



Basic Switch Address Resolution Protocol

Jirasak Sittigorn

Internetworking Standards & Technologies

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

- Introduction to Switch Network

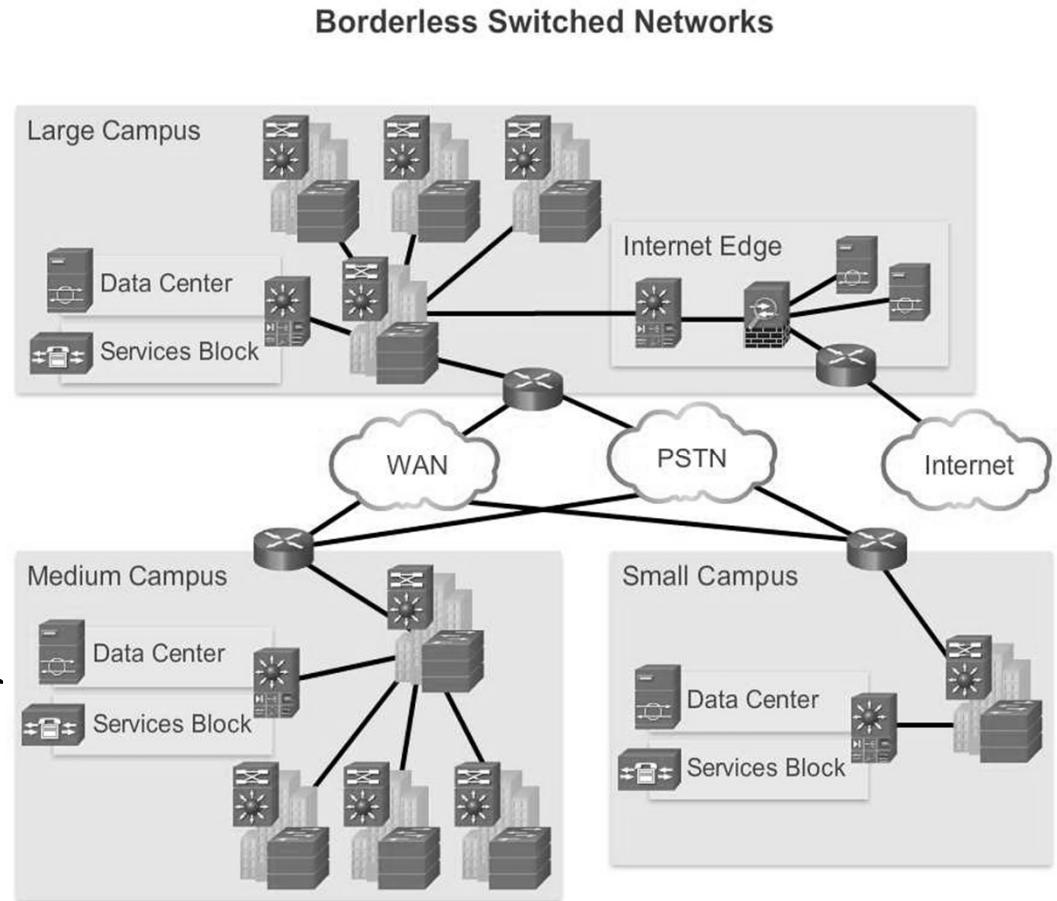
- LAN Design
- The Switched Environment
- Switching Domains

LAN Design

→ Cisco has switch network
switch analysis

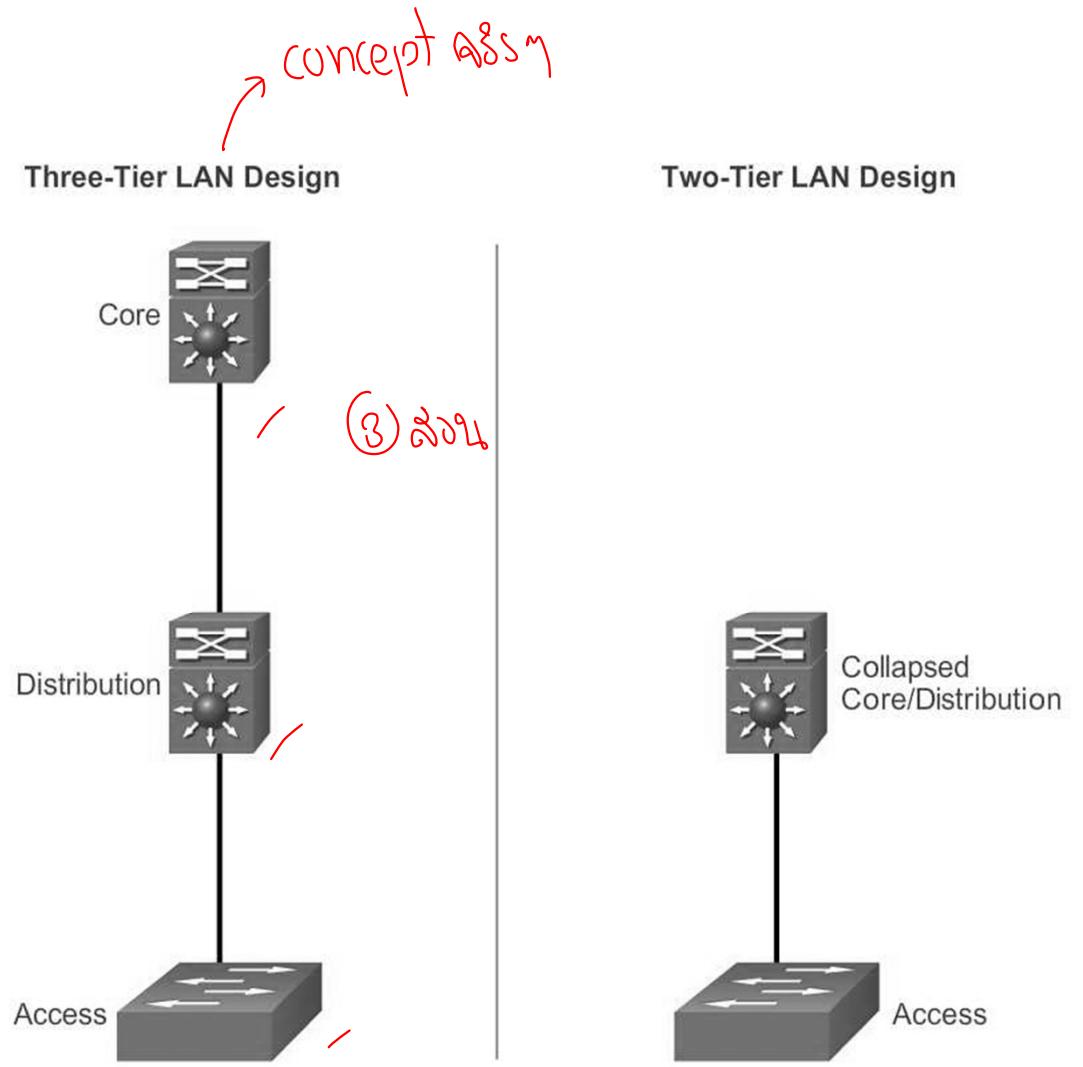
- Borderless Switched Networks

- 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

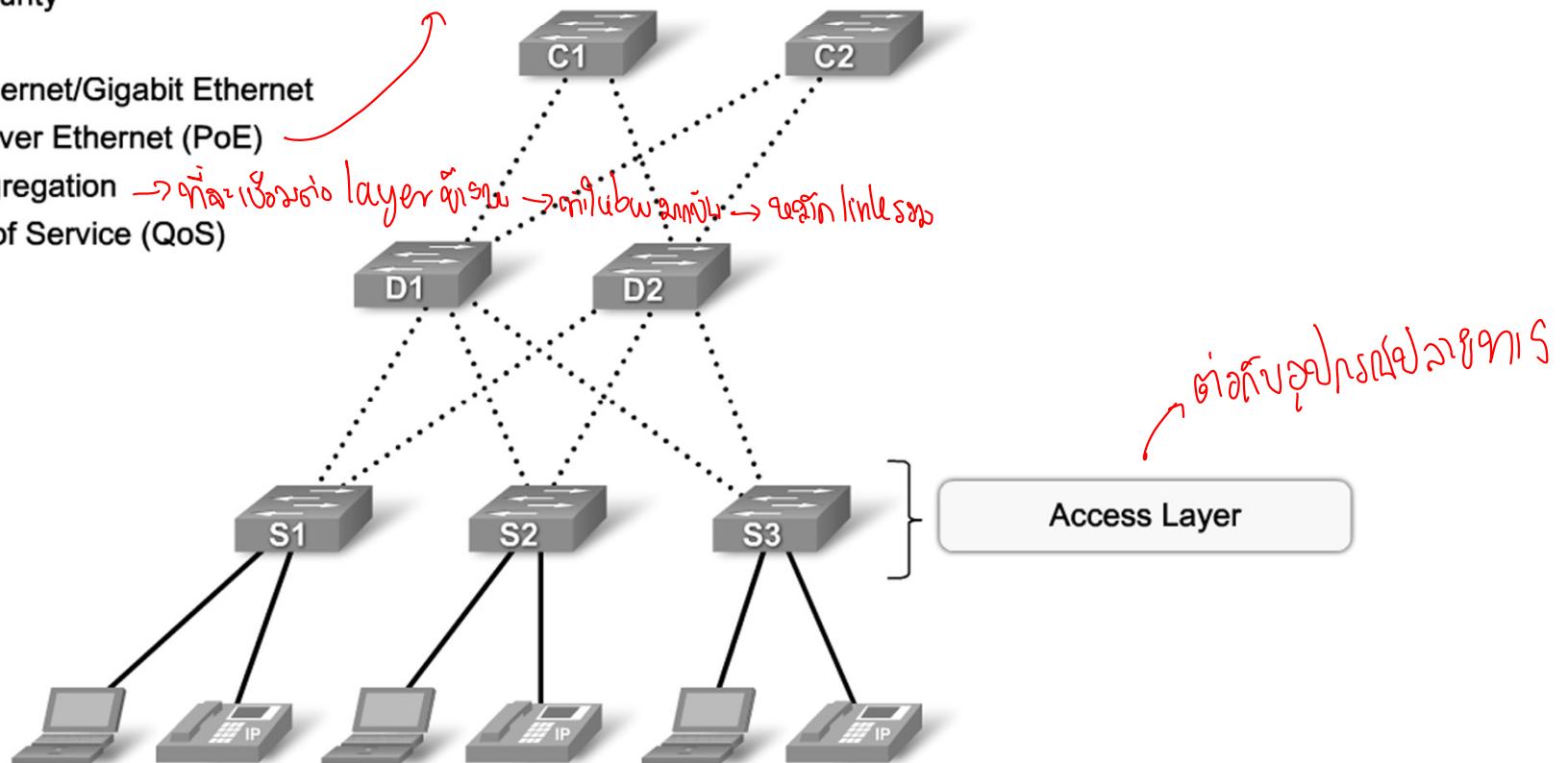
- Borderless switched network design guidelines are built upon the following principles:
 - Hierarchical
 - Modularity
 - Resiliency
 - Flexibility



LAN Design

Access Layer Switch Features

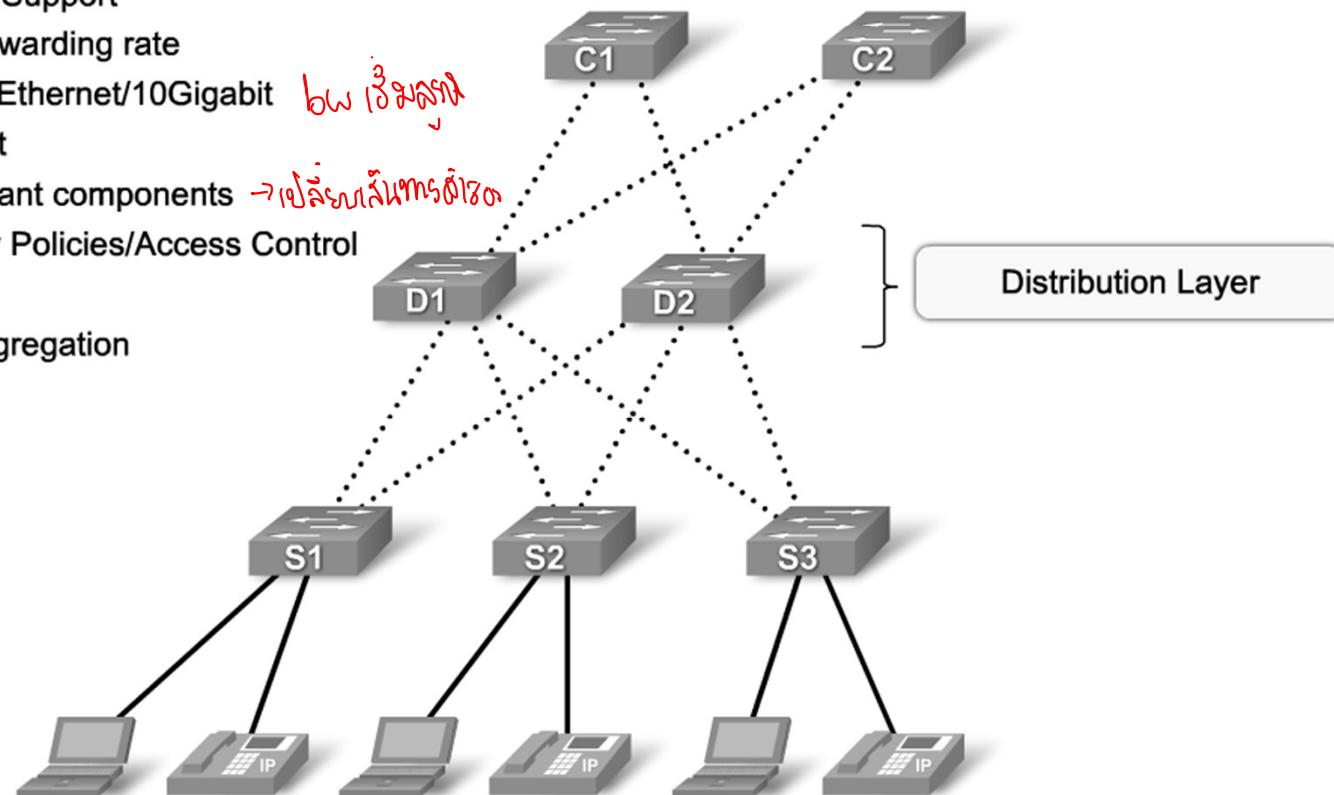
- Port security
- VLANs
- Fast Ethernet/Gigabit Ethernet
- Power over Ethernet (PoE)
- Link aggregation → ពីរបែងចែក layer នេះ → ពិនិត្យវាមួយ → រួមទាំង link សៅ
- Quality of Service (QoS)



