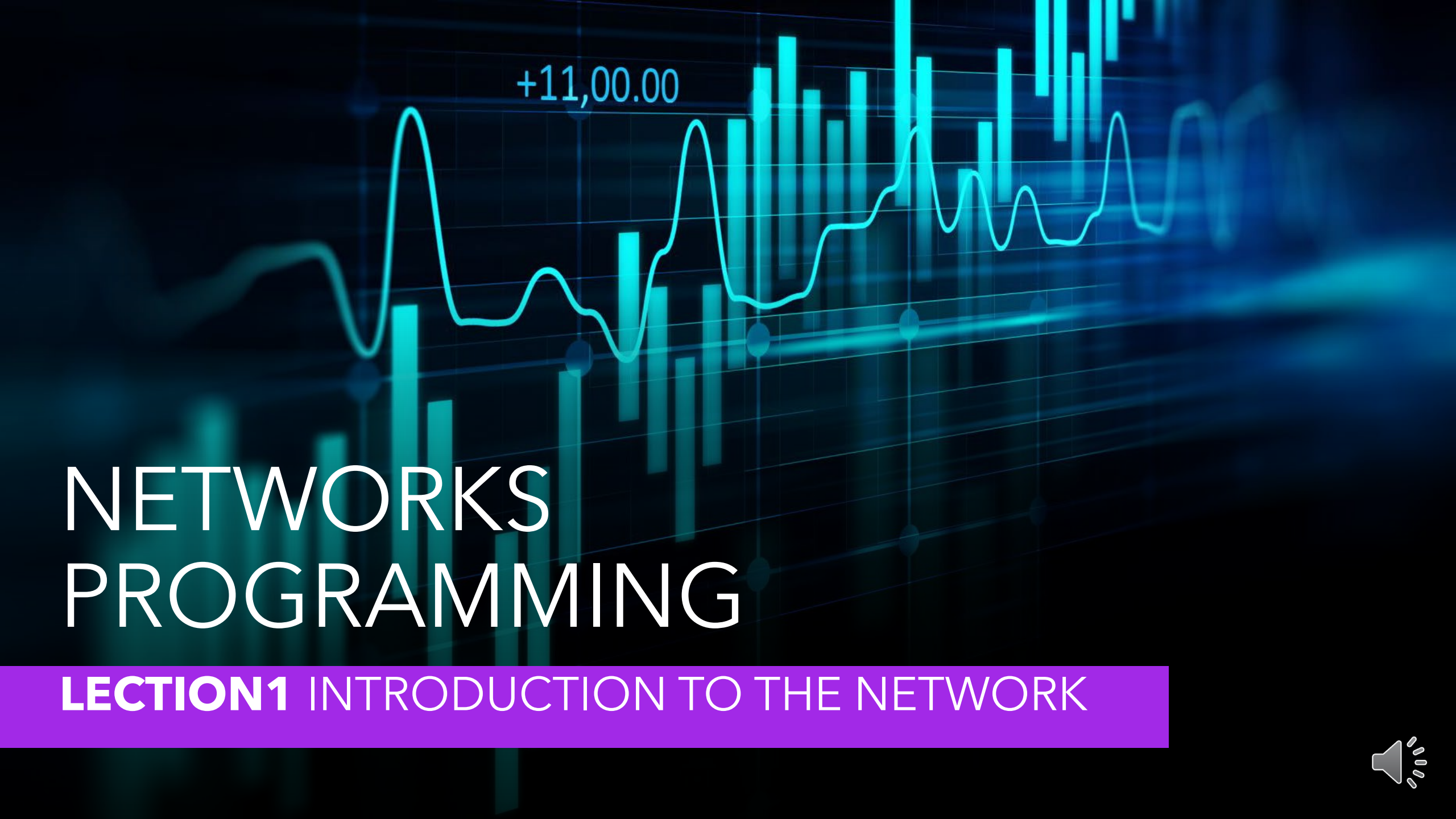


NETWORKS PROGRAMMING

LECTION1 INTRODUCTION TO THE NETWORK

LECTION OBJECTIVES

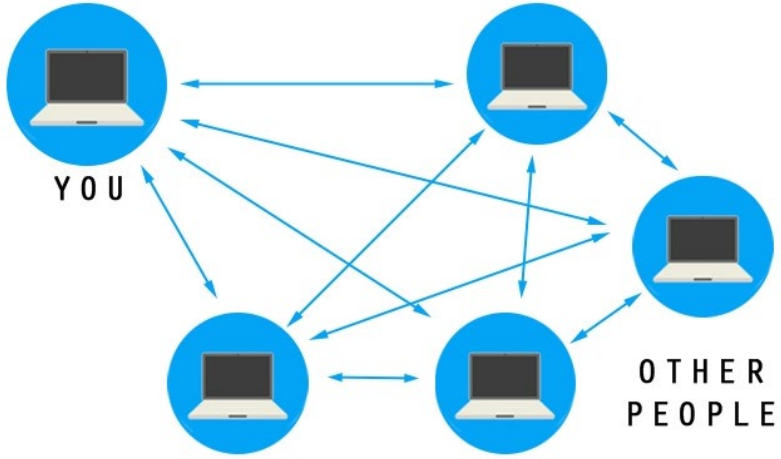
- What Can a Network Program Do
- Basic Network Concepts:
  - Network
  - Devices: NIC/Hub/Switch/Router
  - MAC address
  - IP address, Subnet mask
  - TCP/IP Network Model (5 Layers)
  - TCP vs. UDP
  - Protocols: ARP, RARP, DHCP
  - DNS
- Sending Message through Network Example

Apps = applications – the top level of Network

What Can a Network Program Do

Retrieve/Send Data

Searching the Web (automatically)



Peer to Peer interaction (games, chat, file sharing)

Custom Servers (server for your own needs)

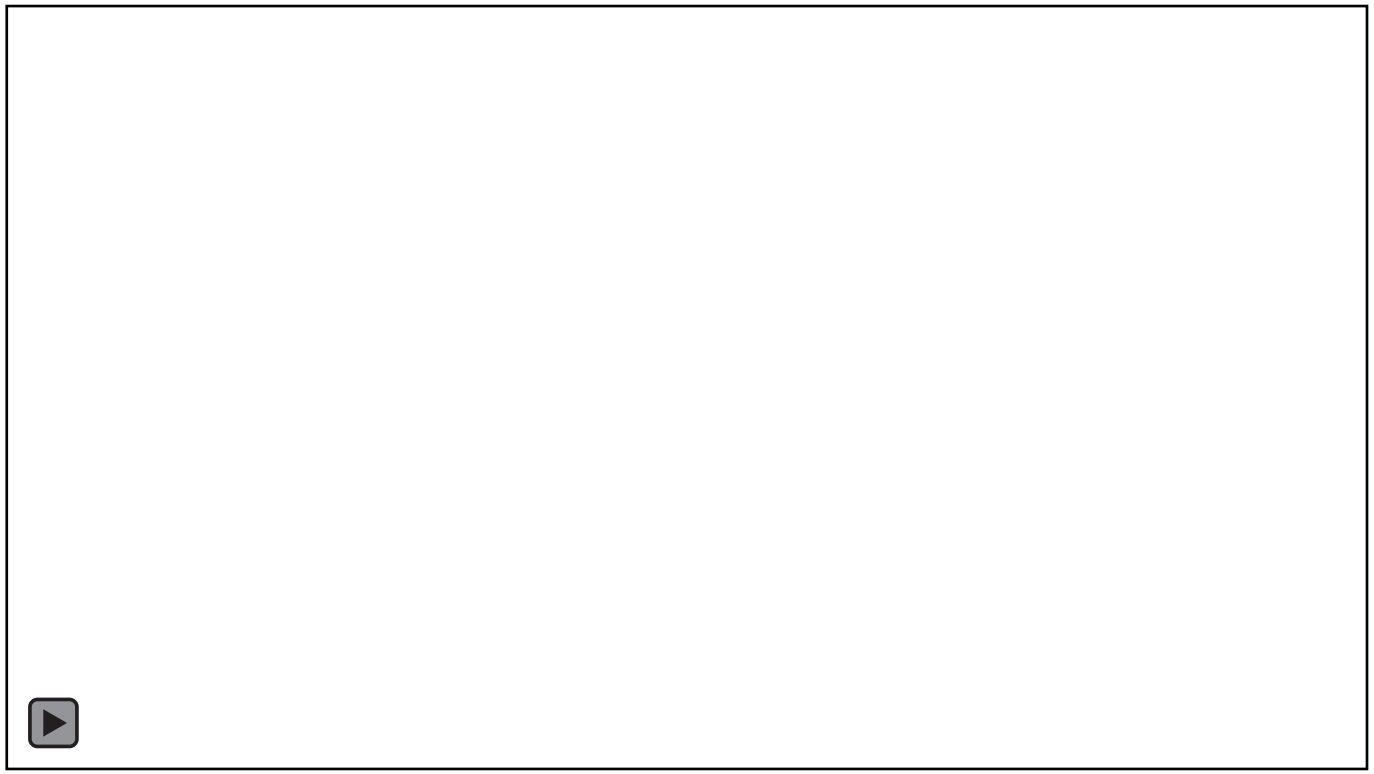
Electronic Commerce

Basic Networks Concepts

A network is a collection of computers and other devices that can send data to and receive data from each other, more or less in real time.

A network is often connected by wires, and the bits of data are turned into electromagnetic waves that move through the wires.

Wireless networks transmit data through infrared light and microwaves, and many long-distance transmissions are now carried over fiber optic cables.



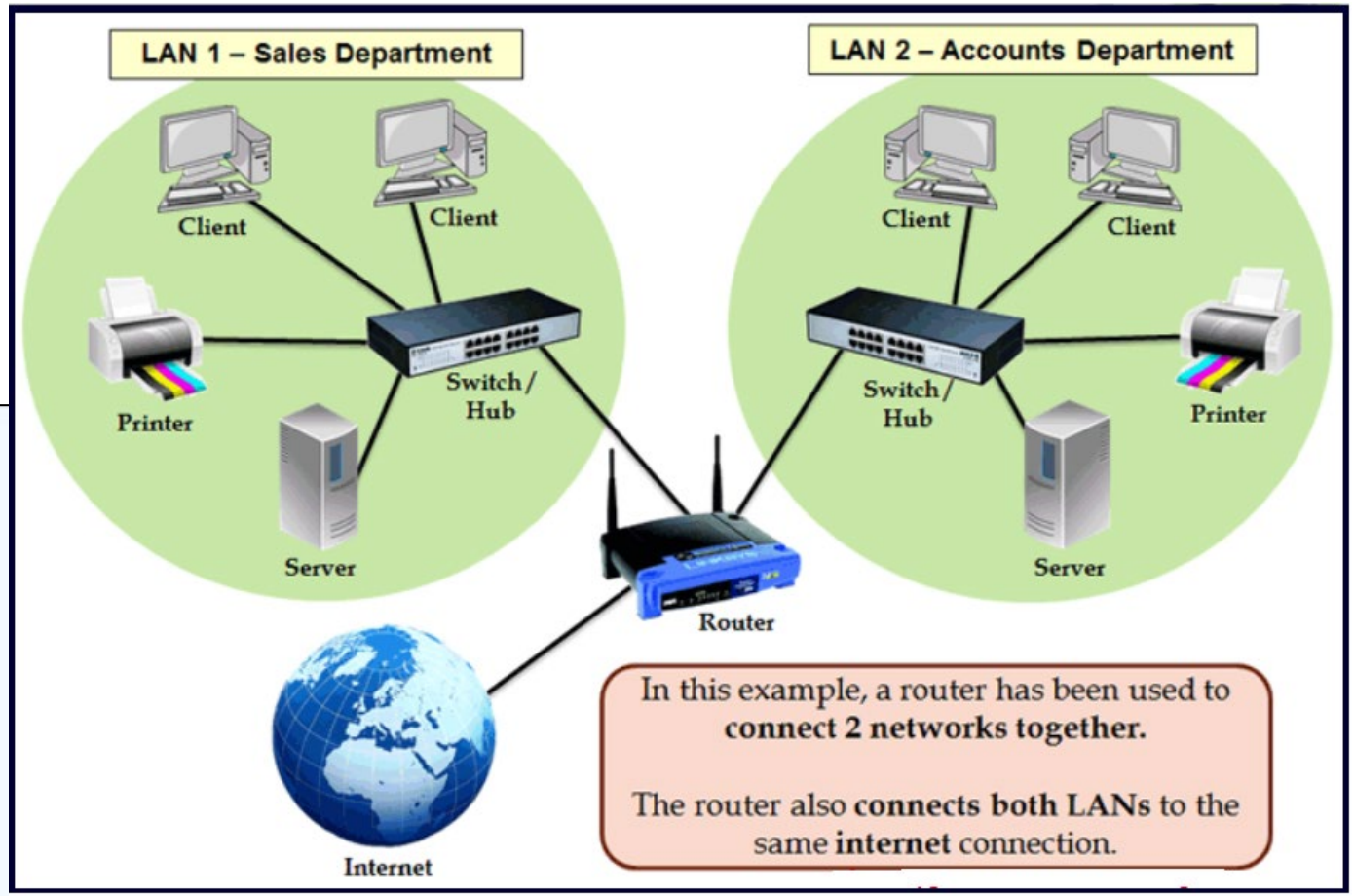
Basic Networks Concepts

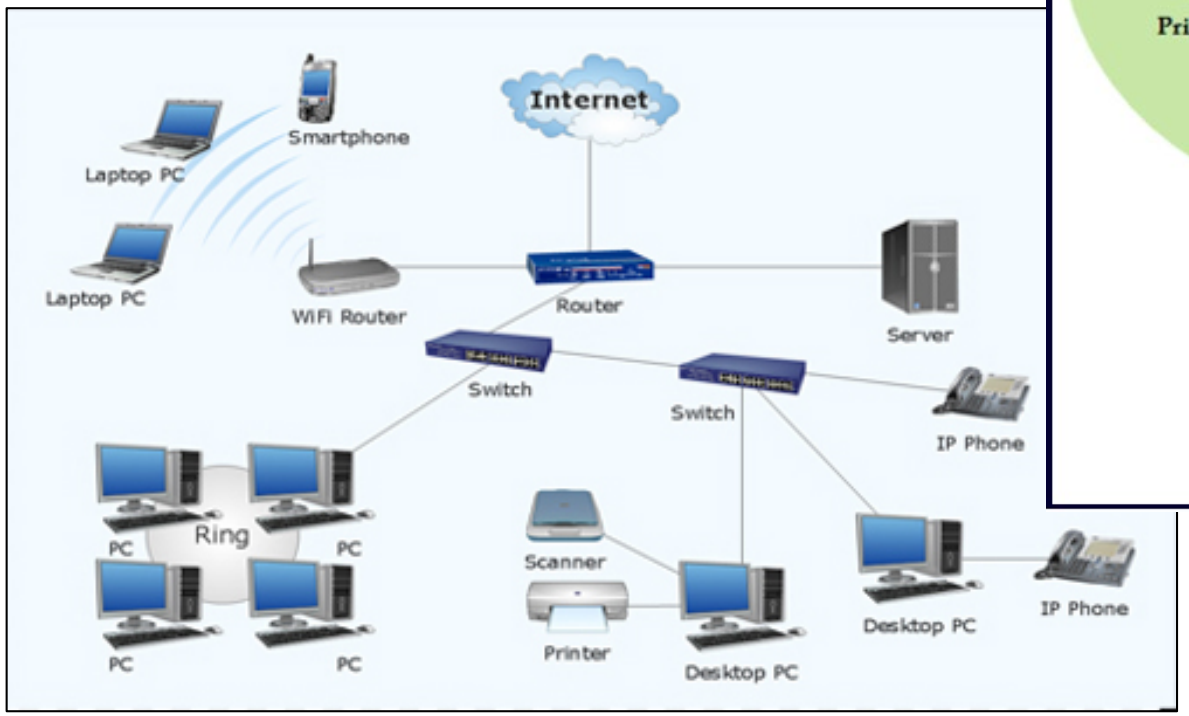
***LAN** = local area network*

***WAN** = wide area network (Internet)*

***Gateway:** Router (provides interoperability between different networks (LAN & WAN))*

***Hosts (Network Nodes):** Laptop PC, Server, PC, Desctop PC, Printer, Scanner, IP Phone…*





The **Internet** is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices.

