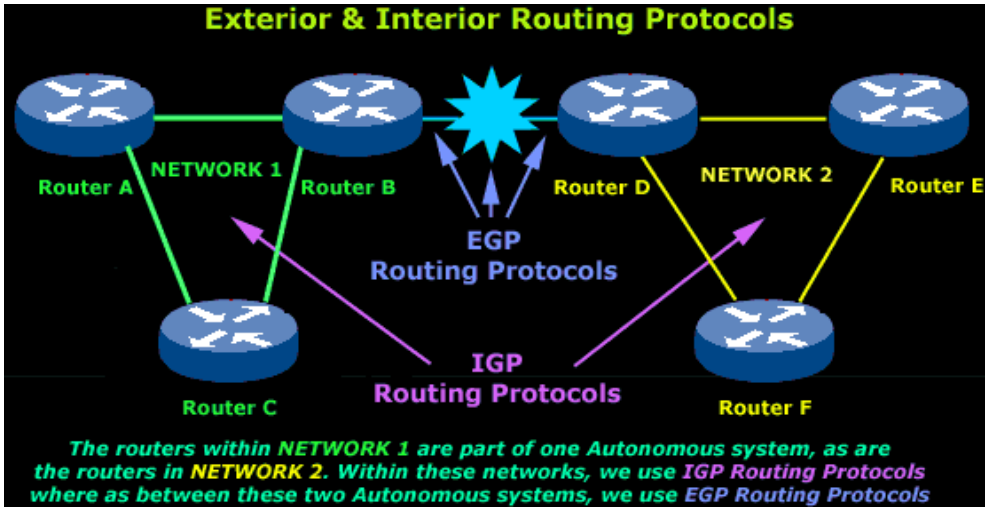
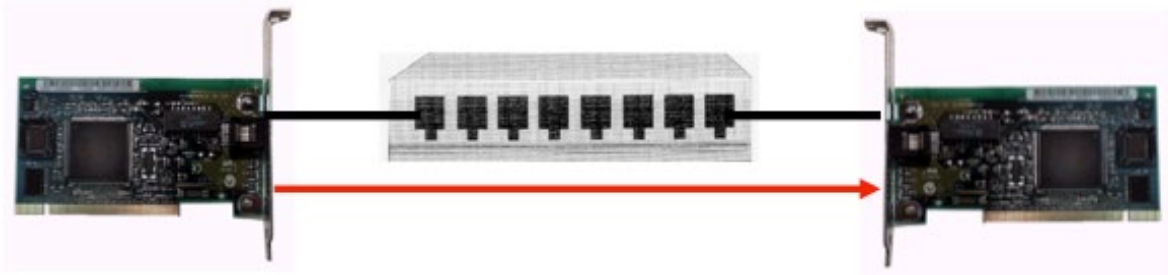
CIS 3210
Switching Concepts



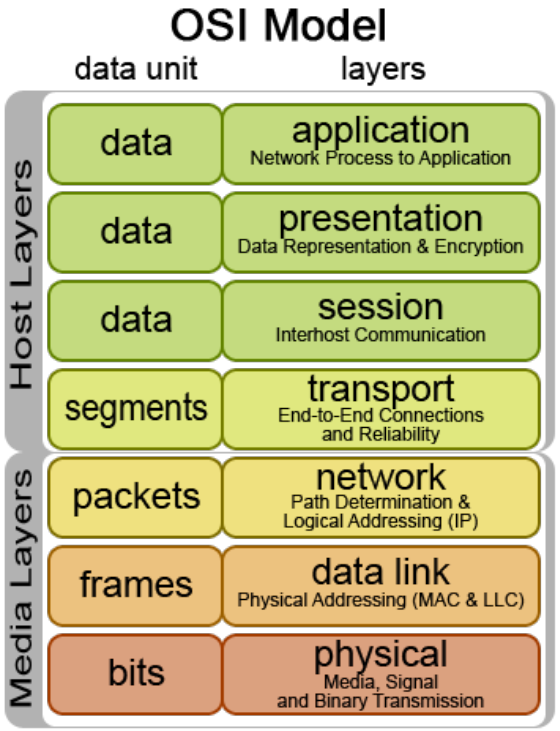
Ethernet



Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)

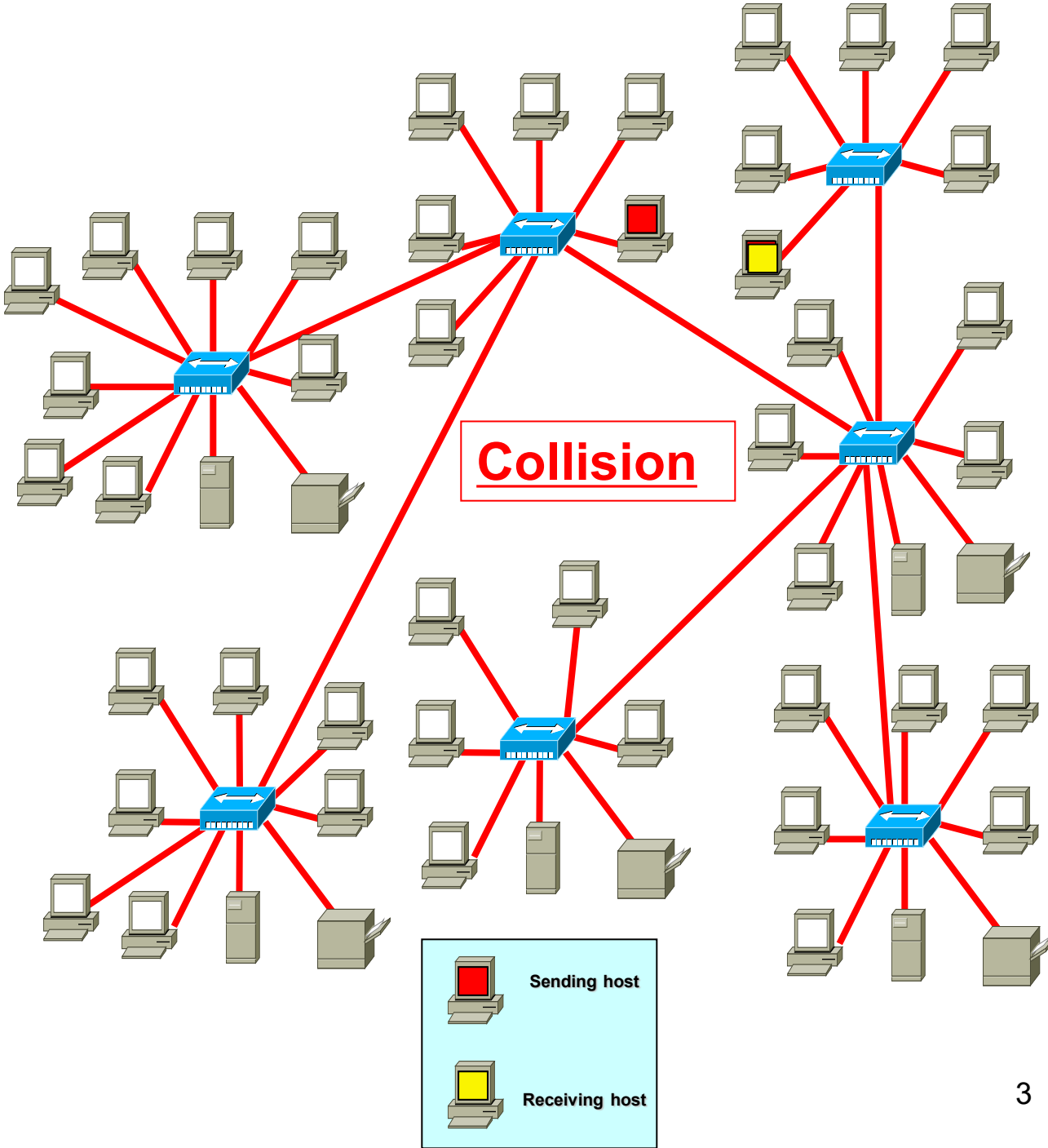
Ethernet

- Layer 2 – Data Link Layer
- NIC (Source MAC address) to NIC (Destination MAC address) communications in the same network
- Source MAC address – Address of the sender's NIC
- Destination MAC address
  - Unicast: MAC address of destination NIC on the same network
  - Broadcast: All 1 bits (F's)



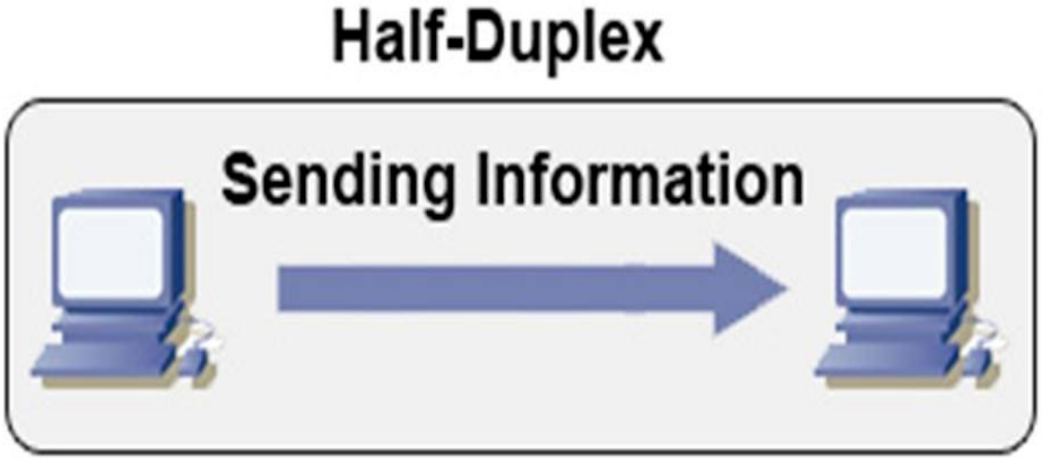
Hubs

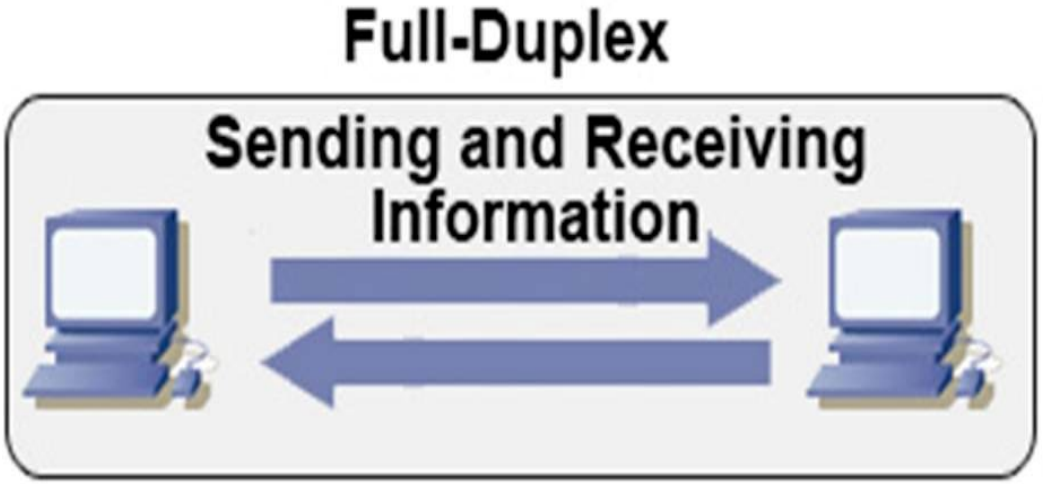
- Legacy
- Layer 1 devices
- Multi-port repeaters
- Shared bandwidth
- Based on legacy bus topology
- CSMA/CD
- Single collision domain



Switches

- Layer 2 devices
- Also operates at layer 1
- Full duplex
- Dedicated bandwidth





Forwarding Frames

Unicast

Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)
BBBB	AAAA			

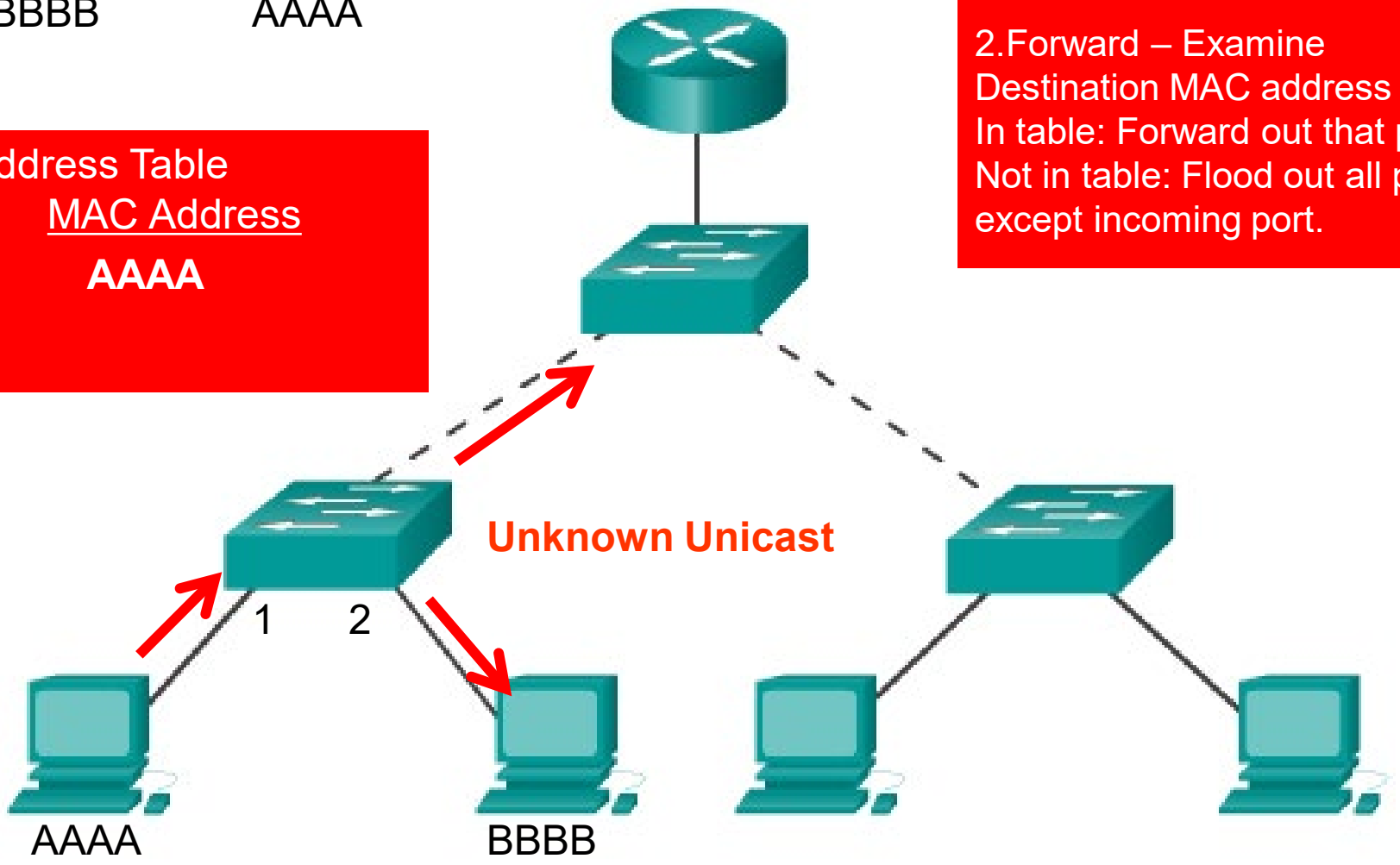
Mac Address Table

Port	MAC Address
1	**AAAA**

Mac Address Table

1.Learn – Examine Source MAC address
In table: Reset 5 min timer
Not in table: Add Source MAC address and port # to table

2.Forward – Examine Destination MAC address
In table: Forward out that port.
Not in table: Flood out all ports except incoming port.



Forwarding Frames

Unicast

Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)
AAAA	BBBB			

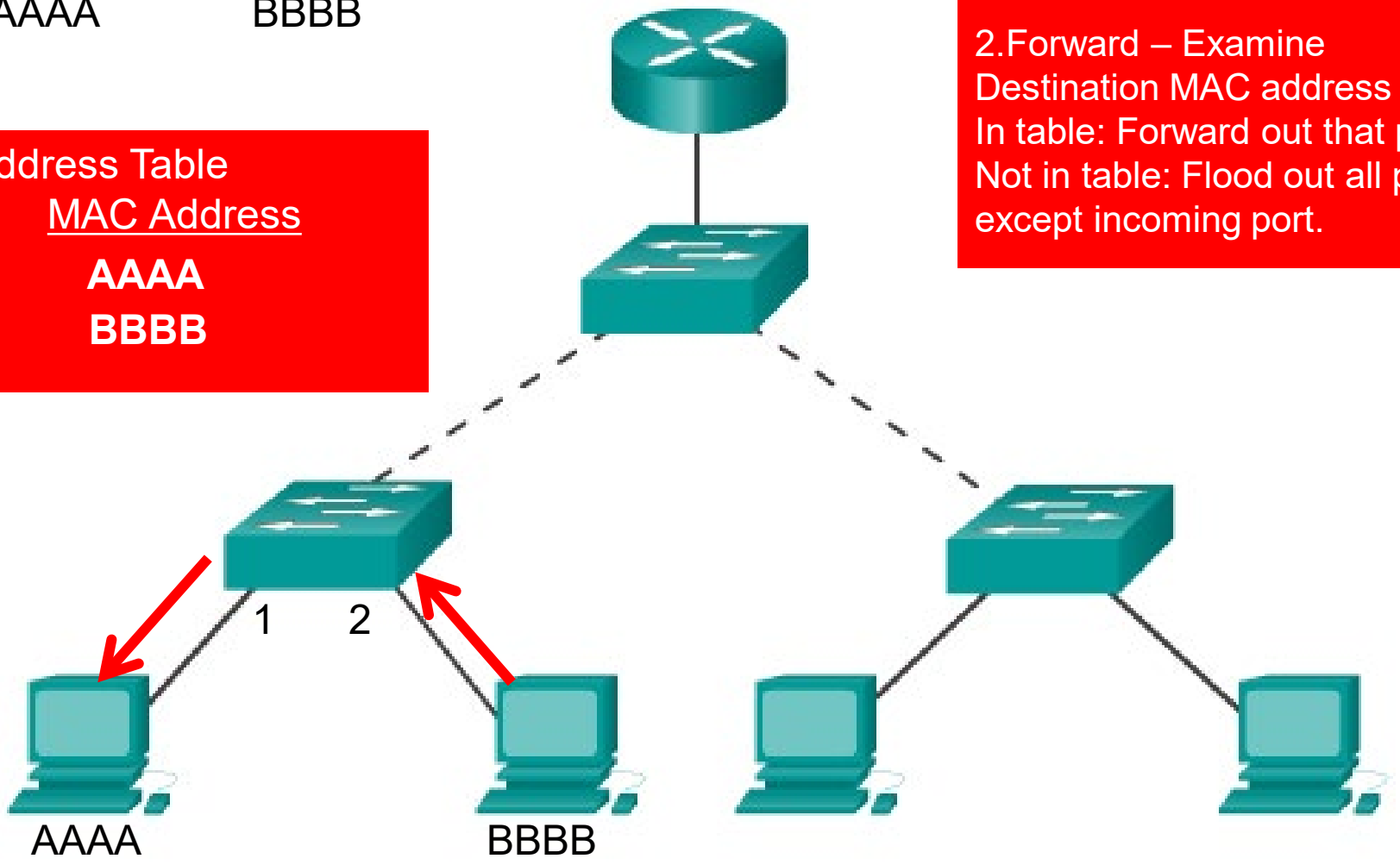
Mac Address Table

Port	MAC Address
1	**AAAA**
2	**BBBB**

Mac Address Table

1.Learn – Examine Source MAC address
In table: Reset 5 min timer
Not in table: Add Source MAC address and port # to table

2.Forward – Examine Destination MAC address
In table: Forward out that port.
Not in table: Flood out all ports except incoming port.



Forwarding Frames

Unicast

Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)
BBBB	AAAA			

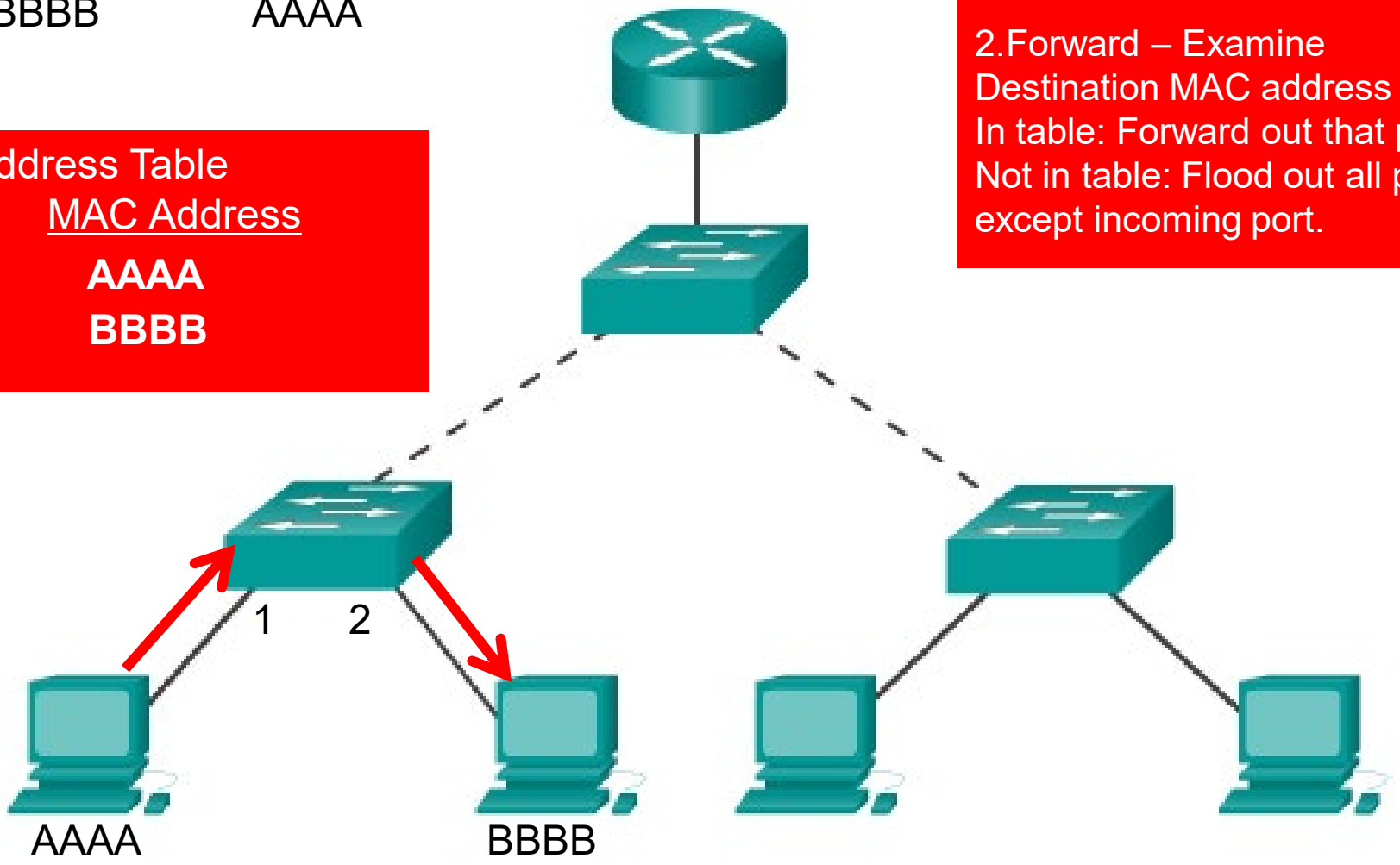
Mac Address Table

Port	MAC Address
1	**AAAA**
2	**BBBB**

Mac Address Table

1.Learn – Examine Source MAC address
In table: Reset 5 min timer
Not in table: Add Source MAC address and port # to table

2.Forward – Examine Destination MAC address
In table: Forward out that port.
Not in table: Flood out all ports except incoming port.



Forwarding Frames

Broadcast

Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)
FFFF	AAAA			

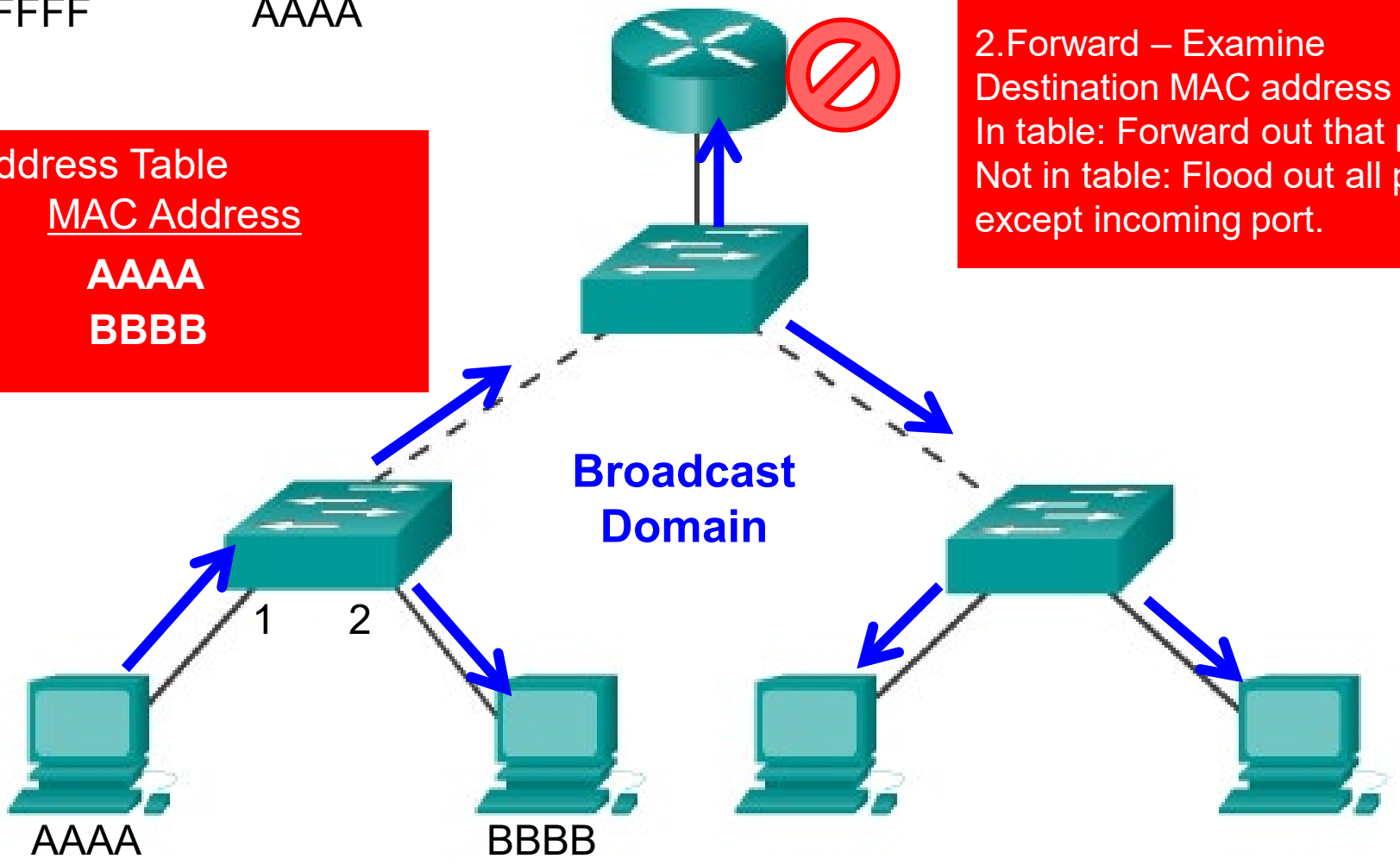
Mac Address Table

Port	MAC Address
1	AAAA
2	BBBB

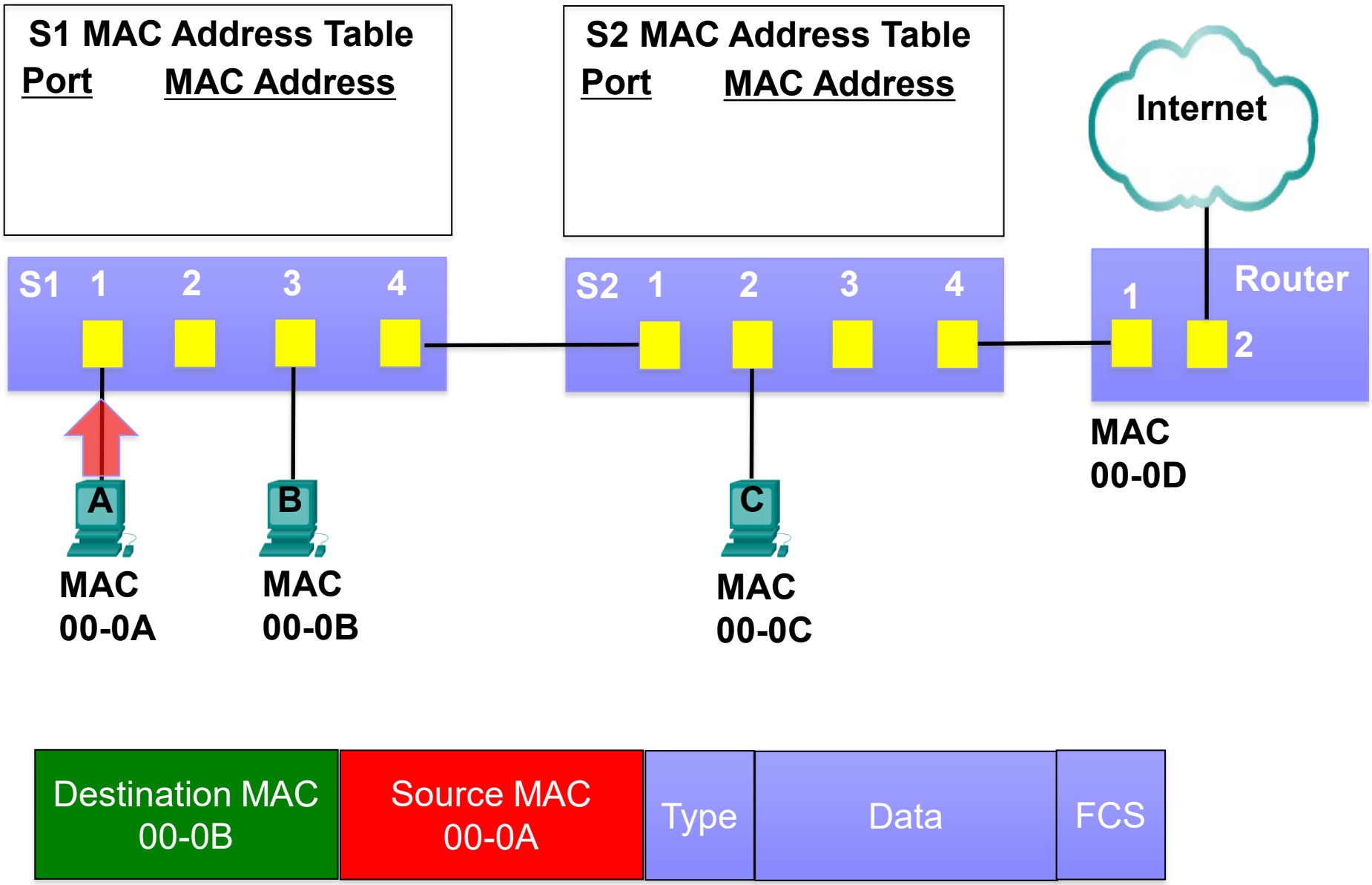
Mac Address Table

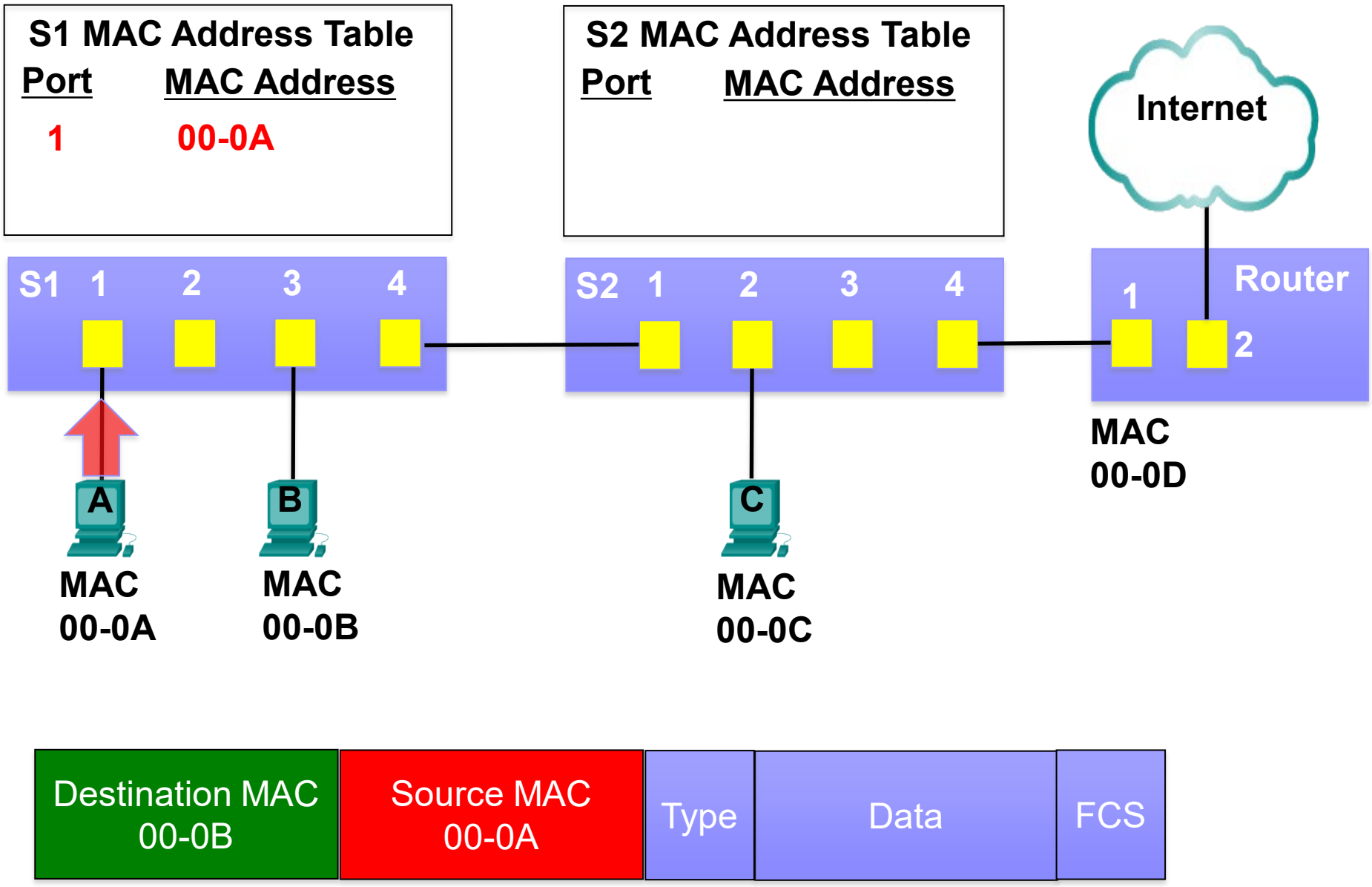
1.Learn – Examine Source MAC address
In table: Reset 5 min timer
Not in table: Add Source MAC address and port # to table

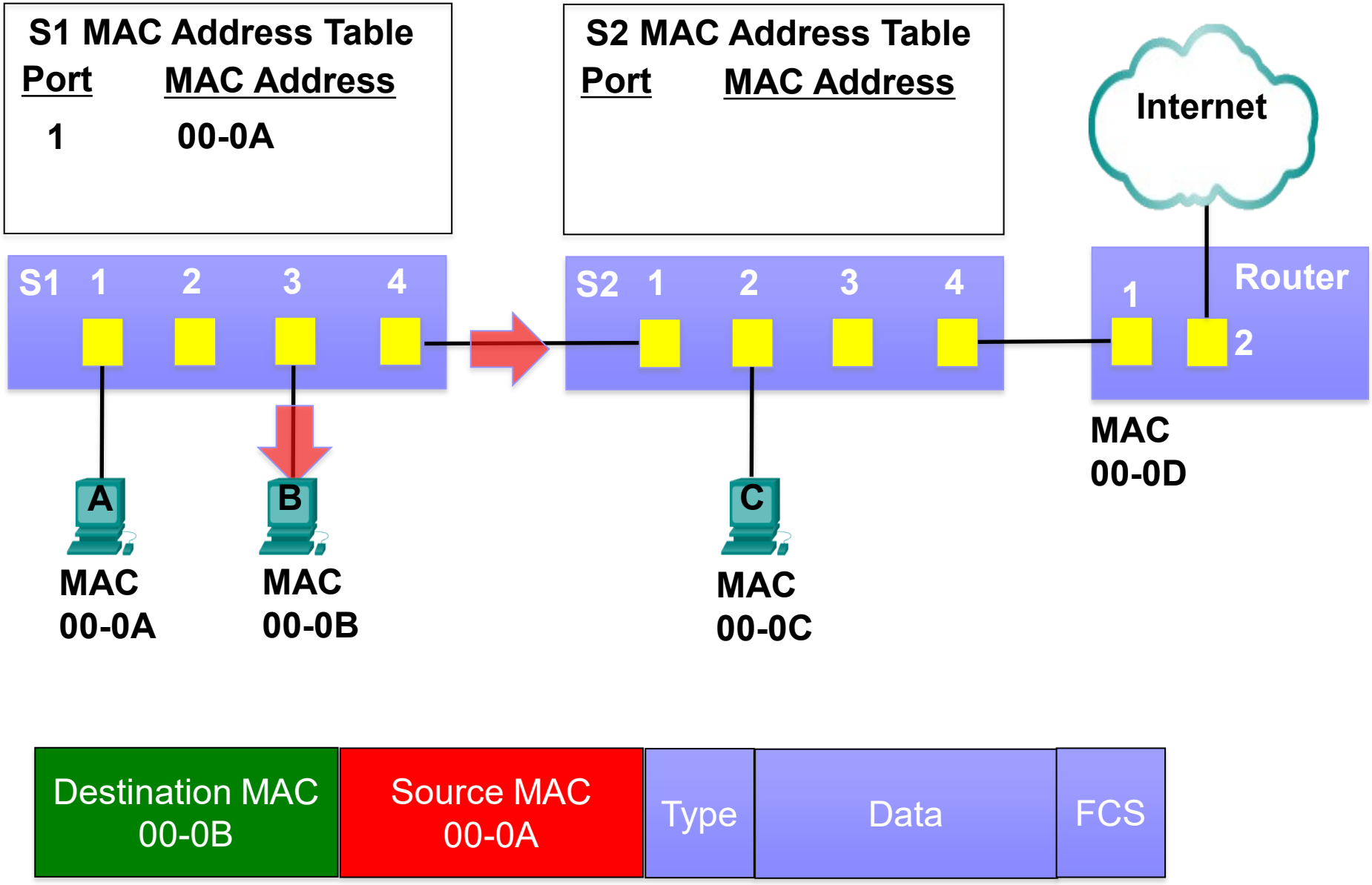
2.Forward – Examine Destination MAC address
In table: Forward out that port.
Not in table: Flood out all ports except incoming port.