LAN Design

Distribution Layer Switch Features

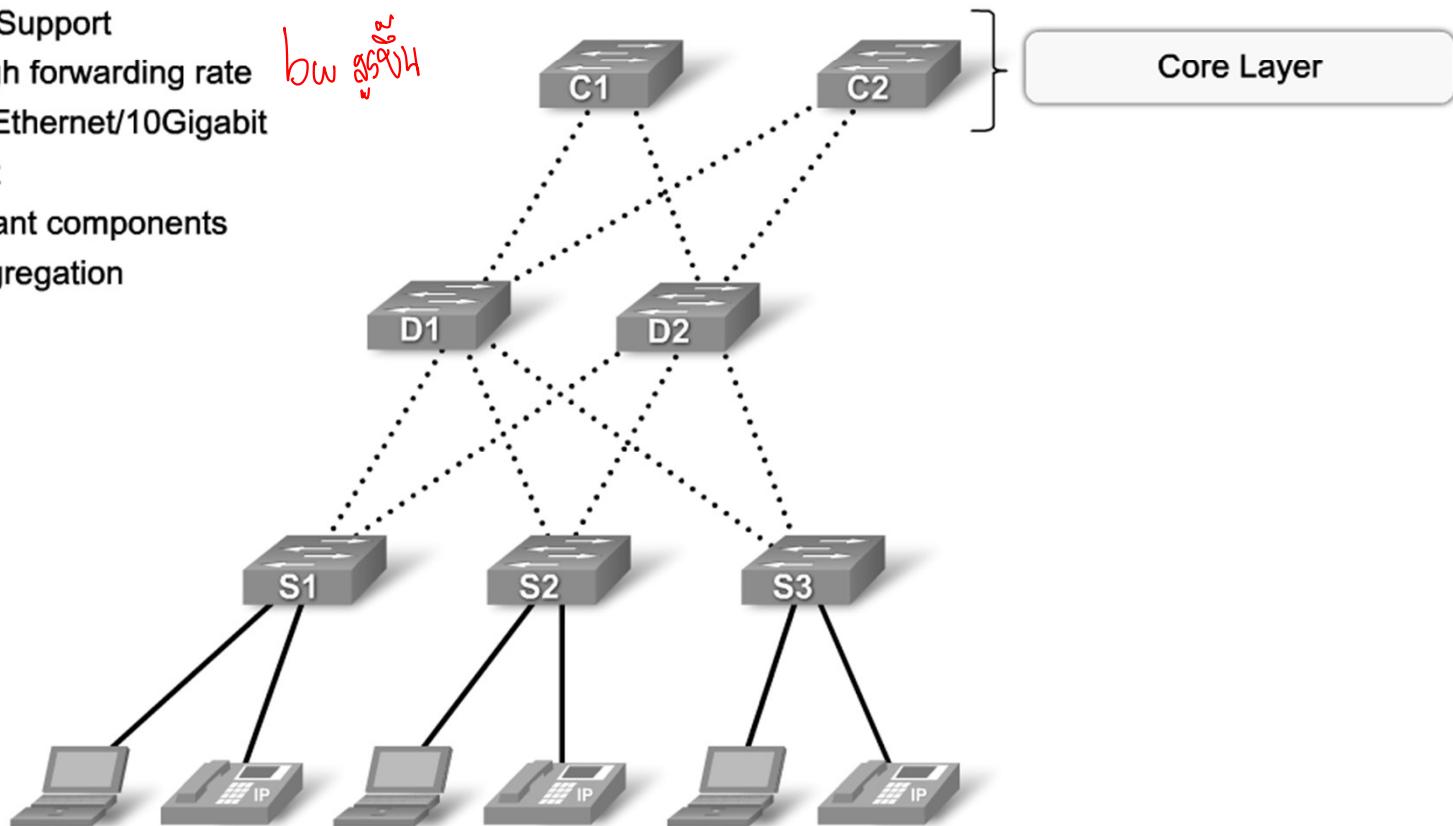
- Layer 3 Support
- High forwarding rate
- Gigabit Ethernet/10Gigabit Ethernet
- Redundant components → *សម្រាប់សំណងចិត្ត*
- Security Policies/Access Control Lists
- Link Aggregation
- QOS



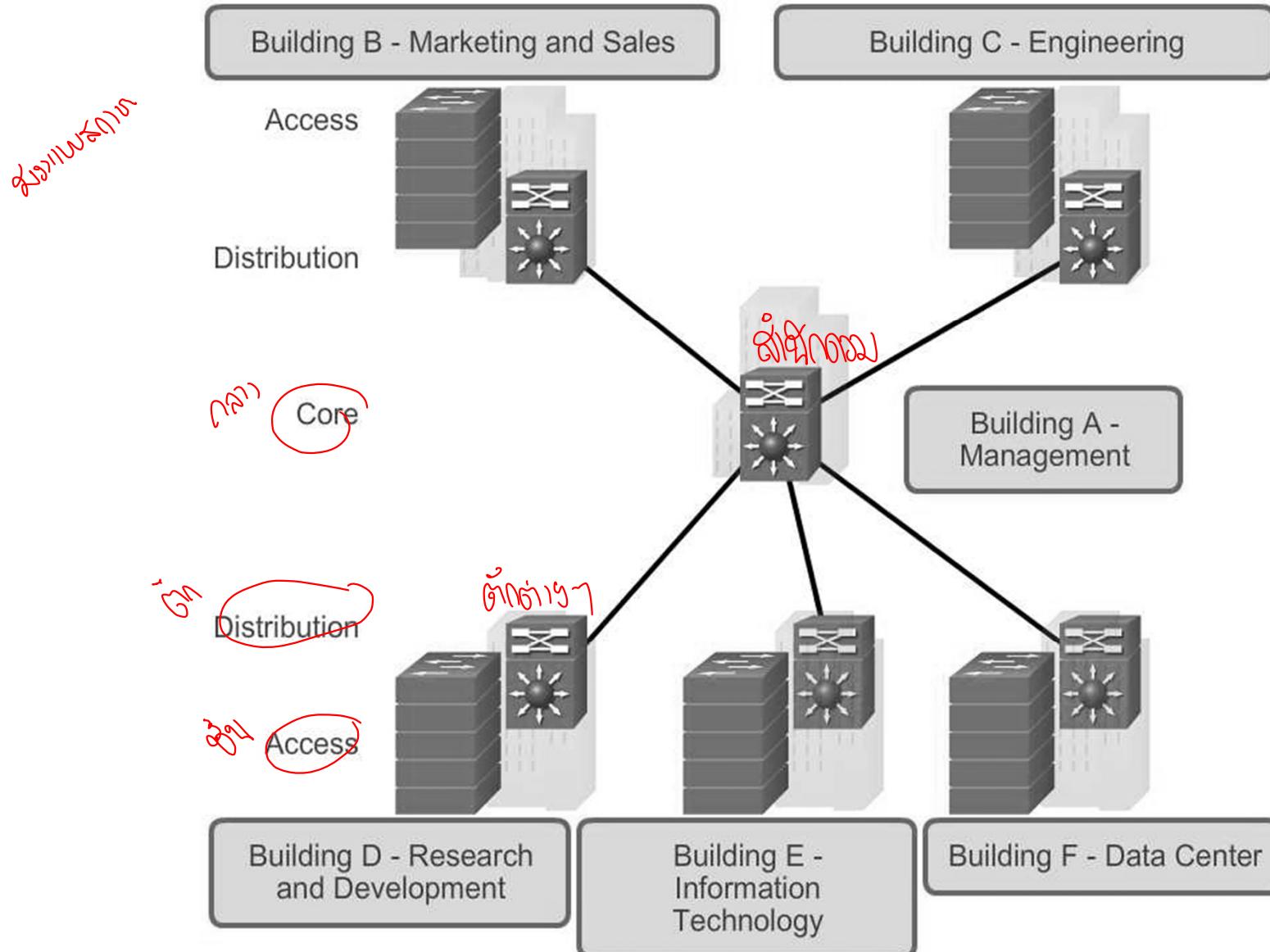
LAN Design

Core Layer Switch Features

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

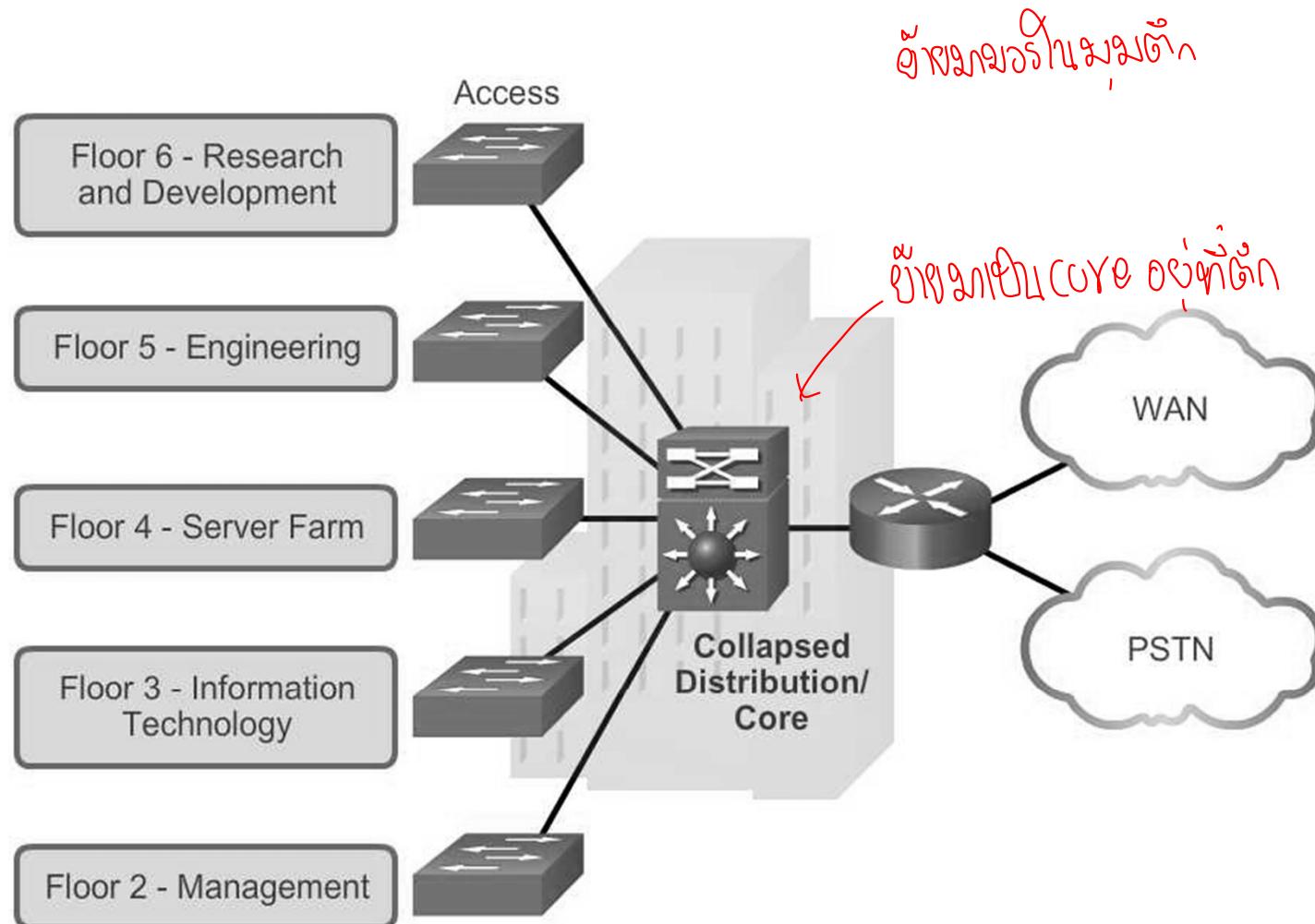


LAN Design စက်ချိန်များပုဂ္ဂန်



LAN Design

→ នៅconcept → និង



LAN Design

Common Business Considerations When Selecting Switch Equipment:

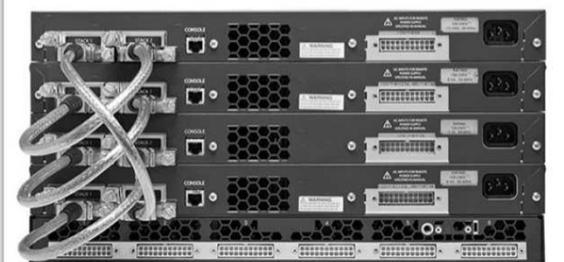
- **Cost** - The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- **Port Density** - Network switches must support the appropriate number of devices on the network.
- **Power** - It is now common to power access points, IP phones, 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.



Modular Configuration Switches



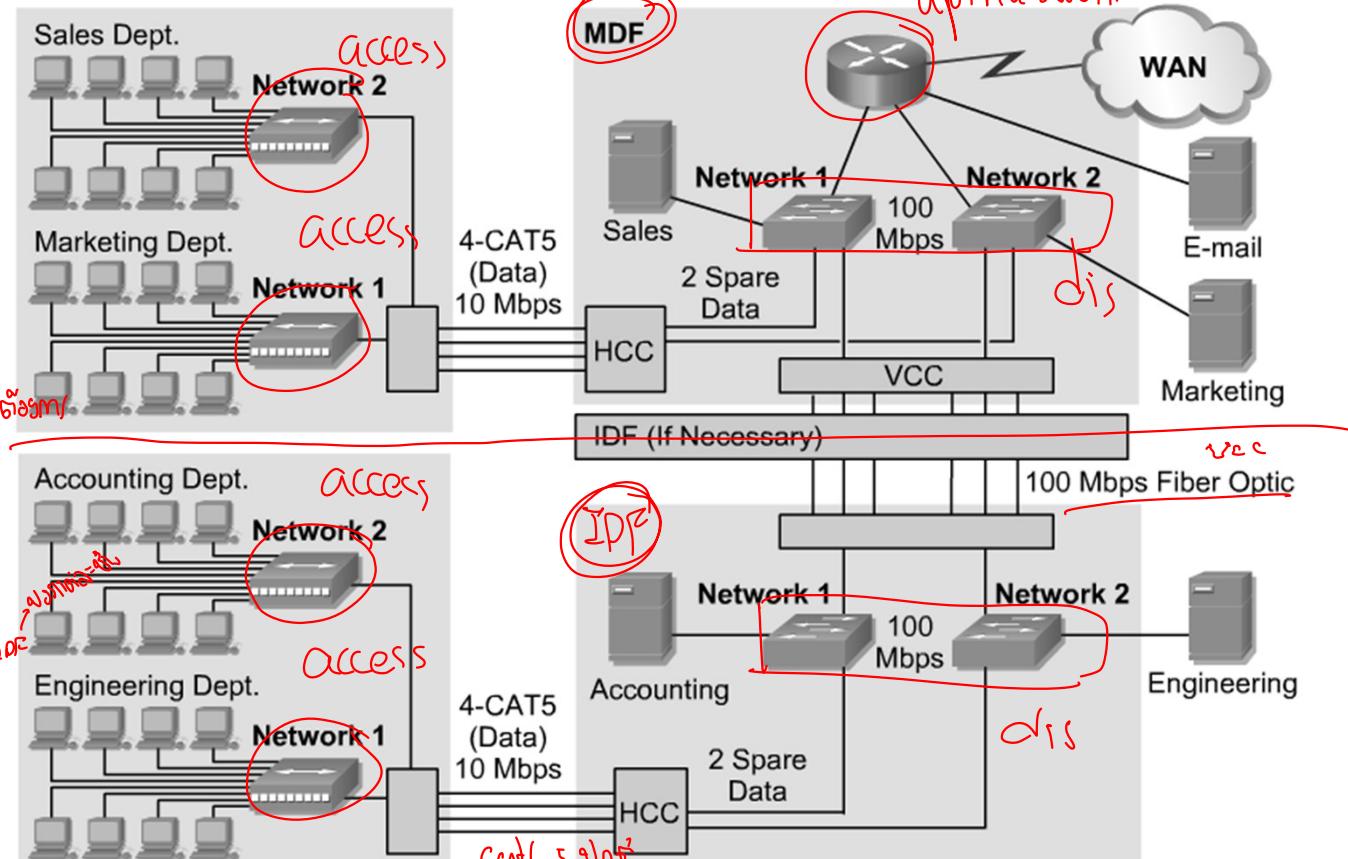
Stackable Configuration Switches



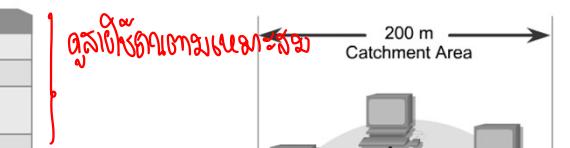
LAN Design

បច្ចេកទេស

- 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



Characteristic	10BASE-T	10BASE-FI	100BASE-TX	100BASE-FX
Data rate	10 Mbps	10 Mbps	100Mbps	100 Mbps
Signaling method	Baseband	Baseband	Baseband	Baseband
Medium type	Category 5e UTP	Fiber-optic	Category 5e UTP	Multi-mode fiber (two strands)
Maximum length	100 meters	2000 meters	100 meters	2000 meters



