledgment	

Edge Ports
- Will never have a switch connected
- Immediately transitions forwarding

Characteristics of the spanning Tree Protocols (STP)

Protocol	Standard	Resources Needed	Convergence	Tree Calc.
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s Cisco	Medium/High	Fast	Per Instance

for Staples

PVST+

Characteristics
- A network can run an independent IEEE 802.1D STP instance for each VLAN in the network
- Optimum load balancing can result
- 1 spanning-tree instance for each VLAN → waste cpu cycles for all switches in network, BW is used for each instance to send own BPDU

Extended System ID
- In PVST+, extended switch ID ensure each switch has a unique BID for each VLAN

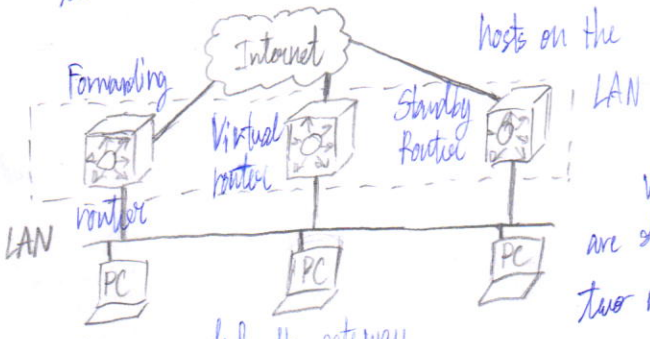
Port States

Processes	Blocking	Listening	Learning	Forwarding	Disabled
Processes received BPDUs	Yes	Yes	Yes	Yes	No
Forward data frames received on interface	No	No	No	Yes	No
Forward data frames switched from another interface	No	No	No	Yes	No
Learn MAC addresses	No	No	Yes	Yes	No

for Staples

First-Hop Redundancy Protocol

- If the default gateway cannot be reached, the local device is unable to send packets hosts on the LAN



acting as default gateway

Virtual IP and MAC are shared between the two routers

Varieties of First-Hop Redundancy Protocols

- Hot Standby Router Protocol (HSRP) → Cisco proprietary → define a group of routers (one active one standby)
- HSRP for IPv6
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
- VRRPv3
- Gateway Load Balancing Protocol (GLBP) → multiple available gateway
- GLBP for IPv6
- ICMP Router Discovery Protocol (IRDP)

VLANs

- (Virtual LAN) is a logical partition of Layer 2 network
- Multiple partition can be created, allow for multiple VLANs to co-exist
- each VLAN is a broadcast domain, usually with its own IP
- VLANs are mutually isolated and packets can only pass between them through a router
- Layer 2 device → usually a switch
- The hosts group of a VLAN are unaware of the VLANs existence

Controlling Broadcast Domains with VLANs

- VLAN can be used to limit the reach of broadcast frames
- VLAN is a broad cast of its own
- a broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only

Tagging Ethernet Frames for VLAN Identification

Dst. MAC	Src MAC	Type/Length	Data	FCS

Ethernet frame

* 802.1Q Frame

Dst. MAC	Src MAC	Tag	Type/Length	Data	FCS

2 byte 3bits 1bit 12 bits

Ethernet Type (0x8100)	Pri	C	VLAN Identifier

(Tag)

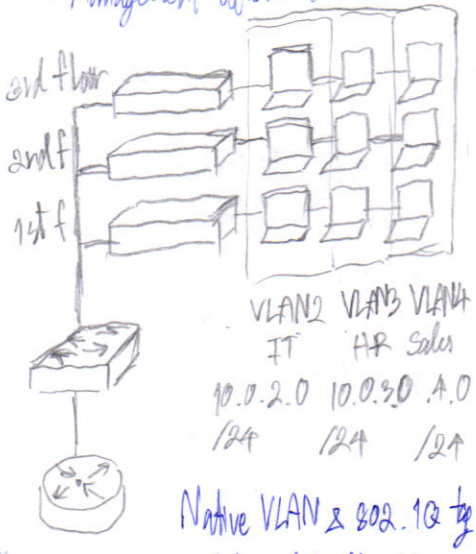
VLANs in a Multi-Switched Environment

VLAN Trunks

- carry more than 1 VLAN
- established between switches so same-VLAN device can communicate
- not associated to any VLANs
- Cisco IOS supports IEEE 802.1q

