ETHERNET

COMPUTER NETWORKS

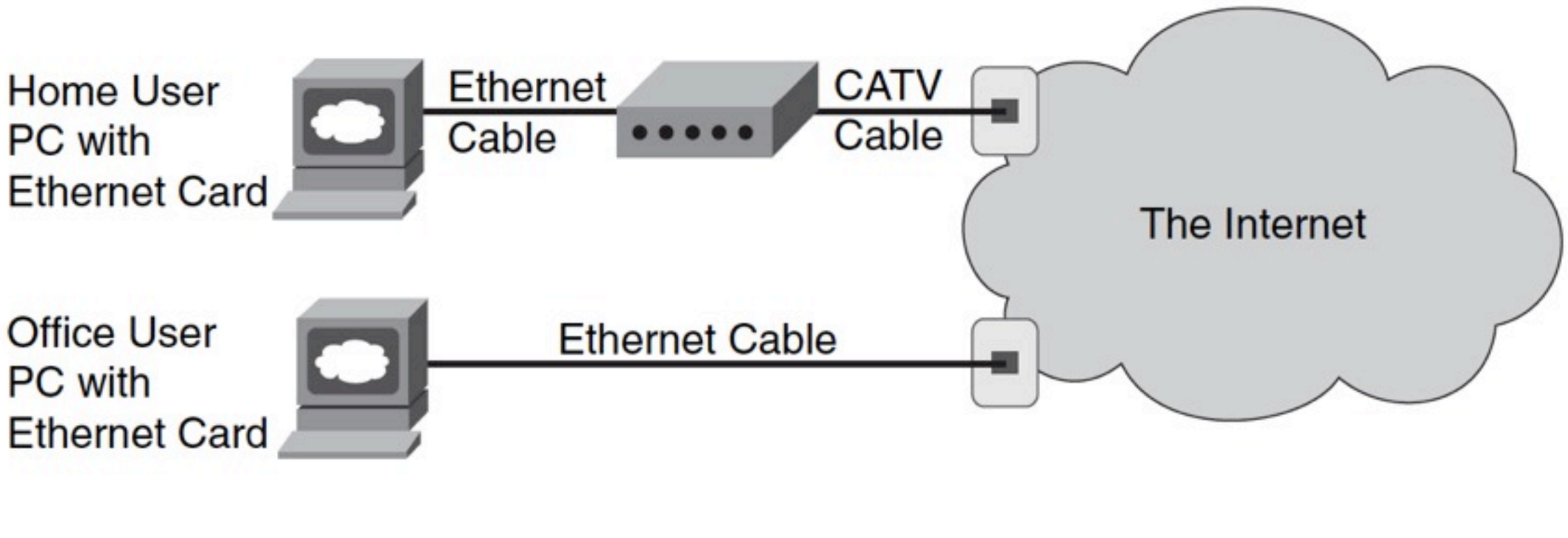
Computers have been networked for over 40 years.

The INTERNET is a collection of networks running a common set of protocols (TCP/IP).

These protocols have become the de-facto standard for networking computers together.

There are many computer networking protocols,we will look at the current state of the art.

The Home/Office user view of the INTERNET



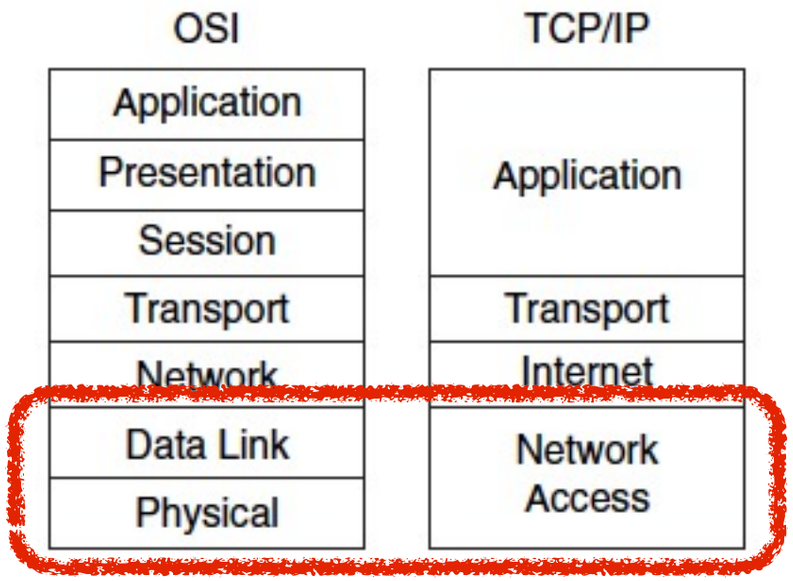
This is the high level view of how you connect to the internet.

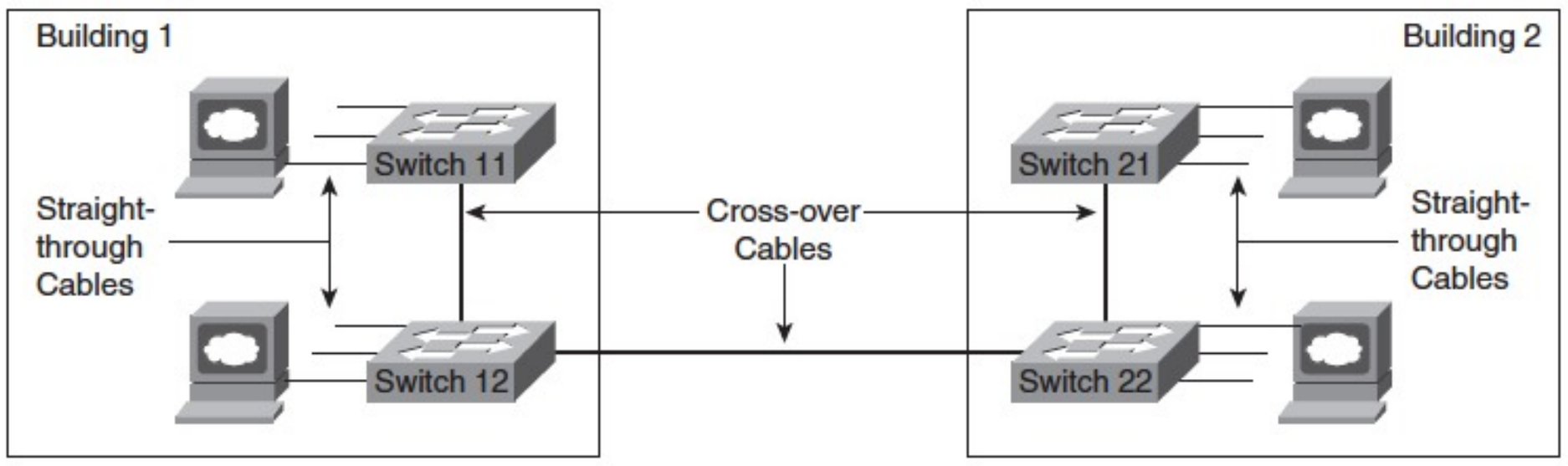
All packet networks are shown as a cloud.

Data goes in and magically pops out the other side.

ETHERNET

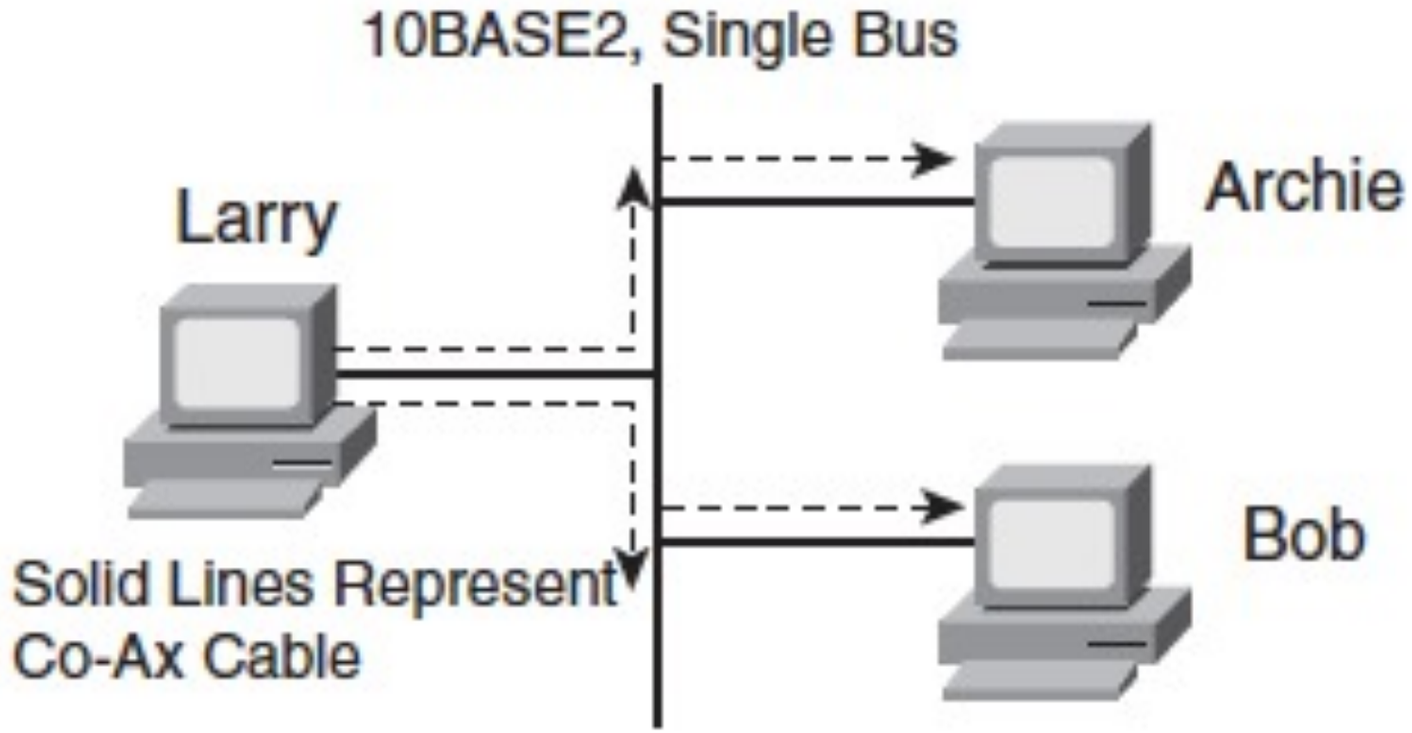
is **Layer 1 and Layer 2 in OSI** and **Layer 1 in TCP/IP Stack**

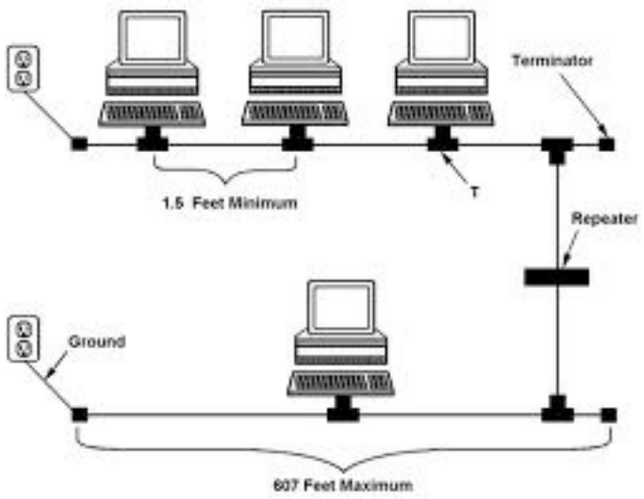




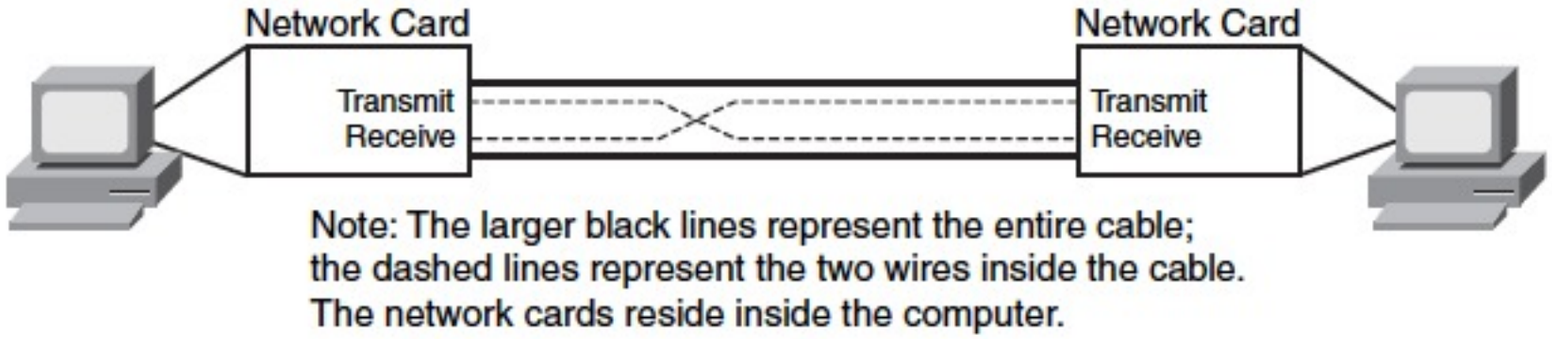
The first version of ETHERNET

10Base2





10 Base T



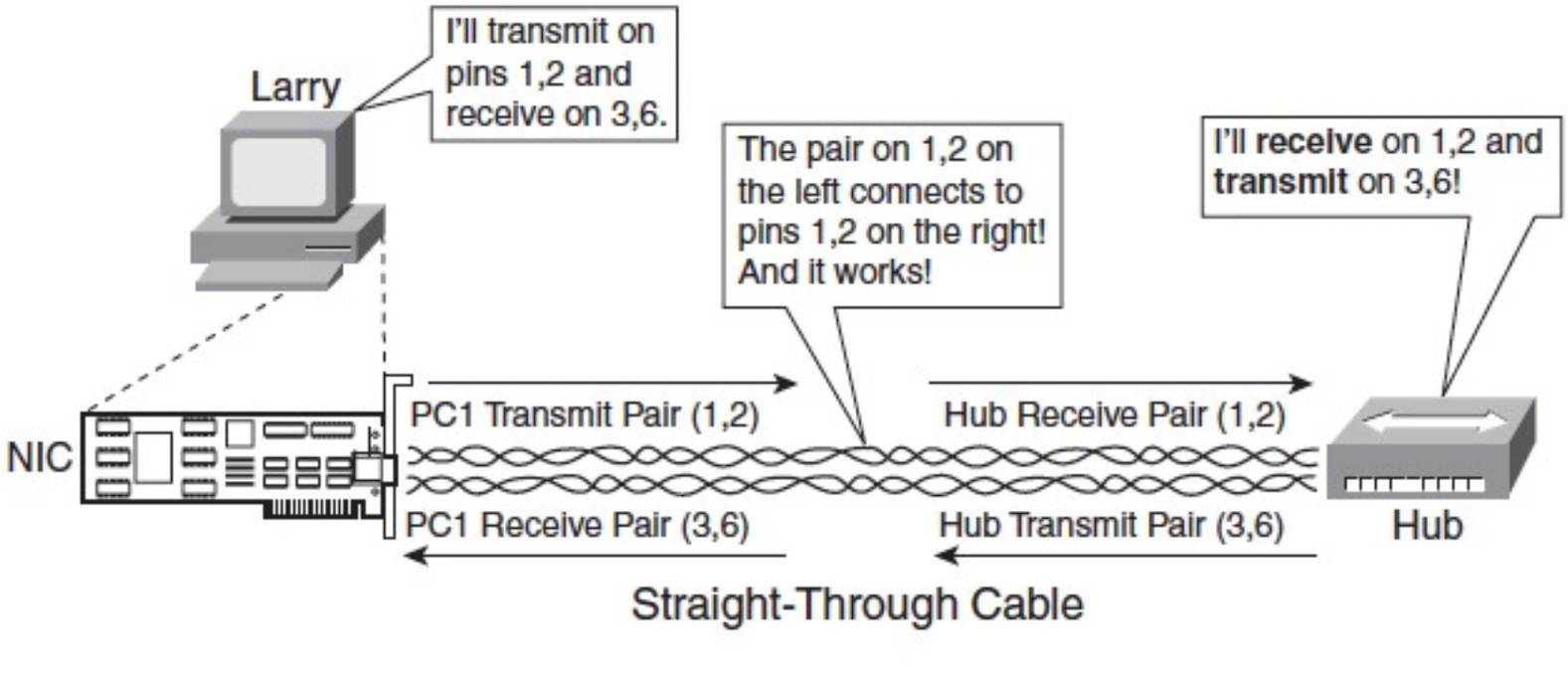
Note: The larger black lines represent the entire cable; the dashed lines represent the two wires inside the cable. The network cards reside inside the computer.

First part of the system to be invented in the late 60's

Layer 1 the wires and the signals. The protocols at this layer dictate the signalling and the electrical specifications for the wire that will be used to carry the signal.

In Ethernet the wires will have a differential signal representing digital information (bits) and will be coded using a line coding.
Ex; Manchester encoding for 10BaseT

10 Base T Cabling

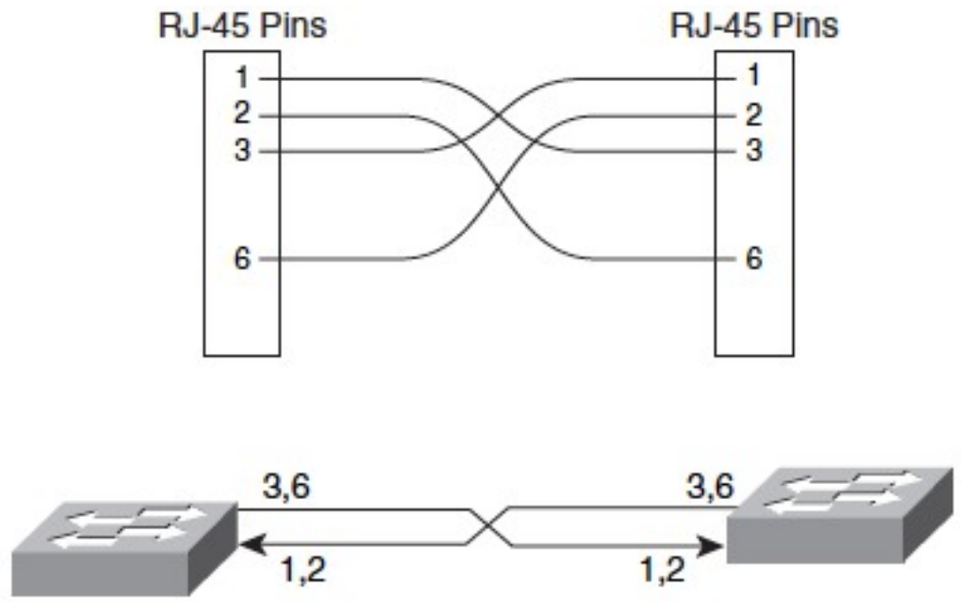


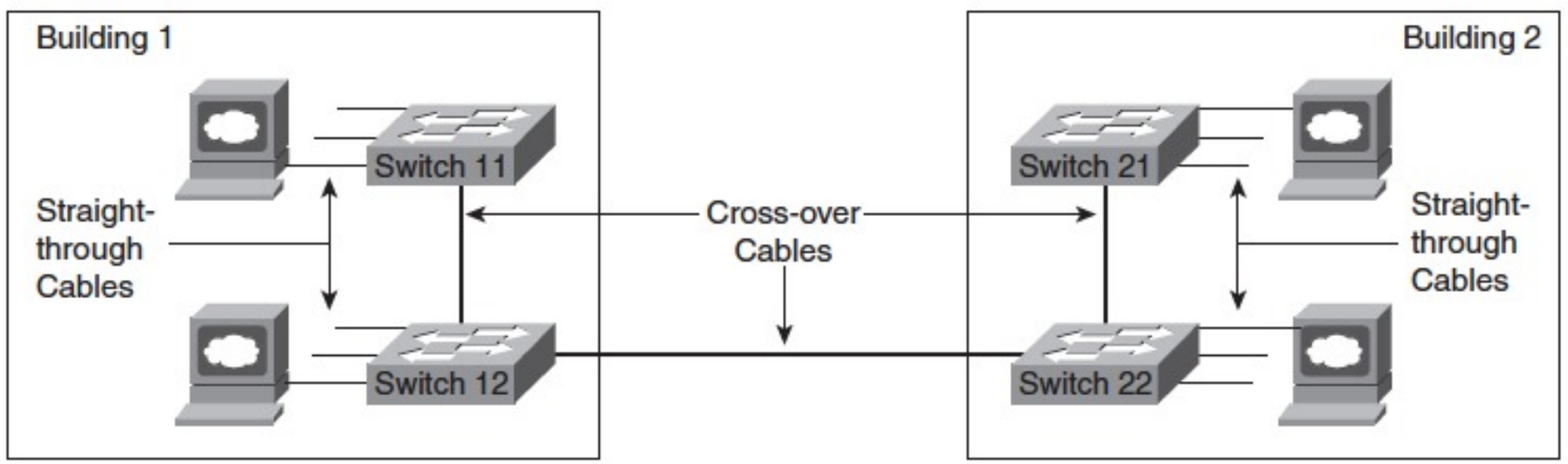
On a HUB or SWITCH the RX pins are 1,2

On a PC or a Router the RX pins are 3,6

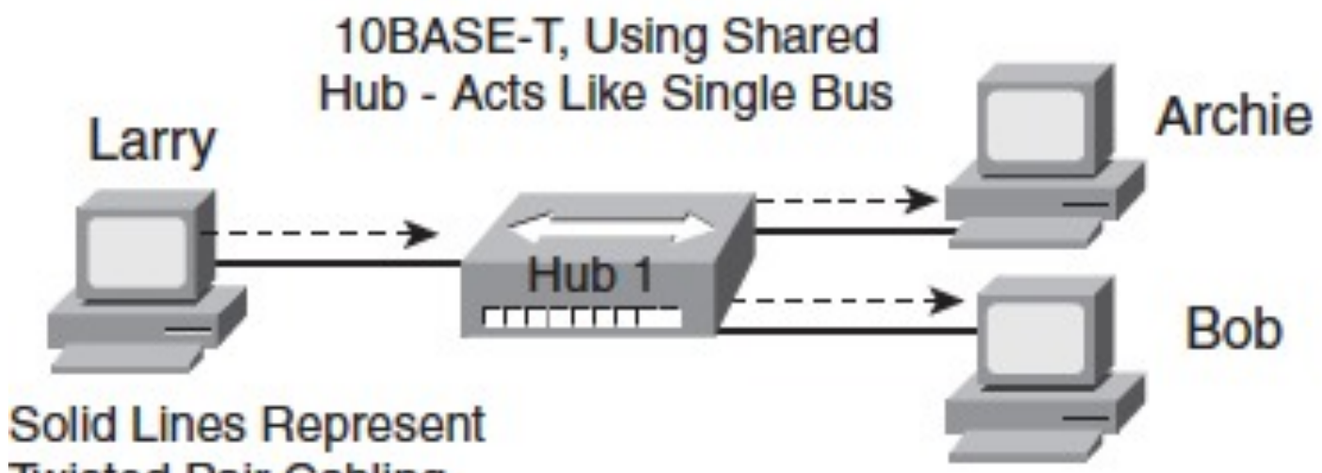
Crossover cables just cross pairs 1,2 with 3,6