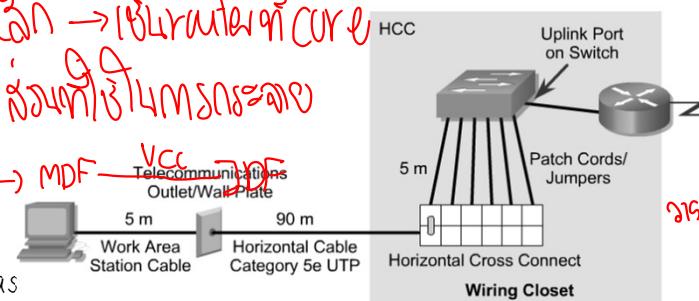
MDF : Main Distribution Facility → ចិត្តផ្ទុក → ចូលរាយទៅ CORE

IDF : Intermediate Distribution Facility → សម្រាកចិត្តផ្ទុក

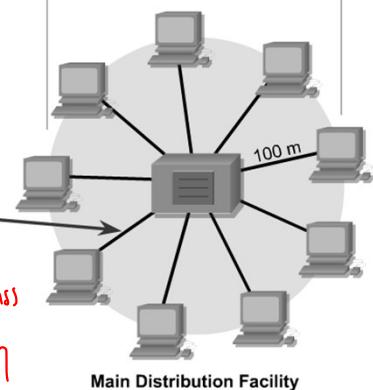
VCC : Vertical cross-connect → MDF → IDF

HCC : Horizontal cross-connect

Internetworking Standards and Technologies, Jiras



នៅលើ MDF, IDF នូវ
ឯកសារពាណិជ្ជកម្ម



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.
-
- កំណត់សម្រាប់សង្គម ឬបន្ទាក់សំឡេរ > hub
ជាថ្វី bus → 1 big collision
Collision Domains
bridge
Collision Domains
layer 2
Router
Broadcast Domain
Broadcast

The Switched Environment

- Switch Operation

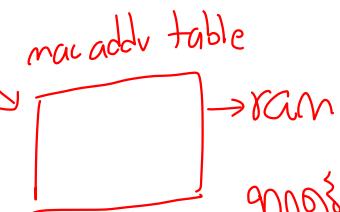
① Learning

→ ផលសេវាដែលបានបង្កើតឡើងនៅលើការបញ្ជូន mac address → ដើរតម្លៃទីតាំងនៃការបញ្ជូននៅលើការបង្កើតឡើង