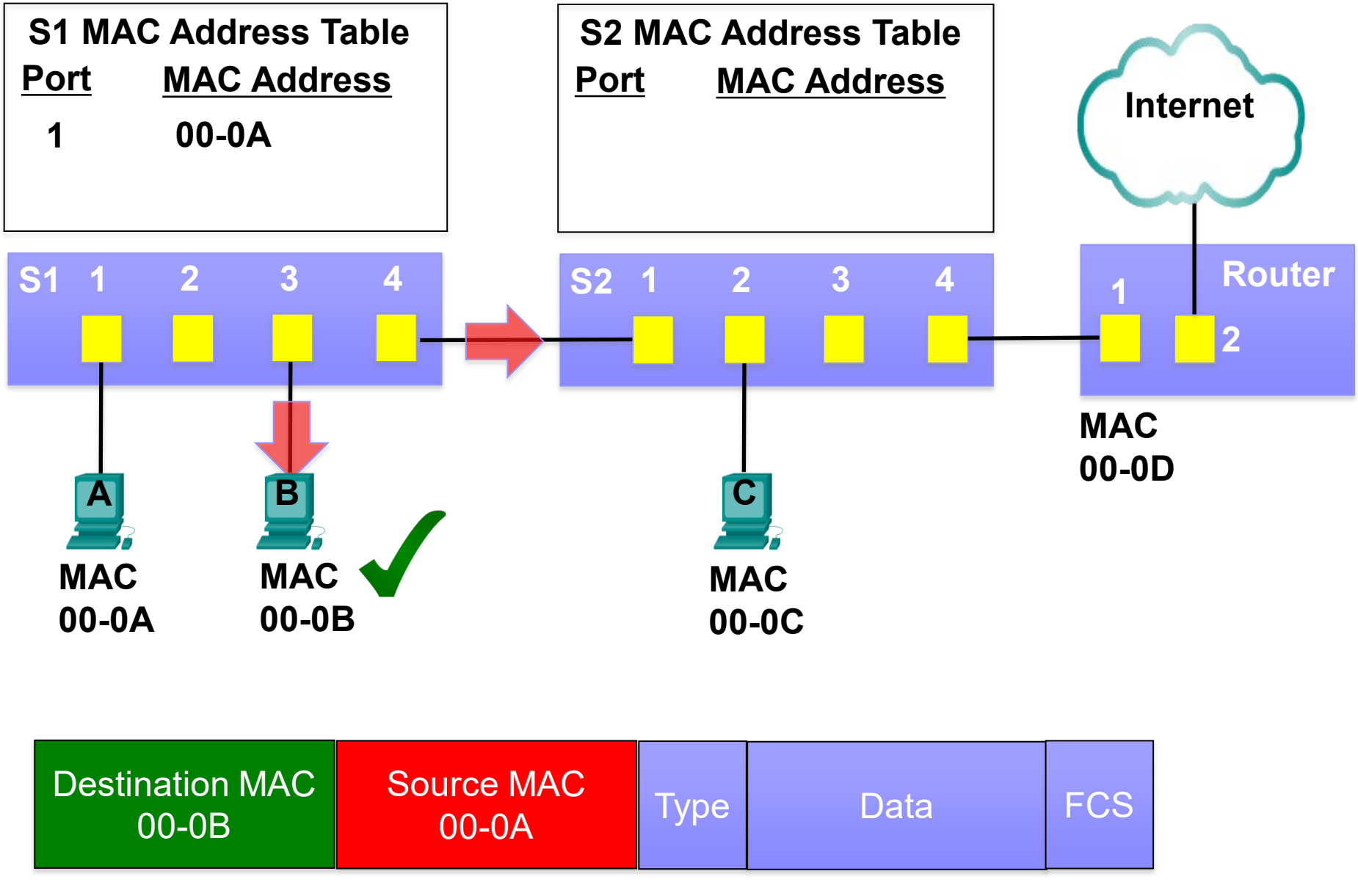


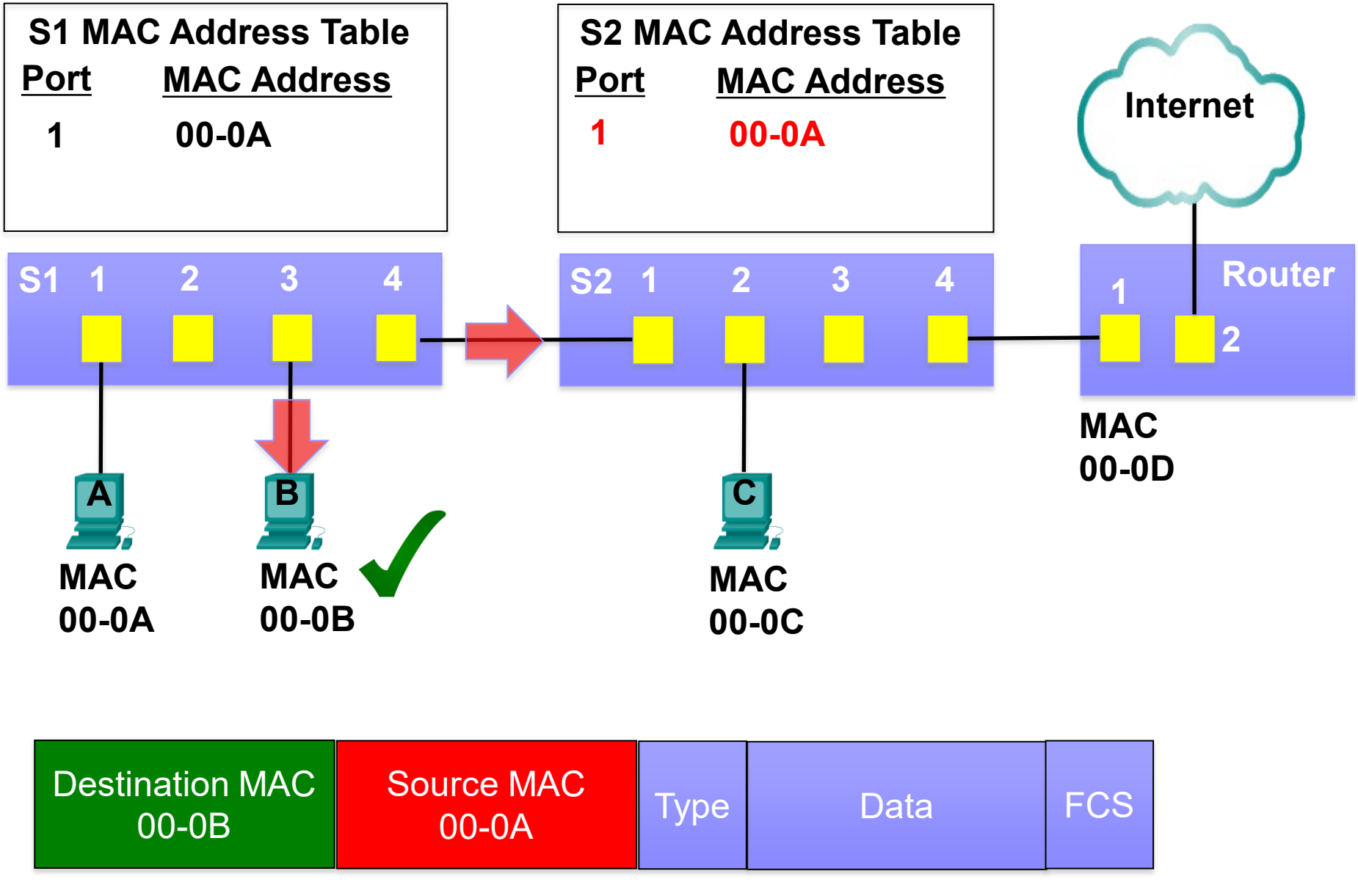
MAC Address Tables on Connected Switches

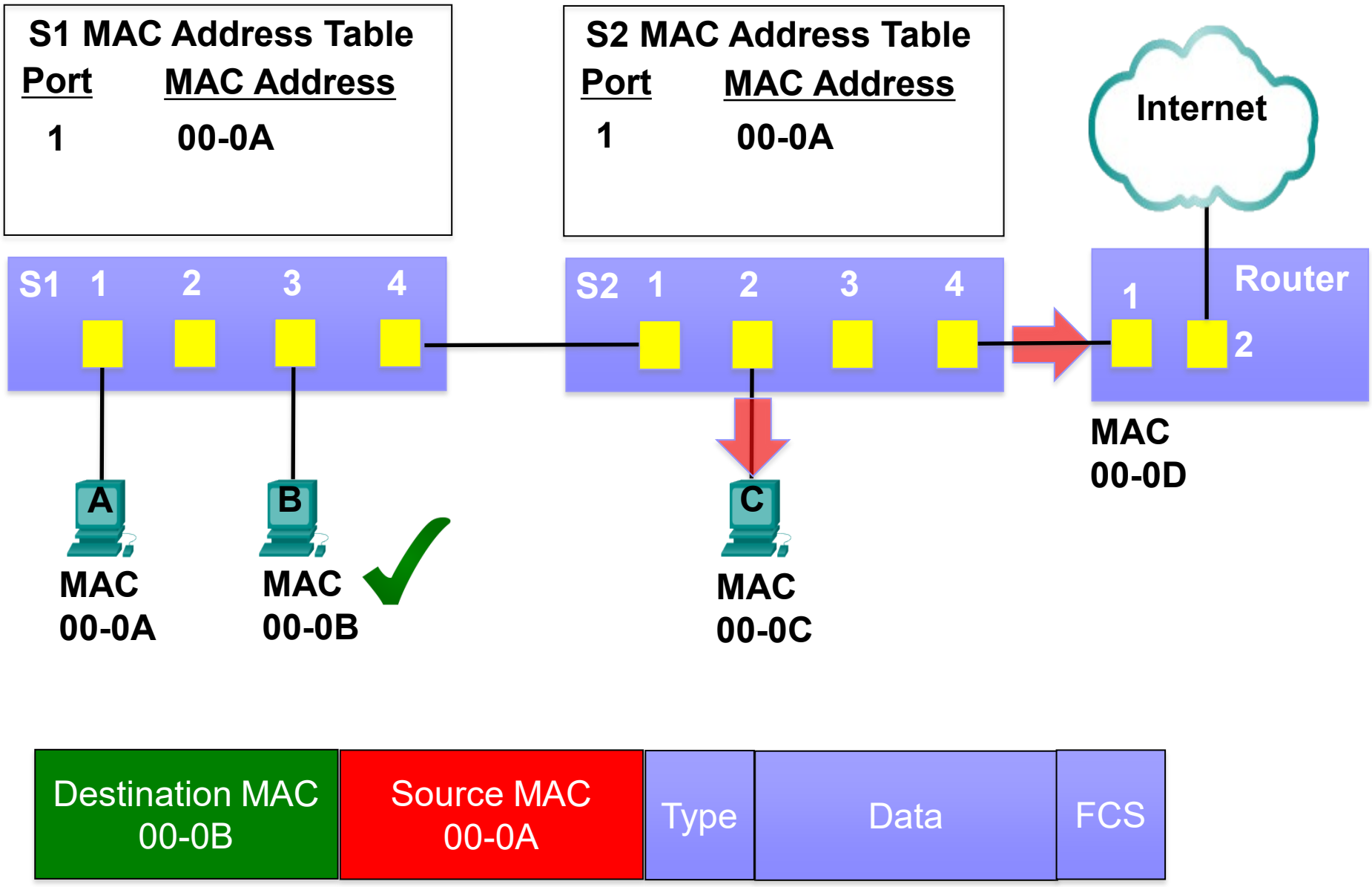

S1 MAC Address Table
Port
MAC Address
S2 MAC Address Table
Port
MAC Address
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS

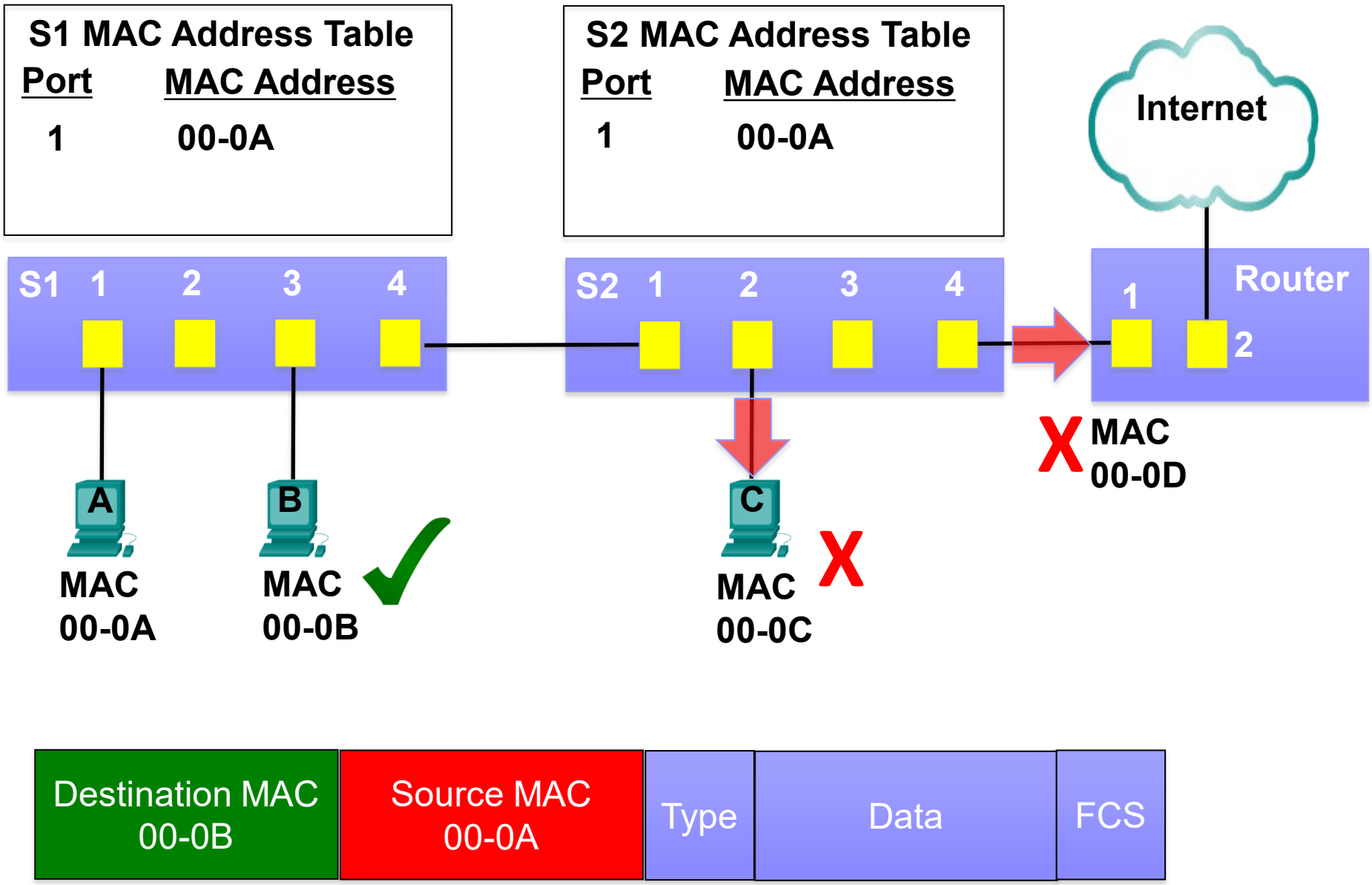

S1 MAC Address Table
Port
MAC Address
1
00-0A
S2 MAC Address Table
Port
MAC Address
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS

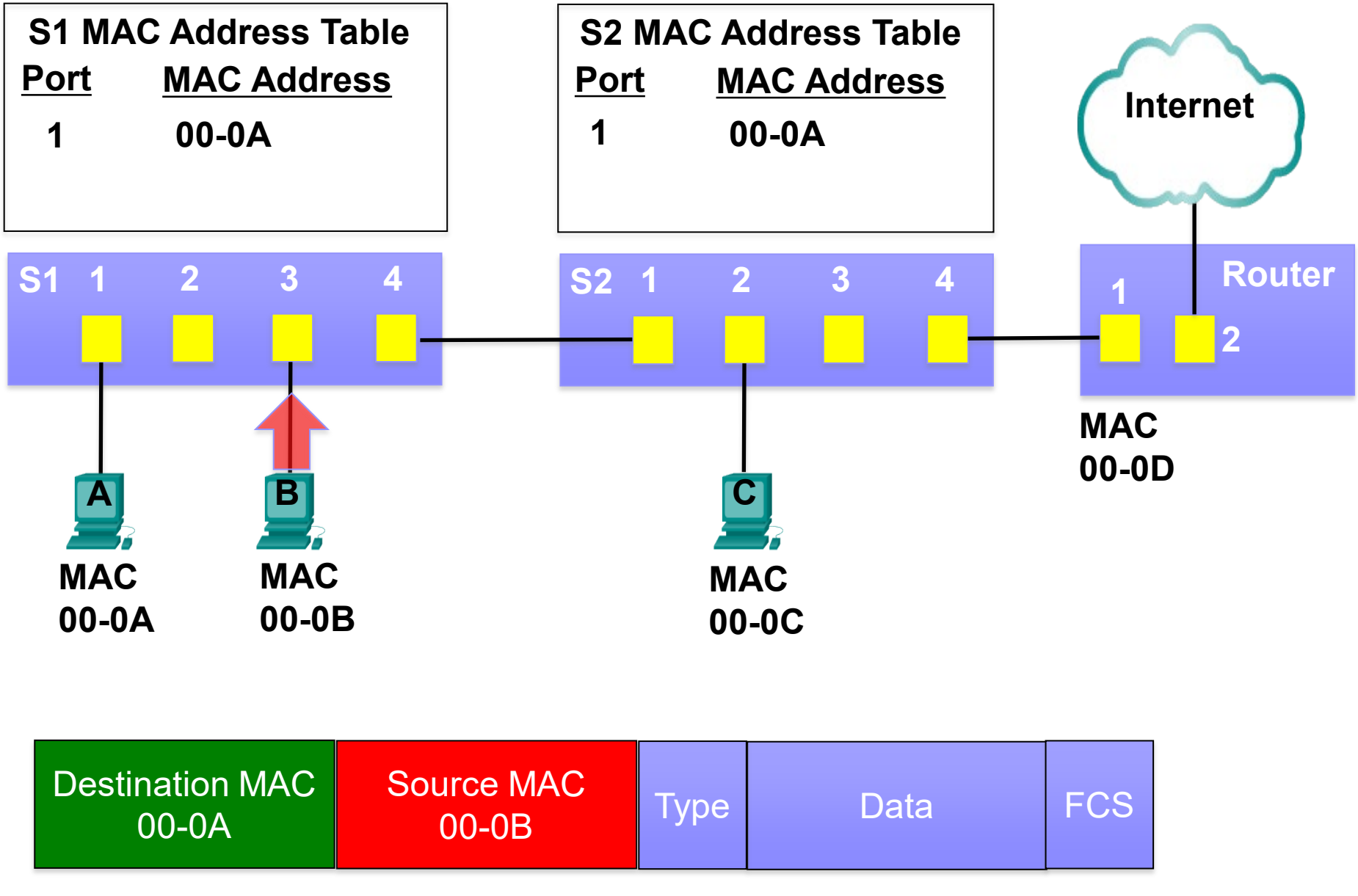

S1 MAC Address Table
Port
MAC Address
1
00-0A
S2 MAC Address Table
Port
MAC Address
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS

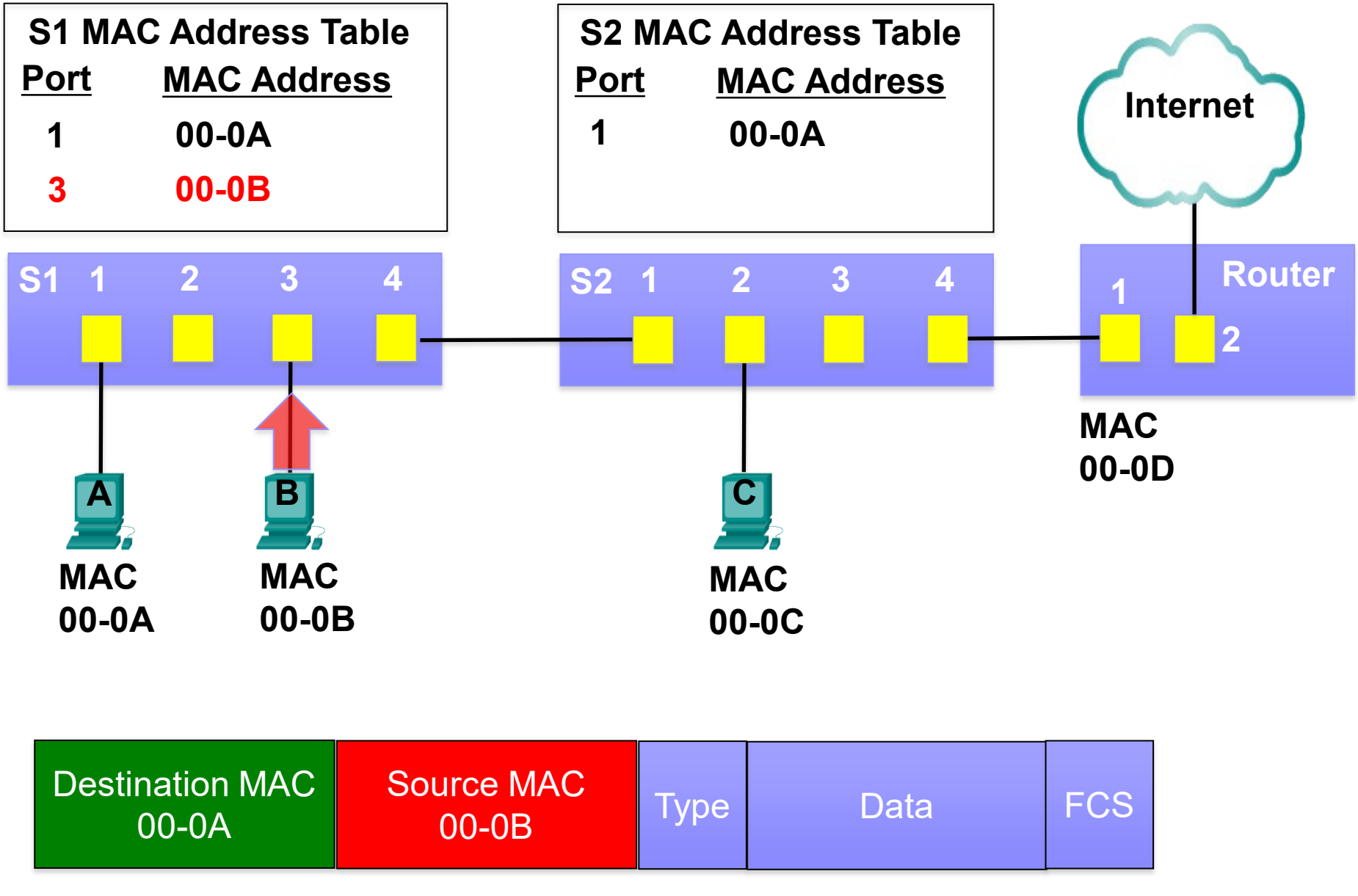

S1 MAC Address Table
Port
MAC Address
1
00-0A
S2 MAC Address Table
Port
MAC Address
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS

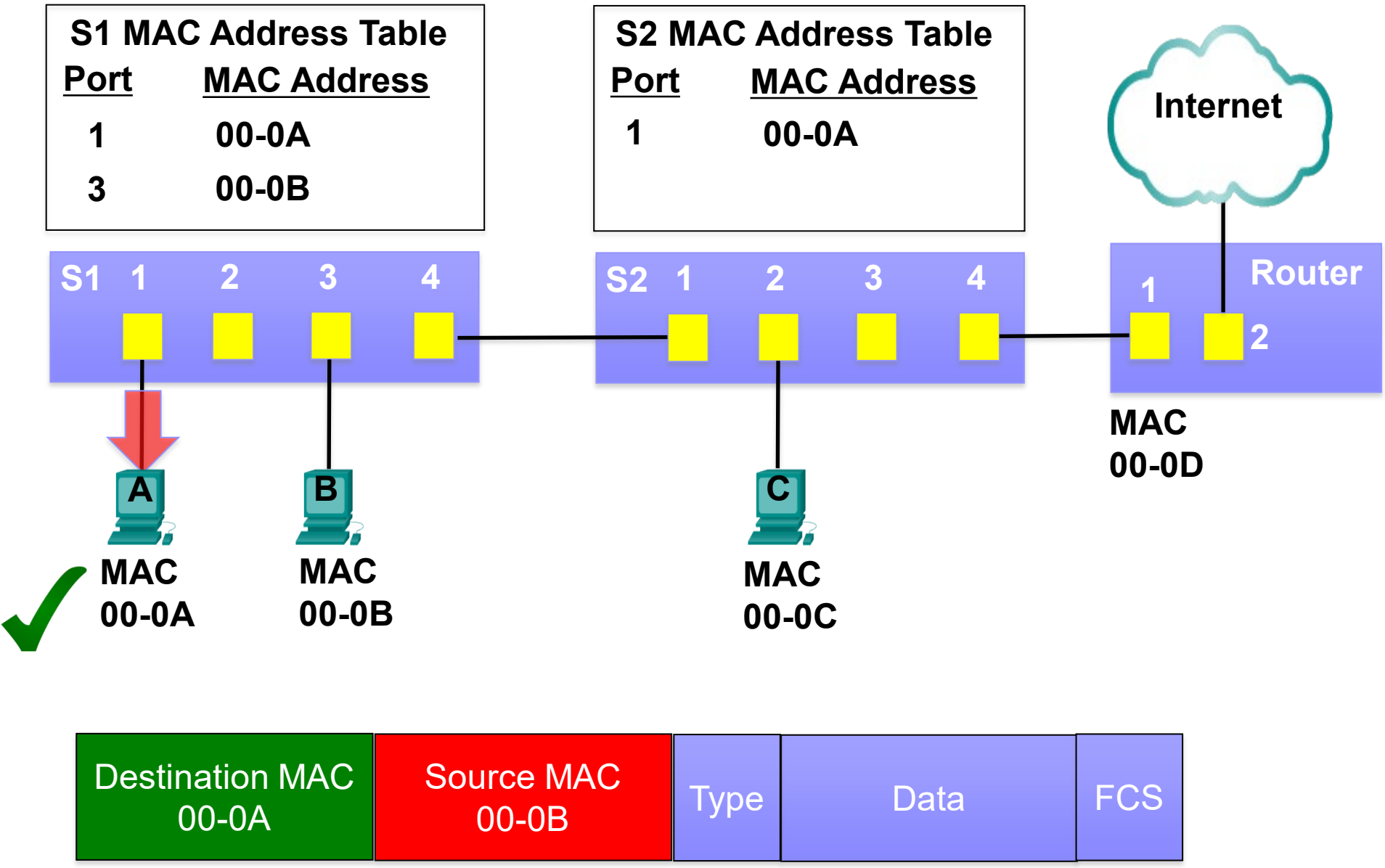

S1 MAC Address Table
Port
MAC Address
1
00-0A
S2 MAC Address Table
Port
MAC Address
1
00-0A
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS


S1 MAC Address Table
Port
MAC Address
1
00-0A
S2 MAC Address Table
Port
MAC Address
1
00-0A
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS


S1 MAC Address Table
Port
MAC Address
1
00-0A
S2 MAC Address Table
Port
MAC Address
1
00-0A
Internet
S1
1
2
3
4
S2
1
2
3
4
Router
1
2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0B
Source MAC
00-0A
Type
Data
FCS


S1 MAC Address Table
Port MAC Address
1 00-0A
S2 MAC Address Table
Port MAC Address
1 00-0A
Internet
S1 1 2 3 4
S2 1 2 3 4
Router
1 2
MAC
00-0D
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
Destination MAC
00-0A
Source MAC
00-0B
Type
Data
FCS


S1 MAC Address Table
Port MAC Address
1 00-0A
3 00-0B
S2 MAC Address Table
Port MAC Address
1 00-0A
Internet
S1 1 2 3 4
S2 1 2 3 4
Router
1 2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0A
Source MAC
00-0B
Type
Data
FCS


S1 MAC Address Table
Port MAC Address
1 00-0A
3 00-0B
S2 MAC Address Table
Port MAC Address
1 00-0A
Internet
S1 1 2 3 4
S2 1 2 3 4
Router
1 2
A
B
C
MAC
00-0A
MAC
00-0B
MAC
00-0C
MAC
00-0D
Destination MAC
00-0A
Source MAC
00-0B
Type
Data
FCS

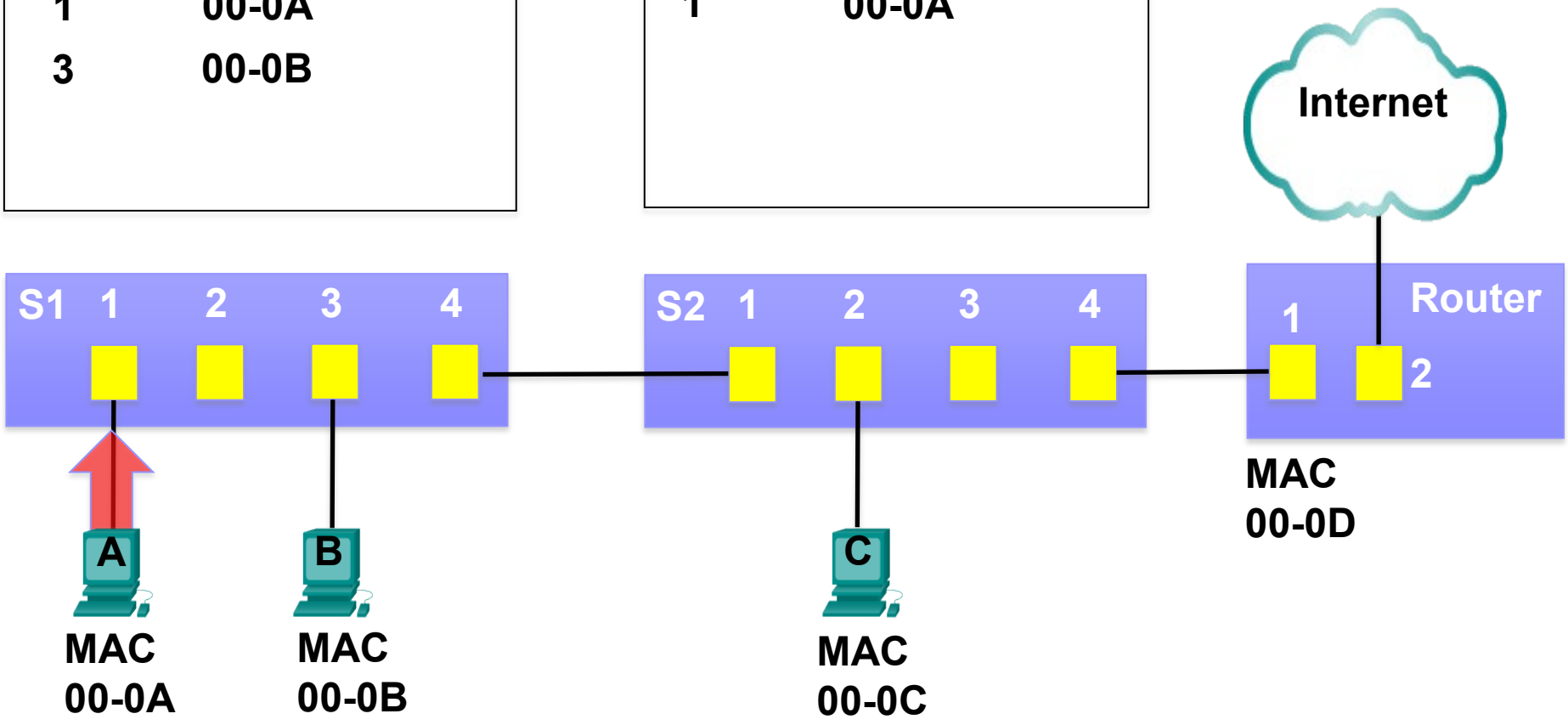
Sending a Frame to the Default Gateway

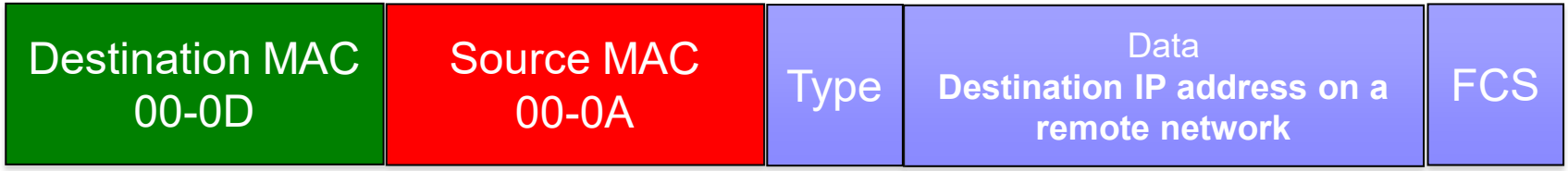
S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A



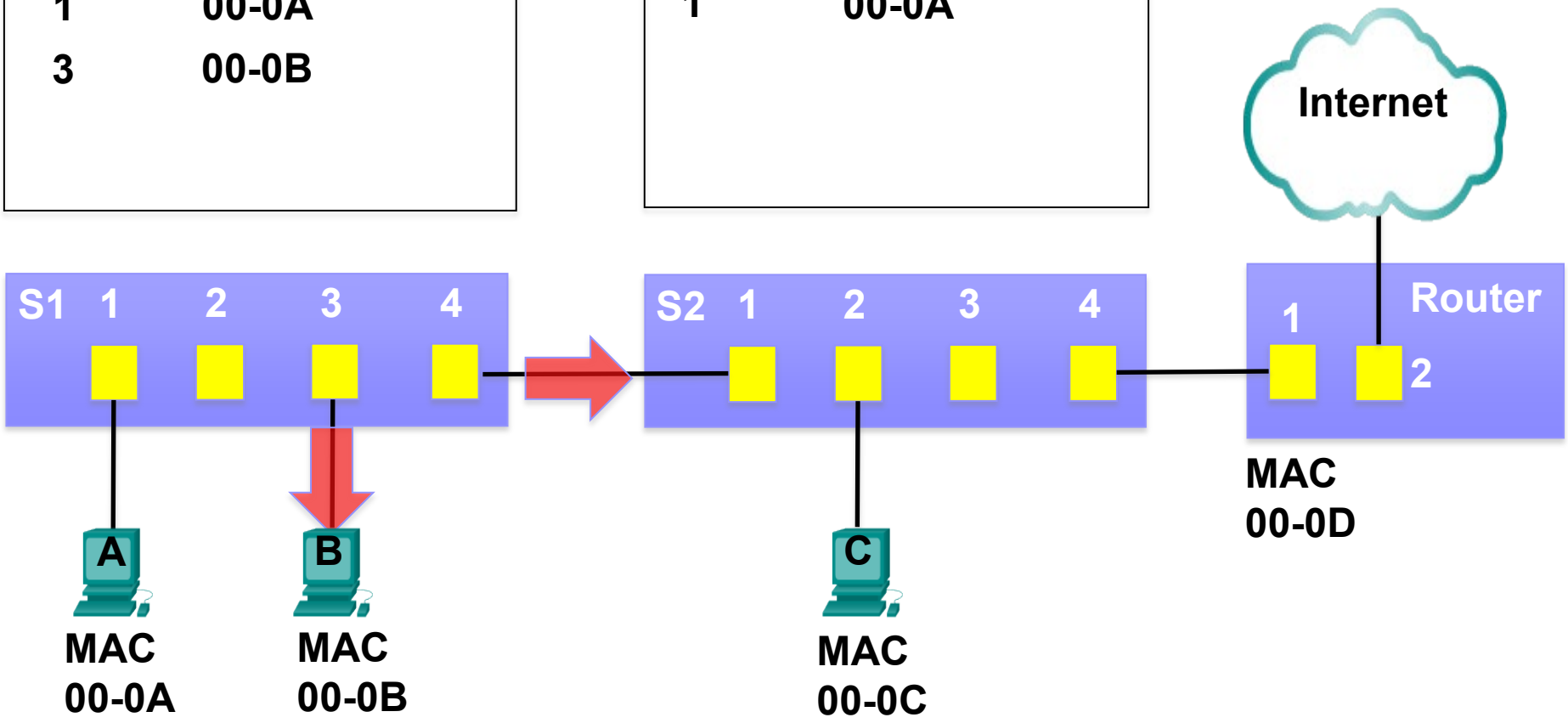


S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A



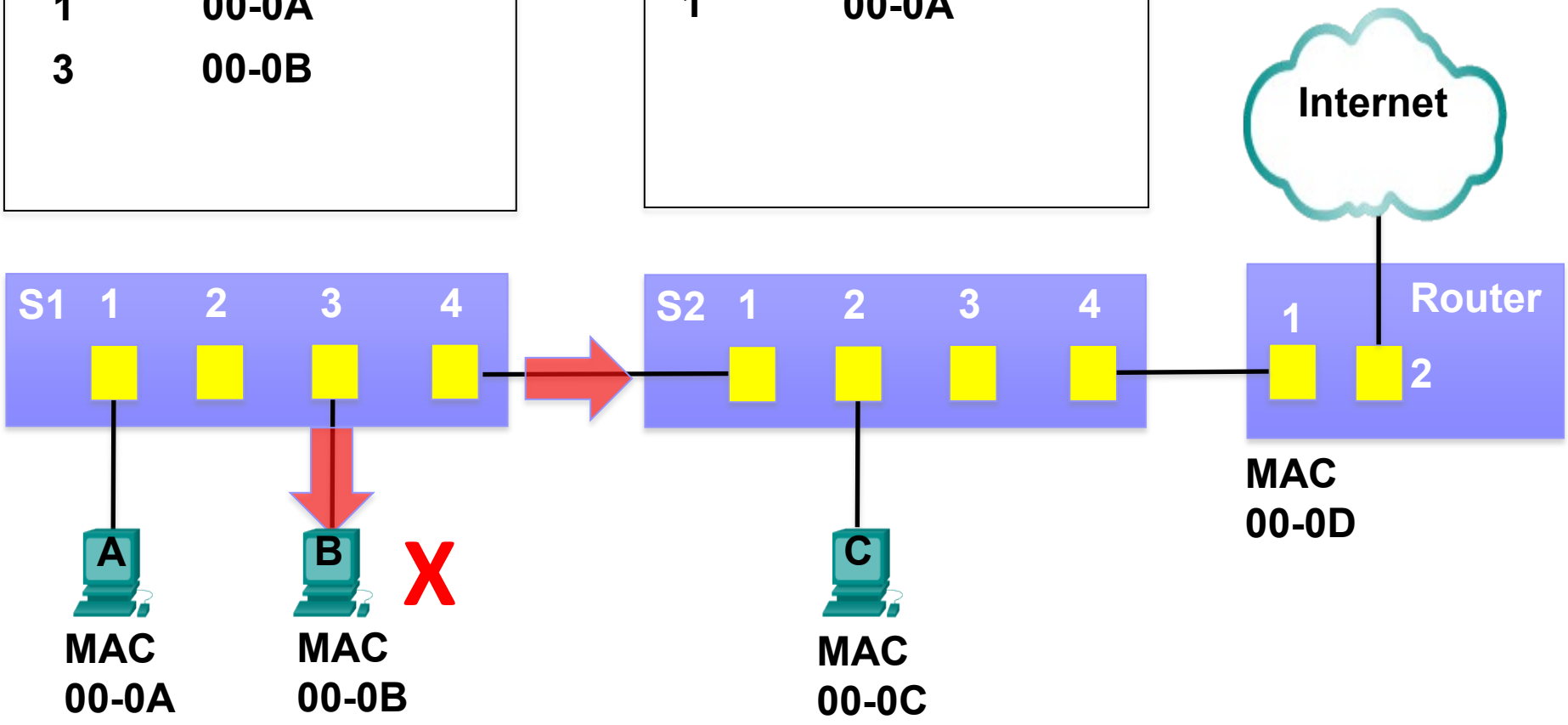
Destination MAC 00-0D	Source MAC 00-0A	Type	Data **Destination IP address on a remote network**	FCS

S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A



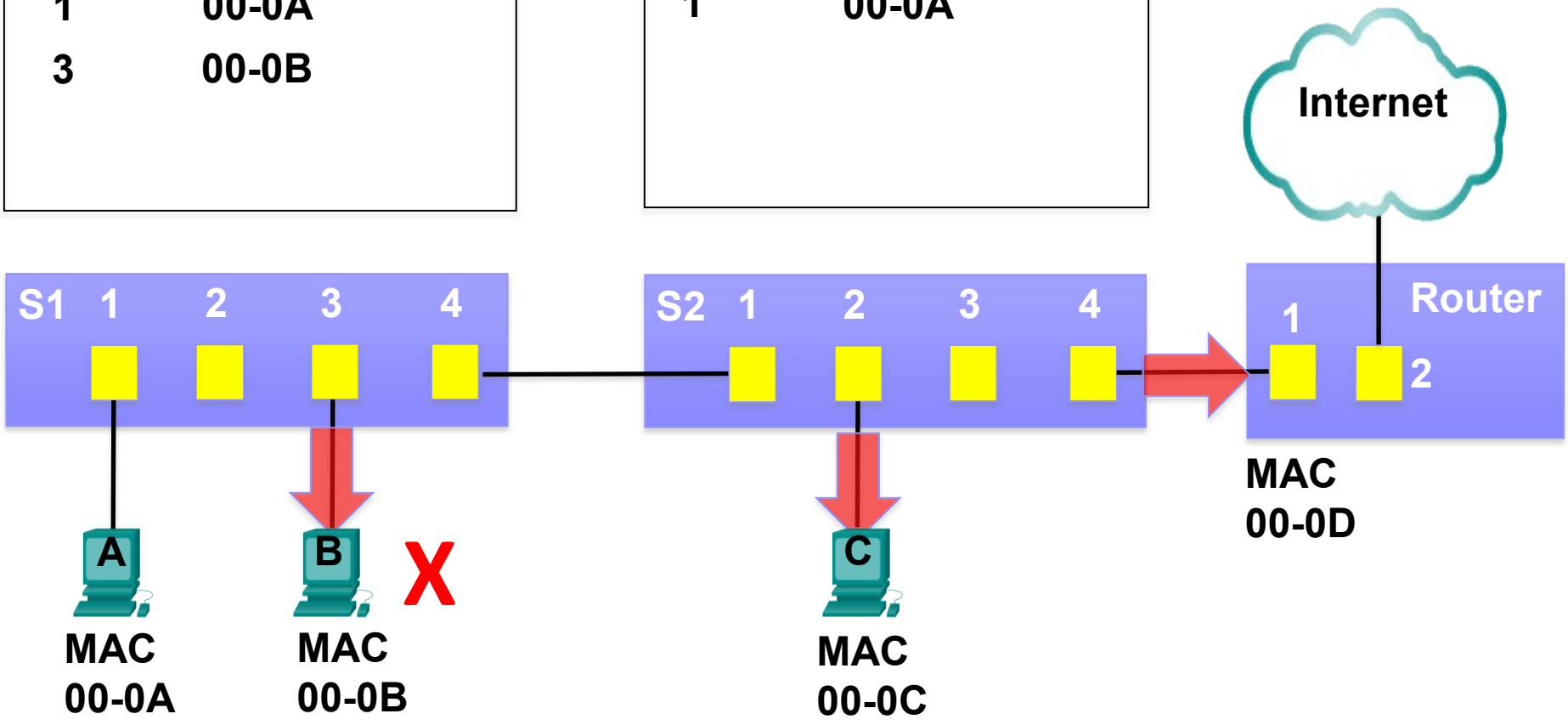
Destination MAC 00-0D	Source MAC 00-0A	Type	Data **Destination IP address on a remote network**	FCS

S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A



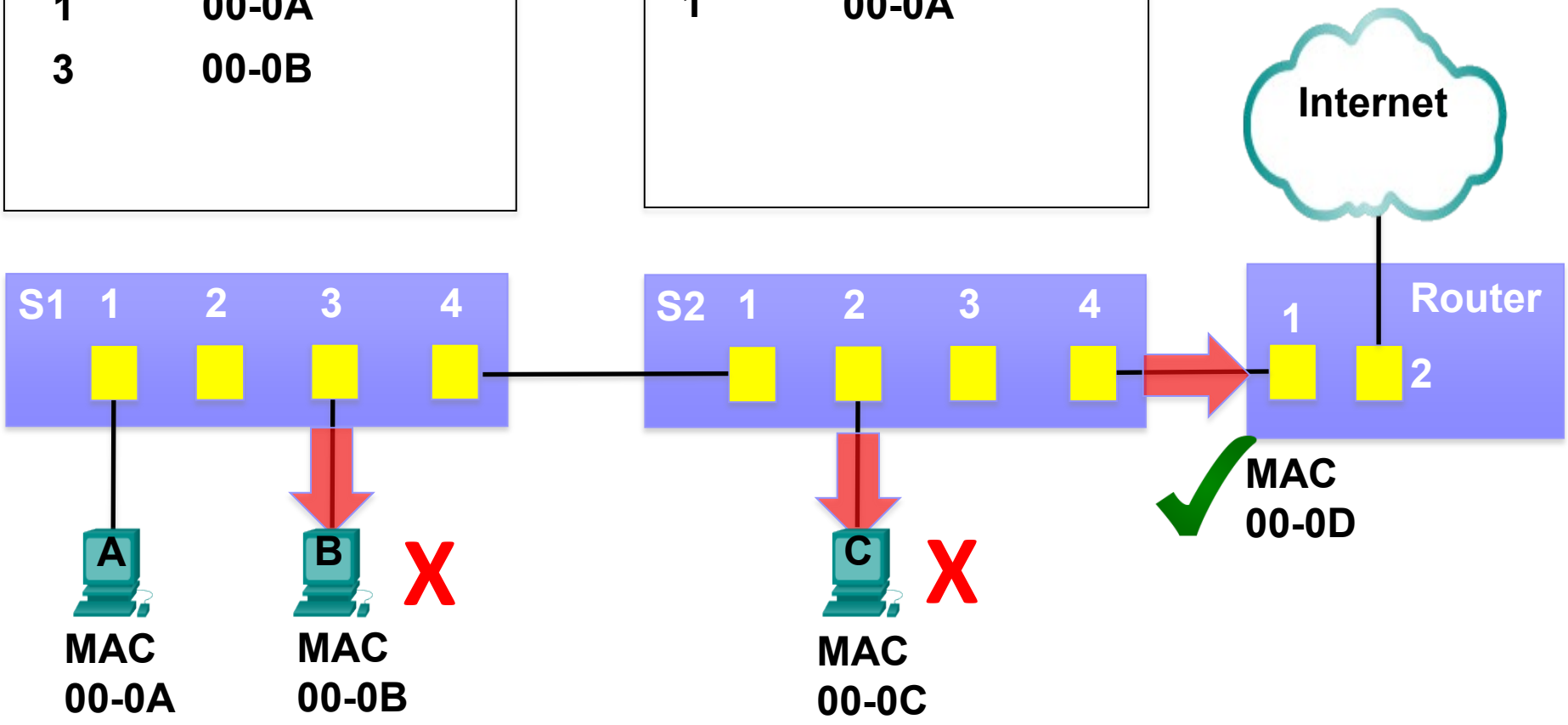
Destination MAC 00-0D	Source MAC 00-0A	Type	Data **Destination IP address on a remote network**	FCS