10 Base T


RJ-45 Pins
RJ-45 Pins
1
2
3
6
1
2
3
6
3,6
3,6
1,2
1,2


Building 1
Building 2
Switch 11
Switch 12
Switch 21
Switch 22
Straight-
through
Cables
Cross-over
Cables
Straight-
through
Cables

10 Base T


10BASE-T, Using Shared
Hub - Acts Like Single Bus
Larry
Archie
Hub 1
Bob
Solid Lines Represent
Twisted Pair Cabling

THE ETHERNET FRAME

IEEE 802.3 (Revised 1997)

Bytes	**Preamble** 7	**SFD** 1	Destination 6	Source 6	**Length/ Type 2**	Data and Pad 46 – 1500	FCS 4

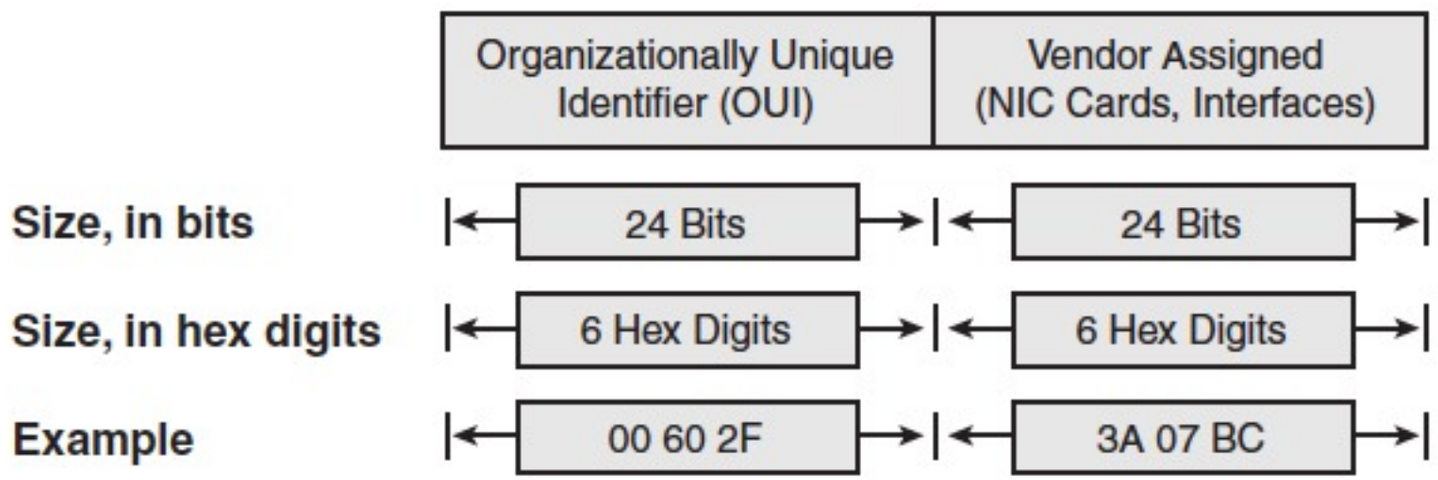
Field	Field Length in Bytes	Description
Preamble	7	Synchronization
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC field
Destination MAC address	6	Identifies the intended recipient of this frame
Source MAC address	6	Identifies the sender of this frame
Length	2	Defines the length of the data field of the frame (either length or type is present, but not both)
Type	2	Defines the type of protocol listed inside the frame (either length or type is present, but not both)
Data and Pad*	46–1500	Holds data from a higher layer, typically an L3 PDU (generic), and often an IP packet
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine if the frame experienced transmission errors

THE MAC ADDRESS

IEEE 802.3 (Revised 1997)

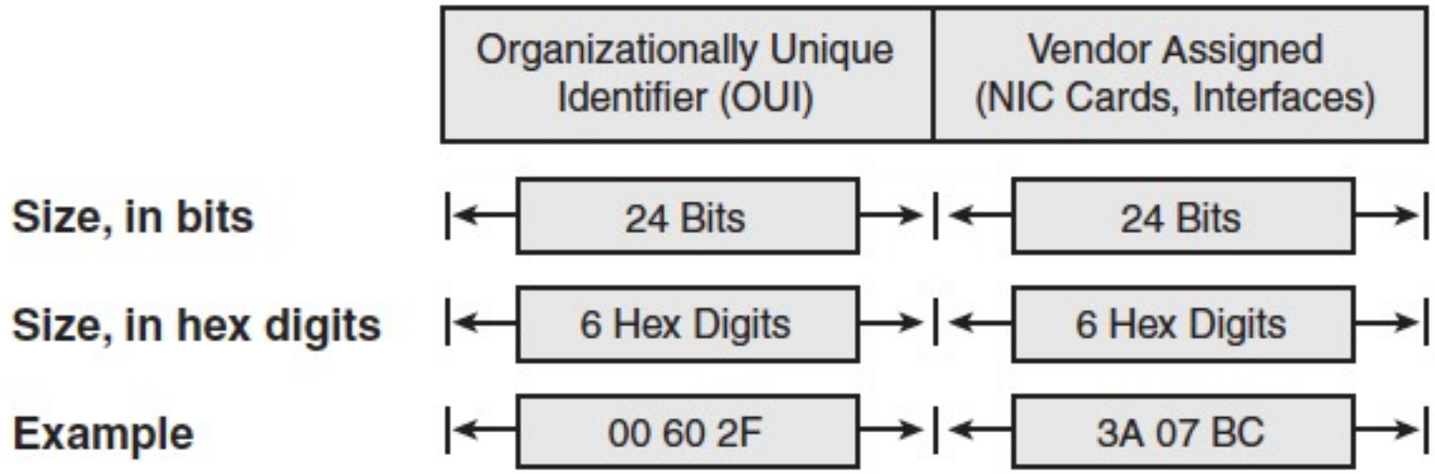
	Preamble	**SFD**	Destination	Source	**Length/**	Data and Pad	FCS
Bytes	7	1	6	6	**Type 2**	46 – 1500	4

Destination MAC address	6	Identifies the intended recipient of this frame
Source MAC address	6	Identifies the sender of this frame



MAC Address

The MAC address is what the SWITCH uses to deliver Layer 2 FRAMES.

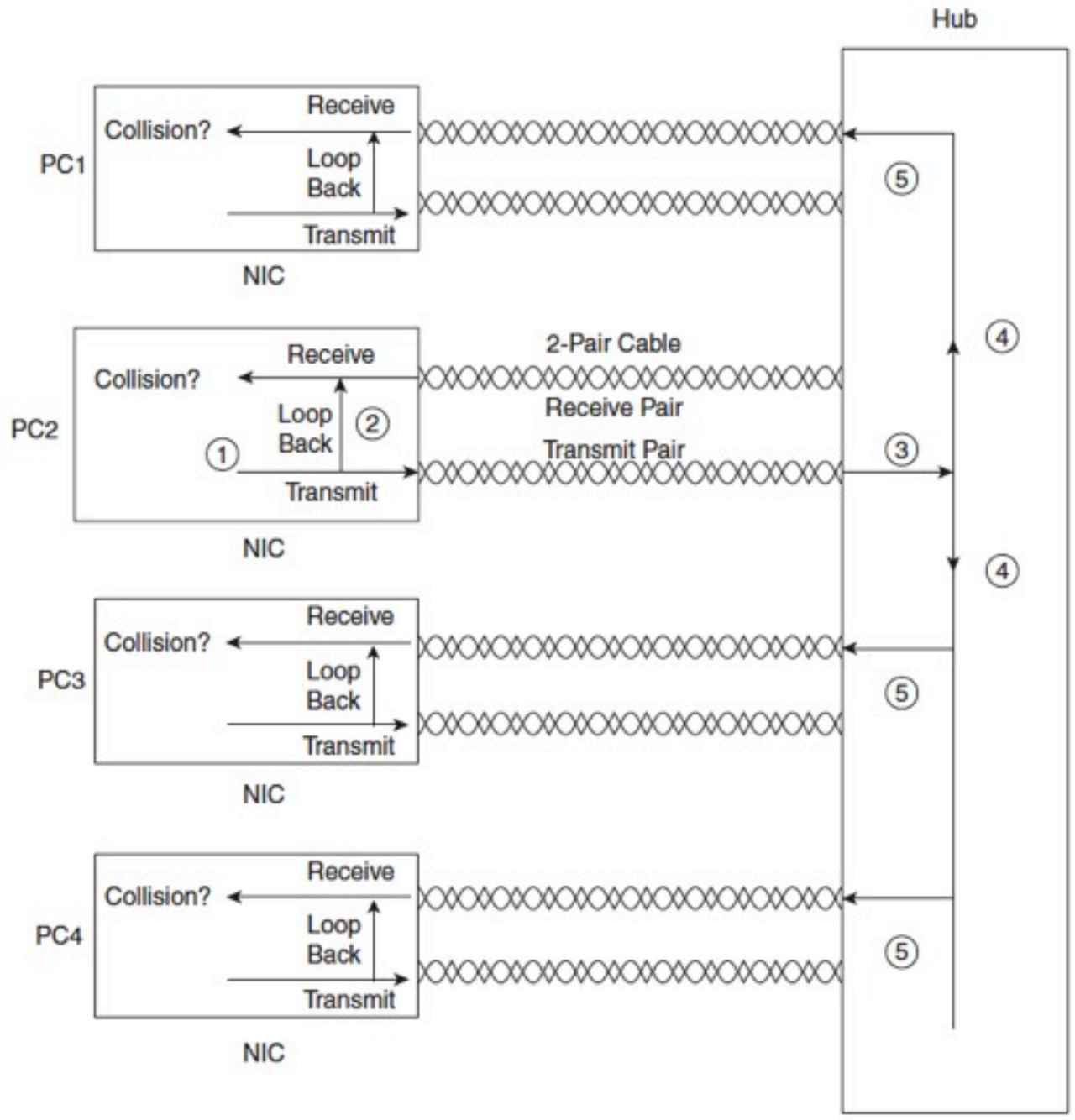


48 Bits or 6 Bytes

In the lab we will see how to check the MAC of your PC.

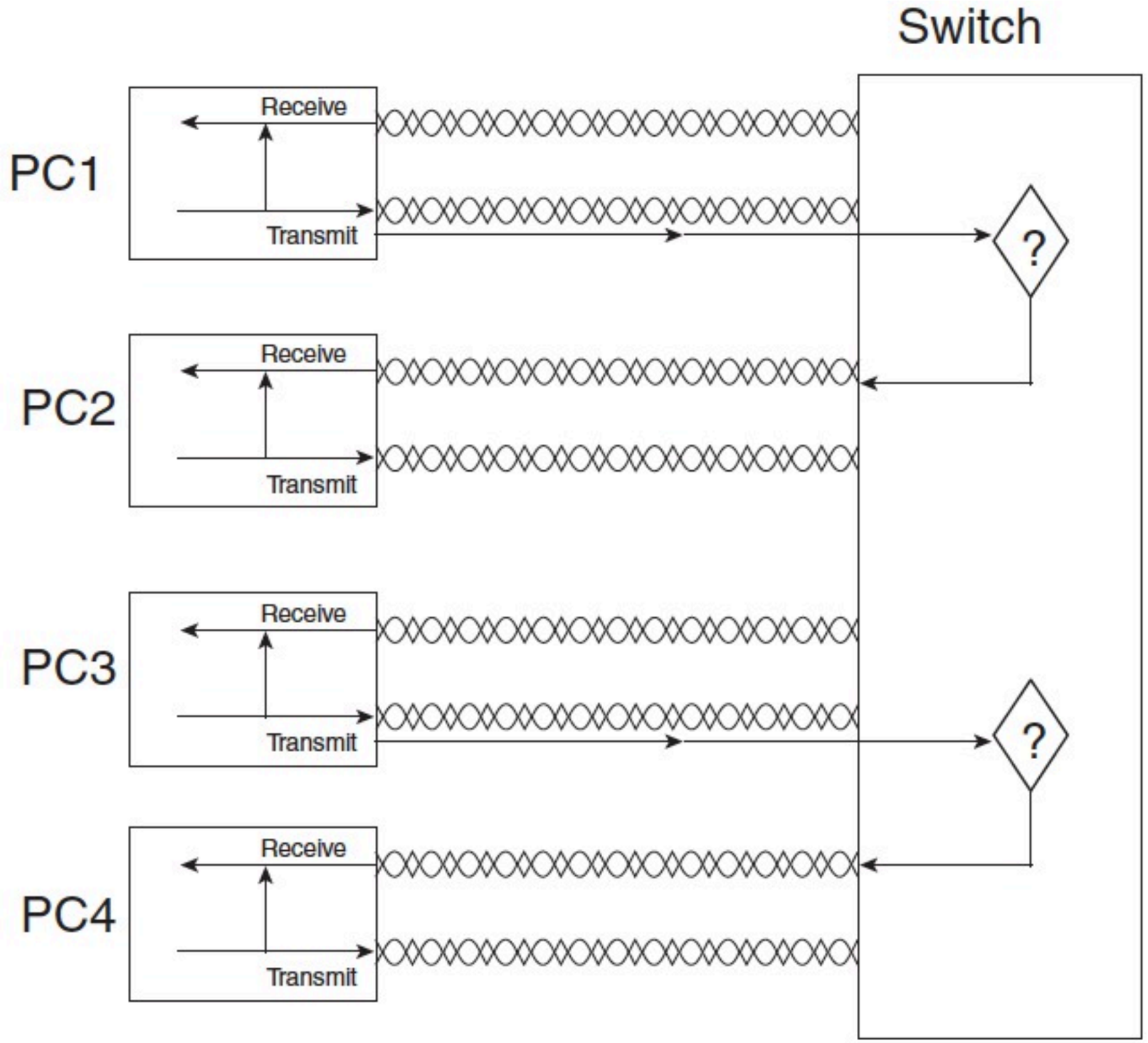
A HUB can be thought of as a BUS.

When a PC transmits a bit it gets copied to all the other ports.



A switch knows what PC is connected to each port

When a PC wants to send data to another PC the switch uses the MAC address to forward the data to the correct port.



Broadcast and Multicast Addresses

Broadcasting is used for DHCP and ARP

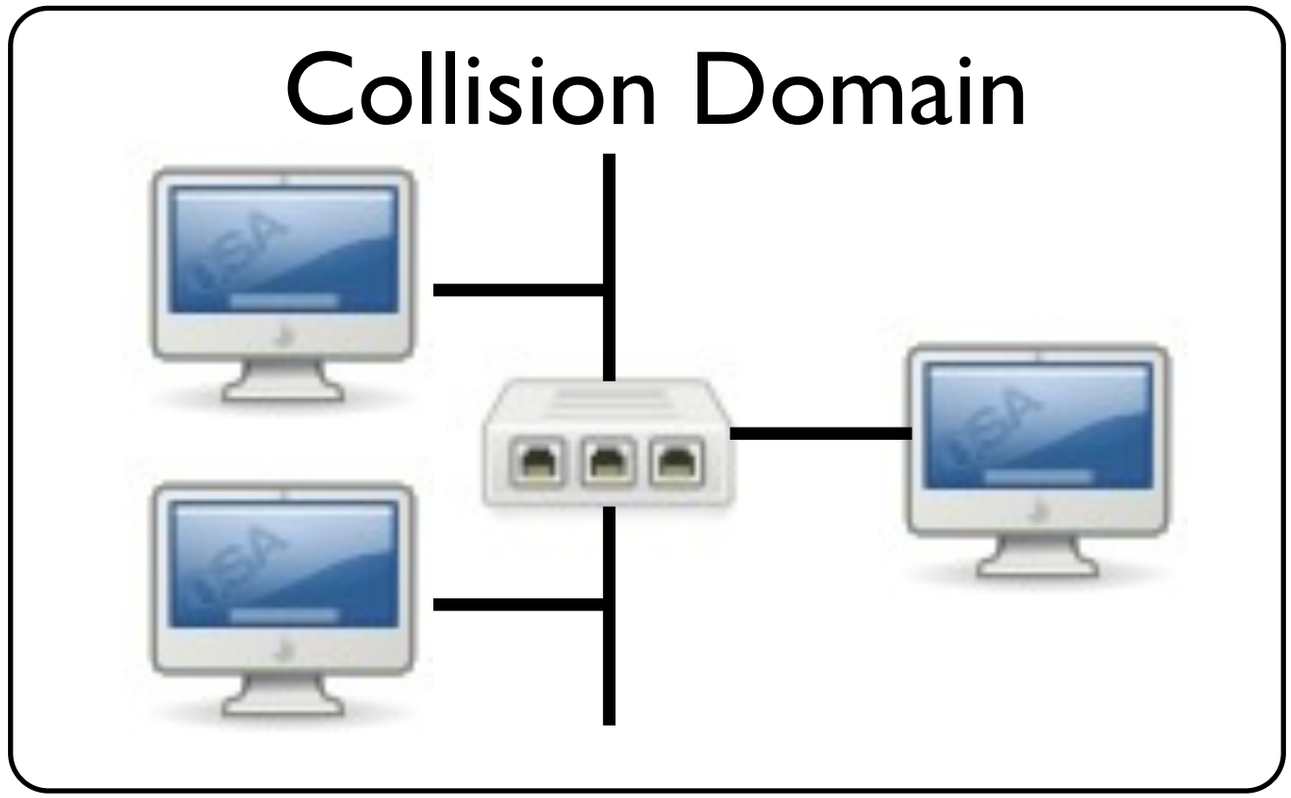
There are lots of situations where you need to broadcast a FRAME

This is done by turning on all the ones in the address:

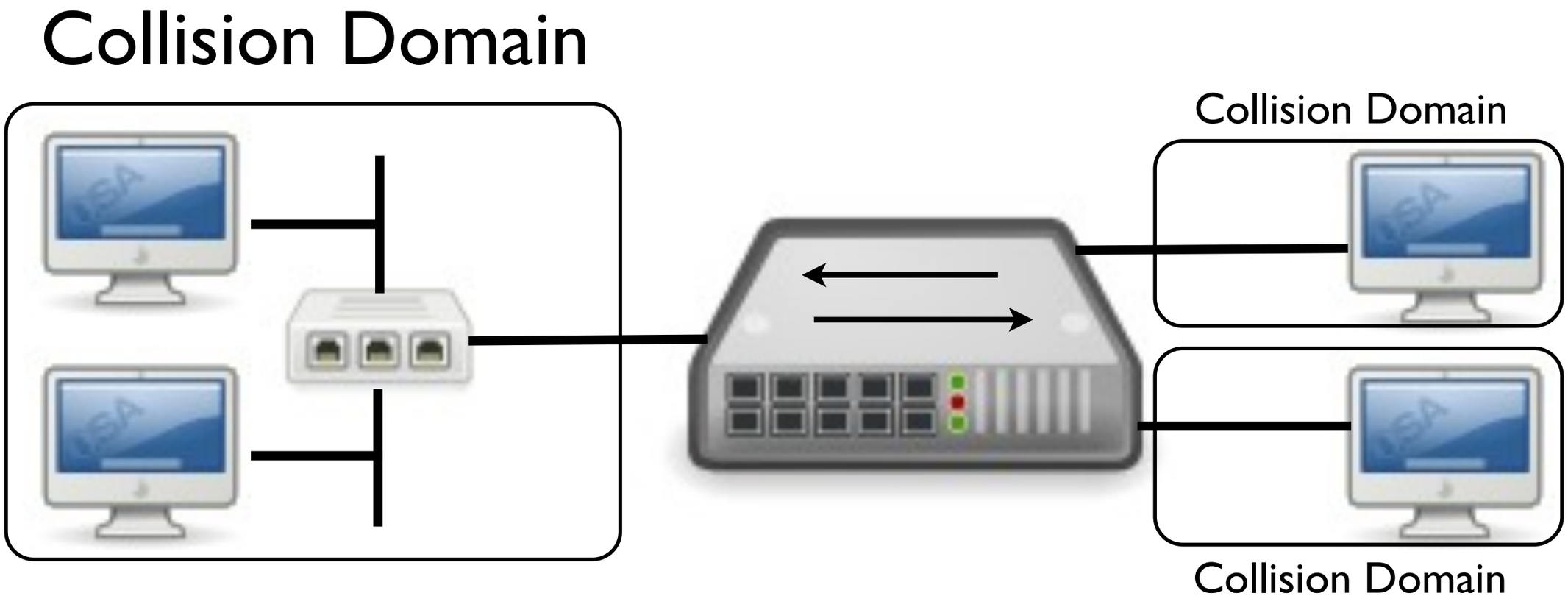
FF.FF.FF.FF.FF.FF

- **Broadcast addresses:** The most often used of the IEEE group MAC addresses, the broadcast address, has a value of FFFF.FFFF.FFFF (hexadecimal notation). The broadcast address implies that all devices on the LAN should process the frame.
- **Multicast addresses:** Multicast addresses are used to allow a subset of devices on a LAN to communicate. When IP multicasts over an Ethernet, the multicast MAC addresses used by IP follow this format: 0100.5e*xx.xxxx*, where any value can be used in the last half of the address.

Multicast is NOT something you will do very often.

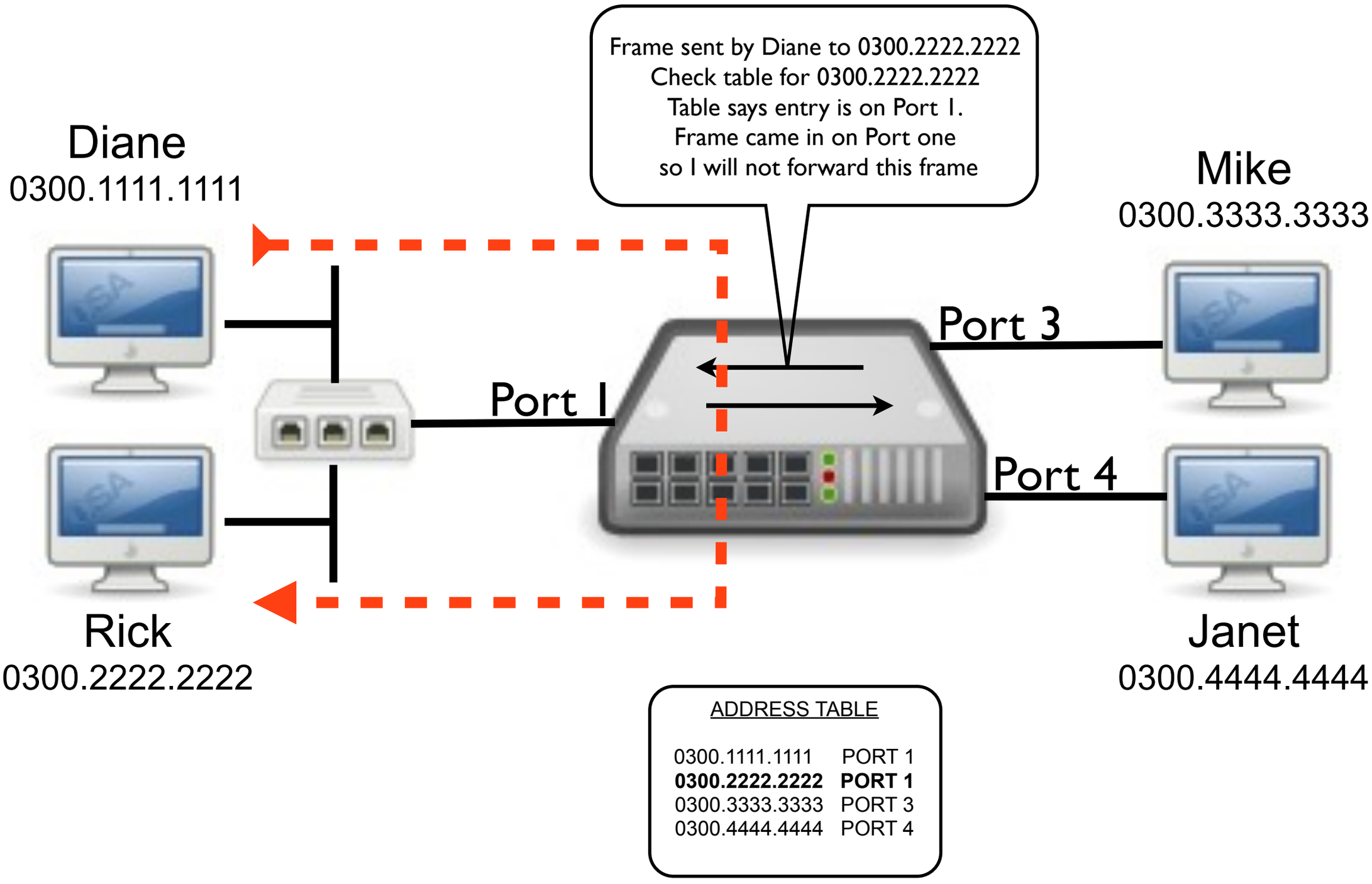


On a hub each port is in the same collision domain

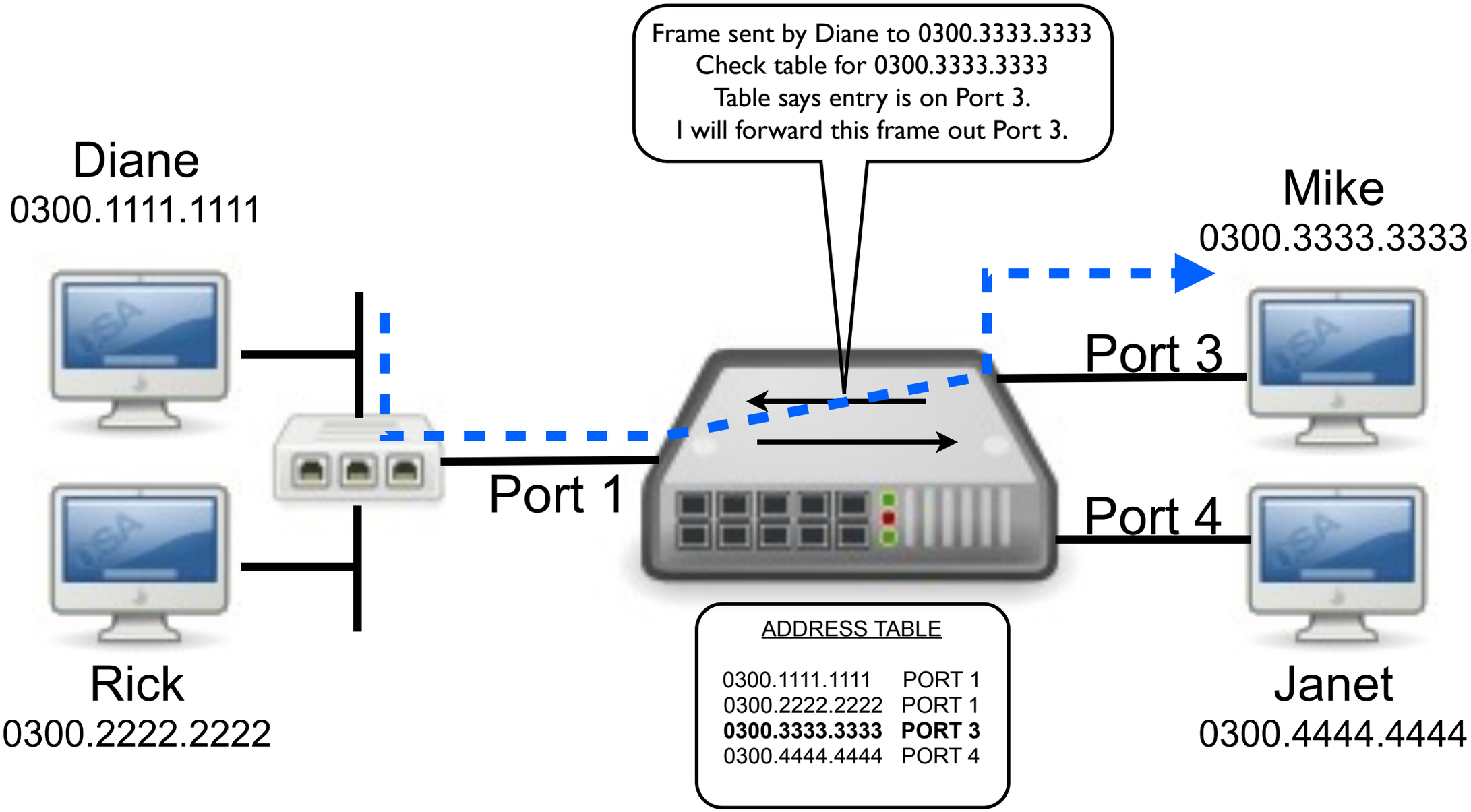


On a SWITCH each port is a separate collision domain.

Switch Forwarding Decisions



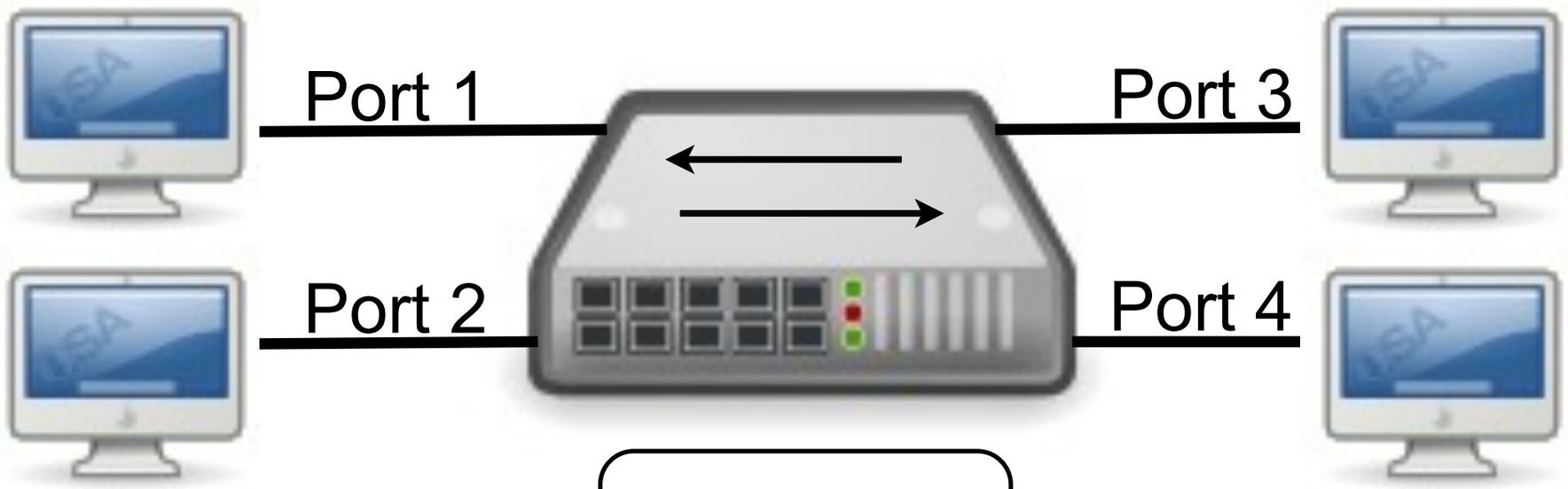
Switch Forwarding Decisions



Switch Layer 2 MAC address learning

Diane
0300.1111.1111

Mike
0300.3333.3333



Rick
0300.2222.2222

ADDRESS TABLE

0300.2222.2222 Port 2

Janet
0300.4444.4444

When **Diane** sends **Mike** a Frame the switch notes that a frame has arrived on Port 1.

Since there is **no entry for Port 1** in the MAC ADDRESS table, the switch **adds 0300.1111.1111 Port 1** to the table.

Finally the switch **forwards the frame** over the two remaining **ports that do not have an entry in the address table**.

Spanning Tree Protocol

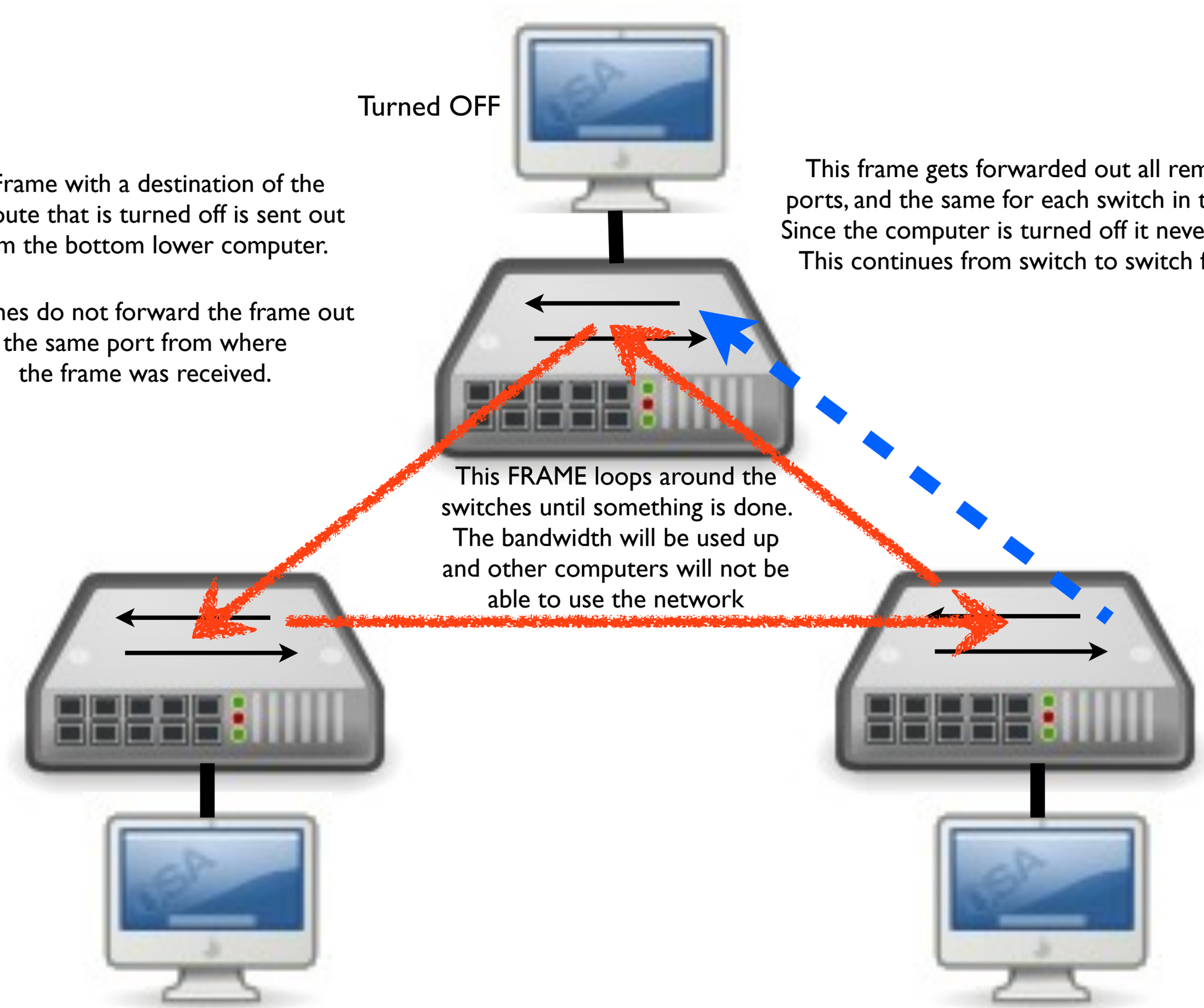
Turned OFF

A Frame with a destination of the compute that is turned off is sent out from the bottom lower computer.

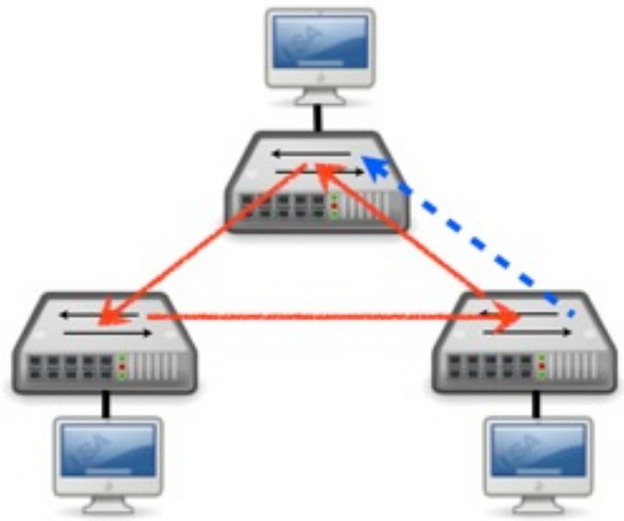
Switches do not forward the frame out the same port from where the frame was received.

This frame gets forwarded out all remaining ports, and the same for each switch in the loop. Since the computer is turned off it never replies. This continues from switch to switch forever.

This FRAME loops around the switches until something is done. The bandwidth will be used up and other computers will not be able to use the network



Spanning Tree Protocol



IEEE 802.1D is the standard developed as reasonable solution to frames going into infinite loops over links put in place for redundancy between switches in an Ethernet network.

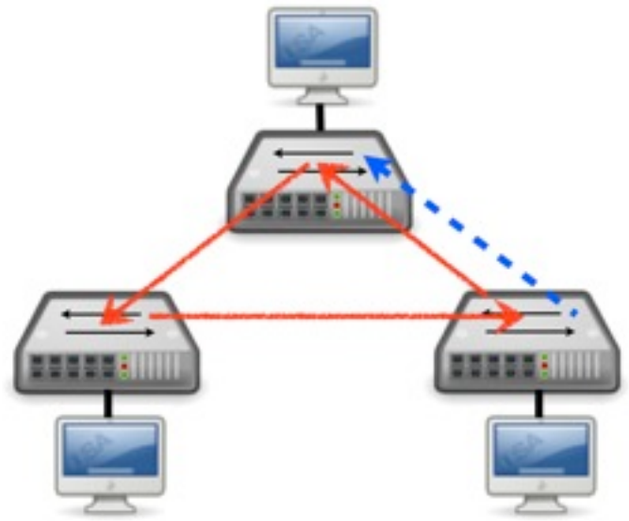
Broadcast storms are the main problem that is addressed by using STP. When a broadcast storm occurs it means that all computers on each port of each switch have to process frames being broadcasted by the switches.