② Aging

→ ផលសេវាដែលបានបង្កើតឡើង

→ ការបញ្ចូន learning → ការបញ្ចូននៃការបង្កើតឡើង → refresh age



ការបញ្ចូននៃការបង្កើតឡើង
និងការបញ្ចូននៃការបង្កើតឡើង
refresh age

③ Flooding

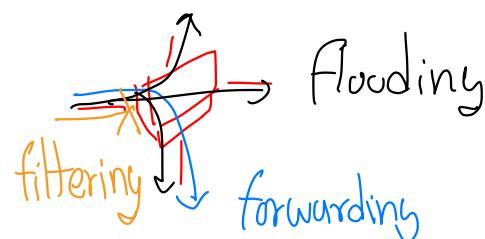
→ ផលសេវាដែលបានបង្កើតឡើង

④ Forwarding

→ ការបញ្ចូន

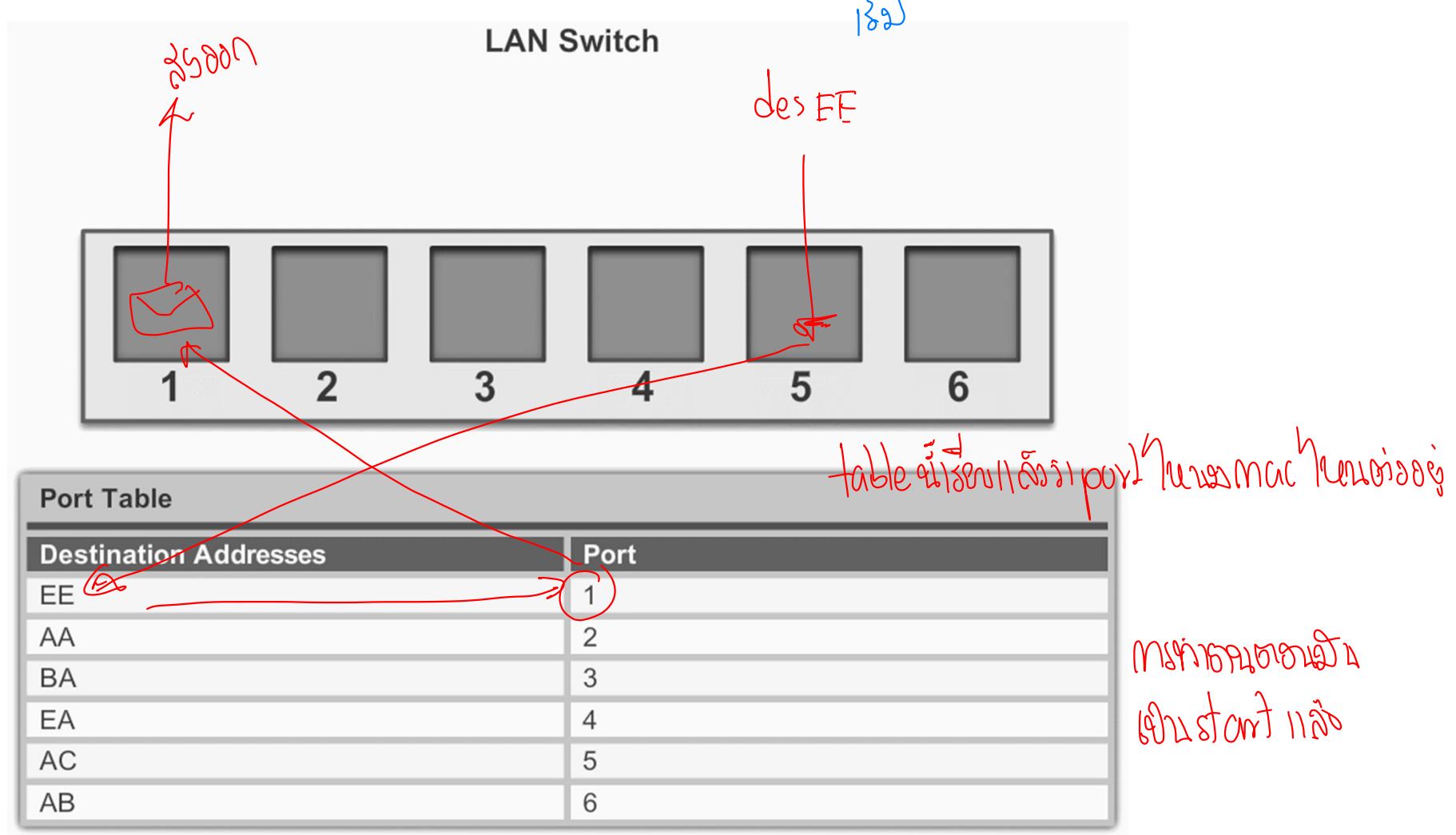
⑤ Filtering

→ ការបញ្ចូន



The Switched Environment

- Switching



ຫວັງເລີນກົດປົກ

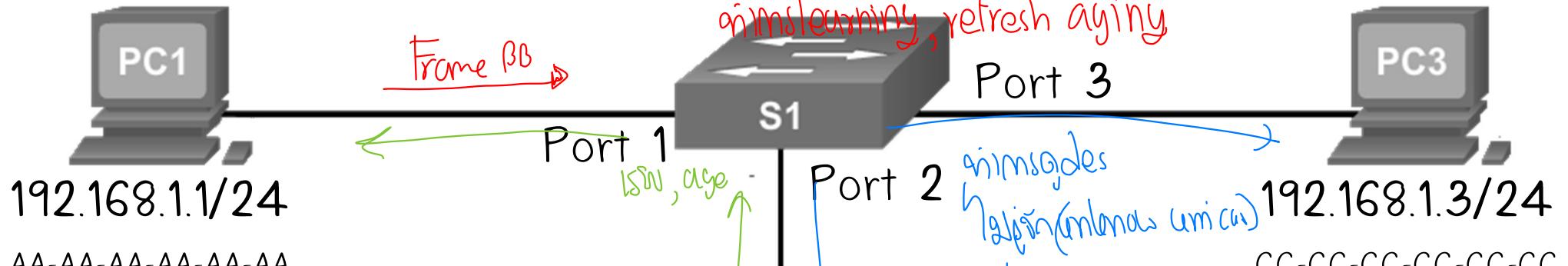
The Switched Environment

ມາດັ່ງສ້າງມາດຕະຖານ

- MAC Addressing & Switch MAC Tables

ກົດປົກສະໜອງ

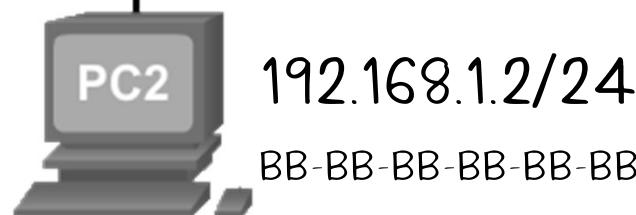
MAC Table	
Port 1	AA
Port 2	BB
Port 3	



MAC Tables

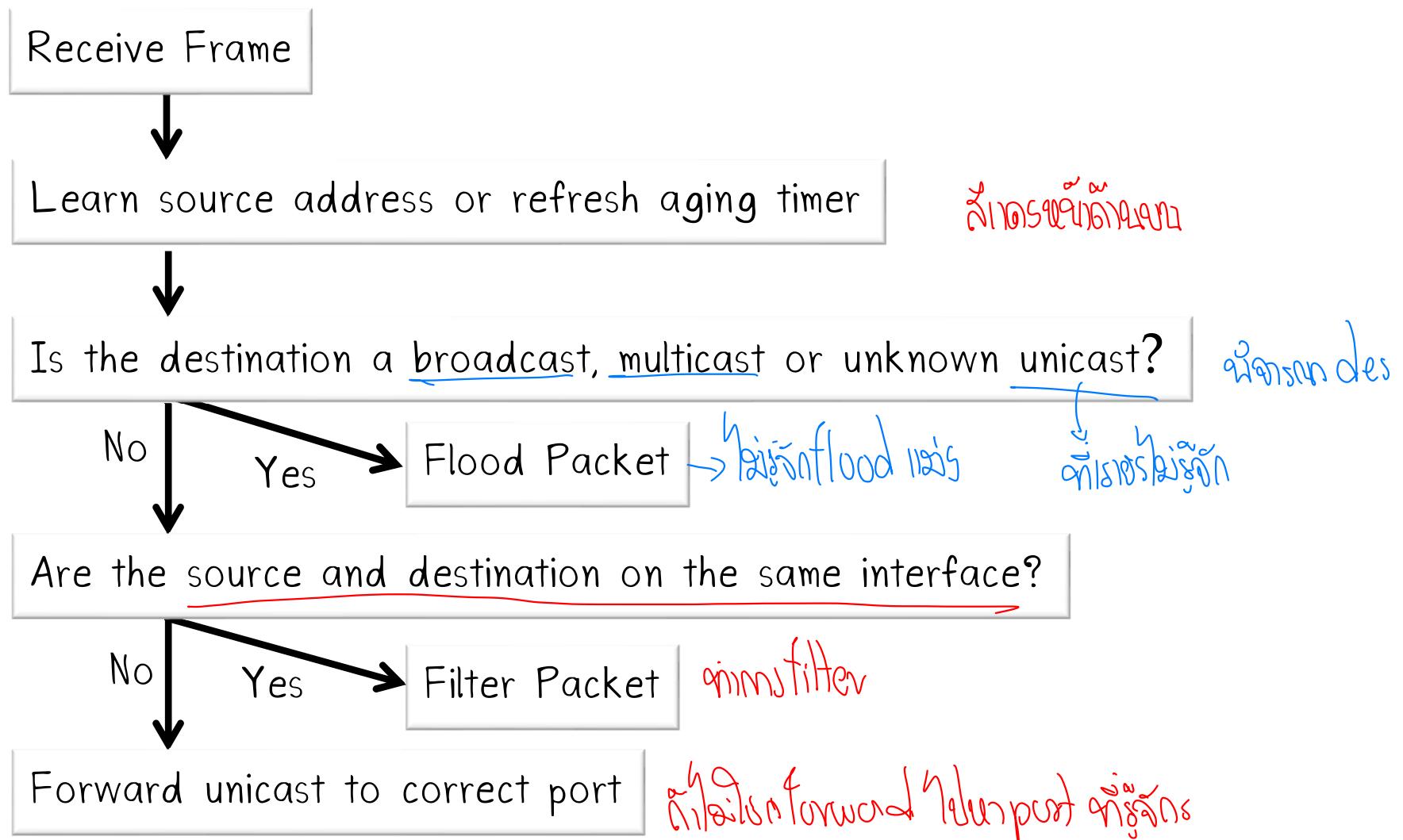
Content addressable memory (CAM) table

Source address table



The Switched Environment

- Transparent Bridge Process - Jeff Doyle

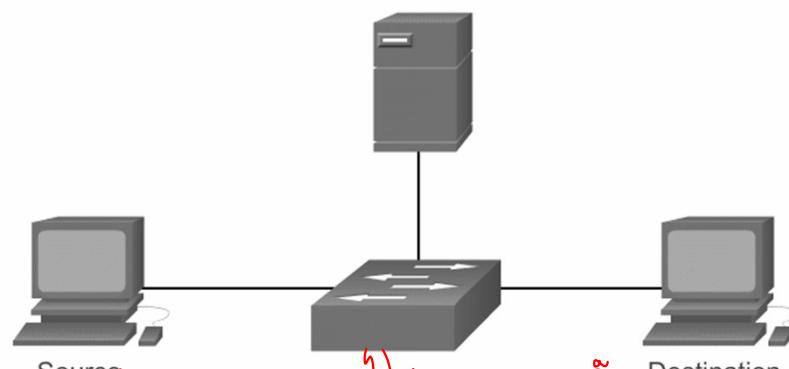


The Switched Environment

- Switch Forwarding Methods

Store-and-Forward Switching

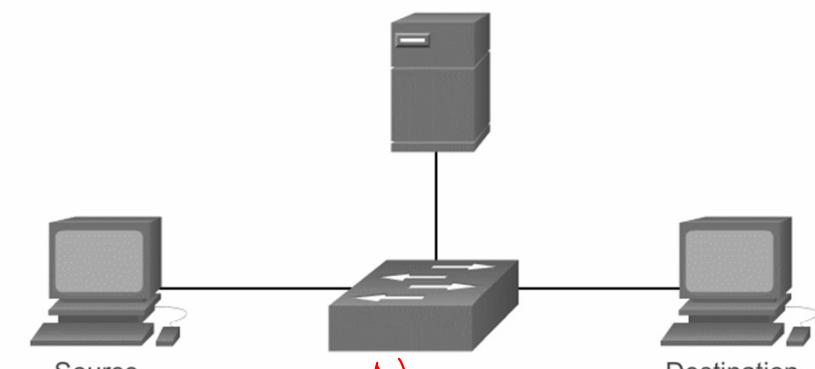
ໃນສິ່ງ frame



ກົບ , ແລ້ວ , ສໍາເລັດ process ຕີ່ນີ້

A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

Cut-Through Switching



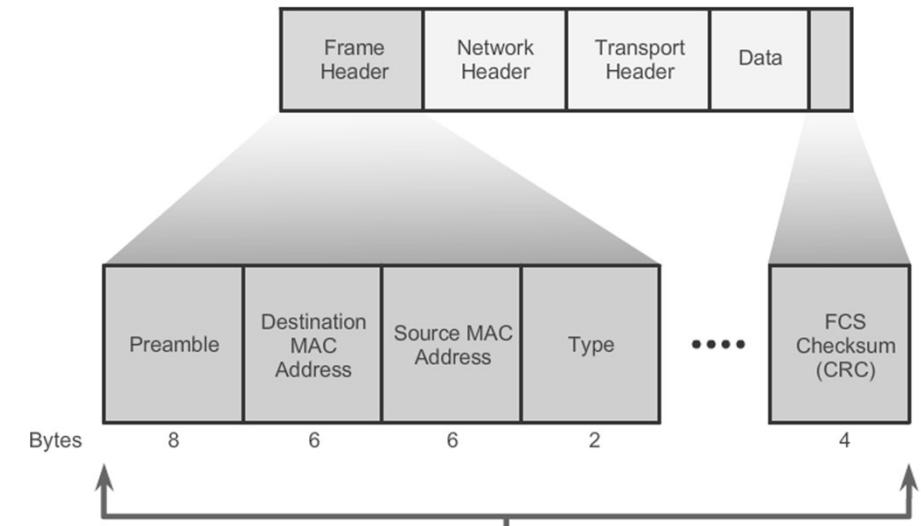
ຂອງຈຳກັດສ່ວນ sw , ອີ່ຈີ process

A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

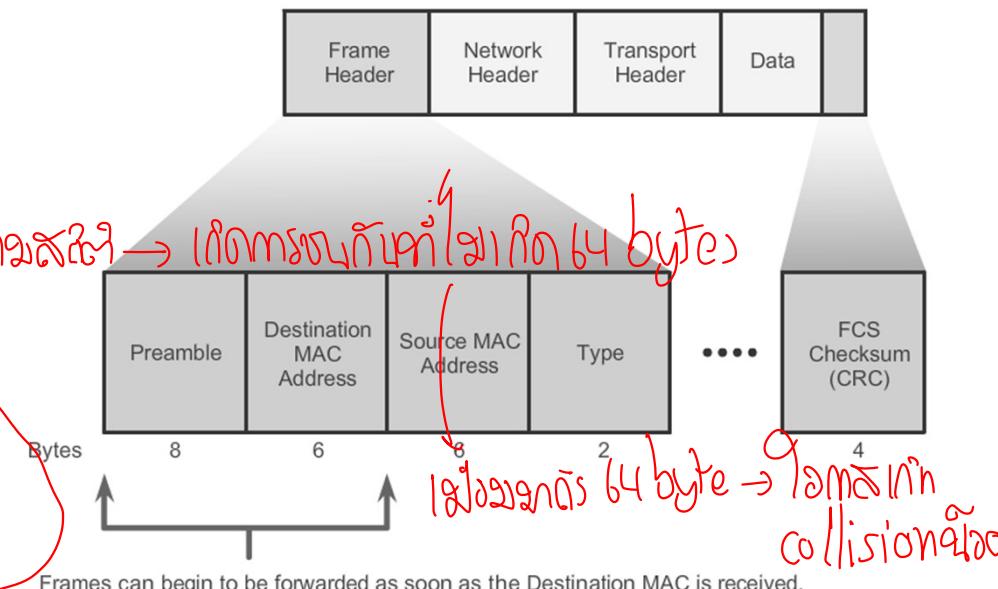
ໃຈໝວຍ
ດີ່ນdestination addr
ດີ່ນຫຼັບສິນ

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



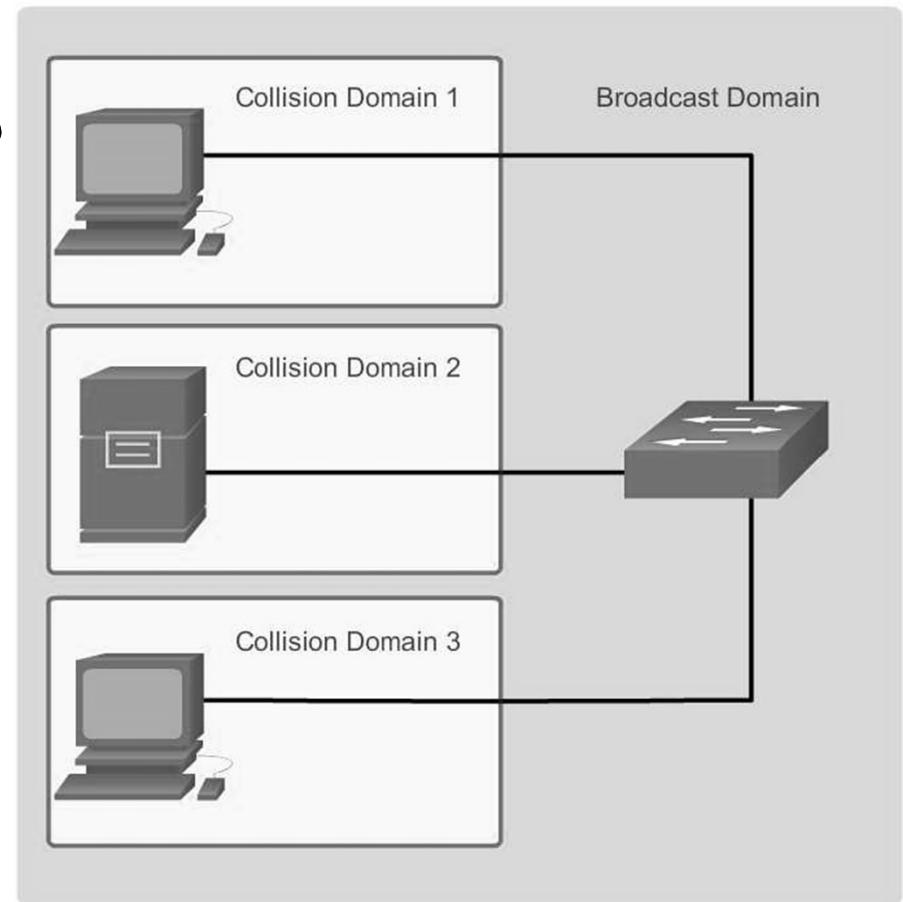
Store-and-forward switching entails receipt of the entire frame (up to about 9,200 bytes for jumbo frames) before a forwarding decision is made.



Switching Domains

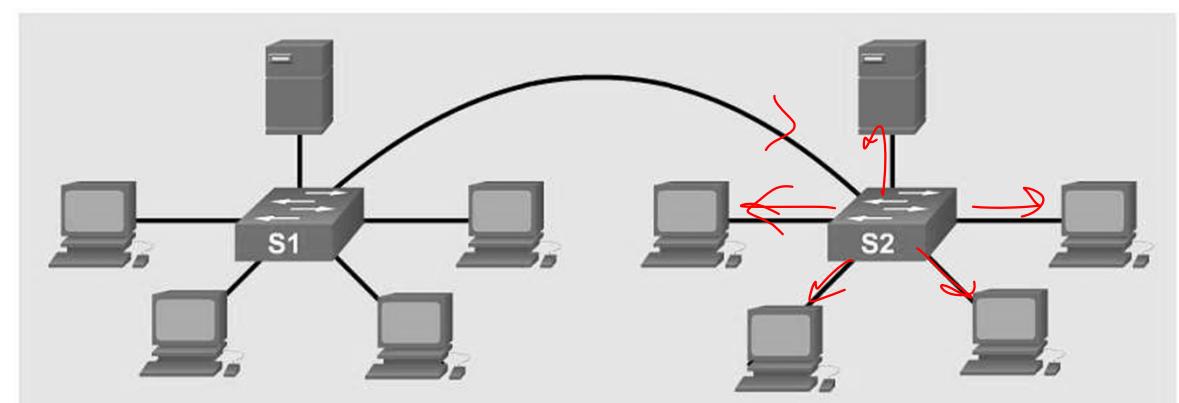
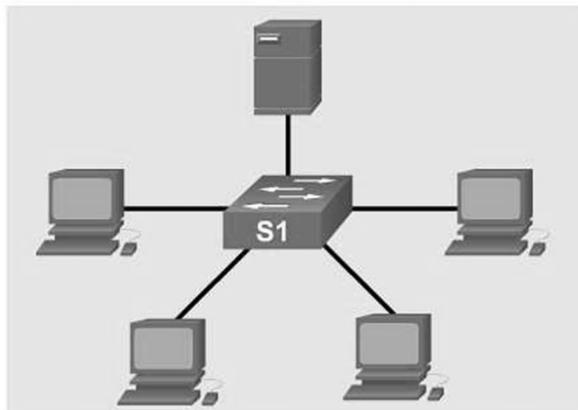
- Collision Domains → *မြတ်နောက်ဆုံးအသွေးပြောင်းလဲခဲ့ရန်*

- 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.

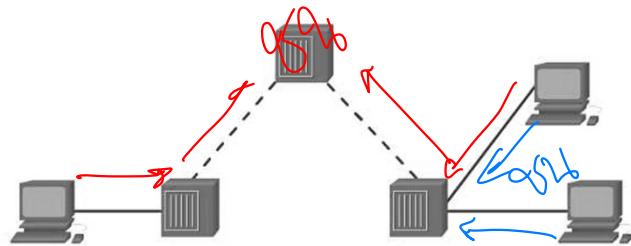


Switching Domains

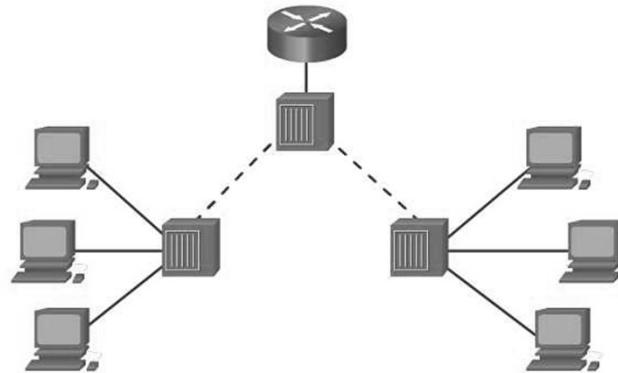
- Broadcast Domains → *Tổng quan về broadcast*
 - Broadcast domain is the extend of the network where a broadcast frame can be heard.
 - Switches forward broadcast frames to all ports. Therefore switches don't break broadcast domains.
 - All ports of a switch (with its default configuration) belong to 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)



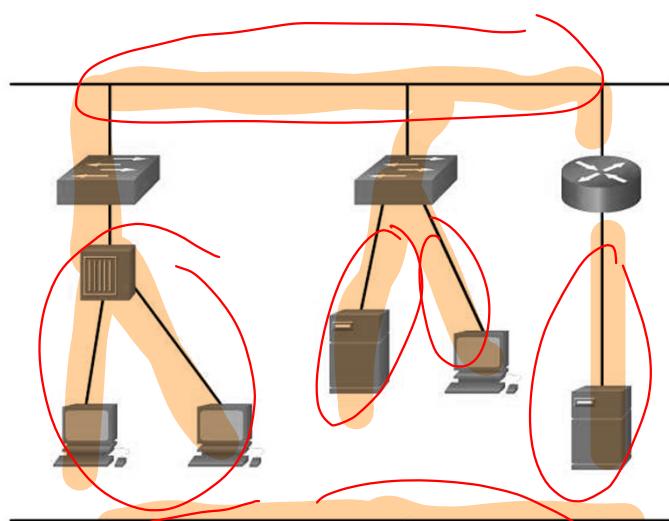
Switching Domains



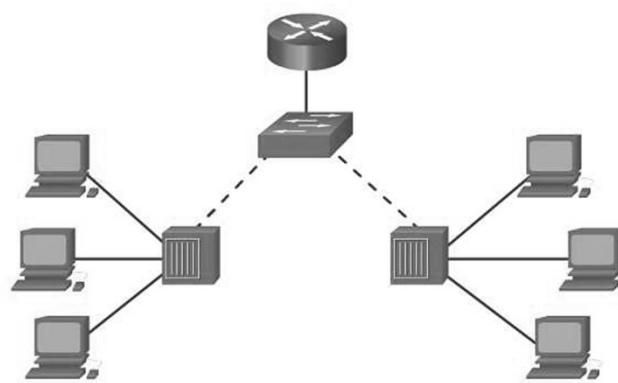
1 collision
1 broadcast



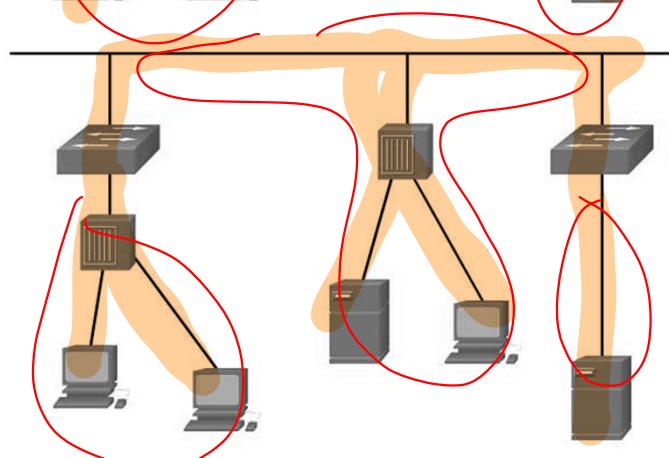
1
1



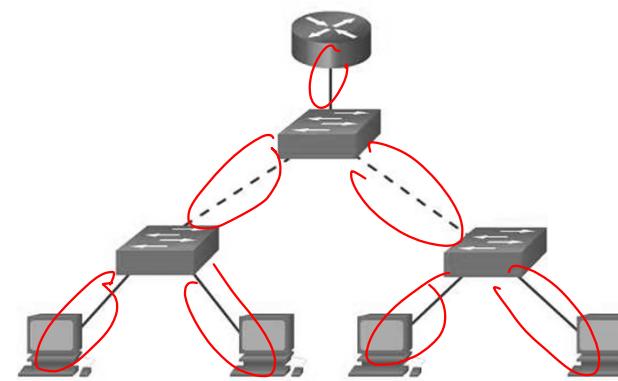
5 collision
2 broadcast



3
3



3 collision
1 broadcast



7
7

- Basic Switch Concept & Configuration

- Basic Switch Configuration *(เรียบเรียง)*

- Switch Boot Sequence

- Preparing for Basic Switch Management

- Configure Switch Ports

- Switch Security : Security Remote Access *(เรียบเรียง)*

- Switch Port Security ?