What are network interface cards used for?

NIC

Network Interface Cards are used to **connect** individual **computers/devices** to a **network**.

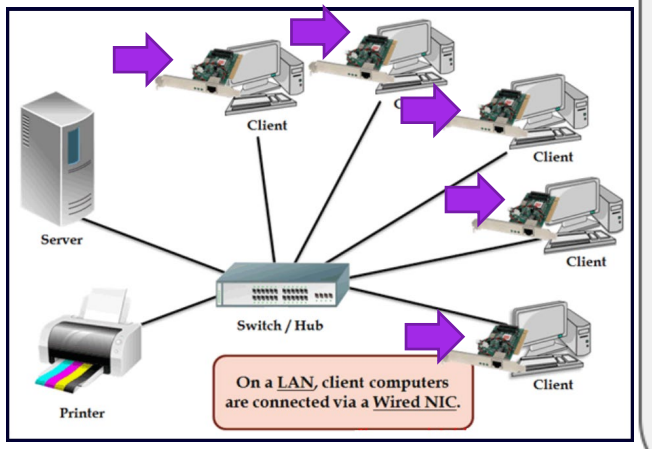
Modern computers usually come with network interface cards already **built-in**.

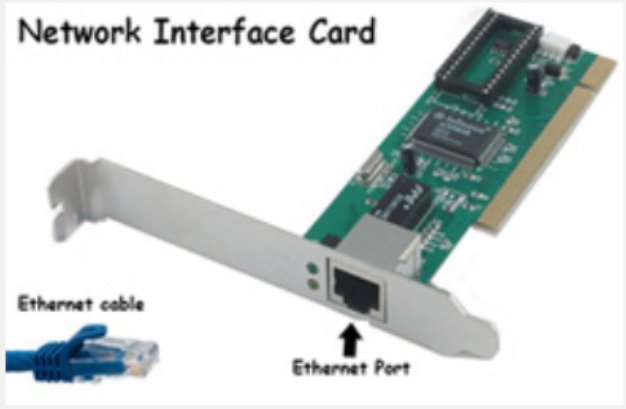
Network interface cards have **ports** which allow **network cables** to be **plugged in** and connect the computer to the network.

Note:

There are **two** types of network interface card:

- Wired network interface card (Where cables are used to connect computers)
- Wireless network interface card (Where computers are connected using Wi-Fi)



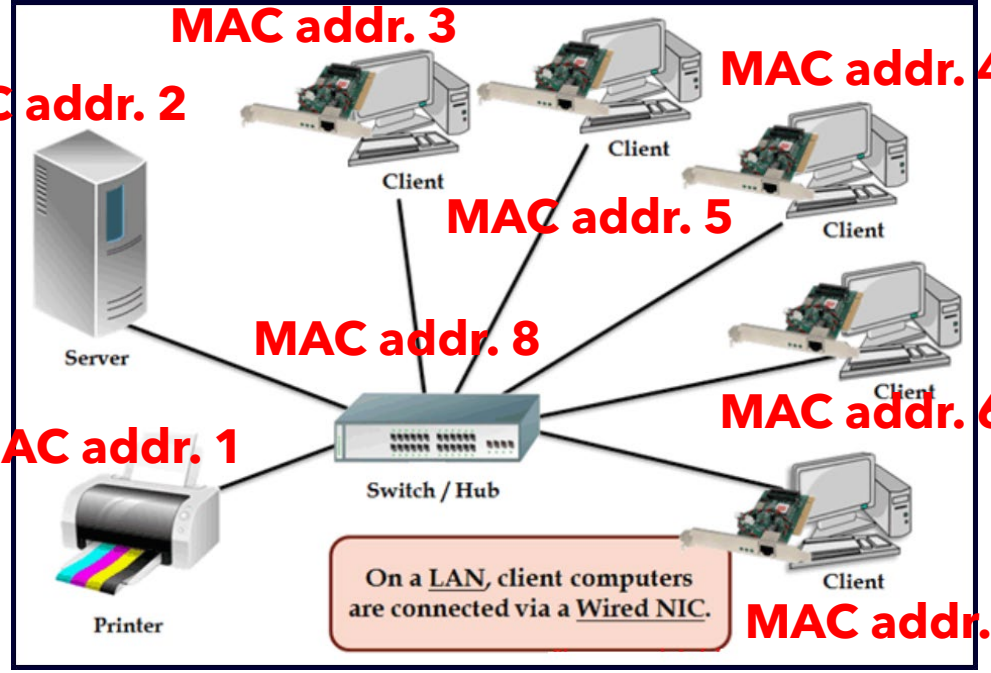


A wired network interface card connects computers to a network using cables.

A wireless network interface card connects computers to a network using Wi-Fi signals.

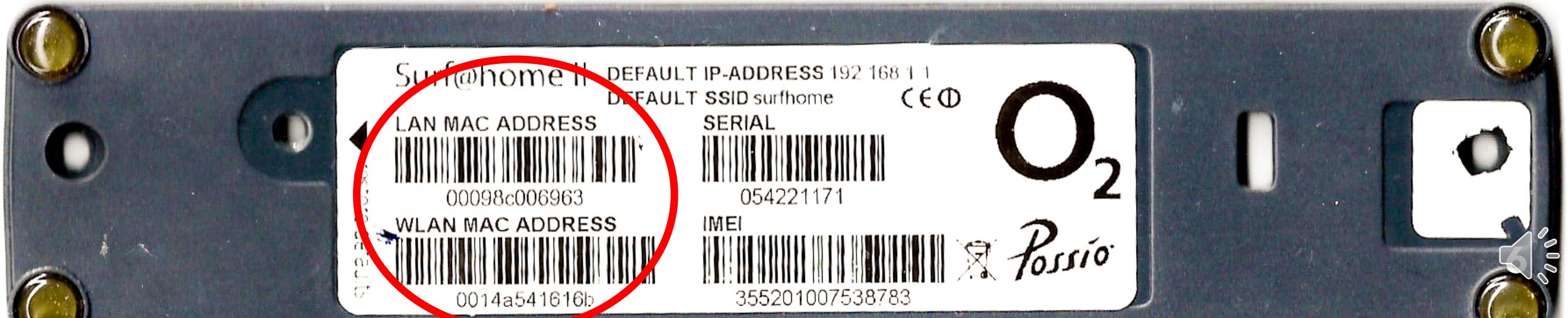
MAC Addr = 00:04:A3:4D:1C:73

A **media access control address** (**MAC address**) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

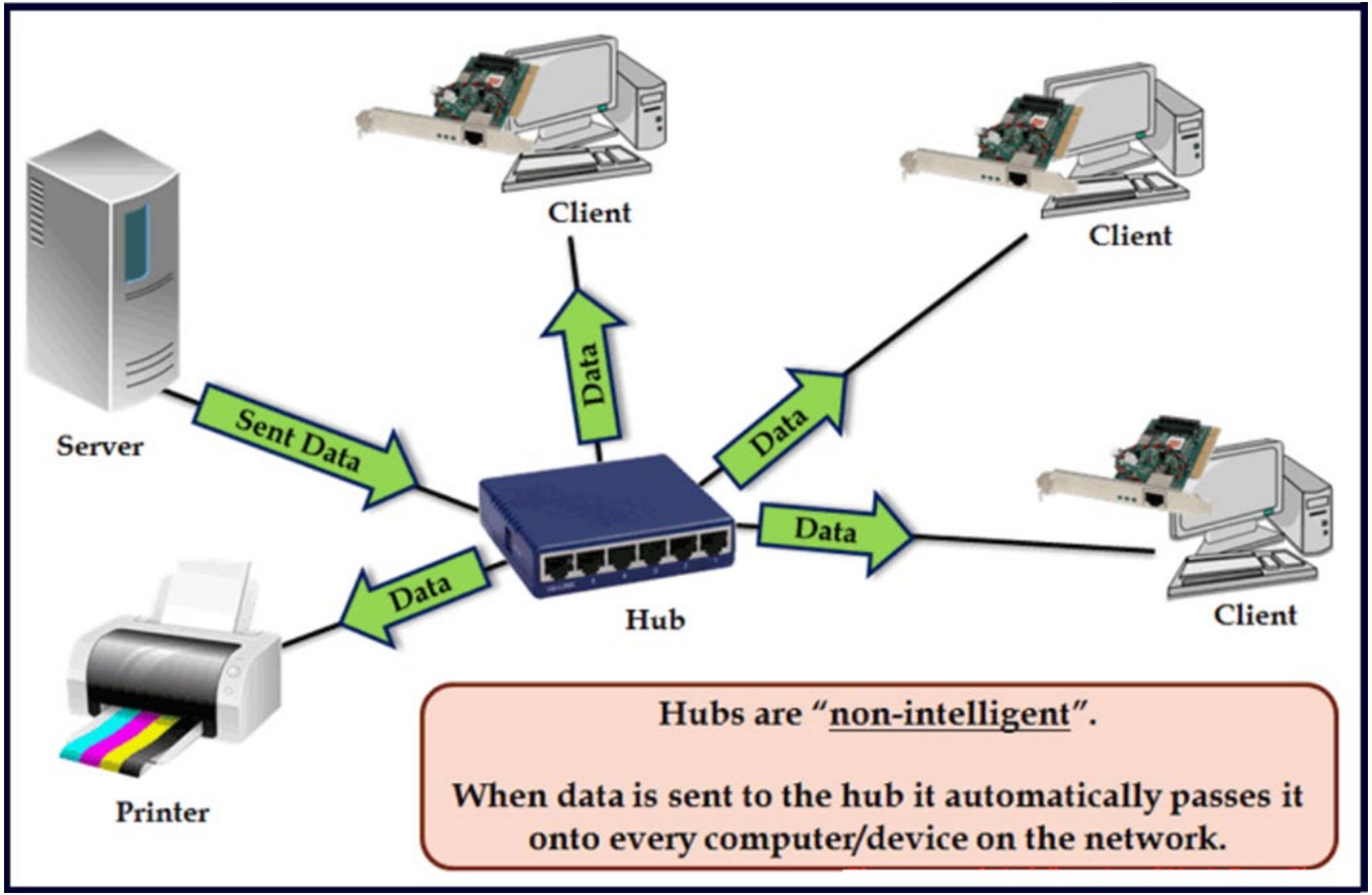


What is a MAC Address?

All hosts have a MAC (Media Access Controller) address. **MAC addresses** are fixed hardware based addresses that never change. They are programmed into a device when it is manufactured and all MAC addresses are globally unique. They are assigned and managed by the IEEE registration authority. MAC addresses contain six eight-bit fields expressed as hex numbers.



Hub


Client
Client
Server
Sent Data
Data
Data
Data
Data
Hub
Client
Printer
Hubs are "non-intelligent".
When data is sent to the hub it automatically passes it onto every computer/device on the network.

What are hubs used for?

Hubs allow computers and devices to plug into their ports in order to **connect** to each other and **share files**, **data** and **resources**.

Hubs are '**non-intelligent**' devices and they **don't manage** any of the data that flows through them.

When data gets sent to the hub, there is **no attempt** to **locate** the computer/device that the data is **meant for**.

The hub simply sends the data onto **every** computer/device on the network.

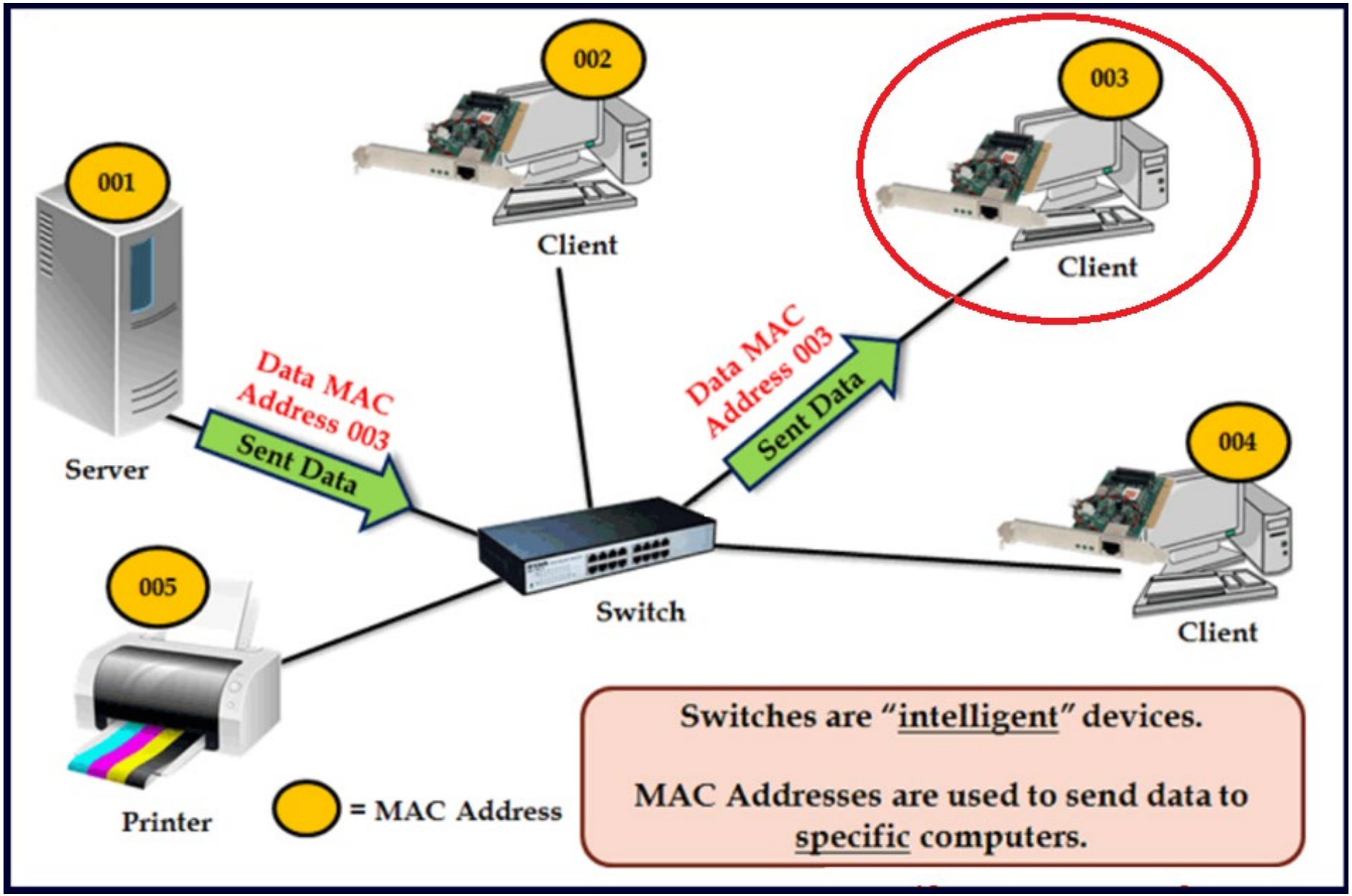
This means that every device on the network will **receive** the **same data** whether they requested it or not.