Broadcast storms can occur very easily in a network with ARP requests present, if someone would plug a loopback from one port to the other port on a switch. That switch's CPU utilization will go to 100% and it will be rendered useless.

STP puts each port on a switch into one of two states forwarding or blocking.

This prevents looping by blocking the redundant link that causes the loop to be completed.

Spanning Tree Protocol



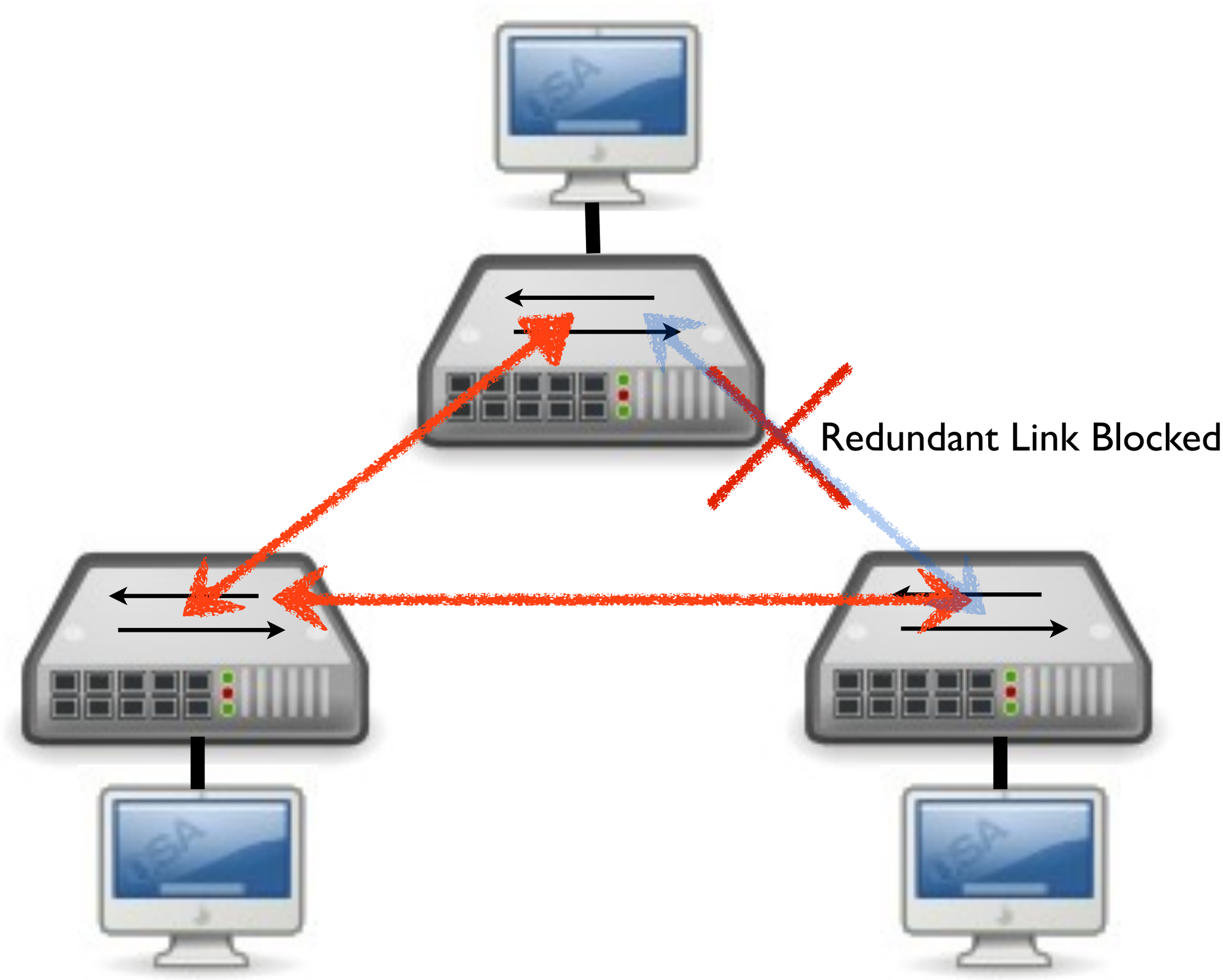
How does this work?

First a ROOT switch is elected and all ports on the ROOT switch are put into forwarding mode.

Each Non-ROOT switch looks at it's ports and chooses the one with the lowest administrative cost between it and the the ROOT. This port is now called the Root Port (RP)
switch and puts that port into the forward mode.

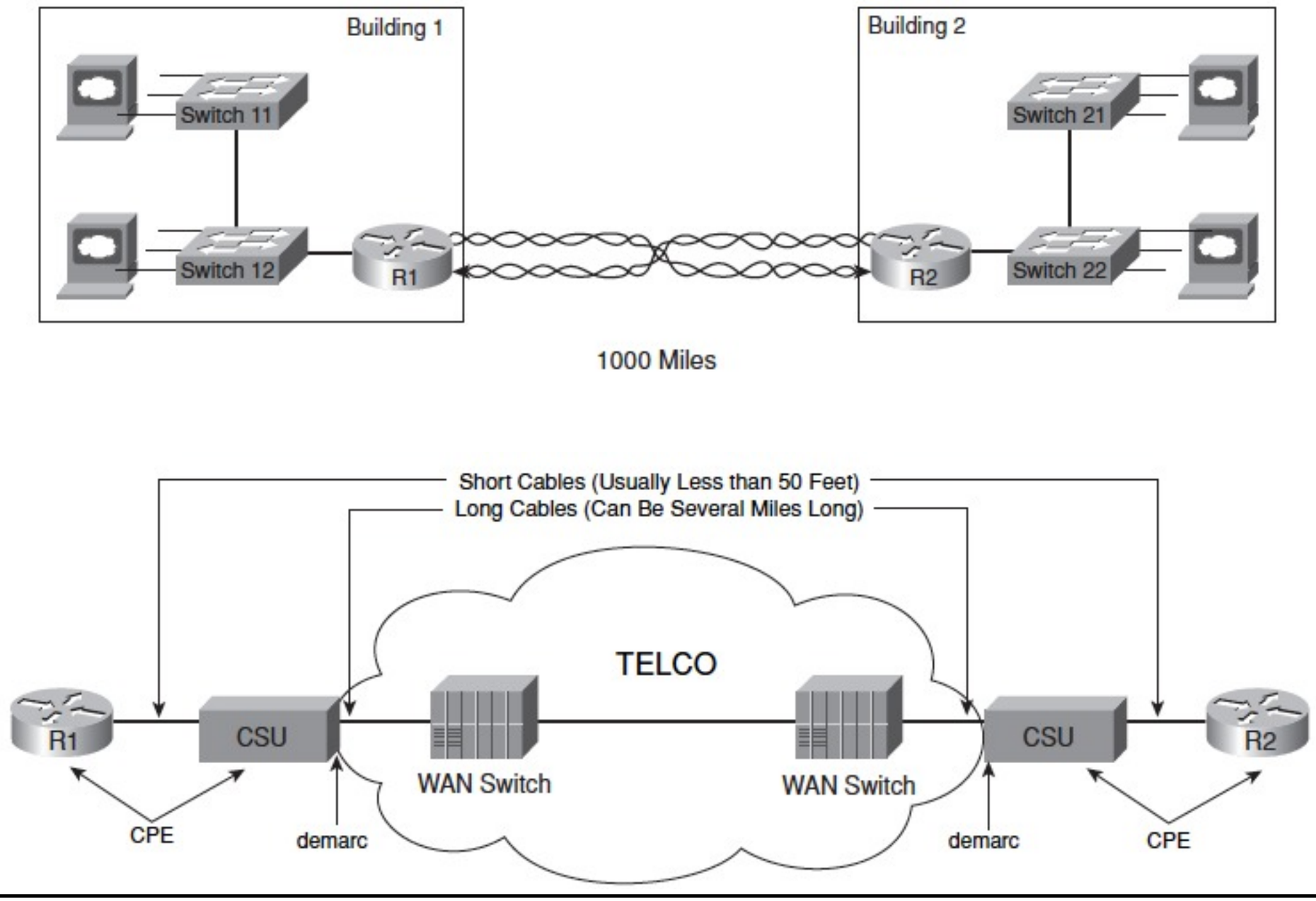
Each Non-ROOT switch is compared to the other switches in an ETHERNET segment and the Switch wit the lowest cost becomes designated switch and the port that attaches to
that segment on that switch becomes the designated port (DP)

Spanning Tree Protocol



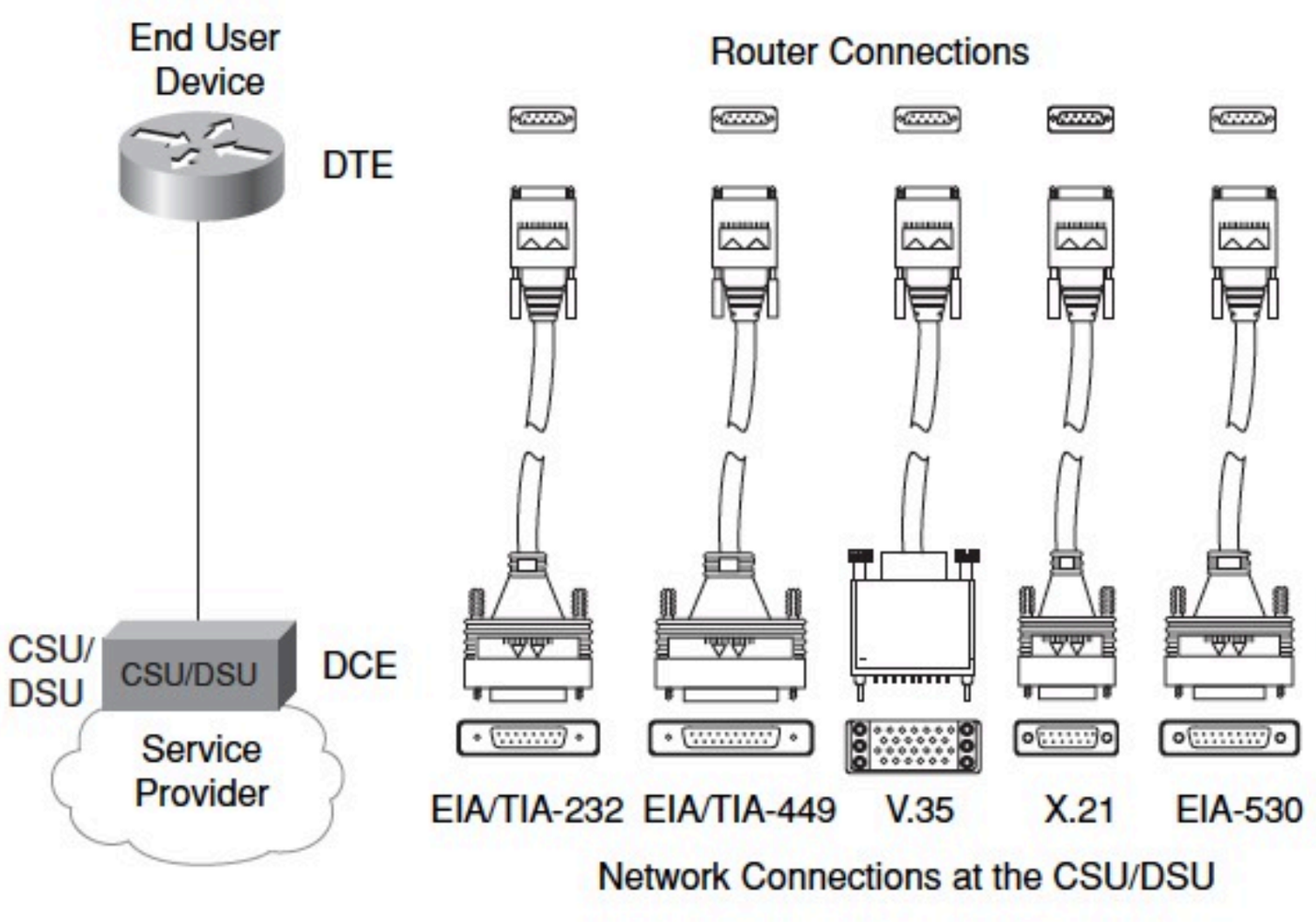
Wide Area Network

The Wide Area Network
WAN



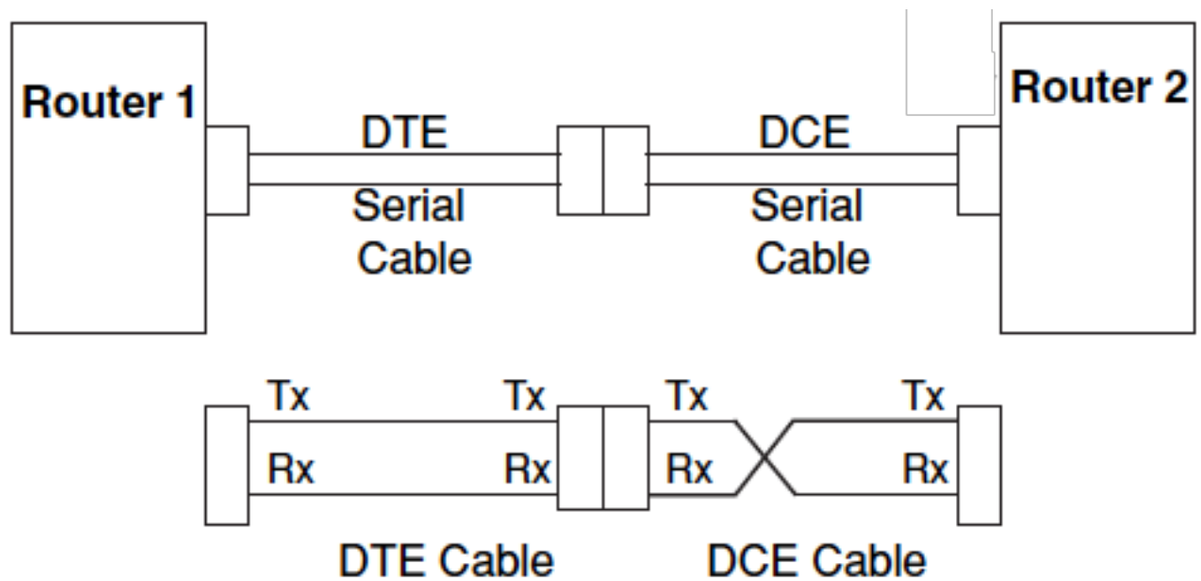
The Wide Area Network

WAN



CABLING

Wide Area Network Cabling

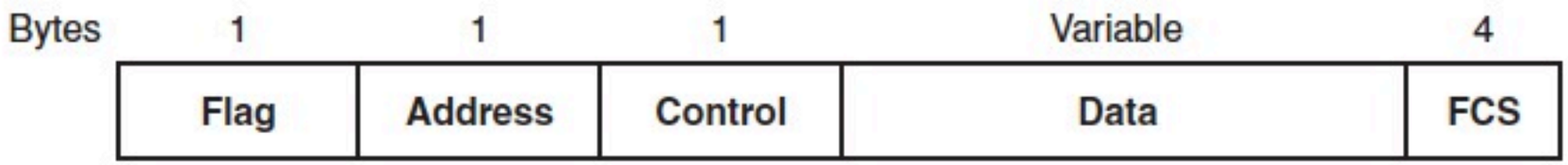


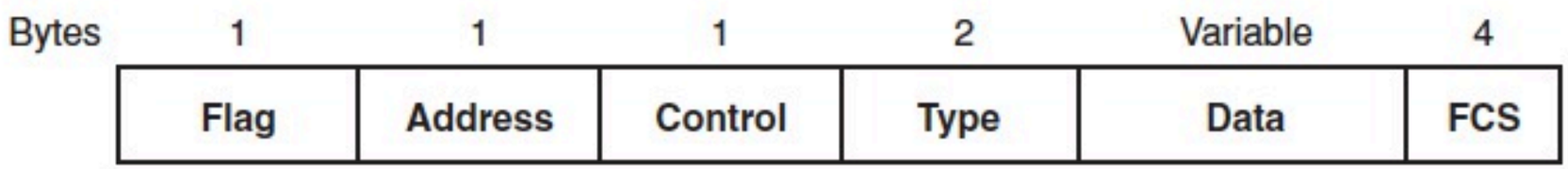
The other side is the DTE or Data Terminal Equipment. DTE is the endpoint in the network, this is the default cable type. In the lab to connect two routers through the *Serial Connection* use a cross over cable.

The DCE or Data Communications Equipment is the service provider side or another router configured to DCE. DCE provides the clocking for the synchronous communications.

HLDC HEADERS

Standard HDLC (No Type Field)



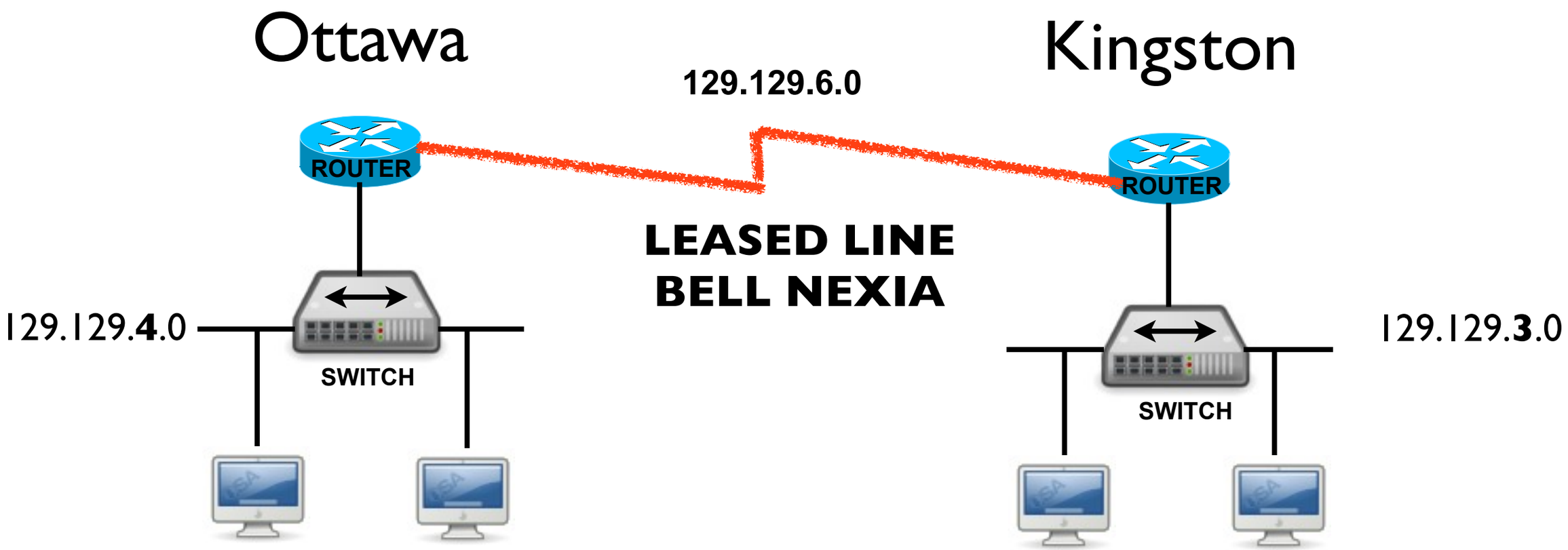


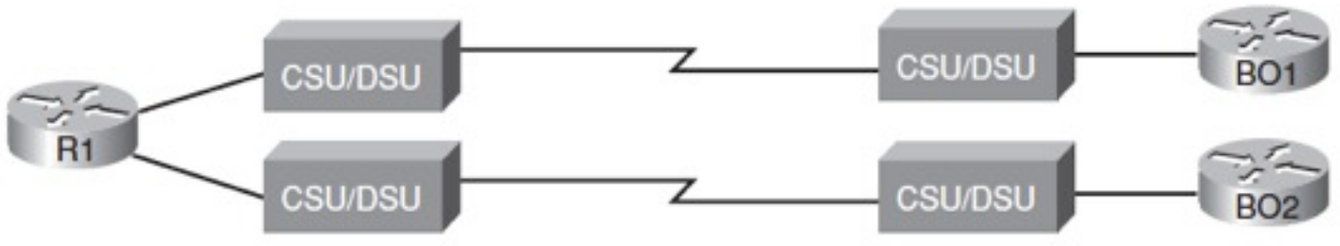
Proprietary Cisco HDLC (Adds Type Field)

HLDC and PPP are the two available protocols for serial ports.

