ชื่อ-สกุล นาย ศิวกร แท่สุวรรณ์ กระดาษแผ่นที่ 1 รหัสนักศึกษา 68089888

for Staples

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

A protocol model
- provides a model that closly 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	Application	Name system	Host Config	Email	File Transfer	Web
Presentation		DNS	BOOTP DHCP	SMTP POP IMAP	FTP TFTP	HTTP
Session						
Transport	Transport	UDP		TCP		
Network	Internet	NAT IP	IP support ICMP	Routing Protocols OSPF	EIGRP	
Data Link	Network Access	ARP	PPP	Ethernet	Interface Drivers	
Physical						

Port Address (0 - 65,535)
IANA → well-known: (0-1023)
→ registered port (1024 - 49,151)
→ dynamic/private port: (49,152 - 65,535)
source → destination
random → well-known

IPv4			Num of Netw	Num of Address
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	2,097,152	256
D	224 - 239	Reserved for Multicast		
E	240 - 254	Reserved for Experiment		

PDU (protocol data units)

session	Data
Transport	Segments
Network	Packet
Data Link	Frame
Physical	Bits

Private addressing (RFC 1918)

	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

MAC address: 48 bits (12 hex)
- by IEEE → assign the vendor a 3-byte code called Organizationally Unique Identifier (OUI)
  - require a vendor follow 2 rules
    1) All MAC address assigned to a NIC/other Ethernet devices must use OUI as the first 3 bytes
    2) All MAC address with the same OUI must be assigned a unique valve in last 3 bytes

- Unicast MAC Address (1→1)
- Broadcast MAC (1→All) → (DHCP, ARP use broadcast)
  - Dest MAC: FF-FF-FF-FF-FF-FF (1s 48 ตัว)
- Multicast MAC (1→some)
  IP: 224.0.0.0 - 239.255.255.255
  Dest MAC: begin with 01-00-5E -...

Mem
- RAM (V) - Running IOS, Configuration files
  - IP routing, ARP tables
  - Packet buffer
- ROM (NV) - Bootup instructions, -Limited IOS
  - Basic diagnostic software
- NVRAM (NV) - startup configuration files
- Flash (NV) - IOS, -other system

for Staples

Router → routing of traffic between networks
- require → CPU
  - OS → router use cisco IOS
  - Mem / Storage (RAM, ROM, NVRAM, Flash, hard drive)

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

Function of Router
- determine best path (routing table)
- forward packet to dest.
- ใช้ static routes, dynamic routing

Document Network Addressing
Device Name / Interface / IP/subnet / Default gateway

Enable IP on Host
- Statically assign IP addr: host manually assign
- Dynamically assign IP addr: assign by server
  - ใช้ Dynamic Host Configuration Protocol (DHCP)

Path Determination
* Best Path: lowest metric
- Dynamic routing protocols use their own rules and metrics
  - RIP → hop count
  - OSPF → cost based on cumulative BW from S → d
  - EIGRP → BW, delay, load, reliability

* Administrative Distance (AD): trustworthiness

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

CIDR: classless Inter-Domain Routing
- จัดสรร IP address ที่ใช้ใน internet โดยใช้ IDR
- คล้าย, summary IP / ไม่มี class A,B,... ช่วย subnet ที่เล็ก

VLSM: 1 Network มีการแบ่ง subnet mask แต่ละ subnet มีขนาดไม่เท่ากันได้

ex. 192.168.20.0/24 → /27
ต้องได้ 8 subnet, 30 host per subnet
Sol 1 $2^5 = 32$
256 ÷ 32 = 8 subnet
11000000.10101000.00010100.000 00000
000 ... 111
$2^5 = 32$
32 - 2 = 30 host