S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A



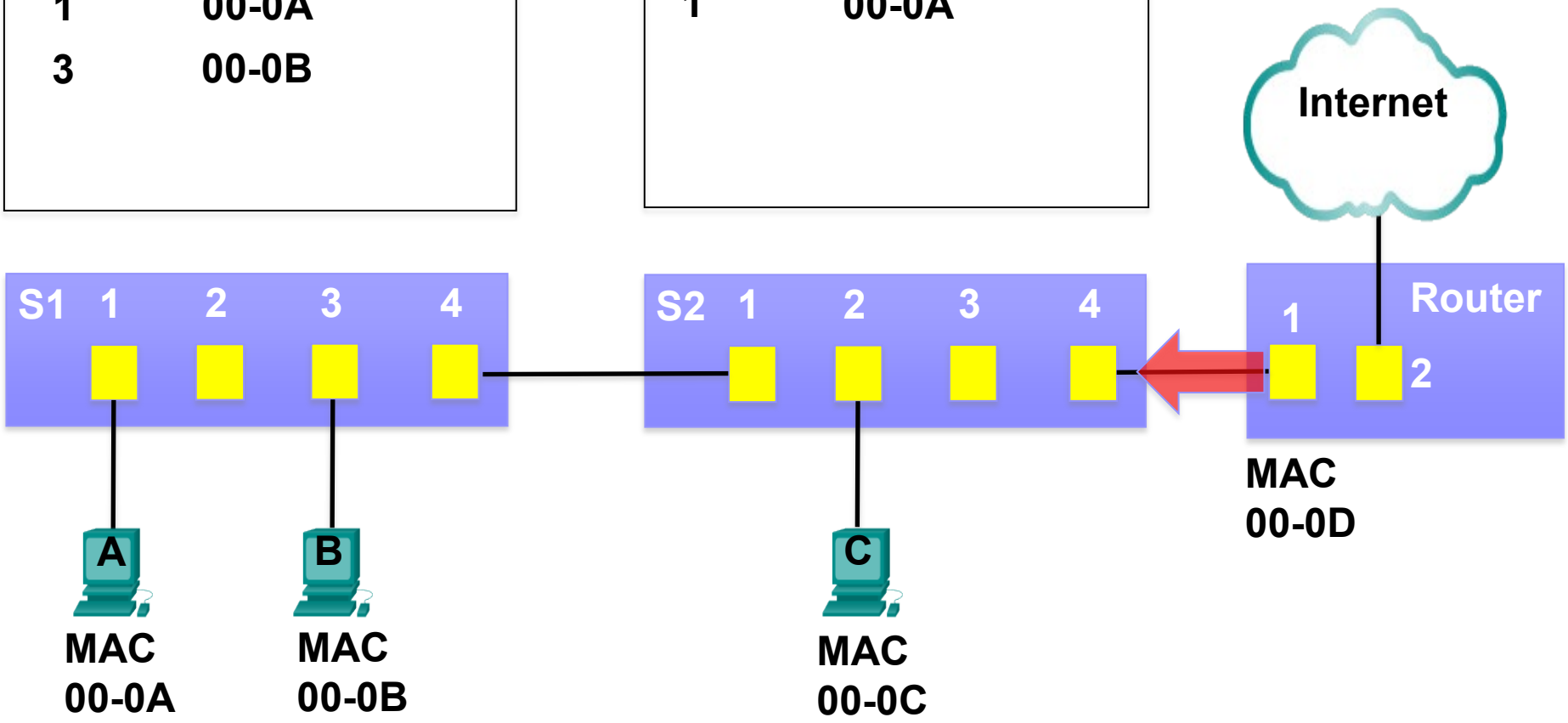
Destination MAC 00-0D	Source MAC 00-0A	Type	Data **Destination IP address on a remote network**	FCS

S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A



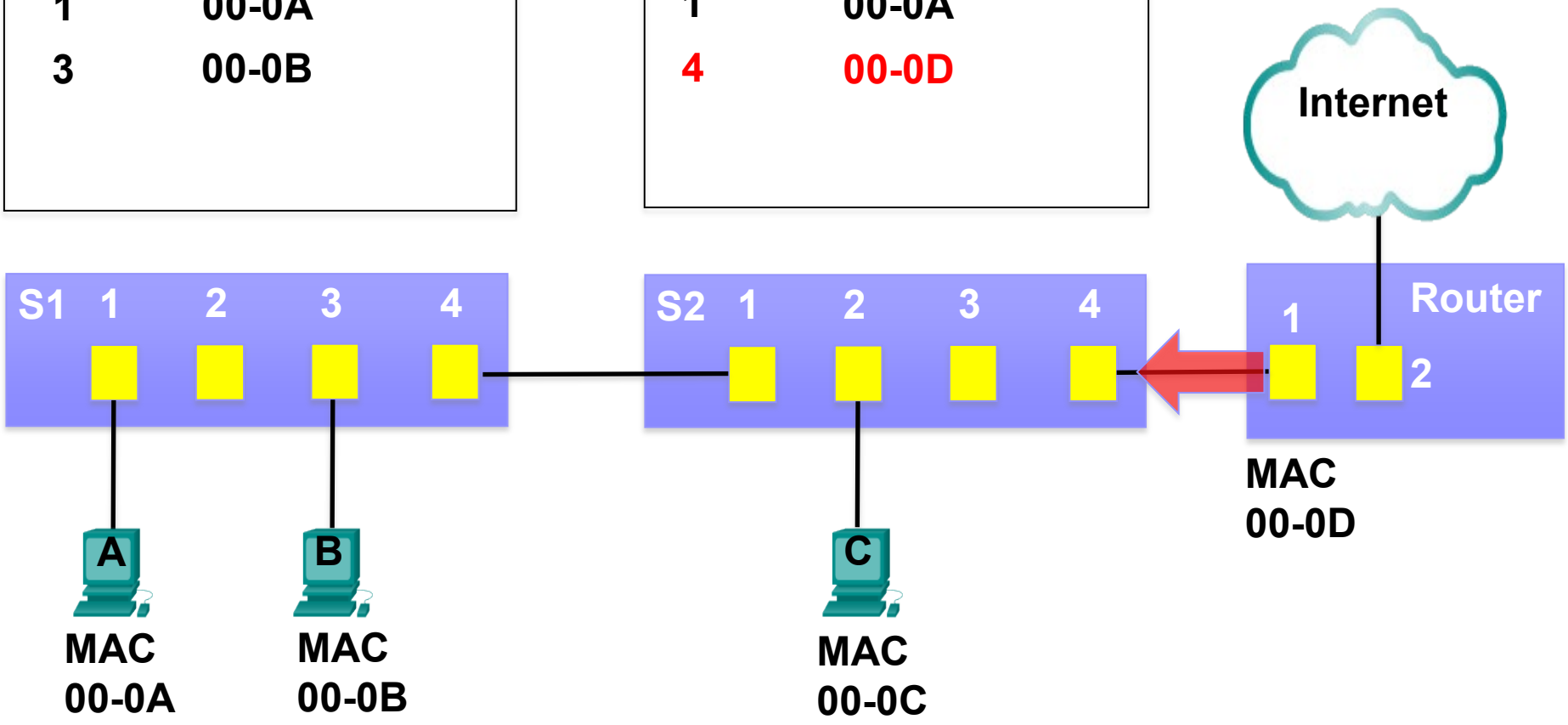
Destination MAC 00-0A	Source MAC 00-0D	Type	Data **Source IP address on a remote network**	FCS

S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B

S2 MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D



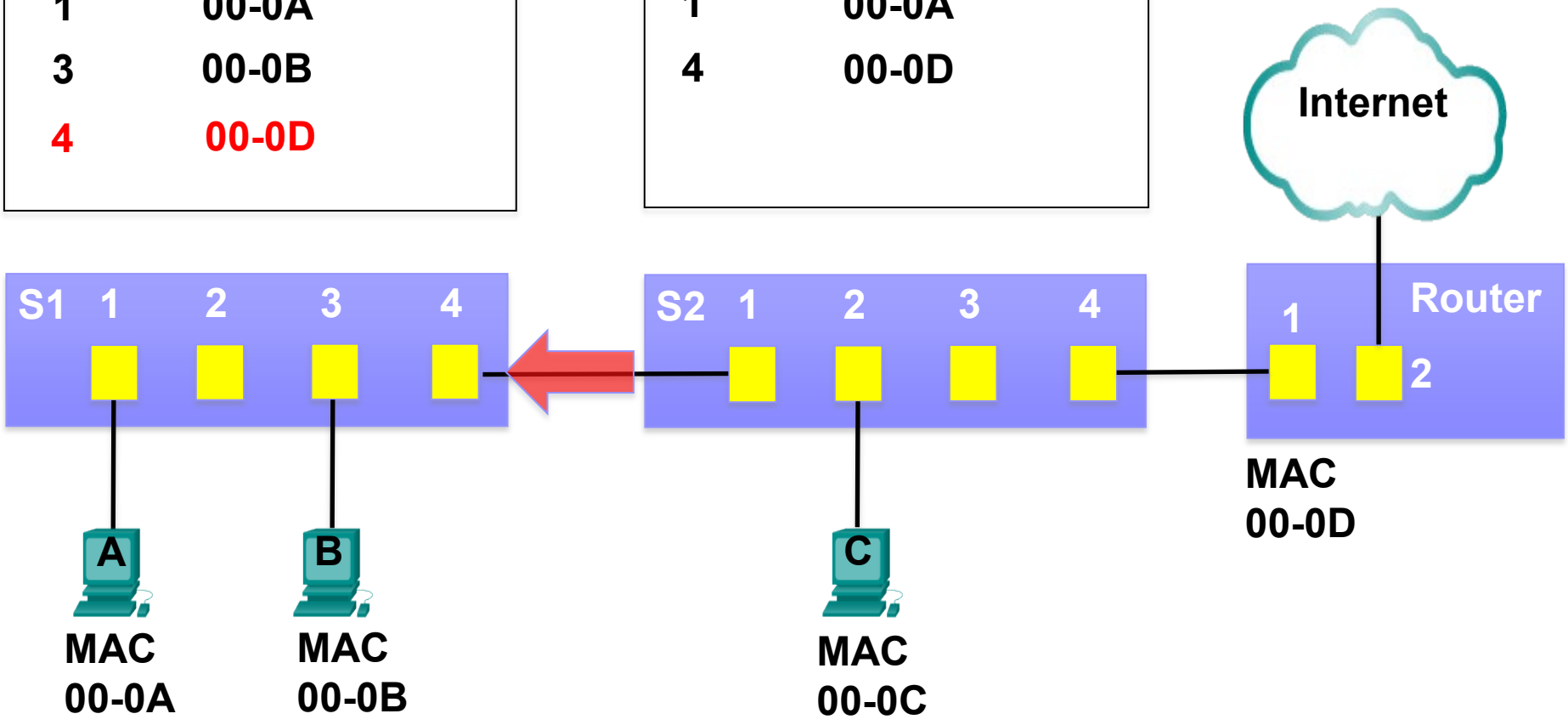
Destination MAC 00-0A	Source MAC 00-0D	Type	Data **Source IP address on a remote network**	FCS

S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B
4	00-0D

S2 MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D



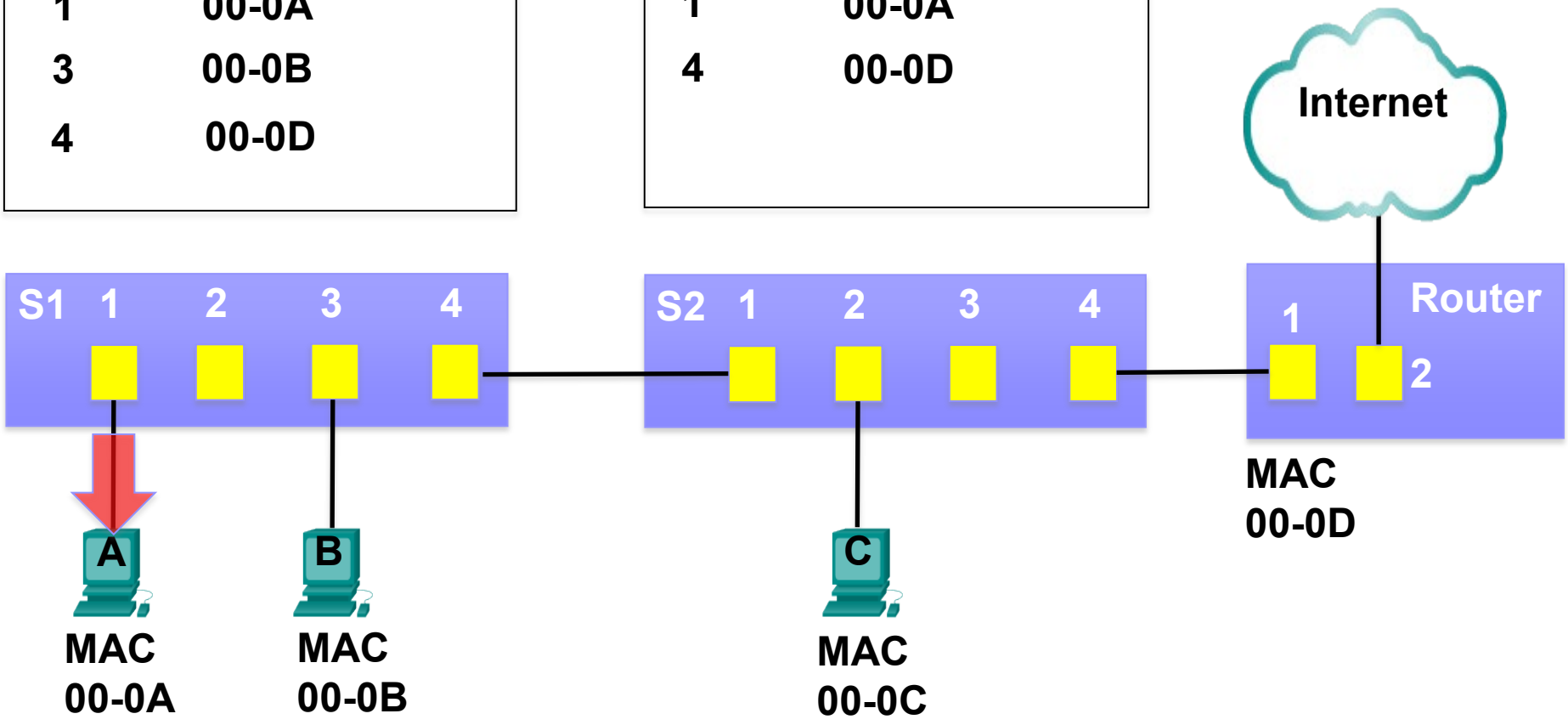
Destination MAC 00-0A	Source MAC 00-0D	Type	Data **Source IP address on a remote network**	FCS

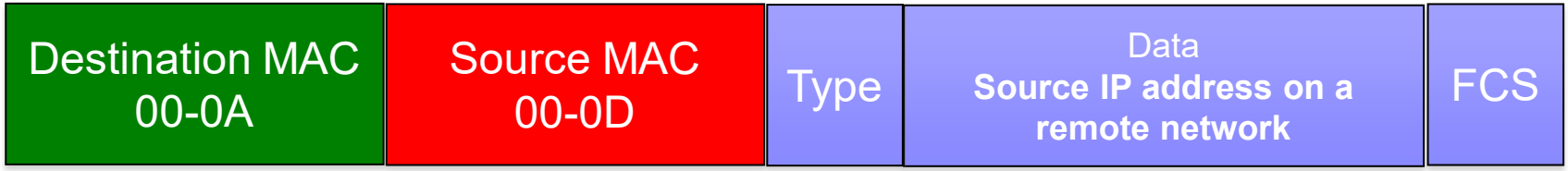
S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B
4	00-0D

S2 MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D



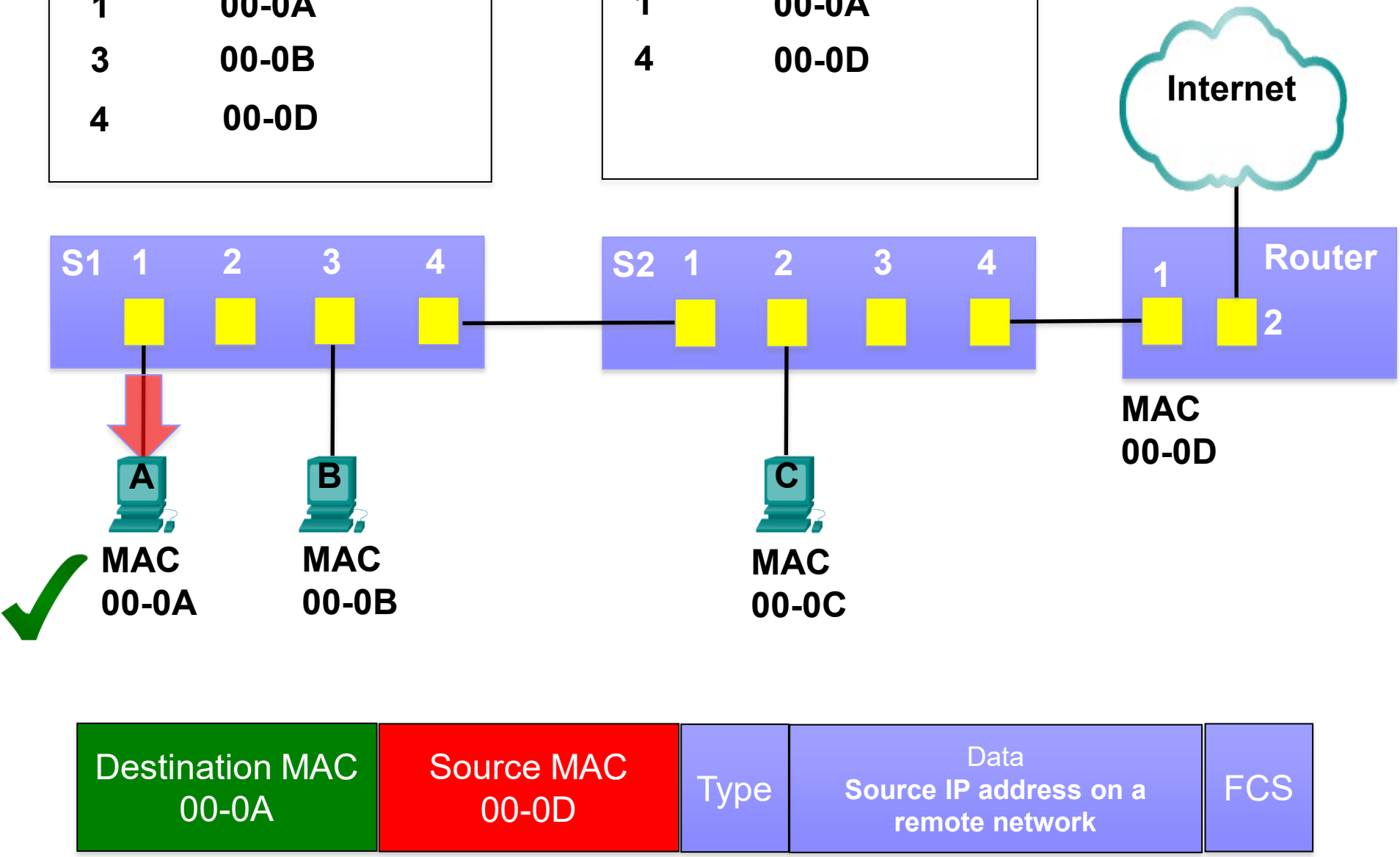


S1 MAC Address Table

Port	MAC Address
1	00-0A
3	00-0B
4	00-0D

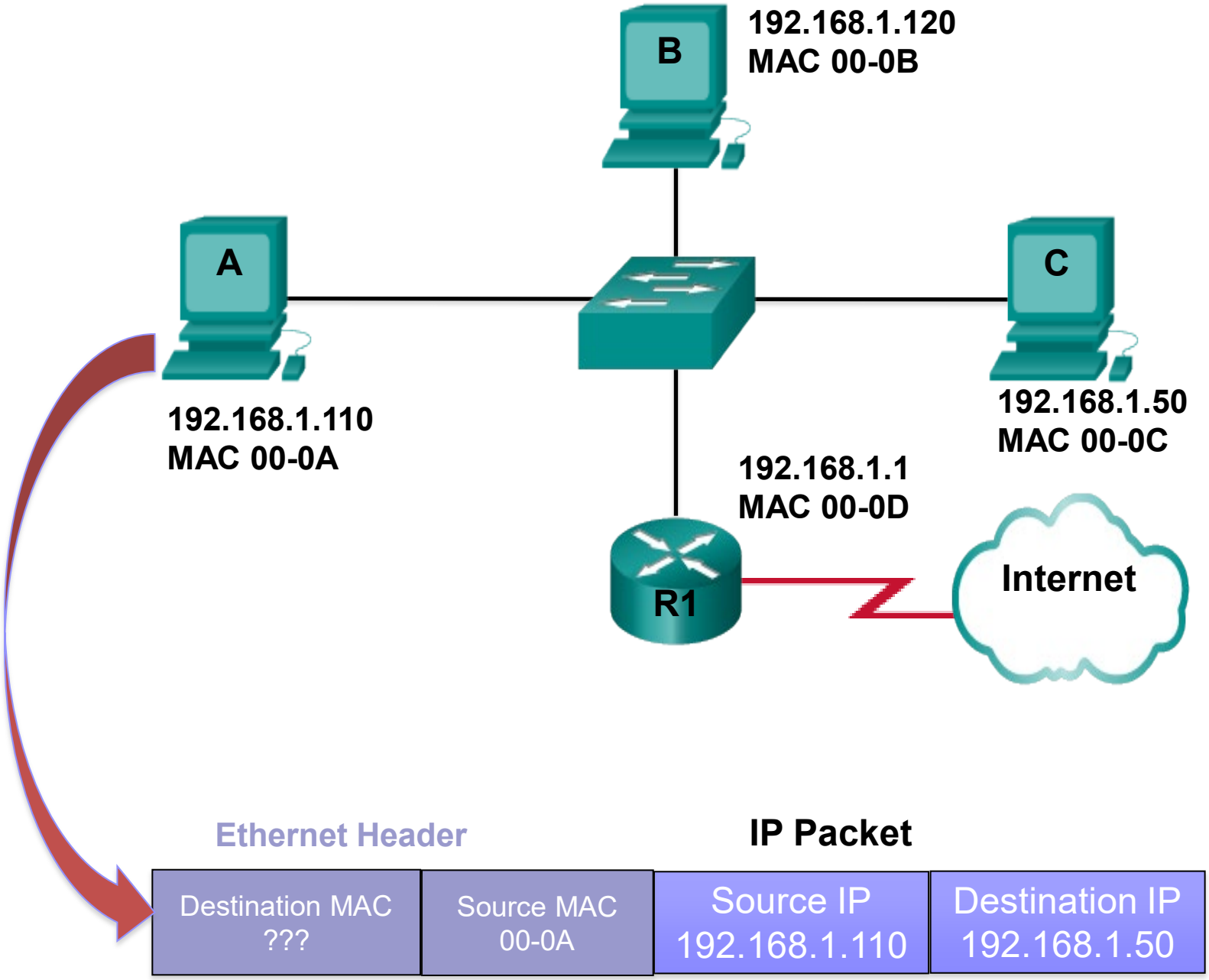
S2 MAC Address Table

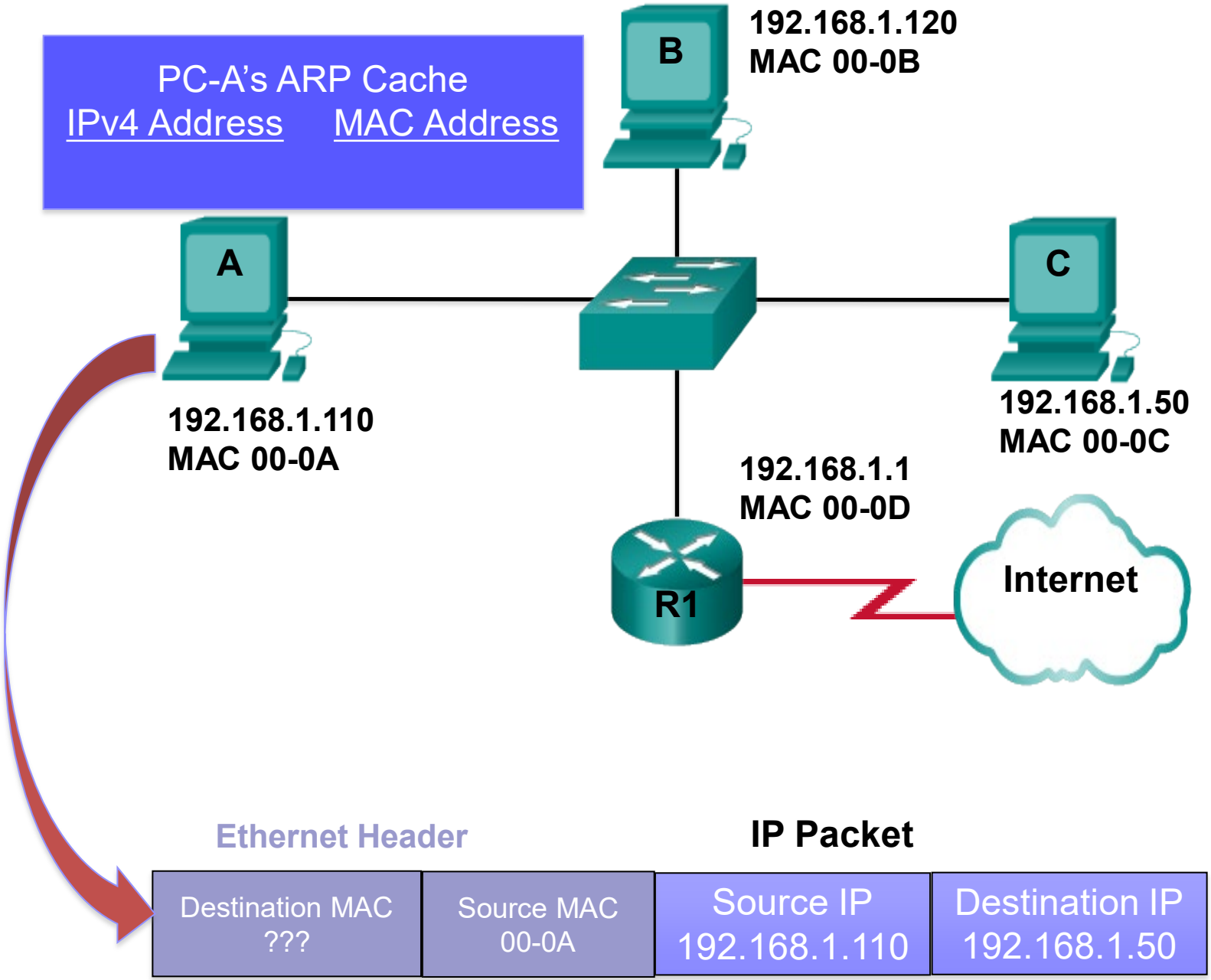
Port	MAC Address
1	00-0A
4	00-0D

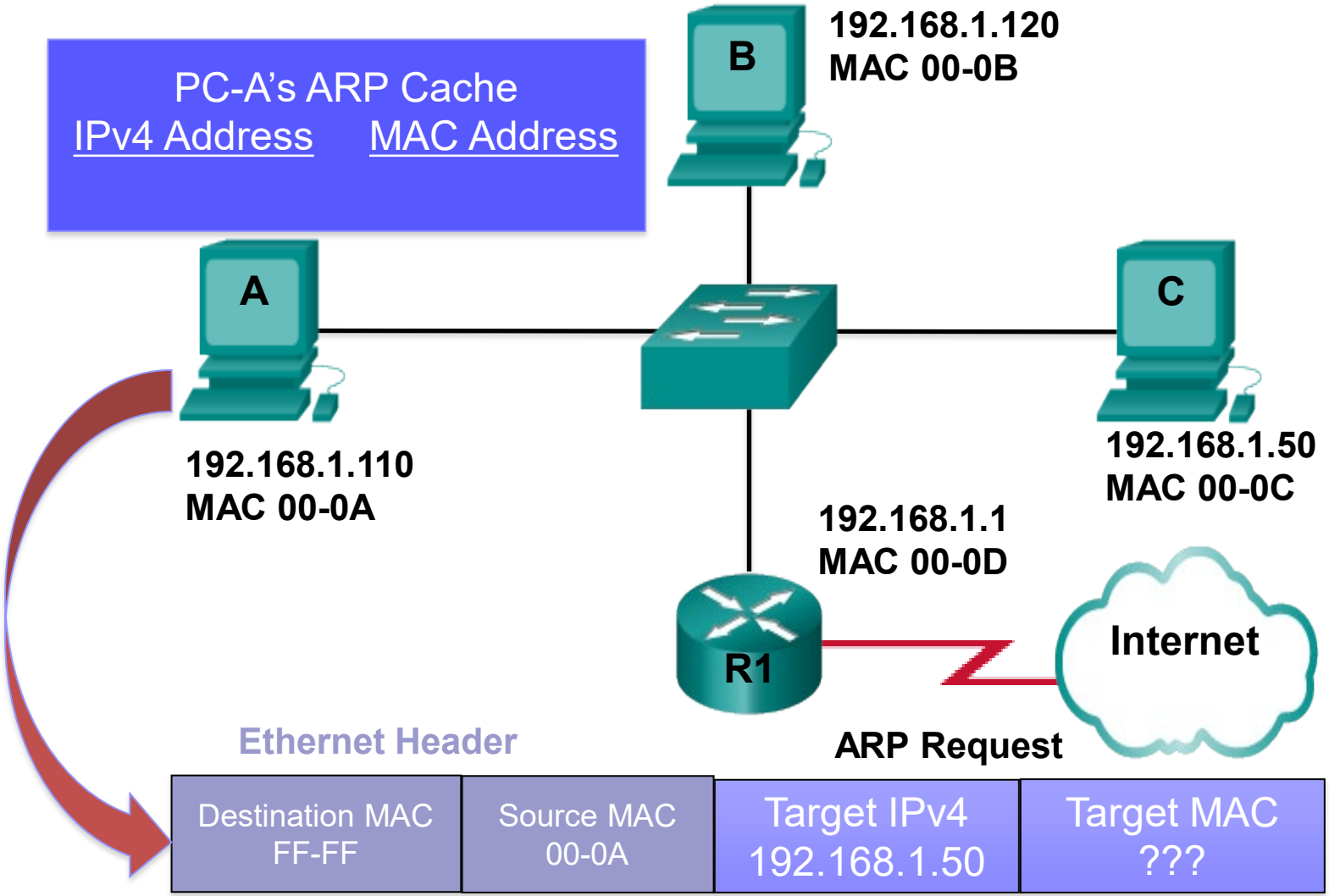


Destination MAC 00-0A	Source MAC 00-0D	Type	Data **Source IP address on a remote network**	FCS

ARP Operation - ARP Request


B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
192.168.1.50


PC-A's ARP Cache
IPv4 Address
MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
192.168.1.50

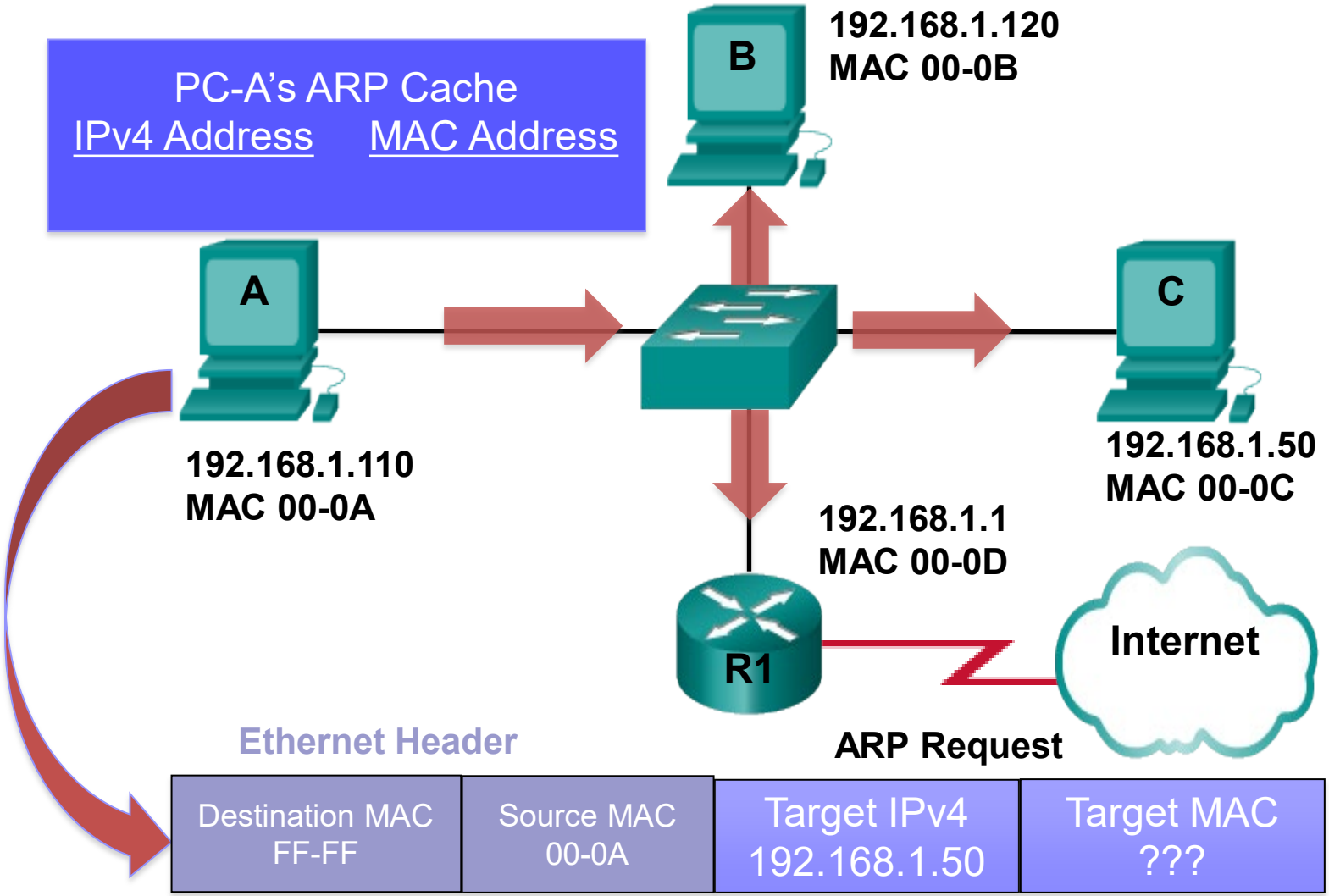


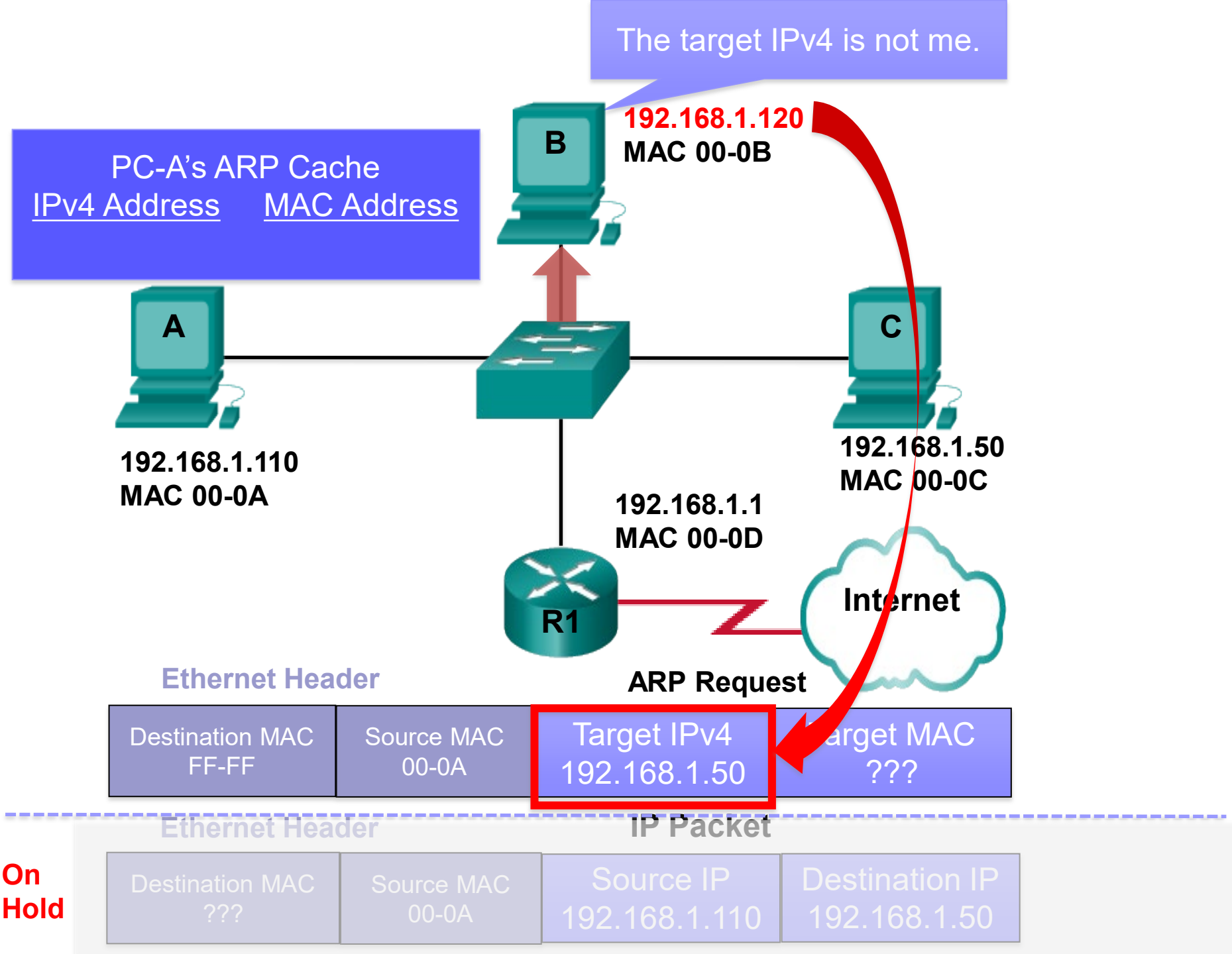
On Hold

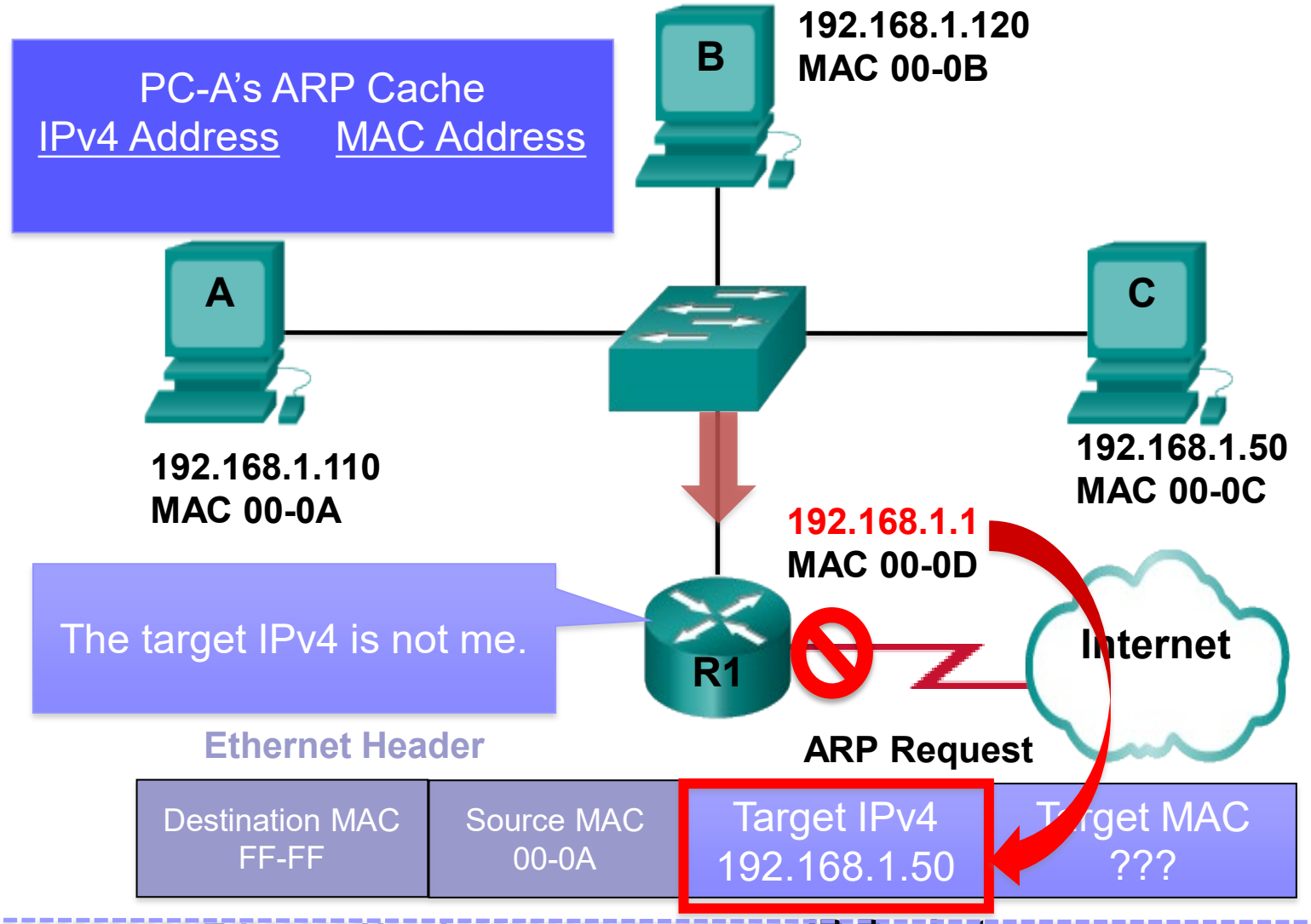
Ethernet Header

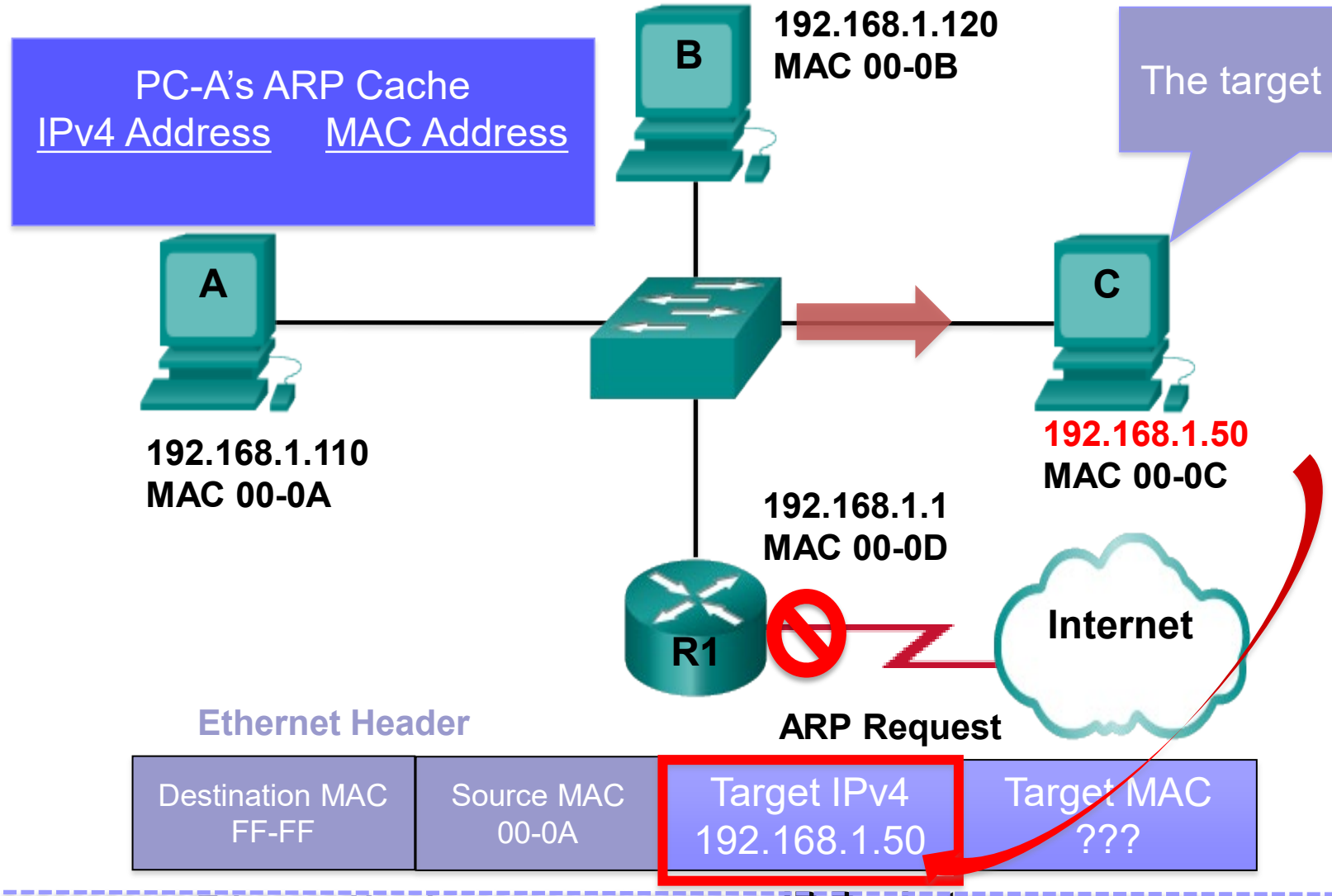
IP Packet

Destination MAC	Source MAC	Source IP	Destination IP
???	00-0A	192.168.1.110	192.168.1.50

