

# Basic Switch Address Resolution Protocol

Jirasak Sittigorn

Internetworking Standards & Technologies

Department of Computer Engineering, Faculty of Engineering  
King Mongkut's Institute of Technology Ladkrabang

Cisco Networking Academy<sup>®</sup>  
Mind Wide Open<sup>™</sup>

- Introduction to Switch Network

- LAN Design

- The Switched Environment

- Switching Domains

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

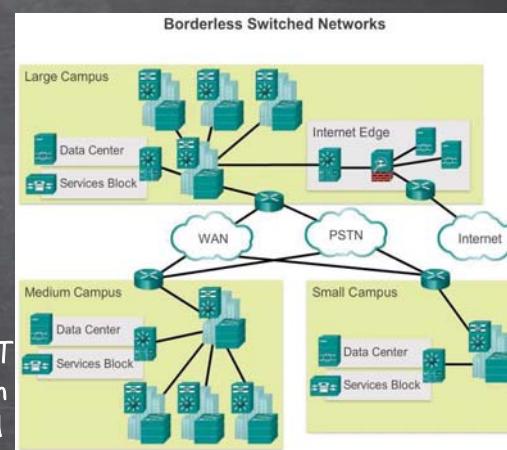
2

## LAN Design

- Borderless Switched Networks

— Cisco Borderless Network is a network architecture that allow organizations to connect anyone, anywhere, anytime, and on any device securely, reliably, and seamlessly

— It is designed to address IT and business challenges, such as supporting the converged network and changing work patterns



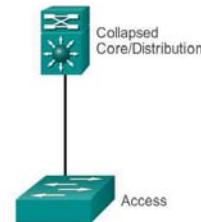
## LAN Design

- Borderless switched network design guidelines are built upon the following principles:

- Hierarchical
- Modularity
- Resiliency
- Flexibility



Three-Tier LAN Design



Two-Tier LAN Design

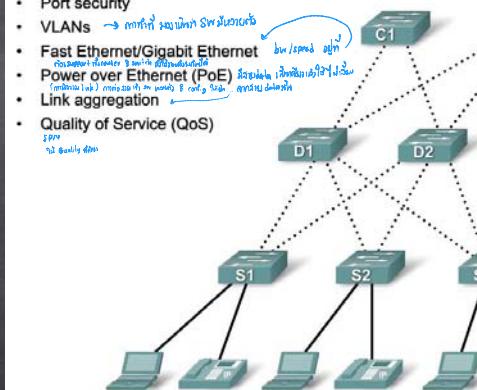
# LAN Design

## Access Layer Switch Features

ผู้ใช้งาน Device

Layer 2

- Port security
- VLANs → แบ่งช่องทางสู่ผู้ใช้งาน
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE) สนับสนุนไฟฟ้าผ่านสายสำหรับอุปกรณ์ที่ต้องการไฟ เช่น กล้องวงจรปิด
- Link aggregation
- Quality of Service (QoS)



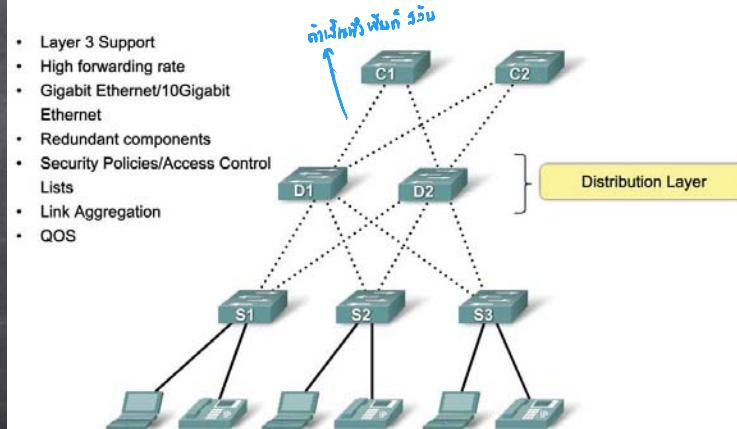
# LAN Design

## Distribution Layer Switch Features

ผู้ใช้งาน Access Layer Core L.

ผู้ใช้งานชั้นที่ 3

- Layer 3 Support
- High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components
- Security Policies/Access Control Lists
- Link Aggregation
- QoS

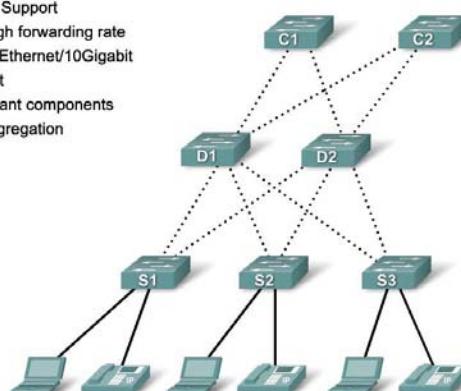


# LAN Design

## Core Layer Switch Features

ผู้ใช้งานชั้นที่ 3

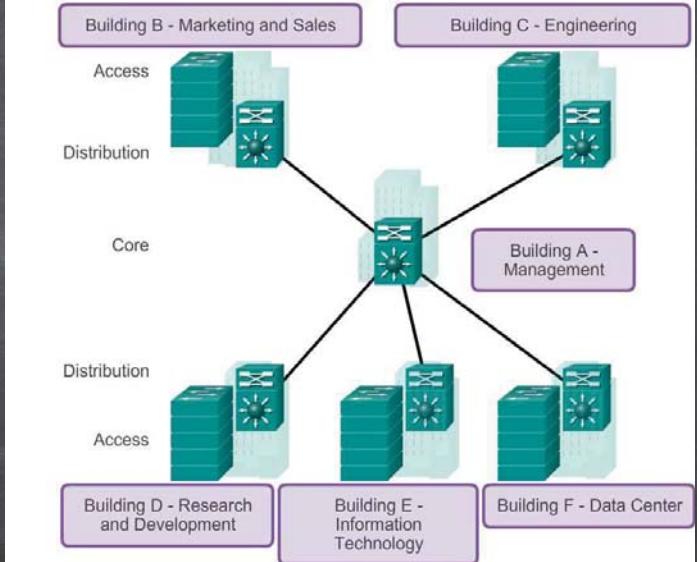
- Layer 3 Support
- Very High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components
- Link Aggregation
- QoS