Dynamic routing Protocols
- Exterior routing Protocols
  - BGP
- Interior Routing Protocols
  - Routing Information Protocol (RIP)
  - Open shortest Path First (OSPF)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - IS-IS (Intermediate System to Intermediate system)

for Staples

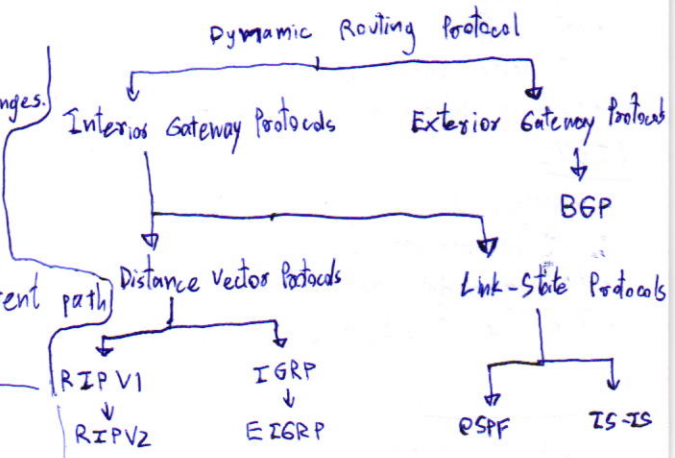
Floating static Router
- มี AD > AD ของ static route อื่น, หรือ dynamic route
- AD ของ static route สามารถเปลี่ยนได้ เพื่อให้ route นี้ทำงานน้อยกว่า static route อื่น, หรือ route ที่ได้จาก dynamic routing Protocols

Dynamic Routing Protocol

Function: - Dynamically share information between routers.
- Automatically update routing table when topology changes.
- Determine best path to a destination

Purpose: - Discover remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks.
- Ability to find a new best path if the current path is no longer available

Component: Algorithm, Routing Protocol message



Dynamic	Static
- Independent of network size	- Increase with nw size.
- Advance knowledge required	- No extra knowledge required
- Automatically adapts to topology changes	- Administrator intervention required
- Suitable for simple and complex topologies	- Suitable for simple topologies
- Less secure	- More secure
- Use CPU, mem, link BW	- No extra resources needed
- Route depends on current topology	- Route to destination is always the same

- Distance vector
  - routes are advertised as vector of distance & direction
  - incomplete view of network topology
  - Generally, periodic updates.
- Link state
  - Complete view of network topology is created
  - updates are not periodic

Metric → Hop count, BW, Cost, Delay, Load, Reliability

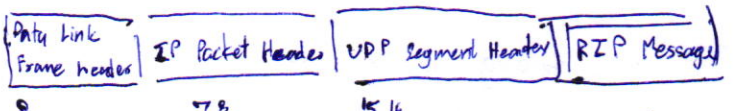
Load balancing → ability of a router to distribute packets among multiple same cost paths = Cost Paths

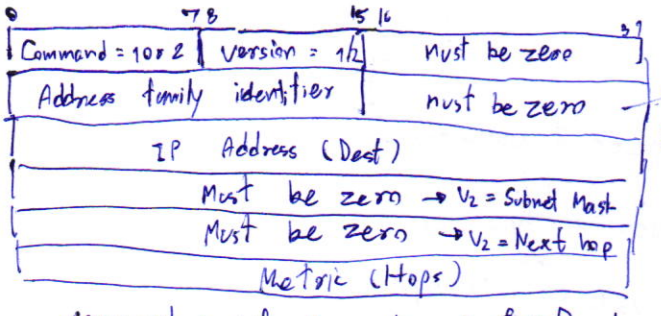
Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
External EIGRP	170
Internal BGP	200

Characteristics of Distance Vector Rou Pro
- Periodic updates, Neighbor, Broadcast updates
- Entire routing table

RIPV1
- classful, Distance vector
- Metric = Hop count
- Routes with a hop count > 15 are unreachable
- Updates are broadcast every 30 seconds

RIP header





Command → 1 for Request, 2 for Reply

AFI → 2 for IP, unless Request is for the full routing table set to 0

IP address → May be a network, subnet, or host addr

RIP message are encapsulated in a UDP segment with source and destination ports of 520

→ interface S e/0/0
→ ip address xxx subnet
→ router rip
→ network xxx
→ passive-interface FastEthernet 0/0
→ end

↓ prevent from sending updates

- debug ip rip
- show ip protocols

RIPV1
- classful dv
- not support discontiguous subnet
- not support VLSM
- not send subnet in routing table
- Routing updates are broadcast

