ชื่อ-สกุล ณยวรวิทย์ ชัยนาณิช กระดาษแผ่นที่ 1 รหัสนักศึกษา 99088809

for Staples

Reliable Network
- Fault Tolerance
- Quality of Service
- Scalability
- Security

- A protocol model
  - provides a model that closely matches the structure of a particular protocol suite
- A reference model
  - provides a common reference for maintaining consistency within all type of network protocols and services

Application	Name System: DNS	Host Config: BOOTP, DHCP	Email: SMTP, POP, IMAP	File Transfer: FTP, TFTP	Web: HTTP
Transport	UDP	TCP			
Internet	NAT, IP	IP Support: ICMP	Routing Protocols: OSPF	EIGRP	
Network Access	ARP	PPP	Ethernet	Interface driver	

PDU (protocol data unit)

Session	TRANSPORT	Network	Data Link	Physics
data	segment	packet	frame	Bits

Logical Address (IPv4)

A	0-127	255.0.0.0	128	16,777,216
B	128-191	255.255.0.0	16,384	65,536
C	192-223	255.255.255.0	2097152	256
D	224-239	Reserved for multicast		
E	240-254	Reserved for experiment		

Network Characteristics
- Topology - Security - Reliability
- Speed - Availability - Lost
- Scalibility

Port Address
0-65,535
- IANA dedicated to reserve the first 1024 port Numbers for requesting entities
- 1024-49151 Registered port
- 49,152-65,535 dynamic, private

well-known port → destination port
Randomly gender → for source port

Router → routing of traffic betw network
↳ Require → CPU
↳ OS → cisco IOS
↳ Memory And storage (RAM, ROM, NVRAM, Flash, hard disk)

mem
RAM (V) - Running IOS, Configuration files
- IP routing, ARP Tables
- Packet buffer

Rom (NV) - Bootup instuctions, Limited IOS
- Basic diagnostic software

NVRAM (NV) - startup configuration file
Flash (NV) - IOS, other system files

MAC Address (Physics Address)
- 48 bits → assign the vendor a 3 byte code
- by IEEE → called OUI
- Required a vendor to follow 2 rules
  1) All Mac Address assigned to a NIC or other Ethernet device must use OUI as the first 3 byte
  2) All Mac addrs with the same OUI must be assigned a unique value in last 3 byte

Major phases to the router boot-up process
- Test router hardware ↳ Power-on self test (POST)
  ↳ Execute bootstrap loader
- Locate & load Cisco IOS software → Locate, Load IOS
- Locate & Load startup config file or enter setup mode
  ↳ bootstrap program looks for config file

UNICAST MAC Address
- when a frame sent from one to one (single)

Broadcast Mac → Dest MAC (FF-FF-FF-FF-FF-FF)
- DHCP, ARP use broadcast
- All host in local netw will receive the packet

Multicast Mac
- To a group of devices
- Mac begin with 01-00-5E

- Router use specialized ports and network interface cards to interconnect to other networks
- Router Choose best Path (Routing table)
  ↳ use static router, dynamic routing to build
- Document Network Addressing
  - Device name . Interface . IP/subnet . Default gateway

Packet Forwarding Method
- process switching
- Fast switching
- Cisco Express forwarding

private addressing (RFC 1918)

A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

CIDR Prefix
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

Statically Assign IP Addr
↳ host is manually assigned IP/subnet/detail getc
dns server IP Address can also be assigned
Dynamically Assign IP
↳ IP inter assign by a server using Dynamic Host Configuratio Protocol (DHCP)

Path Determination

* Best Path : lowest metric
- Dynamic routing protocol : use their own rules and metric
- Routing Information Protocol (RIP) - hop count
- Open shortest path first (OSPF)
  - cost based on cumulative Bw t.., s→d
- Enchanced Interior Gateway Routing Protocol (EIGRP)
  Bw, delay, load, reliability

* Adminstrative Distance (AD) : "trust worthiness"

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

Dynamic routing Protocals
- Exterior R.P.
  - BGP
- Interior Gateway R.P.
  - RIP
  - OSPF
  - EIGRP (Intermediate System-to Intermediate System)

CIDR ใช้ลดขนาด routing table ของ Internet โดยใช้ Inter Domain Routing

VLSM = 1 network สามารถมี subnet mask หลาย subnet ได้ตามใจชอบ

Ex. 192.168.20.0/29 → /27
จะได้ 8 subnet, 30 host per subnet

11000000.10101000.00010100.000|00000

$2^5 = 32$
256 = 32 , 8 subnet

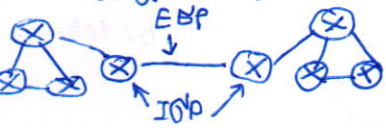
$2^5 = 32$
$32 - 2 = 30$
30 host

ชื่อ-สกุล นายธรินทร์ ปิตนาวินิช กระดาษแผ่นที่ 2 รหัสนักศึกษา 59011179

for Staples

Dynamic Routing Protocols
- Share ข้อมูลระหว่าง Router
- Update table
- หา best path