This lack of data management makes networks that are connected by hubs **very slow** because there is a lot of **unnecessary data** flowing around.

Note:

Hubs are **old technology** and have been replaced by switches which manage data more effectively and operate much faster (more on switches later).

Switch


002
003
001
Client
Client
Data MAC Address 003
Sent Data
Data MAC Address 003
Sent Data
004
Server
Switch
Client
005
Printer
= MAC Address
Switches are "intelligent" devices.
MAC Addresses are used to send data to specific computers.

What are switches used for?

Switches are **similar to hubs** in that they connect computers/devices to form a LAN.

However, switches are '**intelligent**' devices and transmit data around the network **more efficiently**.

How do switches manage network data?

#

How switches manage data is summarised below:

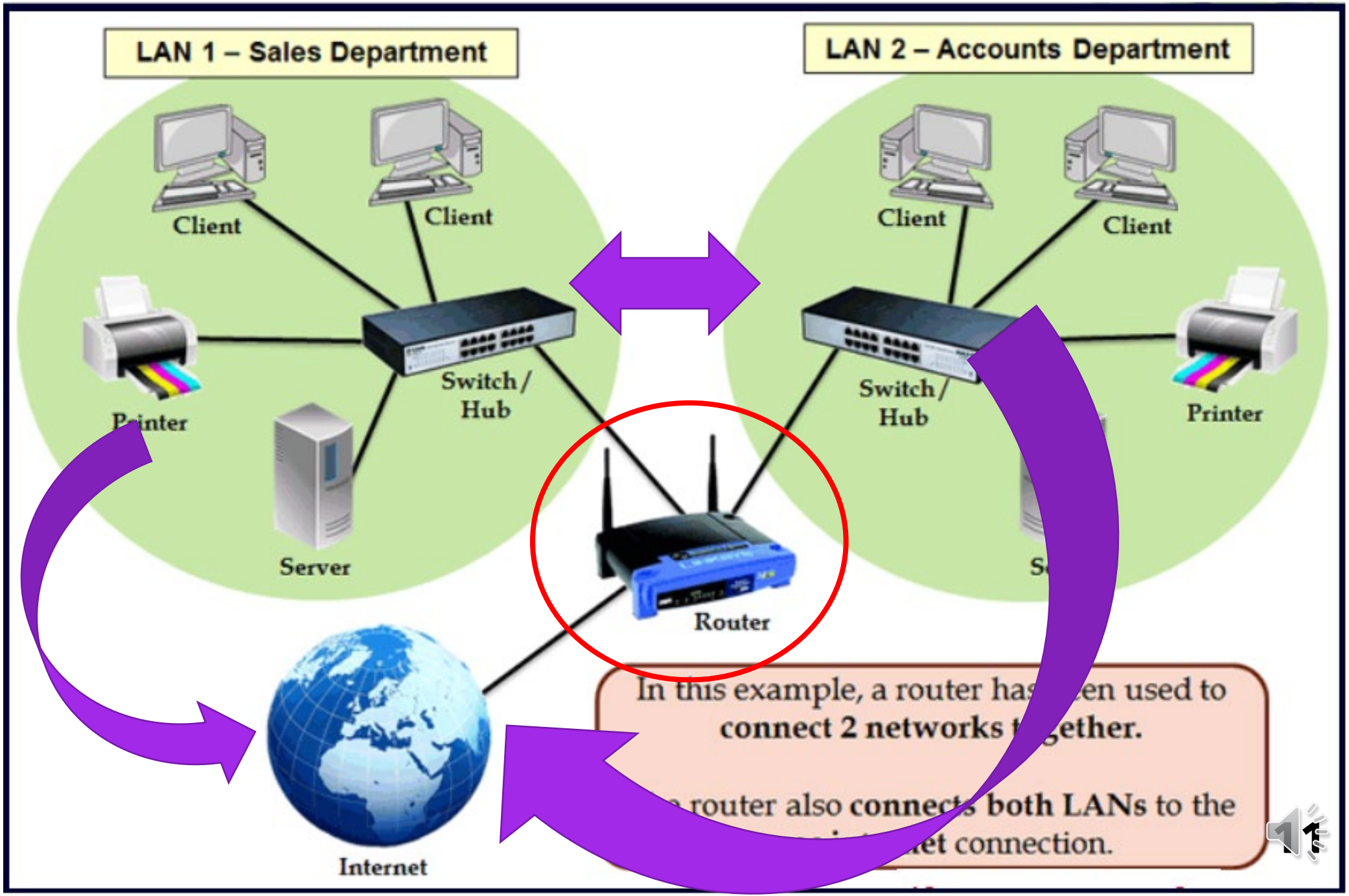
- Each network device has a **Media Access Control (MAC) address** which uniquely identifies it.
- Data sent to the switch contains the MAC address of the **sending device** and the MAC address of the **receiving device**.
- The switch will **check** these addresses and only send the data to the **relevant device** rather than to all devices.

!

See the image to the right for a picture example of how switches work

Because switches send data directly to the correct device, the amount of unnecessary data traveling around the network is **reduced** and the whole network **works faster**.

Router


LAN 1 – Sales Department
LAN 2 – Accounts Department
Client
Client
Client
Client
Switch / Hub
Switch / Hub
Printer
Server
Router
Internet
In this example, a router has been used to connect 2 networks together.
router also connects both LANs to the
connection.

What are routers used for?

Routers enable **data** to be **sent** (routed) between **different** types of **networks**.

For example:
A router could be used to connect a **LAN** (local area network) to a **WAN** (wide area network).

Routers are most commonly used to **connect computers** and **devices** to the **internet** (WAN).

Computers can connect to a router either through cables or wirelessly.

What exactly do routers do?

At this point, you can see that routers can **connect** different types of **networks** together and **send data** between them.

They can do this because they are **intelligent** devices and can perform the following functions:

- They can **read data** and decide **where** to send it
- They can decide on the **fastest route** in which to send the data
- They can make the **format** of the data **suitable** for the network where it is being sent.

This is where the name '**router**' comes from. They can **direct** data between networks using the **best/fastest route** possible.

IP Addresses

All computers and devices connected to the internet are assigned a **unique number** called an **Internet Protocol Address** (IP address).

A computer or device's IP address determines it's **exact location**.

The IP address of the device would depend on **where in the world** it connected to the internet from.

The list below shows some examples of different IP addresses in various countries:

- **Bermuda** - 64.147.80.0
- **United Kingdom** - 80.247.16.0
- **United States** - 168.99.0.0

Computers on the **same network** would share the **same first few numbers** of the IP address.

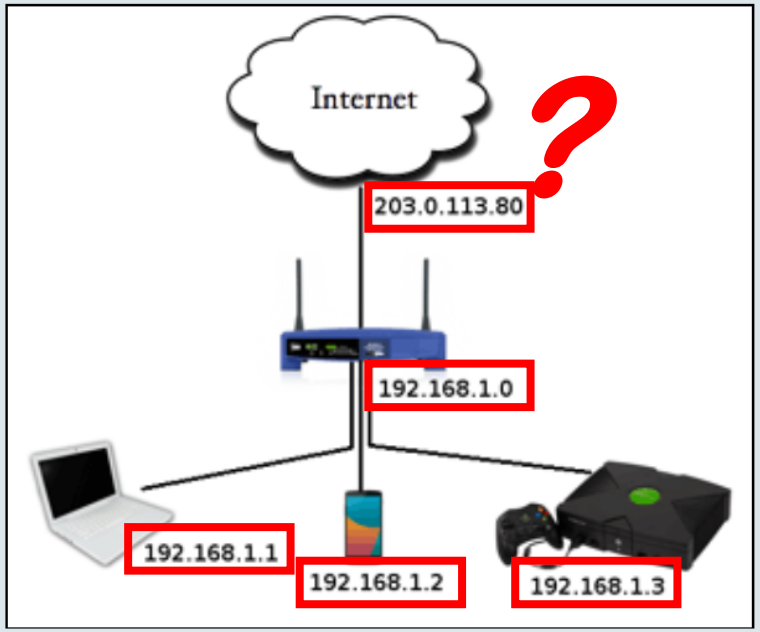
This is used to **locate** the **network** .

Different **devices** on the same network are uniquely identified by the **last few numbers** of the IP address.

On my school's network, IP address for individual devices could be assigned like this:

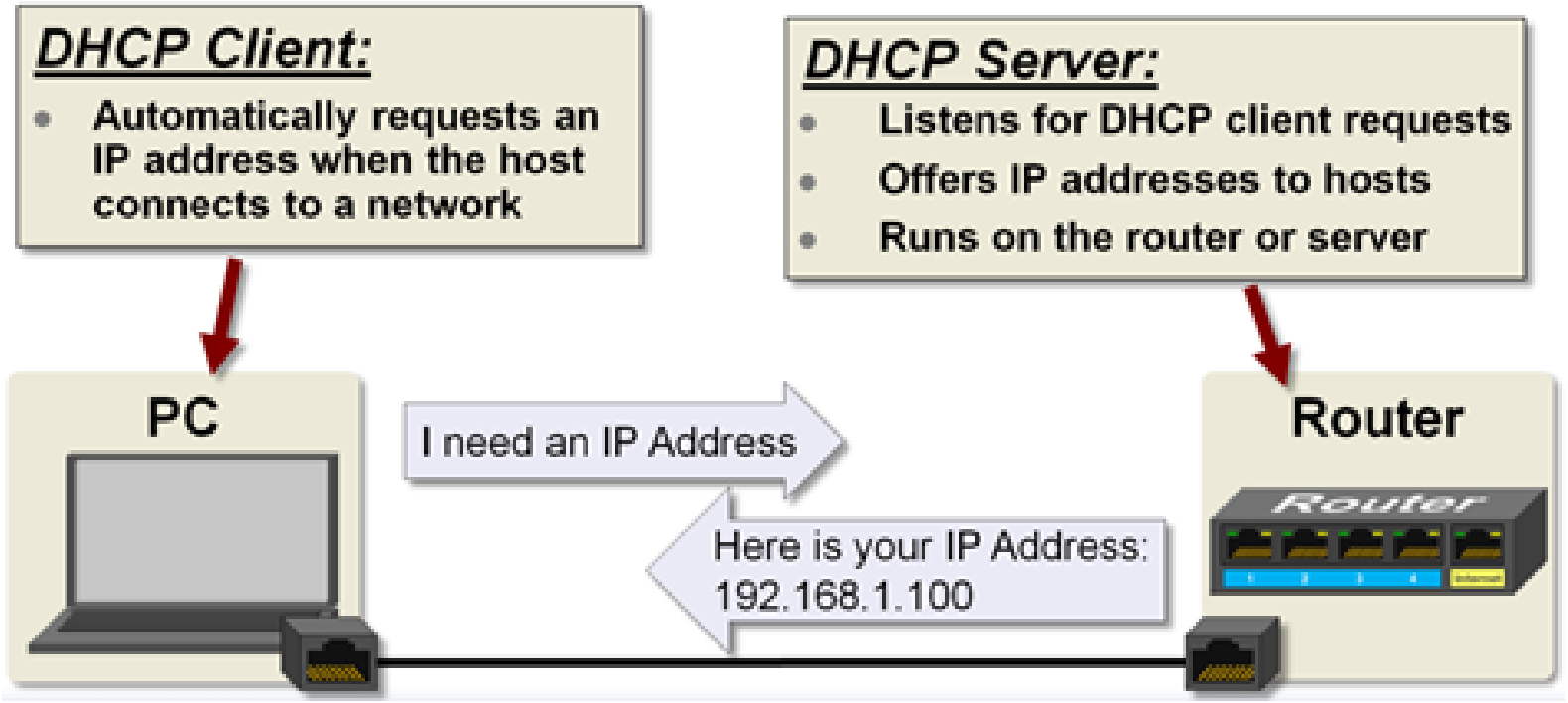
- **Desktop PC** - 64.128.80.**101**
- **Printer** - 64.128.80.**147**

This is used to **locate** individual **devices** on the network.



Routers use IP addresses to work out where to send packets of data.

IP addresses are used to uniquely identify every host (also known as a network node) on a Transmission Control Protocol/Internet Protocol (TCP/IP) network. They are virtual addresses assigned by routers. Each of the four 8-bit fields is represented by a decimal number ranging from 0 to 255. IP addresses are typically owned and controlled by a DHCP server running in the local network's router. Devices requesting to join a local network could be assigned any available local IP address and the assigned IP address could change at any time.



DHCP

Dynamic Host Configuration Protocol (DHCP)

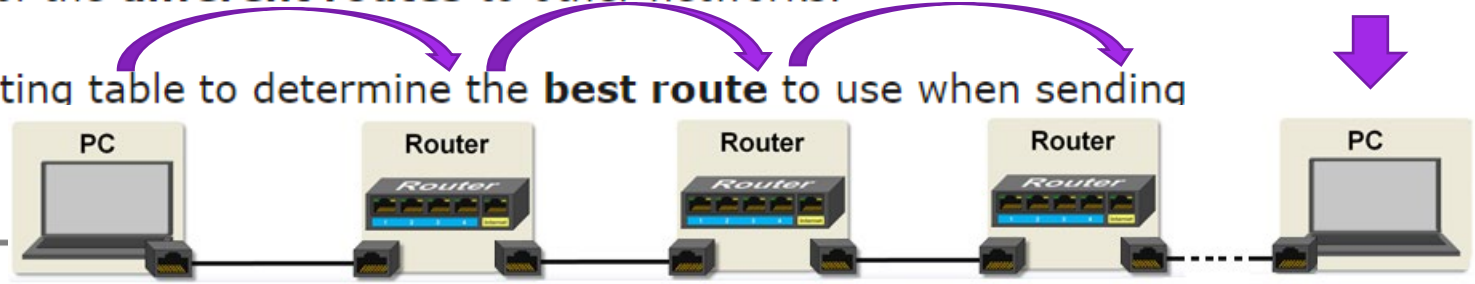
The dynamic host configuration protocol (DHCP) is the application responsible for requesting and offering IP addresses. A DHCP client automatically requests an IP address from a DHCP server when a network is detected. A DHCP server typically runs in a router and offers IP addresses to DHCP clients.

How does a router store IP addresses?

Routers store IP addresses in something called a **routing table**.

The routing table **lists** all of the **different routes** to other networks.

The router will use the routing table to determine the **best route** to use when sending data to another network.



How does a router send data between computers?

Routers send '**packets**' of data between computers on different networks.