บัญชีการจัดการ

Switch Boot Sequence

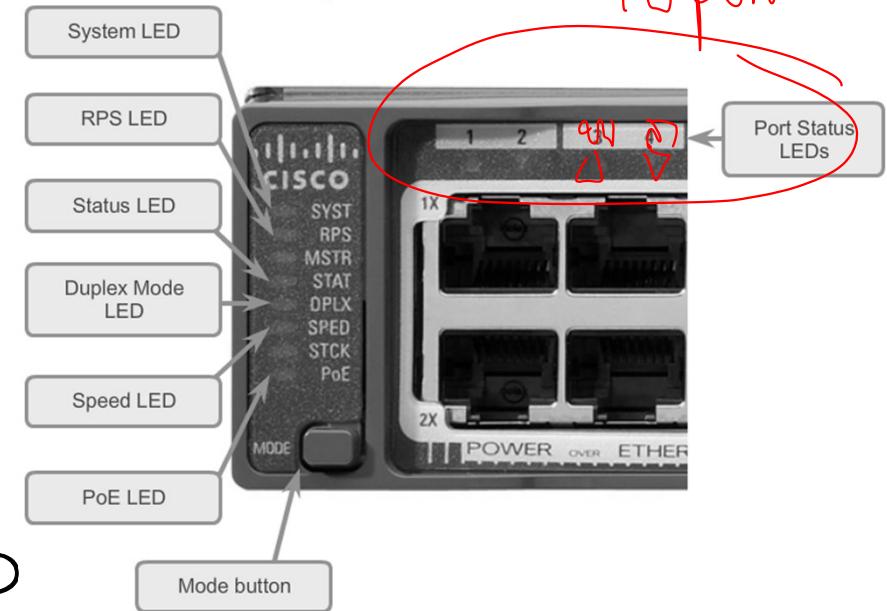
- POST
 - Run boot loader software
 - Boot loader does low-level CPU initialization
 - Boot loader initializes the flash filesystem
 - Boot loader locates and loads a default IOS operating system software image into memory and hands control of the switch over to the IOS.
- boot router

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.

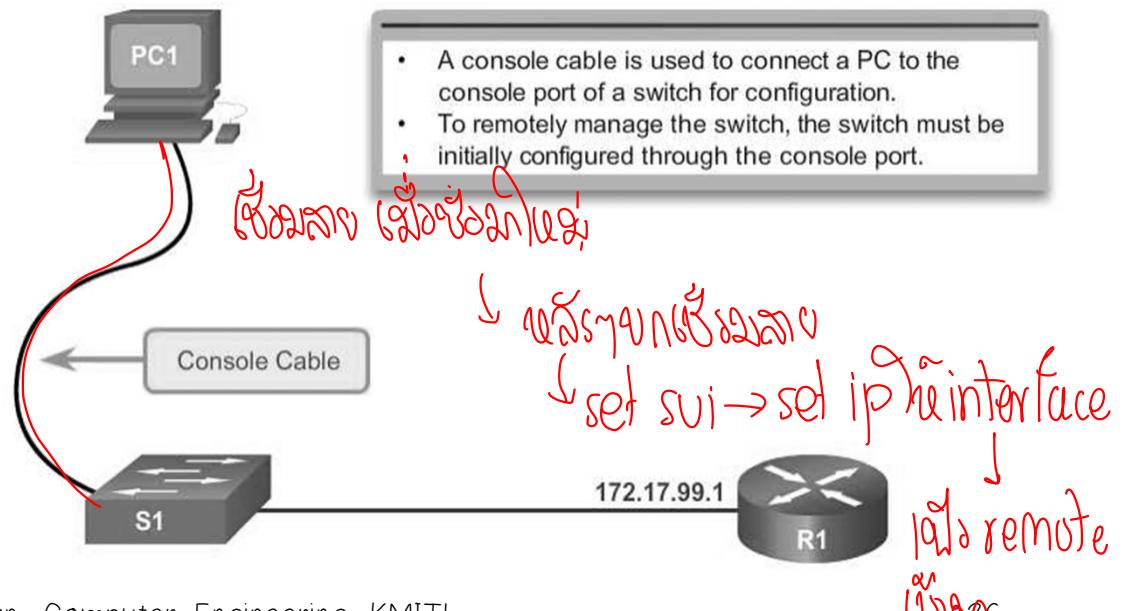
Switch LED Indicators

- 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 *[a] port* 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)
- 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

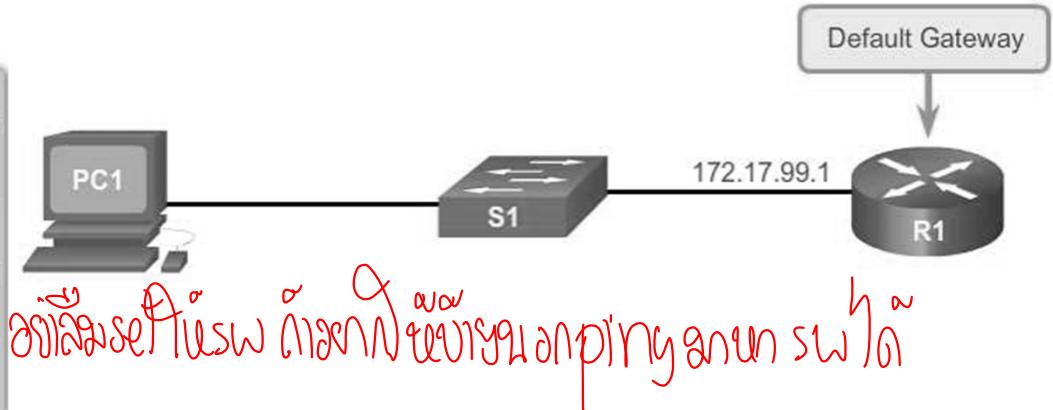
Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode for the SVI.	S1(config)# interface vlan 99
Configure the management interface IP address.	S1(config-if)# ip address 172.17.99.11 255.255.0.0
Enable the management interface.	S1(config-if)# 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

S1# show running-config
...
interface FastEthernet0/18
switchport access vlan 99
switchport mode access
...
<output omitted>
S1# show ip interface brief
Interface IP-Address OK? Method Status Protocol
Vlan99 172.17.99.11 YES manual up up
FastEthernet0/18 unassigned YES unset up up

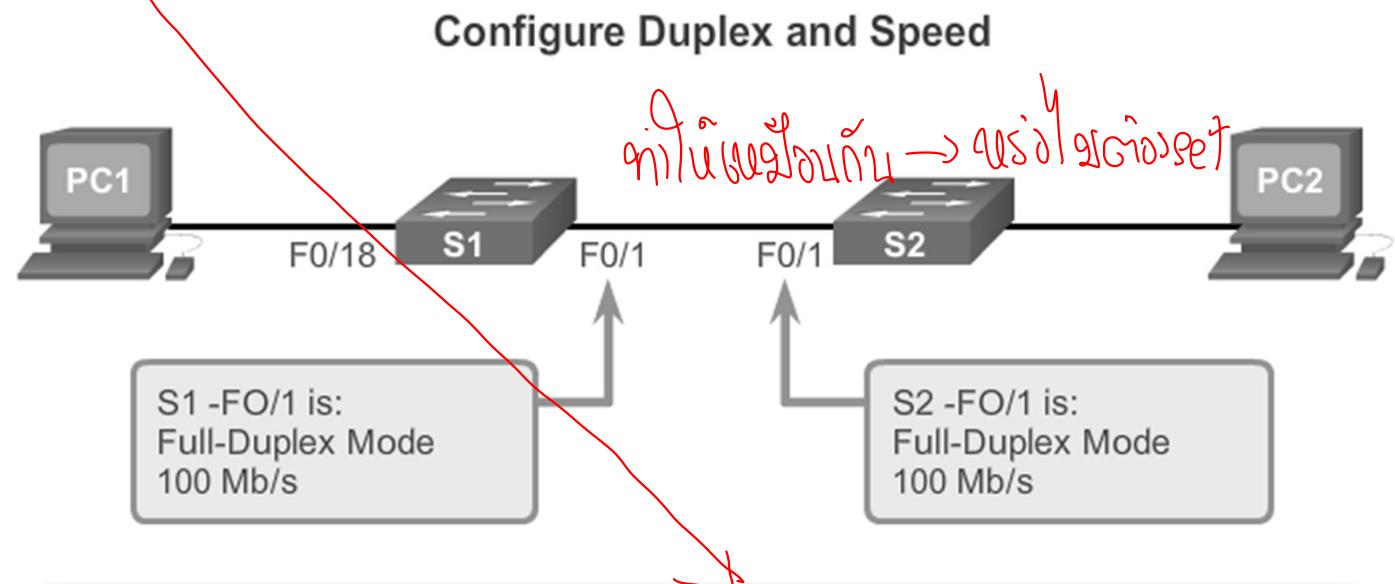
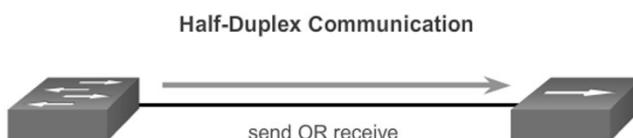
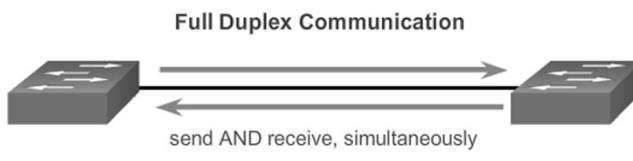
Configure Switch Default Gateway

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Configure the default gateway for the switch.	S1(config)# ip default-gateway 172.17.99.1
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

- Duplex Communication



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 → กำหนดโดยอัตโนมัติ CROSS → ต้อง mode ที่ต้องการต่อไป

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
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

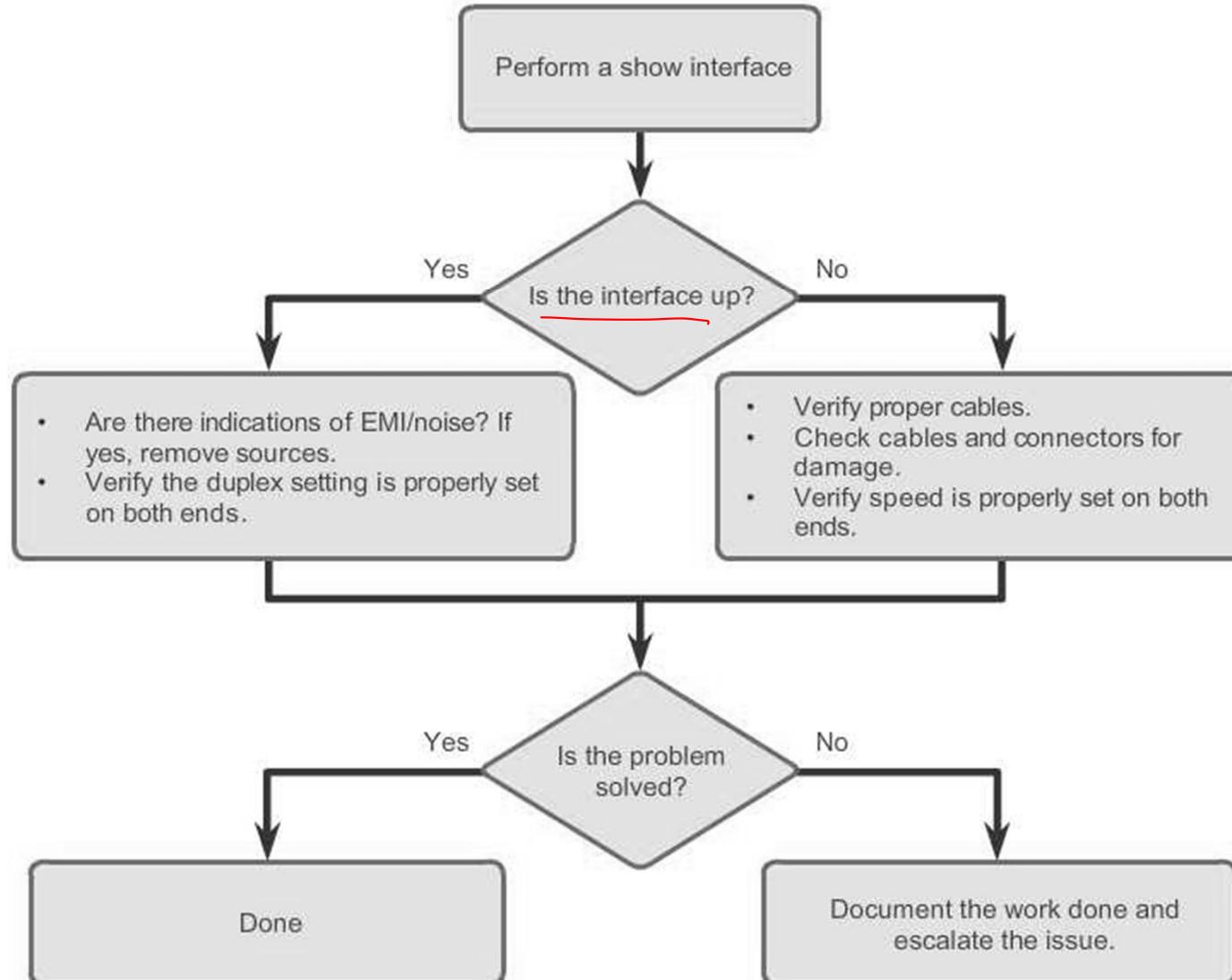
Verification Commands

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 <i>(optional)</i>

Configure Switch Ports

មានវិធានលក្ខណៈអ្នករក្សា ?