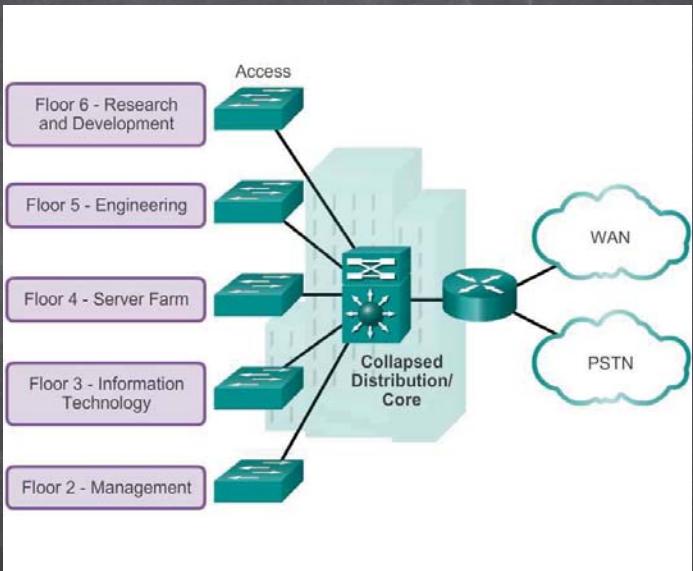
Ex สถาปัตยกรรมเครือข่าย

# LAN Design

## Building Block Diagram



# LAN Design



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

9

# LAN Design

**Common Business Considerations When Selecting Switch Equipment:**

- Cost** - The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- Port Density** - Network switches must support the appropriate number of devices on the network.
- Power** - It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
- Reliability** - The switch should provide continuous access to the network.
- Port Speed** - The speed of the network connection is of primary concern to end users.
- Frame Buffers** - The ability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
- Scalability** - The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

**Fixed Configuration Switches**  
SW independent port partitioning  
module fiber optic = 150Mbit

**Modular Configuration Switches**

**Stackable Configuration Switches**  
Stacked stack Master

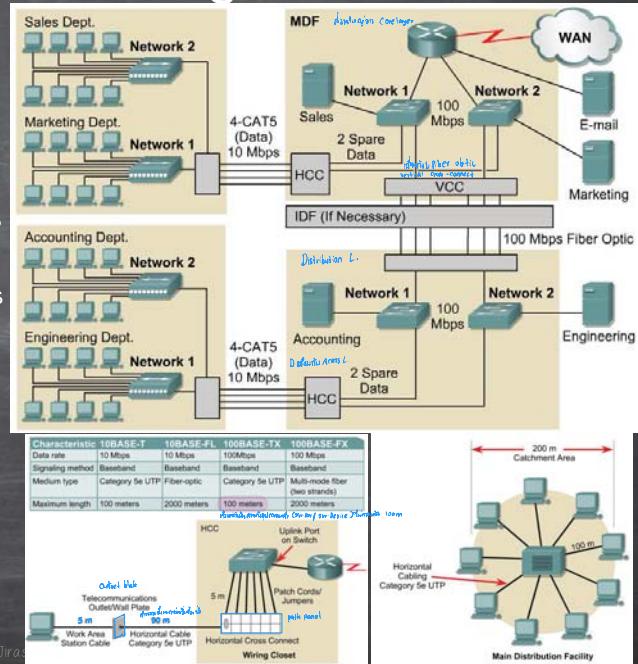
Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

Server - enterprise  
- web server  
- database server  
- mail server

- work group  
- desktop computer  
- client PC

- To maximize available LAN bandwidth and performance:
  - The function and placement of servers
    - Enterprise servers
    - Workgroup servers
  - Collision detection issues
  - Segmentation issues
  - Broadcast domain issues

# LAN Design



MDF : Main Distribution Facility

IDF : Intermediate Distribution Facility

VCC : Vertical cross-connect

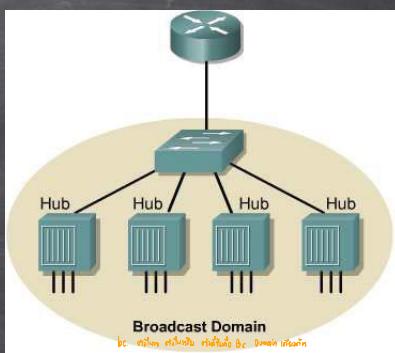
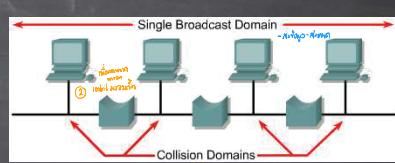
HCC : Horizontal cross-connect

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

# LAN Design



- 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 domains.
- A broadcast domain refers to the set of devices that receive a broadcast data frame originating from any device within that set.
  - Processing the broadcast data will consume the resources and available bandwidth of the host.
  - Layer 2 devices such as bridges 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.



12

# The Switched Environment

- Switch Operation

Learning

learn src addr (mac)  
move to learned port then

Aging

periodic learn src mac  
mac address aging off timer CFC 5 sec. store & forward function

Flooding

look up table to forward message  
if found destination  
1 broadcast  
2 unicast  
3 unknown unicast  
4 unknown dest

Forwarding

as mac address learning, start transmission

Filtering

mac address

Switchable into mac 21  
move addr table  
src addr table  
CAM

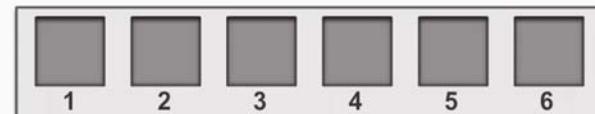
Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

13

# The Switched Environment

- Switching

~~LAN Switch~~



Port Table

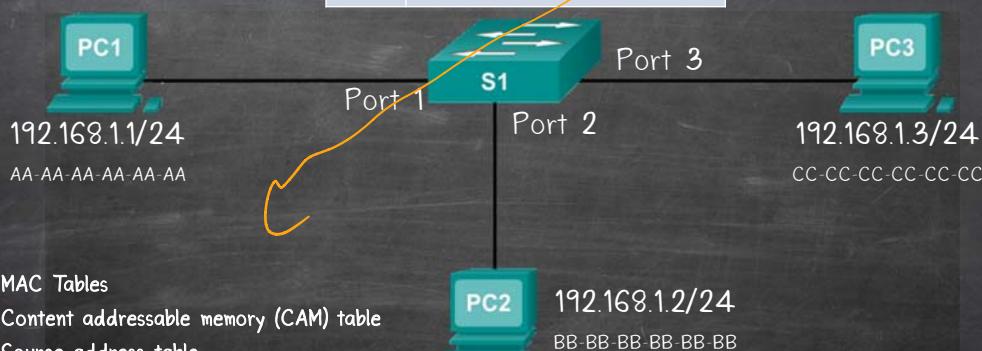
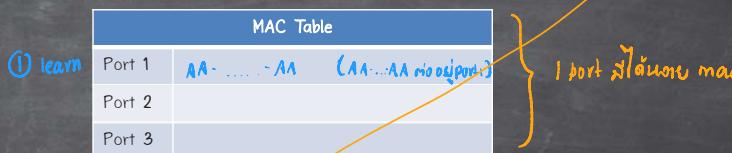
Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

14

# The Switched Environment

- MAC Addressing & Switch MAC Tables



15

# The Switched Environment

การพัฒนาการเชื่อมต่อ SW

- Transparent Bridge Process - Jeff Doyle

Receive Frame

Learn source address or refresh aging timer

9.5 type mac

Is the destination a broadcast, multicast or unknown unicast?