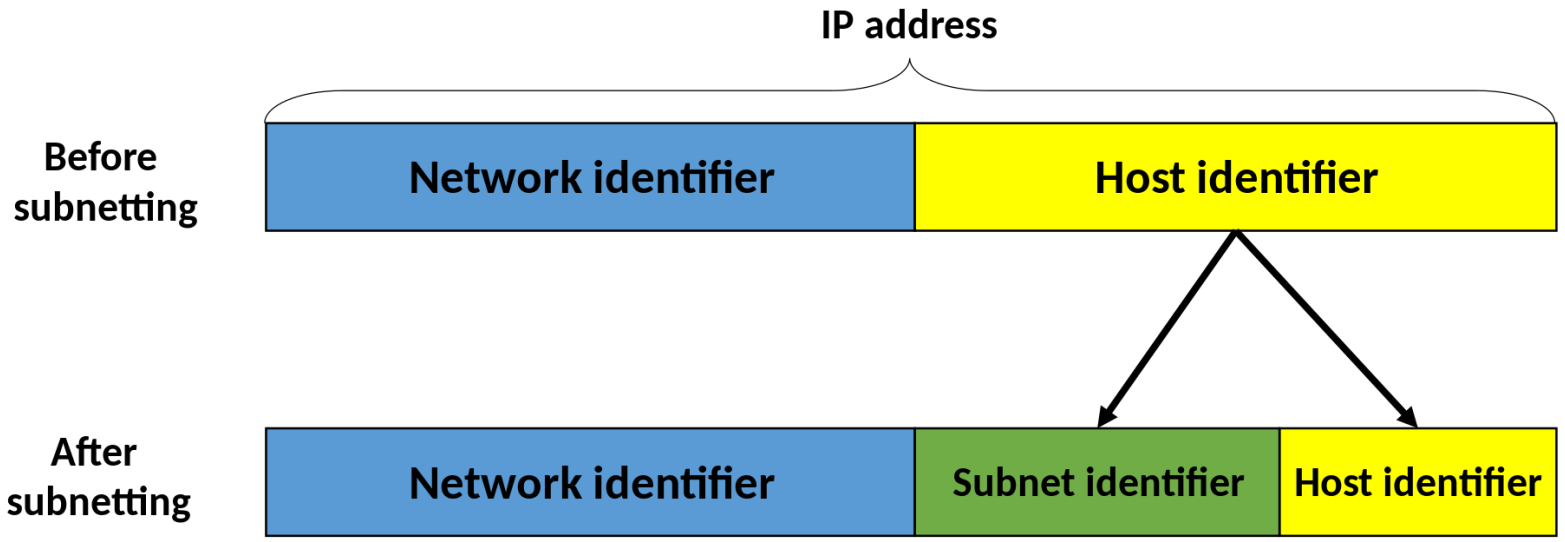
Each data packet contains the **IP address** of the computer/network that the data is being sent to.

The router will use the IP address to work out the **best route** in which to send the data to it's destination.

Remember:
The router will use the **first few numbers** of the IP address to determine the **location** of the **network** and the **last numbers** to determine which **device** on the network has requested the data.

The data will be received by **routers** on other networks which will read the IP address and **re-route** the data until it ends up at the **exact device** it was intended for.

Subnet Mask



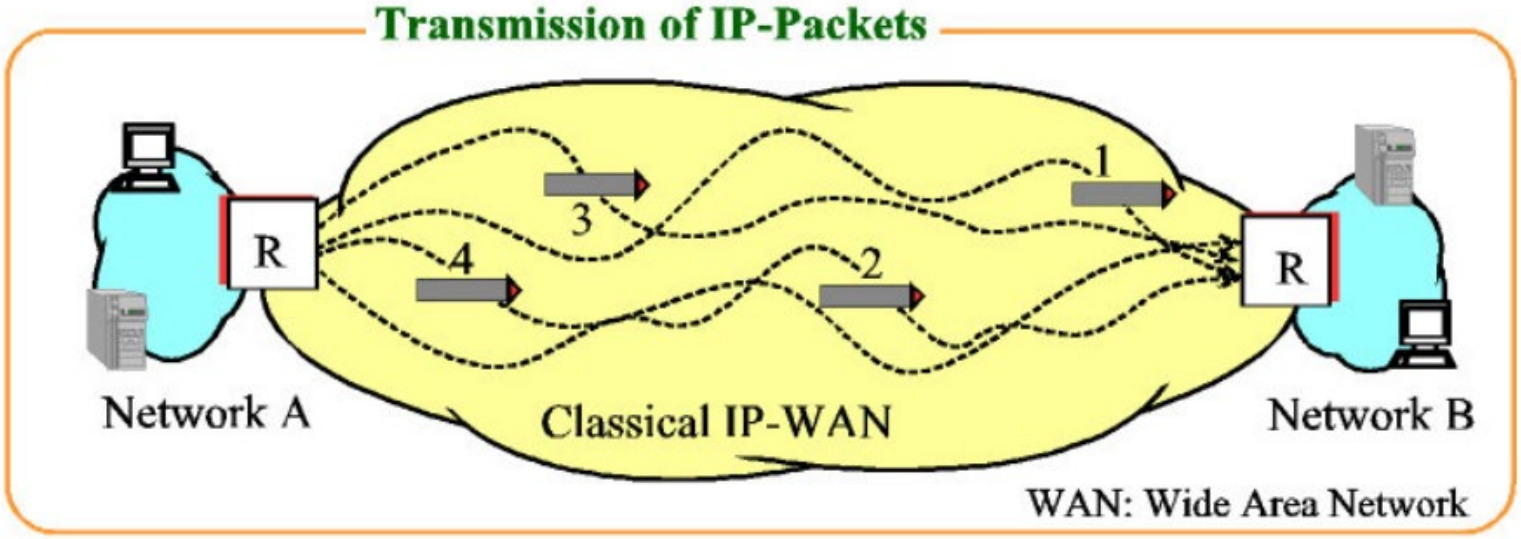
A **subnetwork** or **subnet** is a logical subdivision of an IP network.
For IPv4, a network may also be characterized by its **subnet mask** or **netmask**, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, *255.255.255.0* is the subnet mask for the prefix *198.51.100.0/24*.

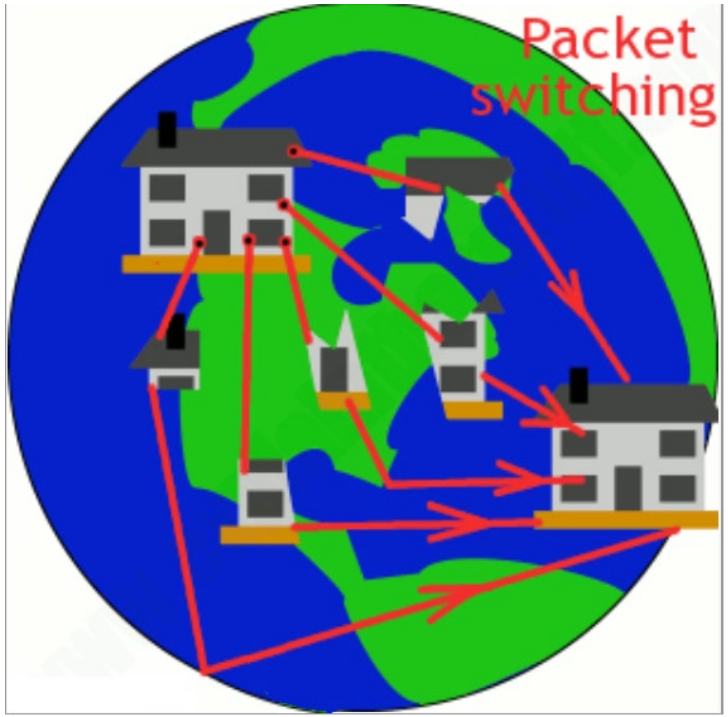
/24 ~ 255.255.255.0

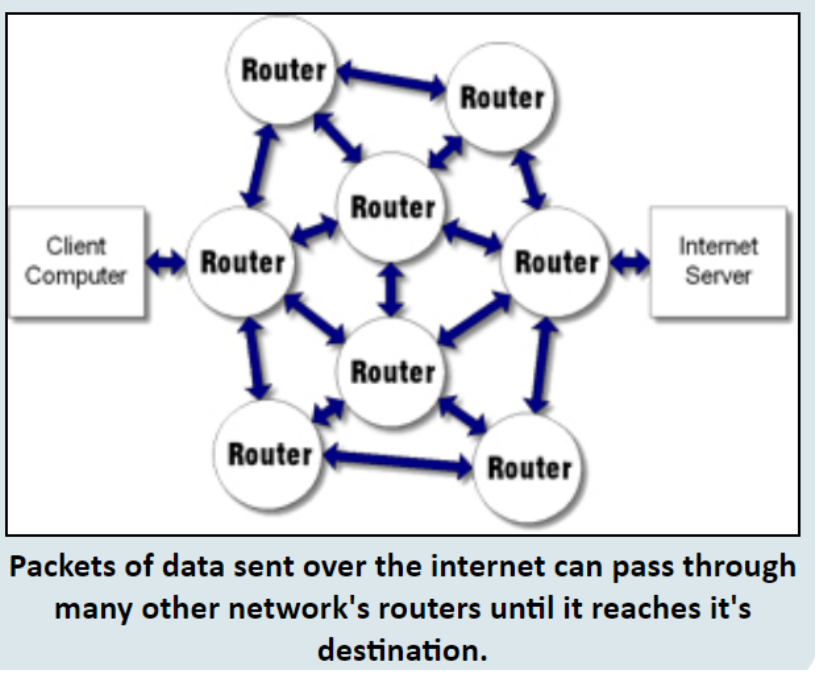
subnet mask *255.255.255.0 = 1111 1111.1111 1111.1111 1111.0000 0000*

IP *198.51.100.0 = 1100 0110.0011 0011.0110 0100.0000 0000*

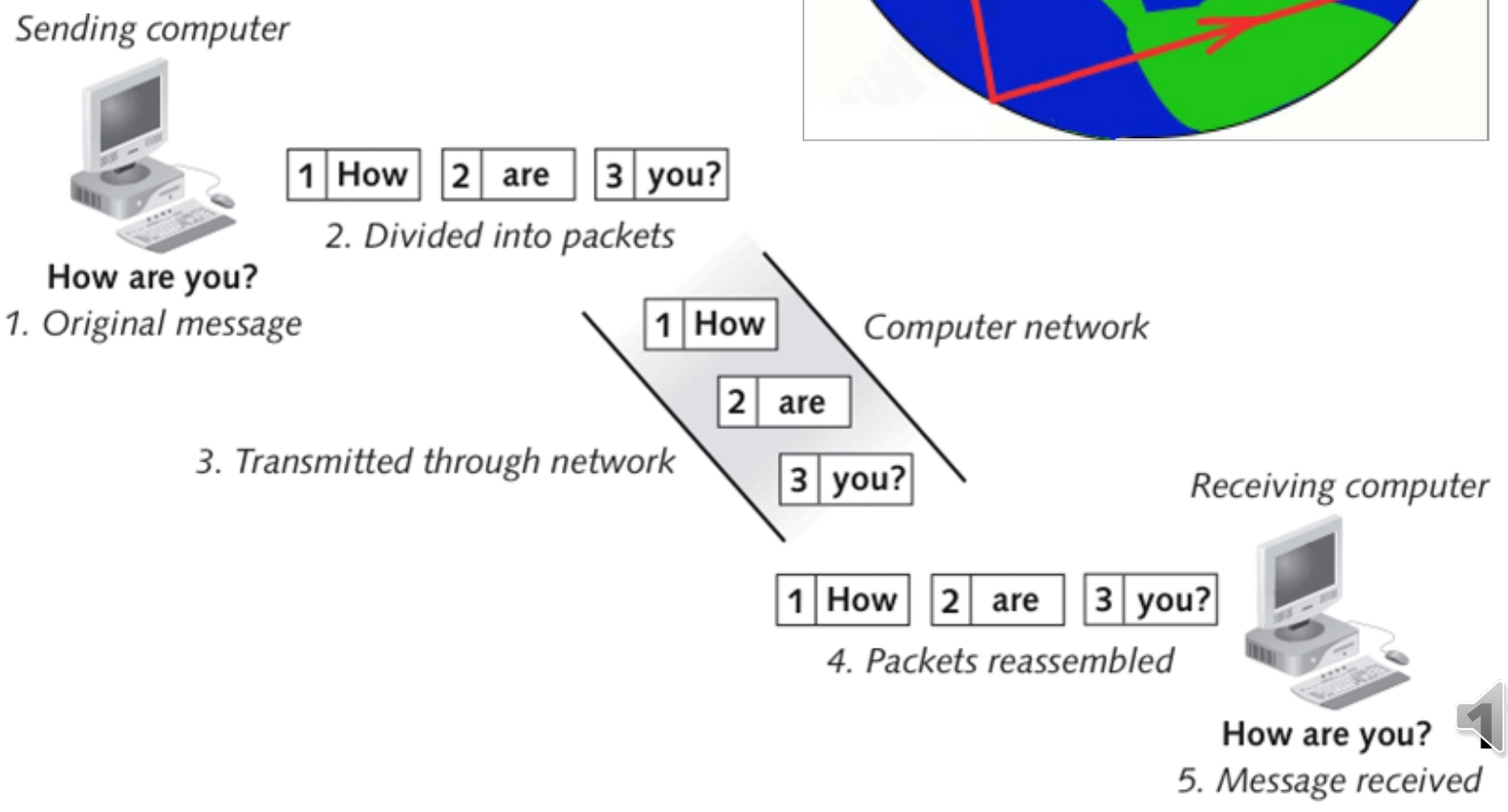
Network+Subnet **Host**





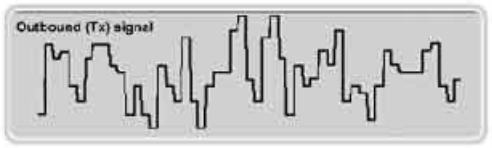


Packets of data sent over the internet can pass through many other network's routers until it reaches it's destination.



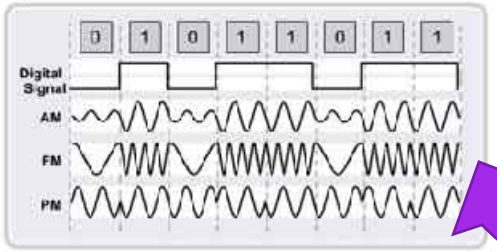
TCP/IP Five Layer Software Model Overview

Representations of Signals on the Physical Media



Sample electrical signals transmitted on copper cable

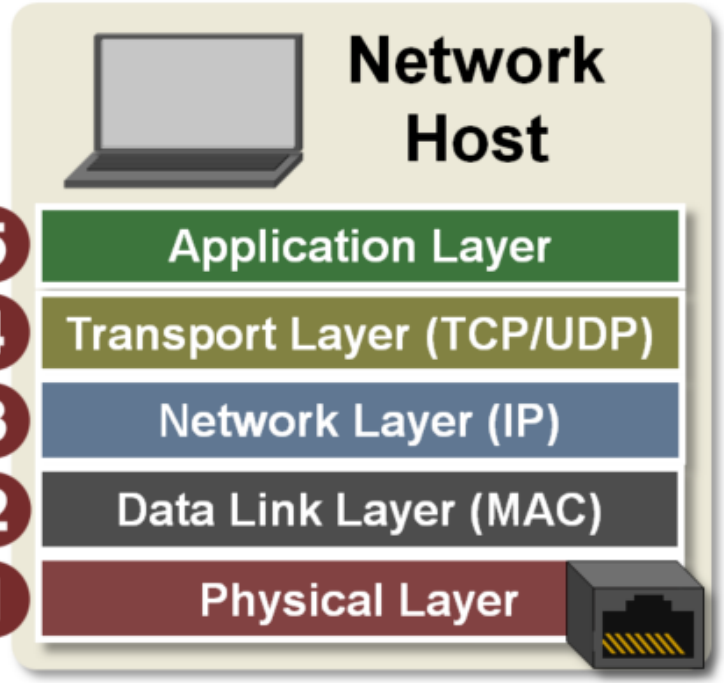
Representative light pulse fiber signals