Classifying - Routing Protocols



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

Classful : subnet mask "same"

Classless : subnet mask "หลากหลาย"

Convergence : ก็ตามเมื่อ router ทุกตัว โดย routing table at state of consistency

Metric : ค่าที่ใช้ใน routing protocol เพื่อตัดสินใจว่าไหนคือ best path

ex hop count, cost, bandwidth
- load balance : เส้นทางที่ cost เท่ากัน จะส่งไปทั้ง 2 เส้นทาง

for Staples

Administrative Distance of route (AD)
: ค่าที่ใช้เจาะจงแต่ละ router (น้อยๆดี)

Distance Vector Routing Protocols

ex: RIP, IGRP, EIGRP

ต้องรู้ 2 อย่าง: - distance to dest.
- direction, traffic ที่ควรไป

หน้าที่ :- periodic update, neighbors, routing table ทั้งหมดอยู่ routing update
- เกณฑ์ที่ใช้ในการเปรียบเทียบ routing protocols. ex. time resource usage, time to convergence

Network Discovery
1) Router initial start up
2) Initial Exchange of routing inform
3) Exchange router information

Routing Table maintenance
Periodic update : RIP
Bounded update : EIGRP
Triggered update
Random jitter

for Staples

Routing loop
- RIP : กำหนด infinity ที่ 16 mbps (unreachable)
- Holddown Timer : no change data in table if have router down

-split horizon rule : router ไม่ควร advertise network ผ่าน interface ที่ update มา

-route poisoning : ใช้ในการ mask route unreachable ใน routing update ที่ส่งไปให้ router อื่นๆ

-split horizon with poision reverse : เมื่อส่ง update ไปยัง specific interface กำหนด network that were learned on that interface as unreachable

-IP & TTL : 8 bit field ใน Ip header โดย limit จำนวน hop ที่ packet สามารถ traverse เดินทางผ่าน network ก่อน discarded

RIP version 1 (AD: 120)
: classful, metric = hop count, hop > 15 = unreachable, update เป็น broadcast ทุก 30 s.

Data link frame header	IP packet header	UDP segment header	RIP Message 512 b up to 20
Command 1 or 2	version 1 or 2	must be 0	
Address family identifier 2, IP		must be 0	
IP Address (Netw. Address)			
Subnet mask if v.2 else must be 0			
next hop if v.2 else must be 0			
metrics (hop)			

Multiple route entries UP to MAX 25

Message :
1.) request : ส่งเมื่อ start up by each RIP enabled interface request all RIP neigbor enabled to send router table
#classfull : ไม่ส่ง subnet netw. ใน routing update
2) respond : message sent to requesting router containing routing table

R1(config) # router RIP
R1(config-router) # network 192.168.1.0

debug ip rip

Passive Interface command : หลีกเลี่ยง router จากการส่ง update ไปยัง interface
R1(config) # router rip
R2 (config-router) # passive-interface Fast 0/0

Automatic Summarization
-Bondary Routers : RIP automatic summerize classful netw.
summerize RIP subnet จาก 1 major netw. ไปยัง another
- sending RIP update : automatic summerize to reduce size of Routing table

#single route are to represent multiple which result in faster lookup in the routing to

#ไม่ support discontiguos netw.

R2(config-router) # default-information

เปรียบเทียบระหว่าง Dynamic vs static
1) config complex ?
D: ไม่ขึ้นอยู่กับ netw. size
S: เพิ่มตาม netw size
2) require admin knowledge ?
D. advance
S: not extra know
3) Topology change
D: auto adapt to topology change
S: ต้องใช้ admin ช่วย
4) scaling
D: เหมาะกับ simple & complex topology
S: เหมาะกับ simple topology
5) Security
D. less
S. more security
6) Resource usage
D. ใช้ cpu, mem, link bandwidth
S: no extra resource needed
7) Predictability
D: route ขึ้นอยู่กับ topology ปัจจุบัน
S: route to dest. เหมือนเดิม

RIP version 2

RIPv1 vs RIPv2

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

เหมือนกันทั้ง V1 และ V2
- timer → prevent routing loop
- มี split horizon และ split horizon with poison
- มี triggered update
- max hop count : 15