No → Flood Packet

del port ที่ส่ง

Are the source and destination on the same interface?

No → Filter Packet

ด้วยวิธี

Forward unicast to correct port

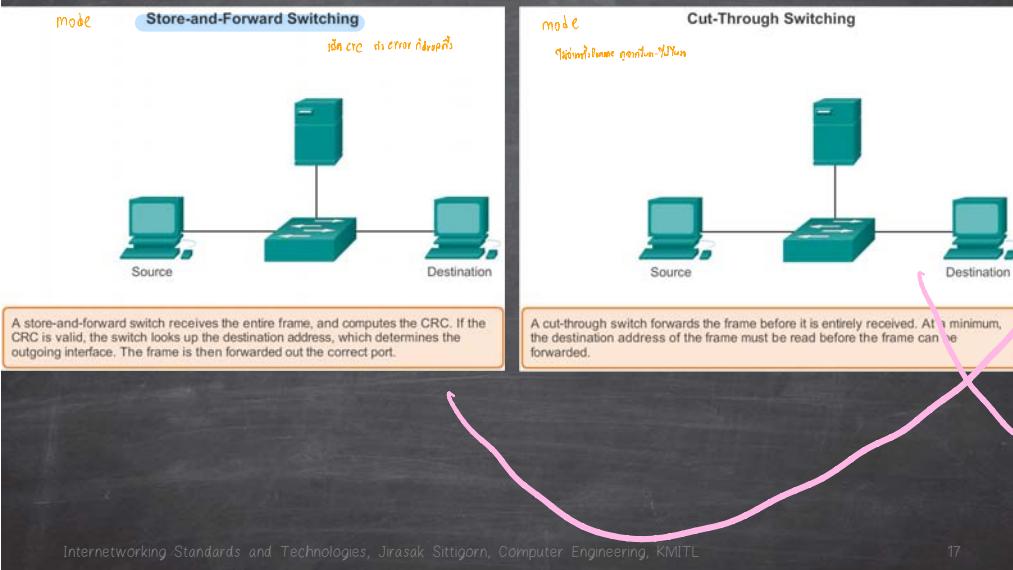


Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

16

# The Switched Environment

- Switch Forwarding Methods



17

# The Switched Environment

- Frame Forwarding

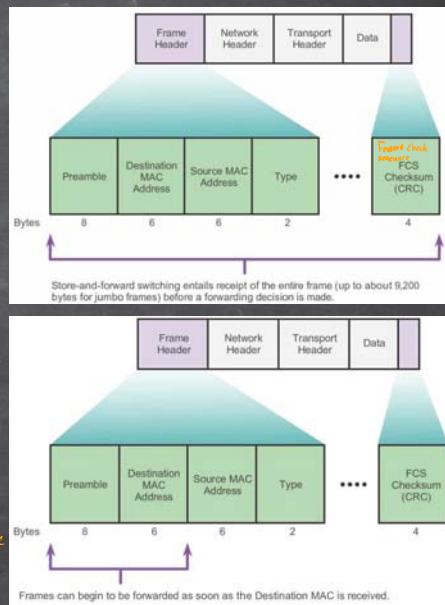
  - Store-and-Forward Switching

    - Store-and-Forwarding allows the switch to:
      - Check for errors (via FCS check)
      - Perform Automatic Buffering
    - Slower forwarding

  - Cut-Through Switching

    - Cut-Through allows the switch to start forwarding in about 10 microseconds
    - No FCS check
    - No Automatic Buffering

Fast-forward ~ 12 bytes      Src mac & dest mac  
Fragment-free ~ 64 bytes  
dst MAC address found in hardware table

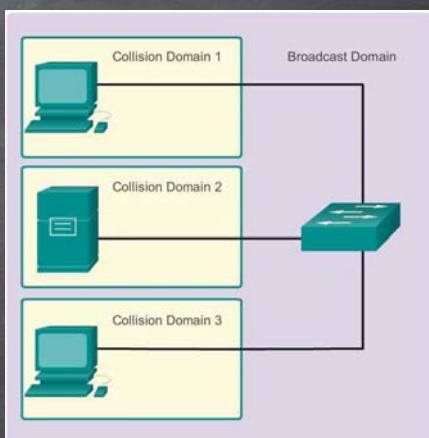


18

## Switching Domains

- Collision Domains

  - Collision domain is the segment where devices must compete to communicate
  - All ports of a 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.

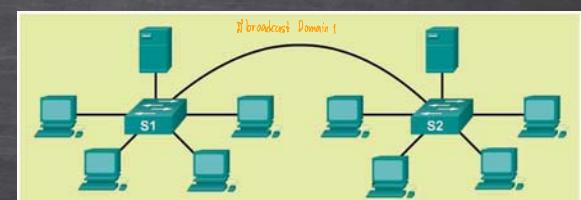
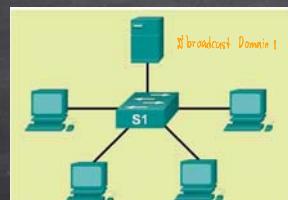


19

## Switching Domains

- Broadcast Domains

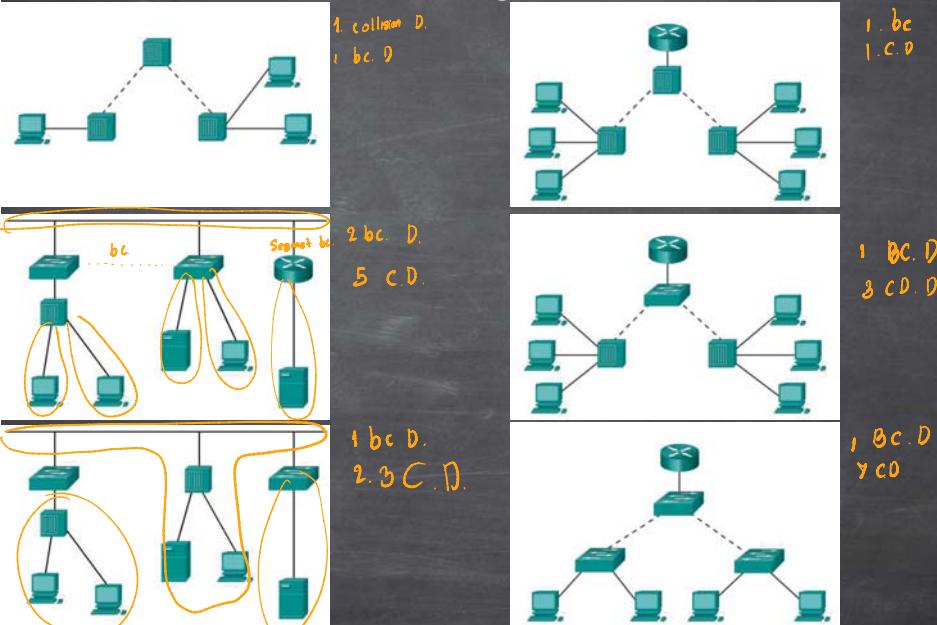
  - Broadcast domain is the extend of the network where a broadcast frame can be heard.
  - Switches forward broadcast frames to all ports. Therefore switches don't break broadcast domains.
  - All ports of a switch (with its default configuration) belong to the same broadcast domain
  - If two or more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