Microwave (wireless) signals

Layer 5 requests connections to remote hosts

Layer 1 encodes and transmits bits

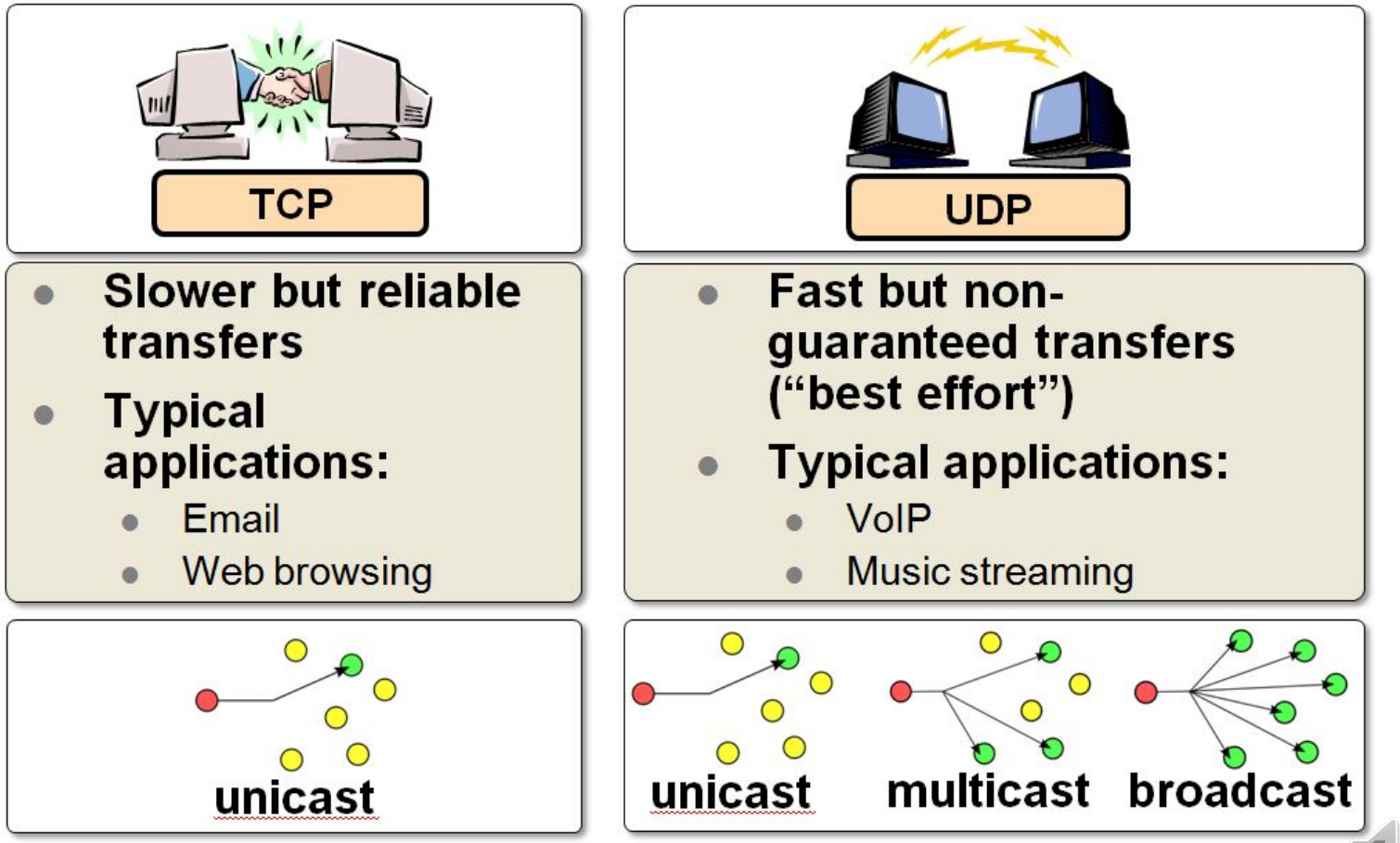


TCP (Transmission Control Protocol) **vs. UDP** (User Datagram Protocol)

Some applications require reliable ordered delivery of packets. The TCP protocol provides this capability. It uses error detection, retransmissions and acknowledgements. This protocol cares about your data.
Other applications don't care if every packet is received. These applications can take advantage UDP's lower overhead to enable faster transmissions.

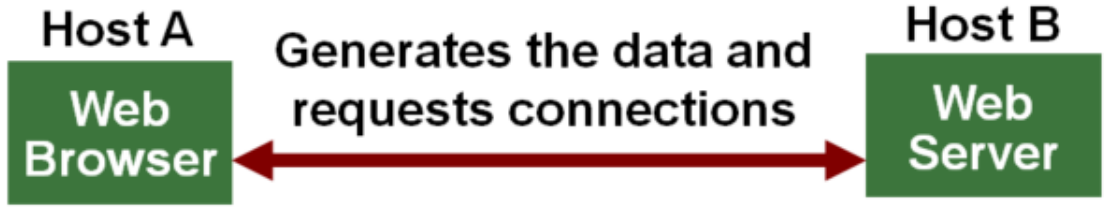
Typical TCP applications include email and web browsing and typical UDP applications include VoIP and music streaming.

TCP is strictly used for point to point or unicast transmissions while UDP can also be used for multicast and broadcast transmissions.



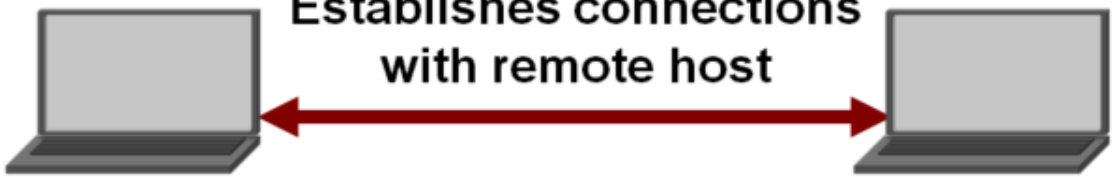
5 Application Layer

The Application layer is the group of applications requiring network communications.



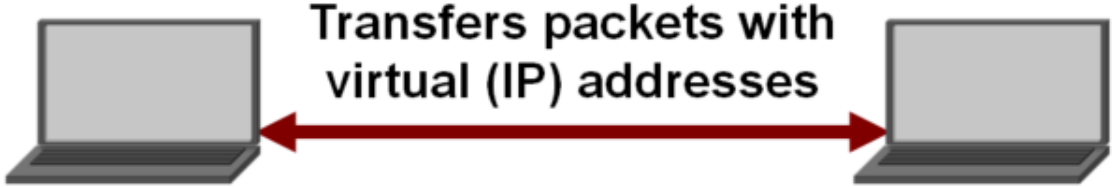
4 Transport Layer (TCP/UDP)

The Transport layer establishes the connection between applications on different hosts.



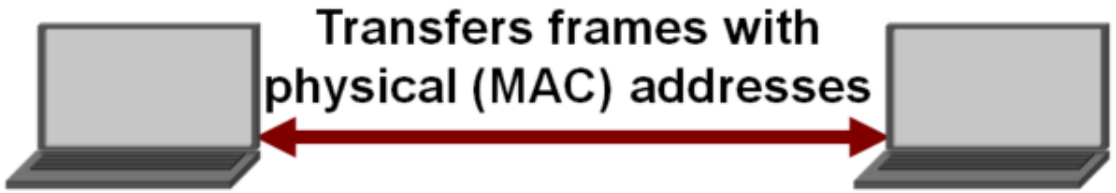
3 Network Layer (IP)

The Network layer is responsible for creating the packets that move across the network.



2 Data Link Layer (MAC)

The Data Link layer is responsible for creating the frames that move across the network.



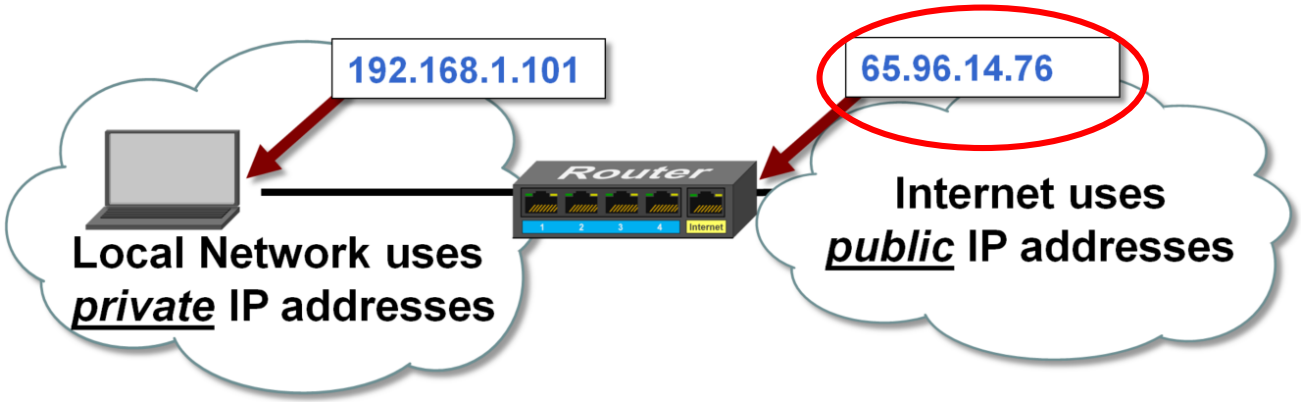
1 Physical Layer

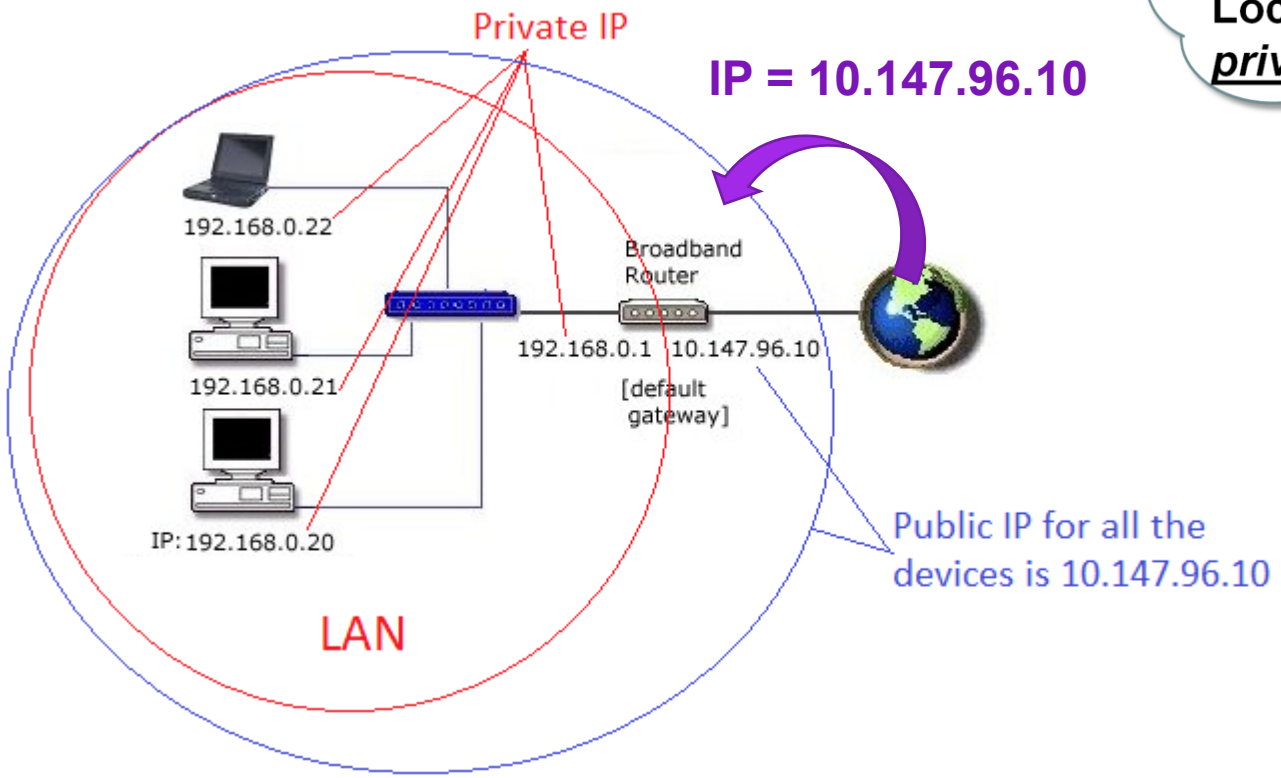
The Physical layer is the transceiver that drives the signals on the network.

Network Address Translation (NAT)

NAT translates between local network and Internet IP addresses.

All hosts that connect to the local network are assigned with local network IP addresses by the DHCP server running in the local network's router. When this router connects to the Internet, it is assigned with one IP address from the Internet service provider's DHCP server. All local network hosts will share this public IP address to access the Internet.





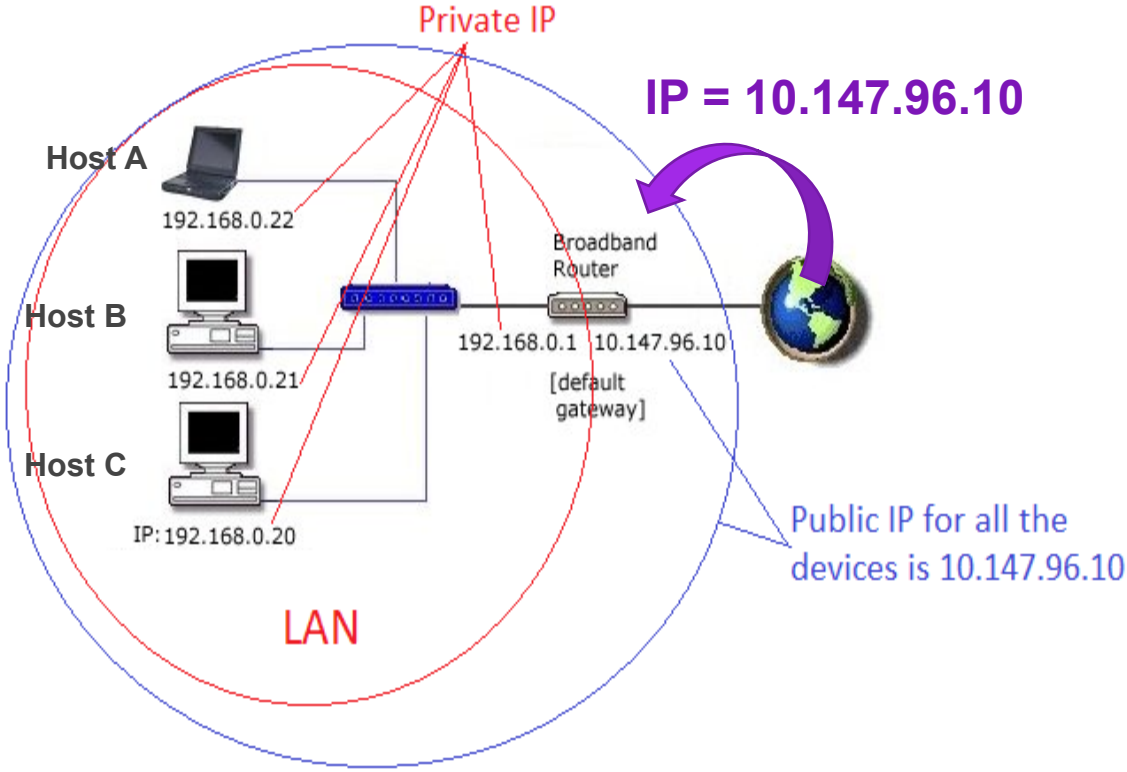
NAT Translation Table

How do all hosts on a local network share the same public IP address?