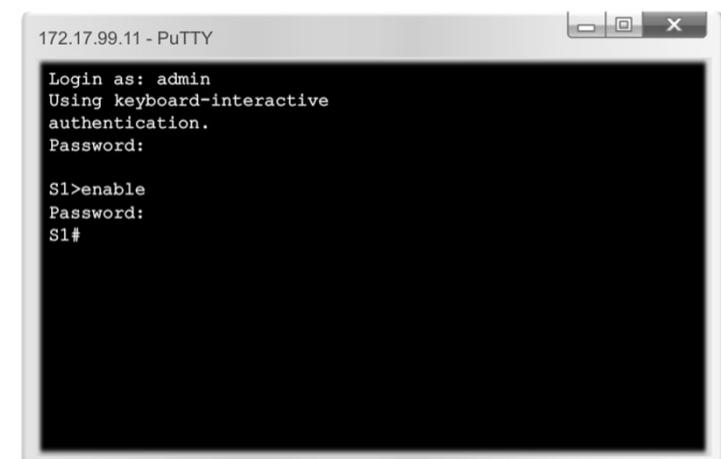
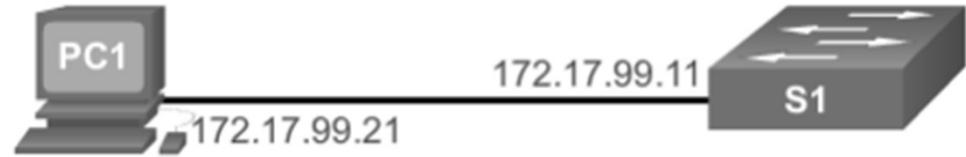
Troubleshooting Switch Media Issues



Security Remote Access

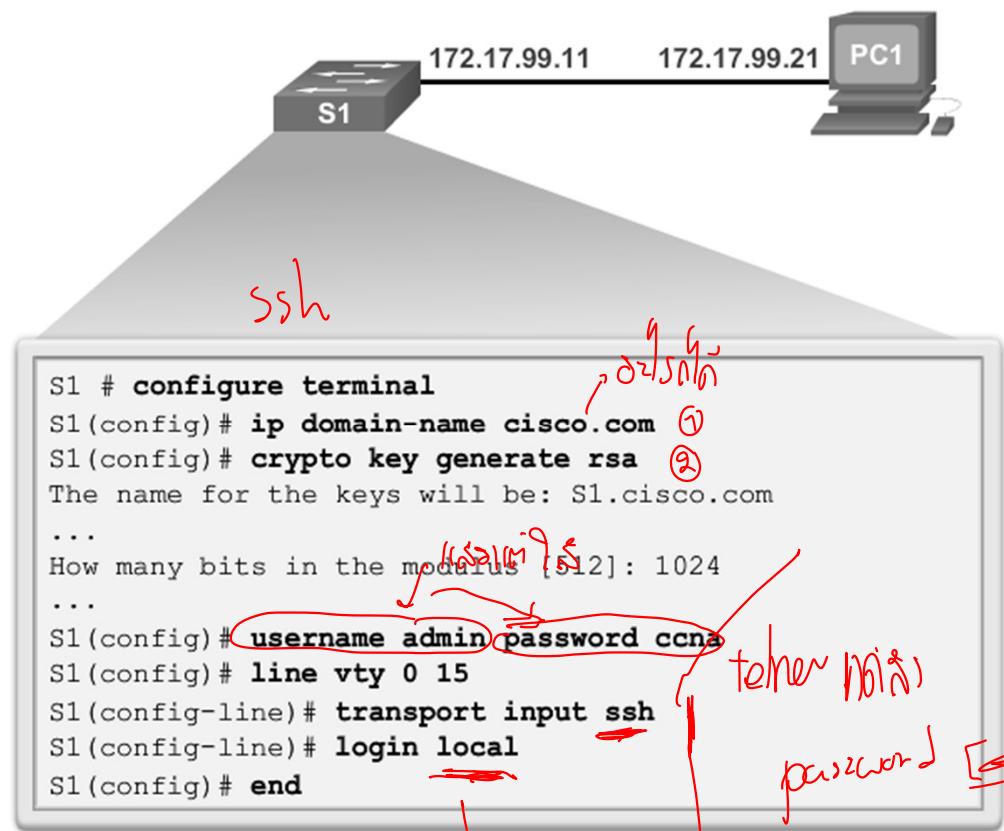
- SSH Operation

- 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 *ssh more secure on telnet over*
- 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

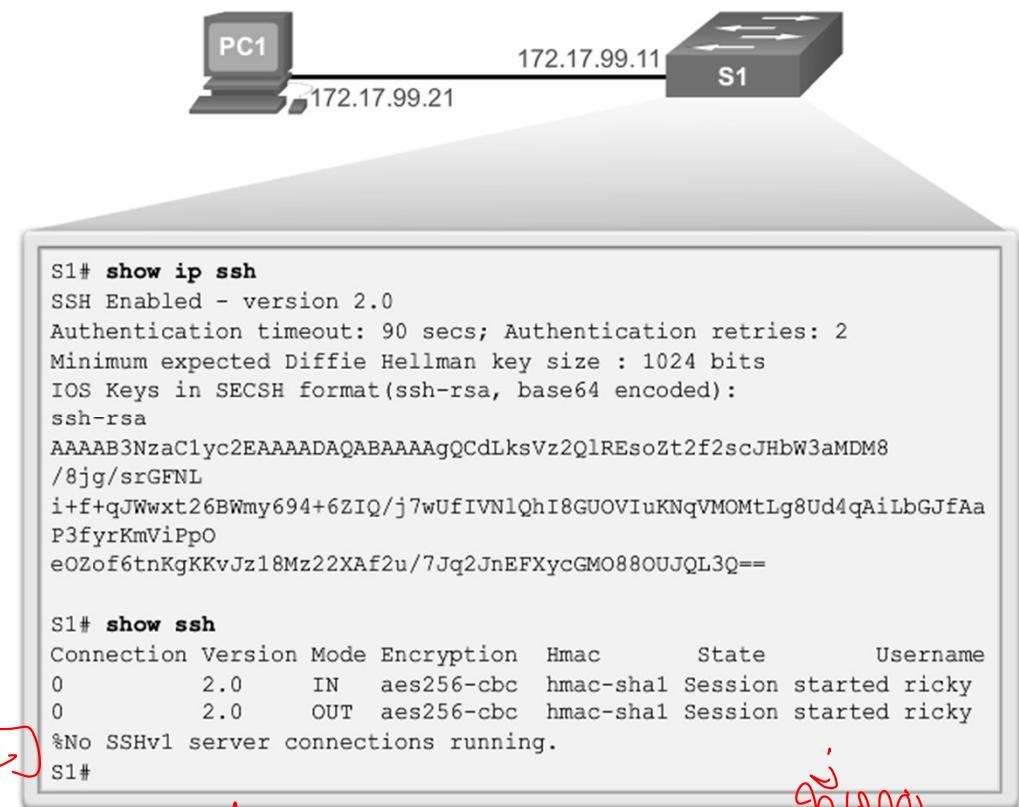


Security Remote Access

- Configuring SSH



- Verifying SSH



Switch Port Security

- Operation : Secure MAC Address Types

ຕິດຕະCommand ດັ່ງ

- 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.

ໃນຕະຫຼາດ

- 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

ທີ່ມີມອວຍຕົວເລື່ອກ່າວຂອງ ສົມຜູ້ມາຈຸດທີ່ມີໄປ-ໄດ້ໂສລະ

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

Switch Port Security

Mode នៃមែនសម្រាប់ security → ទទួលបានពាក្យសេវាដោយណា

- 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	No	Yes	No
Shutdown	No	No	No	Yes	Yes

port shutdown
↑

good default → no violation

Switch Port Security

Port Security Defaults

↳ ឧបត្ថម្ធចុងគម្រោង
រាយការពិនិត្យ
↳
↳ shutdown
no shutdown

Feature	Default Setting
Port security	Disabled on a port <u>លើកឡាតាំង</u>
Maximum number of secure MAC addresses	1 <u>មិនអាច 1 mac បាន</u>
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

Switch Port Security

ឧបករណ៍ផ្លូវការ

សម្រាប់លាន interface នៅក្នុង

- Static secure MAC addresses

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address [MAC-ADD]
```

- Dynamic secure MAC addresses

```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address [sticky]
```

- Maximum MAC addresses *por port*

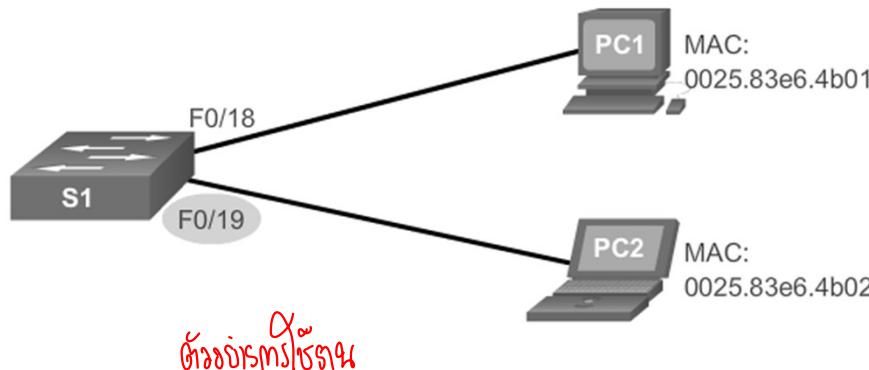
```
Switch(config-if)#switchport port-security maximum [MAX]
```

- Violation mode

```
Switch(config-if)#switchport port-security violation [?]
protect    Security violation protect mode
restrict   Security violation restrict mode
shutdown  Security violation shutdown mode
```

protect
restrict
shutdown

Switch Port Security



Cisco IOS CLI Commands

S1(config)#interface fastethernet 0/18	Specify the interface to be configured for port security.
S1(config-if)#switchport mode access	Set the interface mode to <u>access</u> .
S1(config-if)#switchport port-security	Enable port security on the interface.
S1(config-if)#switchport port-security maximum 50	Set the maximum number of secure addresses allowed on the port.
S1(config-if)#switchport port-security mac-address sticky	Enable <u>sticky learning</u> .