PPP Header is identical to the CISCO proprietary HDLC Header

USE PPP TO CONNECT ROUTERS FROM DIFFERENT VENDORS

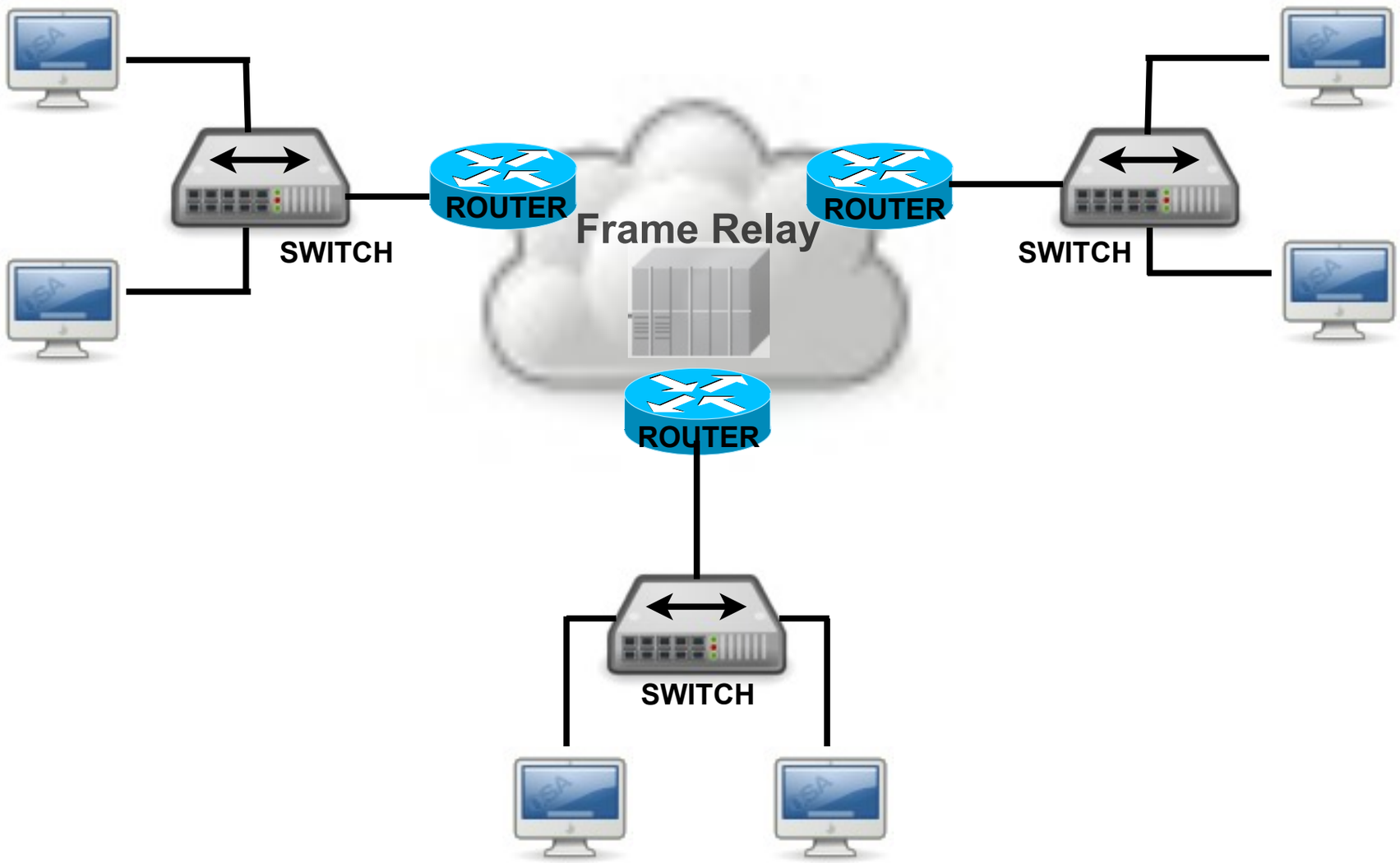

Ottawa
Kingston
129.129.6.0
ROUTER
ROUTER
LEASED LINE
BELL NEXIA
129.129.4.0
129.129.3.0
SWITCH
SWITCH
Harry
129.129.4.2
Mo
129.129.4.3
Marcy
129.129.3.2
Peggy
129.129.3.3


R1
CSU/DSU
CSU/DSU
CSU/DSU
CSU/DSU
BO1
BO2

FRAME RELAY

Ottawa

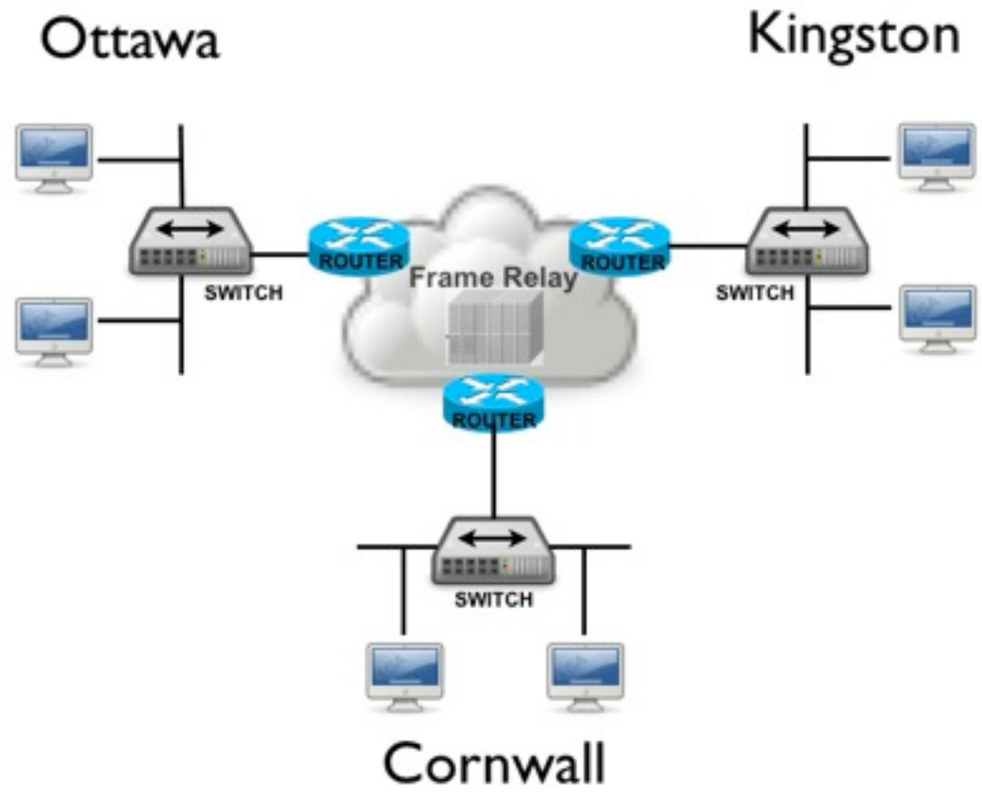
Kingston



Cornwall

With Frame Relay you only need one connection per router into the backhaul network.

FRAME RELAY

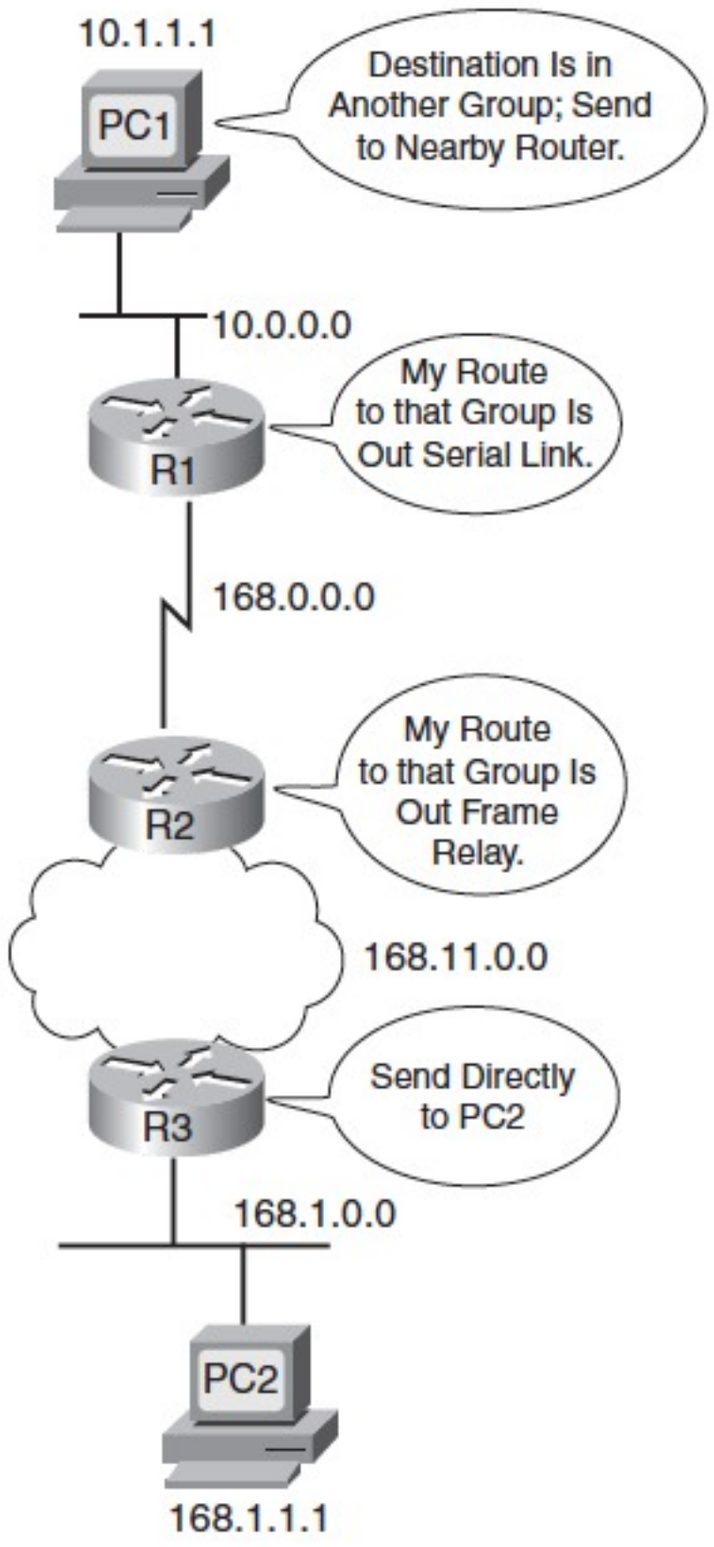


Frame Relay is a standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology.

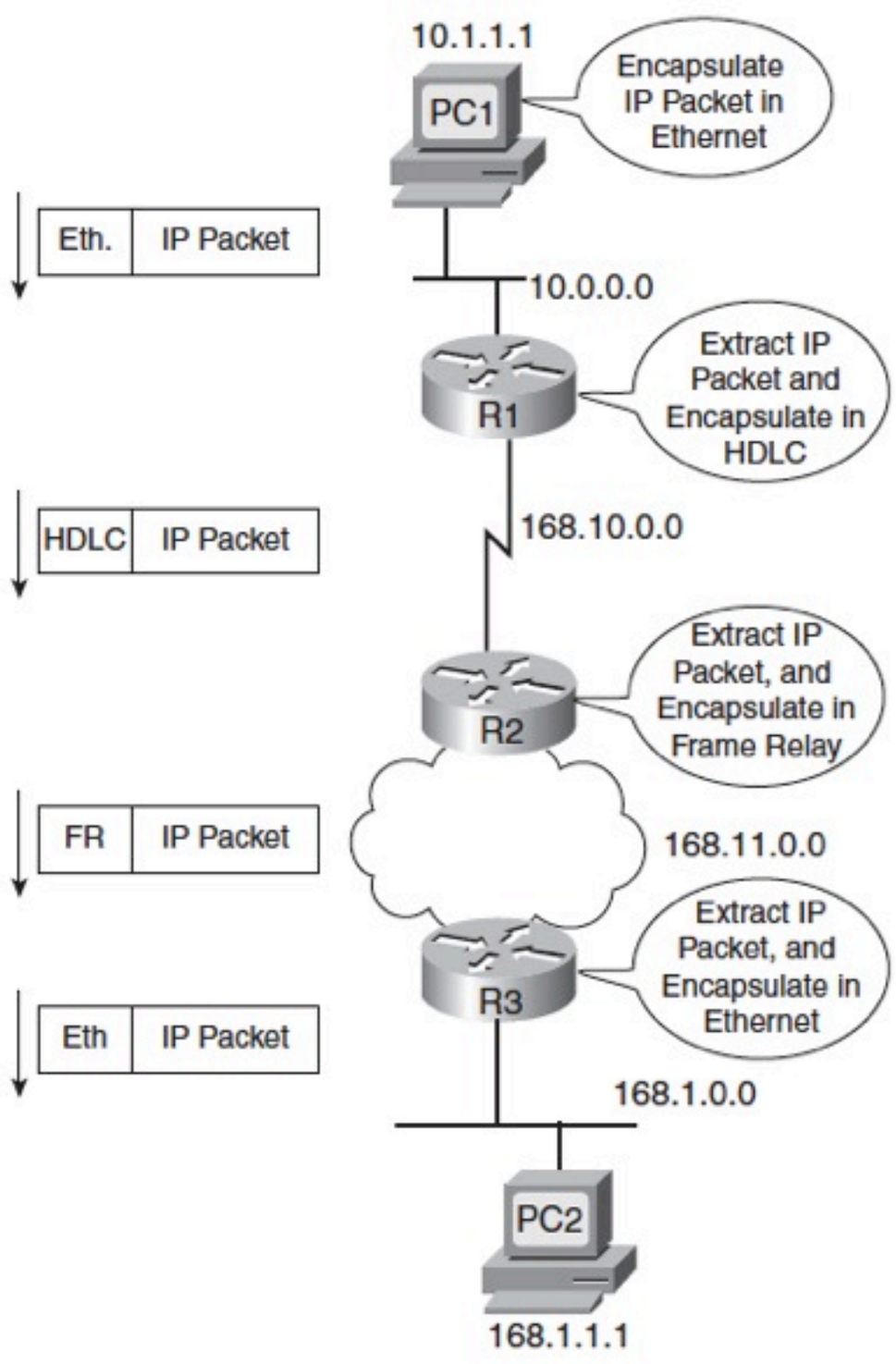
Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces.

Each end-user gets a private line (or leased line) to a Frame Relay node.
The Frame Relay network handles the transmission
over a frequently-changing path transparent to all end-users.

Your Packet can travel over many different modes before it reaches it's destination.

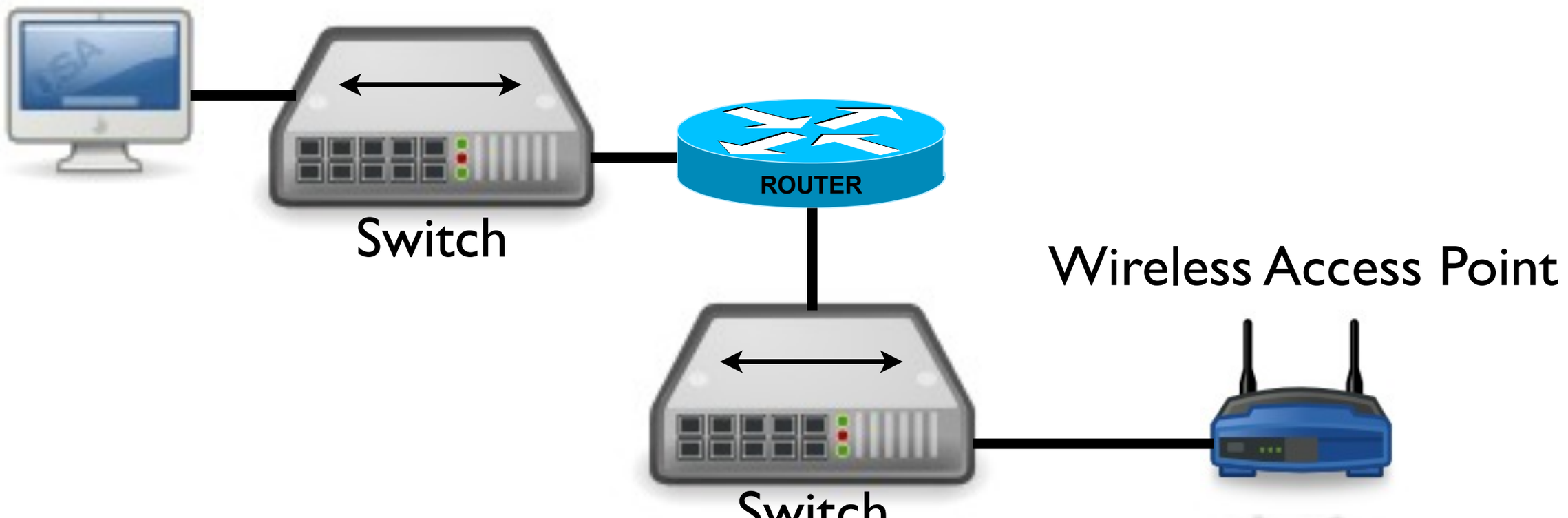


Each router de-encapsulates the data makes a decision based on IP address destination then encapsulates and sends the data on it's way.



Wireless LAN

Wireless LAN



Wi-Fi allows wireless access to the internet.

BSS Basic Service Set
One AP creates a Single LAN

Wireless LAN

There are four types of Wireless LAN in use currently

802.11 Network Standards								
802.11 Protocol	Release Date	Freq. (GHz)	Bandwidth (MHz)	DATA RATE per stream Mb/s	Max MIMO streams	Modulation	Approximate Range Indoor (m)	Approximate Range Outdoor (m)
Original	June 1997	2.4	20	12	1	DSSS, FHSS	20	100
A	Sept 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	120
B	Sept 1997	2.4	20	1, 2, 5.5, 11	1	DSSS	34	140
G	June 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	140
N	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM	70	250
AC (DRAFT)	Nov 2011	5	20-160	87.6 - 866.7	8		Unknown	Unknown

Wireless LAN modes

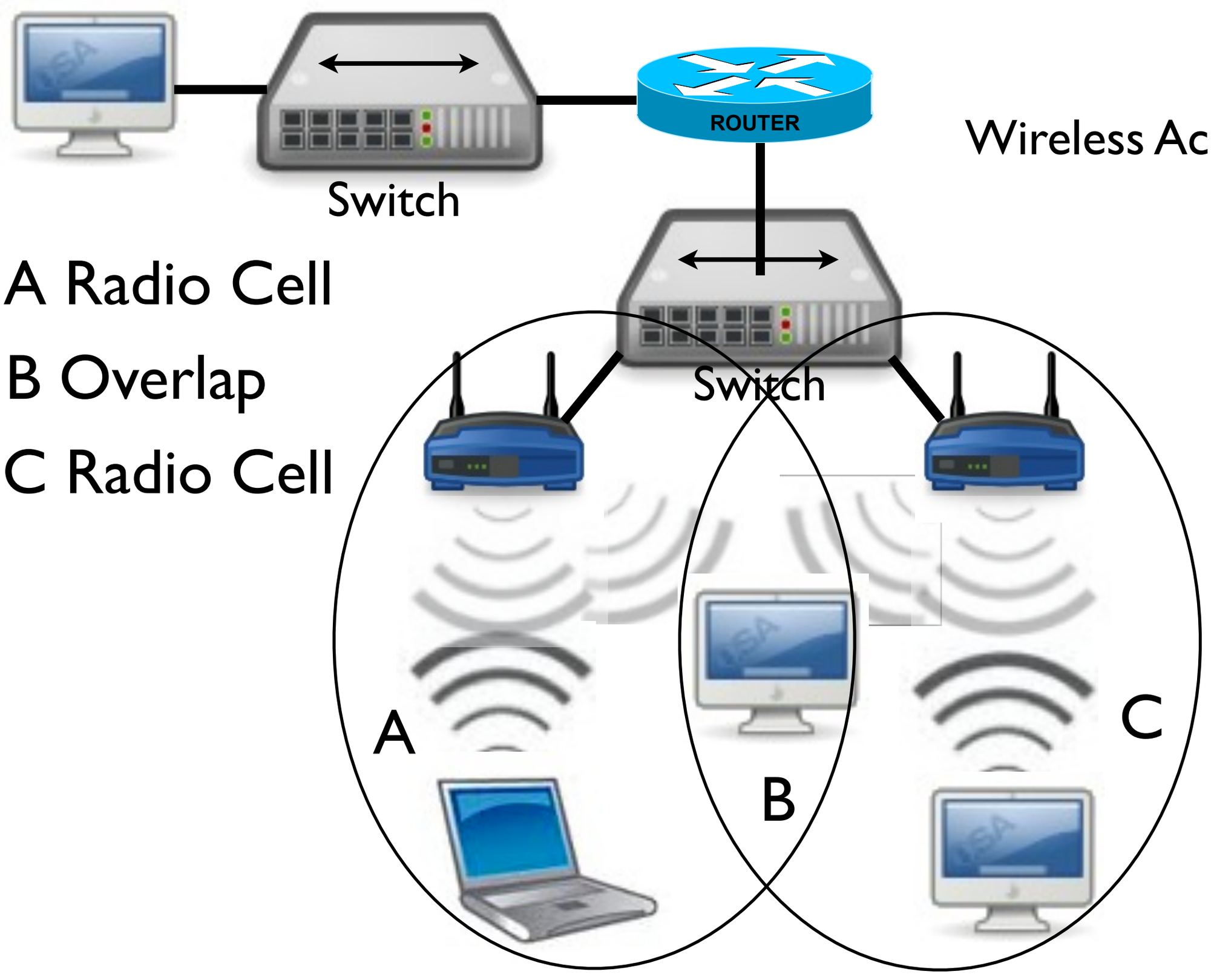
Ad Hoc	**IBSS** **Independent Basic Service Set**	Allows two devices to talk without an AP.
Infrastructure	**BSS** **Basic Service Set**	A single wireless LAN created with an AP and the devices that associate with the APP.
	ESS **Extended Service Set** **(> 1 AP)**	Multiple AP's create one wireless LAN, allowing roaming and a larger coverage area.