RIPV2
- classless dv
- Next hop address is included in updates
- Routing updates are multicast
- The use of authentication is an option

RIPV1 Limitation
- Loopback interface
- Null Interface
- static route and null interface } WTF
- Route redistribution: inserts static route
- Verifying and Testing Connectivity)
-

VLSM & CIDR
- verify RIPv2 automatic summarization turn off
- 设 VLSM IP addressing scheme
- CIDR use supernetting

access-list 10 permit 192.168.30.0 0.0.0.255
wild card

ACL

3 Ps
1) 1 ACL per protocol
2) 1 ACL per direction
3) 1 ACL per interface

debug ip packet 101

	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

Link-State Routing Protocol

- A link-state routing protocol is like having a complete map of the network topology
- work best where → The network design is hierarchical, usually occurring in large networks
  → Fast convergence of the network is crucial
  → The administrators have good knowledge of the implemented link-state routing protocol

Process

- Each router learns about each of its own directly connected networks
- Each router is responsible for "saying hello" to its neighbor on directly connected networks.
- Each router builds a Link-state-Packet (LSP) containing the state of each directly connected link.
- Each router floods the LSP to all neighbors who then store all LSP's received in database
- Each router uses the database to construct a complete map of the topology and computes the best path to each destination network

Advantage

- Each router builds its own topological map of the network to determine the shortest path
- Immediate flooding of LSPs achieves faster convergence
- LSPs are sent only when there is a change in the topology and contain only the information regarding that change.
- Hierachical design used when implementing multiple areas.

Disadvantage

- Maintaining a link-state database and SPF tree requires additional memory.
- Calculating the SPF algorithm also requires additional CPU processing.
- Bandwidth can be adversely affected by link-state packet flooding.

Database	Table	Description
Adjacency Database	Neighbor Table	• List of all neighbor routers to which a router has established bidirectional communication. • This table is unique for each ~~number~~ router • Can be view → show ip ospf neighbor
Link-State Database (LSDB)	Topology Table	• List information about all other routers in the network • The database shows the network topology • All routers within an area have identical LSDB • Can be viewed → show ip ospf database
Forwarding Database	Routing Table	• List of routes generated when an algorithm is run on the link-state database • Each routers routing table is unique and contains information on how and where to send packets to other routers • can be view → show ip route

OSPF hello packet are transmitted

- To 224.0.0.5 in IPv4, FF02::5 in IPv6
- every 10 seconds (default on multiaccess and point-to-point networks
- every 30 seconds (default on non-broadcast multiaccesses [NBMA] networks)
- Dead interval → period that the routes waits to recieve a Hello message

When an OSPF initially connected to a network, it attemps to

- Create adjacencies with neighbors
- Exchange routing information
- Calculate the best routes
- Reach convergence
- OSPF poogresses through several states while attempting to reach convergence

OSPF cost

cost = reference bandwidth / interface BW (bps)

* reference bandwidth (default) = 10^8 bps

Fast Ethernet	100,000,000 bps
Gigabit Ethernet	1,000,000,000 bps
10 Gigabit Ethernet	10,000,000,000 bps

* default Interface BW = 1.544 Mb/s

• Broadcast Domains
- Broadcast Domain is the extend of the network where a broadcast frame can be heard.
- Switches foorword broadcast frame to all ports. Therefore Switches don't break broadcast domains.
- All port of a switch (with its default configuration) belong to the same broadcast domain
- If two or more switches are connected, broadcasts will be foorword to all switches (except for the port that originally recieved the broadcast.

Dynamic Host Configuration Protocol → provides automatic IP addressing and other information to clients:
↳ uses 3 different address allocation methods
- Manual Allocation → The administrator assigns a pre-allocated IPv4 address to the client, and DHCPv4 communicates only the IPv4 address to the device
- Automatic Allocation → DHCPv4 automatically assigns a static IPv4 address permanently to a device, selecting it from a pool of available address. No lease
- Dynamic Allocation → DHCPv4 dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address. Most commonly used.