```
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
```

S1# show port-security address

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)

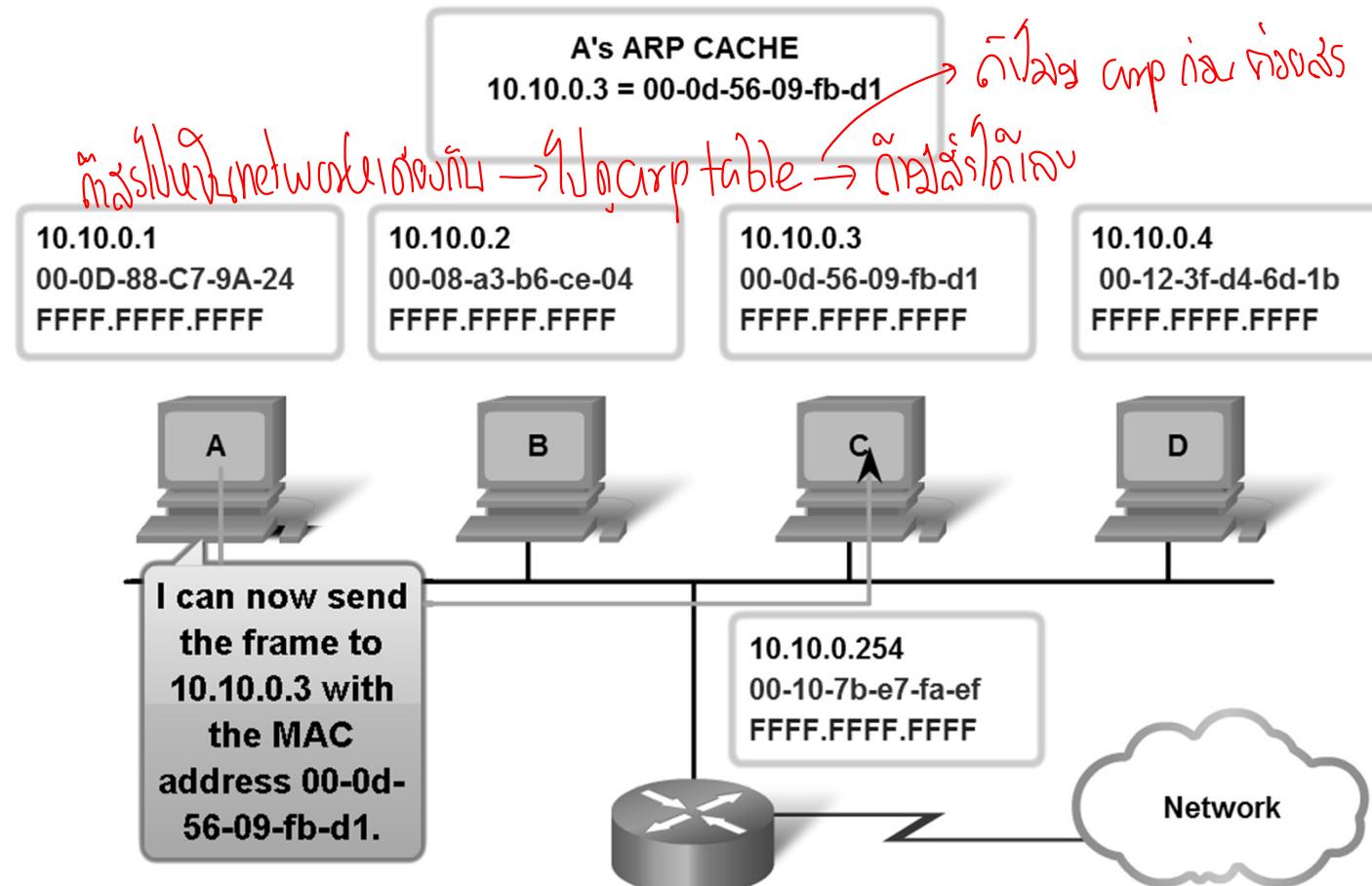
Address Resolution Protocol

- Mapping IP to MAC Addresses

arp կայուն լիք

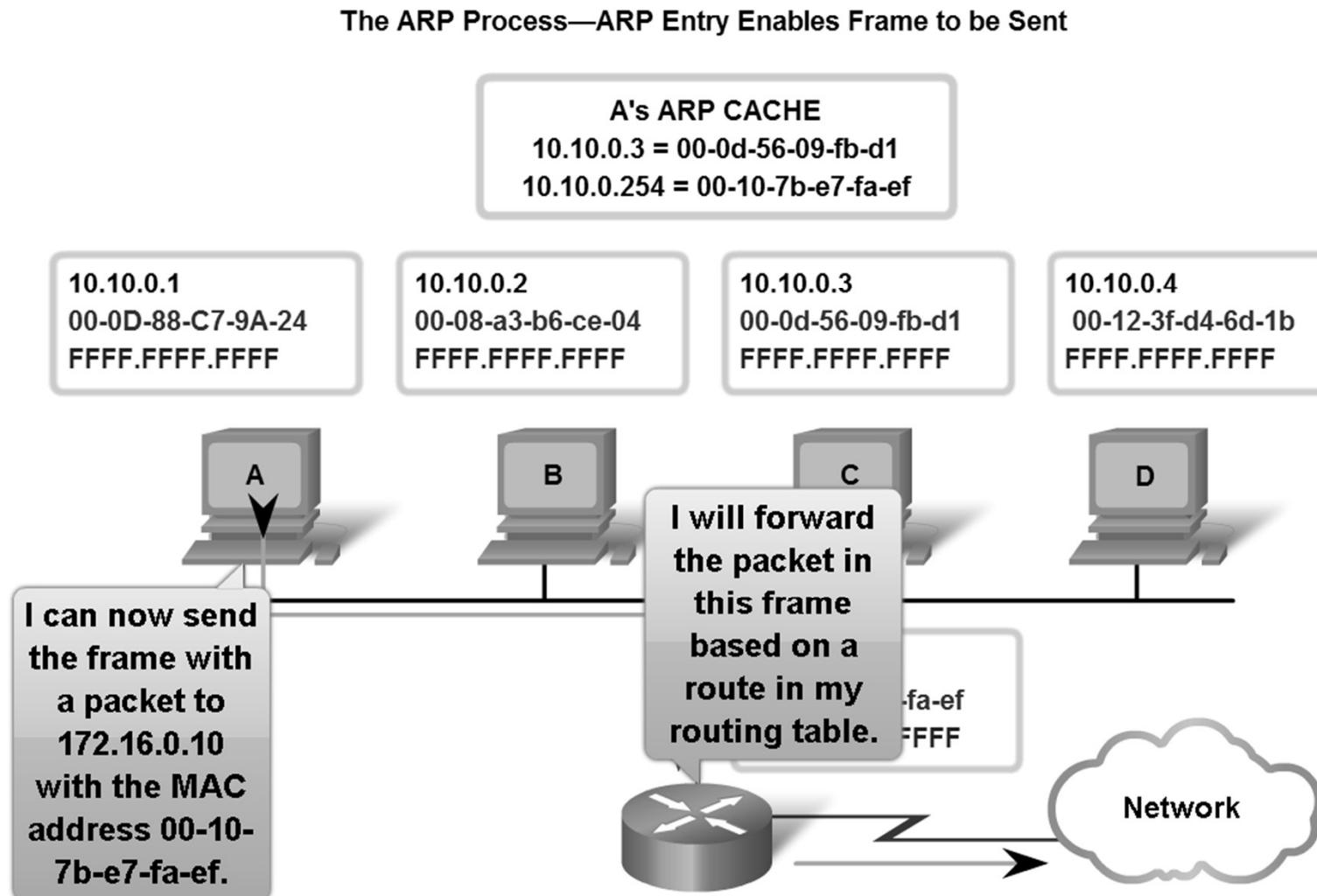
ուրիշ լիք mac հիմա

The ARP Process—ARP Entry Enables Frame to be Sent



Address Resolution Protocol

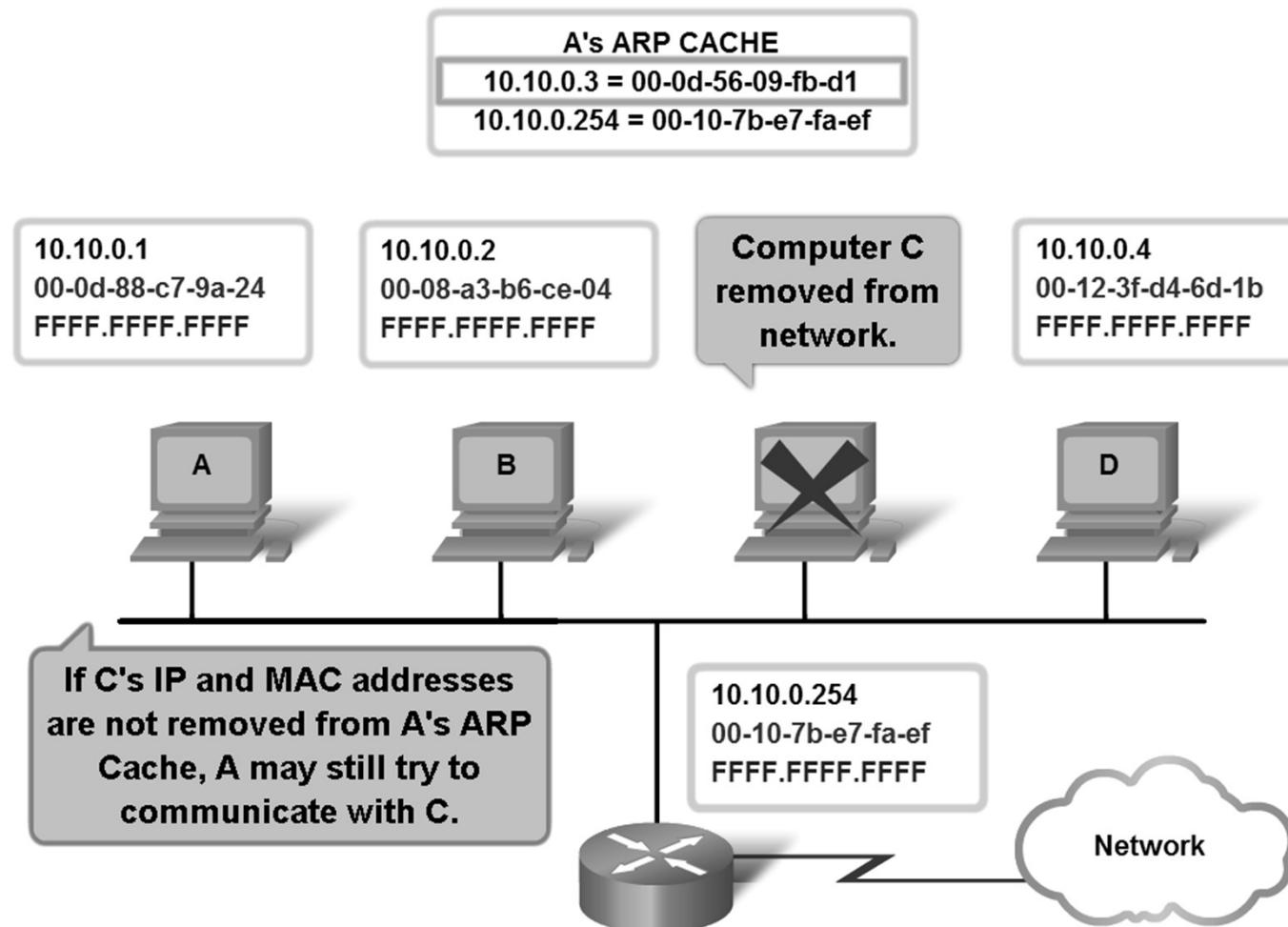
- ARP - Destinations Outside the Local Network



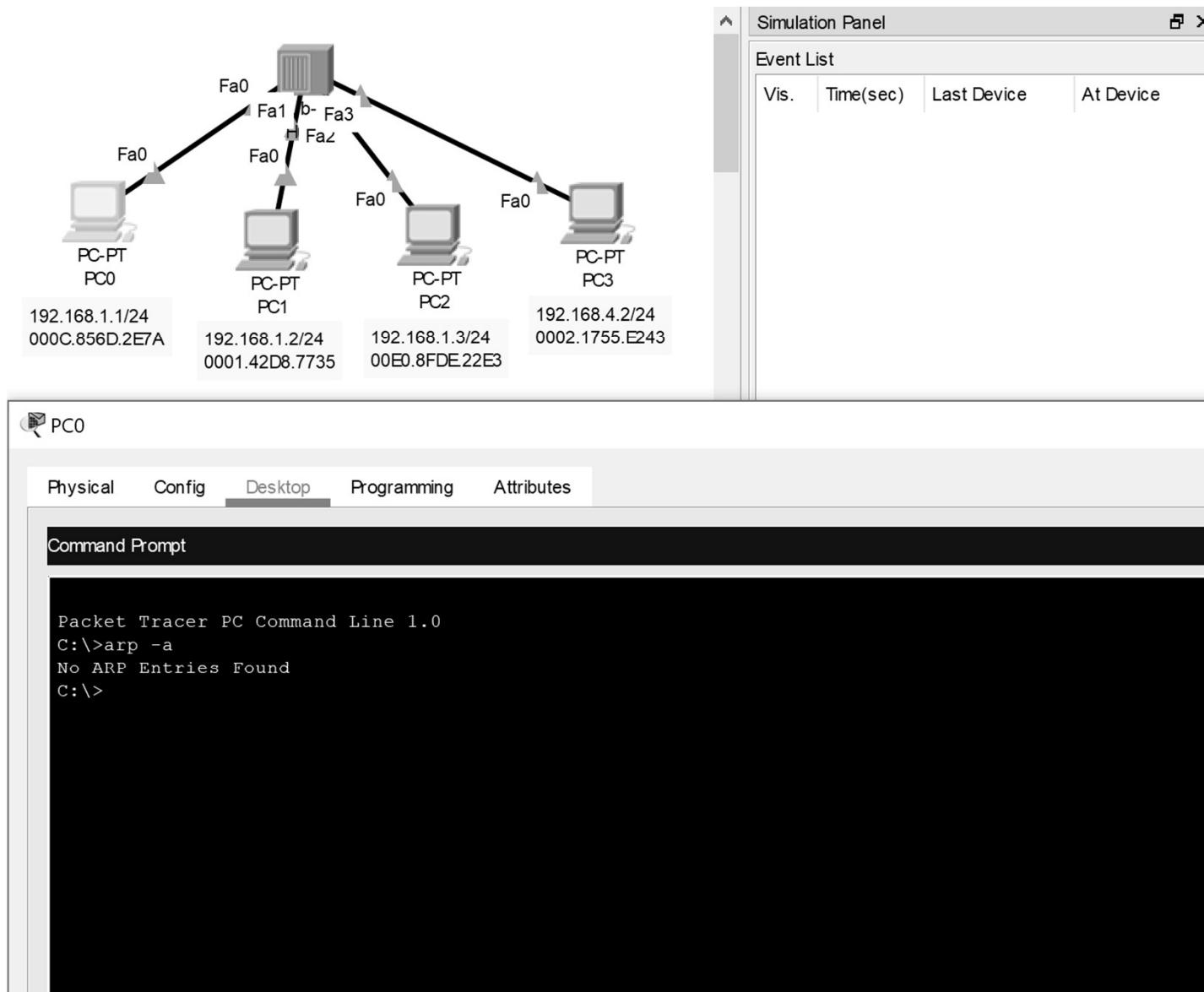
Address Resolution Protocol

- ARP - Removing Address Mappings

The ARP Process - Removing Address Mappings



Address Resolution Protocol



Address Resolution Protocol

សំណងចាន់ចាន់ នៃ ARP (លើមហូប)

PC-PT PC0	192.168.1.1/24 000C.856D.2E7A	PC-PT PC1	192.168.1.2/24 0001.42D8.7735	PC-PT PC2	192.168.1.3/24 00E0.8FDE.22E3	PC-PT PC3	192.168.4.2/24 0002.1755.E243
--------------	----------------------------------	--------------	----------------------------------	--------------	----------------------------------	--------------	----------------------------------

Simulation Panel

Vis.	Time(sec)	Last Device	At Device
Visible	0.000	--	PC0
Visible	0.000	--	PC0

PDU Information at Device: Hub0

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

EthernetII

0	4	8	Bytes
PREAMBLE: 101010..10		DEST ADDR: FFFF.FFFF.FFFF	
SRC ADDR: 000C.856D.2E7A	TYP: E0x	DATA (VARIABLE LENGTH)	FCS: 0x00000000

ARP

HARDWARE TYPE: 0x0001		PROTOCOL TYPE: 0x0800
HLEN: 0x06	PLEN: 0x04	OPCODE: 0x0001
SOURCE MAC: 000C.856D.2E7A		
SOURCE IP: 192.168.1.1		
TARGET MAC: 0000.0000.0000		
TARGET IP: 192.168.1.3		

ARP request

PC0

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:>arp -a
No ARP Entries Found
C:>ping 192.168.1.3
① arp
② សុចរម្យ នៅលើ
③ សាស្ត្រ ដែលមាន = FRX6 ត្រូវបាន ពិនិត្យ
Ping 192.168.1.3 with 32 bytes of data: ④ សិក្សា ping
|
```

Internetworking Standards and Technologies, Jirasak Sittigorn, Com

Address Resolution Protocol

• ARP reply

PC	IP Address	MAC Address
PC0	192.168.1.1/24	000C.856D.2E7A
PC1	192.168.1.2/24	0001.42D8.7735
PC2	192.168.1.3/24	00E0.8FDE.22E3
PC3	192.168.4.2/24	0002.1755.E243

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device
0.000	--	PC0	
0.000	--	PC0	
0.001	PC0	Hub0	
0.002	Hub0	PC1	
0.002	Hub0	PC2	

PDU Information at Device: Hub0

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160	164	168	172	176	180	184	188	192	196	200	204	208	212	216	220	224	228	232	236	240	244	248	252	256	260	264	268	272	276	280	284	288	292	296	300	304	308	312	316	320	324	328	332	336	340	344	348	352	356	360	364	368	372	376	380	384	388	392	396	400	404	408	412	416	420	424	428	432	436	440	444	448	452	456	460	464	468	472	476	480	484	488	492	496	500	504	508	512	516	520	524	528	532	536	540	544	548	552	556	560	564	568	572	576	580	584	588	592	596	600	604	608	612	616	620	624	628	632	636	640	644	648	652	656	660	664	668	672	676	680	684	688	692	696	700	704	708	712	716	720	724	728	732	736	740	744	748	752	756	760	764	768	772	776	780	784	788	792	796	800	804	808	812	816	820	824	828	832	836	840	844	848	852	856	860	864	868	872	876	880	884	888	892	896	900	904	908	912	916	920	924	928	932	936	940	944	948	952	956	960	964	968	972	976	980	984	988	992	996	1000
---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

ARP

0	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	136	144	152	160	168	176	184	192	200	208	216	224	232	240	248	256	264	272	280	288	296	304	312	320	328	336	344	352	360	368	376	384	392	400	408	416	424	432	440	448	456	464	472	480	488	496	504	512	520	528	536	544	552	560	568	576	584	592	600	608	616	624	632	640	648	656	664	672	680	688	696	704	712	720	728	736	744	752	760	768	776	784	792	800	808	816	824	832	840	848	856	864	872	880	888	896	904	912	920	928	936	944	952	960	968	976	984	992	1000
---	---	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

Physical

```

Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
| 

```

Config

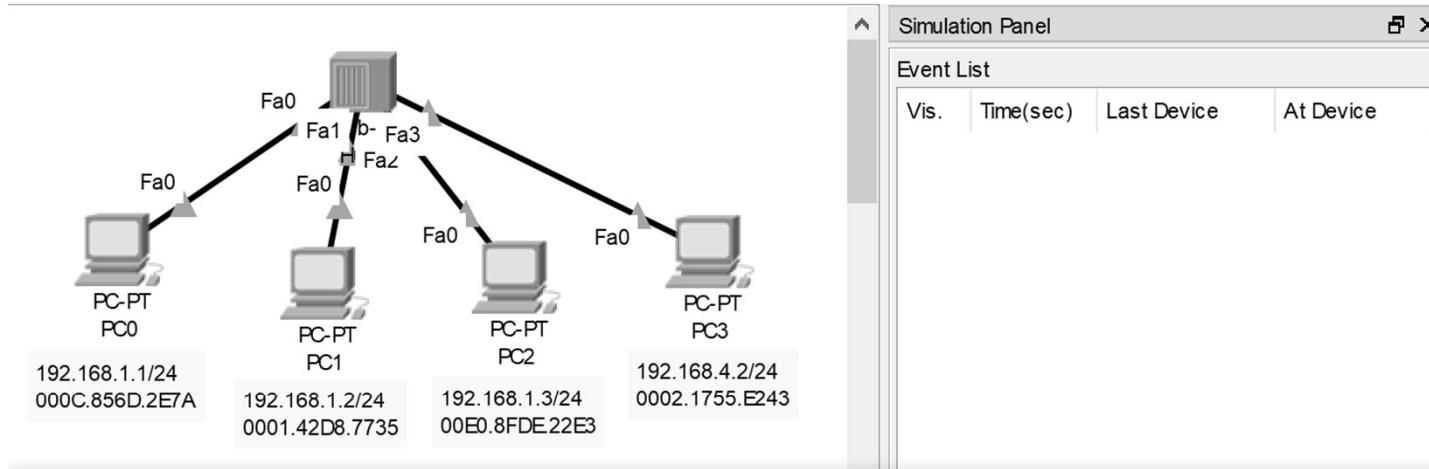
Desktop

Programming

Attributes

Attributes

Address Resolution Protocol



PC0

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=8ms TTL=128
Reply from 192.168.1.3: bytes=32 time=22ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 22ms, Average = 7ms

C:\>arp -a
Internet Address      Physical Address          Type
 192.168.1.3           00e0.8fde.22e3       dynamic