CIDR (classless inter-domain routing)
- update include subnet mask
- support VLSM, route summerization

RIP V1 Limitation
- Loopback interface
- Null interface
- Static route and null interface
- Route Redistribution : ระบบที่ static route
- Verifying and Testing Connectivity
- ไม่ส่ง subnet ใน update
- Summerize netw. at major netw. ไม่ได้
- ไม่ support VLSM, CIDR

Configuring RIP v2
- automatically summerize route ที่ major netw. boundaries & summerize route ด้วย subnet

VLSM & CIDR
- Verify RIPv2 automatic summerization off
- ใช้ VLSM IP Address scheme
- CIDR use supernetting

Verifying & Troubleshooting RIP v2
step 1) check status of all link
2) check cabling
3) check IP address & subnet mask config
4) remove unneeded configuration command

Examine : version, network statement, automatic summerization
Authen : ตั้งค่าให้ invalid routing update ด้วยการ
routing update encryption

Access Control list
- last state ของ ACL จะมี implict deny

Standard IPv4 ACL (ระบุที่ dest.)
- Check source address
- permit/deny entry protocol suit

access-list 10 permit 192.168.20.0
0.0.0.255

wan protocols
ex FTP, Telent

Extend ACL (ควรใช้ใกล้ source)
- Check source and destination address
- Permit/deny specific protocols

access-list 103 permit 192.168.20.0 0.0.0.255 any any 80

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

Guide line for ACL creation
- ใช้ ACL บน firewall
- config บน border router

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

Best Practice : 1) ACL security 2) decrypt 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 192.165.10.0 0.0.0.255
R1(config)# access-list 1 deny any
R1(config)# interface s0/0
R1(config-if)# ip access-group 1 in

VTY port → secure standard ACL

Configure Extended IPv4 ACLs

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

Limiting Debug Output
- to verify and troubleshoot network operation
- easy to view debug

Link-state Protocols

- When uses? → network design เป็นลำดับชั้น (large netw.)
  - → 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 ตัวตนของตัวเองและ network ospf
  - each router ส่งข้อความ say hello neighbors
  - each router builds a link-state Packet (LSP) containing the state of เพื่อนบ้านของตัวเอง
  - each router แลก LSP to all neighbors → store all LSP's recieve in a db
  - each router use db to construct a compute map of topology & Compute best path

Routing Protocols Classification

Dynamic routing
- Interior Gateway (IGPs)
  - Link-state: OSPF, IS-IS
  - Distance-vector: RIPv1, IGRP, RIPv2, EIGRP
- Exterior Gateway (EGPs)
  - path-Vector: BGP

OSPF

- Message
- Cost = reference bandwidth / Interface bandwidth (default is 10^2) → auto-cost ref-bw 100

IPv4 Header Field

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

InterfaceType	cost
100 Mbps	1
1 Gbps	1
Fast Ethernet (100)	1
Ethernet	10
Serial (1544 kbps)	64
serial (128 kbps)	781
serial (64 kbps)	1562

When OSPF router is initially connected to a network
- Create adjacent w/ neigbors
- exchange routing inform
- calculate best routes
- Reach Convergence

OSPF state

- Down state → Init state → Two-way state: Established Neigbor Adjacent
- Ex start state → Exchange State → Loading: Synchronize OSPF Database
- → Full stach

type	Packet Name
1	Hello
2	database description (DBD)
3	Link-state request (LSR)
4	Link-State Update (LSU)
5	Link-state Ack (LSAck)

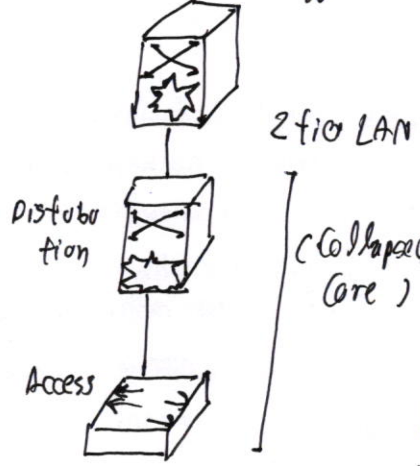
DHCP (Dynamics Host Configuration Protocols)

- provide automatic IP addressing and often information to clients
  - IP addr.
  - Subnet mask (IPv4) or prefix length (IPv6)
  - Default gateway address
  - DNS server address
- 3 different address allocation
  - Manual : admin assign a pre allocated IPv4 addr. to client, communicate Only IPv4 to device
  - Automatic : auto assigns static IPv4 addr. permanently to a device, select from available
  - Dynamic : dynamic assigns an IPv4 addr. from a pool of addr. for a limited period of time chosen