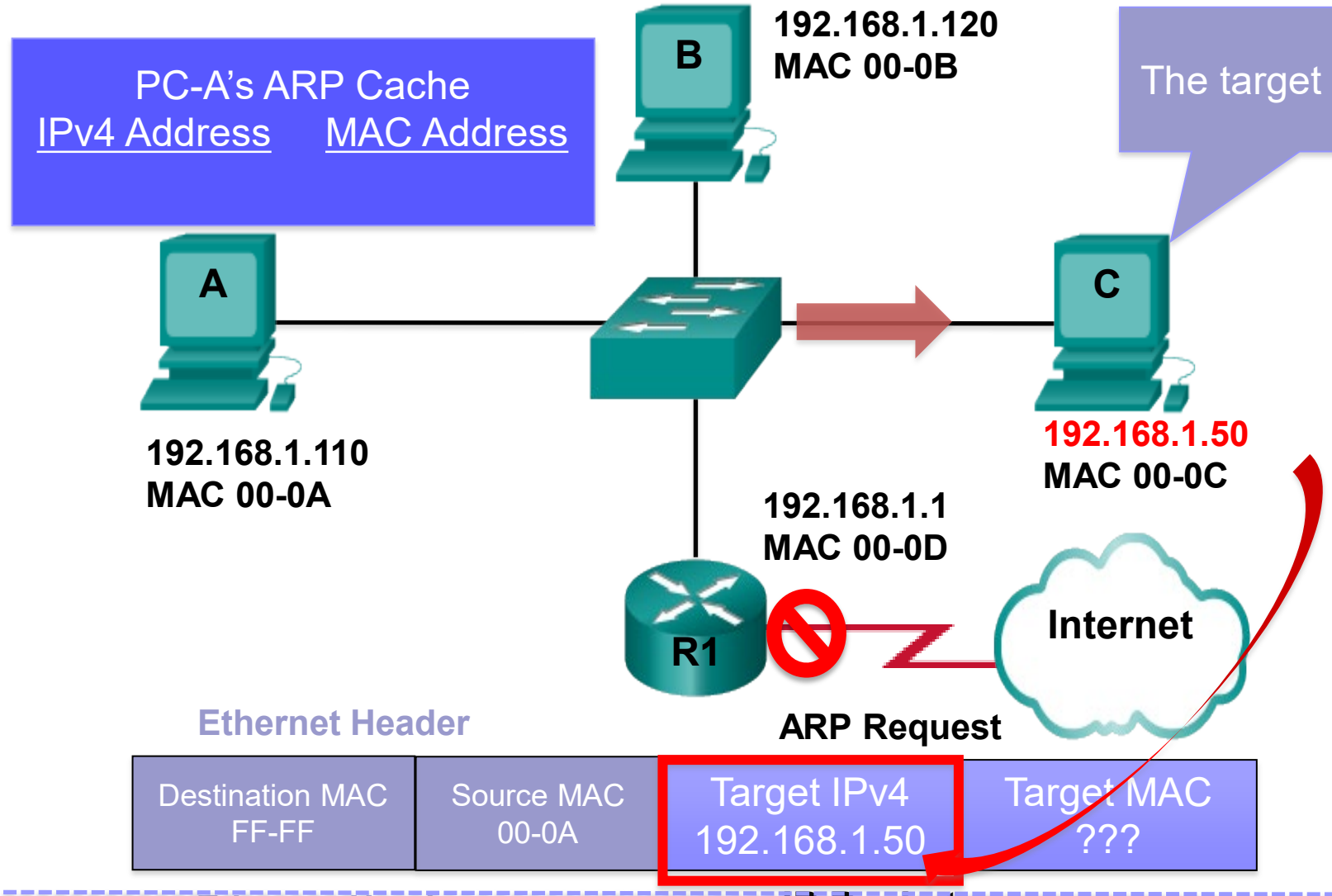

PC-A's ARP Cache
IPv4 Address
MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Request
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.50
Target MAC
???
On Hold
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
192.168.1.50

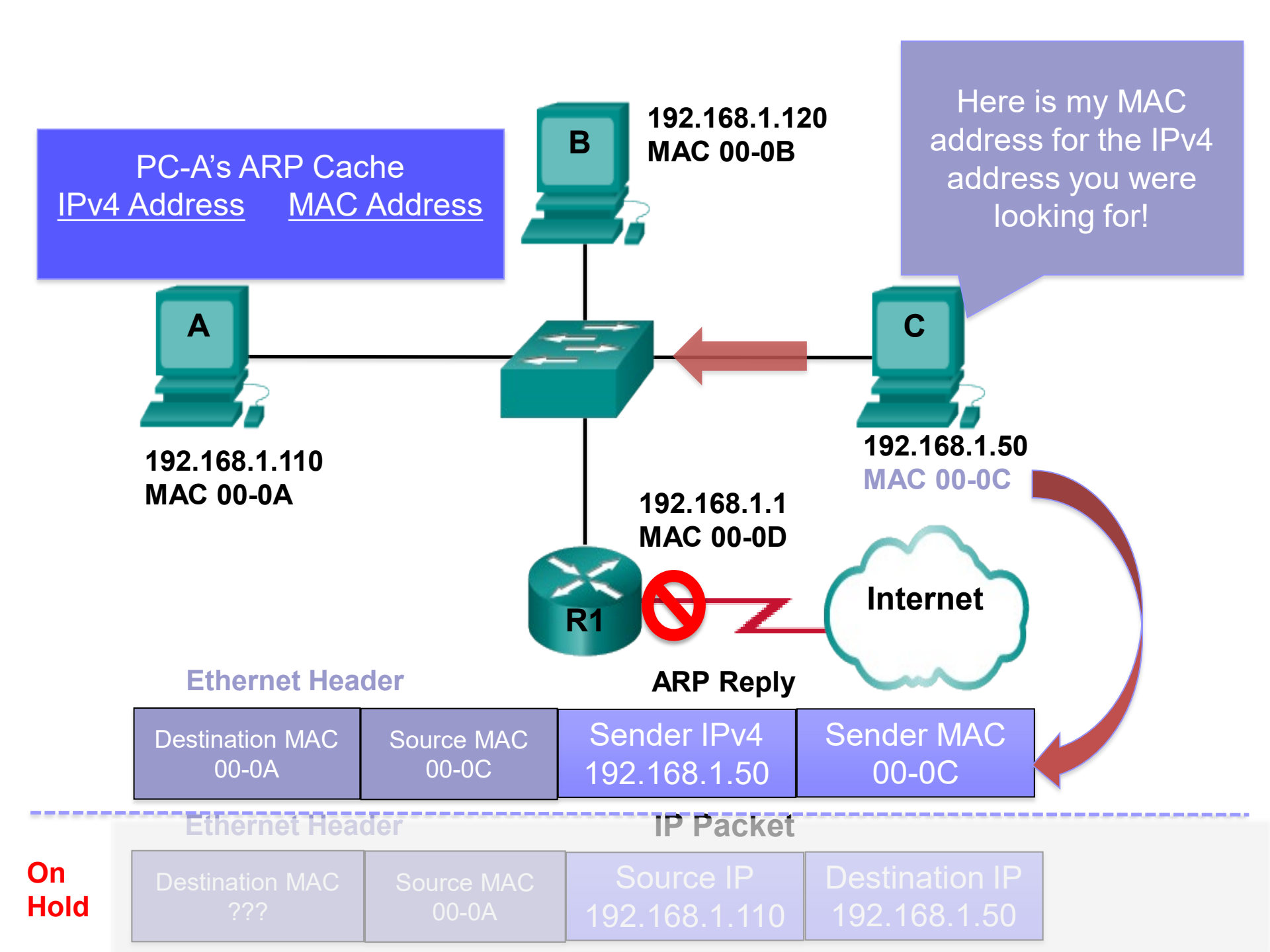

The target IPv4 is not me.
PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Request
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.50
arget MAC
???
On Hold
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
192.168.1.50

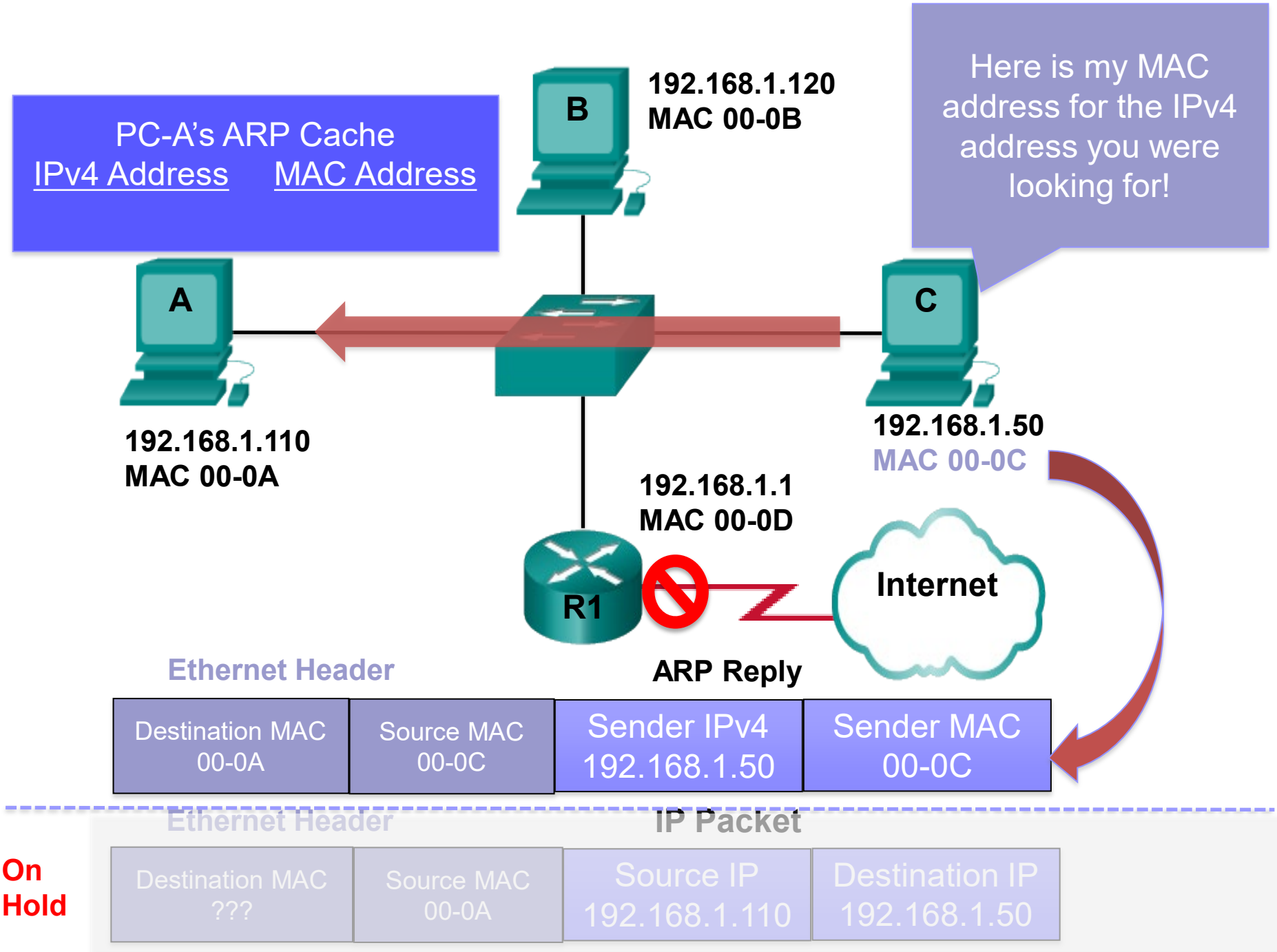

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
The target IPv4 is not me.
R1
Internet
Ethernet Header
ARP Request
Destination MAC FF-FF
Source MAC 00-0A
Target IPv4 192.168.1.50
Target MAC ???
Ethernet Header
IP Packet
On Hold
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 192.168.1.50

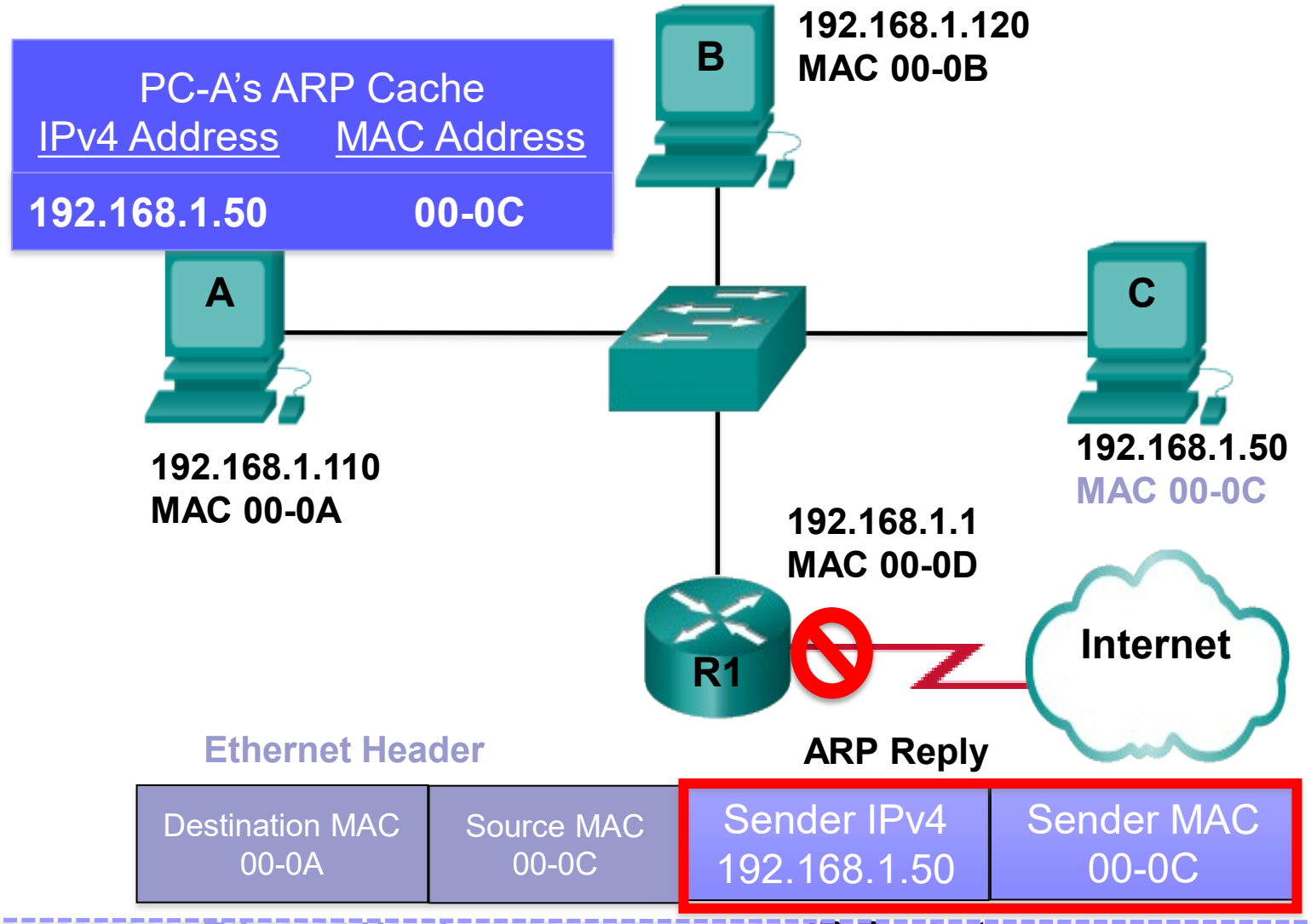

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
The target IPv4 is me!
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
ARP Request
Ethernet Header
Destination MAC FF-FF
Source MAC 00-0A
Target IPv4 192.168.1.50
Target MAC ???
Ethernet Header
IP Packet
On Hold
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 192.168.1.50

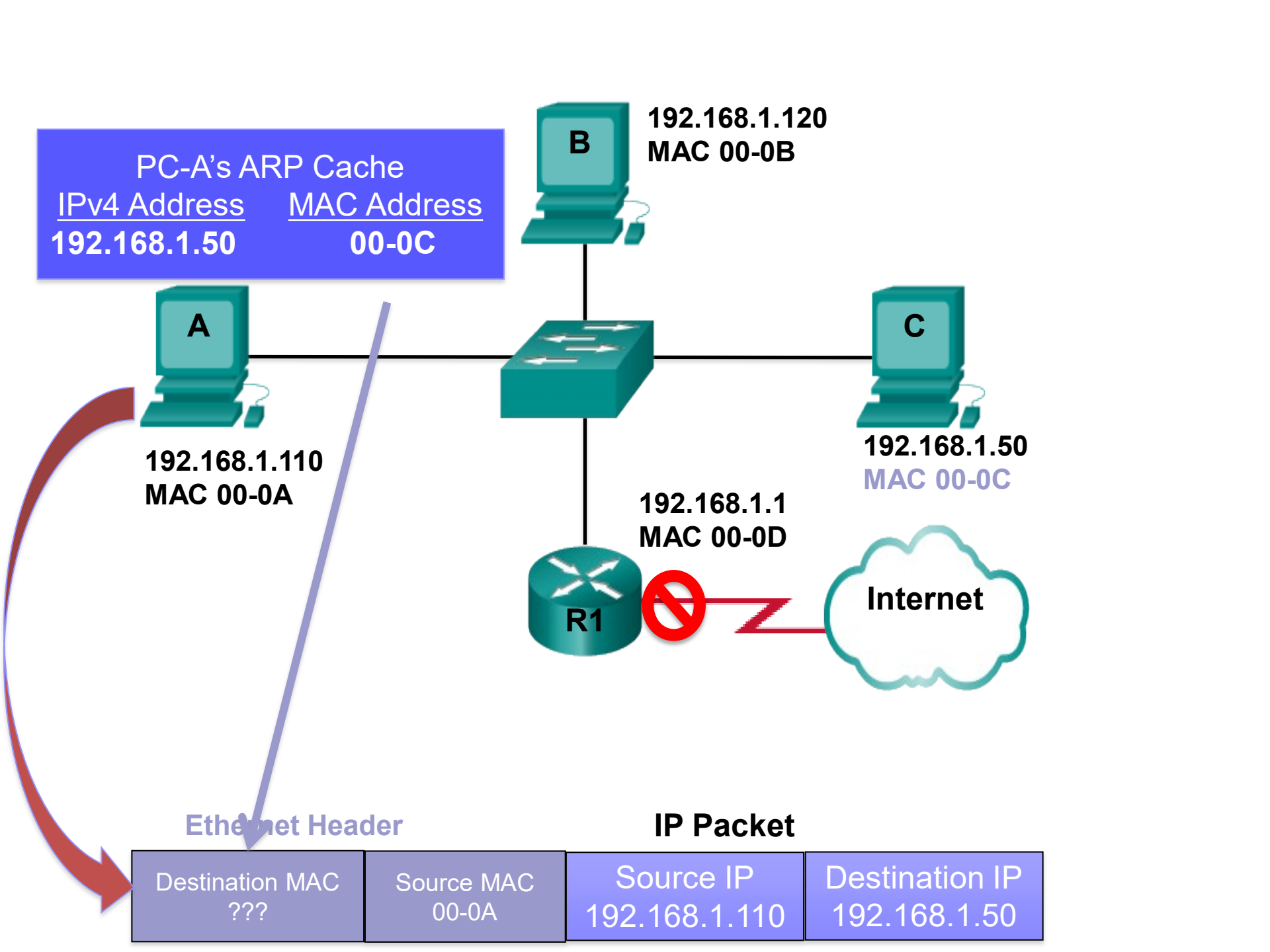
ARP Operation - ARP Reply

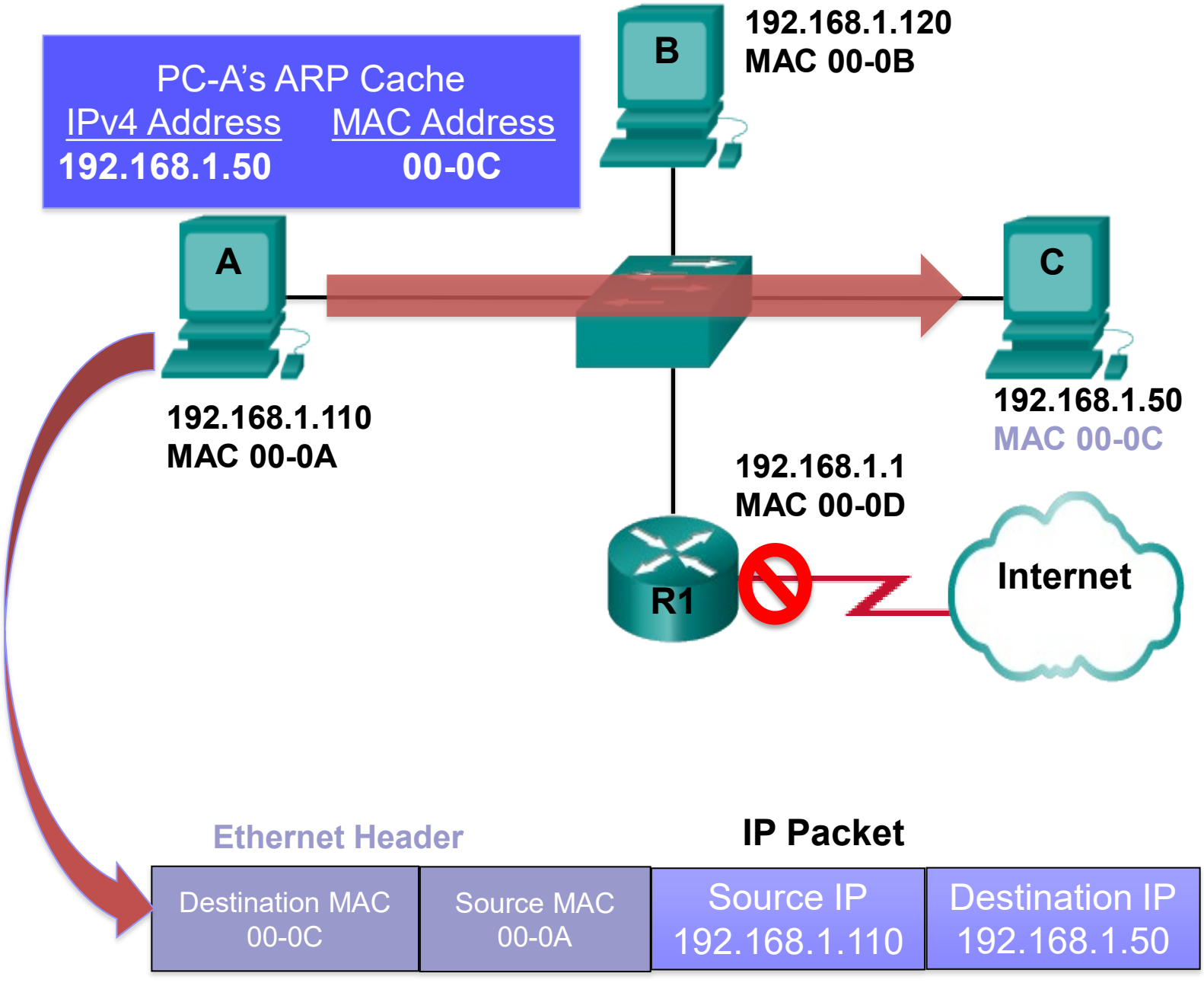

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
The target IPv4 is me!
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
ARP Request
Ethernet Header
Destination MAC FF-FF
Source MAC 00-0A
Target IPv4 192.168.1.50
Target MAC ???
Ethernet Header
IP Packet
On Hold
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 192.168.1.50


PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
Here is my MAC address for the IPv4 address you were looking for!
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Reply
Destination MAC 00-0A
Source MAC 00-0C
Sender IPv4 192.168.1.50
Sender MAC 00-0C
Ethernet Header
IP Packet
On Hold
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 192.168.1.50

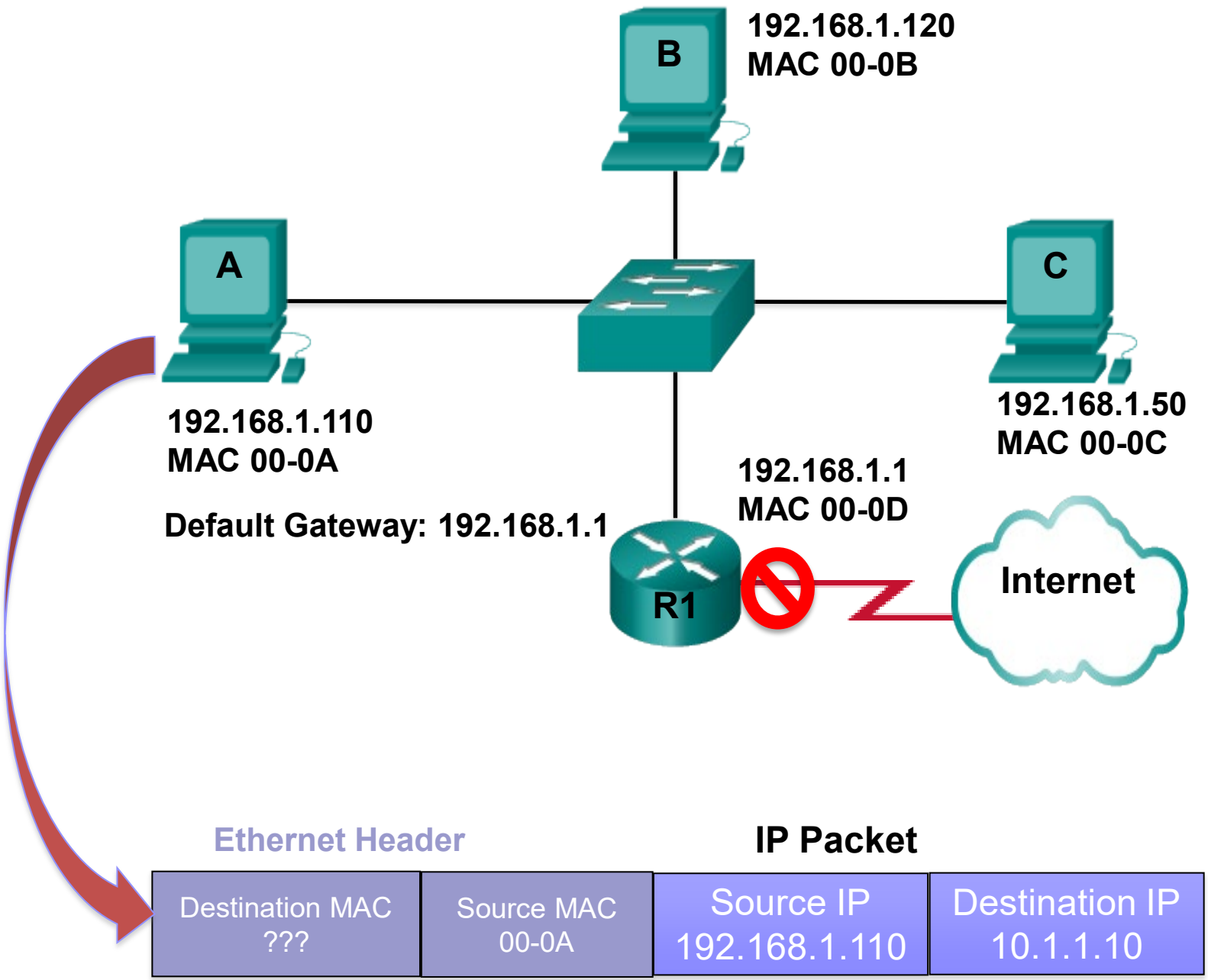

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
Here is my MAC address for the IPv4 address you were looking for!
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Reply
Destination MAC 00-0A
Source MAC 00-0C
Sender IPv4 192.168.1.50
Sender MAC 00-0C
Ethernet Header
IP Packet
On Hold
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 192.168.1.50

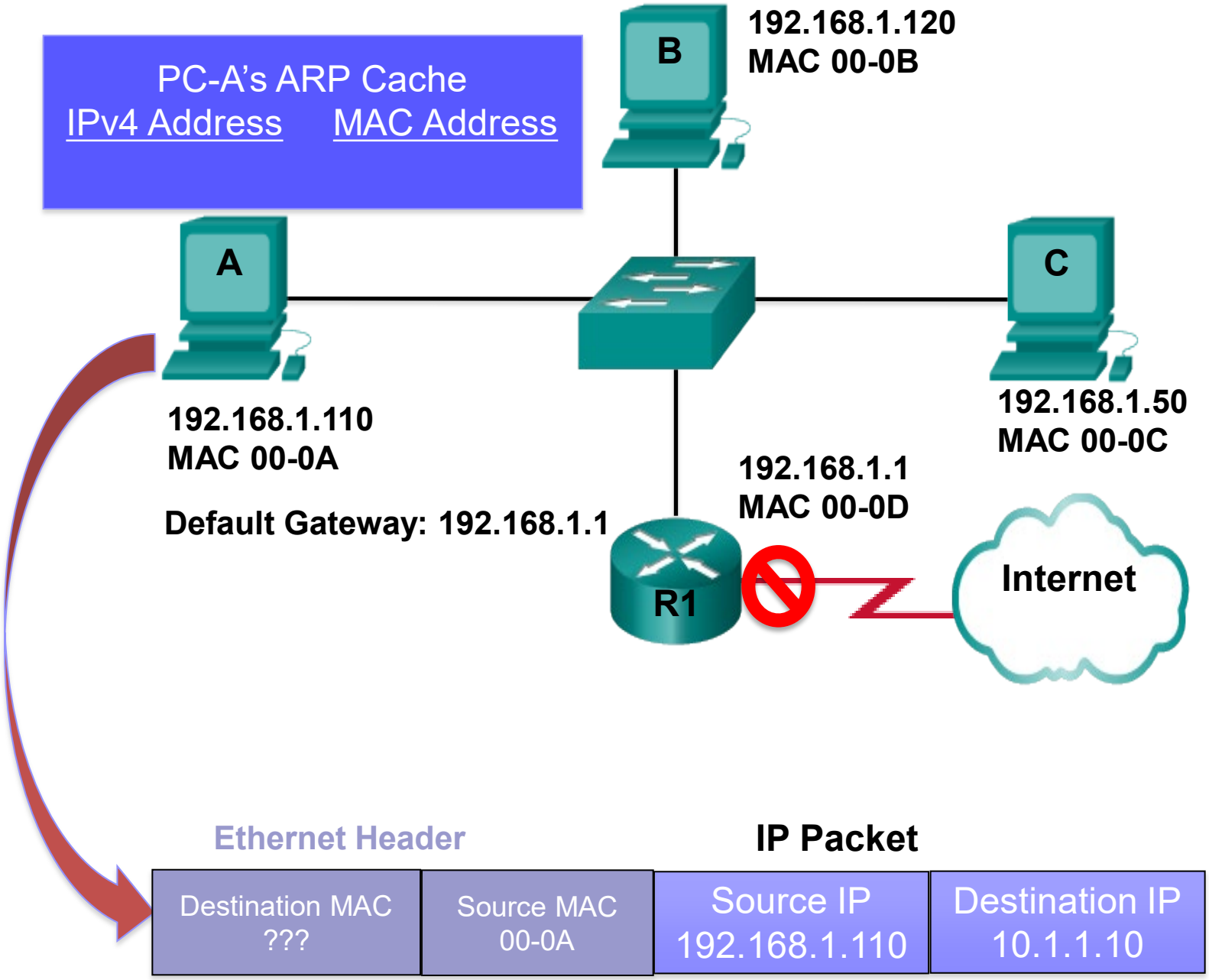

PC-A's ARP Cache
IPv4 Address
MAC Address
192.168.1.50
00-0C
B
192.168.1.120
MAC 00-0B
A
192.168.1.110
MAC 00-0A
C
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
Destination MAC
00-0A
Source MAC
00-0C
ARP Reply
Sender IPv4
192.168.1.50
Sender MAC
00-0C
On Hold
Ethernet Header
Destination MAC
???
Source MAC
00-0A
IP Packet
Source IP
192.168.1.110
Destination IP
192.168.1.50

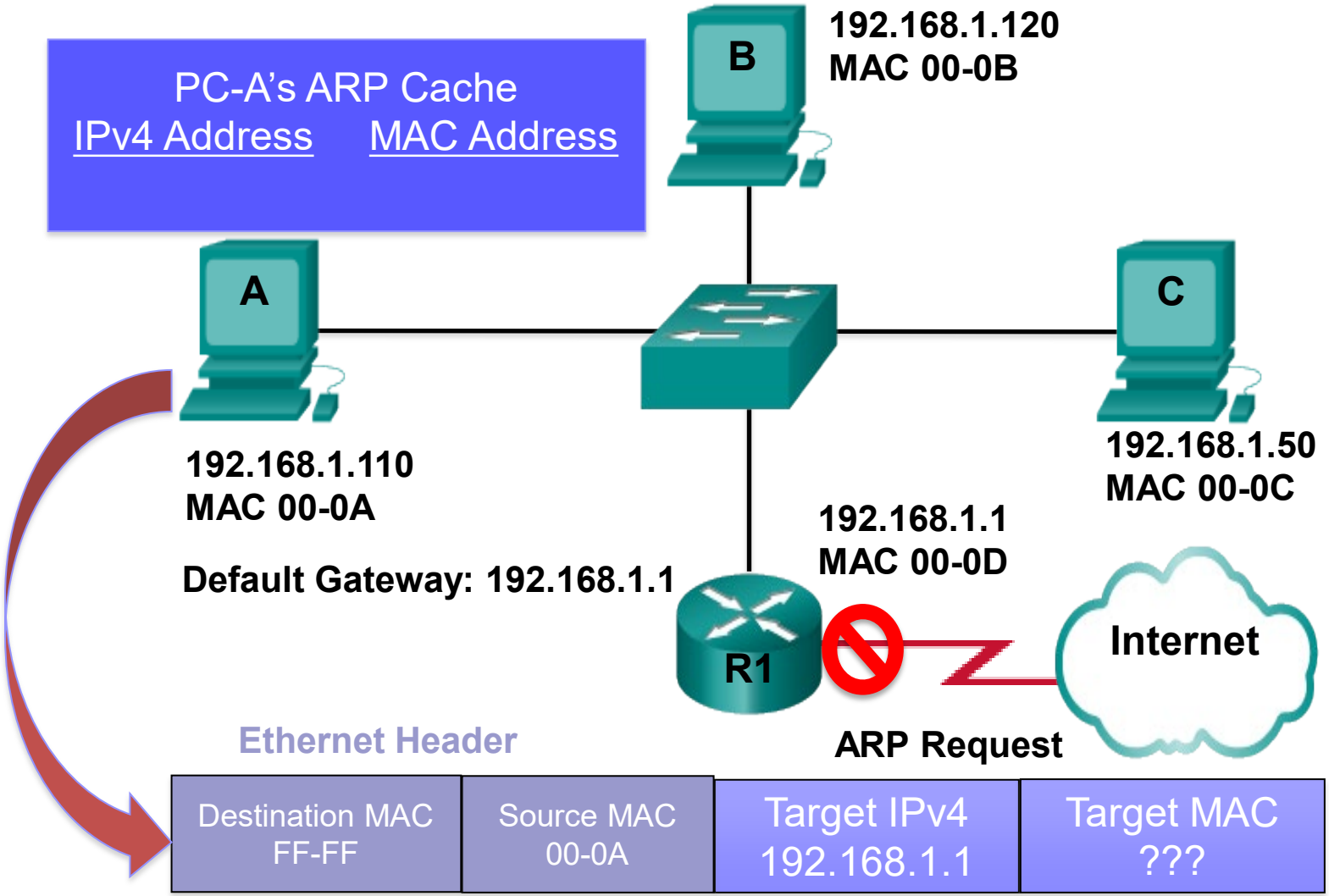

PC-A's ARP Cache
IPv4 Address
MAC Address
192.168.1.50
00-0C
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
192.168.1.50


PC-A's ARP Cache
IPv4 Address
MAC Address
192.168.1.50
00-0C
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
00-0C
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
192.168.1.50