20

# Switching Domains

1 SW 1 port = 1 CD



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

21

## • Basic Switch Concept & Configuration

### • Basic Switch Configuration

- Switch Boot Sequence
- Preparing for Basic Switch Management
- Configure Switch Ports
- Switch Security : Security Remote Access
- Switch Port Security

{  
min main router  
}

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

22

# Switch Boot Sequence

conceptualization

- POST
- Run boot loader software
- Boot loader does low-level CPU initialization
- Boot loader initializes the flash filesystem
- Boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

23

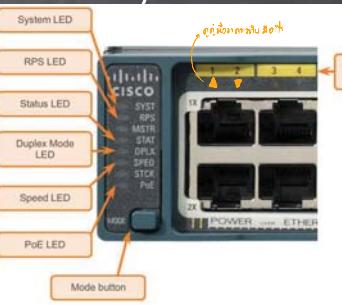
# Switch Boot Sequence

- In order to find a suitable IOS image, the switch goes through the following steps:
  - It attempts to automatically boot by using information in the BOOT environment variable
  - If this variable is not set, the switch performs a top-to-bottom search through the flash file system. It will load and execute the first executable file, if it can.
  - The IOS operating system then initializes the interfaces using the Cisco IOS commands found in the configuration file, startup configuration, which is stored in NVRAM.
- Note: the command `boot system` can be used to set the BOOT environment variable.

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

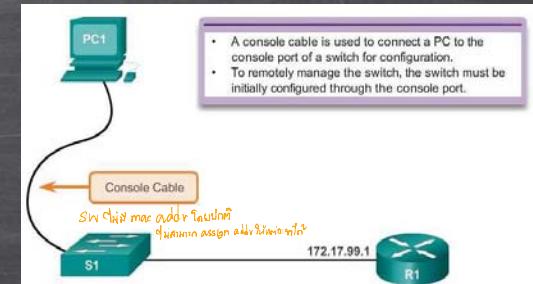
24

# Switch LED Indicators

- Each port on Cisco Catalyst switches have status LED indicator lights.
  - By default these LED lights reflect port activity but they can also provide other information about the switch through the Mode button
  - The following modes are available on Cisco Catalyst 2960 switches:
    - System LED
    - Redundant Power System (RPS) LED
    - Port Status LED
    - Port Duplex LED
    - Port Speed LED
    - Power over Ethernet (PoE) Mode LED
- 

# Preparing for Basic Switch Management

- In order to remotely manage a Cisco switch, it needs to be configured to access the network
- An IP address and a subnet mask must be configured
- If managing the switch from a remote network, a default gateway must also be configured
- The IP information (address, subnet mask, gateway) is to be assigned to a switch SVI (switch virtual interface) กำหนดค่า config
- Although these IP settings allow remote management and remote access to the switch, they do not allow the switch to route Layer 3 packets.



# Preparing for Basic Switch Management

## Configure Switch Management Interface

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode for the SVI.	S1(config)# interface vlan 99 <small>ตรวจสอบแล้วต้องเป็นช่องที่มีอยู่แล้ว</small>
Configure the management interface IP address.	S1(config-if)# ip address 172.17.99.11 255.255.0.0 <small>ตรวจสอบแล้วต้องเป็นช่องที่มีอยู่แล้ว</small>
Enable the management interface.	S1(config-if)# no shutdown
Return to the privileged EXEC mode.	S1(config-if)# end
Save the running config to the startup config.	S1# copy running-config startup-config

## Verify Switch Management Interface Configuration

Cisco Switch IOS Commands	
	S1# show running-config

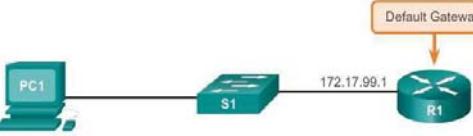
```

...
interface FastEthernet0/18
switchport access vlan 99
switchport mode access
...
<output omitted>

```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan99	172.17.99.11	YES	manual	up	up
FastEthernet0/18	unassigned	YES	unset	up	up

## Configure Switch Default Gateway

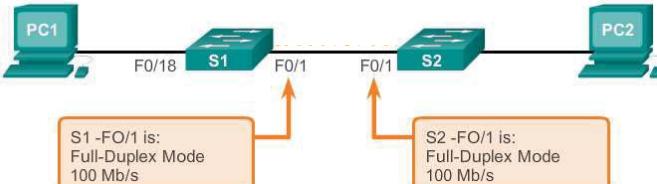


# Configure Switch Ports

- Duplex Communication



## Configure Duplex and Speed



## Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1(config)# interface fastethernet 0/1
Configure the interface duplex.	S1(config-if)# duplex full
Configure the interface speed.	S1(config-if)# speed 100
Return to the privileged EXEC mode.	S1(config-if)# end
Save the running config to the startup config.	S1# copy running-config startup-config

# Configure Switch Ports

- Auto-MDIX

Enable auto-MDIX

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1(config)# interface fastethernet 0/1
Configure the interface to autonegotiate duplex with the connected device.	S1(config-if)# duplex auto
Configure the interface to autonegotiate speed with the connected device	S1(config-if)# speed auto
Enable auto-MDIX on the interface.	S1(config-if)#mdix auto <i>(Screenshot note: 2nd argument is missing)</i>
Return to the privileged EXEC mode.	S1(config-if)#end
Save the running config to the startup config.	S1#copy running-config startup-config