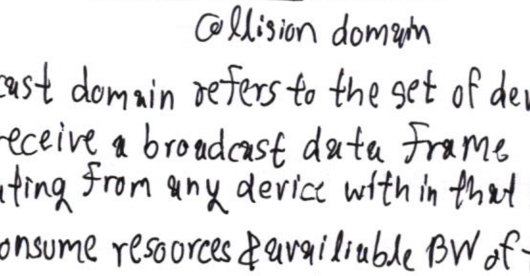
LAN Design

- Borderless Switched Networks
  - is a network architecture that allow organization to connect anyone, securely
  - Support converged network and diverging work pattern
  - การสร้างขึ้นอยู่กับ → ลำดับชั้น → ต้นแบบ → ยืดหยุ่น

3 Tier LAN Design



- Considaration when selecting switch Equipment
  - Cost : depend on number and speed of interface
  - Port density
  - Power
  - Reliability
  - Port speed : speed of network connection
  - Frame Buffer : May be congested port
  - Sealalibity
- 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 with in that set
  - Consume resources & availiable BW of the host
  - Layer 2 device (brigde/switch) reduce the size of collison domain but don't reduce the size of broadcast domain
  - Router reduce collision domain & broadcast domain @ layer 3

Switched envirorment

- Operation
  - Learning
  - Aging
  - Flooding
  - Forwarding
  - Filtering

Transparent Bridge Process

Reciere frame
↓
Learn src addr. / refesh aging timer
↓
Is the des. a broadcast, multcast or unknown Unicast
- Yes → Flood Packet
- No ↓

Are the src. and des. the same interface
- Yes → Filter Packet
- No ↓

Forward unicast to correct port

Frame Forwarding
- Store-and-Forward Switching (Slow)
  - Check for error (FCS check) → CRC
  - automatic buffering
- Cut-Through Switching
  - Start forward in 10 ms
  - No FCS check, No Automatic buffering
  - Fast-Forward ≈ 12 byte
  - Fragement-free ≈ 64 byte

SSH uses TCP port 22, Telnet uses TCP port 23

Security Violation modes

Violation Mode	Forward traffic	Sends Syslog Message	Display Error	increase Violation Counter	Shut down port
protect	NO	NO	NO	NO	NO
restrict	NO	YES	NO	YES	NO
shutdown	NO	NO	NO	YES	YES

ชื่อ-สกุล นายวรวิทย์ ชำนาญใจ กระดาษแผ่นที่ 4 รหัสนักศึกษา 59011179

for Staples

Spaning Tree Algorithm
- Only 1 logical path between all bus
- block port when use data is prevented from entering / leaving
- physical paths still exist to provide redondancy (but disabled)
- If switch failore, STP recalcolates the path

Rapid PVST +
- prevent layer2 loops in a switched network enviroment
- Independent instance of RSTP runs for each VLAN (discard, learn, forward)
- no blocking ports. RSTP define port station
- RSTP keeps the same BPDU ~~define port stats~~ format as IEEE 802.1D except V2, flag 8 bits

STP Operation
- Root Bridge

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

Field	Byte length
Protocode ID = 0x000	(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)

Flags	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 Acknowledgment	(7)

Characteristics of the spanning Tree Protocols (STP)

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

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

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

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 switch in network, BW is used for each instance to send own BPDU

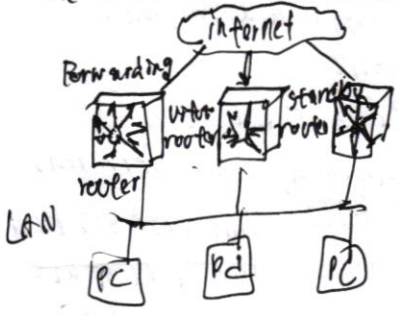
Port Stat

Processes	Blocking	Listening	Learning	Forward	Disable
Processes received BPDUs	✓	✓	✓	✓	✗
Forward data frames received on interface	✗	✗	✗	✓	✗
Forward data frames switched from another instance	✗	✗	✗	✓	✗
Learn MAC Addresses	✗	✗	✓	✓	✗

for Staples

First-Hop Redundancy Protocols

- If the default gateway cannot be reached the local device is unable to send packet



acting as default gateway

Variety of first-Hop Redundancy protocols

- Host standby Router Protocol (HSRP)
- HSRP for IPv6
- Virtual Router Redundancy Protocol v2 (VRRPv2)
- VRRP V3
- Gateway Load Balancing Protocol (GLBP)
- 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 natually isolated and packets can only pass between them through a router
- The hosts group of a VLAN are unaware of the VLAN existence