Network Address Translation (NAT) re-assigns IP addresses and port numbers and keeps track of these re-assignments using its NAT translation table.

When the router receives a packet from a local host containing a public IP address, it changes the source IP address to use its Internet IP address and changes the source port number so it knows which local host process to deliver received packets to.

This re-assignment is entered into the translation table. Each process requiring Internet access running on the local network is assigned a new IP address and port number by NAT. Each re-assignment is then entered into the NAT translation table.



NAT Translation Table

	Local IP	Source Port		Internet IP Address	Source Port
Process X, Host A	192.168.0.22	54847	⇔	10.147.96.10	1
Host B	192.168.0.21	24123	⇔	10.147.96.10	2
Process Y, Host A	192.168.0.22	42156	⇔	10.147.96.10	3
Host C	192.168.0.20	33543	⇔	10.147.96.10	4

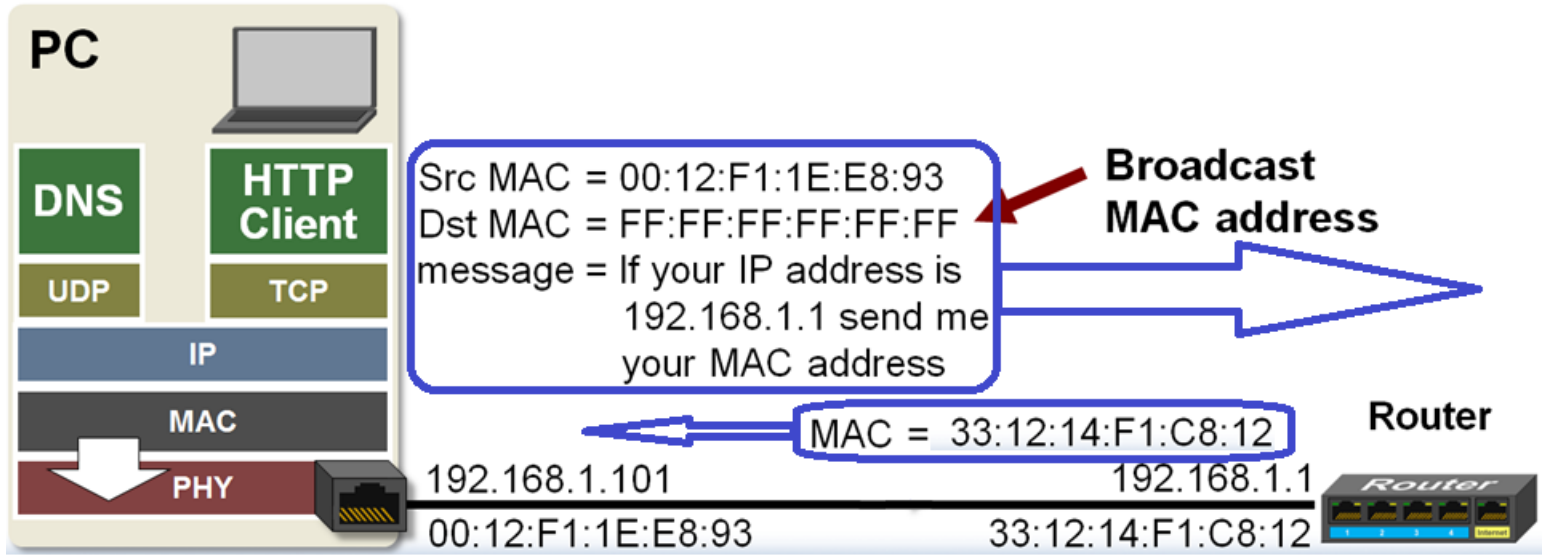
Address Resolution Protocol Request (ARP)

When the DHCP server running in the local router assigned the PC its IP address, it also let the PC know what the default gateway's IP address is. So the PC knows the IP address of its default gateway, but it doesn't know the MAC address of the default gateway. This is where ARP steps in to save the day.

The **Address Resolution Protocol (ARP)** enables a local host to discover another local host's MAC address corresponding to its IP address.

ARP creates a message that says, "if this is your IP address, send me your MAC address".

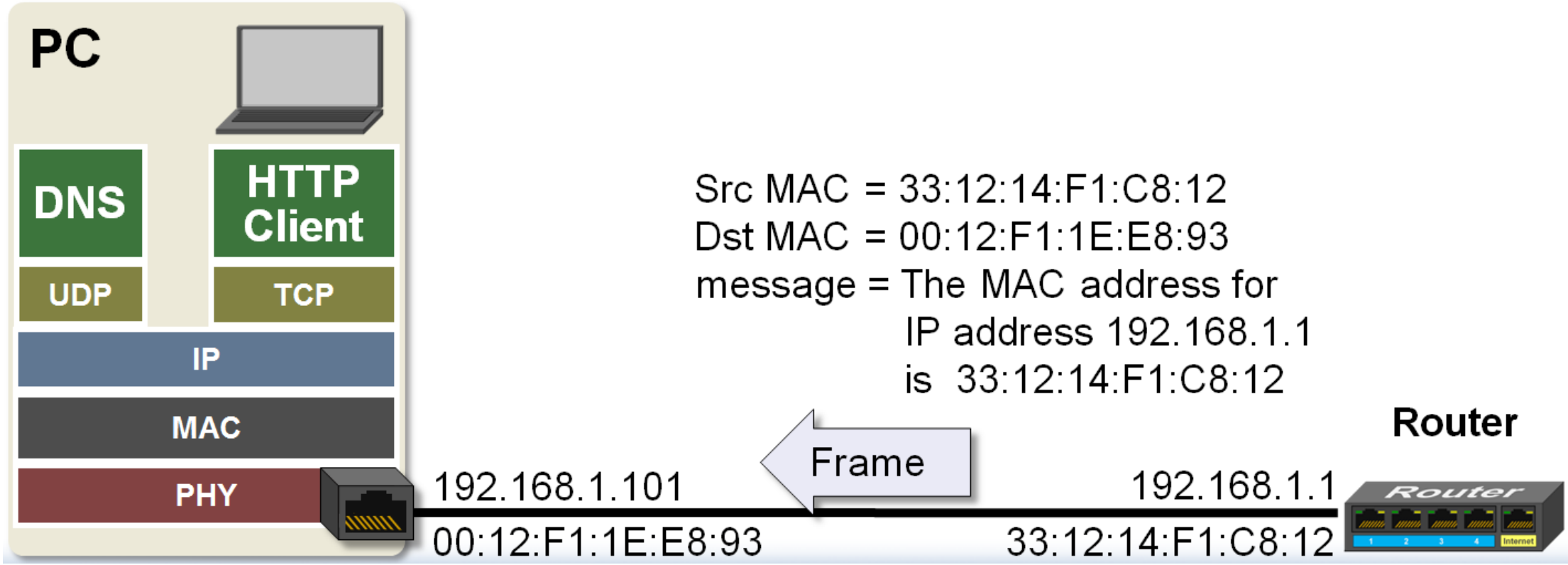
The Link layer creates the frame header by adding its MAC address as the source and the broadcast MAC address as the destination. The frame is then sent to every host on the local network.



Address Resolution Protocol (ARP) Response

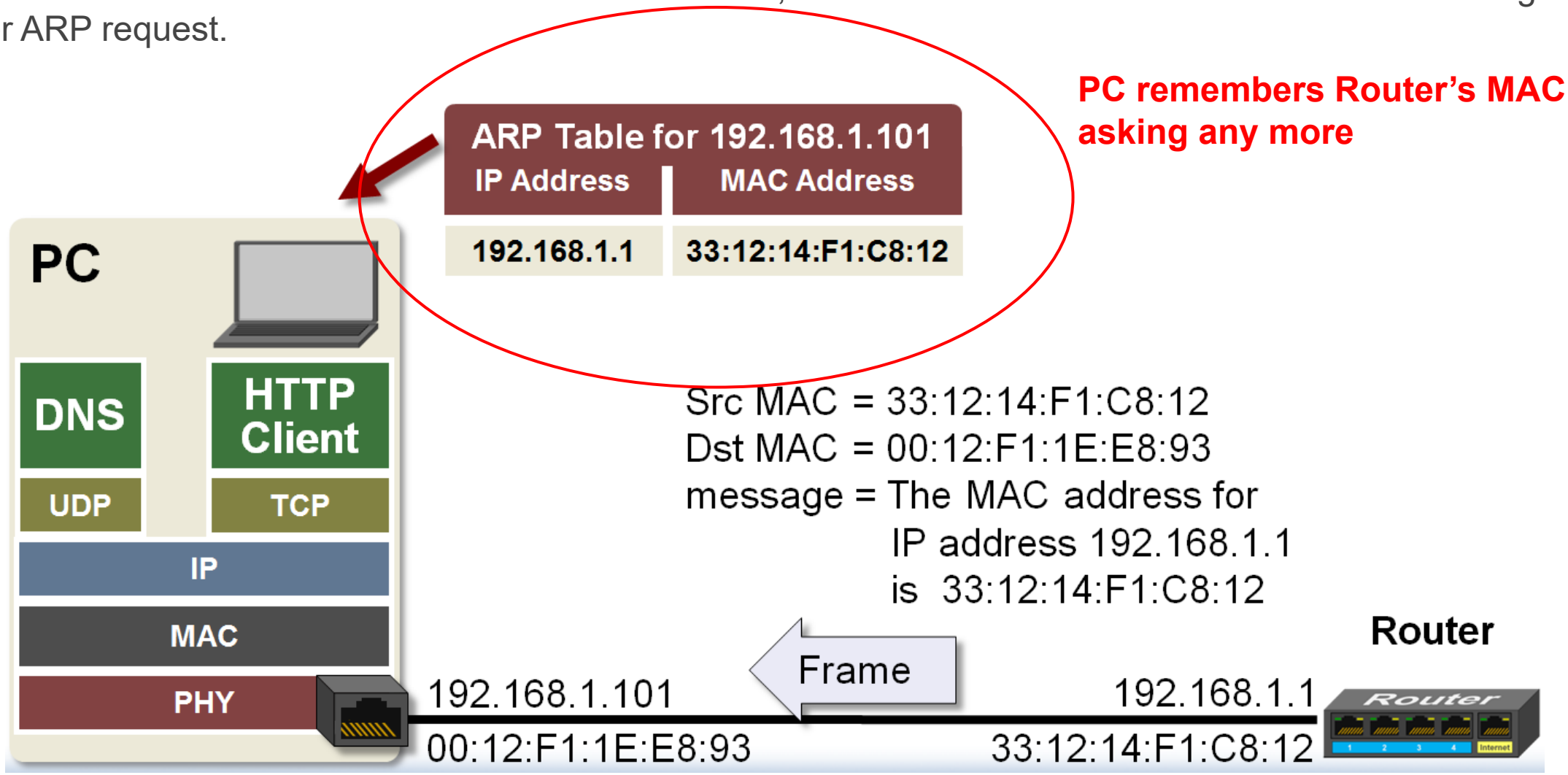
When the router and every other host on the local network receives the frame, they will look at the destination MAC address to determine if they should pay attention to the frame. They will all see the broadcast MAC address as the destination so all will open the message and read it. Once the other hosts see the message is an ARP request for an IP address other than their own, they will discard the frame and do nothing. The router will read the message, compare the IP address (the default gateway) to its own, and discover someone has sent it an ARP request. It is now required to send an ARP response.

It creates an ARP response message that includes its MAC address. The router's Link layer then creates a frame header with the source and destination MAC addresses, adds it to the message, then sends it to its physical layer to transmit the frames bits.



ARP Table

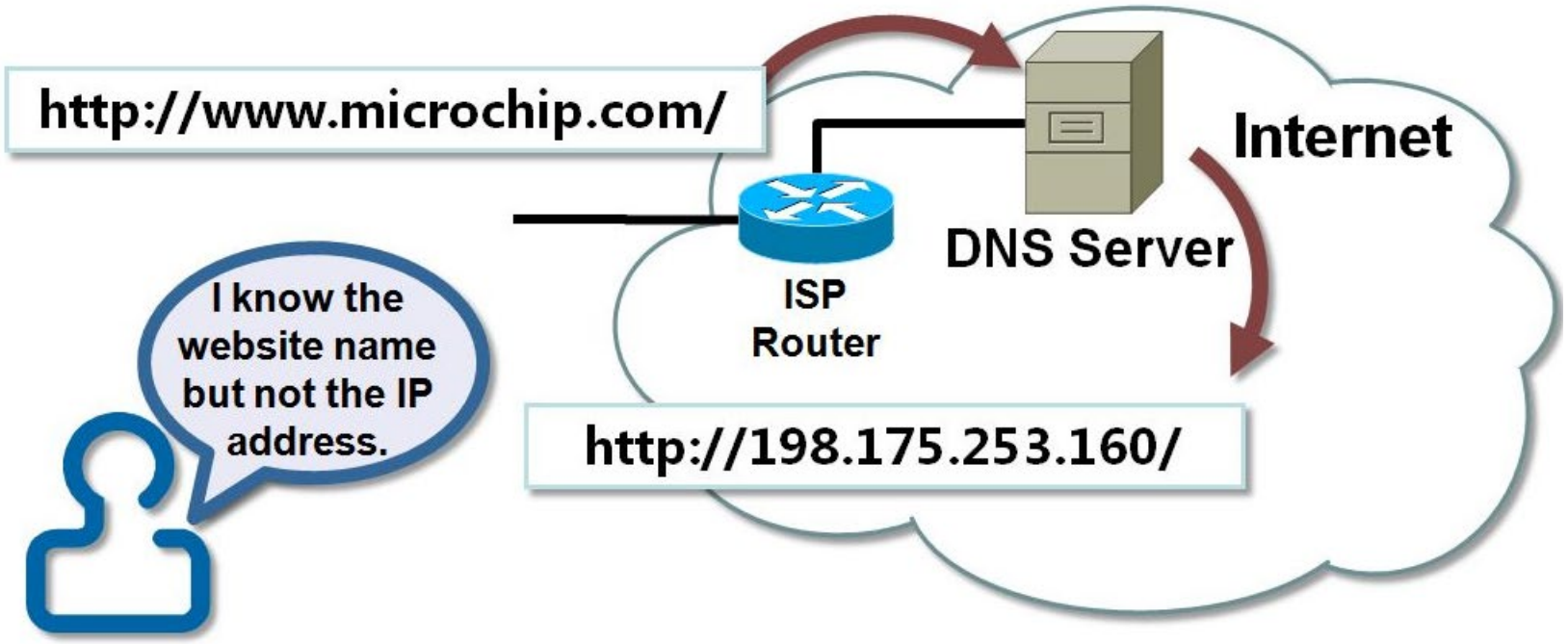
When the requesting host receives the ARP response, it adds the MAC and IP address to its ARP table. The next time the host needs the MAC address for this IP address, it will find it in its ARP table and won't need to generate another ARP request.



DNS (Domain Name System)

A Domain Name System **(DNS)** enables us to browse to a website by providing the website or domain name instead of the website's IP address.

It maps domain names to IP addresses. A network host needs the IP address (not the domain or host name) of the web server to generate a Packet.