Benefits of VLANs

- Improved security
- reduced cost
- better Performance
- Smaller Broadcast Domains
- It efficiency
- Management efficiency



Native VLAN & 802.1Q tg

- Cisco Switch: default = VLAN
- A frame that received untagged will remain untagged and placed in the native VLAN when forwarded

VLAN assignment

- The catalyst 2960 & 3560 series switches sup over 4000 VLANs

Normal range	Extended range	NVRAM
- number 1-1005	- number 1006-4096	
- Config stored vlan.dat	- Config stored in running config	
- VTP can only learn and store normal range VLANs	- VTP does not learn extended range VLANs	

flash

Inter-VLAN → process for forwarding network traffic from one VLAN (using router)

ชื่อ-สกุล [illegible] กระดาษแผ่นที่ 5 รหัสนักศึกษา [illegible]

for Staples

VTP → use layer 2
→ Cisco switch (VTP default already configured)

	serv	Client	Transparent
Source VTP	✓	✓	×
Listen VTP	✓	✓	×
Create VLANs	✓	×	✓ local
Remember VLANs	✓	×	✓ local

→ (serv) VLAN config save in Catalyst NVRAM
→ Client doesn't save config
→ Trans. only forward VTP ad. (no message)
→ VTP V.2 (support Token ring VLANs) (no compatible w/ V.1)
→ domain name (1-32 char) } case
→ password ((8-64) char) } sensitive

for Staples

VTP config
→ global config → VLAN conf

global config	VLAN conf
conf t	vlan database
vtp v 2	vtp v2-mode
vtp m serv	vtp serv
vtp dom cisco ↔ n	n
vtp pass password ↔ n	n

VTP Pruning
→ enhance network bw.
→ VLAN1 (default)

Conf.
(vl)# vtp pruning
#int fa 0/3
#sw tr pruning
vlan remove vlan-id

for Staples

Static NAT (one-to-one)
- useful when server hosted in the inside netw must be accessible from outside network

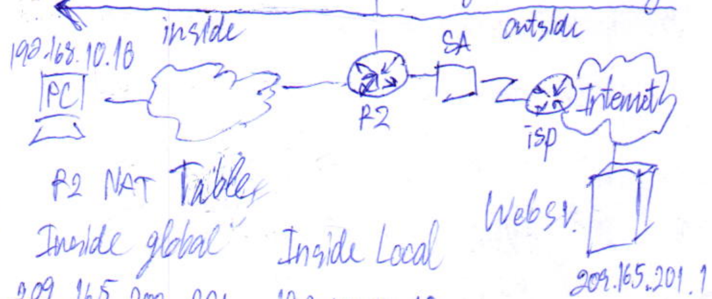
NAT → IPv4 Private Address Space

· Private Internet RFC 1918:

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

4 types NAT
- Inside local
- Inside global
- Outside local
- Outside global

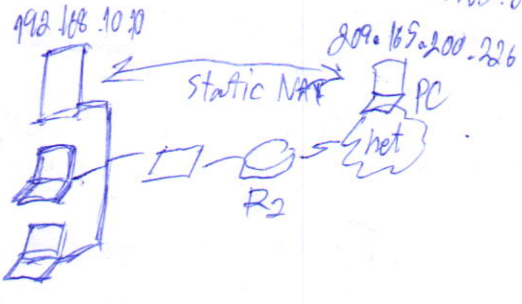
SA inside loc	DA outside loc	SA inside global	DA out global
192.168.10.10	209.165.201.1	209.165.200.226	209.165.201.1
DA in loc	SA out loc	DA in glo	SA out glo



R2 NAT Table

Inside global	Inside Local
209.165.200.226	192.168.10.10
Outside Local	**Outside Global**
209.165.201.1	209.165.201.1

(PC)
(Web server)



Dynamic NAT

- pool of addr.

ex.