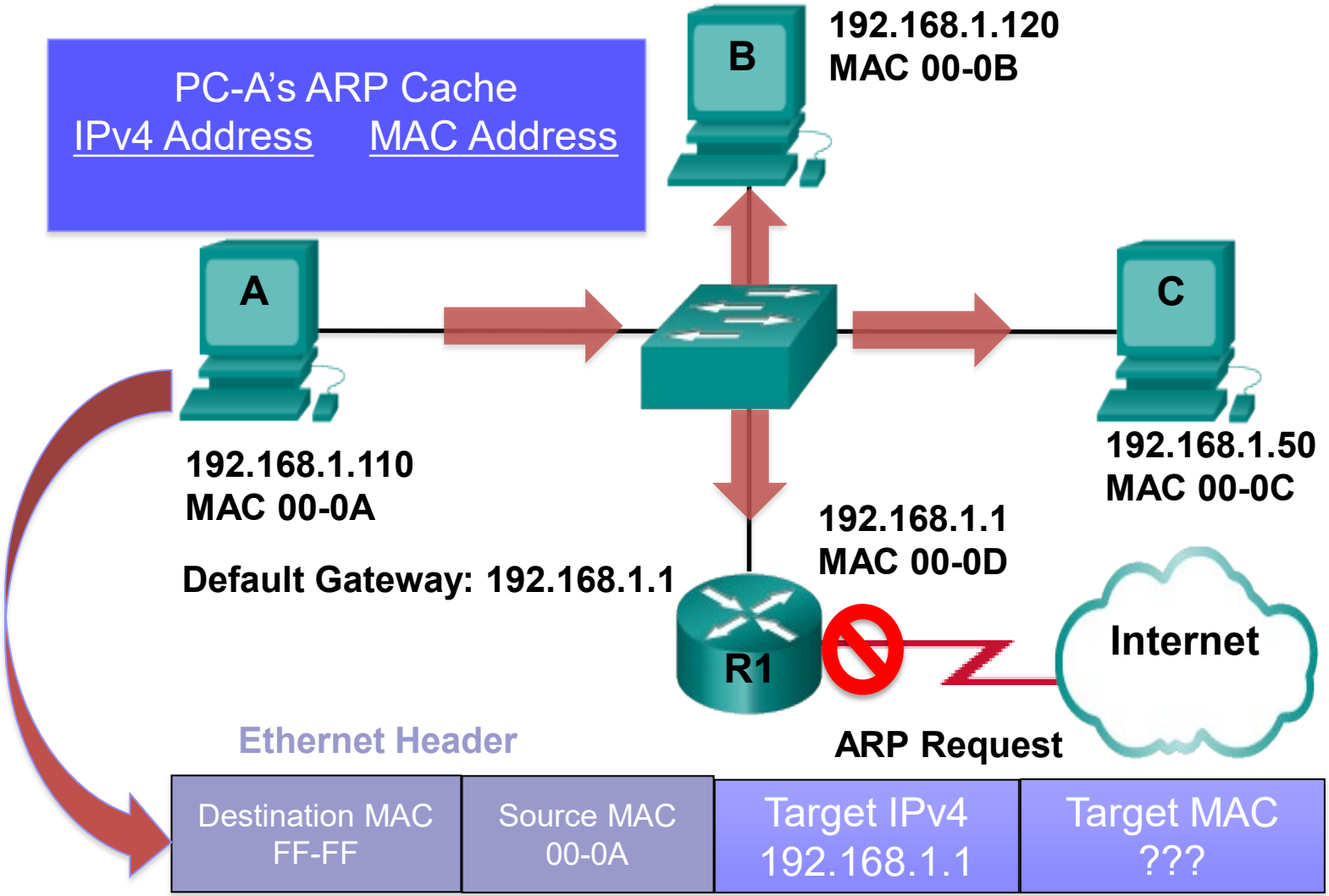
ARP Role in Remote Communication


B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10

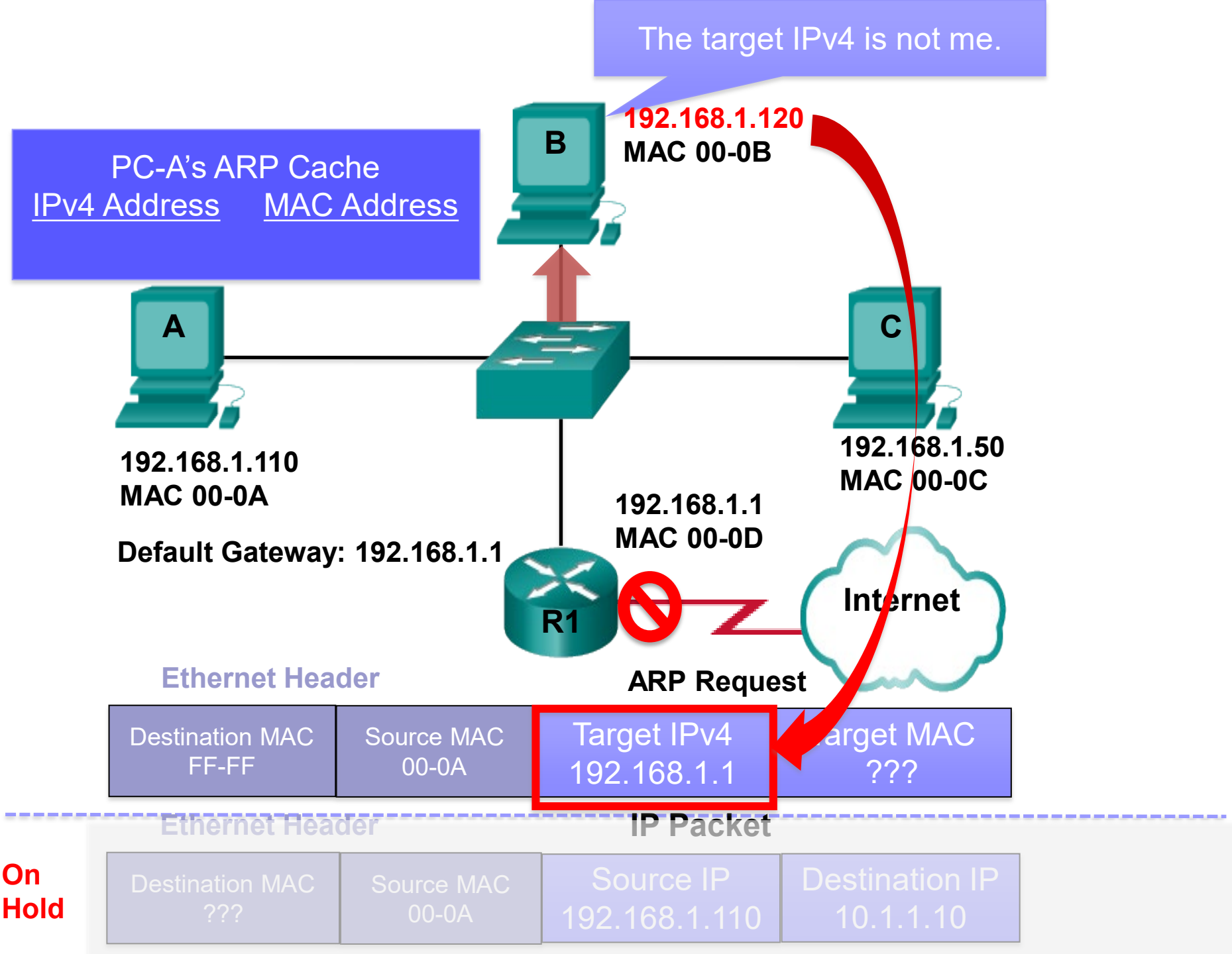

PC-A's ARP Cache
IPv4 Address
MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10

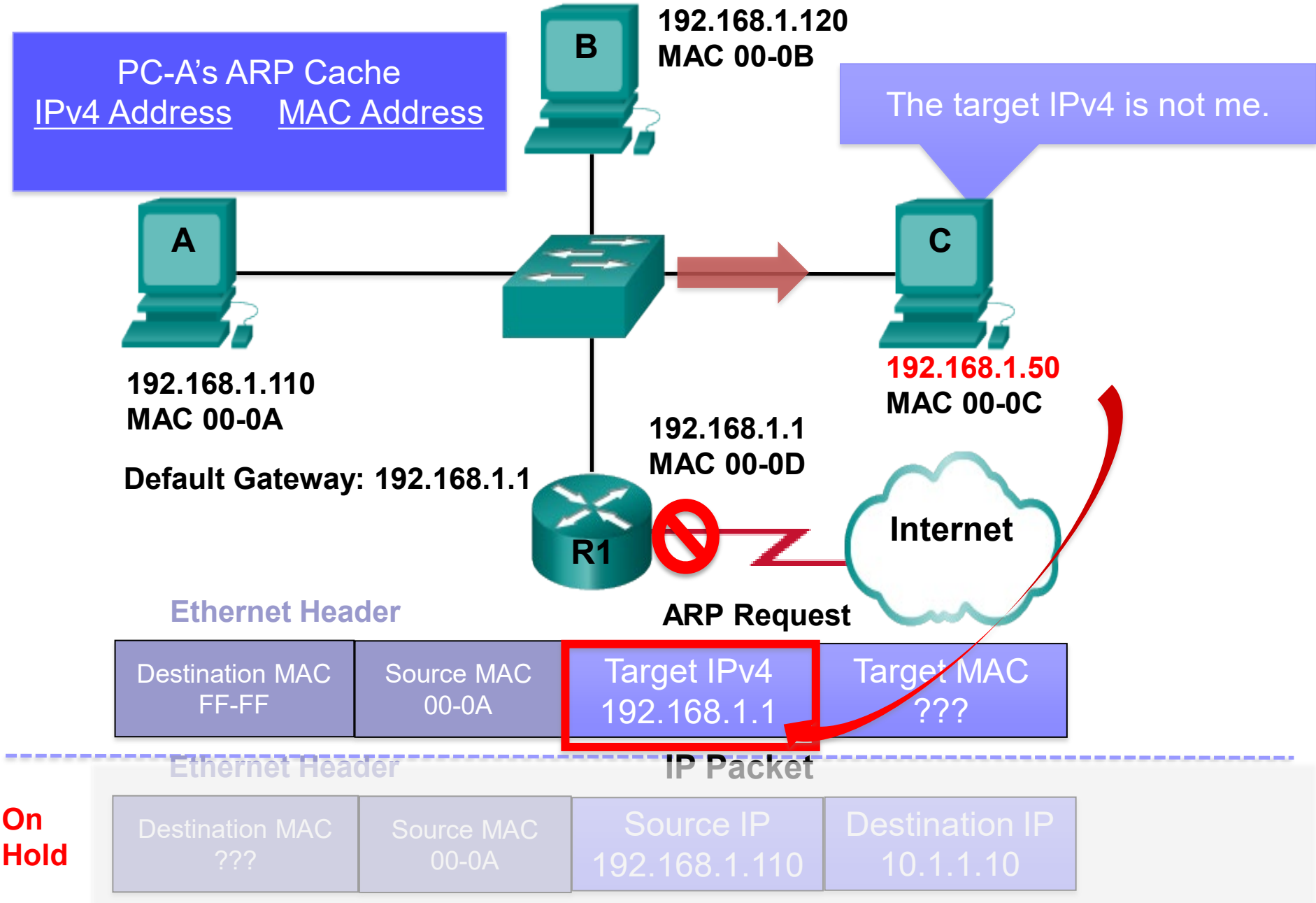

PC-A's ARP Cache
IPv4 Address
MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
ARP Request
Ethernet Header
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.1
Target MAC
???
IP Packet
Ethernet Header
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10

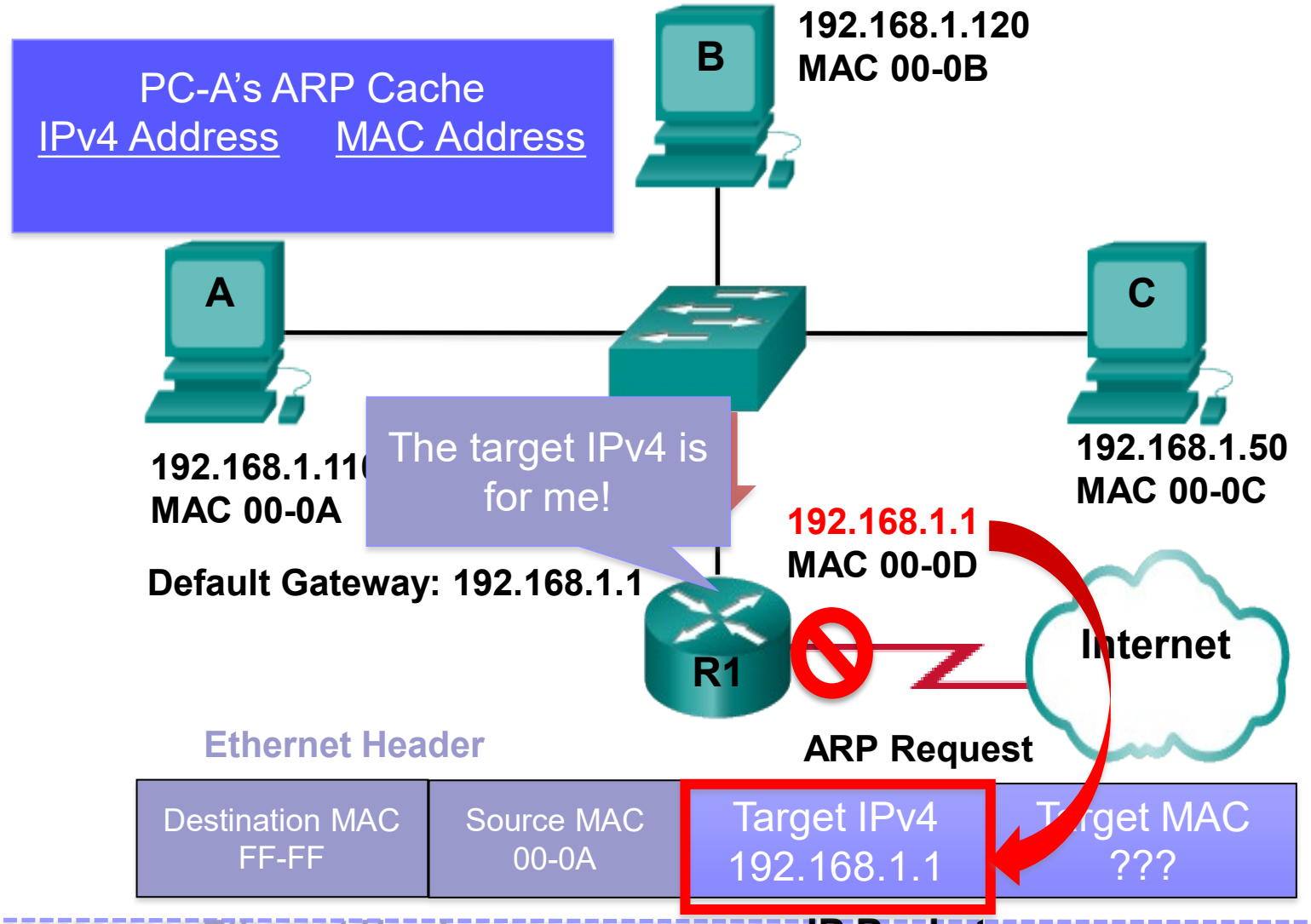
On Hold

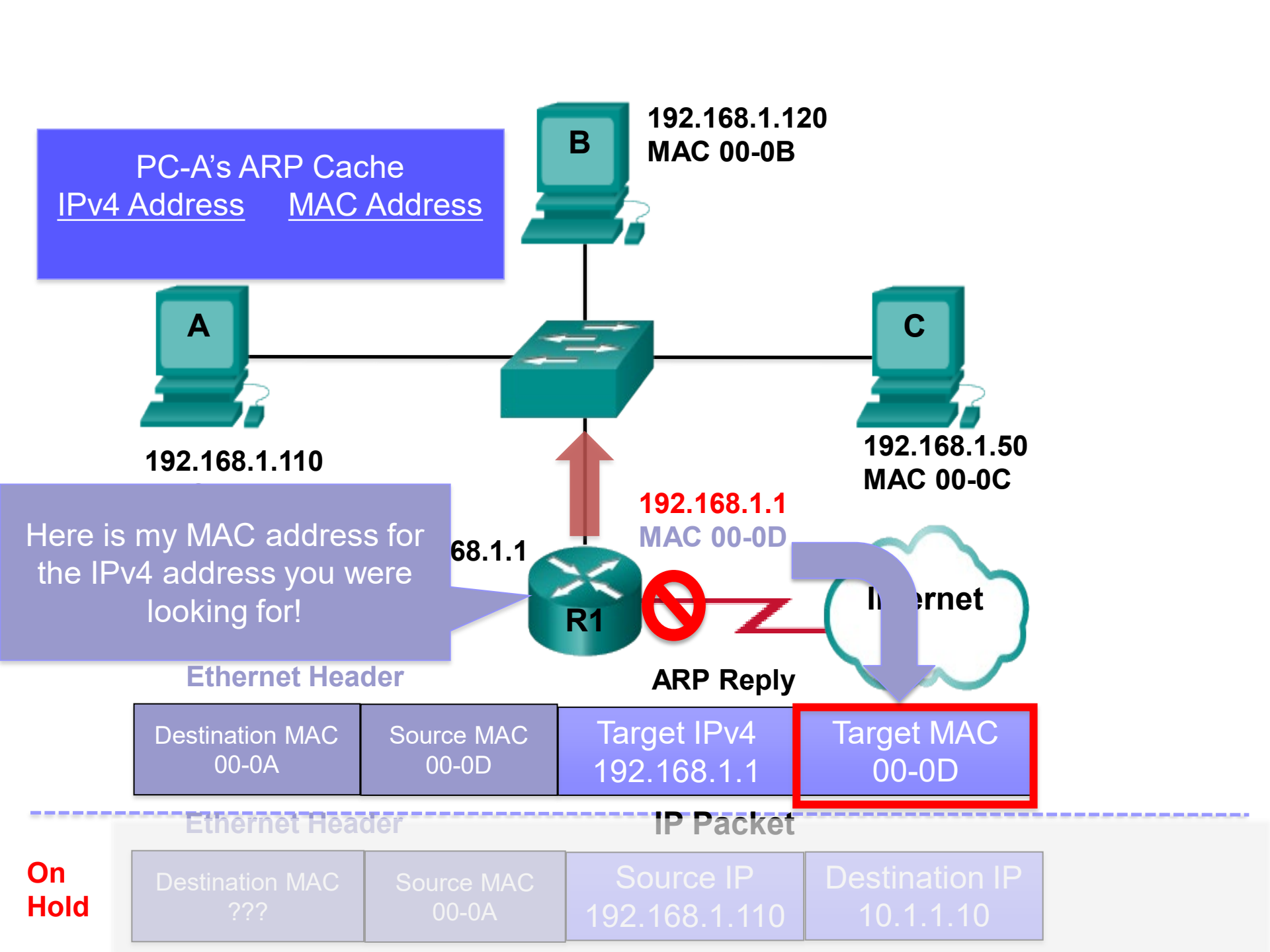

PC-A's ARP Cache
IPv4 Address
MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
ARP Request
Ethernet Header
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.1
Target MAC
???
IP Packet
Ethernet Header
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10

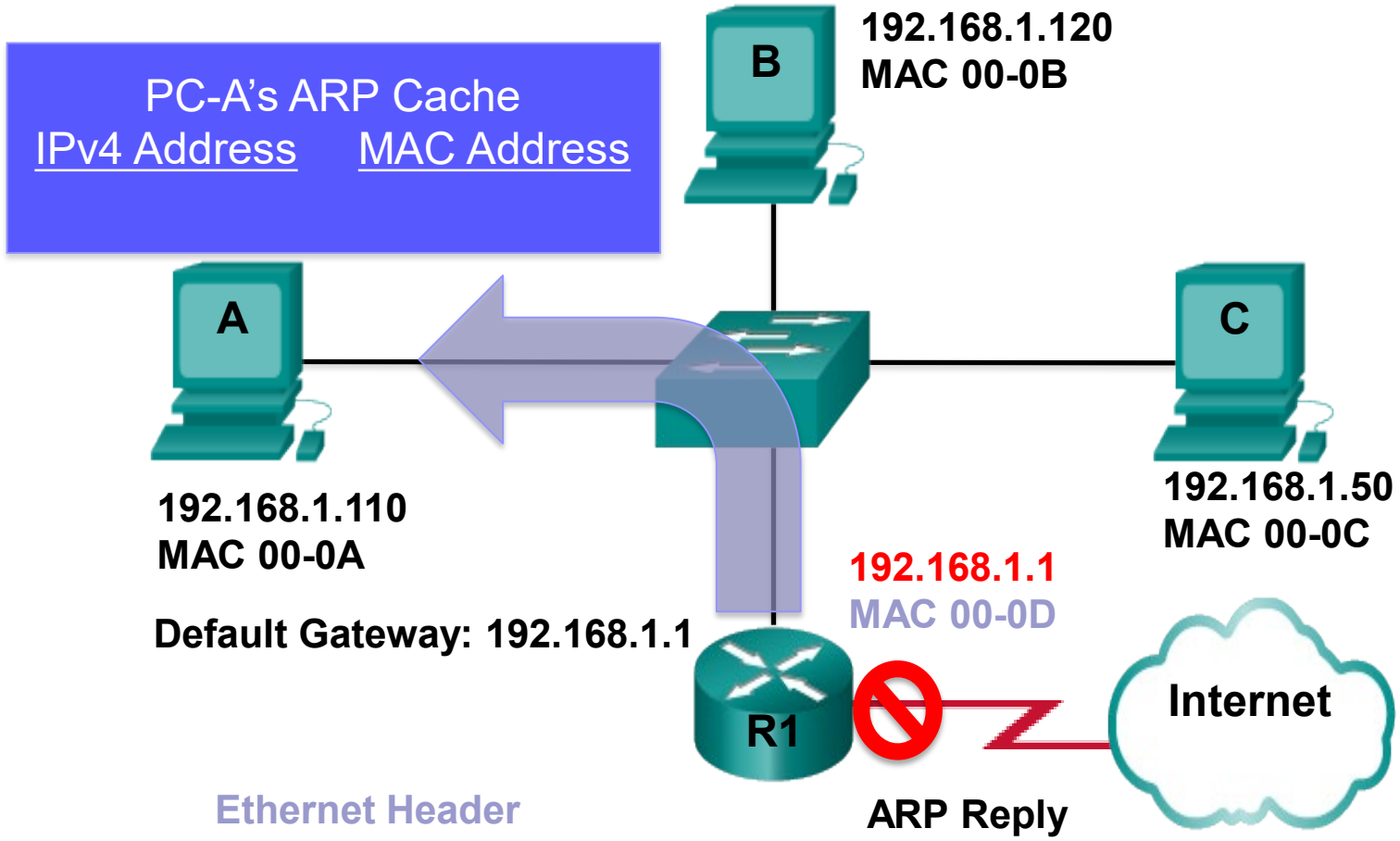
On Hold


The target IPv4 is not me.
PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Request
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.1
arget MAC
???
On Hold
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10

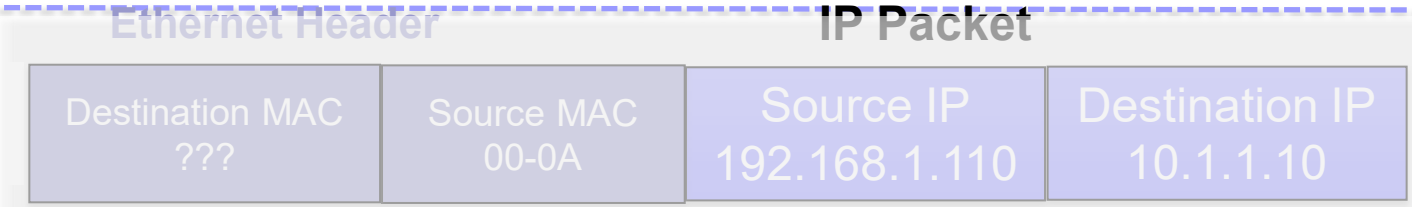

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
The target IPv4 is not me.
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
ARP Request
Ethernet Header
Destination MAC FF-FF
Source MAC 00-0A
Target IPv4 192.168.1.1
Target MAC ???
IP Packet
Ethernet Header
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 10.1.1.10
On Hold

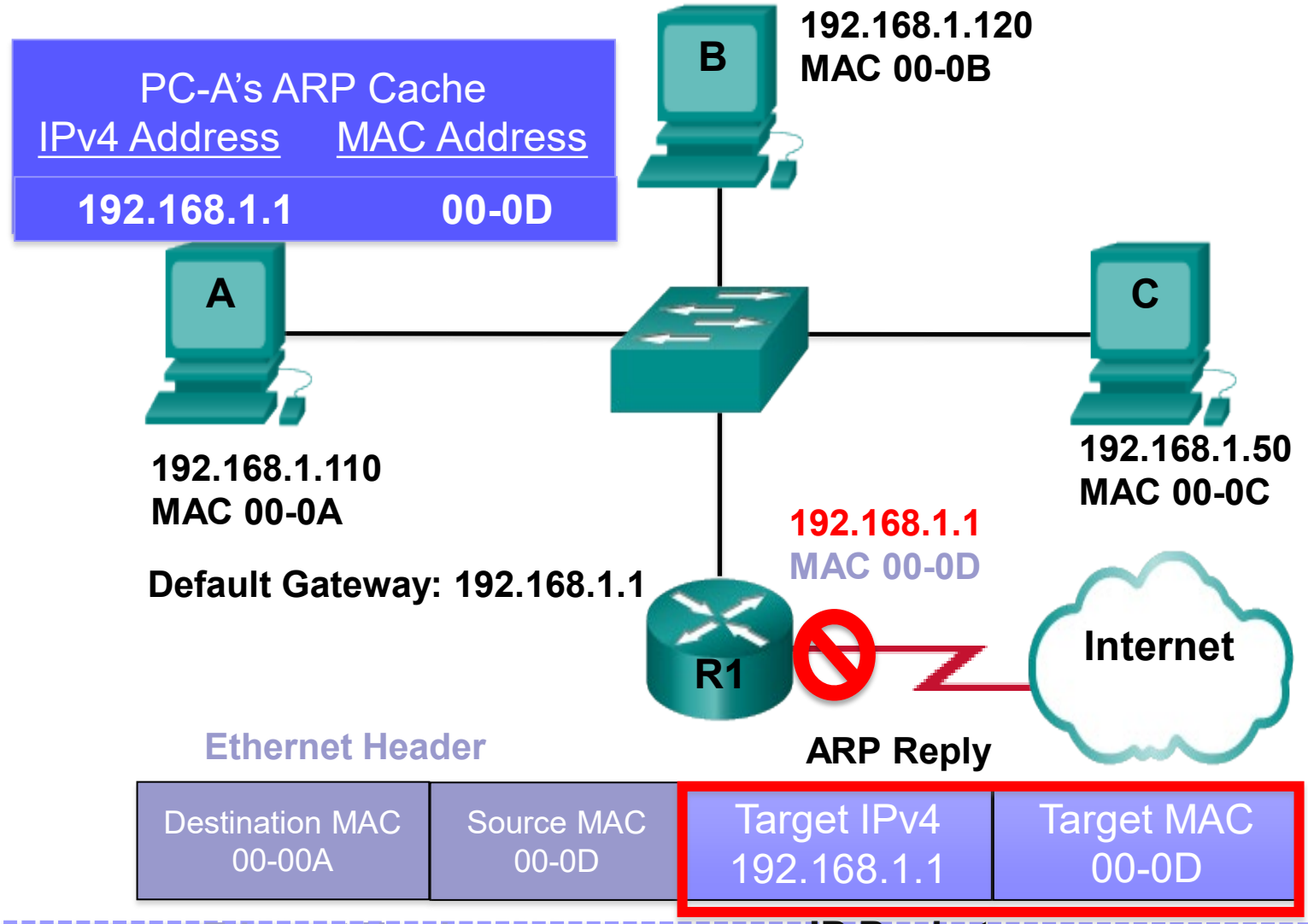

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.11(
MAC 00-0A
192.168.1.50
MAC 00-0C
The target IPv4 is for me!
192.168.1.1
MAC 00-0D
Default Gateway: 192.168.1.1
R1
Internet
Ethernet Header
ARP Request
Destination MAC FF-FF
Source MAC 00-0A
Target IPv4 192.168.1.1
Target MAC ???
Ethernet Header
IP Packet
On Hold
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 10.1.1.10

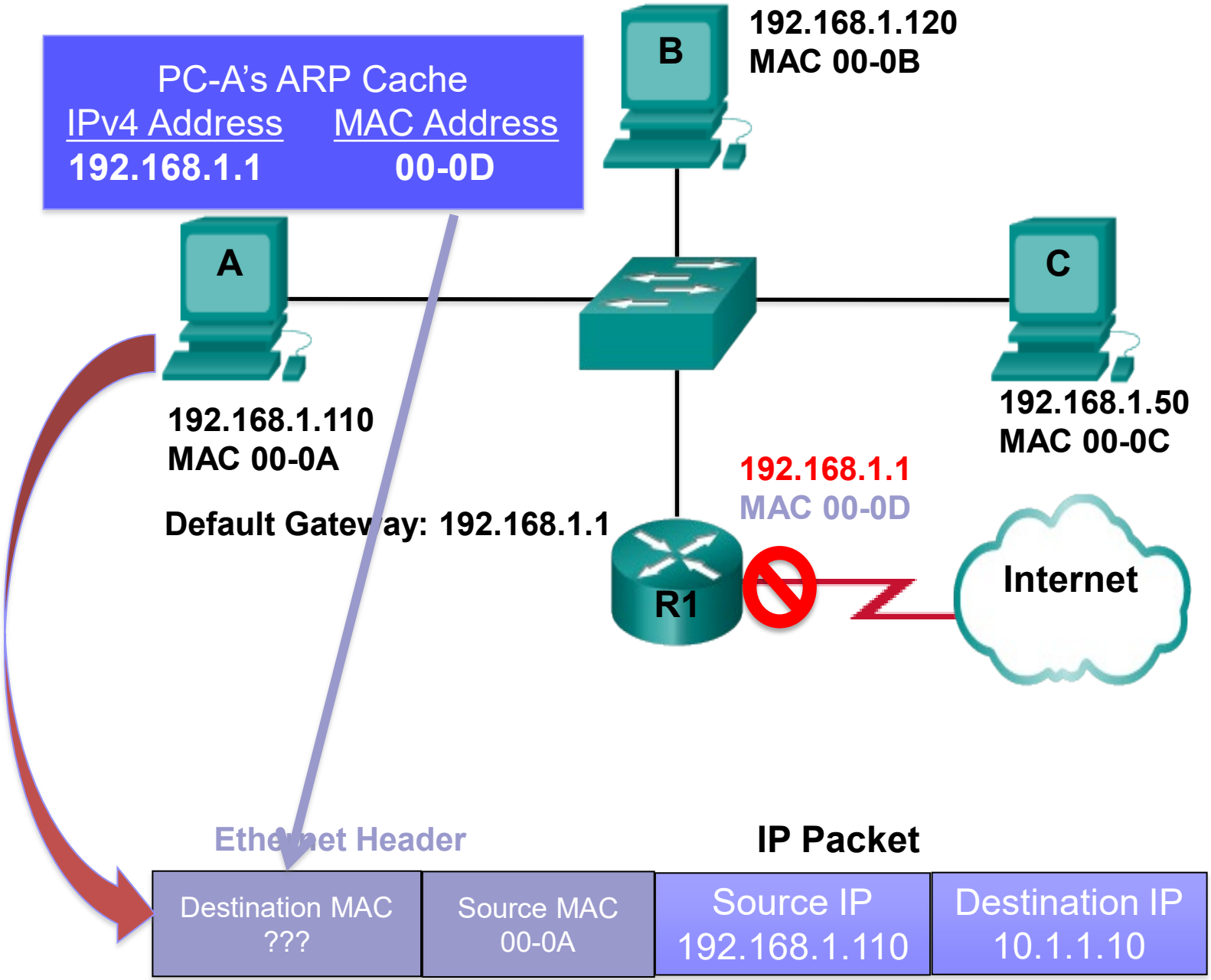

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
68.1.1
R1
Here is my MAC address for the IPv4 address you were looking for!
ARP Reply
Ethernet Header
Destination MAC 00-0A
Source MAC 00-0D
Target IPv4 192.168.1.1
Target MAC 00-0D
IP Packet
Ethernet Header
Destination MAC ???
Source MAC 00-0A
Source IP 192.168.1.110
Destination IP 10.1.1.10
On Hold

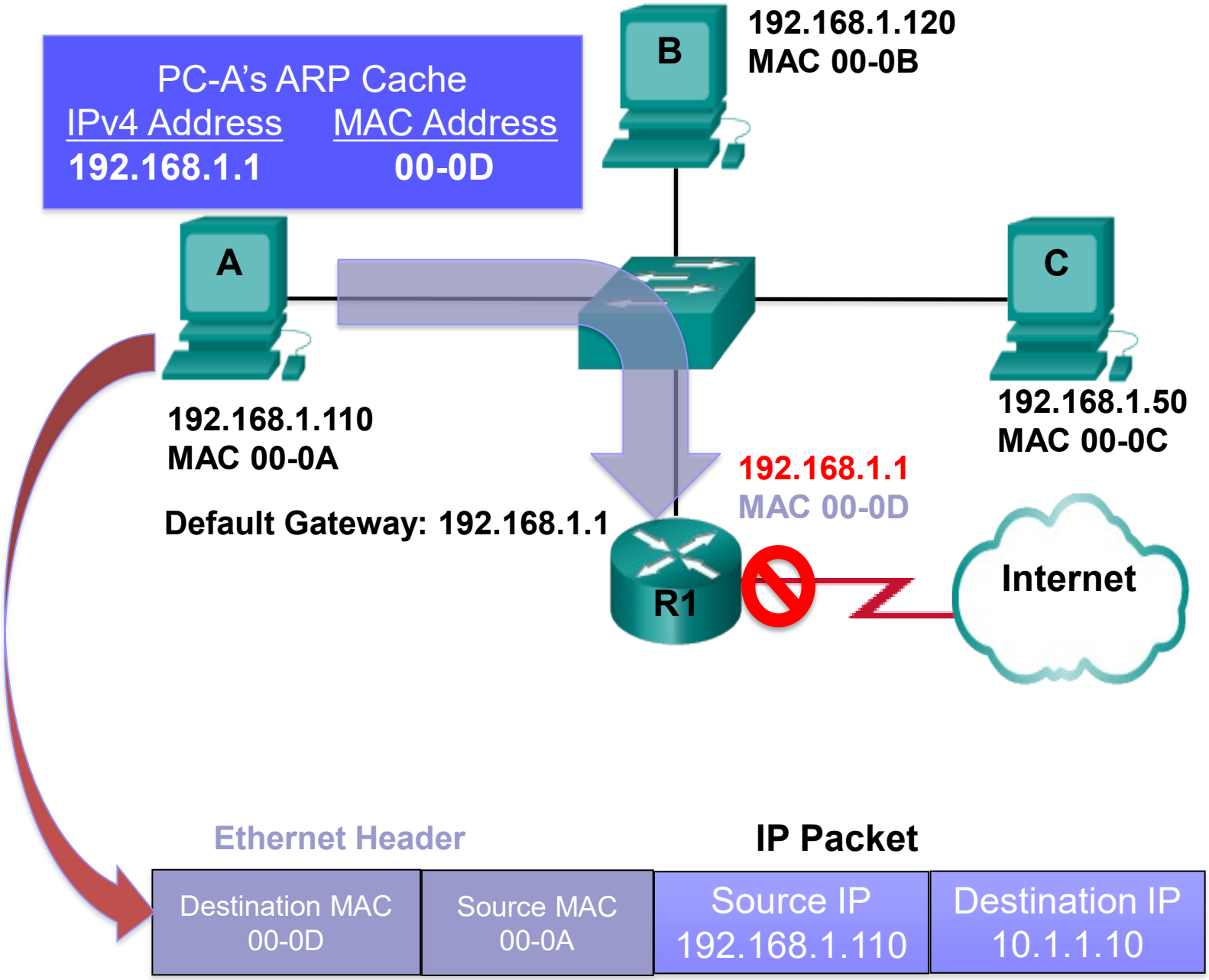

PC-A's ARP Cache
IPv4 Address
MAC Address
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
ARP Reply
Ethernet Header
Destination MAC
00-0A
Source MAC
00-0D
Target IPv4
192.168.1.1
Target MAC
00-0D

On Hold


Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10


PC-A's ARP Cache
IPv4 Address
MAC Address
192.168.1.1
00-0D
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
Destination MAC
00-00A
Source MAC
00-0D
Target IPv4
192.168.1.1
Target MAC
00-0D
ARP Reply
Ethernet Header
IP Packet
On Hold
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10


PC-A's ARP Cache
IPv4 Address
MAC Address
192.168.1.1
00-0D
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
???
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10


PC-A's ARP Cache
IPv4 Address
MAC Address
192.168.1.1
00-0D
B
192.168.1.120
MAC 00-0B
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
IP Packet
Destination MAC
00-0D
Source MAC
00-0A
Source IP
192.168.1.110
Destination IP
10.1.1.10

It's all about the IP Address

Emmy, you are in my neighborhood so I can take the letter to you!

Jean
Burlington, VT

Emmy
Burlington, VT

Lucy, I see by your address that you are somewhere else. So I have to take your letter to the Post Office.

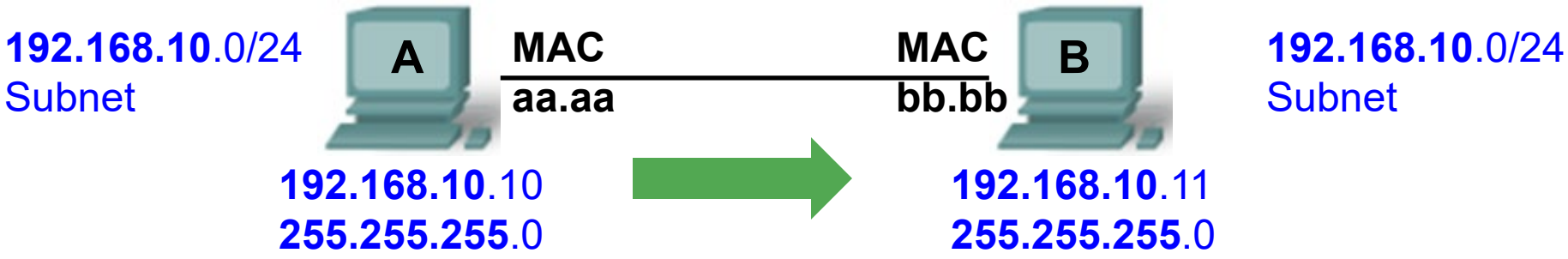
Jean
Burlington, VT

Lucy
Capitola, Ca

Emmy
Burlington, VT

- Even if two houses are on the same street, you only know the address so must take it to the local post office

Understanding IP communications



Destination Address bb.bb	Source Address aa.aa	Type	IP DA 192.168.10.11	FCS

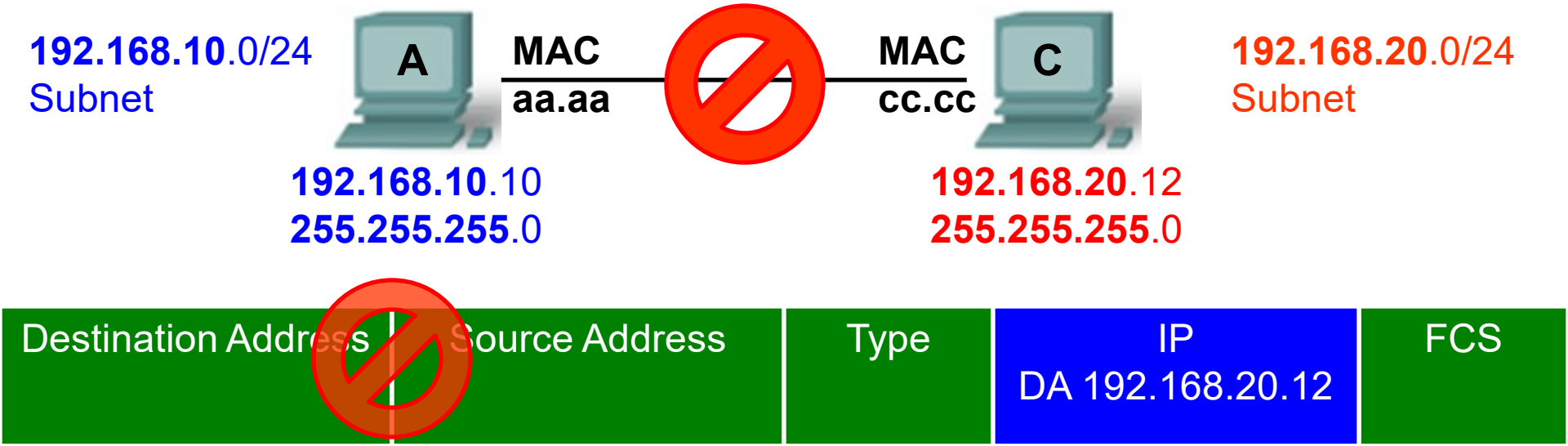
- Devices can only communicate with other devices on the same subnet
- A knows that it is on the 192.168.10.0/24 subnet (AND operation with its IP address and subnet mask). (Same subnet = Same subnet mask)
- A knows that B (192.168.1.11) is on its **same subnet** (AND operation with B's IP address and A's subnet mask)

```
A        192.168.10.10
   AND   255.255.255.0
 ---------------------
         192.168.10.0
```

SAME Subnet
A can reach B directly without going through a router

```
B        192.168.10.11
   AND   255.255.255.0
 ---------------------
         192.168.10.0
```

Understanding IP communications

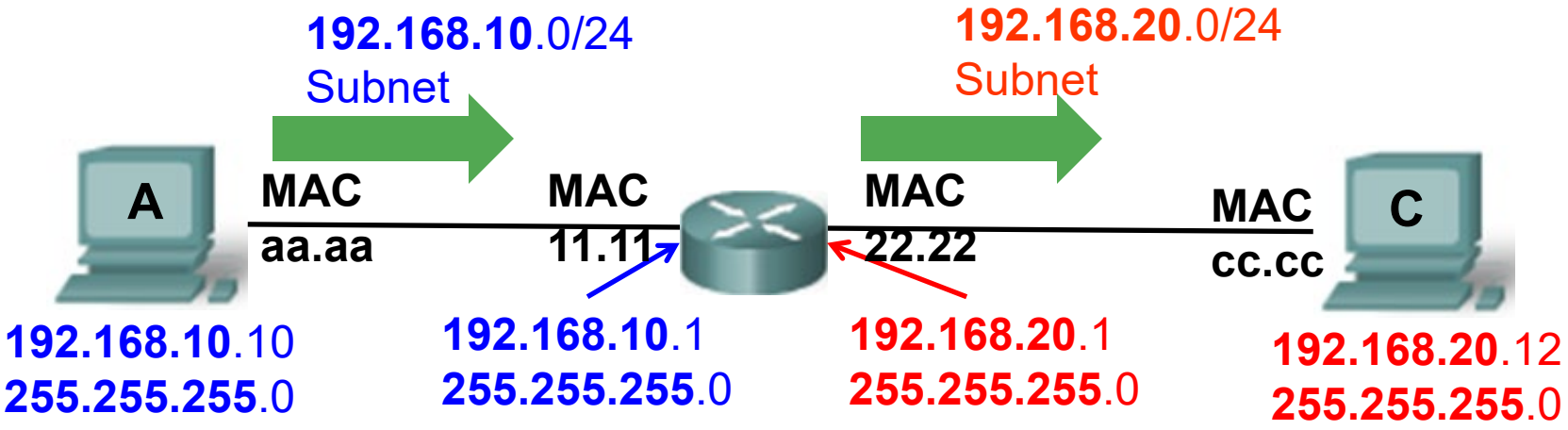


- Devices can only communicate with other devices on the same subnet
- A knows that it is on the 192.168.10.0/24 subnet (AND operation with its IP address and subnet mask) (Same subnet = Same subnet mask)
- A knows that C (192.168.20.12) is on a **different subnet** (AND operation with B's IP address and A's subnet mask) – ***Can't get there directly!***

```
A        192.168.10.10
    AND  255.255.255.0
  ------------------
         192.168.10.0
```