C:\>
C:\>
```

IPv4 *(IPv4 là classful)*

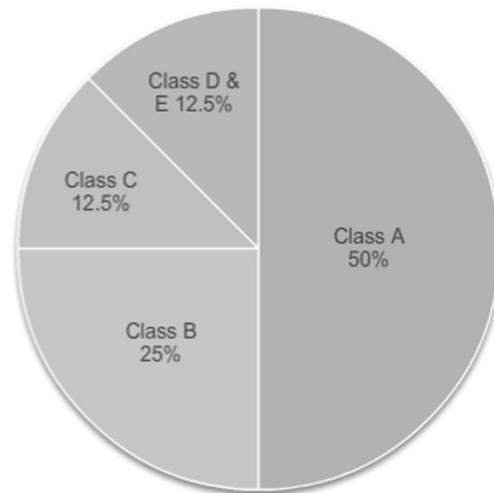
- Classful Addressing Waste

Classfull IP Address Allocation = Inefficient

Class A (1 - 126)
 # of possible networks: 126
 # of Hosts/Net: 16,777,214
 Max. # Hosts: 2,113,928,964

Class B (128 - 191)
 # of possible networks: 16,384
 # of Hosts/Net: 65,534
 Max. # Hosts: 1,073,709,056

Class C (192 - 223)
 # of possible networks: 2,097,152
 # of Hosts/Net: 254
 Max. # Hosts: 532,676,608



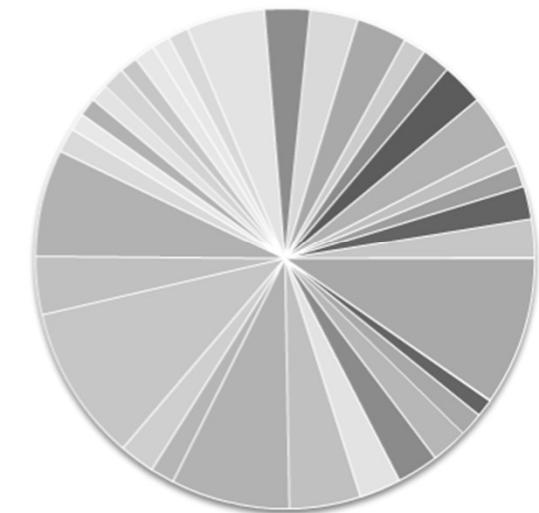
- Classless Inter-Domain Routing

CIDR = Efficient

Class A (1 - 126)
 X
 # of possible networks: 126
 # of Hosts/Net: 16,777,214
 Max. # Hosts: 2,113,928,964

Class B (128 - 191)
 X
 # of possible networks: 16,384
 # of Hosts/Net: 65,534
 Max. # Hosts: 1,073,709,056

Class C (192 - 223)
 X
 # of possible networks: 2,097,152
 # of Hosts/Net: 254
 Max. # Hosts: 532,676,608



Min 120 30 25 10] 110 in 192.168.1.0/24
 Max 128 32 32 16 11]
 192.168.1.0/24

IPv4

- Classless Inter-Domain Routing
 - Fixed Length Subnet Masking
 - 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

Subnet Mask	CIDR Value
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

0	_____
4	_____
8	_____
12	_____
16	_____
20	_____
24	_____
28	_____
32	_____
36	_____
40	_____
44	_____
48	_____
52	_____
56	_____
60	_____
64	_____
68	_____
72	_____
76	_____
80	_____
84	_____
88	_____
92	_____
96	_____
100	_____
104	_____
108	_____
112	_____
116	_____
120	_____
124	_____
128	_____
132	_____
136	_____
140	_____
144	_____
148	_____
152	_____
156	_____
160	_____
164	_____
168	_____
172	_____
176	_____
180	_____
184	_____
188	_____
192	_____
196	_____
200	_____
204	_____
208	_____
212	_____
216	_____
220	_____
224	_____
228	_____
232	_____
236	_____
240	_____
244	_____
248	_____
252	_____
256	_____

Subnet Planning

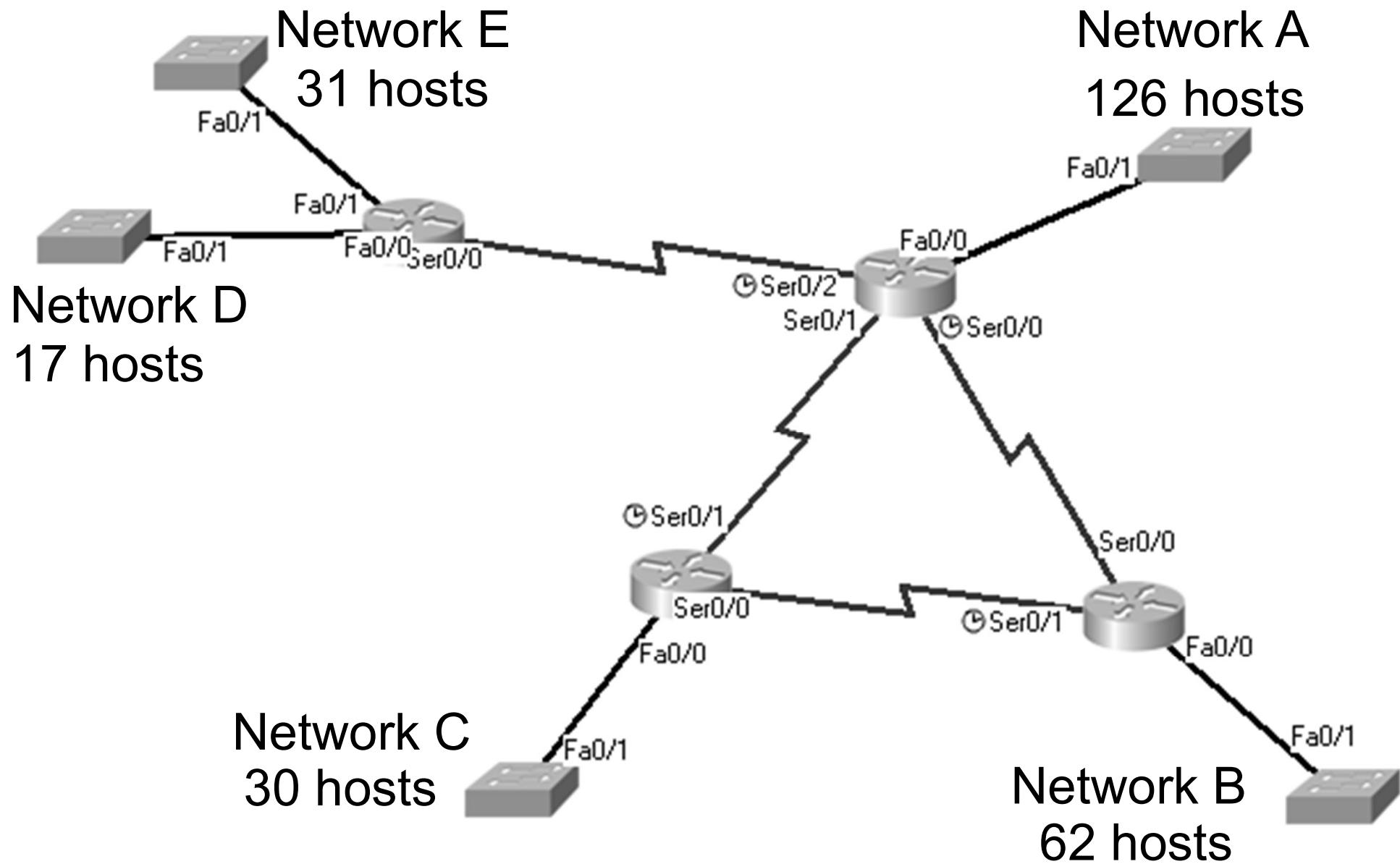
- Network 161.246.6.0/23

- 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

Subnet Planning

4a
08/11/2021



Subnet Planning

③ សំគាល់

①

④ តម្លៃសុវត្ថិភាព

② ផលិតផល

Network	Req. Host	Max. Host	Subnetwork 	Subnet mask
A	① 126	126	check 0	255.255.255.0
B	② 62	60		255.255.255.192
C	③ 30	30		255.255.255.224
D	④ 17	30		255.255.255.224
E	⑤ 31	66		255.255.255.192

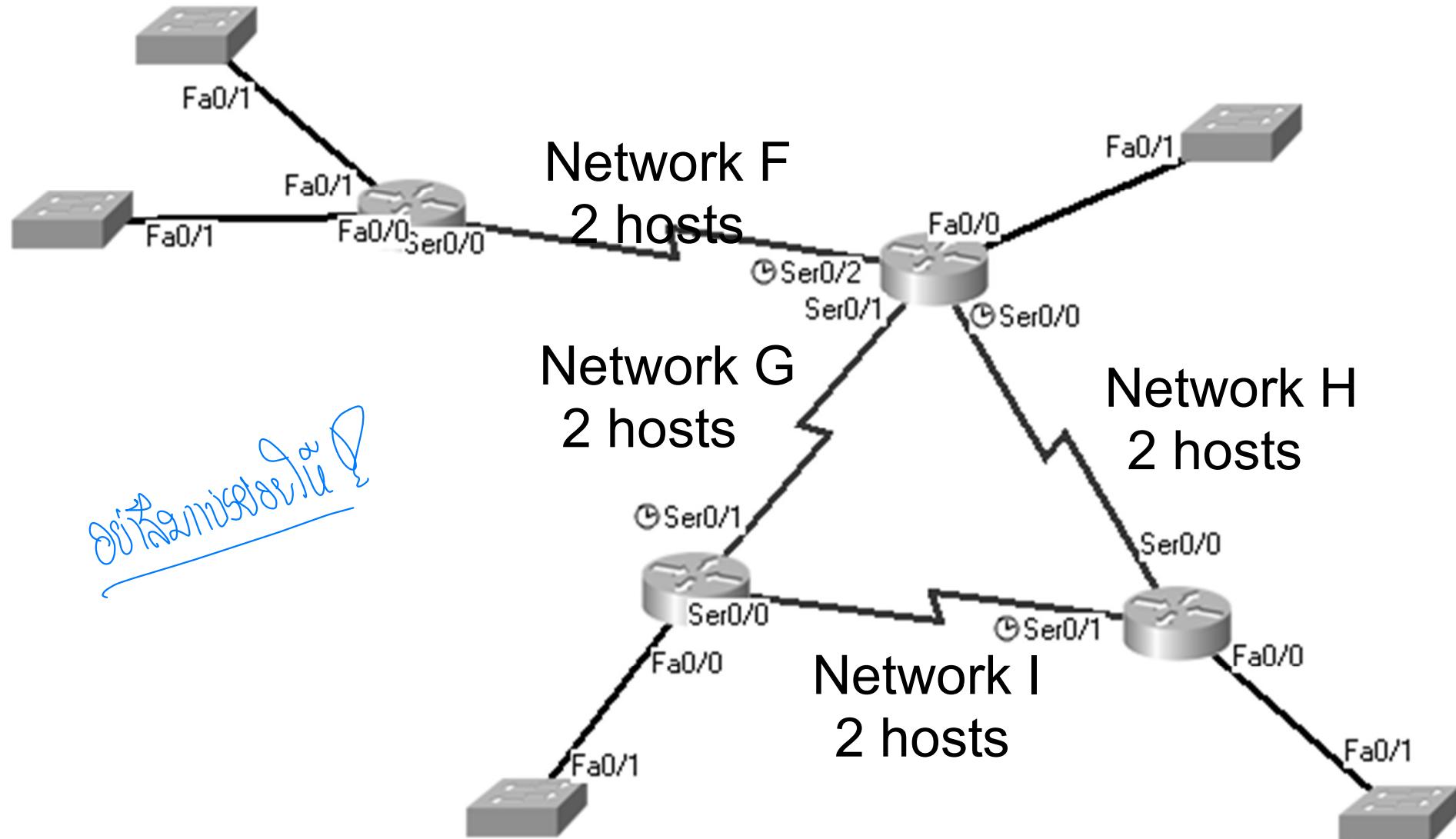
ក្រោមនេះជាបង្ហាញ → ឈ្មោះ (IP) នៅ → ឈ្មោះ (ផលិតផល)

161.246.6.x
0
4
8
12
16
20
24
28
32
36
40
44
48
52
56
60
64
68
72
76
80
84
88
92
96
100
104
108
112
116
120
124
128
132
136
140
144
148
152
156
160
164
168
172
176
180
184
188
192
196
200
204
208
212
216
220
224
228
232
236
240
244
248
252
256

6 ពាន់ខ្លួន

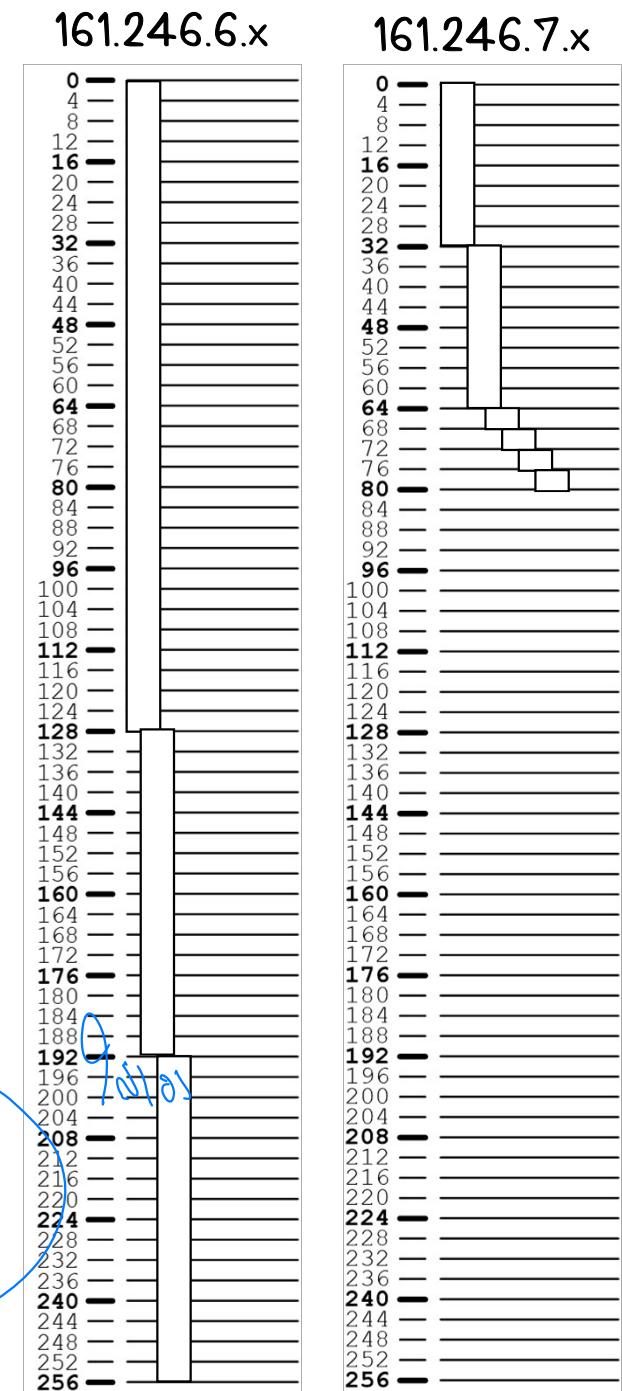
6 ពាន់ខ្លួន

Subnet Planning



Subnet Planning

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



Questions and Answers