Inside local	Inside global pool
192.168.10.12	209.165.200.226
available	209.165.200.227
available	209.165.200.228

PAT (Port Address Translation)

- PAT = NAT overload
- PAT maps multi private IPv4 to a single public IPv4 or few addr.

Config Static NAT

1. (config)# ip nat inside source static local-ip global-ip
2. (config)# int type num
3. (config-if)# ip nat inside
4. exit
5. (conf-if) int type num
6. ip nat outside

Config Dynamic NAT

1. ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
2. access-list access-list-number permit src [src-wildcard]
3. ip nat inside source list access-list-number pool name
4. int type num → ip nat inside
5. int type num → ip nat outside

Config PAT Single Add

1. access-list access-list-number permit source [source wildcard]
2. ip nat inside source list access-list-num int type num overload

3 in
4 out

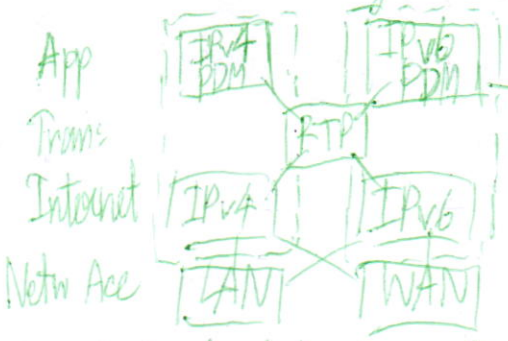
Config PAT pool → same as Dynamic nat but

IP addr : Port ex. 192.168.100.1:1444

step 3: put overload at very last port

EIGRP → Distance Vector Routing

- → Classless
- → Feature
  - → establish neighbor
  - → Reliable Transport
  - → Eq / not Eq cost Load balance
- → PDMs (Protocol-dependence modules)
  - → Maintain EIGRP neighbor
  - → compute metric using DUAL
  - → filtering & access-list
  - → perform redistribute
- → RTP → Transport layer protocol delivery/reception EIGRP packets (not all RTP is reliably sent)



→ neighbor table
→ Topo
→ Routing

PACKets types

Hello - Discover always unreliably
Update - Convey route info
Ack - Ack
Query - Request info from neighbor
Reply - respond to a query

EIGRP → multicast IPv4 : 224.0.0.10
→ multicast IPv6 : FF02::A
→ Update reliable (req, ACK)
→ Update only contain needed routing (mul/uni) (uni)
→ query & Reply are used by DUAL when searching for network