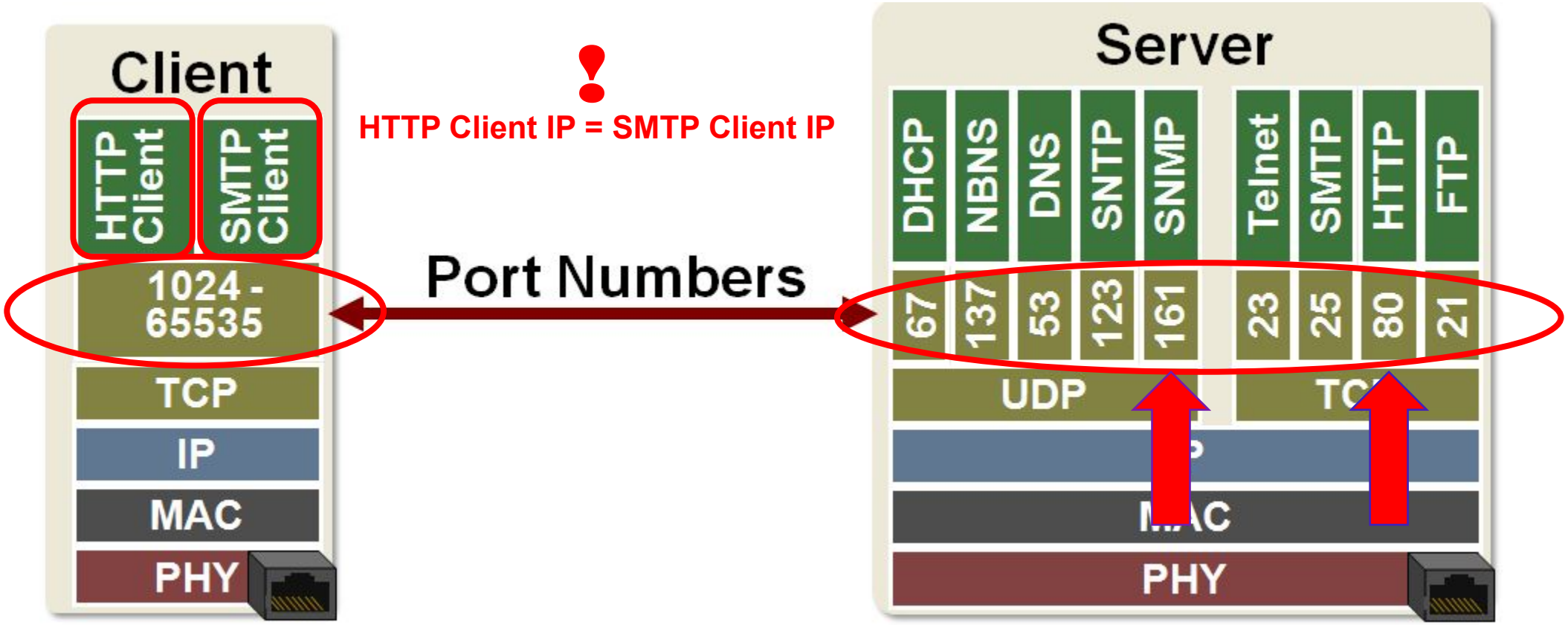
TCP/IP Ports

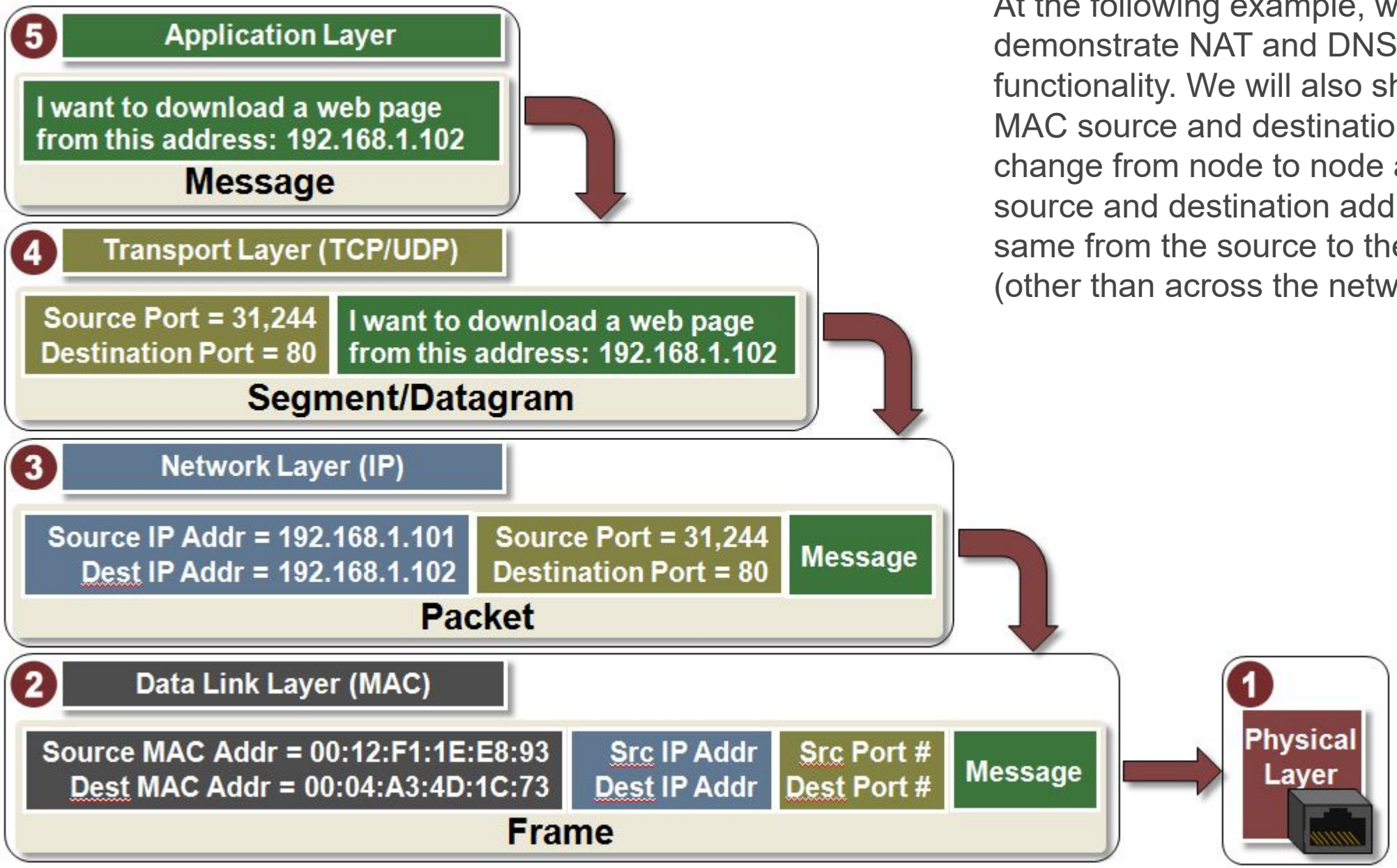
Common TCP/IP Applications

Application	Description
DHCP	Dynamic Host Configuration Protocol assigns IP addresses
DNS	Domain Name System translates website names to IP addresses
HTTP	Hypertext Transfer Protocol used to transfer web pages
NBNS	NetBIOS Name Service translates local host names to IP addresses
SMTP	Simple Mail Transfer Protocol sends email messages
SNMP	Simple Network Management Protocol manages network devices
SNTP	Simple Network Time Protocol provides time of day
Telnet	Bi-directional text communication via a terminal application
TFTP	Trivial File Transfer Protocol used to transfer small amounts of data

TCP/IP Ports

Ports are used to identify processes running in the applications on a host.
Let's assume we have two applications running on one PC that require TCP/IP communications. Assume one is a web browser and the other is an email client.
Both applications send and receive packets with the same IP address, so how does the Transport layer differentiate a web browser packet from an email packet?
The answer is port numbers.





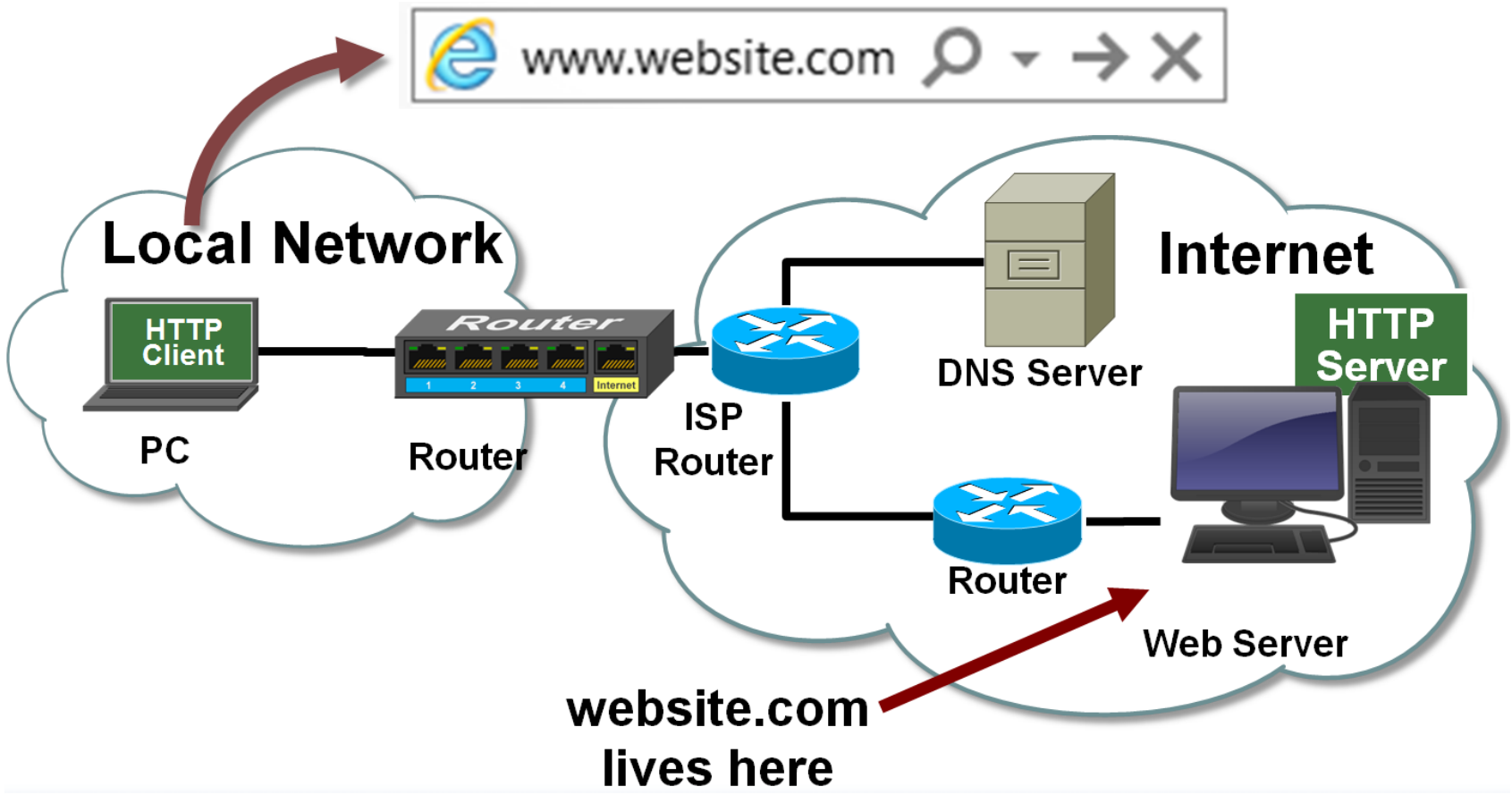
At the following example, we will demonstrate NAT and DNS server functionality. We will also show how the MAC source and destination addresses change from node to node and that the IP source and destination addresses stay the same from the source to the destination (other than across the network boundary).

Detailed TCP/IP Communication Example

Example: Download a Webpage from the Internet

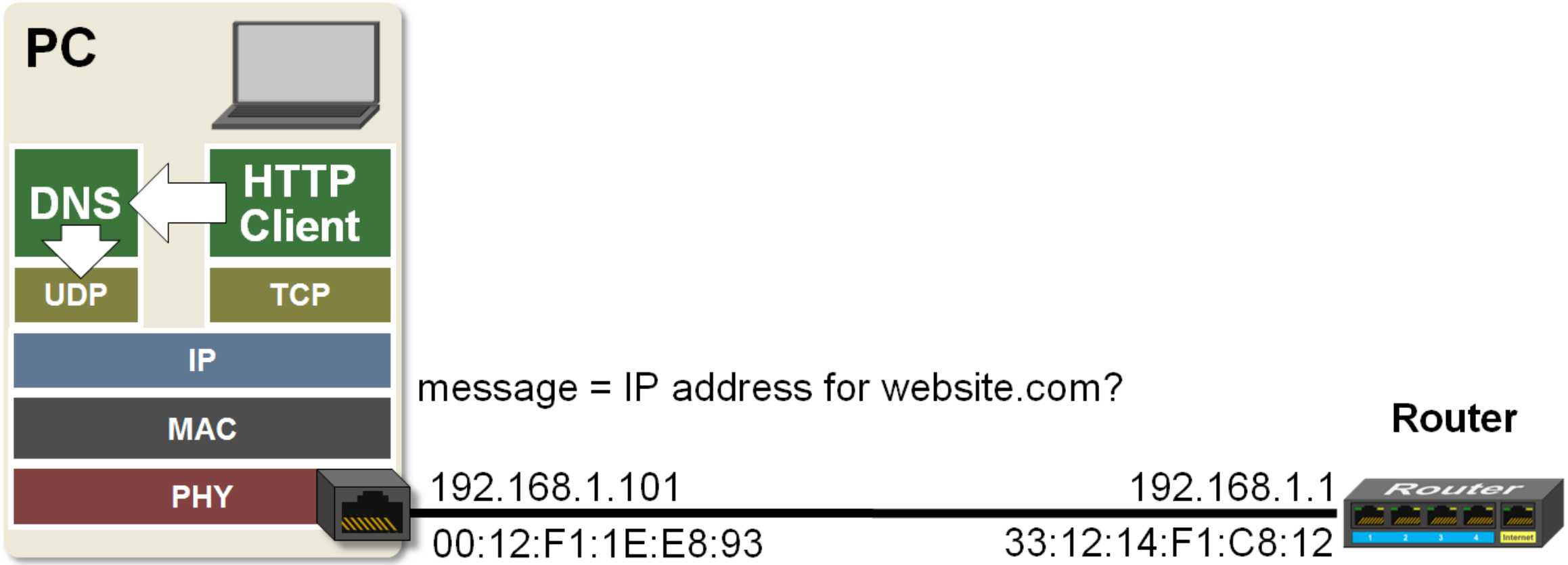
1. Enter website in browser

Open a web browser on the PC and enter the website name.