DIFFERENT Subnets
A can NOT reach B directly. Must go through a router

```
B        192.168.20.12
    AND  255.255.255.0
  ------------------
         192.168.20.0
```



Destination Address 11.11	Source Address aa.aa	Type	IP DA 192.168.20.12	FCS
Destination Address cc.cc	Source Address 22.22	Type	IP DA 192.168.20.12	FCS

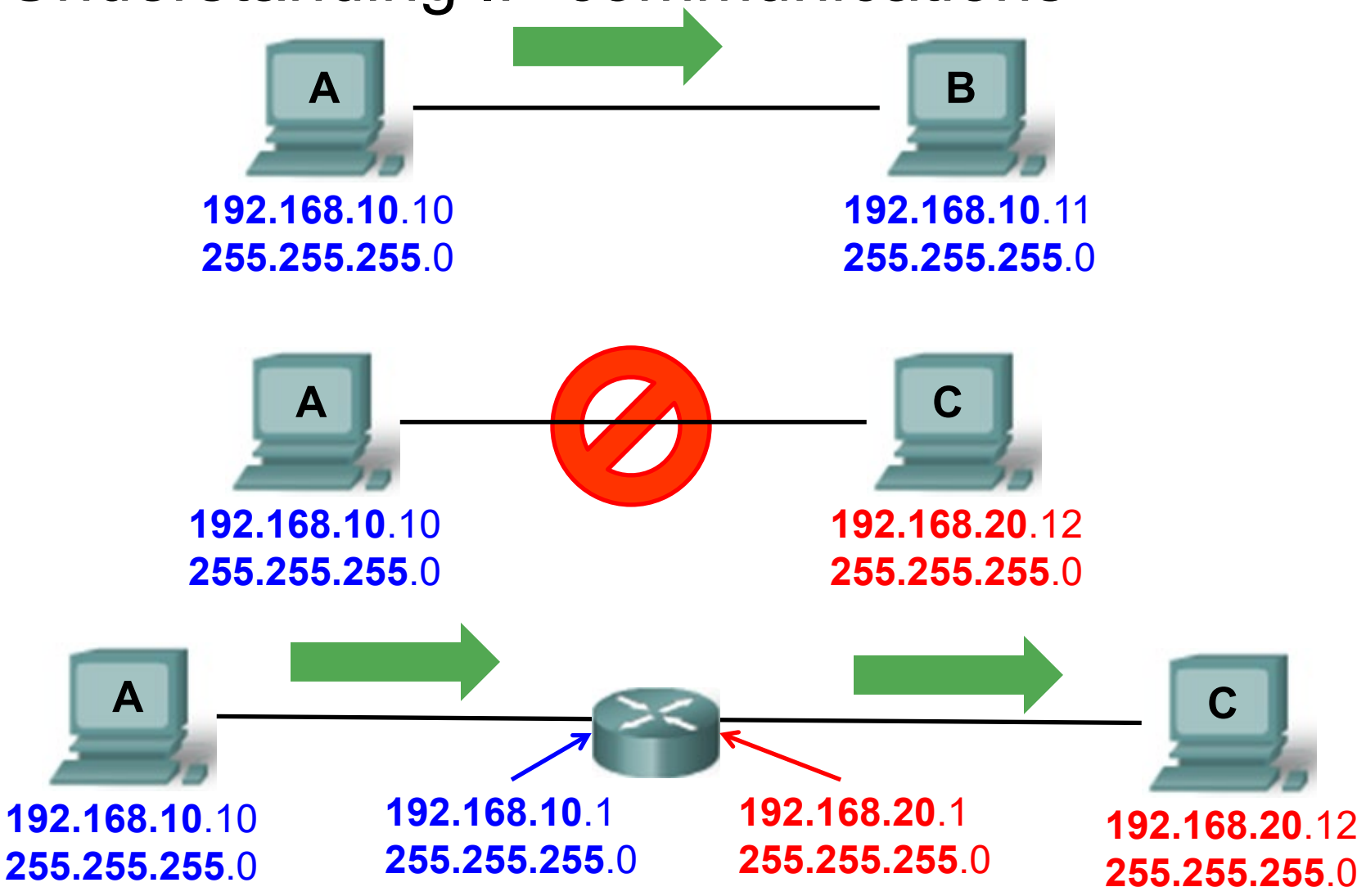
- A sends packet to devices in a DIFFERENT subnet directly to a router which is on the same subnet as A.
- The router will take care of it from there.

```
      192.168.10.10
AND   255.255.255.0
-------------------
      192.168.10.0
```

DIFFERENT Subnets
A can NOT reach B directly. Must go through a router

```
      192.168.20.11
AND   255.255.255.0
-------------------
      192.168.20.0
```

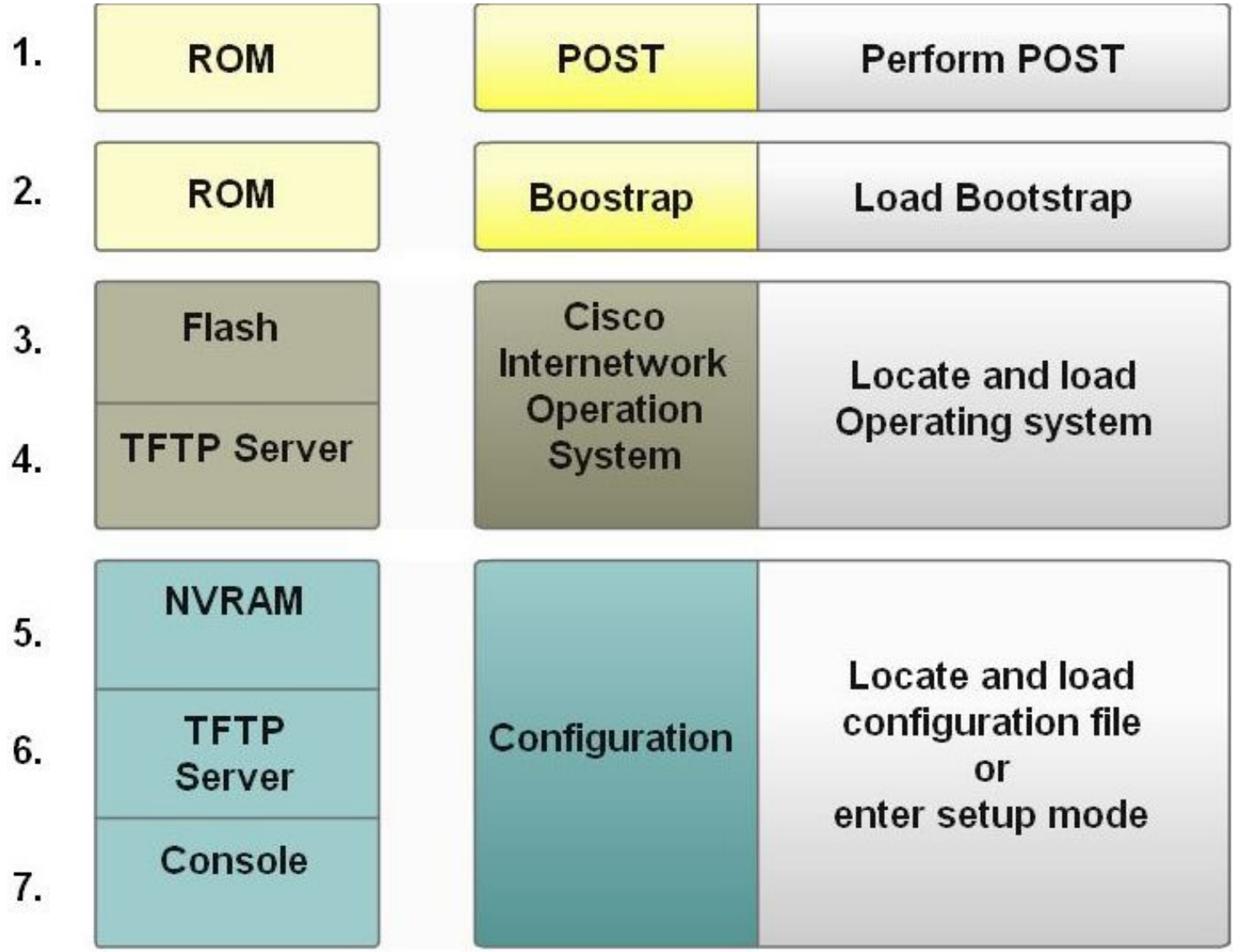
Understanding IP communications



- Devices can only communicate with other devices on the same subnet
- Otherwise, they must go through a router, that is on its same subnet

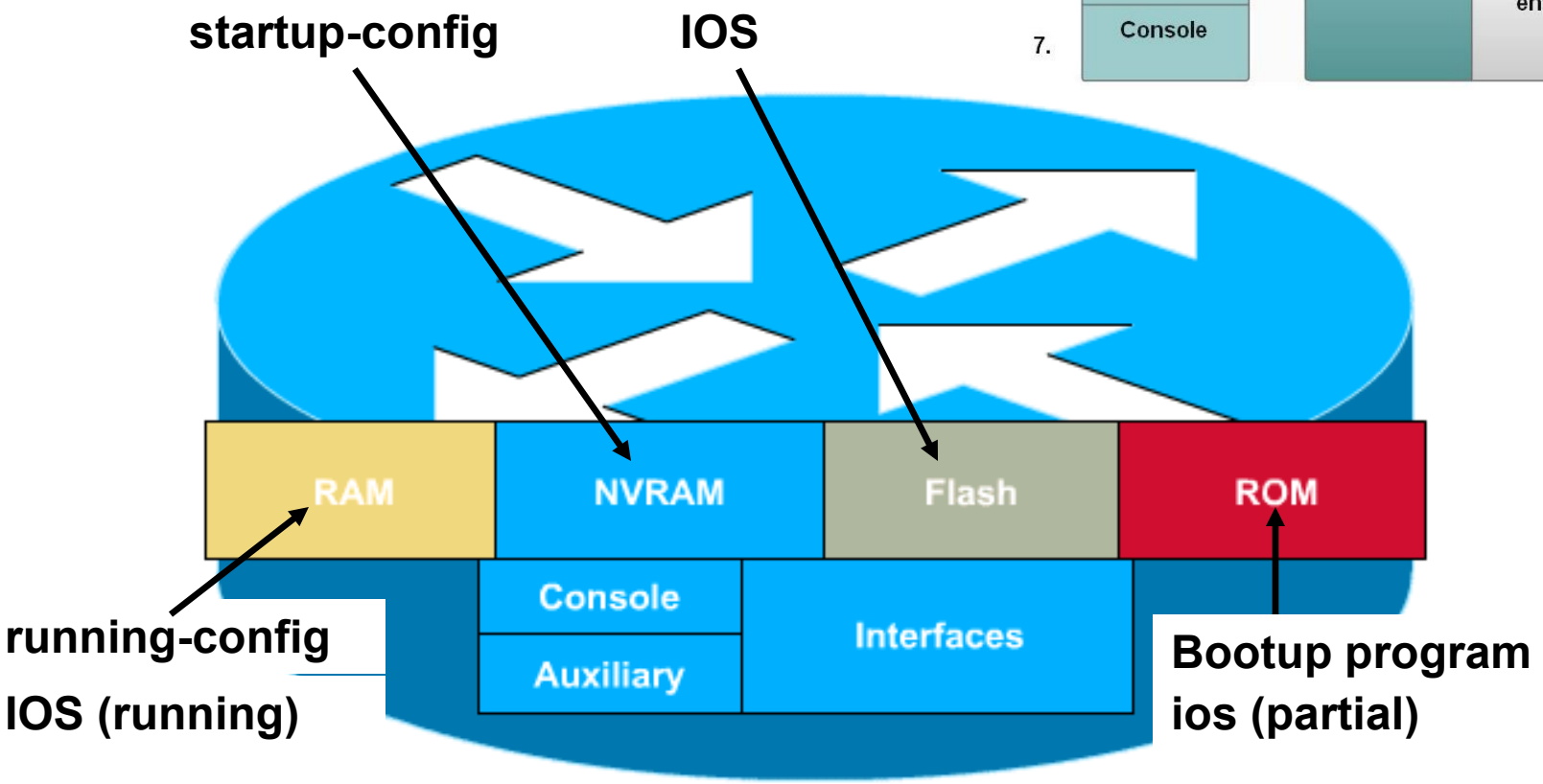
Switched Environment

Router/Switch Bootup Process

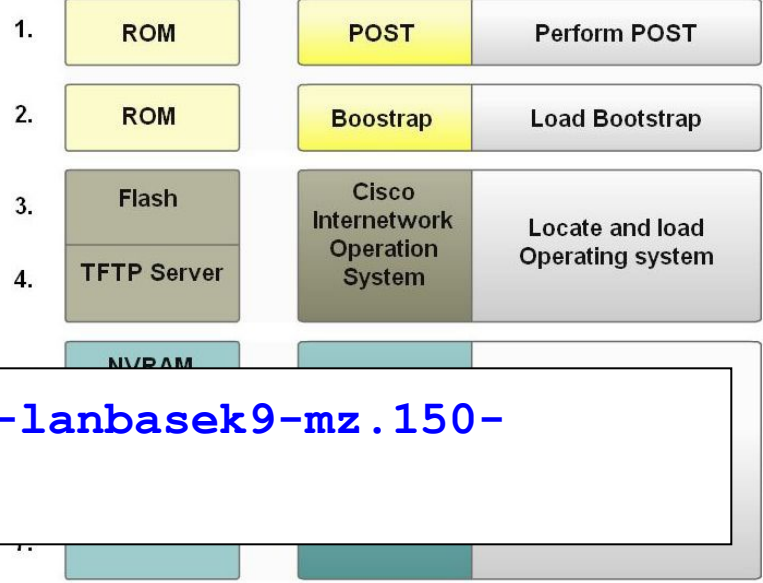


Bootup Process

1.	ROM	POST	Perform POST
2.	ROM	Boostrap	Load Bootstrap
3.	Flash	Cisco Internetwork Operation System	Locate and load Operating system
4.	TFTP Server		
5.	NVRAM	Configuration	Locate and load configuration file or enter setup mode
6.	TFTP Server		
7.	Console		



Switch Boot Sequence




```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-
2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

- By default, the the boot loader attempts to load and execute the first executable file it can by searching the flash file system.
- If **`boot system`** commands in **startup-config**

a. **Run `boot system` commands** in order they appear in startup-config to locate the IOS

b. If boot system commands **fail**, use default fallback sequence to locate the IOS (**Flash**, TFTP, ROM)

- On Catalyst 2960 Series switches, the image file is normally contained in a directory that has the same name as the image file.

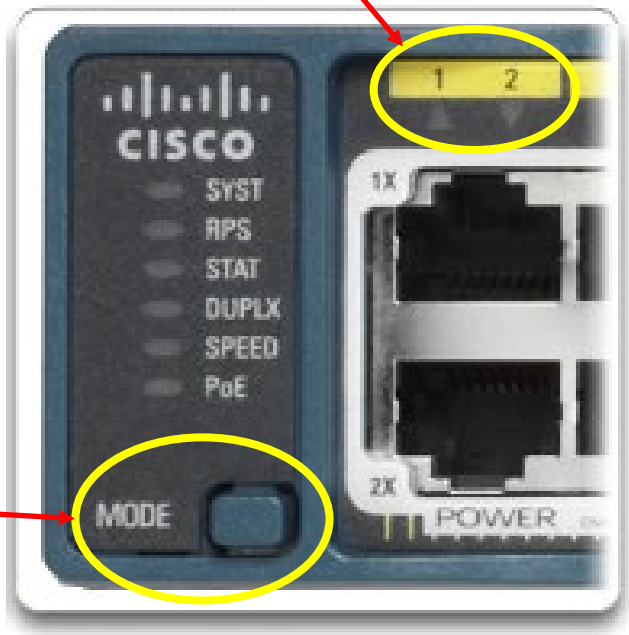
Directory Listing in Boot Loader

```
Switch# dir flash:
Directory of flash:/

    2  -rwx    11607161   Mar 1 2013 03:10:47 +00:00  c2960-
lanbasek9-mz.150-2.SE.bin
    3  -rwx        1809   Mar 1 2013 00:02:48 +00:00  config.text
    5  -rwx        1919   Mar 1 2013 00:02:48 +00:00  private-
config.text
    6  -rwx       59416   Mar 1 2013 00:02:49 +00:00  multiple-fs

32514048 bytes total (20841472 bytes free)
Switch#
```

Switch LED Indicators

- Each port on the Cisco Catalyst switches have status LED indicator lights.
  - LED lights reflect port activity, but they can also provide other information about the switch through the Mode button.

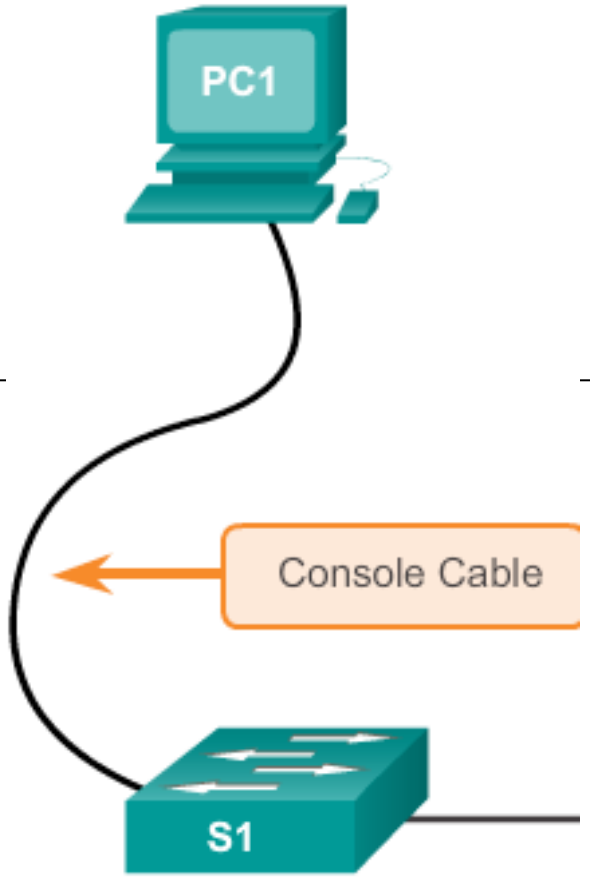
- The following modes are available on Catalyst 2960 switches:
  1. System LED
  2. Redundant Power System (RPS) LED
     - If RPS is supported on the switch
  3. Port Status LED (Default mode)
  4. Port Duplex LED
  5. Port speed LED
  6. PoE Status (If supported)
  7. Port LEDs
  8. Mode button



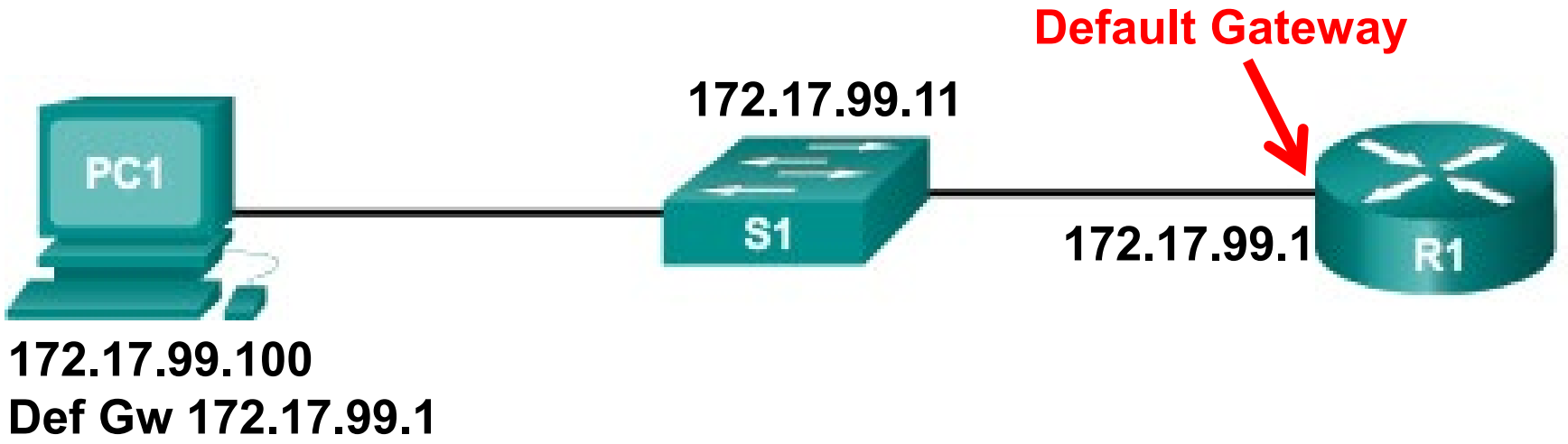
Status LEDs	LED is …	Description
System LED	Off	System is not powered
	Green	System is operating normally
	Amber	System is receiving power but is not functioning properly
Redundant Power	Off	RPS is off or not properly connected
	Green	RPS is connected and ready to provide back-up
	Blinking Green	RPS providing power to another device
	Amber	RPS is in standby mode or in a fault condition.
	Blinking Amber	Internal power supply has failed, and the RPS is providing power.
Port Status LED	Green	A link is present.
	Off	There is no link, or the port was administratively shut down
	Blinking green	Activity and the port is sending or receiving data.
	Alternating Green-Amber	There is a link fault.
	Amber	Port is blocked to ensure there is no STP loop
	Blinking amber	Port is blocked to prevent a possible loop in the forwarding domain.
Port Duplex LED	Off	Ports are in half-duplex mode.
	Green	Port is in full-duplex mode.
Port speed LED	Off	Port is operating at 10 Mb/s.
	Green	Port is operating at 100 Mb/s.
	Blinking Green	Port is operating at 1000 Mb/s.
PoE Status (If supported)	Off	LED is off, the PoE is off.
	Green	LED is green, the PoE is on
	Alternating Green-Amber	PoE is denied because it will exceed the switch power capacity
	Blinking Amber	LED is blinking amber, PoE is off due to a fault.
	Amber	PoE for the port has been disabled.

Configure Switch Management Interface

```
S1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# interface vlan 99
S1(config-if)# ip address 172.17.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

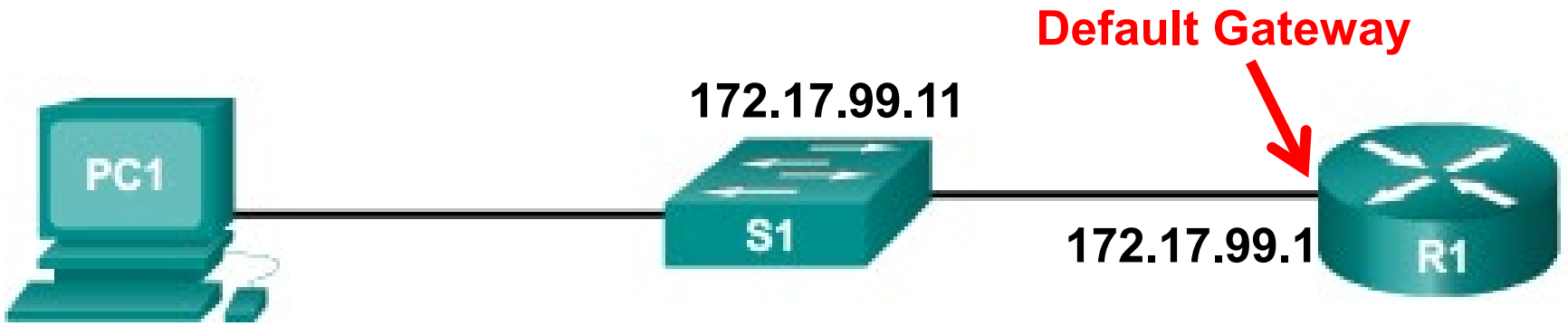


Assign a Default Gateway




```
S1(config)# ip default-gateway 172.17.99.1
S1(config)# end
S1#
```

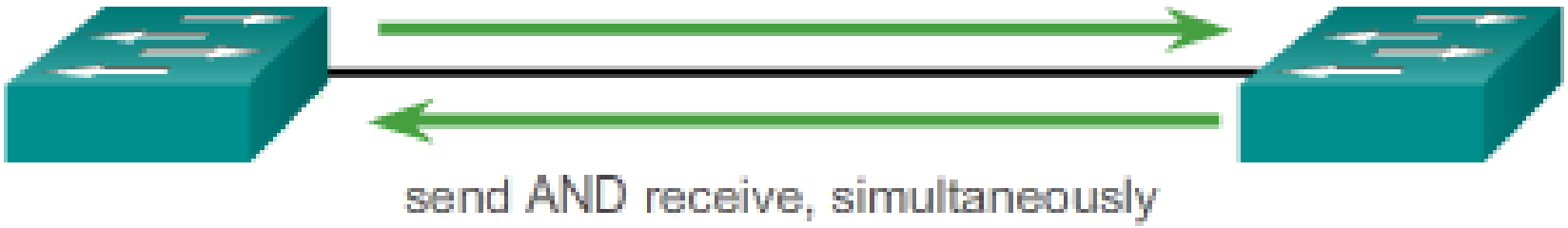
Assign a Default Gateway




```
S1# show ip interface brief

Interface              IP-Address      OK?     Method  Status   Protocol
Vlan99                 172.17.99.11    YES     manual  up       up
```

Configure Switch Ports

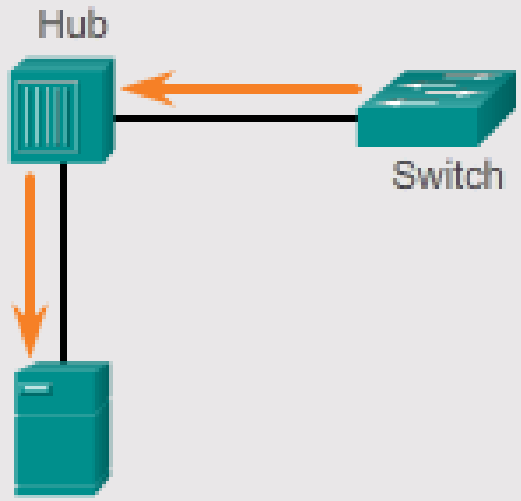
Full-Duplex Communication



- Switch ports by default operate in full duplex (unless attached to a hub).
- Increases effective bandwidth allowing bidirectional forwarding.

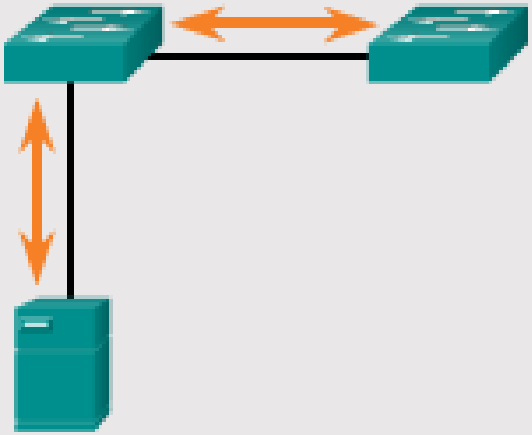
Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

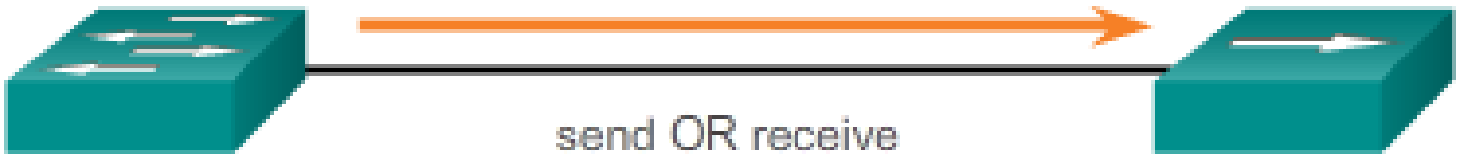


Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled



Half-Duplex Communication



- **Half-dup**lex communication is unidirectional and sending and receiving data does not occur at the same time.
  - **Half-duplex** communication often resulting in **collisions**.
  - Typically seen in ***older hardware***, such as hubs.

- Most Ethernet and Fast Ethernet NICs sold today offer **full-duplex** capability.
  - **Gigabit Ethernet and 10Gb NICs** require full-duplex connections.

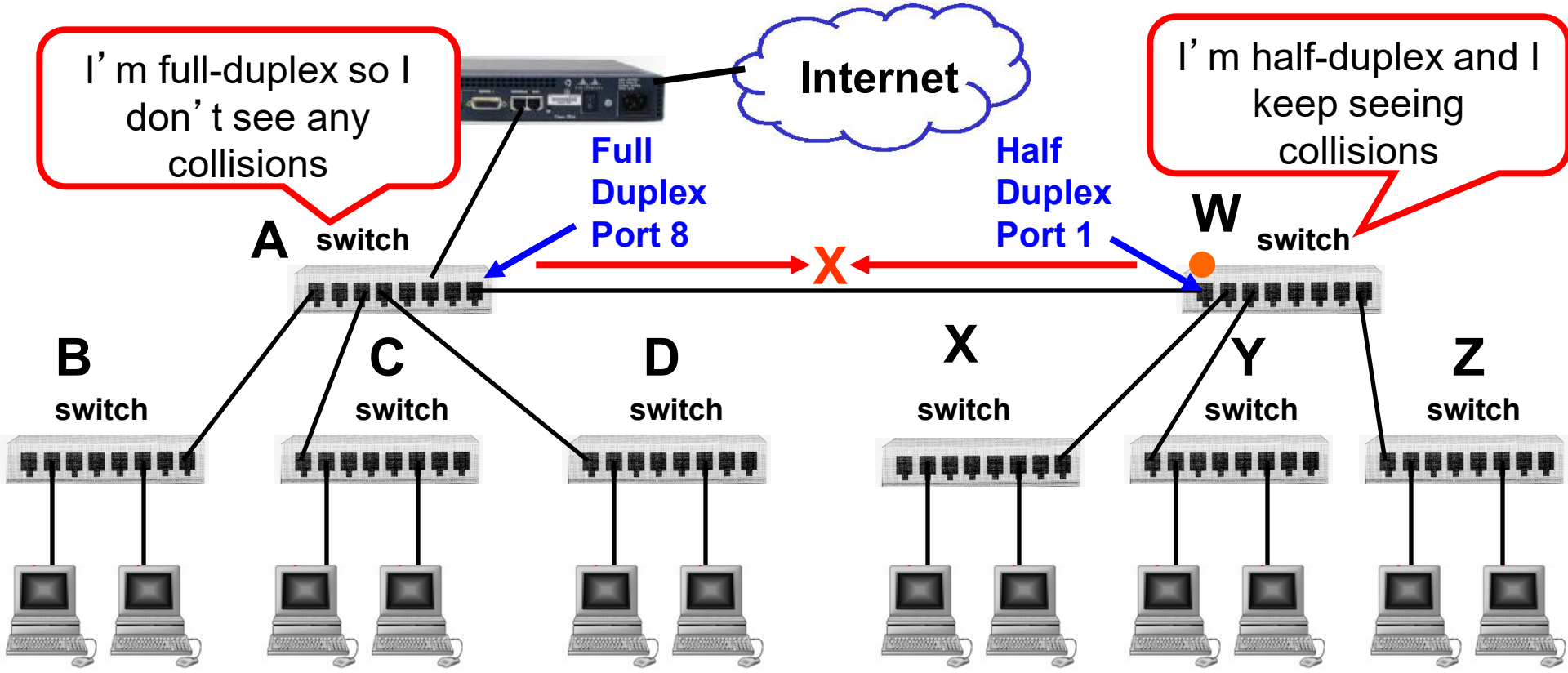
Configure Duplex and Speed

- Duplex and speed settings on most switches are autosensed.
- Manual

```
Switch(config-if)# speed [10 | 100 | 1000 | auto]
Switch(config-if)# duplex [half | full | auto]
```

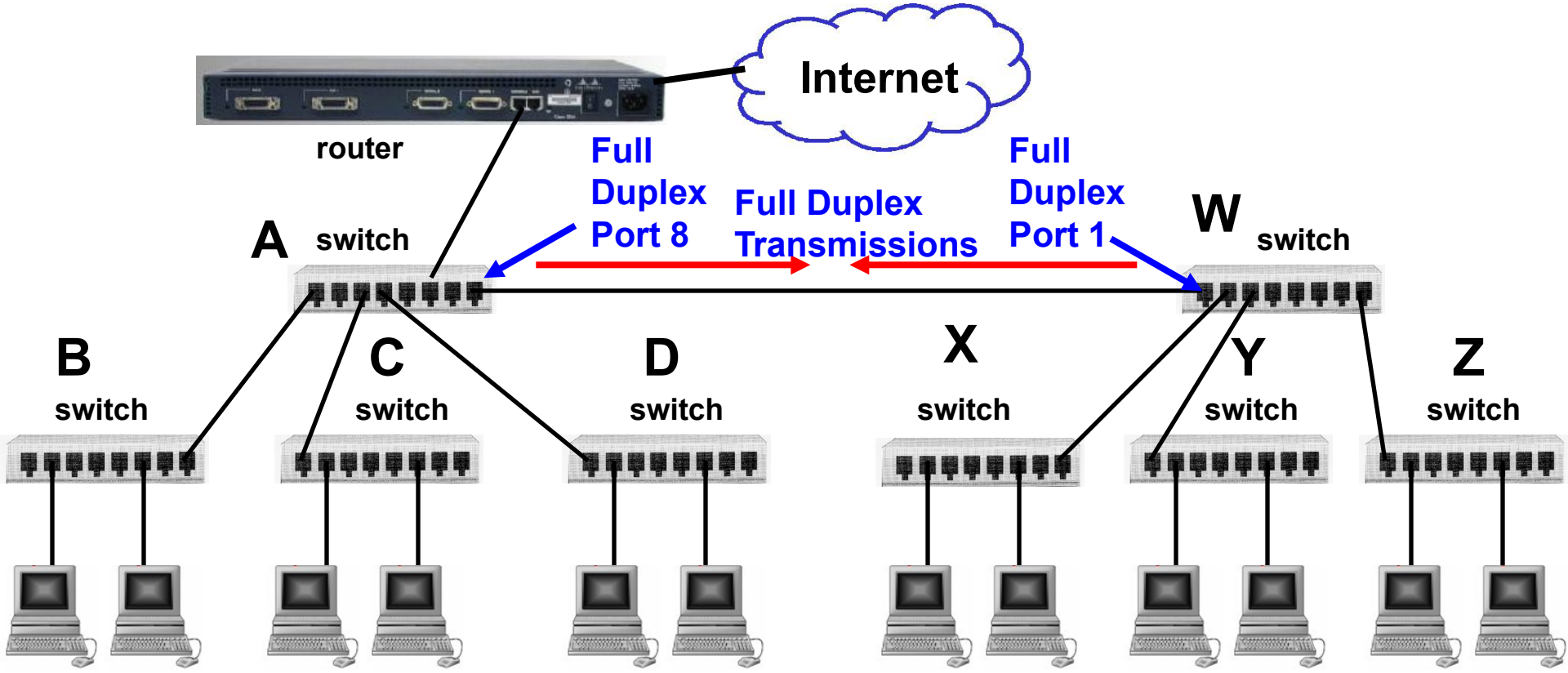
- When troubleshooting switch port issues, the duplex and speed settings should be checked.
  - Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues.
  - Auto-negotiation failure creates mismatched settings.

Real World Troubleshooting – Duplex Mismatch



- The problem is that
  - Switch A, Port 8 is in Full-duplex mode
  - Switch W, Port 1 is in Half-duplex mode
- Switch A sends whenever it wants to without listening first to see if Switch W is sending.

Real World Troubleshooting – Duplex Mismatch



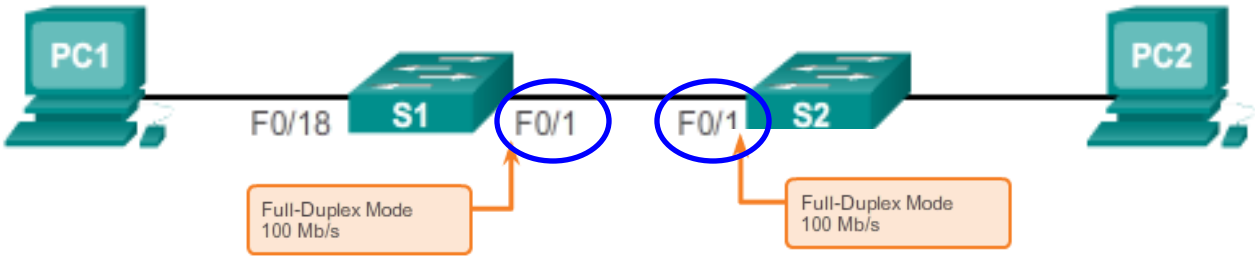
- Configure Switch W, Port 1 to be in full duplex, the same as Switch A, Port A.

Duplex and Speed settings

- Auto-negotiation (i.e., **`duplex auto`** and **`speed auto`**) is useful when the speed and duplex settings of the device connecting to the port are unknown or may change.
  - When connecting to known devices, such as servers, dedicated workstations, or network devices, best practice is to manually set the speed and duplex settings.

- When troubleshooting switch port issues, the duplex and speed settings should be checked.
  - Mismatched settings for the duplex mode and speed of switch ports can cause connectivity issues.
  - Auto-negotiation failure creates mismatched settings.

Configure Duplex and Speed



- It's best practice is to manually set the speed/duplex settings when connecting to known devices (i.e., servers, dedicated workstations, or network devices).

```
S1(config)# interface fastethernet 0/1
S1(config-if)# speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
S1(config-if)# speed 100
S1(config-if)# duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
S1(config-if)# duplex full
S1(config-if)# ^Z
S1#
```

```
S2(config)# interface fastethernet 0/1
S2(config-if)# speed 100
S2(config-if)# duplex full
S2(config-if)# ^Z
S2#
```

MDIX Setting

Straight-through cable

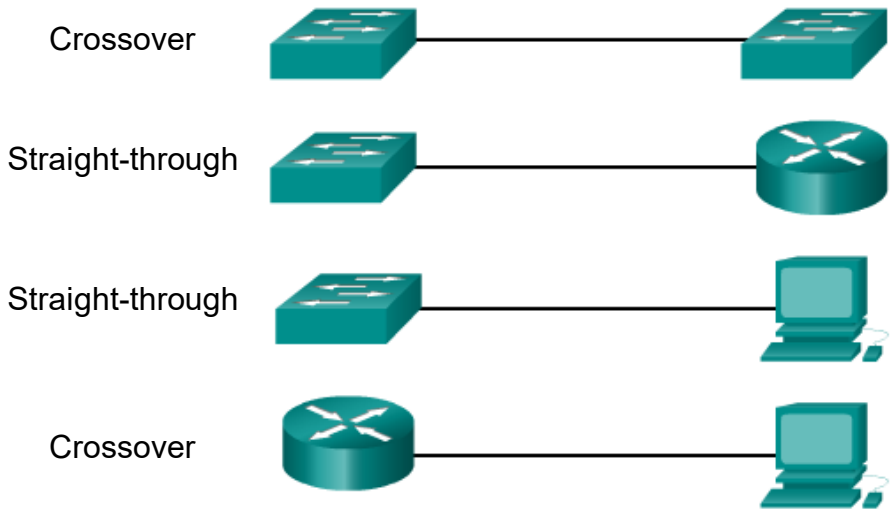
Crossover cable

- Older switches must use the correct cable when connecting to another device.

- To connect:
  - Servers, workstations, or routers: Straight-through cable
  - Two switches: Crossover cable

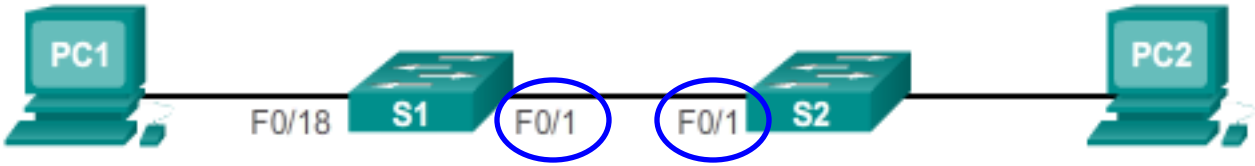
- Newer switches support the automatic medium-dependent interface crossover (**auto-MDIX**) feature.
  - This automatically detects the required cable connection type and configures the connection appropriately therefore either type of cable can be used to connect to other devices.

Auto-MDIX



- Connections between specific devices, such as switch-to-switch, switch-to-router, switch-to-host, and router-to-host device, once required the use of a specific cable types (crossover or straight-through).
- Modern Cisco switches support the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature.

Configuring MDIX Setting



- **`mdix auto`** interface configuration
  - Requires the commands **`speed auto`** and **`duplex auto`**

```
S1(config)# interface fa0/1
S1(config-if)# speed auto
S1(config-if)# duplex auto
S1(config-if)# mdix auto
S1(config-if)#
```

```
S1(config)# interface fa0/1
S1(config-if)# speed auto
S1(config-if)# duplex auto
S1(config-if)# mdix auto
S1(config-if)#
```

- **Note:**
  - The auto-MDIX feature is enabled by default on Catalyst 2960 and Catalyst 3560 switches, but is not available on the older Catalyst 2950 and Catalyst 3550 switches.
  - Don't depend on auto-mdix – use the correct cable in the lab.