AD HOC

Allows two devices to communicate with each other directly without an Access Point

ESS Extended Service Set

Multiple AP's implement a single LAN



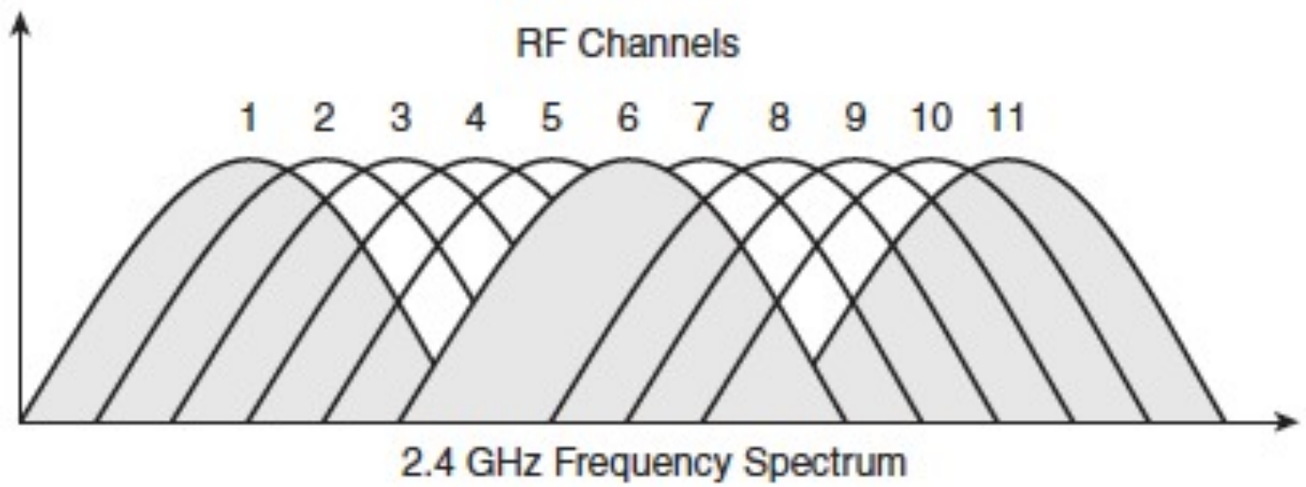
Wireless Access Point

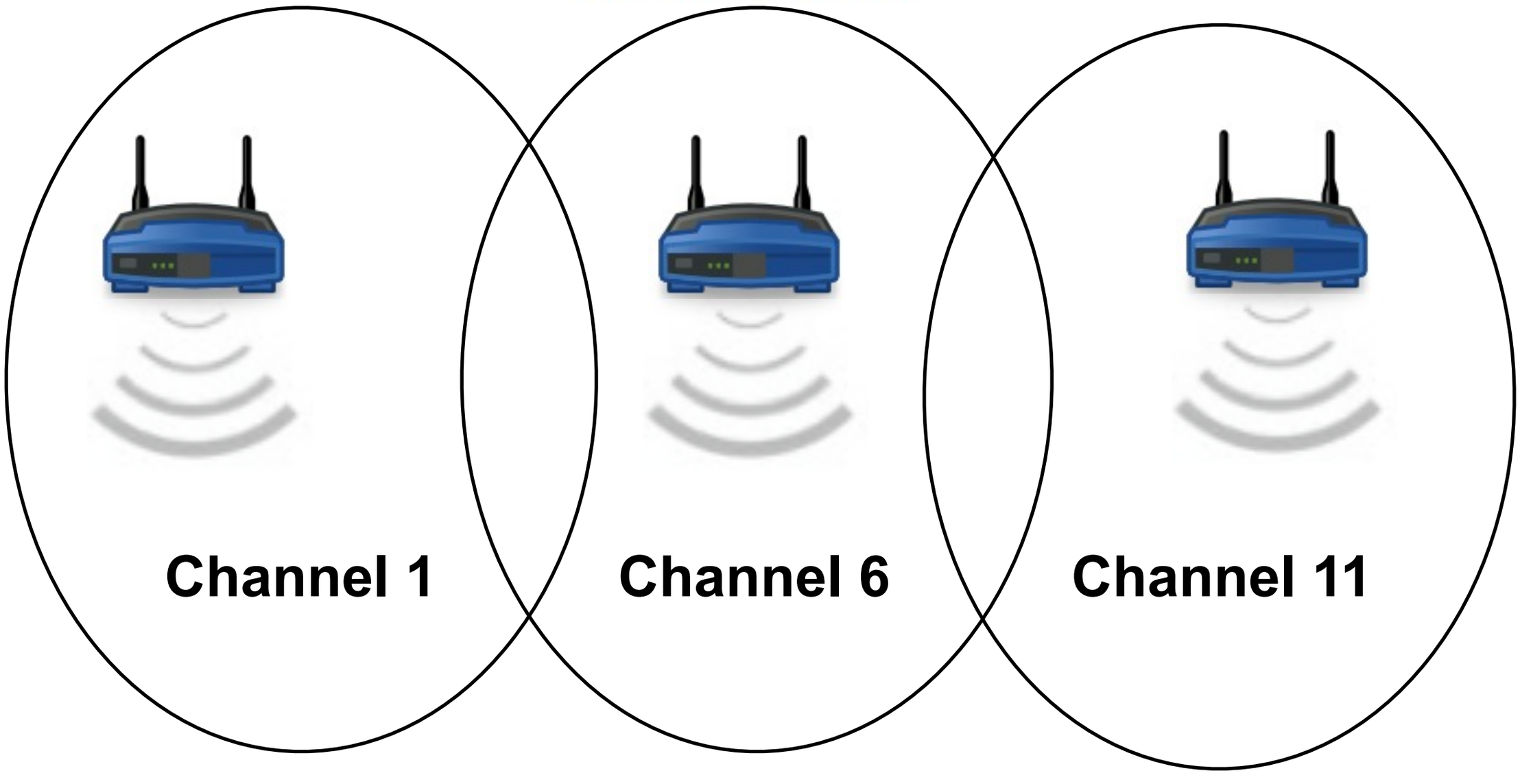
A Radio Cell

B Overlap

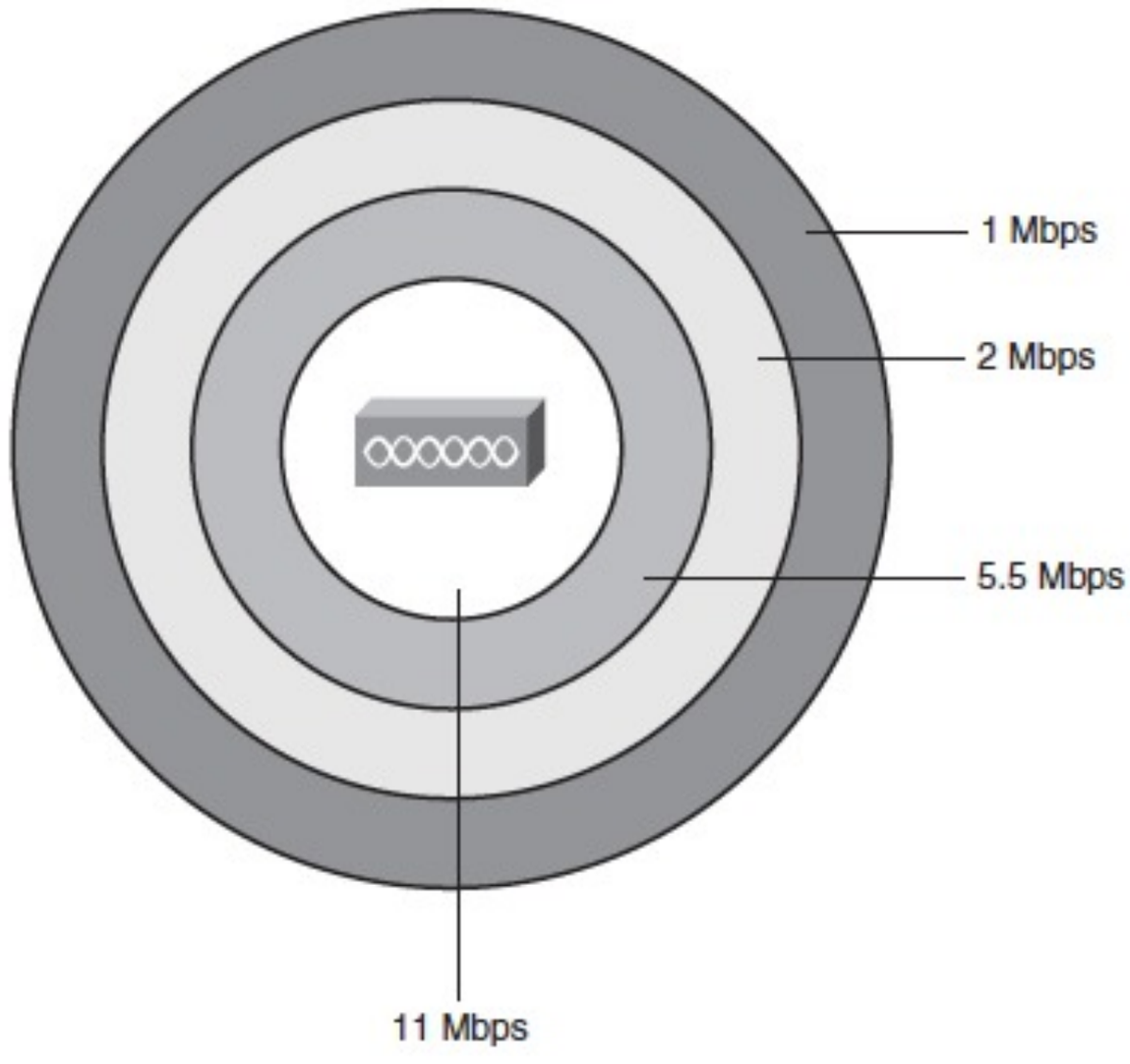
C Radio Cell

Choosing NonOverlapping Frequencies for each AP





Range and Speed for a Wireless AP

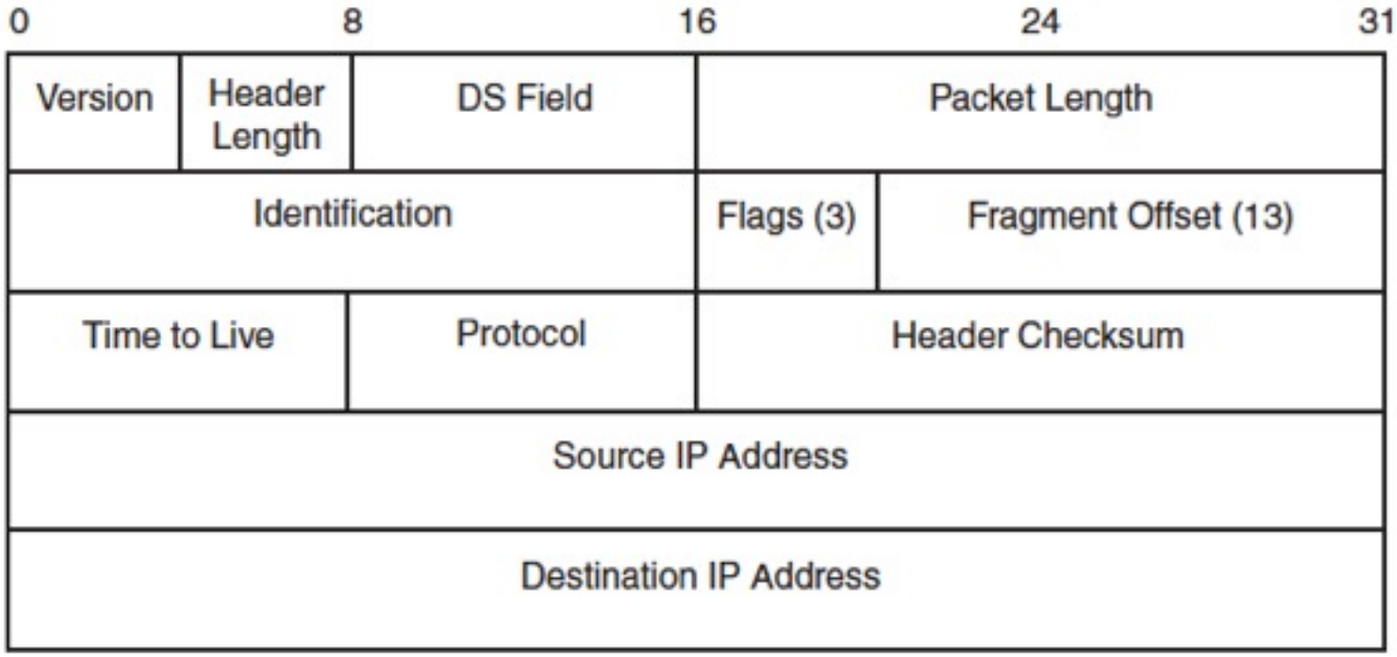


Wireless Security

Standard	Key Distribution	Device Authentication	User Authentication	Encryption
WEP	Static	Yes (Weak)	None	Yes (Weak)
WPA	Both	YES	Yes (802.11x)	YES (TKIP)
WPA2	Both	YES	Yes (802.11x)	YES (AES)

Internet Protocol

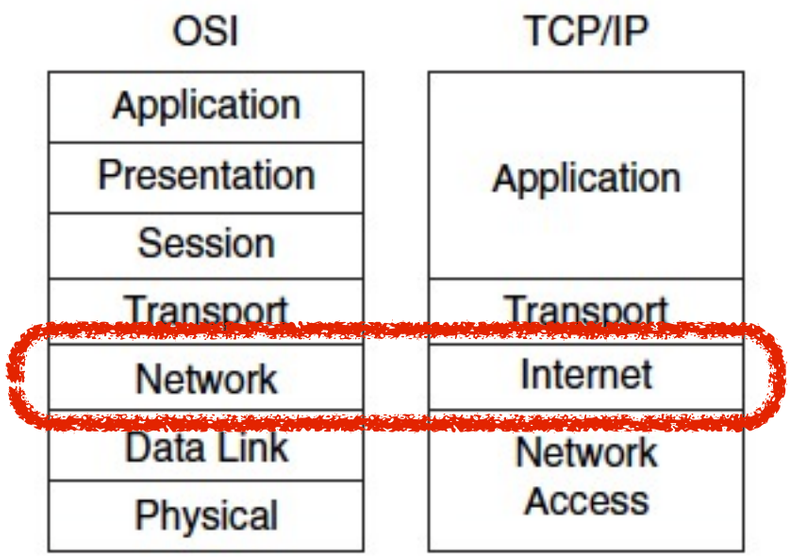
IP HEADER

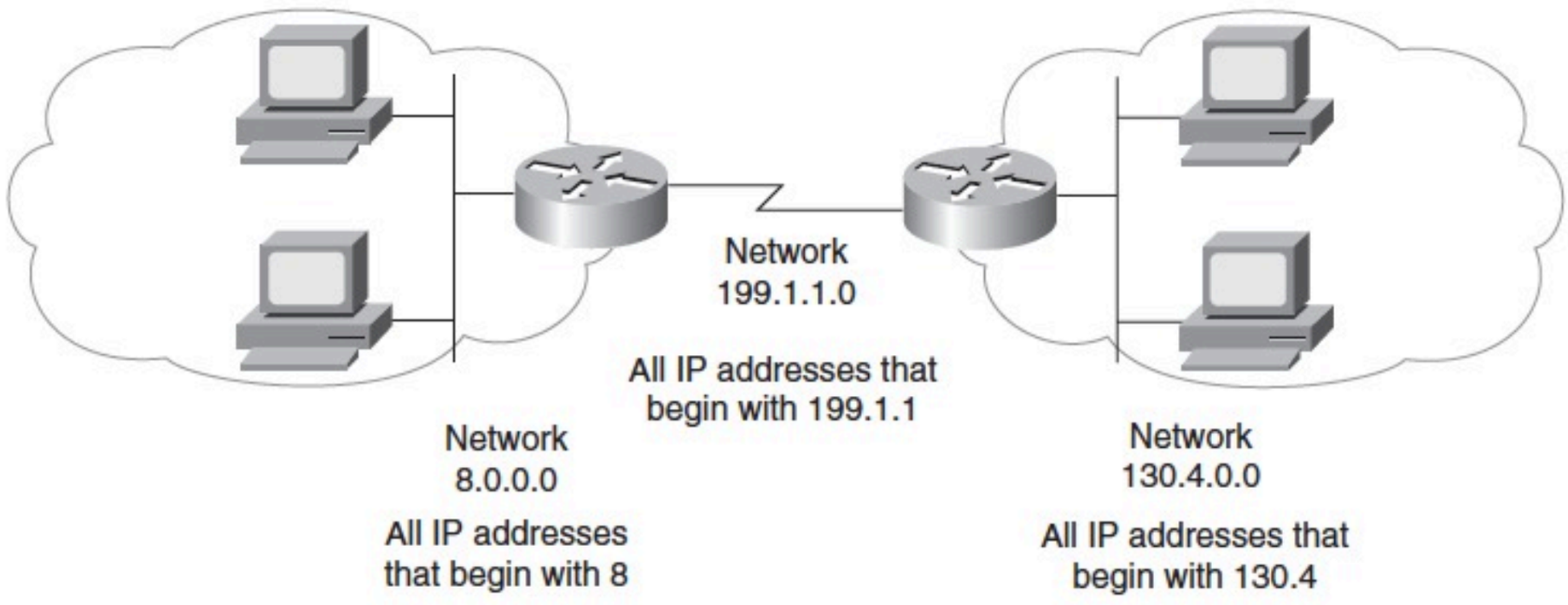


Field	Meaning
Version	Version of the IP protocol. Most networks use version 4 today.
IHL	IP Header Length. Defines the length of the IP header, including optional fields.
DS Field	Differentiated Services Field. It is used for marking packets for the purpose of applying different quality-of-service (QoS) levels to different packets.
Packet length	Identifies the entire length of the IP packet, including the data.
Identification	Used by the IP packet fragmentation process; all fragments of the original packet contain the same identifier.
Flags	3 bits used by the IP packet fragmentation process.
Fragment offset	A number used to help hosts reassemble fragmented packets into the original larger packet.
TTL	Time to live. A value used to prevent routing loops.
Protocol	A field that identifies the contents of the data portion of the IP packet. For example, protocol 6 implies that a TCP header is the first thing in the IP packet data field.
Header Checksum	A value used to store an FCS value, whose purpose is to determine if any bit errors occurred in the IP header.
Source IP address	The 32-bit IP address of the sender of the packet.
Destination IP address	The 32-bit IP address of the intended recipient of the packet.