LAN design
- Common Considerations → Cost, Port Density, Power, Reliability, Port speed, Frame Buffers, Scalability
- To maximize available LAN BW and Performance → The function and placement of servers
  → Collision detection issues
  → Segmentation issues
  → Broadcast domain issues

• Segmentation is the process of splitting a single collision domain into smaller collision domains.
- Creating smaller collision domains reduces the number of collisions on a LAN segment, and allows for greater utilization of bandwidth.
- Layer 2 devices such as bridges and switches can be used to segment a LAN into smaller collision domain

• Broadcast domain refers to the set of devices that recieve a broadcast data frame originating from any device within that set.
- Processing the broadcast data will consume the resources and available BW of the host
- Layer 2 devices such as bridge and switches reduce the size of a collision domain but do not reduce the size of the broadcast domain
- Routers reduce the size of the collision domain and the size of the broadcast domain at Layer 3

Switched
• Transparent Bridge Process

Recieve Frame
↓
Learn source address / refresh aging timer
↓
Is the destination a broadcast, multicast or unknown unicast?
no ↓ yes → Flood Packet
Are the source & Destination on the same interface?
no ↓ yes → Filter Packet
Foorword unicast to correct port

• Frame Foorwarding
- Store-and-Foorward switching
  → check for errors (via FCS check)
  → perform Automatic Buffering
- slower foorwarding
- Cut-Through Switching
  → start foorwarding in ≈ 10 microseconds
  → No FCS check
  → No Automatic Buffering
  Fast-Forward ~ 12 byte
  Fragment-free ~ 64 byte

Collision Domains
↳ the segment where devices must compete to communicate

- All port of hub belong to the same collision domain
- Every port of a switch is a collision domain on its own
- A switch break the segment into smaller collision domains, easing device competition

ชื่อ-สกุล ศิวกร แก่สุวรรณ์ กระดาษแผ่นที่ 4 รหัสนักศึกษา 68088802

for Staples

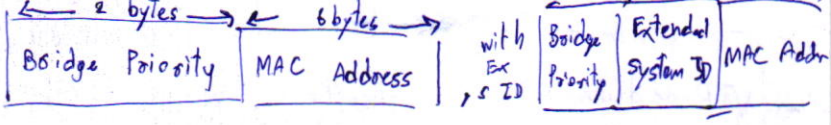
LAN Issues with Layer 1 Redundancy

- MAC database instability
- Broadcast storms
- Multiple frame transmission

Spanning Tree Algorithm

- Root Bridge
- Root ports
- Designated ports
- Non-Designated ports
- Alternate and backup ports

→ Without the Extended System ID



Protocol	standard	Resource Needed	Convergence	Tree Calculation
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

STP Configuration Issue

Analyze STP
↓
Discover Layer 2 Topology
↓
Prepare expected Layer 2 path
↓
Verify root bridge
↓
Confirm Layer 2

PVST+ → Port states and PVST+ Operation

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

VLAN is a logical partition of a Layer 2 Network

- each VLAN is a broadcast domain, usually with its own IP network
- only pass between VLAN through a router

Benefits of VLANs

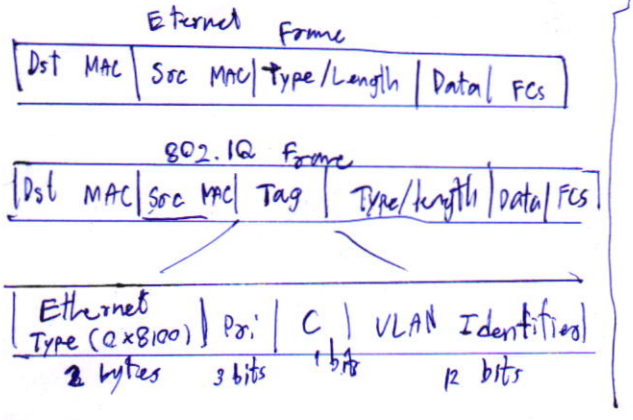
- Improved Security
- Reduced Cost
- Better Performance
- Smaller Broadcast Domains
- IT Efficiency
- Management Efficiency

VLAN Range on Catalyst switches

- V 2960, 3560 supports over 4,000 VLANS
- Normal Range VLAN (1-1005) (vlan.dat) (flash)
- Extend (1006 - 4096) (running-config) (NVRAM)