Controlling Broadcast Domains with VLANs

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

ชื่อ-สกุล ฌนบวรรัทธ์ ปัญญาเมธ กระดาษแผ่นที่ 5 รหัสนักศึกษา 59000079

EIGRP → multicast IPV4 : 224.0.0.10
↳ multicast IPV6 : FF02::A
↳ Update reliable
↳ Update only contain needed routing (mul/uni) (uni)
↳ query & Reply are used by DUAL

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
3. network addrs [wildcard mask]

Passive Interface prevent EIGRP update
out a specified router interface
(configure-router)# passive-interface type num [default]
EIGRP administrative distance on R1 are Internal AD of 90
external of 170 (default)

EIGRP OP

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

EIGRP metrics
- BW (lowest BW src to dest.)
- Delay (cumulative interface delay along path)
- Reliability worst reliability src to des
- Load worst load on a link src to dest.

default value

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

	default
K1 BW (kbps)	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 - bw-value

calc metric ((10,000,000/bw) + (sum of delay/10)) * 256 = metric
1. link w/ slowest bw 2 use bw - (10^7/bw) ← slowest
2. delay value each outgoing interface to dest. (sum of delay/10)
3. Composite metric produce 24 bit value which eigrp ~~neg~~ mul w/ 256.

Media	delay in msec
Gigabit	10
FA	100
FDDI	100
16M token ring	630
Ethernet	1000
T1 (serial default)	20,000
DS0 (64 kbps)	20,000
1024 kbps	20,000

DUAL (Diffusing Update Algor)

term	Description
Successor	Is its shown in routing table after "via"
Feasible	Backup path & is loop Free (some neighbor of successor)
Successor (FS) reported	advertised distance
Distance (RD)	if RD < FD then nexthop router is down
feasible distance (FD)	actual metric from current router lowest calc metric, second num inside []

- passive → unstable route
- active → recomputed by DUAL

DUAL ⇝ PREVENT routing loop
↳ use FSM (like flowchart)

ชื่อ-สกุล ขจพงรรัตน์ ปกเนาวนิช กระดาษแผ่นที่ 6 รหัสนักศึกษา 59[illegible]

or Staples

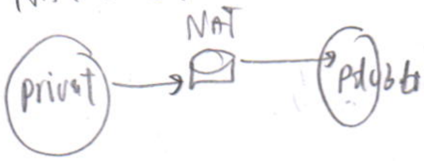
VTP → use layer 2
↳ cisco switch (VTP default already configured,

	server	client	Transparent
Source VTP msg	✓	✓	✗
Listen VTP msg	✓	✓	✗
Create VLANs	✓	✗	✓*
Remember VLANs	✓	✗	✓*

↳ VLAN config save in NVRAM (serv)
- Client doesn't save config
↳ Trans only forward VTP ad (no msg)
→ VTP V_2 (support tokening VLAN) .
(Not compatible V_1)
→ domain name (1-32 Char) } case
→ pass (8-64 Char) } sensitive

NAT: 4 type
- inside local
- inside global
- Outside global
- Outsid local

NAT concept



VSP config
1. conf t
2. vtp v2
3. VTP mode serv
4. VTP dom cisco
5. VTP pass

or Staples

VTP Pruning
→ enhance network bw.
↳ VLAN 1 (default)

1. conf t
2. int fa 0/3
3. sw trunk pruning
vlan remove vlan_id

or Staples

dynamic NAT
- pool of Addr.

ex Inside local	Inside global pool
192.168.10.92	209 ~ .220
Available	209 ~ .229
Available	209 ~ .228

PAT
= NAT overload
PAT MAP multi private IPv4 to a single IPv4

Config NAT (static)
1. ip nat inside source static [IP] [IP]
2. int fa0/0
3. ip NAT Inside
4. int se0/0
5. ip NAT outside

Config dynamic NAT (start END)
1. ip nat pool name IP → IP
2. สร้าง Access list
3. access-list num permit permit สิ่งที่อยู่ Wild card
3. ip nat inside source list num_access-list pool [NAME]
4. inside outside

Config PAT
1. Ip NAT pool name startip – END ip
2. Access-list num permit source wildcard
3. เหมือนข้อ overload
4. inside outside

EIGRP ~~is~~ distance vector Routing
- classless
- feature → estimate neighbor
  - reliable transport
  - Eq / not Eq cost
  - Load Balance
- EDMS (Protocol-dependencies modules)
  - Maintain EIGRP neighbor
  - compute metric using dual
  - filtering & access-list
  - Perform redistribute