Internet Protocol

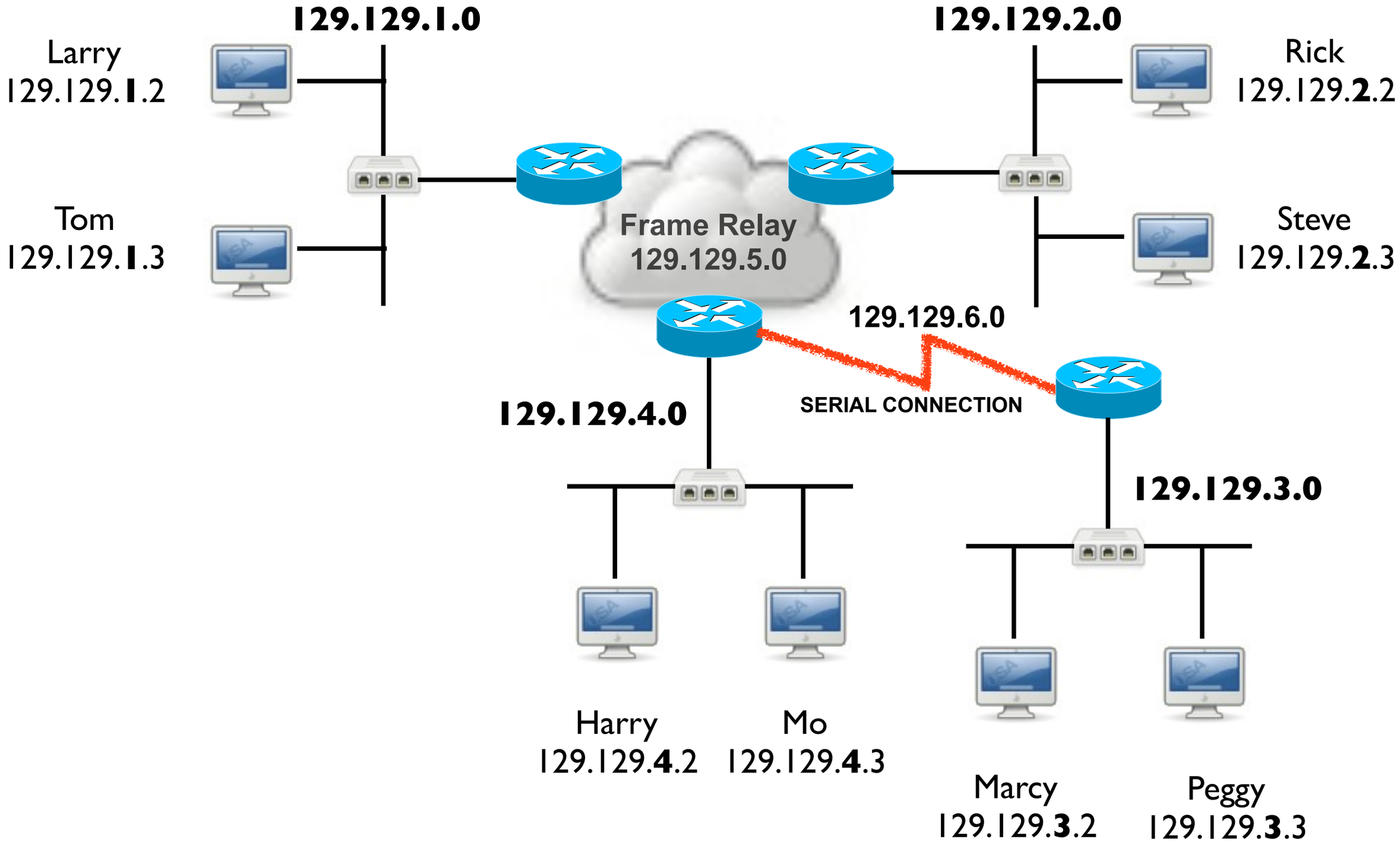
IP is Layer 2 in TCP/IP stack and Layer 3 in OSI model



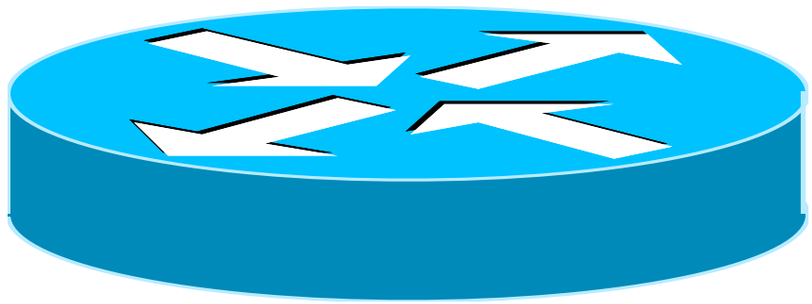


Typical WAN with IP addressing

Here we split up the **Class B 129.129** network
The natural subnet mask for this network will be
255.255.0.0



ROUTER

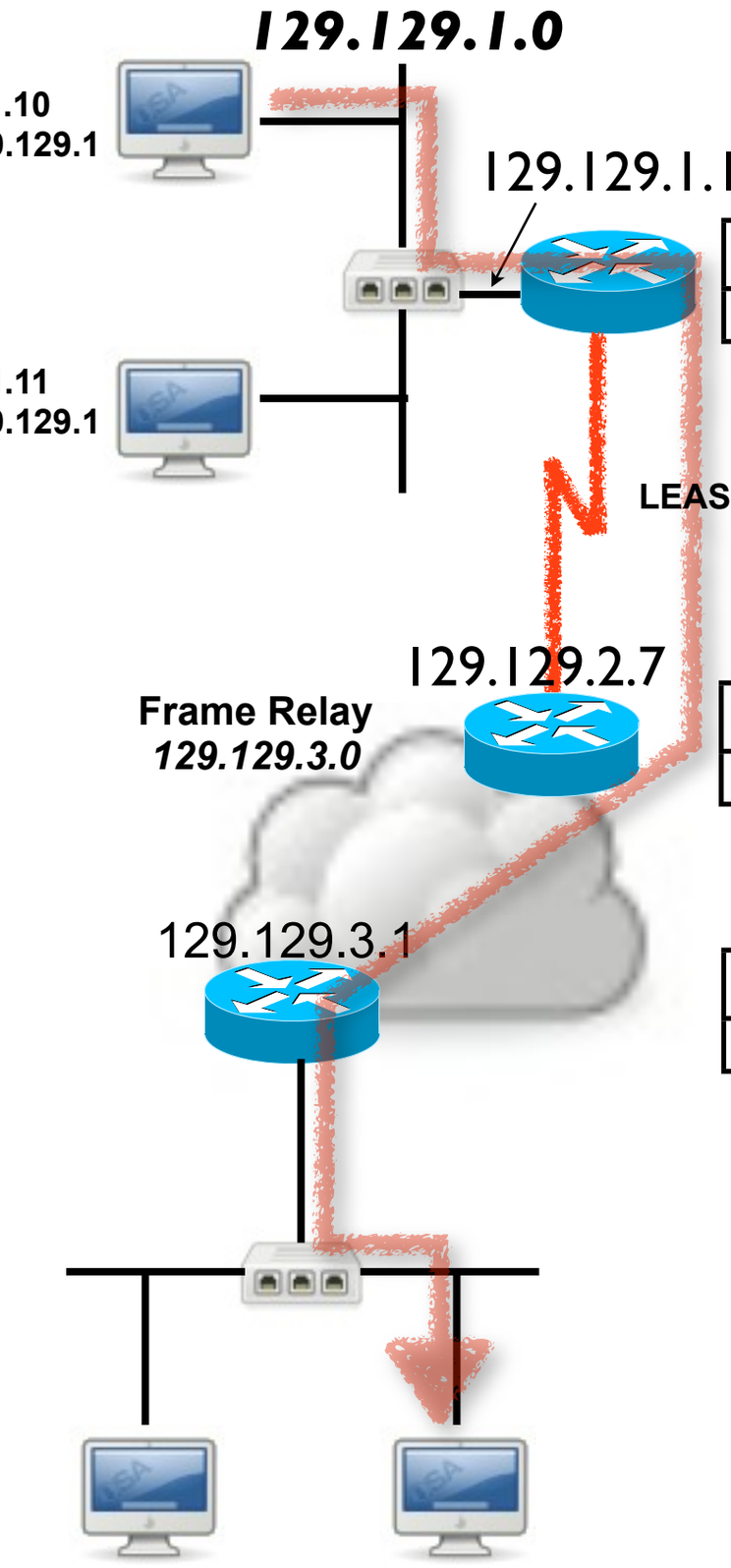


Uses the IP address to route Internet Packets

It can have Serial Ports and Ethernet Ports and Optical Ports either running ATM or Ethernet.

It takes the IP packet unwraps the Ethernet Frame and looks at the IP address, then it looks in it's routing table to make a decision.

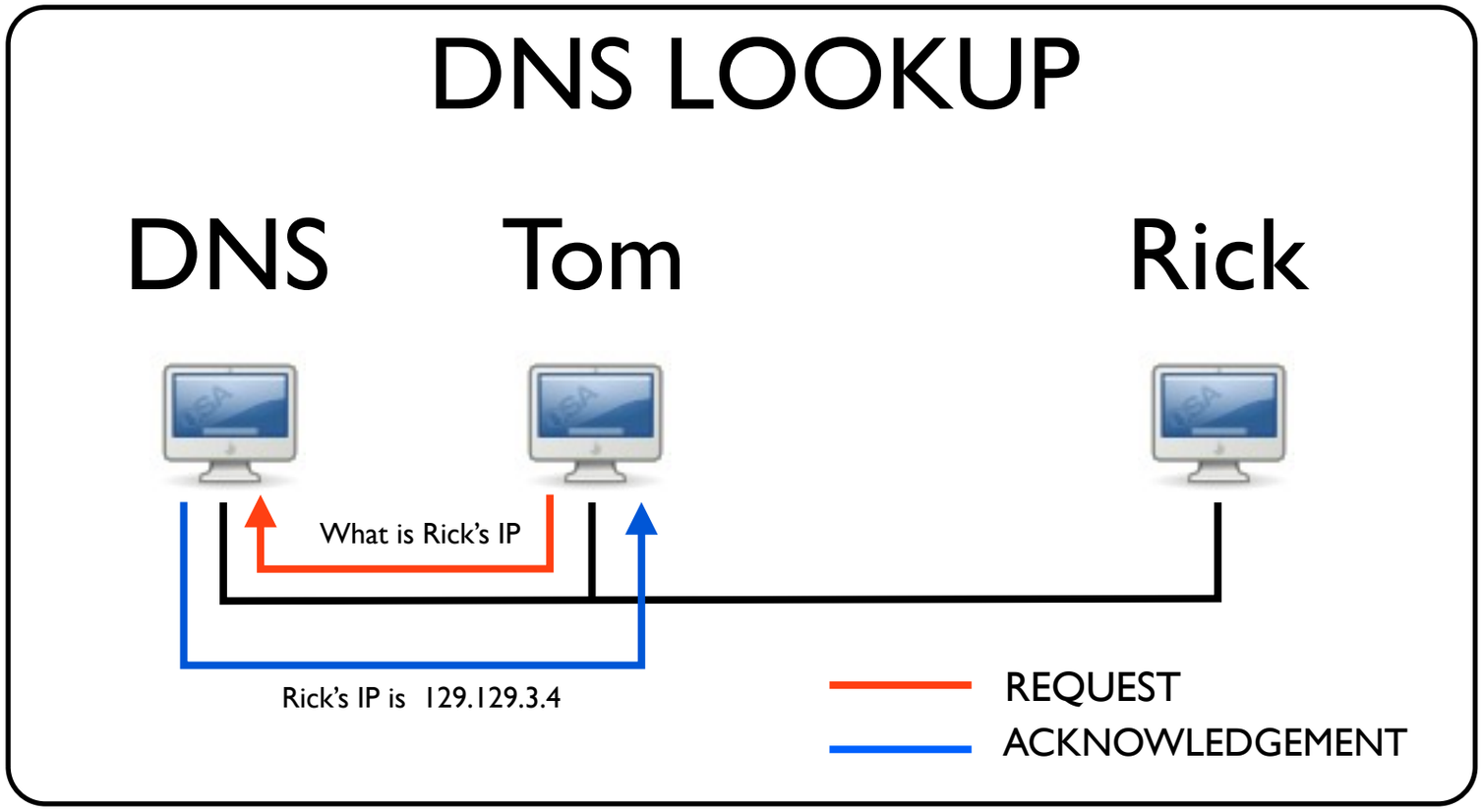
ROUTING TABLES



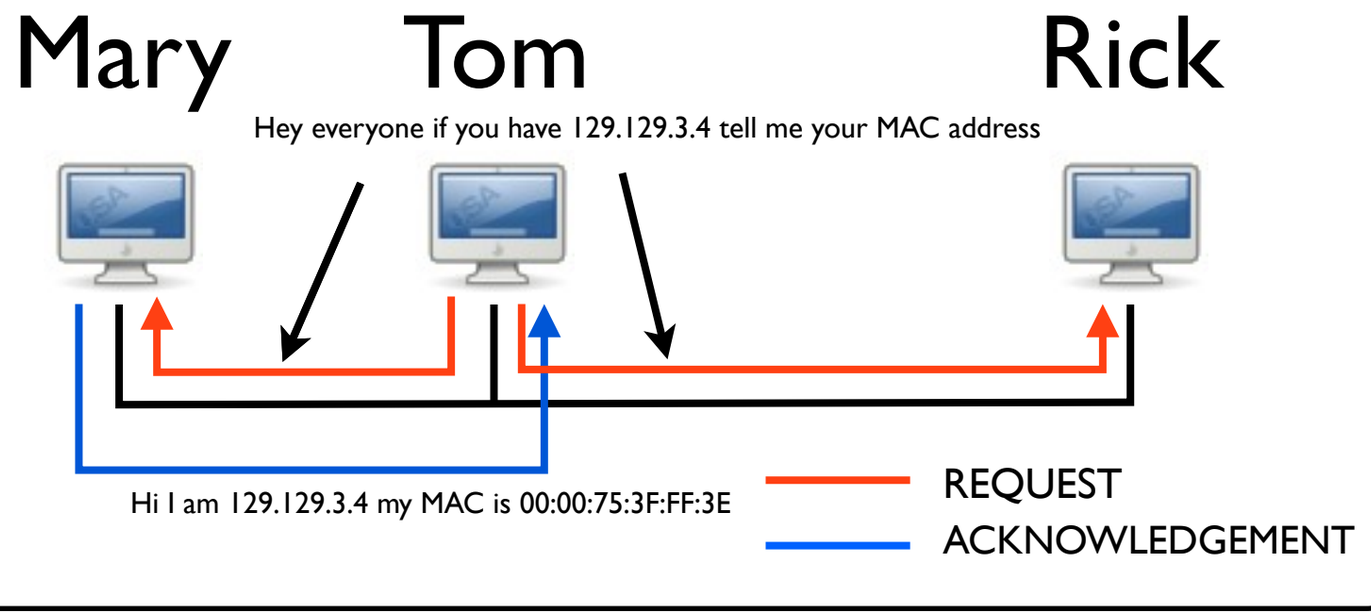
SUBNET	OUT INTERFACE	NEXT HOP IP ADDRESS
129.129.4.0	Serial 0	129.129.2.7

SUBNET	OUT INTERFACE	NEXT HOP IP ADDRESS
129.129.4.0	Serial 1 (FR)	129.129.3.1

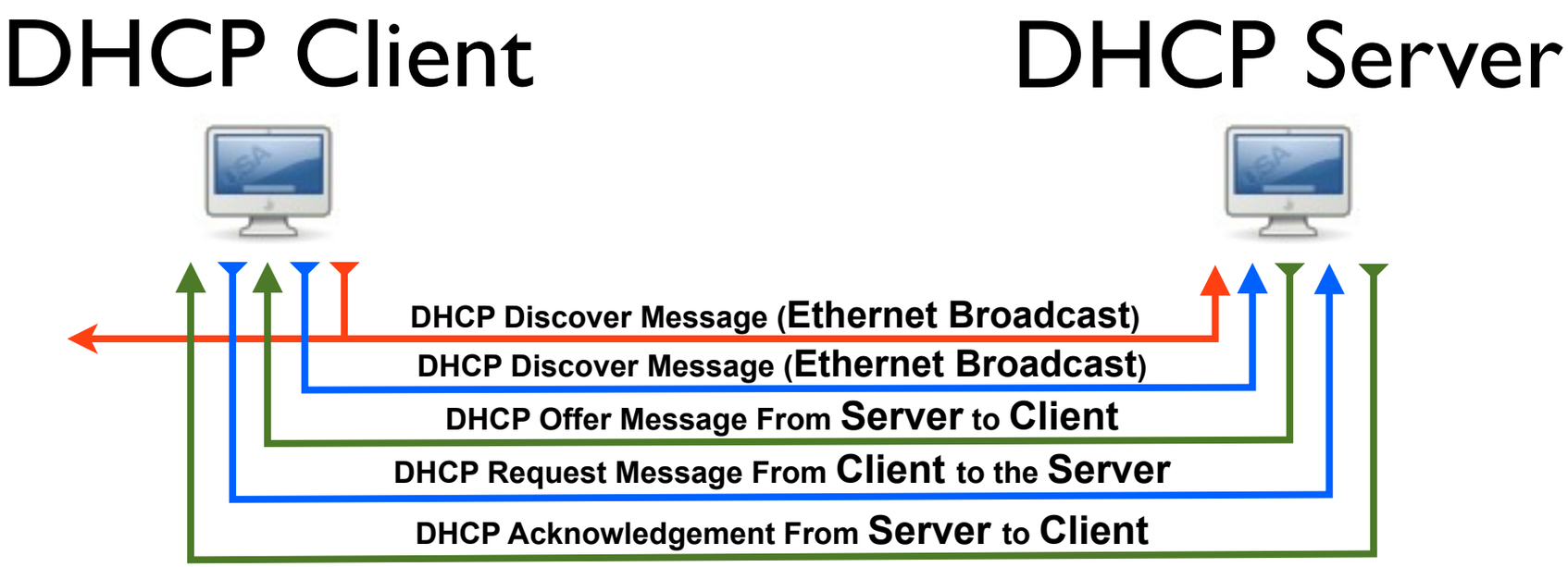
SUBNET	OUT INTERFACE	NEXT HOP IP ADDRESS
129.129.4.0	Ethernet 0	NA


DNS LOOKUP
DNS
Tom
Rick
What is Rick's IP
Rick's IP is 129.129.3.4
REQUEST
ACKNOWLEDGEMENT

ARP PROCESS


Mary
Tom
Rick
Hey everyone if you have 129.129.3.4 tell me your MAC address
Hi I am 129.129.3.4 my MAC is 00:00:75:3F:FF:3E
REQUEST
ACKNOWLEDGEMENT

DHCP PROCESS

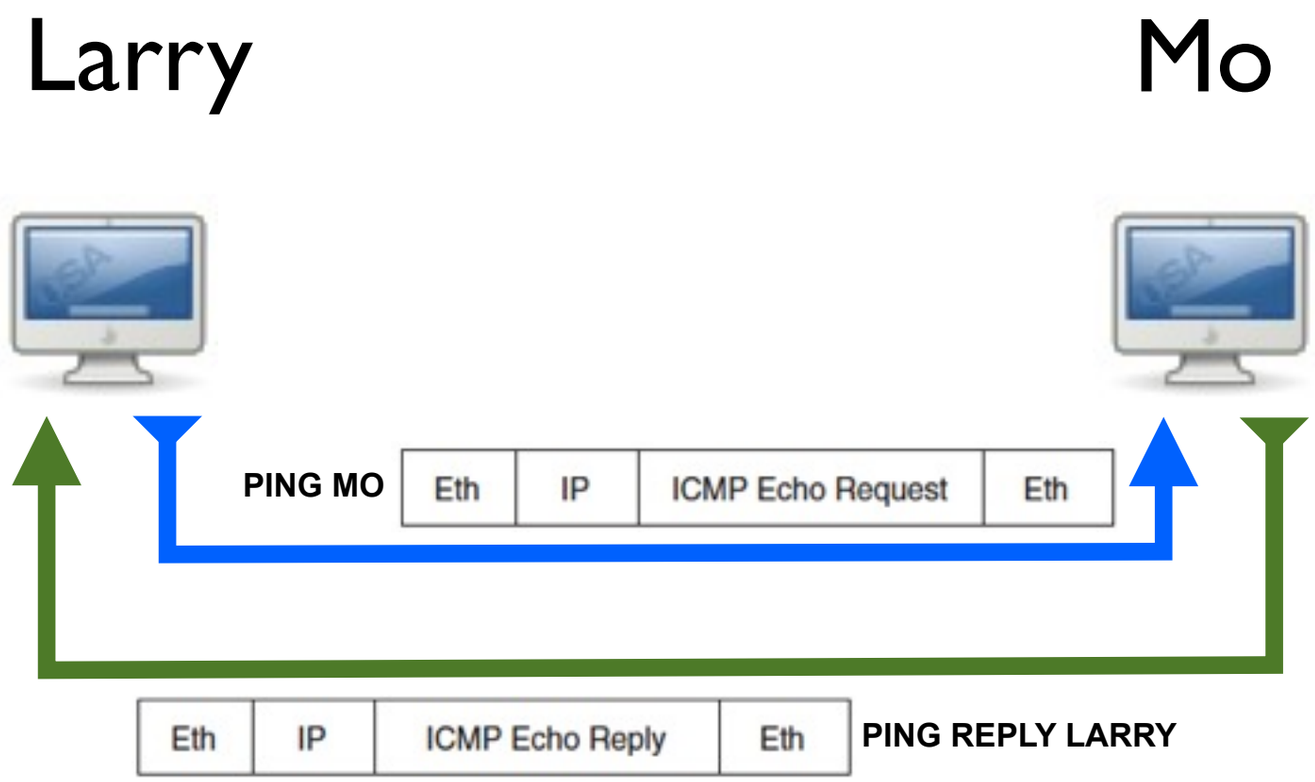


Dynamic Hardware Configuration Protocol

This protocol is used on a network to provide addresses to individual end user PC's.