# Configure Switch Ports

- Verifying Switch Port Configuration

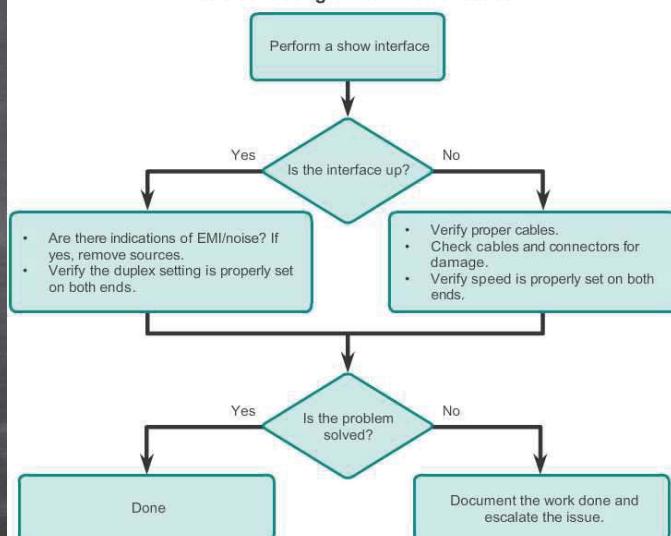
## Verification Commands

### Cisco Switch IOS Commands

Display interface status and configuration.	S1# show interfaces [interface-id]
Display current startup configuration.	S1# show startup-config
Display current operating config.	S1# show running-config
Displays info about flash filesystem.	S1# show flash
Displays system hardware & software status.	S1# show version
Display history of commands entered.	S1# show history
Display IP information about an interface.	S1# show ip [interface-id]
Display the MAC address table.	S1# show mac-address-table

# Configure Switch Ports

### Troubleshooting Switch Media Issues

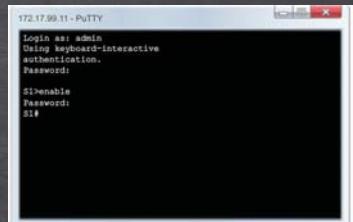


# Security Remote Access

Telnet *Warning: encrypt min password  
+-----+ encrypt*

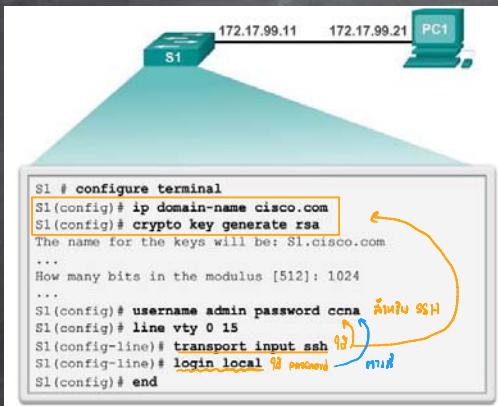
- SSH Operation

- Secure Shell (SSH) is a protocol that provides a secure (encrypted) command-line based connection to a remote device
- SSH is commonly used in UNIX-based systems
- Cisco IOS also supports SSH
- A version of the IOS software including cryptographic (encrypted) features and capabilities is required in order to enable SSH on Catalyst 2960 switches
- Because its strong encryption features, SSH should replace Telnet for management connections
- SSH uses TCP port 22 by default.  
Telnet uses TCP port 23



# Security Remote Access

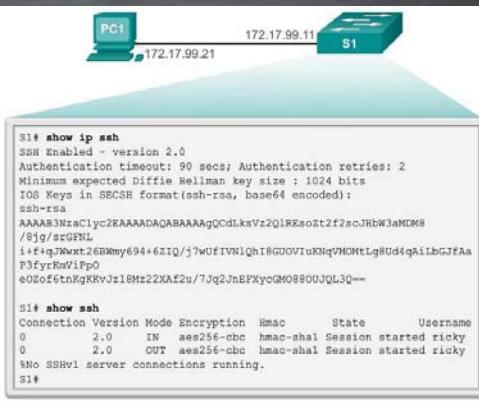
## • Configuring SSH



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL



## • Verifying SSH



33

# Switch Port Security

การตั้งค่า

## • Operation : Secure MAC Address Types

### ① — Static secure MAC addresses

- MAC addresses that are manually configured on a port by using the **switchport port-security mac-address mac-address** interface configuration mode command.

### ② — Dynamic secure MAC addresses

- MAC addresses that are dynamically learned and stored only in the address table by using **switchport port-security mac-address sticky** interface configuration mode command.

### — Sticky secure MAC addresses

- MAC addresses that can be dynamically learned or manually configured, then stored in the address table and added to the running configuration.

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

34

# Switch Port Security

การตั้งค่า 9 ข้อความยุบรวม

- Violation mode :** IOS considers a security violation when either of these situations occurs:
  - The maximum number of secure MAC addresses for that interface have been added to the CAM, and a station whose MAC address is not in the address table attempts to access the interface.
  - An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.
- There are three possible action to be taken when a violation is detected:

Security violation modes include: Protect, Restrict, and Shutdown.

Security Violation Modes					
Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes กรณี log / counter 0	No	Yes	No
Shutdown	No	No	No	Yes	Yes

กรณี log / counter 0  
กรณี log / counter 0

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

35

# Switch Port Security

## Port Security Defaults

Feature	Default Setting
Port security	Disabled on a port สร้างเมื่อท่าน开启了 port security
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded. default
Sticky address learning	Disabled

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

36

# Switch Port Security Config

①, ④ *normal access mode*

- Static secure MAC addresses

① Switch(config-if)#switchport mode access  
 ② Switch(config-if)#switchport port-security  
 ③ Switch(config-if)#switchport port-security mac-address MAC-ADD

- Dynamic secure MAC addresses *monitoring with dynamic default 1 mac*

① Switch(config-if)#switchport mode access  
 ② Switch(config-if)#switchport port-security  
 ③ Switch(config-if)#switchport port-security mac-address sticky

- Maximum MAC addresses

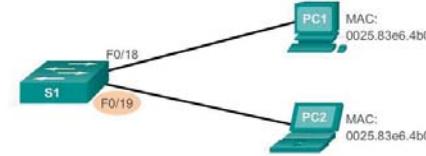
Switch(config-if)#switchport port-security maximum MAX

- Violation mode *(เมื่อเกินจำนวนที่กำหนด)*

Switch(config-if)#switchport port-security violation ?

protect Security violation protect mode  
 restrict Security violation restrict mode  
 shutdown Security violation shutdown mode