Verify MDIX Setting

```
S1# show controllers ethernet-controller fa 0/1 phy | include Auto-MDIX
 Auto-MDIX                       :  On    [AdminState=1    Flags=0x00056248]
S1#
```

Verifying Switch Port Configuration

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** or S1# **show mac address-table**

Troubleshooting Access Layer Issues

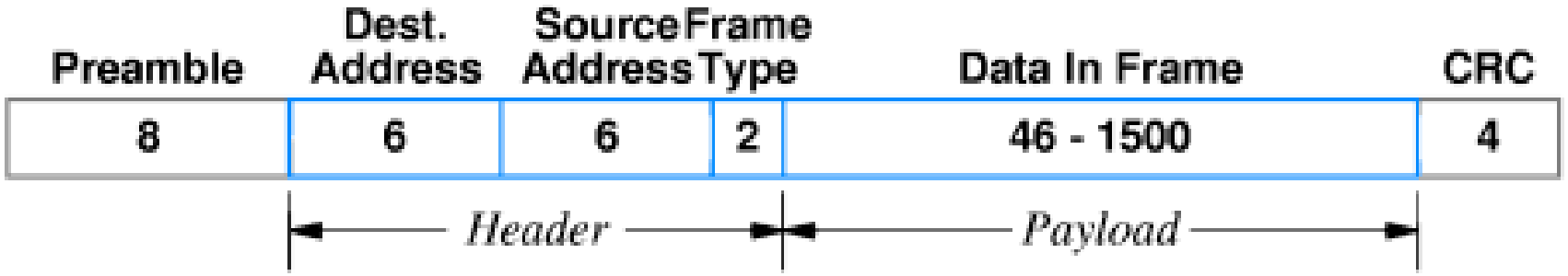
```
S1# show interfaces fa 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 000d.bda1.5601 (bia 000d.bda1.5601)
 BW 100000 Kbit, DLY 1000 usec,
```

If the output is:

- **up down**: Encapsulation type mismatch, the interface on the other end could be error-disabled, or there could be a hardware problem.
- **down down**: A cable is not attached or some other interface problem exists.
- **administratively down**: The **shutdown** command has been issued.

```
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
S1#
```

Troubleshooting Access Layer Issues



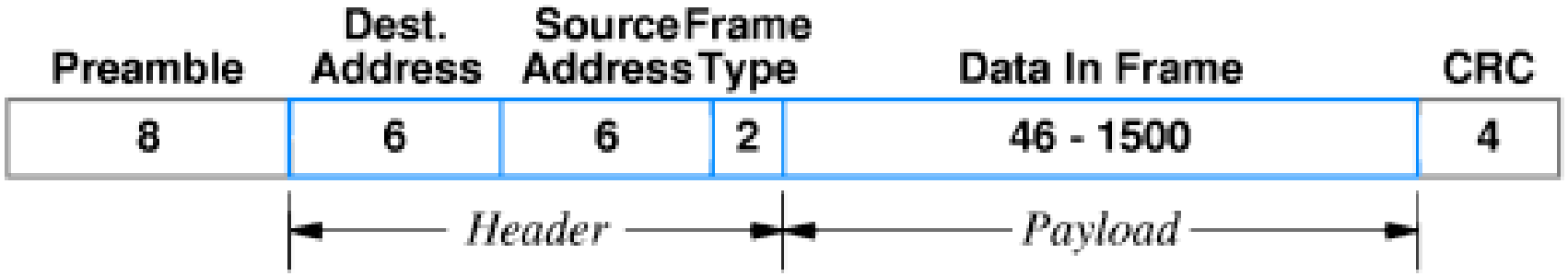
Runt Frames - Ethernet frames that are shorter than the 64-byte minimum allowed length are called runts.

Giants - Ethernet frames that are longer than the maximum allowed length are called giants. (Bad NIC)

CRC errors - On Ethernet and serial interfaces, CRC errors usually indicate a media or cable error.

```
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
S1#
```

Troubleshooting Access Layer Issues



Collisions – Only part of normal operations if interface is operating in half duplex – connected to a hub.

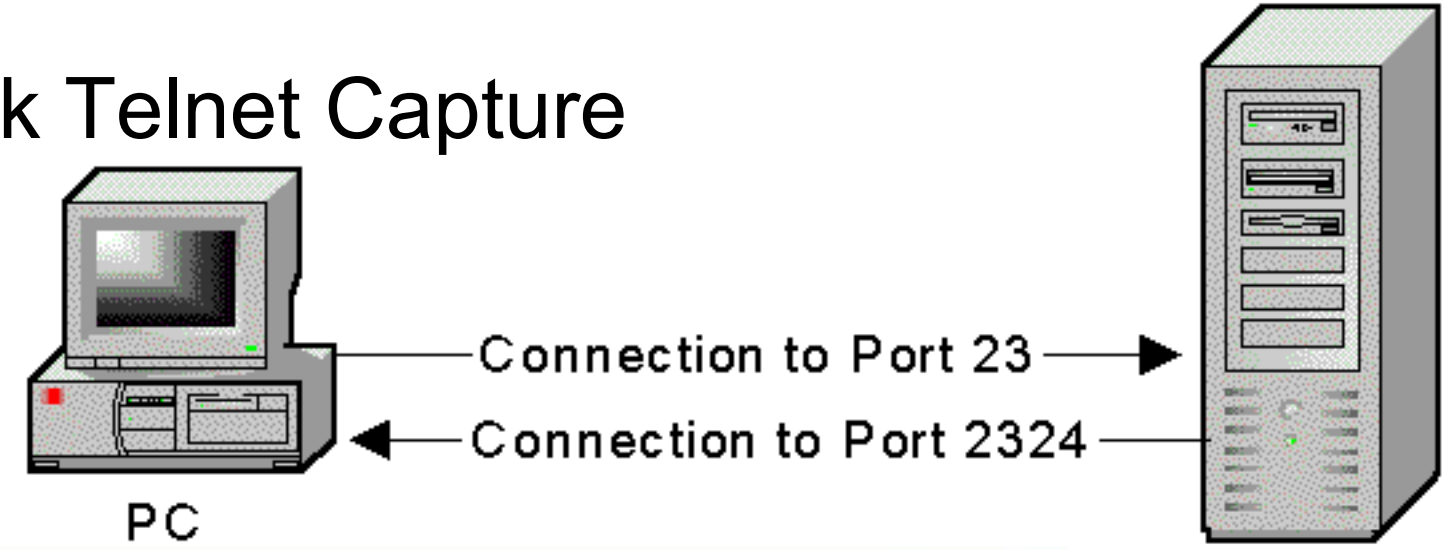
Late Collisions – Operating in half duplex and excessive cable length.

Cause – Result of duplex mismatch

- One side half duplex
- Other side full duplex

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
S1#
```

Wireshark Telnet Capture



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: telnet Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
8	1.711459	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...
9	1.716817	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...
20	6.207655	192.168.2.7	192.168.2.101	TELNET	Telnet Data ...
21	6.210896	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...
22	6.210979	192.168.2.7	192.168.2.101	TELNET	Telnet Data ...
23	6.211027	192.168.2.101	192.168.2.7	TELNET	Telnet Data ...

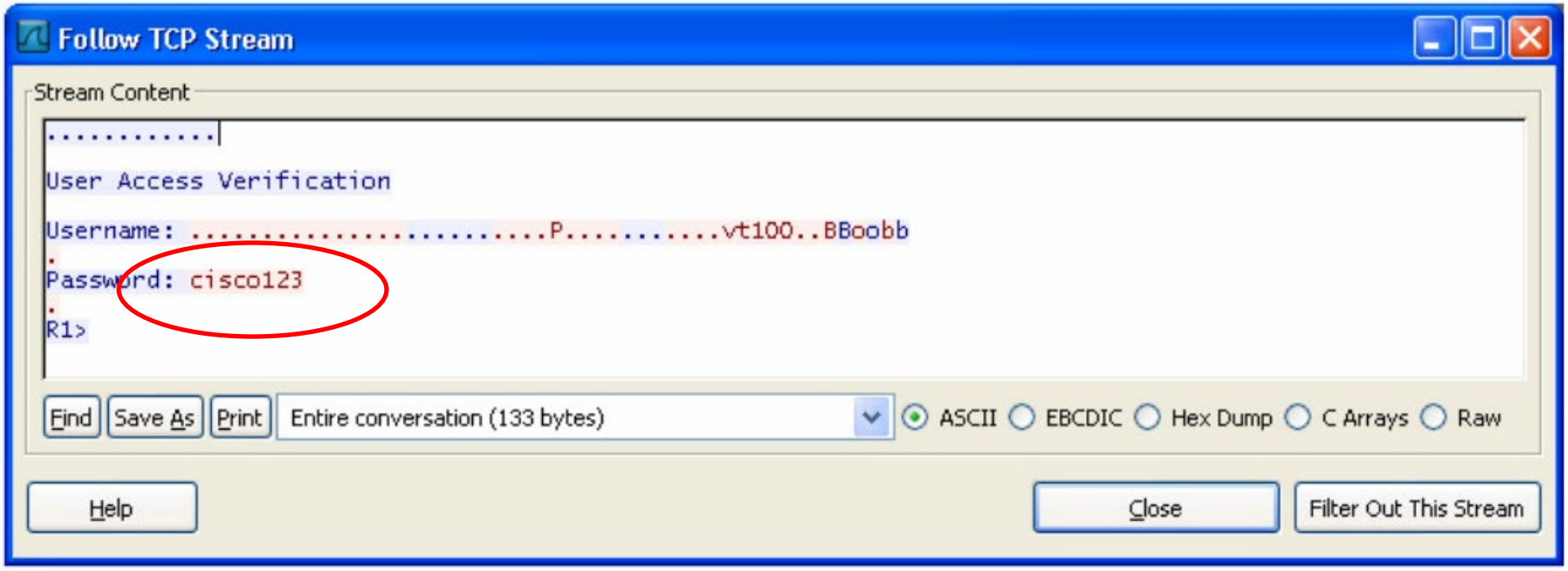
```
Frame 8 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Cisco_54:e2:a0 (00:11:92:54:e2:a0), Dst: Usi_e4:82:43 (00:16:41:e4:82:43)
Internet Protocol, Src: 192.168.2.101 (192.168.2.101), Dst: 192.168.2.7 (192.168.2.7)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1297 (1297), Seq: 1, Ack: 1, Len: 12
Telnet
```

```
0000  00 16 41 e4 82 43 00 11  92 54 e2 a0 08 00 45 00   ..A..C.. .T....E.
0010  00 34 12 5d 00 00 ff 06  23 aa c0 a8 02 65 c0 a8   .4.]....  #....e..
0020  02 07 00 17 05 11 d7 9b  5f 53 a1 31 5a 9c 50 18   ........  _S.1Z.P.
0030  10 20 ce e2 00 00 ff fb  01 ff fb 03 ff fd 18 ff   . ......  ........
0040  fd 1f                                             ..
```

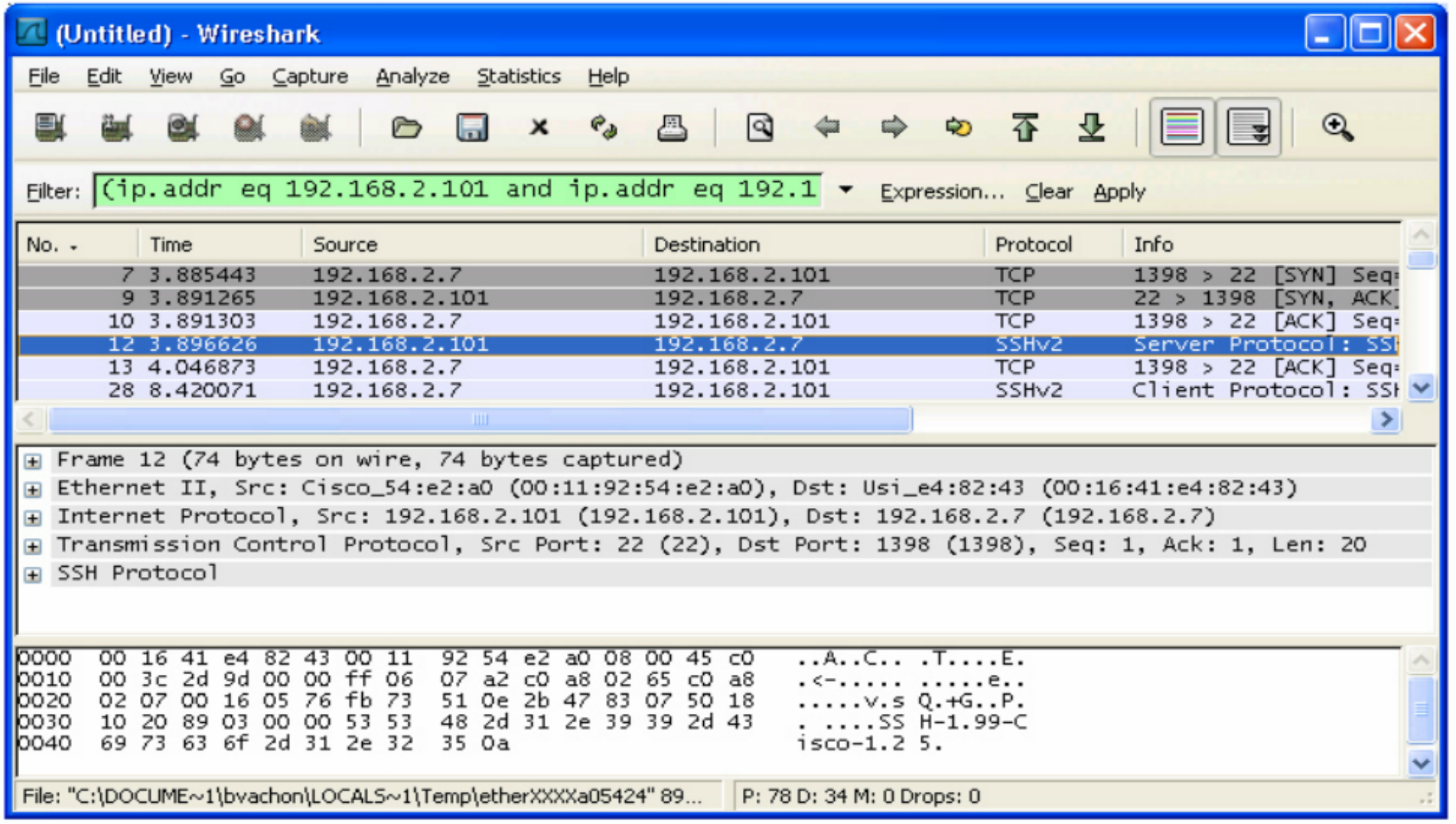
Frame (frame), 66 bytes | P: 60 D: 24 M: 0 Drops: 0

Configuring Secure Remote Access

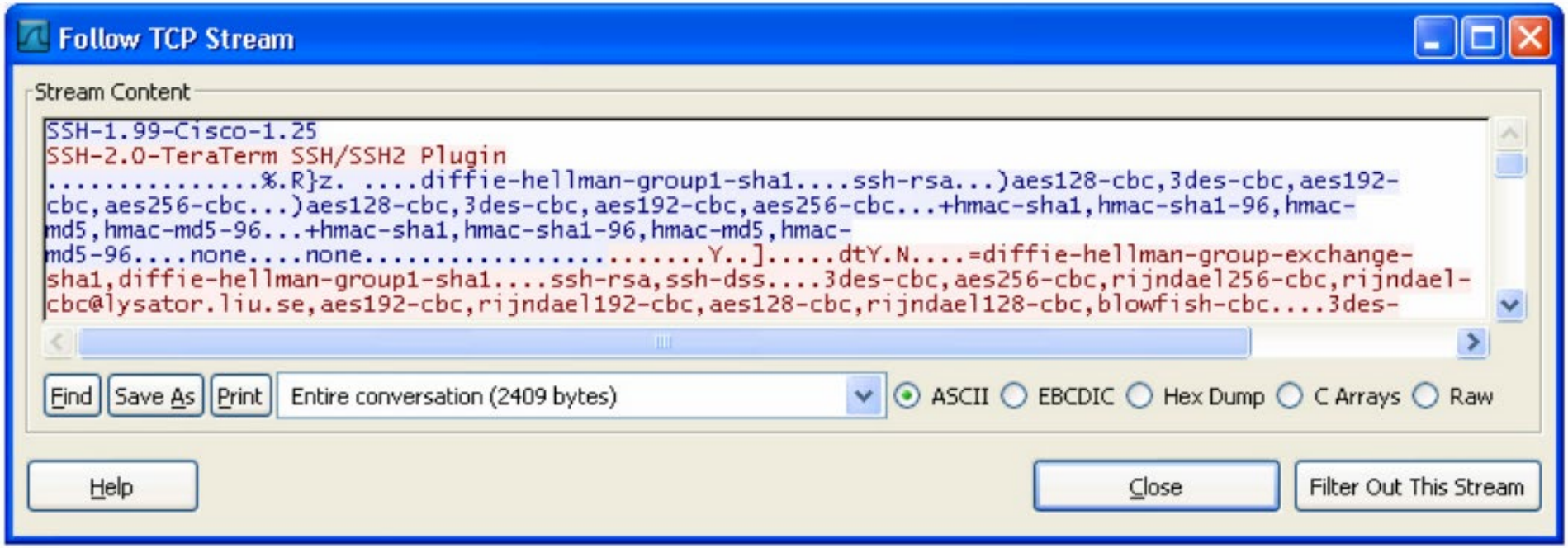
Plaintext Username and Password Captured



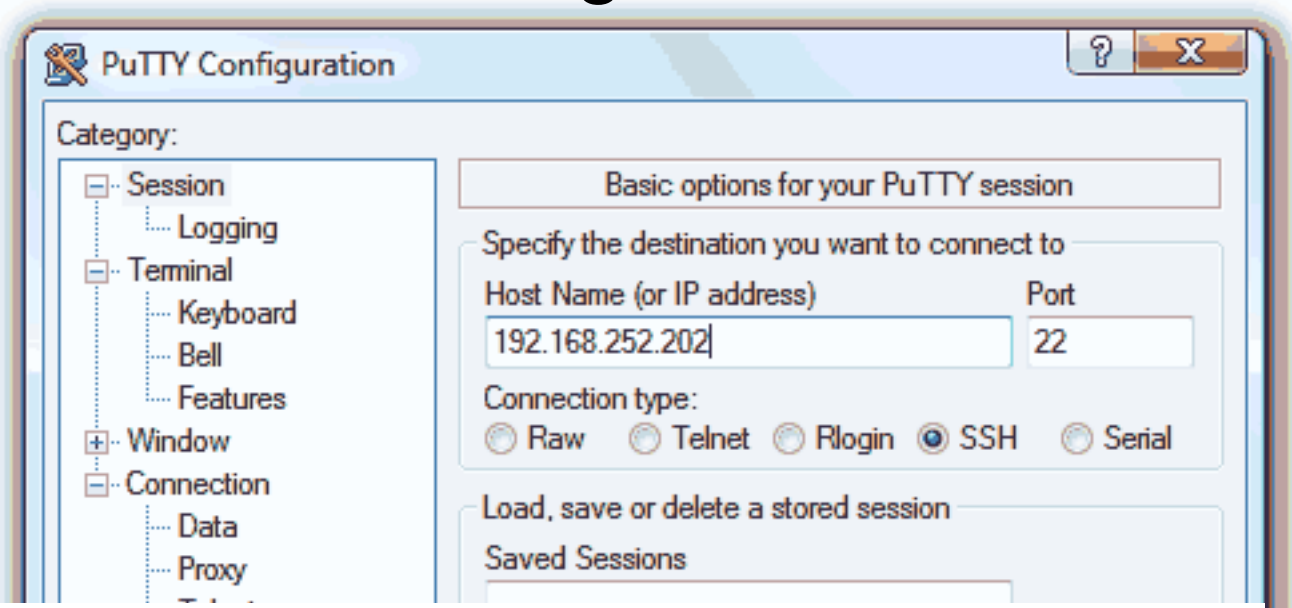
Wireshark SSH Capture



Username and Password Encrypted



Secure Remote Access Using SSH



- 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/Linux-based systems.
  - The IOS software also supports SSH.
- Because of its strong encryption features, SSH should replace Telnet for management connections.
- Note:
  - By default, SSH uses TCP port 22 and Telnet uses TCP port 23.

Secure Remote Access Using SSH

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE, RELEASE SOFTWARE (fc1)

<output omitted>
```

- Not all IOS support SSH.
- A version of the IOS software, including cryptographic (encrypted) features and capabilities, is required to enable SSH on Catalyst 2960 switches.
- Use the **show version** command to verify the IOS version.
  - "K9" indicates that the version supports SSH.
- Verify SSH support using the **show ip ssh** command
  - The command is unrecognized if SSH is not supported.

Steps to Configuring SSH

- A switch must be minimally configured with a unique hostname and the correct network connectivity settings.

1. Verify SSH support using the **`show ip ssh`** command
   - The command is unrecognized if SSH is not supported.
2. Configure the IP domain using the **`ip domain-name`** *`domain-name`* global config command. (The domain name and hostname) are the parameters used in order to name the key. There are other ways to do it.)
3. Generate RSA key pairs using the **`crypto key generate rsa`** global configuration mode command.
   - Cisco recommends a minimum modulus size of 1,024 bits.
   - A longer modulus length is more secure, but it takes longer to generate and to use.
   - Generating an RSA key pair automatically enables SSH.

Steps to Configuring SSH

4. Configure user authentication using the **`username`** and global configuration mode command.
5. Configure the vty lines.
   - Use the **`line vty`** global configuration mode command
   - Enable local login using the **`login local`** line configuration mode command to require local authentication for SSH connections from the local username database.
   - Enable the SSH using the **`transport input ssh`** line configuration mode command.
6. Enable SSH version 2.
   - SSH version 1 has known security flaws.
   - Use the **`ip ssh version 2`** global configuration mode command.

Configuring SSH

```
S1(config)# ip domain-name cislab.vermontstate.edu
```

1. Configure the IP domain using the **ip domain-name** *domain-name* global config command. (The domain name and hostname are the parameters used in order to name the key. There are other ways to do it.)

Configuring SSH

```
S1(config)# ip domain-name cislab.vermontstate.edu
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cislab.vermontstate.edu
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

2. Generate RSA key pairs using the **`crypto key generate rsa`** global configuration mode command.

- Cisco recommends a minimum modulus size of 1,024 bits.
- A longer modulus length is more secure, but it takes longer to generate and to use.
- Generating an RSA key pair automatically enables SSH.

Configuring SSH

```
S1(config)# ip domain-name cislab.vermontstate.edu
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cislab.vermontstate.edu
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 2:59:12.78:  %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)# username admin secret class
S1(config)# line vty 0 15
```

3. Configure user authentication using the **username** in global configuration mode command.

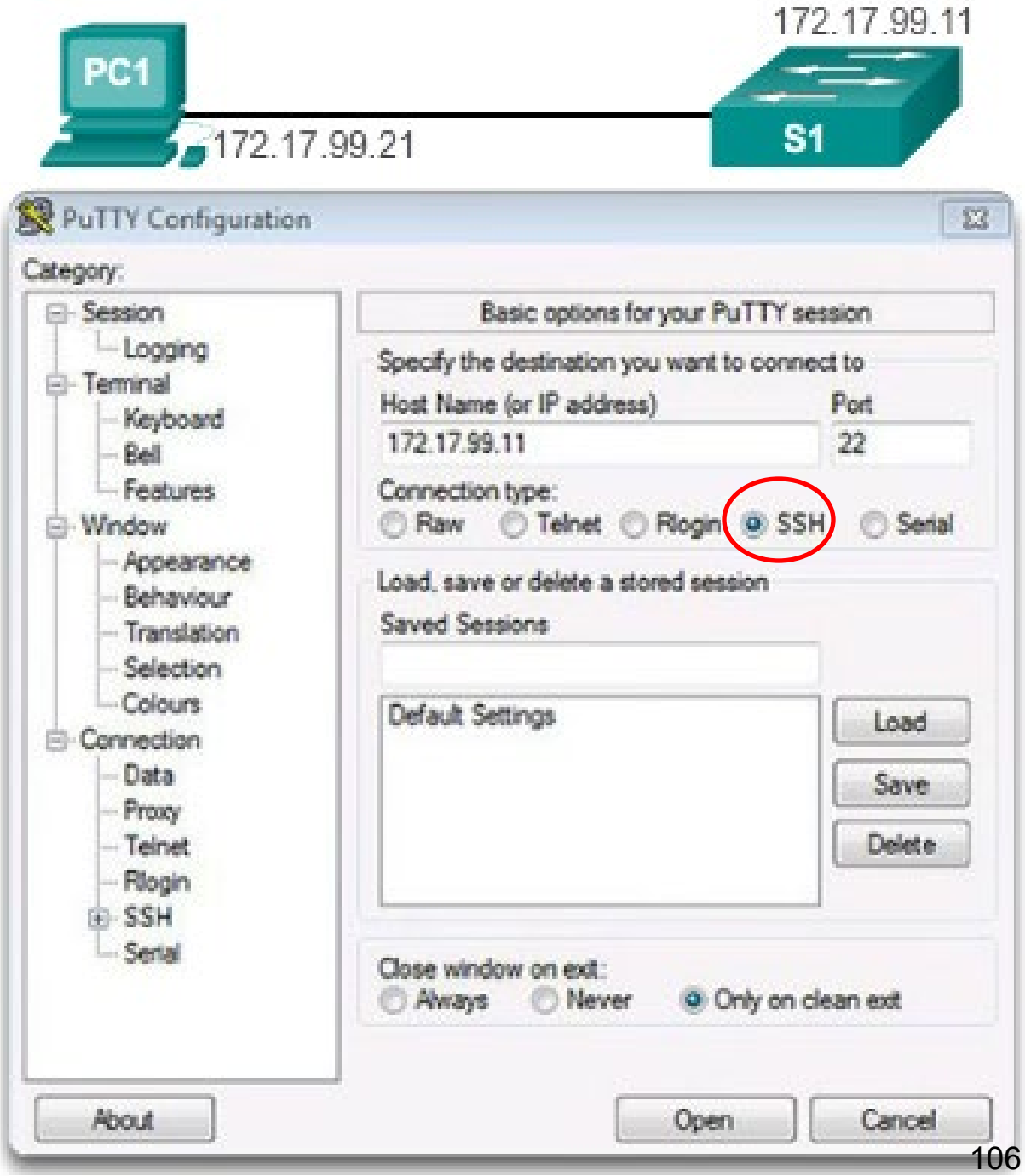
```
S1(config)# ip ssh version 2
S1(config)#
```

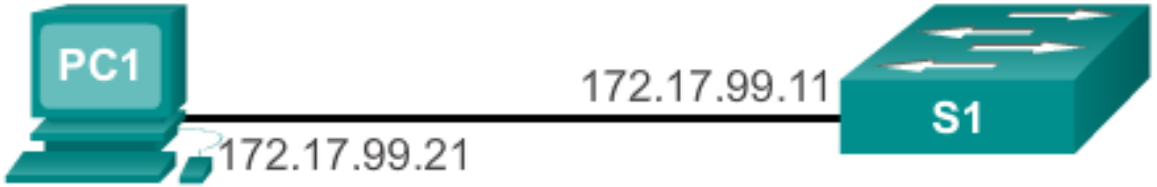
Configuring SSH

```
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 2:59:12.78:  %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)# username admin secret class
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

4. Configure the vty lines.
   - **Enable local login** using the **`login local`** line configuration mode command to require local authentication for SSH connections from the local username database.
   - **Enable the SSH** using the **`transport input ssh`** line configuration mode command.

Verifying SSH Operation

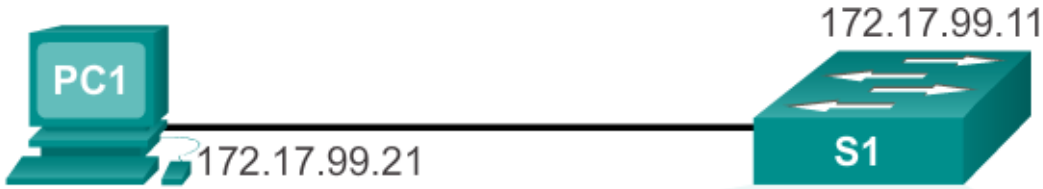




172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Verify SSH Status and Settings




```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac       State         Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

Security Concerns in LANs

Switch Vulnerabilities

- Switches are vulnerable to a variety of attacks including:
  - Password attacks
  - DoS attacks
  - CDP attacks
  - MAC address flooding
  - DHCP attacks

- To mitigate against these attacks:
  - Disable unused ports
  - Disable CDP
  - Configure Port Security
  - Configure DHCP snooping

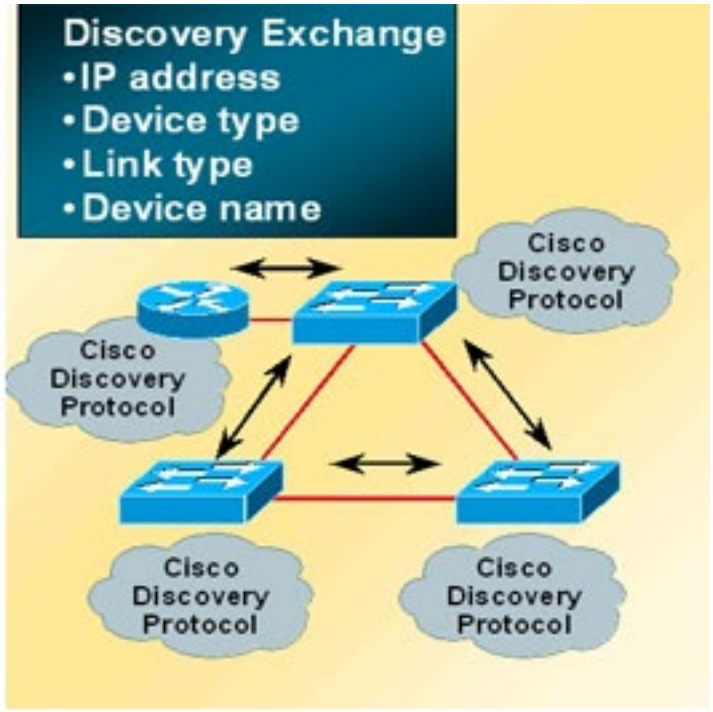
Password Attacks

- How to protect against brute force password attack?
  - Use strong passwords.
    - Change them regularly.
  - Use ACLs to control which devices are able to access vty lines.
  - Use network security tools for audits and penetration testing.
- How to protect against DoS attack?
  - Update to newest IOS version.
- Disable unused ports.

Disable Unused Ports and Assign to an Unused (Garbage) VLAN

```
S1(config)#int range fa0/20 - 24
S1(config-if-range)# switchport access vlan 100
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to
  administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to
  administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to
  administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to
  administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
  administratively down
S1(config-if-range)#
```

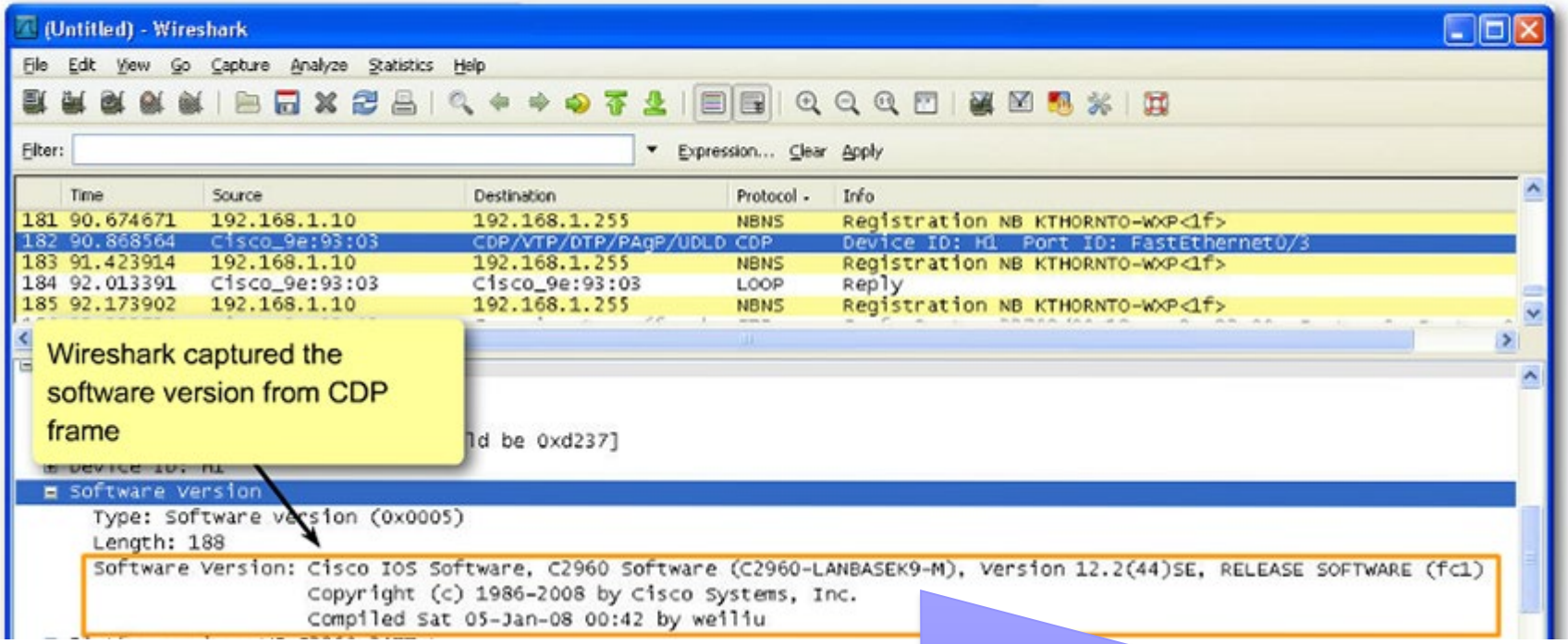
Leveraging the Cisco Discovery Protocol



- The Cisco Discovery Protocol is a Layer 2 Cisco proprietary protocol used to discover other directly connected Cisco devices.
  - It is designed to allow the devices to autoconfigure their connections.
- If an attacker is listening to Cisco Discovery Protocol messages, it could learn important information, such as the device model or the running software version.

Leveraging the Cisco Discovery Protocol

CDP Attacks




```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
12.2(44)SE, RELEASE SOFTWARE (fc1)…
```

- Cisco recommends disabling CDP when it is not in use.

Disabling CDP

```
S1(config)# no cdp run
S1(config)#
```

```
S1(config)# interface range fa0/1 - 24
S1(config-if-range)# no cdp enable
S1(config-if-range)#exit
S1(config)#
```

Unicast Flooding

Unicast

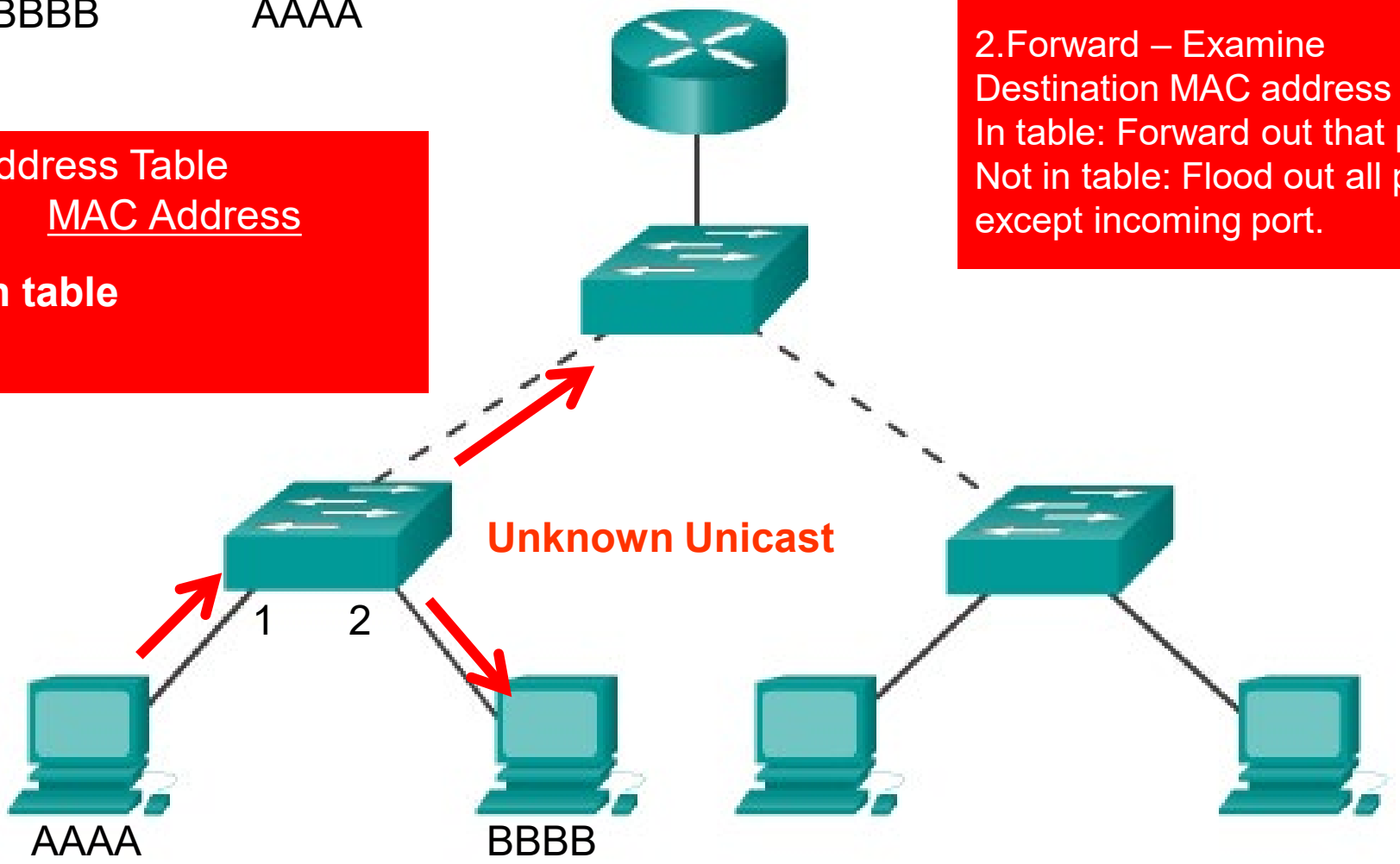
Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)
BBBB	AAAA			

Mac Address Table
1.Learn – Examine Source MAC address
In table: Reset 5 min timer
Not in table: Add Source MAC address and port # to table

2.Forward – Examine Destination MAC address
In table: Forward out that port.
Not in table: Flood out all ports except incoming port.

Mac Address Table

Port	MAC Address
Not in table	



MAC Flood Attack

- If the attack is launched before the beginning of the day, the Content Addressable Memory (CAM) table would be full as the majority of devices are powered on.
- If the initial, malicious flood of invalid CAM table entries is a one-time event:
  - Can generate 155,000 MAC entries per minute
  - “Typical” switch can store 4,000 to 8,000 MAC entries
  - Eventually, the switch will age out older, invalid CAM table entries
  - New, legitimate devices will be able to create an entry in the CAM
  - Traffic flooding will cease

Unicast Flooding

Unicast

Destination Address (MAC)	Source Address (MAC)	Type (Data?)	DATA (IP, etc.)	FCS (Errors?)
BBBB	AAAA			

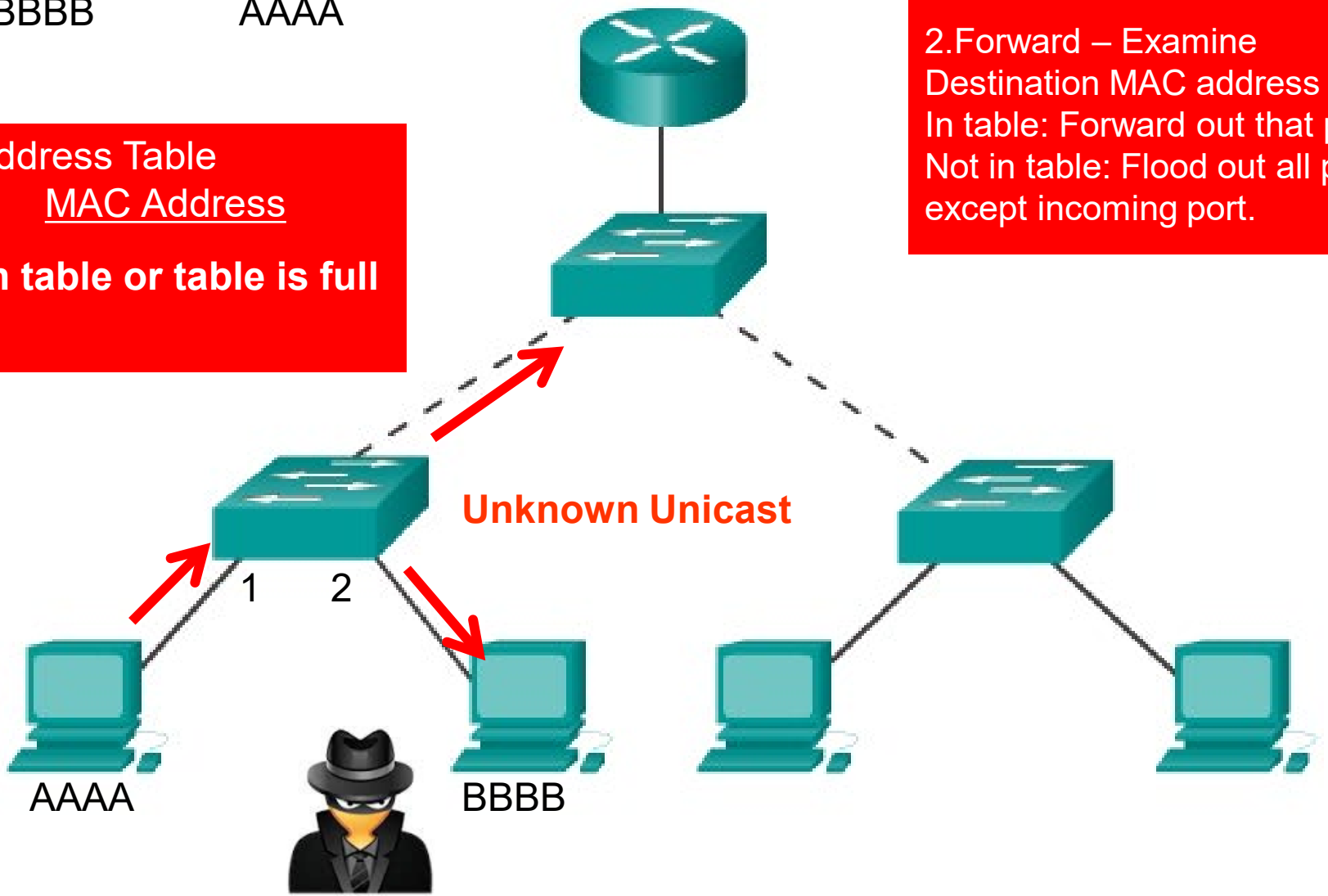
Mac Address Table
1.Learn – Examine Source MAC address
In table: Reset 5 min timer
Not in table: Add Source MAC address and port # to table

2.Forward – Examine Destination MAC address
In table: Forward out that port.
Not in table: Flood out all ports except incoming port.

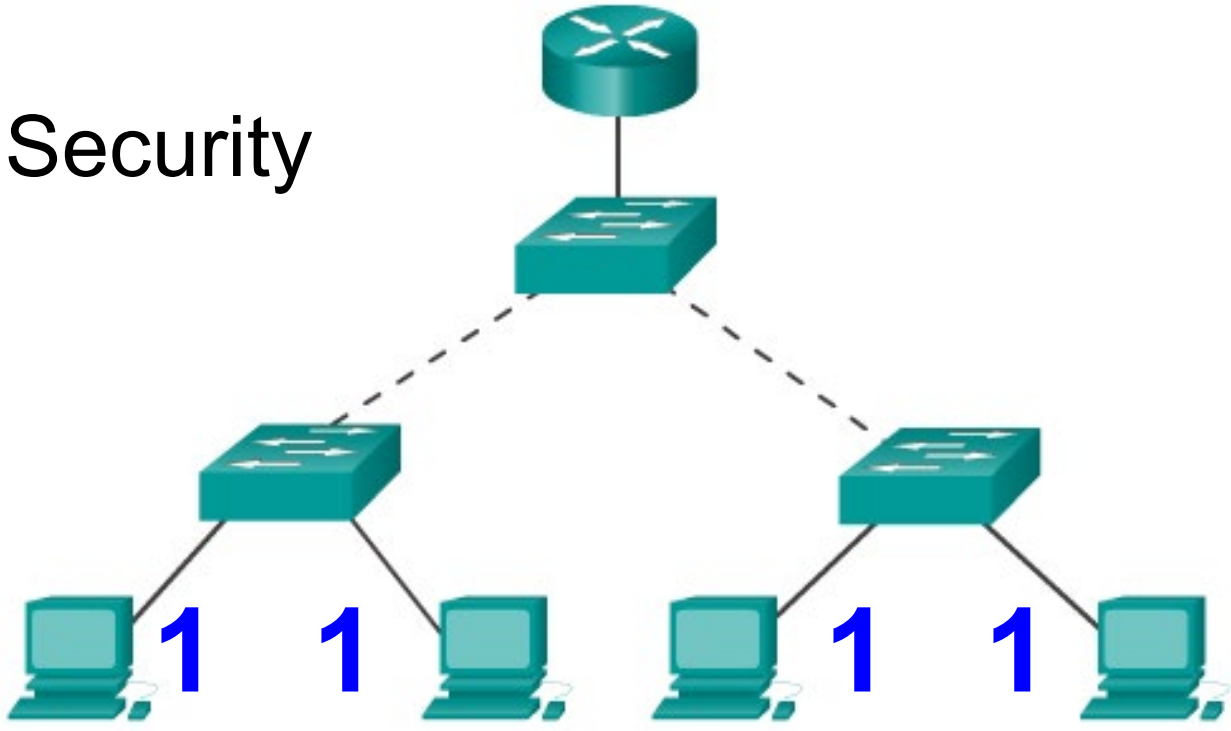
Mac Address Table

Port	MAC Address

Not in table or table is full



Configure Port Security



- Port security allows an administrator to limit the number of MAC addresses learned on a port.
  - If this is exceeded, a switch action can be configured.
- Configure each access port to accept 1 MAC address only or a small group of MAC addresses.
  - Frames from any other MAC addresses are not forwarded.
  - By default, the port will shut down if the wrong device connects.
    - It has to be brought up again manually.

Configuring Port Security

- Use the **`switchport port-security`** interface command to enable port security on a port.