Datalink Frame Header	IP Packet Header	EIGRP Header	TLV types

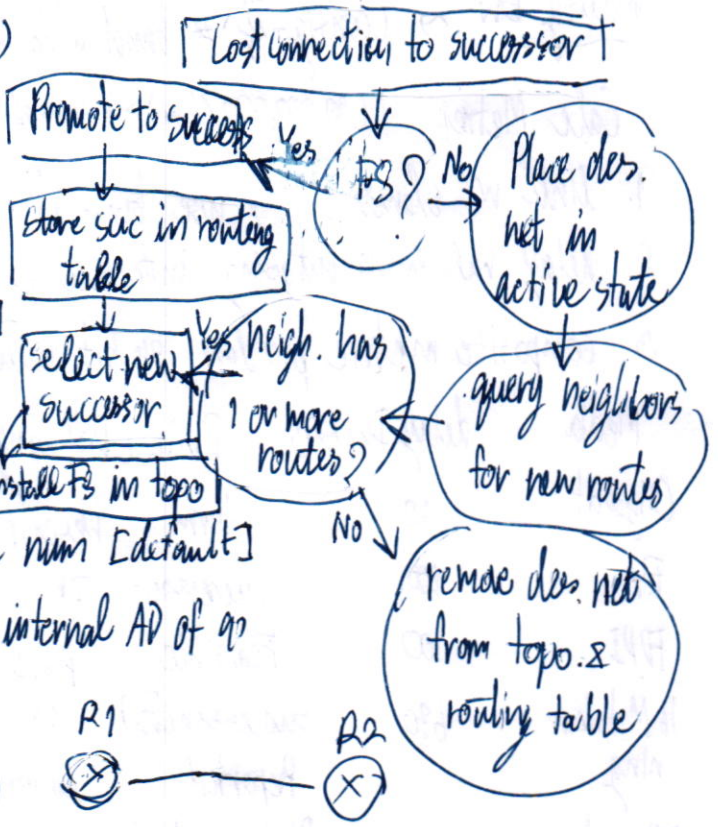
0 | Version 7 8 | Opcode 15 16 | Checksum 23 24 31
Flags
Sequence
Ack
AS number

AS number → a collection of networks under the control of a single auth.
→ need to exchange routes between AS
→ 16-bit numbers (0-65535)

Config EIGRP
1. router eigrp as-#
2. eigrp router-id 1.1.1.1 (optional)
3. network net-addr [wildcard mask]

Passive Interface prevent EIGRP update out a specified router interface
(configure-router)# passive-interface type num [default]

EIGRP administrative distances on R1 are internal AD of 90 & external of 170 (default)



EIGRP OP (Initial Route Discovery)

1 R1 join EIGRP routing domain & send EIGRP Hello package out all int.
2 R2 receive Hello → add R1 to neighbor table → send update all routes
3 R1 update its neighbor table w/ R2 → send Hello to R1
4 R1 add all update to topology table
5 R1 reply w/ Eigrp Ack to R2
6. R1 send update to R2 advertising the routes that is aware
7. R2 recieve → add to topology table
8. Response Ack to R1
9 R1 use DUAL to calc best route → then update to routing table
10. R2 use DUAL update new routes same as 9)

EIGRP Metrics
↳ Bw (lowest BW src to des)
↳ Delay (cumulative interface delay along path)
↳ Reliability (optional) worst reliability src to des
↳ Load (optional) worst load on a link src to des

Default Composite Formula
metric = [K1 * bandwidth + K3 * delay] * 256

	default value
K1 Bw. (kb/s)	1
K3 delay (μs)	1
K4 load (255)	0
K5 reliability (255)	0

Complete
metric = [K1 * bw + (K2 * bw) / (256 - load) + K3 * delay] * [K5 / (reliability + K4)]
if K5 = 0 → replace [K5 / (reliability + K4)] → * 256
modify Bw → (config-if) # bandwidth kilobits - bandwidth-value
Calc Metric ((10,000,000 / bw) + (sum of delay / 10)) * 256 = metric
1. link w/ slowest bw ∴ use bw = (10^7 / bw) ← slowest
2. delay val each outgoing interface to des (sum of delay / 10)
3 composite metric produce 24 bit value which eigrp mul w/ 256.

Media	delay In Usec
Gigabit	10
FA	100
FDDI	100
16 M token ring	630
Ethernet	1000
T1 (Serial default)	20000
DS0 (64 kbps)	20000
1024 kbps	20,000
56 kbps	20000

DUAL (Diffusing Update Algorithm)

term	Description
Successor	IP its shown in routing table after "via"
Feasible Successor (FS)	Backup Path, a loop-free (same network as successor)
Reported Distance (RD)	advertised distance
	if RD < FD then next hop router is down
Feasible distance (FD)	actual metric from current router lowest calc metric, second num inside [ ]
	- passive → available for use - active → recompute by DUAL

DUAL → prevent routing loop
↳ use FSM (like flowchart)