# Switch Port Security



```
S1# show port-security interface fastethernet 0/19
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 50
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

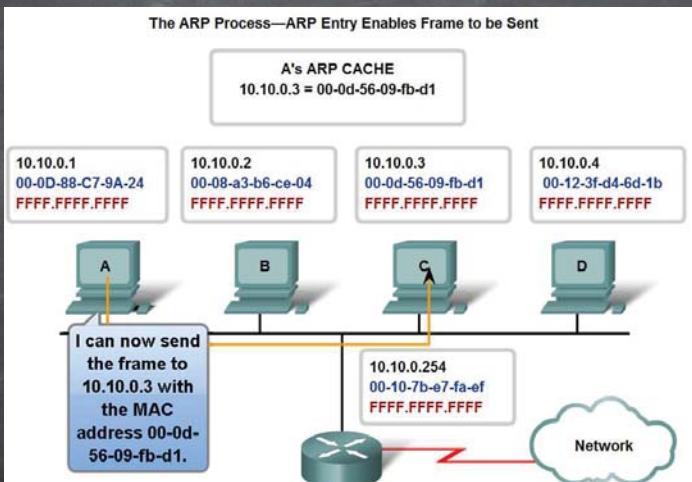
Cisco IOS CLI Commands				
Switch(config)#interface fastethernet 0/18	Specify the interface to be configured for port security.			
Switch(config-if)#switchport mode access	Set the interface mode to access.			
Switch(config-if)#switchport port-security	Enable port security on the interface.			
Switch(config-if)#switchport port-security maximum 50	Set the maximum number of secure addresses allowed on the port.			
Switch(config-if)#switchport port-security mac-address sticky	Enable sticky learning.			
Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	0025.83e6.4b01	SecureDynamic	Fa0/18	-
1	0025.83e6.4b02	SecureSticky	Fa0/19	-

Total Addresses in System (excluding one mac per port) : 0  
 Max Addresses limit in System (excluding one mac per port) : 0

# Address Resolution Protocol Animation

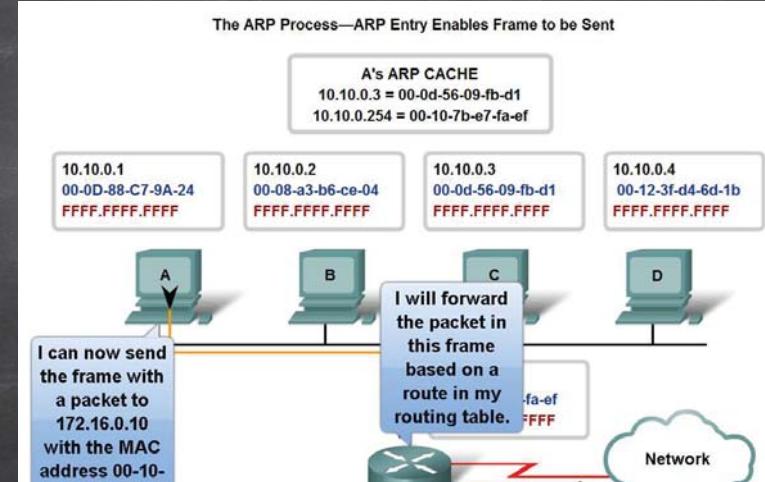
①

- Mapping IP to MAC Addresses



# Address Resolution Protocol

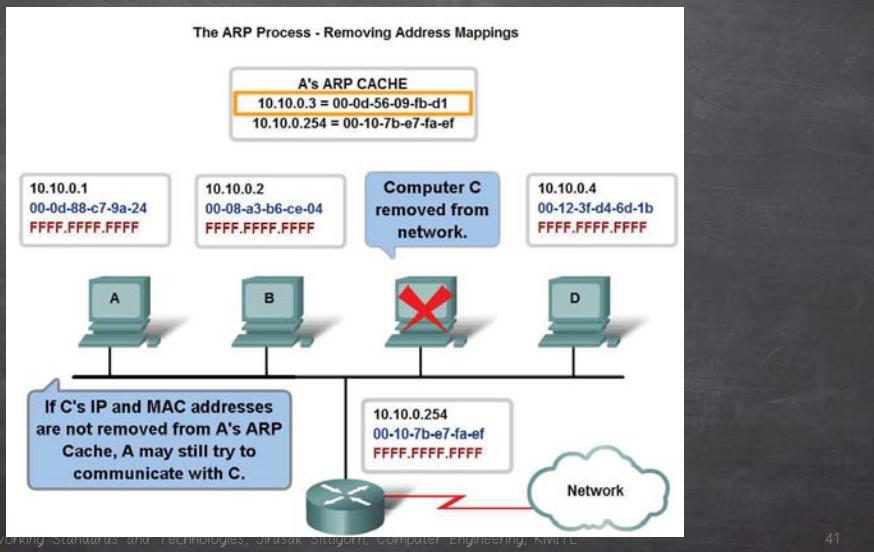
- ARP - Destinations Outside the Local Network



3

# Address Resolution Protocol

- ARP - Removing Address Mappings

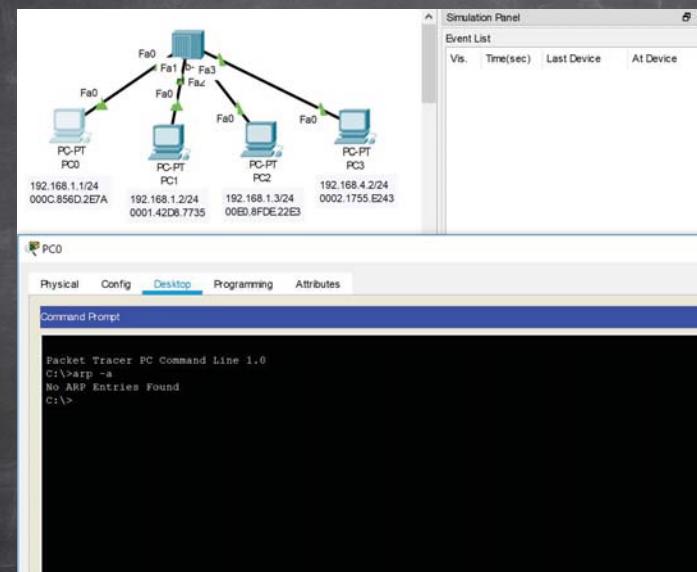


Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

cisco

4

# Address Resolution Protocol

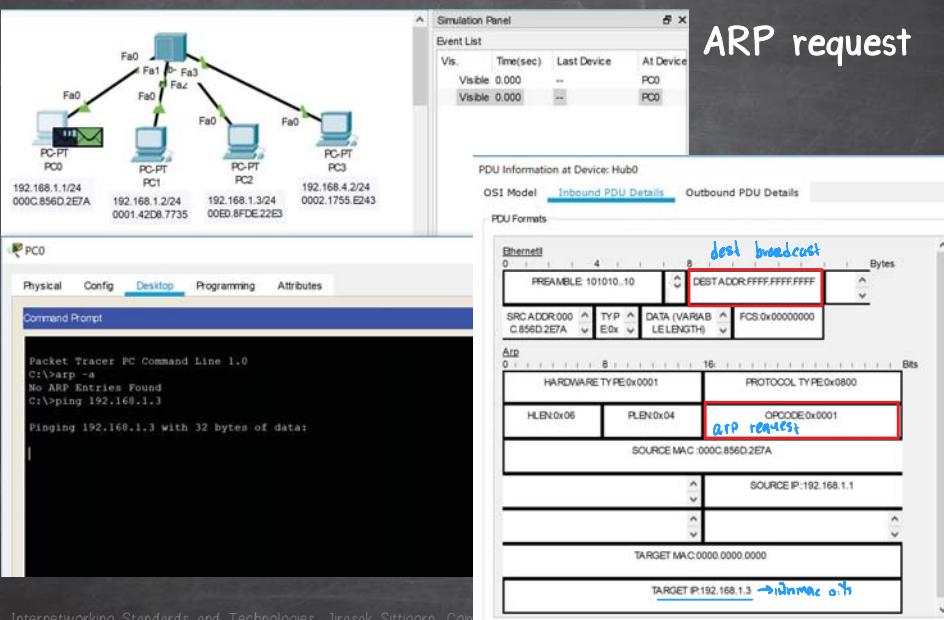


Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

cisco

5

# Address Resolution Protocol

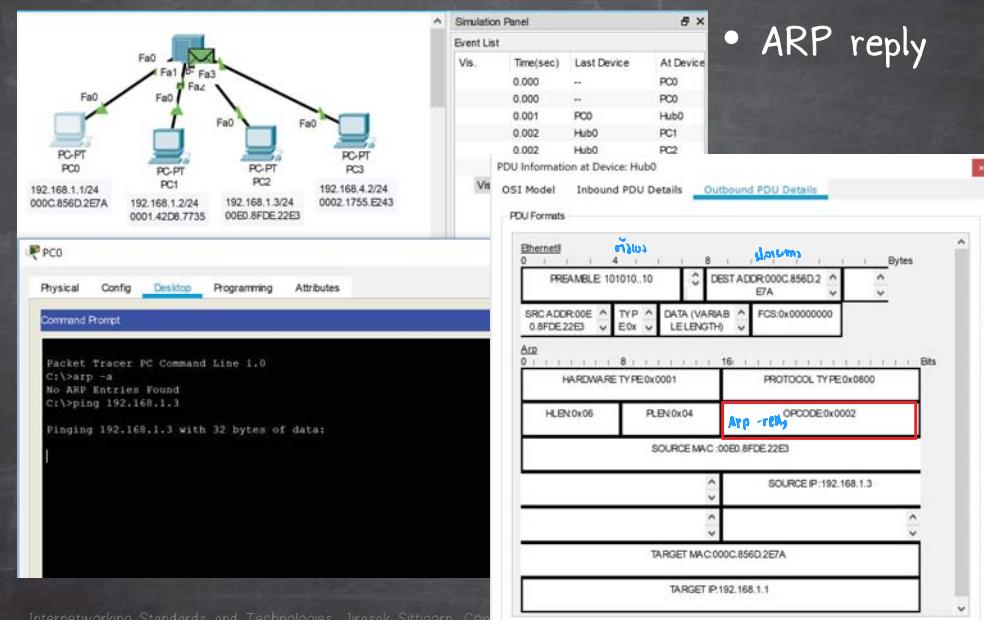


Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

6

# Address Resolution Protocol

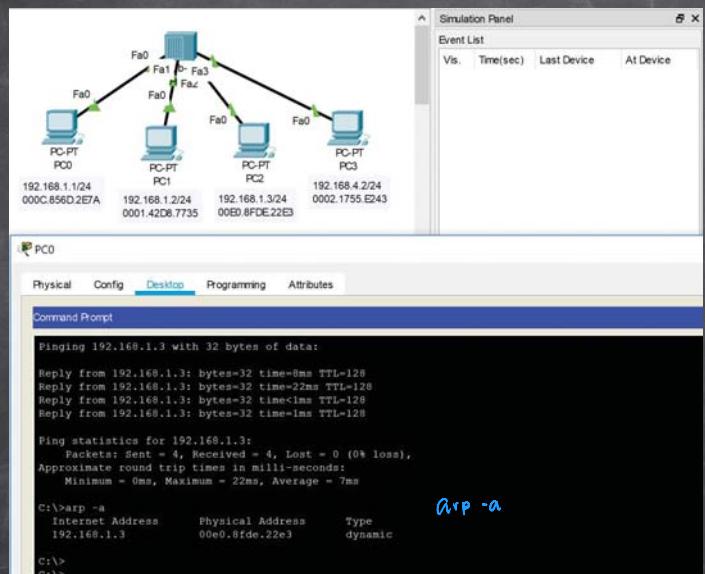
- ARP reply



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

cisco

# Address Resolution Protocol

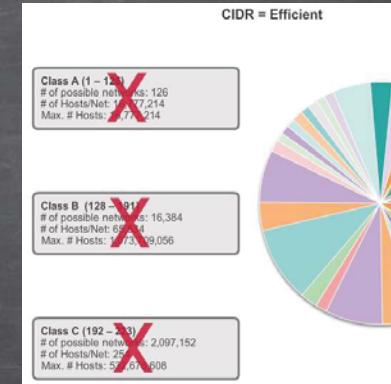
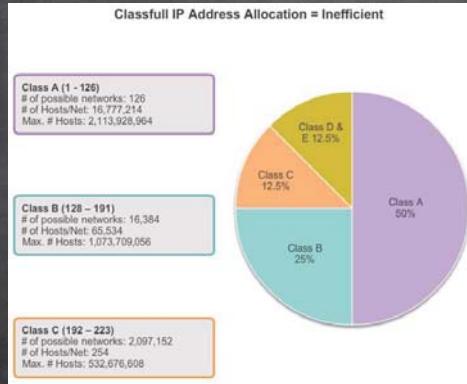


Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

45

# IPv4

- Classful Addressing Waste



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

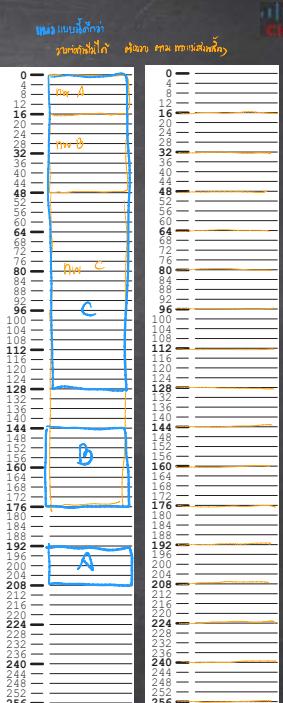
46

Ex VI.

IPv4

- Classless Inter-Domain Routing
  - Fixed Length Subnet Masking (CLM) ຕົວເລີກຕົວ
  - Variable Length Subnet Masking

Subnet Mask	CIDR Value
255.0.0.0	/8
255.128.0.0	/9
255.192.0.0	/10
255.224.0.0	/11
255.240.0.0	/12
255.248.0.0	/13
255.252.0.0	/14
255.254.0.0	/15
255.255.0.0	/16
255.255.128.0	/17
255.255.192.0	/18
255.255.224.0	/19
255.255.240.0	/20
255.255.248.0	/21
255.255.252.0	/22
255.255.254.0	/23
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31 Not valid



ຫຼັບພັກງົດ ອາກມໍານອກງານໂຄດໂນໂອຣຸນ