```
Switch(config-if)#
switchport port-security [max value] [violation {protect |
restrict | shutdown}] [mac-address mac-address [sticky]]
[aging time value]
```

- It is used to:
  - Set a maximum number of MAC addresses.
  - Define violation actions.
  - MAC address(es) can be learned dynamically, entered manually, or learned and retained dynamically.
  - Set the aging time for dynamic and static secure address entries.
- To verify port security status: **`show port-security`**

Port Security: Secure MAC Addresses

- The switch supports these types of **secure MAC addresses**:
- **Static**
  - Configured using **`switchport port-security mac-address`** *`mac-address`*
  - Stored in the address table
  - Added to running configuration.
- **Dynamic**
  - These are dynamically configured
  - Stored **only** in the address table
  - Removed when the switch restarts
- ***Sticky***
  - These are dynamically configured
  - Stored in the address table
  - Added to the running configuration.
  - If running-config saved to startup-config, when the switch restarts, the interface does not need to dynamically reconfigure them.
  - **Note**: *When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. The interface adds all the sticky secure MAC addresses to the running configuration.*

Port Security: Steps

To configure port security, follow the steps listed in the table.

Step	Description
1.	
2.	
3.	
4.	

Port Security Defaults

Feature	Default setting
Port Security	Disabled on a port
Maximum # of Secure MAC Addresses	1
Violation	**Shutdown** • The port shuts down when the maximum number of secure MAC addresses is exceeded, and an SNMP trap notification is sent.
Sticky Address Learning	Disabled

- Secure MAC addresses can be configured as follows:
  - Dynamically (learned but not retained after a reboot)
  - Statically (prone to errors)
  - Sticky (learned dynamically and retained)

Dynamic Secure MAC address

- Learned dynamically
  - `S1(config-if)# switchport mode access`
  - `S1(config-if)# switchport port-security`
- By default, only 1 address is learned.
  - Put in MAC address table
  - Not shown in running configuration
- It is not saved or in the configuration when switch restarts.

Static Secure MAC address

- Static secure MAC address is manually configured in interface config mode

```
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security mac-address
000c.7259.0a63
```

- MAC address is stored in MAC address table
- Shows in the running configuration
- Can be saved with the configuration.

Sticky Secure MAC address

- Dynamically learned and can be retained.
  - `S1(config-if)# switchport mode access`
  - `S1(config-if)# switchport port-security mac-address sticky`

- You can choose how many can be learned (default 1).
- Added to the running configuration
- Saved only if you save running configuration.
- Note:
  - When you enter this command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.
  - The interface adds all the sticky secure MAC addresses to the running configuration.

`interface FastEthernet0/2`

`switchport mode access`

- Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.

`switchport port-security`

- Enables port security on the interface

`switchport port-security maximum 6`

- (Optional) Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 132; the default is 1.

`switchport port-security aging time 5`

- Learned addresses are not aged out by default but can be with this command. Value from 1 to 1024 in minutes.

`switchport port-security mac-address 0000.0000.000b`

- (Optional) Enter a static secure MAC address for the interface, repeating the command as many times as necessary. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.

`switchport port-security mac-address sticky`

- (Optional) Enable stick learning on the interface.

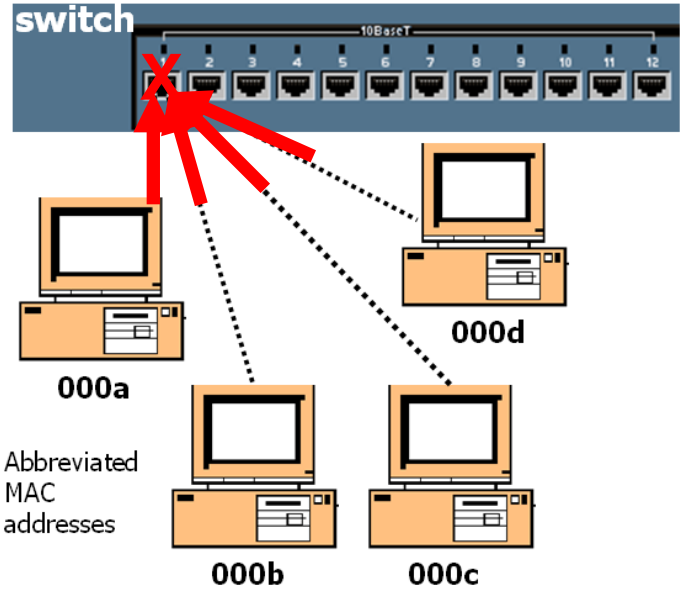
`switchport port-security violation shutdown`

- (Optional) Set the violation mode, the action to be taken when a security violation is detected. (Next)

NOTE: **`switchport host`** command will disable channeling, and enable access/portfast

```
Switch(config-if)# switchport host
  switchport mode will be set to access
  spanning-tree portfast will be enabled
  channel group will be disabled
```

Port Security: Static Addresses

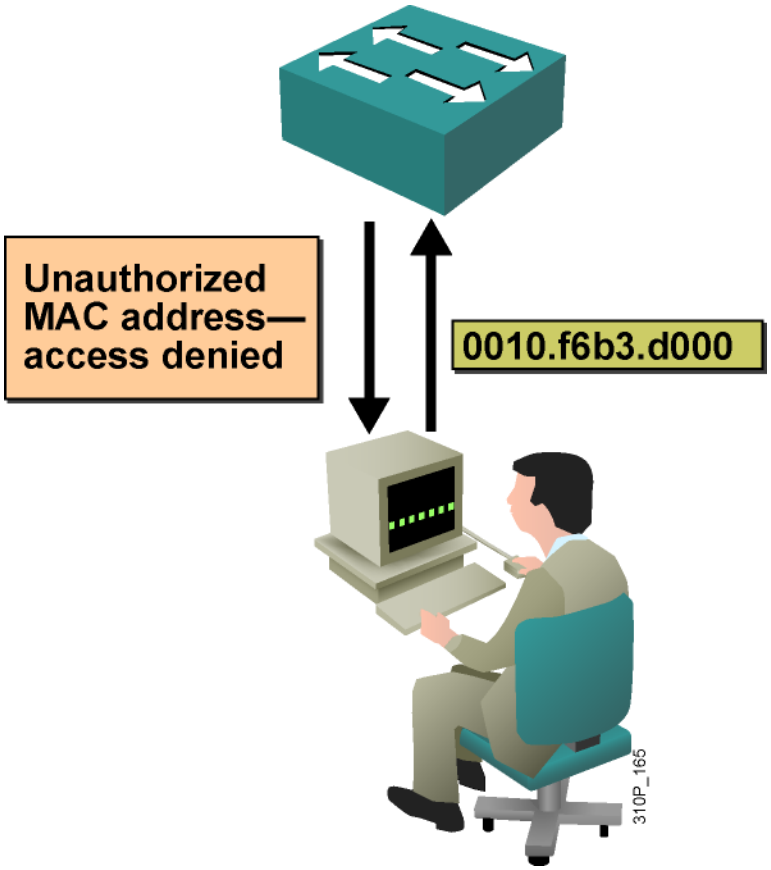



```
Switch(config)# interface fa 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 3
Switch(config-if)# switchport port-security mac-address 0000.0000.000a
Switch(config-if)# switchport port-security mac-address 0000.0000.000b
Switch(config-if)# switchport port-security mac-address 0000.0000.000c
```

- Restricts input to an interface by limiting and identifying MAC addresses of the stations **allowed to access the port**.
- The port does not forward packets with source addresses outside the group of defined addresses.

Port Security: Violation

- Station attempting to access the port is different from any of the identified secure MAC addresses, a **security violation occurs**.

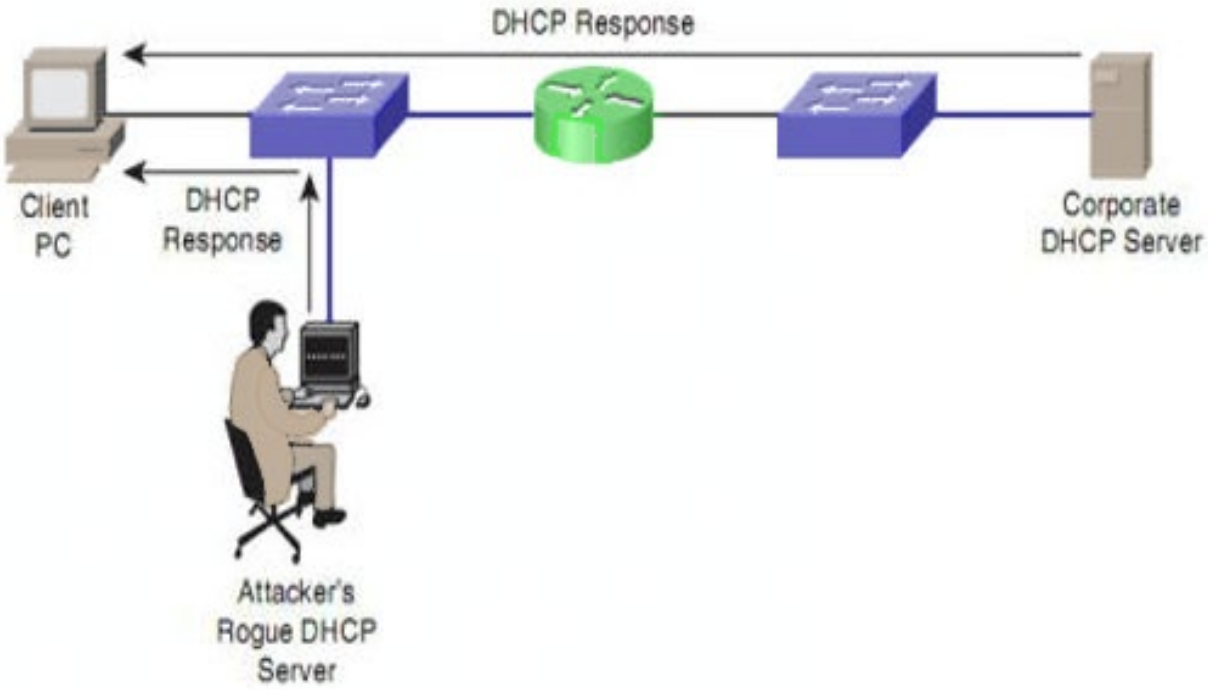


Port Security: Violation

```
Switch(config-if)#switchport port-security violation
{protect | restrict | shutdown}
```

- By default, if the maximum number of connections is achieved and a new MAC address attempts to access the port, the switch must take one of the following actions:
- **Protect:** Frames from the nonallowed address are dropped, but there is no log of the violation.
- **Restrict:** Frames from the nonallowed address are dropped, a log message is created and Simple Network Management Protocol (SNMP) trap sent.
- **Shut down:** If any frames are seen from a nonallowed address, the interface is errdisabled, a log entry is made, SNMP trap sent and manual intervention (no shutdown) or errdisable recovery must be used to make the interface usable.

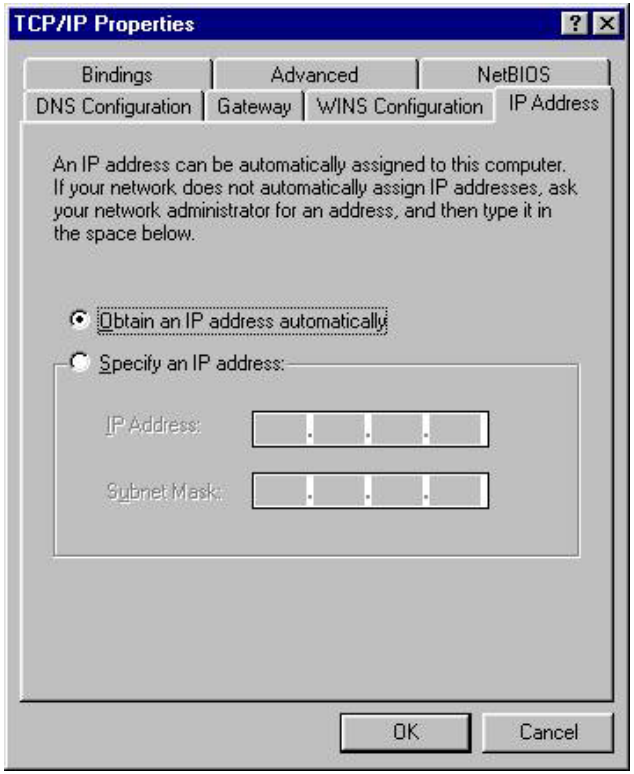
DHCP Attacks

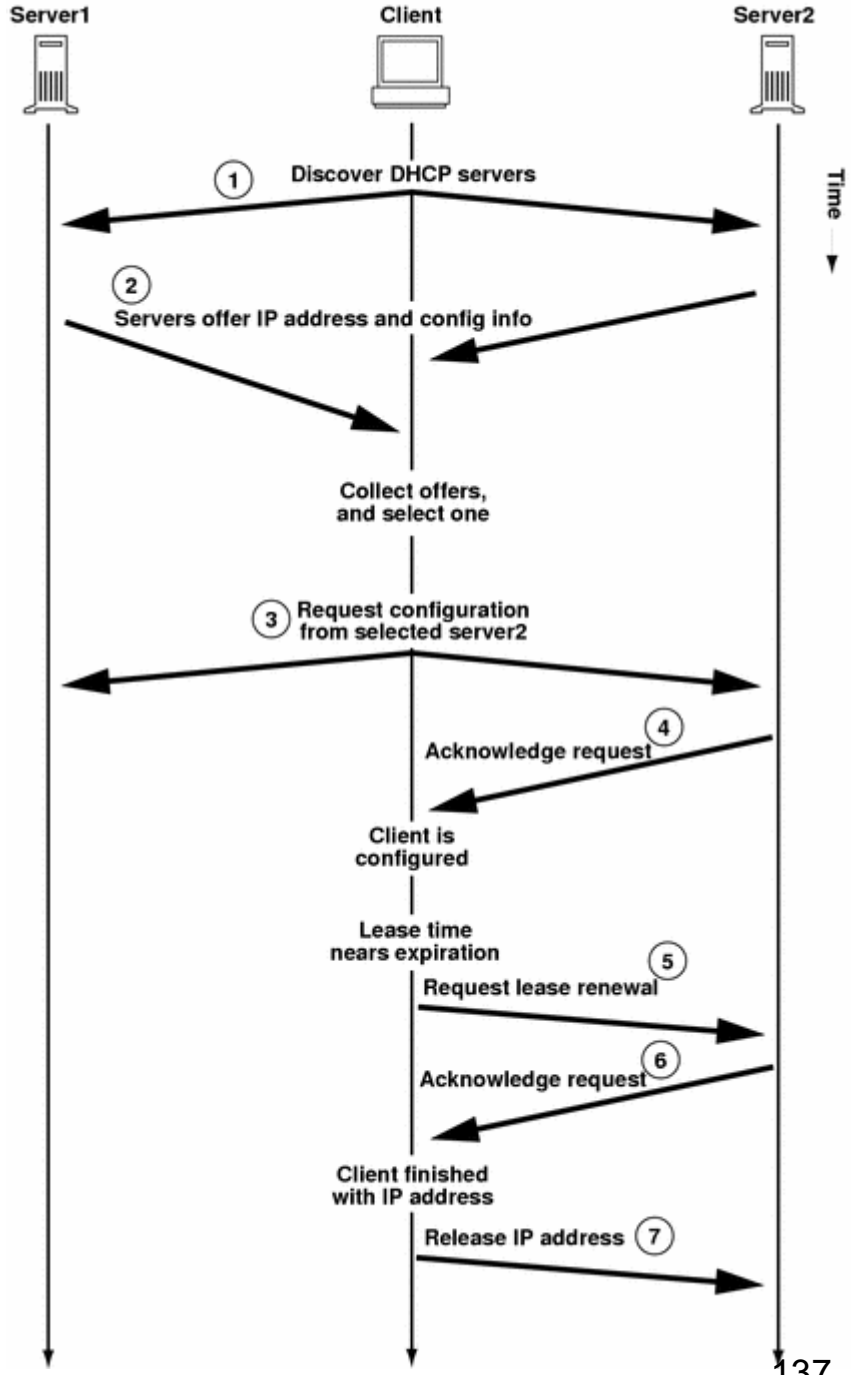


- DHCP is a network protocol used to automatically assign IP information.

- Two types of DHCP attacks are:
  - **DHCP spoofing**: A fake DHCP server is placed in the network to issue DHCP addresses to clients.
  - **DHCP starvation**: DHCP starvation is often used before a DHCP spoofing attack to deny service to the legitimate DHCP server.

DHCP Review


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

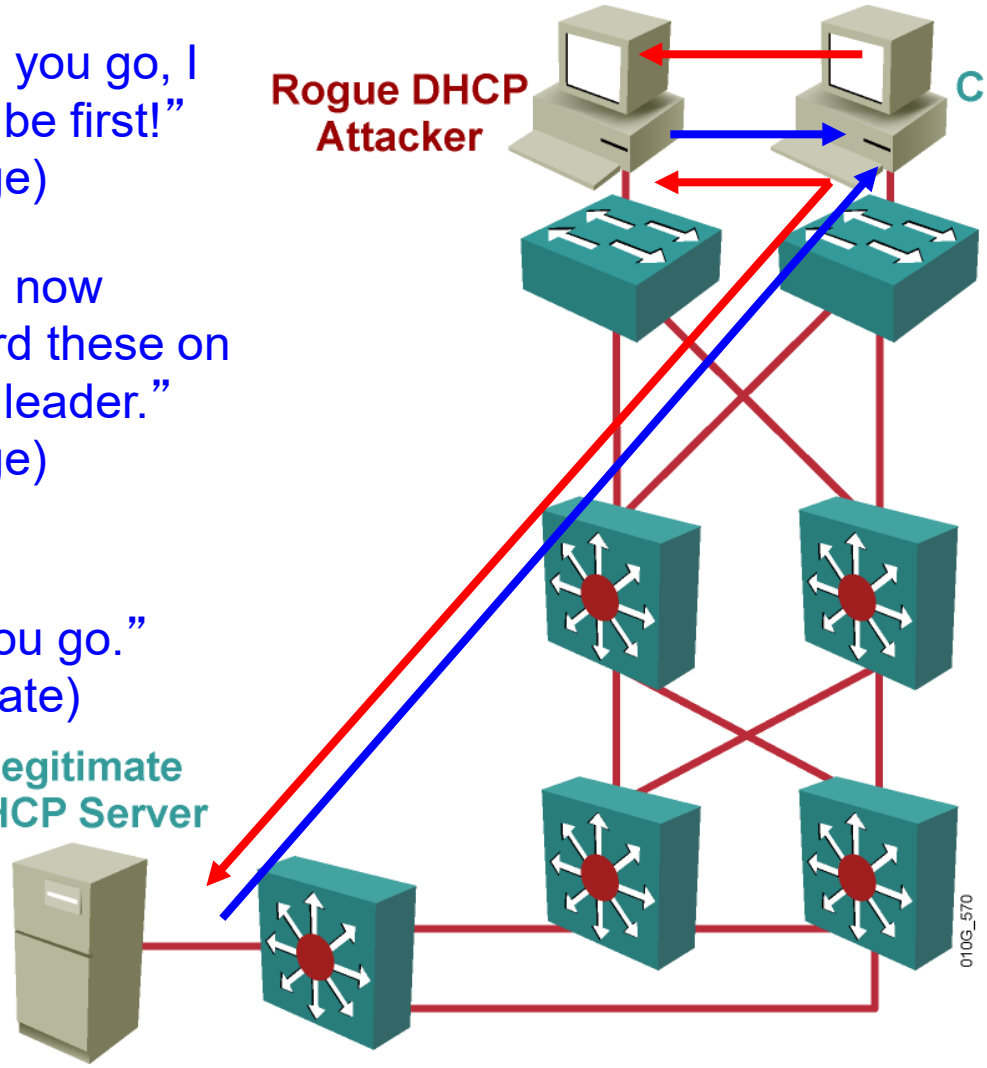

Server1
Client
Server2
Time
1 Discover DHCP servers
2 Servers offer IP address and config info
Collect offers, and select one
3 Request configuration from selected server2
4 Acknowledge request
Client is configured
Lease time nears expiration
5 Request lease renewal
6 Acknowledge request
Client finished with IP address
Release IP address 7

DHCP Spoof Attacks

"Here you go, I might be first!" (Rouge)

"I can now forward these on to my leader." (Rouge)

"Here you go." (Legitimate)



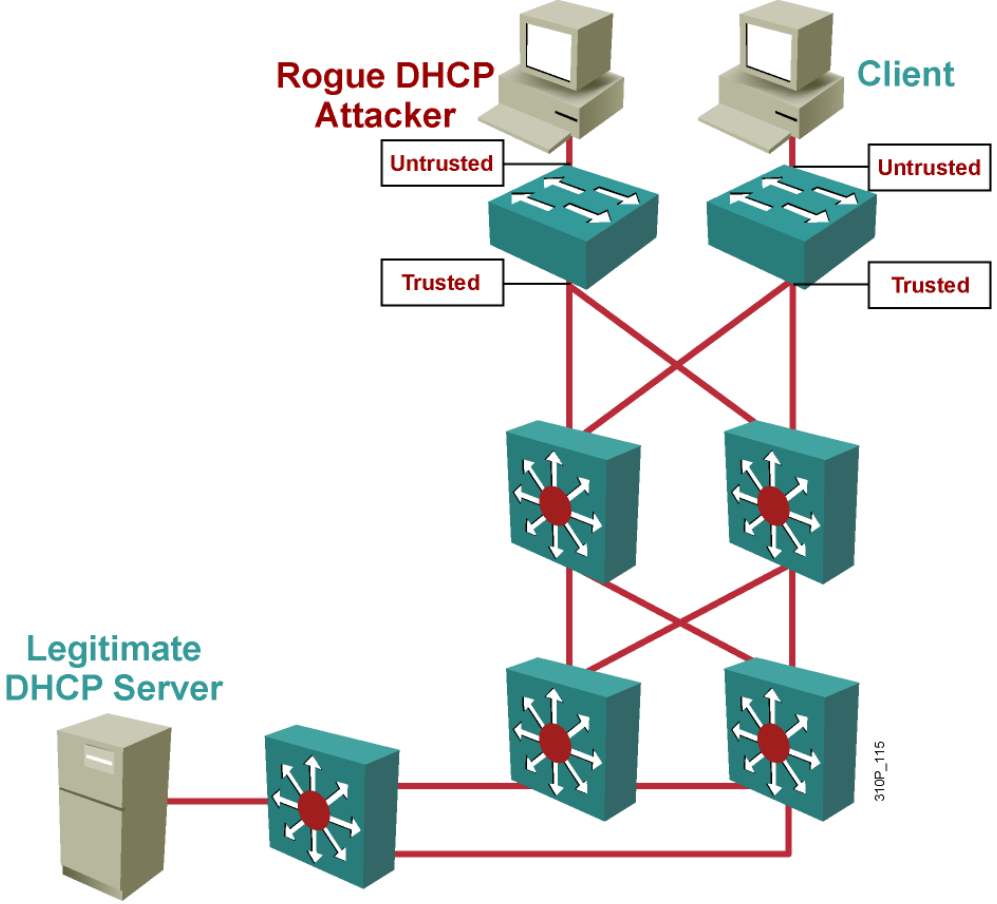
"I need an IP address/mask, default gateway, and DNS server."

"Got it, thanks!"

"Already got the info."

All default gateway frames and DNS requests sent to Rogue.

Solution: Configure DHCP Snooping

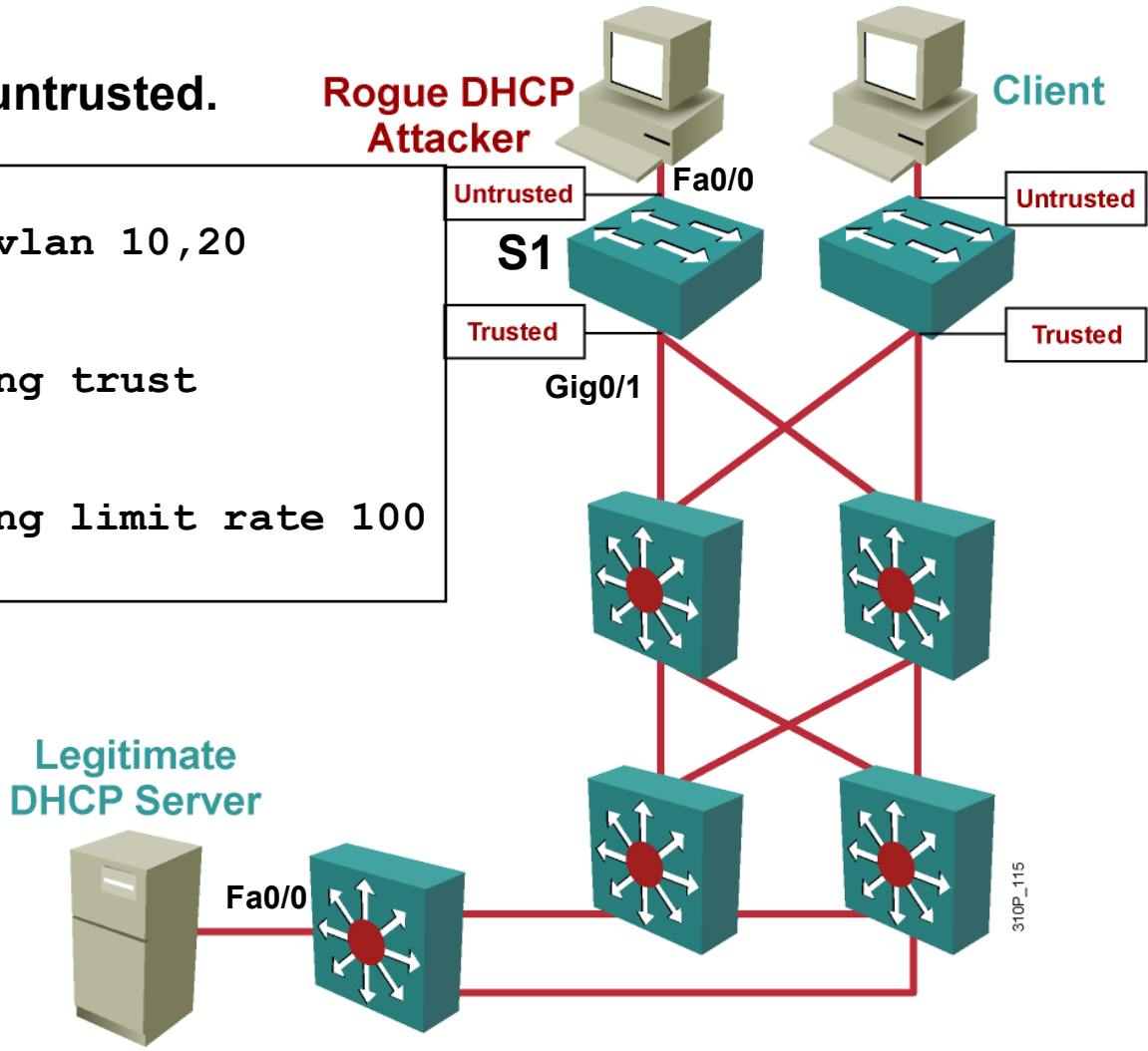


- DHCP snooping is a Cisco Catalyst feature that determines which switch ports can respond to DHCP requests.
- Ports are identified as trusted and untrusted.
  - **Trusted ports**: Host a DHCP server or can be an uplink toward the DHCP server and can source all DHCP messages, including DHCP offer and DHCP acknowledgement packets
  - **Untrusted ports**: Can source requests only.

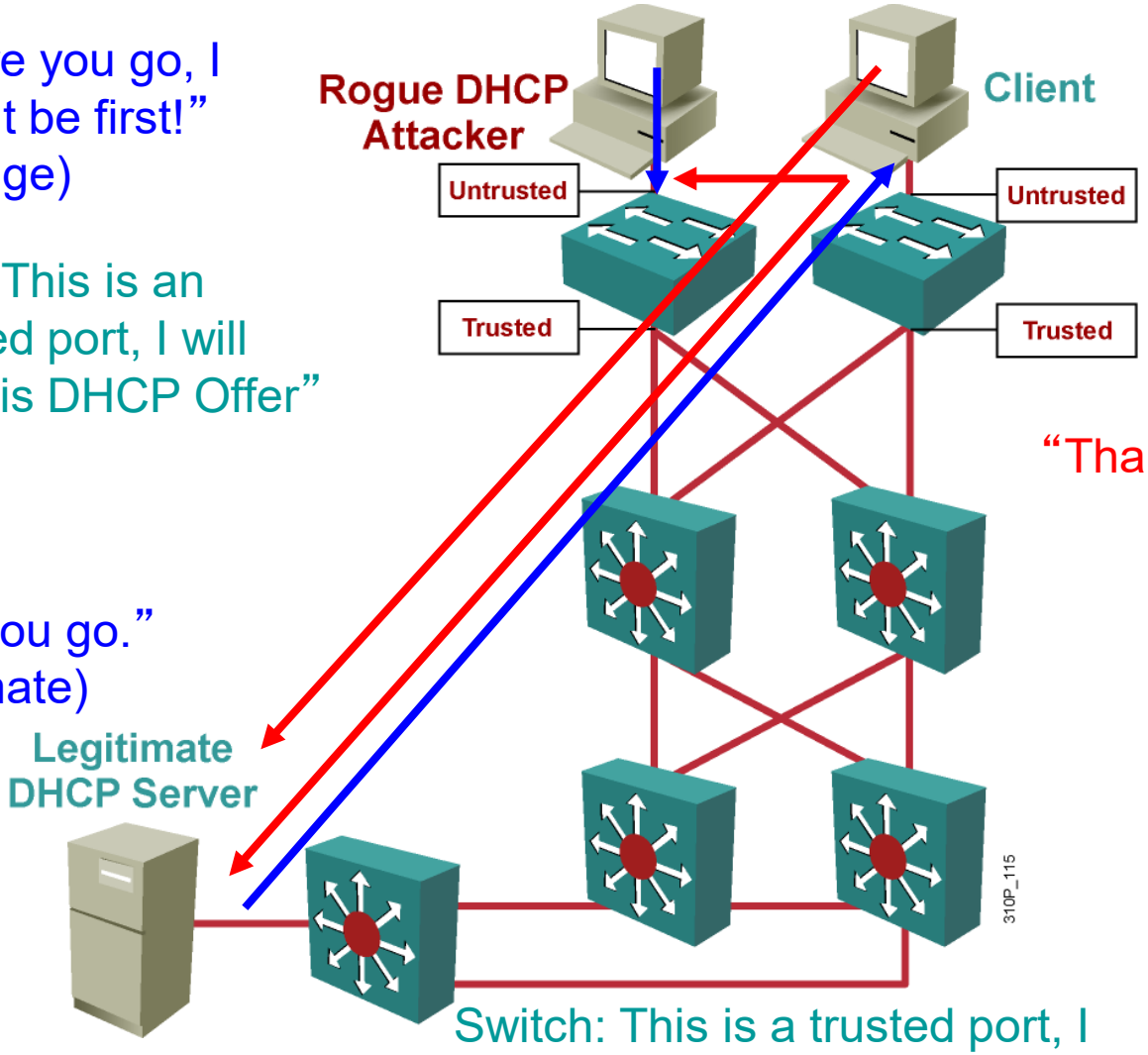
DHCP Snooping

By default all interfaces are untrusted.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20

S1(config)# interface gig 0/1
S1(config-if)# ip dhcp snooping trust

S1(config)# interface fa 0/0
S1(config-if)# ip dhcp snooping limit rate 100
```



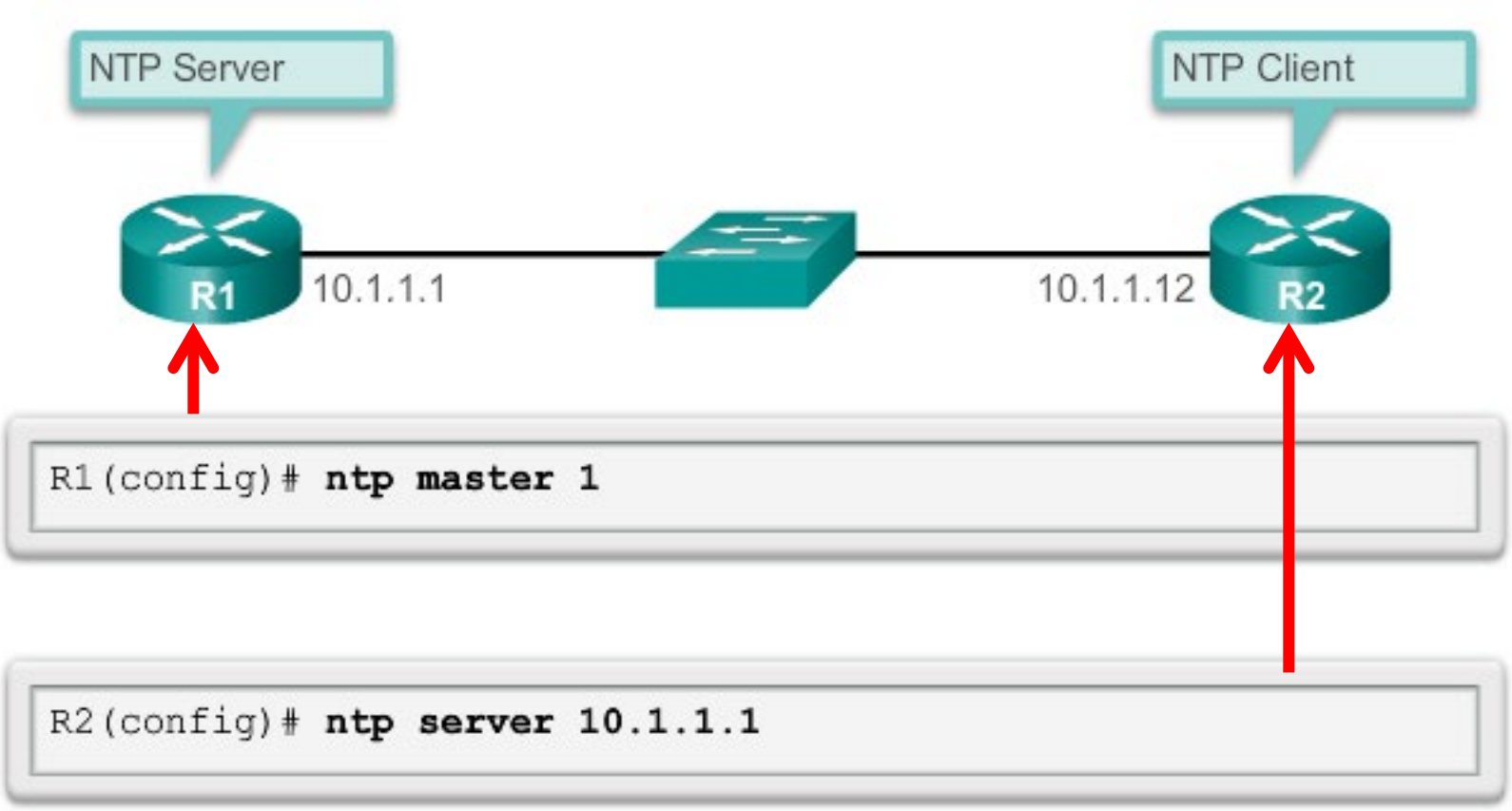
DHCP Snooping



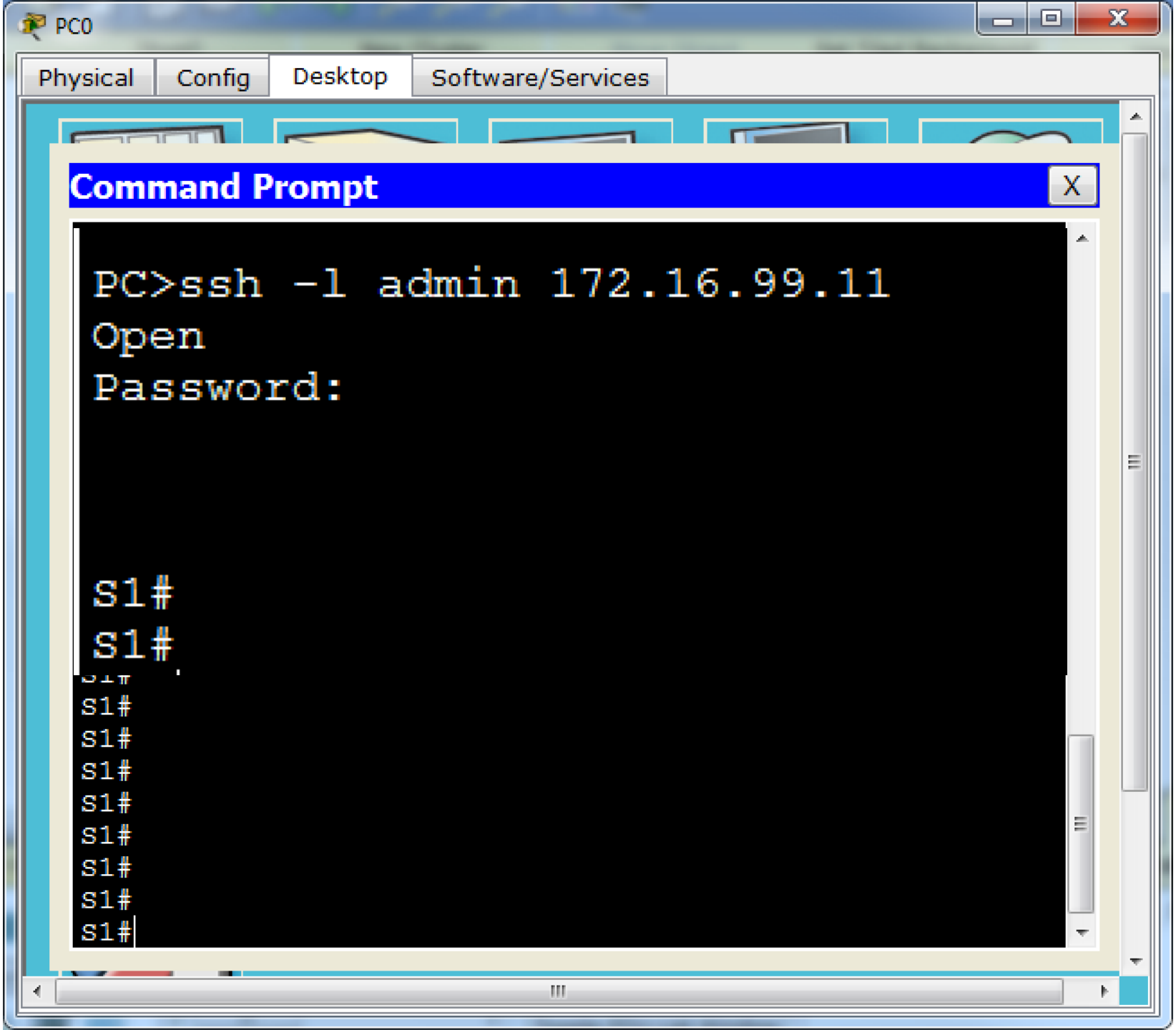
Network Time Protocol (NTP)

- Having the correct time within networks is important.
- Network Time Protocol (NTP) is a protocol that is used to synchronize the clocks of computer systems over the network
  - NTP allows network devices to synchronize their time settings with an NTP server.
- Some administrator prefer to maintain their own time source for increased security.
  - However, public time sources are available on the Internet for general use.
- A network device can be configured as either an NTP server or an NTP client.

Network Time Protocol (NTP) (cont.)



- R2 is configured as a NTP client, receiving time updates from the server, R1.


PC0
Physical
Config
Desktop
Software/Services
Command Prompt
X
PC>ssh -l admin 172.16.99.11
Open
Password:
S1#
S1#
S1#
S1#
S1#
S1#
S1#
S1#
S1#
S1#
S1#

Managing Switch Configurations

TO CLEAR A SWITCH

- ALWAYS DO THE FOLLOWING TO CLEAR A SWITCH!!

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]

S1# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
  Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S1# reload
Proceed with reload? [confirm]
```