Servers almost always have a private static address.

ICMP PING



One of the most basic tools
used on IP networks is the PING.

IP ADDRESSING & SUBNETTING

IP Version 4
ADDRESS

32 bits long

4 bytes usually **converted to decimal**
for applications or tools

12.12.12.12
is easier to read and remember then

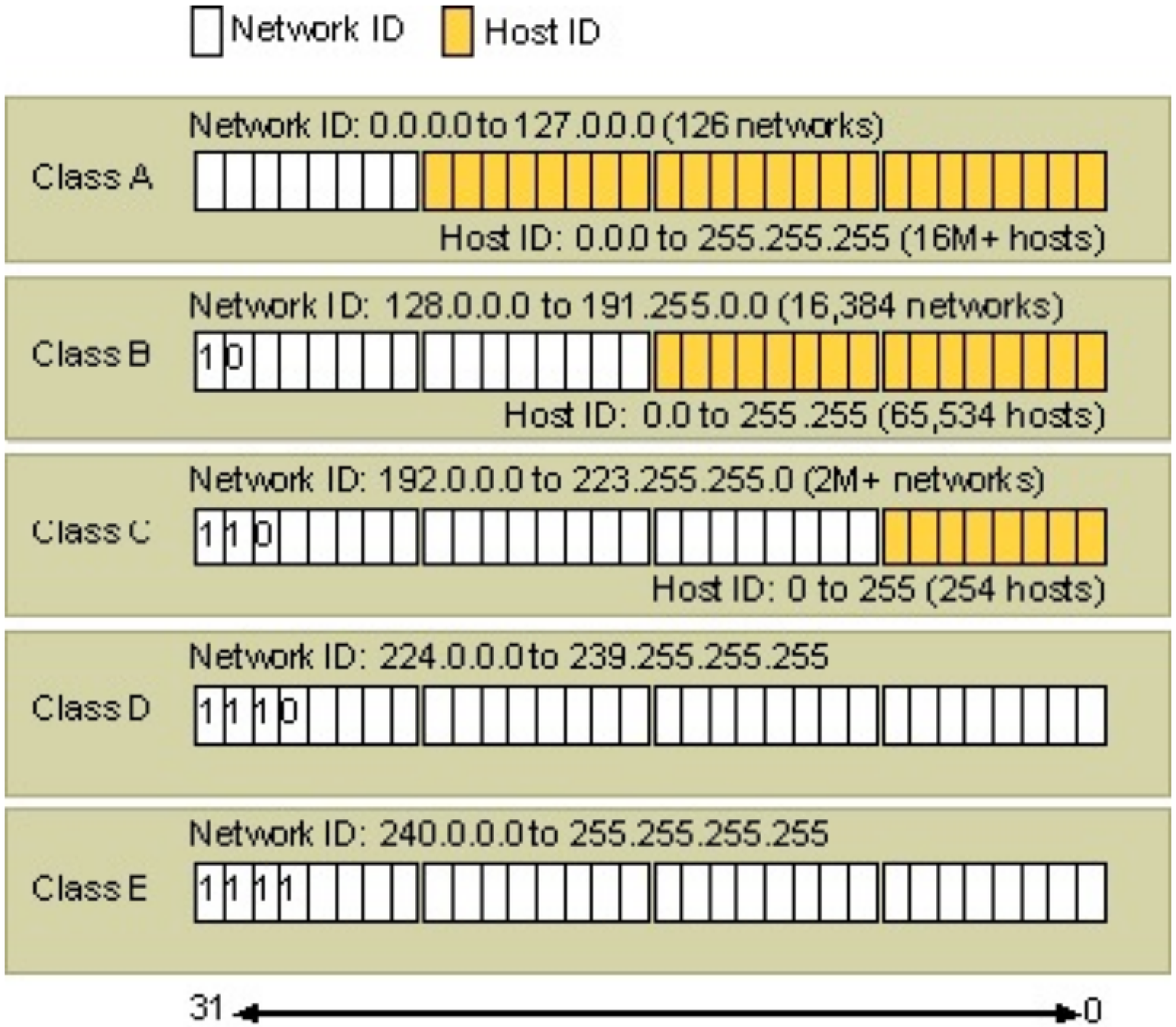
00001100. 00001100. 00001100. 00001100

IP Addresses are separated into **three main** classes.

A, B, and C

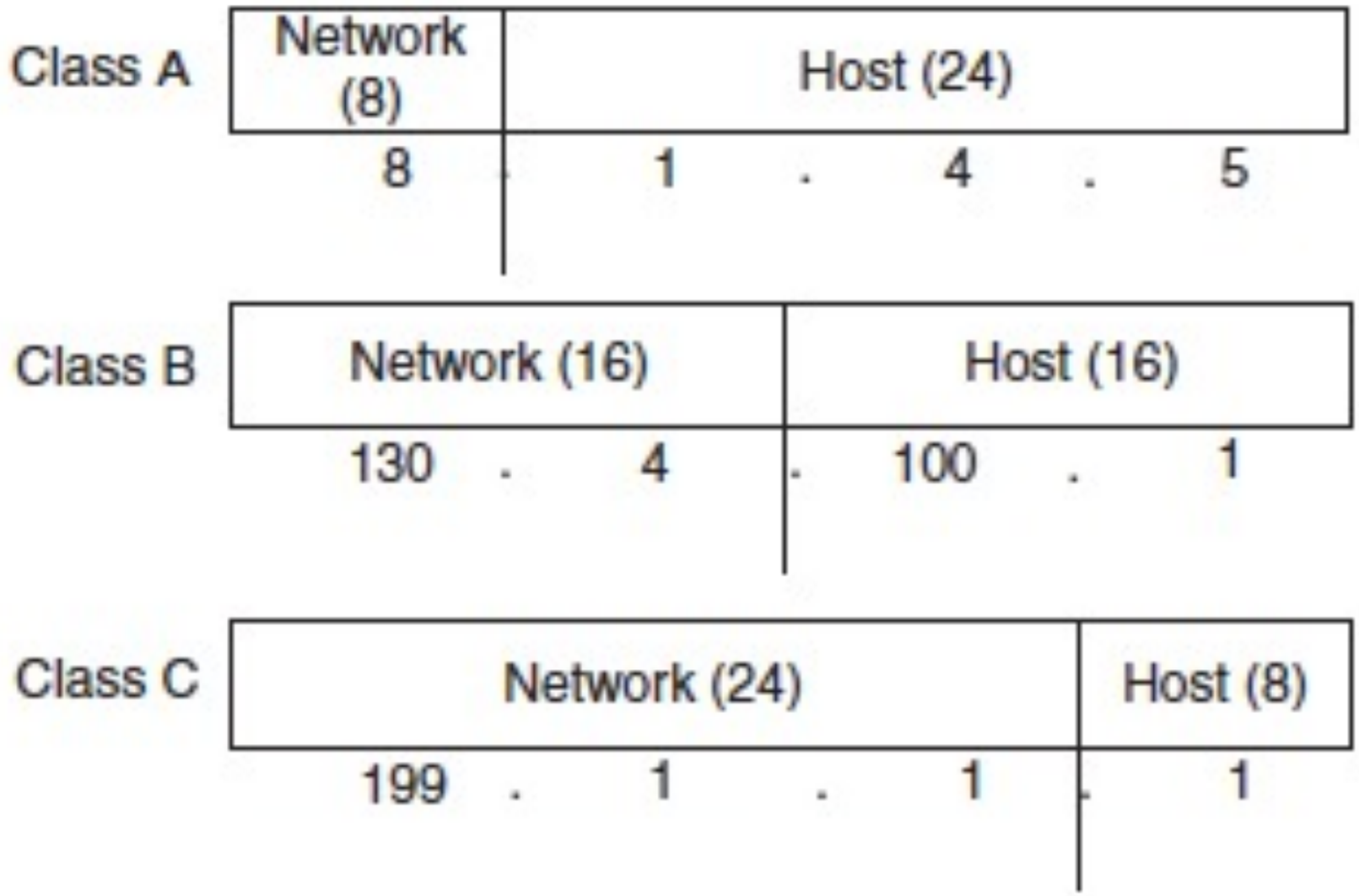
There are two more ;
Multicast (D) and Experimental (E)
We will focus on A, B, and C.

IP ADDRESS CLASSIFICATION



Only Class A, B,C are commonly used.
Class D is used for multicasting

IP Networks have two parts. Network and Host.



Private IP ranges of each Class

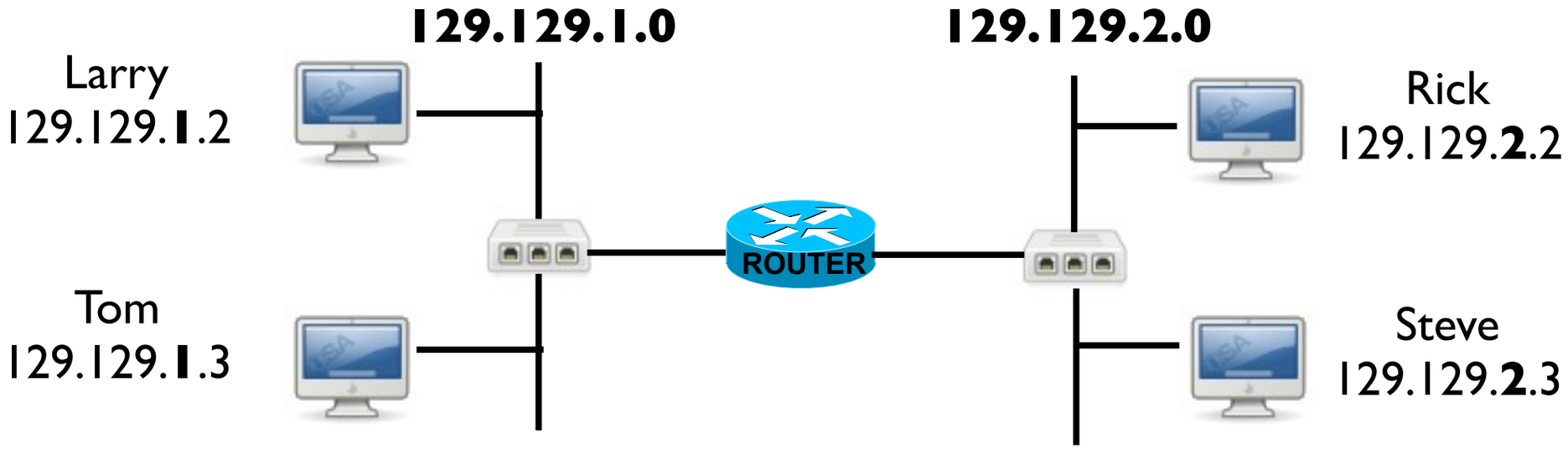
These addresses **cannot** be routed to the public Internet

Private IP Networks	Class of Networks	Number of Networks
10.0.0.0	A	1
172.16.0.0 through 172.31.0.0	B	16
192.168.0.0 through 192.168.255.0	C	256

Each network that hangs of a port on a ROUTER is a separate SUBNET.

The ROUTER interconnects subnets.

An entire network is built of ROUTERS and SWITCHES.

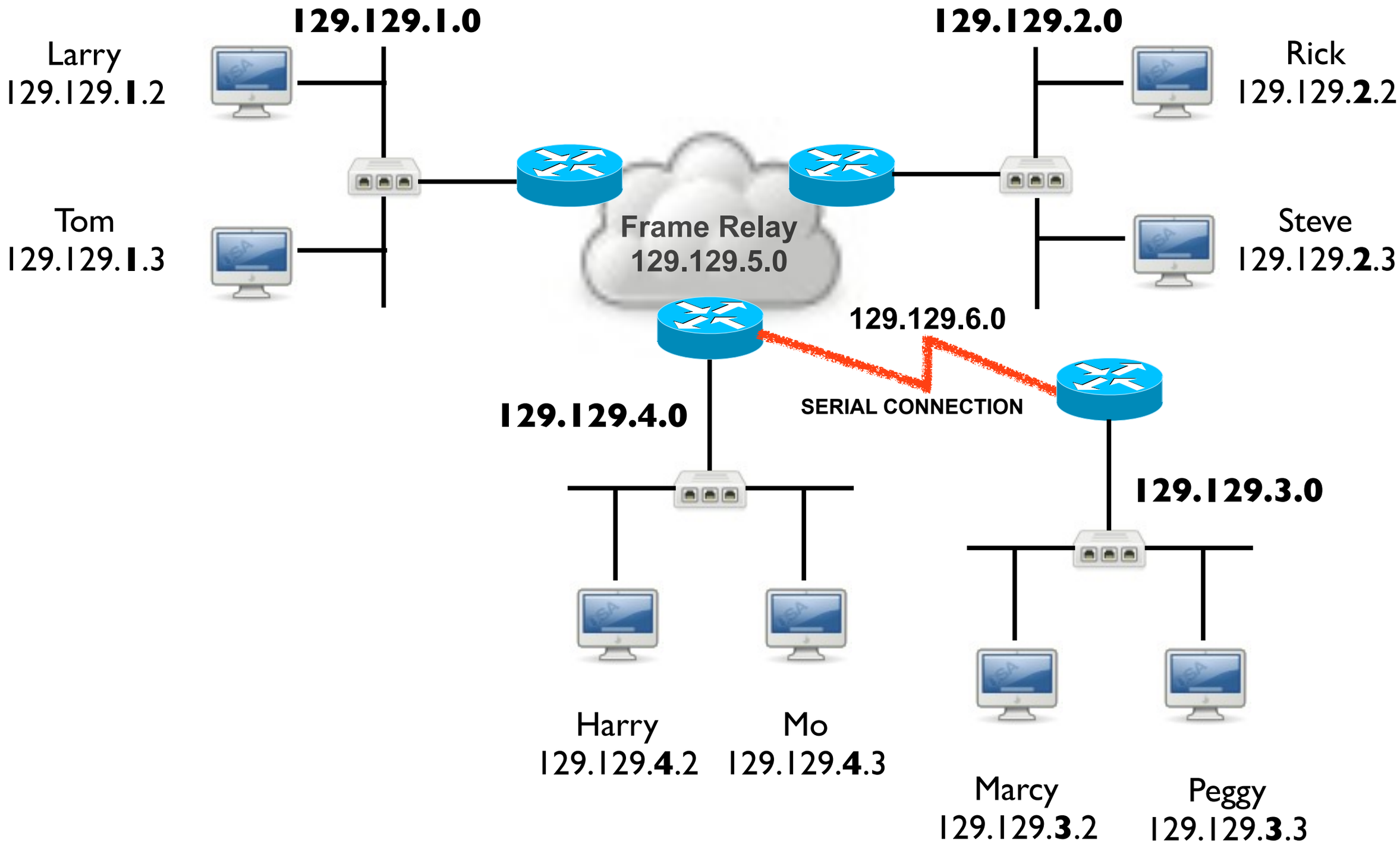


Here the router interconnects two networks 129.129.1.0 with 129.129.2.0

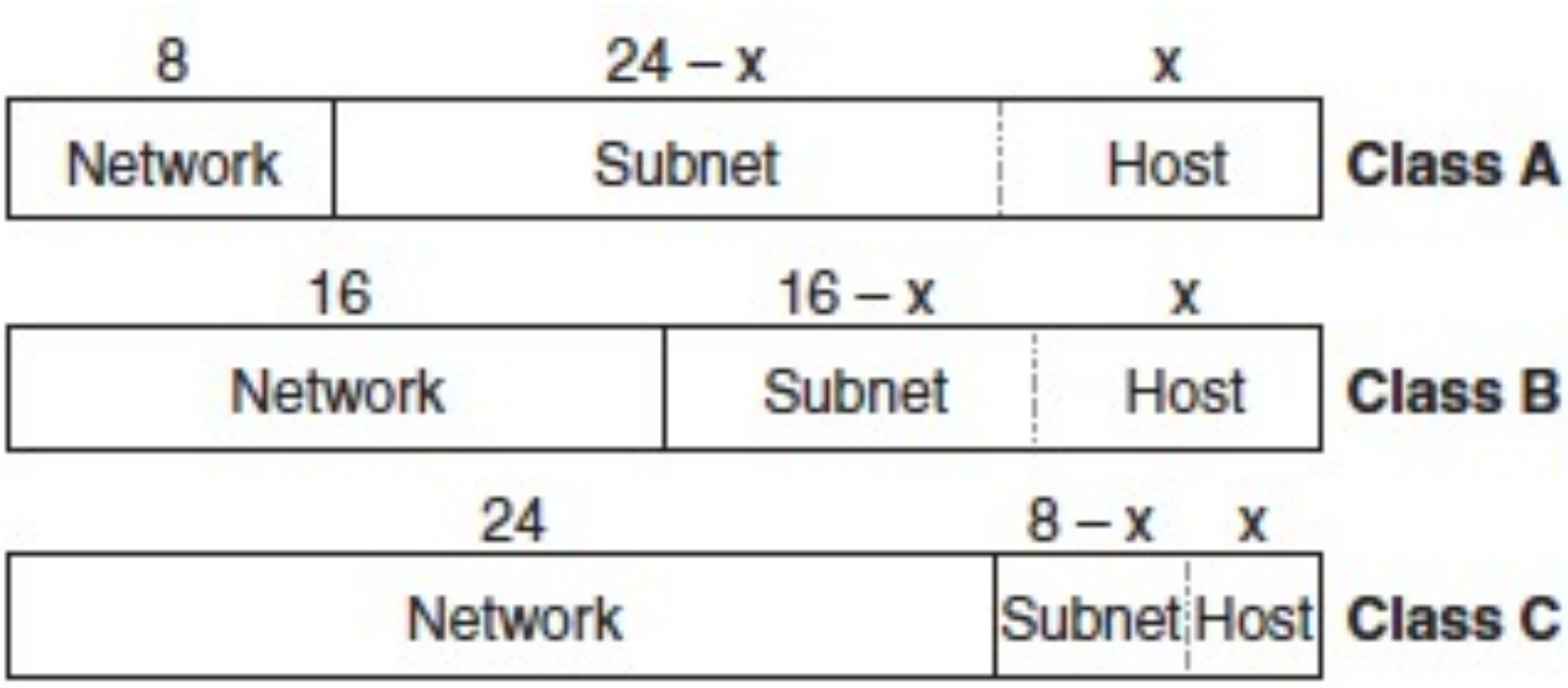
Each network that a router connects can also be referred to as an IP layer **broadcast domain**

When IP broadcasts are sent all the switches broadcast the message sent from the router.

Here we split up the **Class B 129.129.0.0** network
The natural subnet mask for this network will be
255.255.255.0



Subnetting


8
24 – x
x
Network
Subnet
Host
Class A
16
16 – x
x
Network
Subnet
Host
Class B
24
8 – x
x
Network
Subnet
Host
Class C

Subnetting **Class C** Network

255.255.255.0 Natural **Class C** Subnet Mask

Number of Subnet Bits	# of Subnets	Host Bits	Bit Pattern 11111111.11111111.11111111.xxxxxxxx	# of Hosts	DECIMAL MASK 255.255.255.xxxx	CIDR NOTATION
6	64	2	11111100	4 - 2	252	/30
5	32	3	11111000	8 - 2	248	/29
4	16	4	11110000	16 - 2	240	/28
3	8	5	11100000	32 - 2	224	/27
2	4	6	11000000	64 - 2	192	/26
1	2	7	10000000	128 - 2	128	/25