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

47

# Subnet Planning

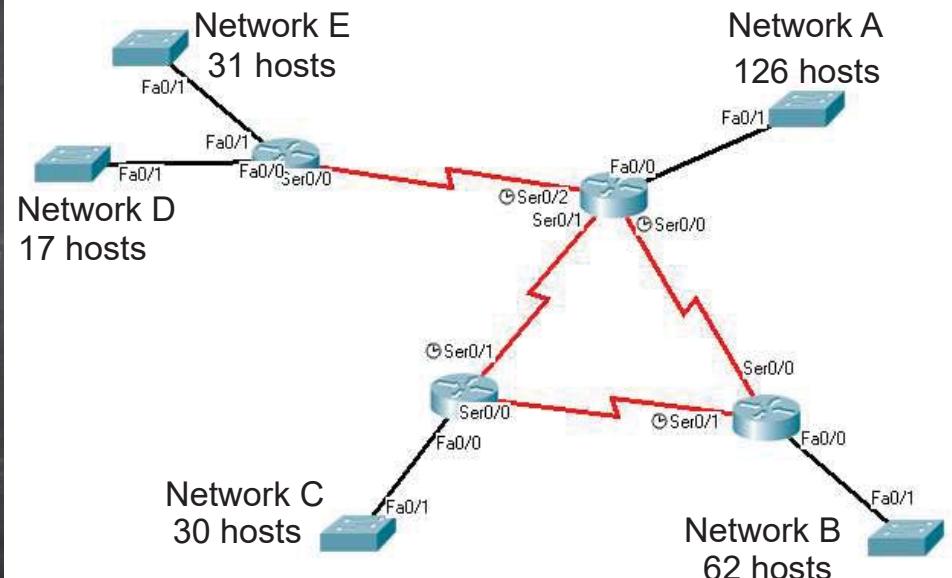
- Network 161.246.6.0/23
  - IP Address 161.246.6.0
  - IP Address 161.246.6.1
  - ...
  - IP Address 161.246.6.255
  - IP Address 161.246.7.1
  - IP Address 161.246.7.2
  - ...
  - IP Address 161.246.7.255

512 IP Address

Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

48

## Subnet Planning



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

49

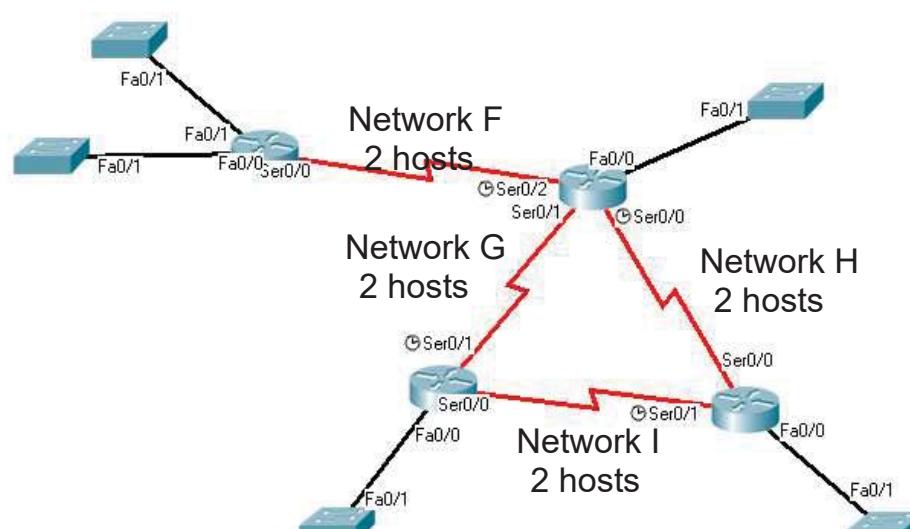
## Subnet Planning

Network	Req. Host	Max. Host	Subnetwork	Subnet mask
A	126	126 (128)		255.255.255.128
B	62	62 (64)		255.255.255.192
C	30	30 (32)		255.255.255.224
D	17	30 (32)		255.255.255.192
E	31	62 (64)		255.255.255.192

50

50

## Subnet Planning



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

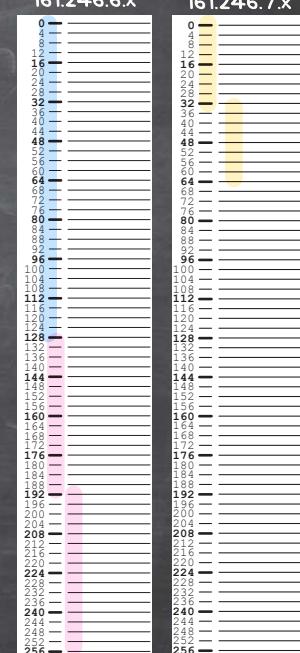
51

## Subnet Planning

Network	Req. Host	Max. Host	Subnetwork	Subnet mask
A	126			
B	62			
C	30			
D	17			
E	31			
F				
G				
H				
I				

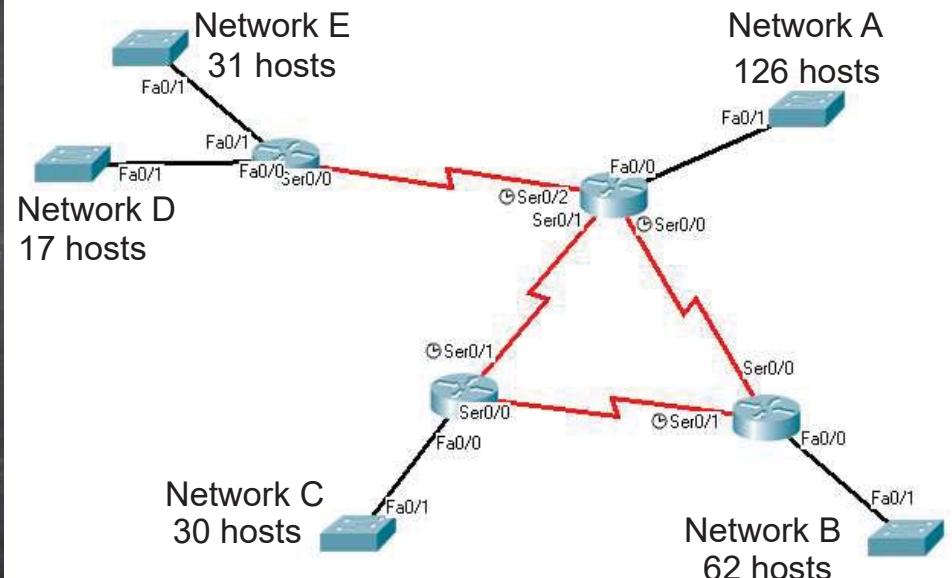
161.246.6.x

161.246.7.x



52

## Subnet Planning



Internetworking Standards and Technologies, Jirasak Sittigorn, Computer Engineering, KMITL

49

## Subnet Planning

Network	Req. Host	Max. Host	Subnetwork	Subnet mask
A	126			
B	62			
C	30			
D	17			
E	31			