* VLAN trunk protocol → IEEE 802.1q

Tagging Ethernet frames for VLAN Identification



for Staples

for Staples

- VTP → VLAN Trunking Protocol
  - ↳ uses Layer 2 trunk frames to ~~manage~~ manage the addition, deletion, rename of VLAN
  - ↳ encaped in either Cisco proprietary ISL / IEEE 802.1Q
  - ↳ b4 creating VLANs on the switch, you must 1st set up a VTP manggement domain

- VTP is a Cisco proprietary protocol that allows VLAN configuration to be consistently maintained across a common administrative domain
- VTP minimizes the possible configuration inconsistencies that arise when changes are made
- VTP reduces the complexity of managing & monitoring VLAN network, allow change on one switch to be propagated to other switches via VTP
- On most Cisco switches, VTP is running and has certain defaults already configured

Feature	Server	Client	Transparent
Source VTP Message	Y	Y	N
Listen to VTP message	Y	Y	N
Create VLANs	Y	N	Y
Remember VLANs	Y	N	Y

VTP configuration

1. Determine the version of VTP that will be utilized
2. Decide if this switch is to be a member of an existing manggement domain or if a new domain should be created, If a manggement domain does exist, determine the name / password of the domain
3. choose a VTP mode for the domain

EIGRP is a Cisco-proprietary distance-vector routing protocol released in 1992
- classless version of IGRP

EIGRP Feature

Diffusing Update Algorithm (DUAL)	• EIGRP uses DUAL as its routing algorithm • DUAL guarantee loop free and backup path
Establishing Neighbor Adjacencies	• EIGRP establishes relationships with directly connected EIGRP • adjacent are used to track status of neighbors
Reliable Transport Protocol	• RTP and neighbor adjacencies are used by DUAL

EIGRP uses protocol-dependent modules (PDMs) to support different protocols such as IPv4, IPv6, and legacy protocols IPX and AppleTalk

PDMs are responsible for : • Maintain EIGRP neighbor and topology tables
• Computing the metric using DUAL
• Performing redistribution with other routing protocols

- RTP is the EIGRP Transport layer protocols used for the delivery and reception of EIGRP packet
- Auten does not encrypt the EIGRP routing updates

Packet Type	Used to..
Hello	Discover other EIGRP routers in the network
Update	Convey routing information to known destinations
Acknowledgement	Acknowledge the recipt of any EIGRP packet
Query	Request specitic information from a neighbor router
Reply	Respond to a query

EIGRP use multicast and unicast rather than broadcast
- As result, end stations are unaffected by routing updates or queries
- EIGRP multicast IPV4 is 224.0.0.10
- IPV6 is FF02::A

Autonomous System is a collection of networks under the control of a single authority (RFC 1930)

AS numbers are usually 16 bit, ranging from 0 - 65535
since 2007, AS numbers can now be 32 bits

EIGRP Operation

1. Router R1 starts has joined the EIGRP routing domain and sends an EIGRP Hello packet out all EIGRP enabled interfaces
2. Router R2 recieves the Hello packet and adds R1 to its neighbor table
   - R2 sends an update packet that contain all the route it knows
   - R2 also sends an EIGRP Hello packet to R1
3. R1 updates its neighbor table with R2

1. R1 adds all update from R1 (topology table)
2. updates packets are reliable delivery: therefore, R1 replies with an EIGRP acknowledgment packet informing R2 that it recieved updates
3. R1 send an update to R2 (except those learned from R2; (split horizon)
4. R2 recieves update from R1
5. R2 send ack to R1

1. R1 uses DUAL to calculate the best route to each destination
2. R2 uses DUAL like R1

BW - (in kb/s)
DLY - Delay of the interface (in microseconds)
Reliability - of 255 (255/255 is 100% reliability)
Tx load, Rx load - over 5 minutes

Metric = (Bandwidth + Delay) x 256

Command

ipv6 unicast-routing # global config mode command enables IPv6 routing on the router
ipv6 router eigrp
ipv6 router-id router-id 2.0.0.0
no shutdown