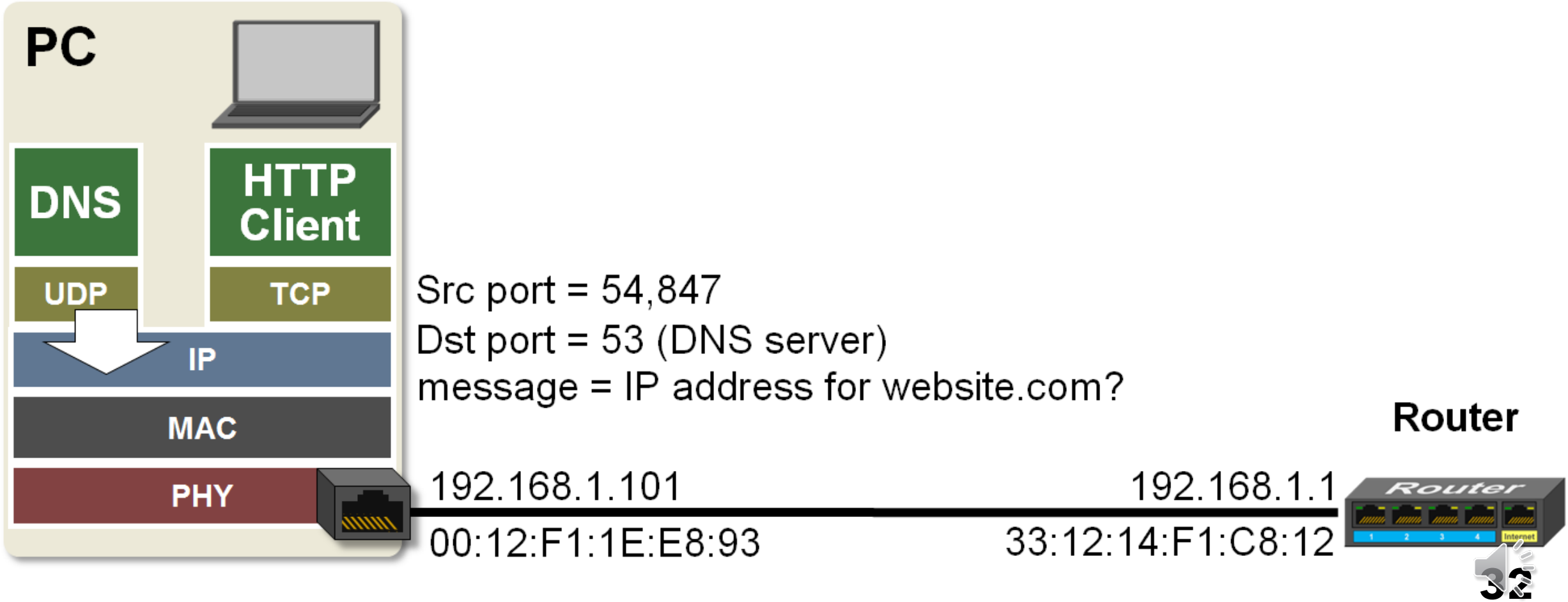
2. DNS client creates a message

The HTTP client in the PC tries to generate a message requesting the HTML file from www.website.com.
It needs to supply the destination IP address in the message it generates but doesn't have it,
so it employs the PC's DNS client to get it.
The DNS client sends a message to the Transport layer requesting the IP address for website.com.



3. Create a datagram

The Transport layer adds the UDP header containing the source and destination port to the message. It creates the source port number and assigns it to the DNS process requesting the IP address. The "Well-Known" DNS server port number is used as the destination port. The resulting datagram is then sent to the Network layer.



TCP and UDP Headers

The header added to messages by the Transport layer includes more than just the source and destination port numbers. Here we are showing all the information included in TCP and UDP headers.
Note how the TCP protocol requires more information and overhead to guarantee data delivery.

TCP Segment Header Format

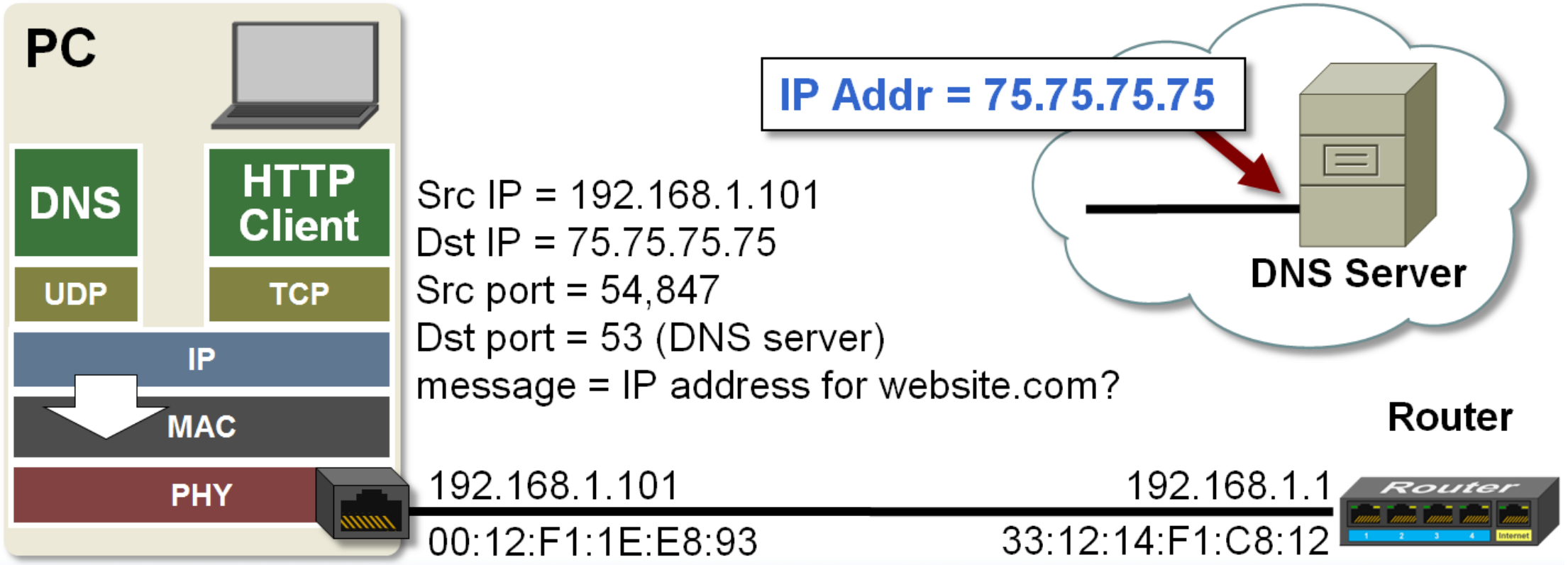
Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

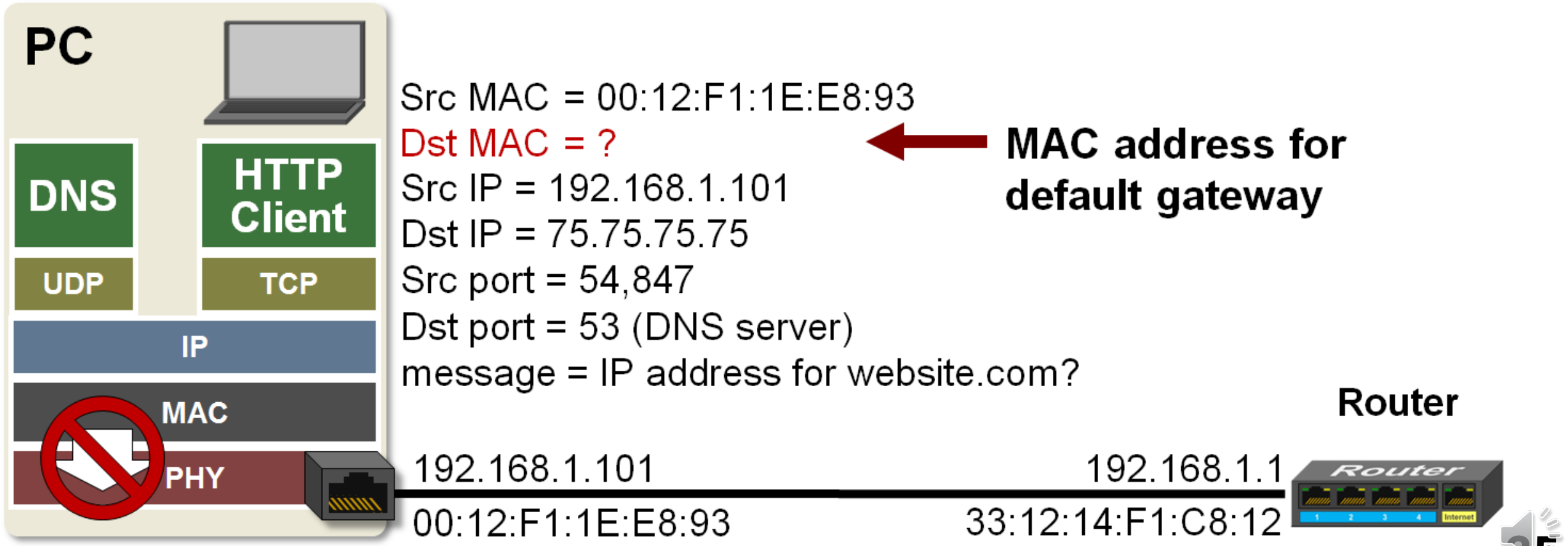
4. Create a packet

The Network layer adds the IP header containing the source and destination IP address to the datagram.
It adds its own IP address as the source and the DNS server IP address as the destination. The PC knows the DNS server's IP address because the router provided the PC with it when it assigned its local IP address. The resulting packet is sent to the Link layer.



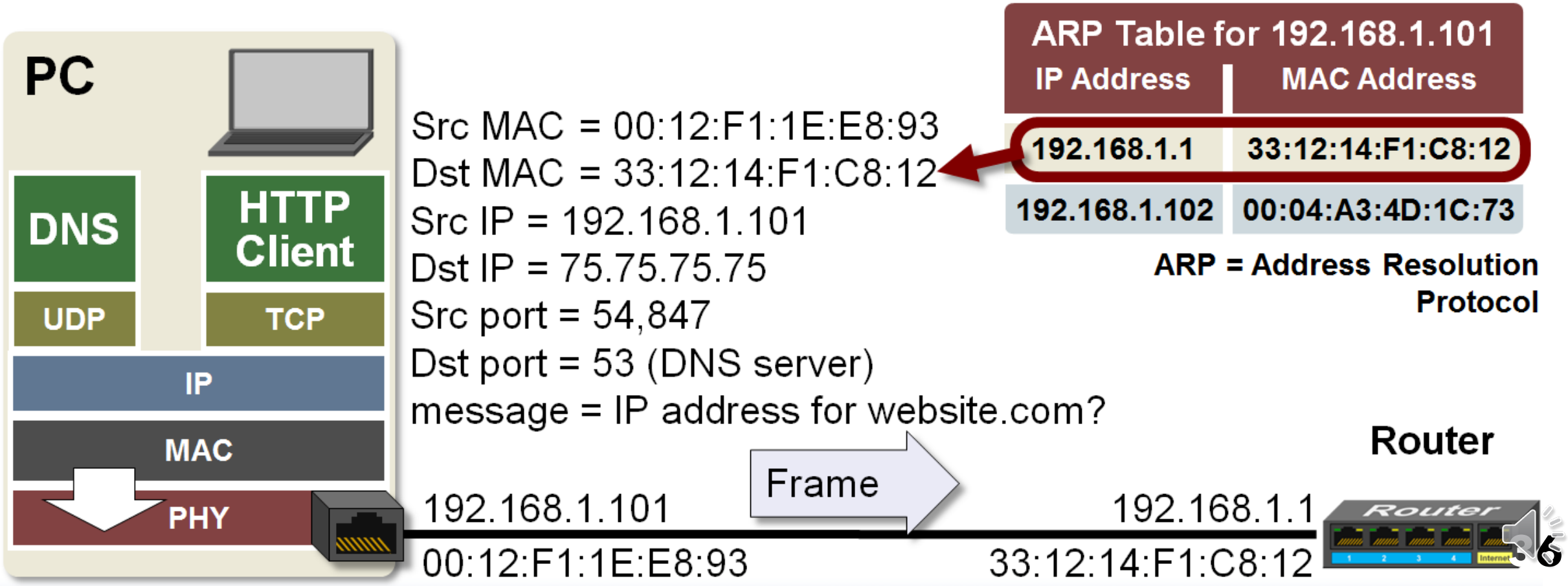
5. Determine destination MAC address

The Link layer that determines the destination IP address for this packet is not on the local network. It, therefore, needs to send the packet to its default gateway which in this example is the router.
Now we have a problem. The Link Layer can't create the frame because it doesn't know the MAC address of the default gateway. The Address Resolution Protocol (ARP) was created to solve this problem.



6. Create and transmit a frame

After using ARP to get the MAC address for its default gateway, the Link Layer can complete the frame for the DNS transaction.
It adds the source and destination MAC addresses to the packet to create a frame. The source MAC address is its own and the destination MAC address is that of the default gateway.
This frame is then sent to the Physical layer to transmit the frame's bits.



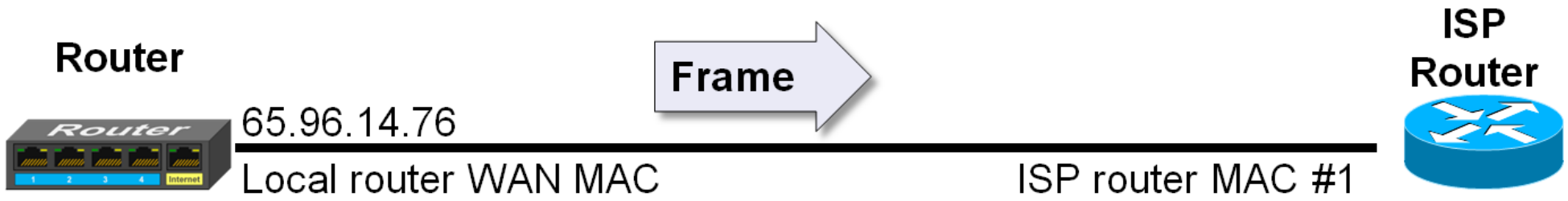
7. NAT and forward frame to Internet

The router receives the frame from the PC, opens the packet and determines the destination IP address is not on the local network, so it must forward this frame to the Internet.
The router creates a new Network Address Translation (NAT) entry and changes the local network IP address to its public Internet IP address. It also uses the same NAT table entry to change the source port so the router can determine which host and host process to deliver in-coming packets to.
The router has to change the source MAC from its local network MAC to its Wide Area Network (WAN) or Internet MAC. The destination MAC address also needs to be changed to that of the router's default gateway, which in this example is the ISP's router. The local router references its ARP table to get the Internet Service Provider (ISP) router's MAC address.
The local router forwards this new frame to the ISP's router.

Src MAC = Local router WAN MAC
Dst MAC = ISP router MAC #1
Src IP = **65.96.14.76**
Dst IP = 75.75.75.75
Src port = **1**
Dst port = 53 (DNS server)
message = IP address for website.com?

NAT Translation Table

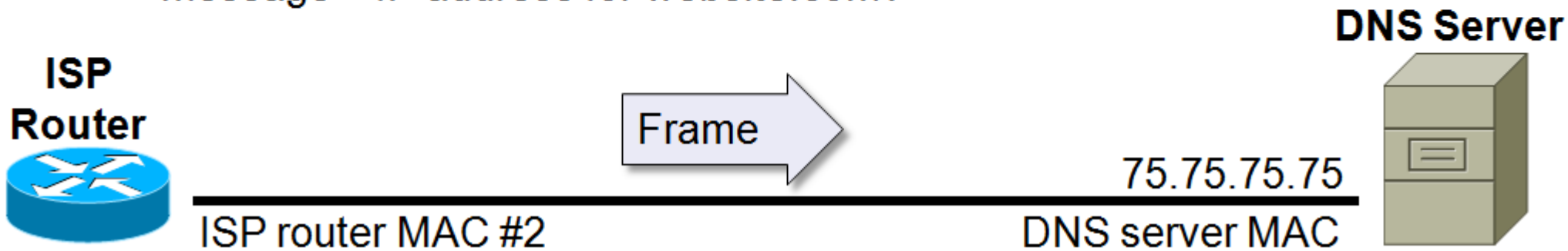
Local IP Address	Source Port #		Internet IP Address	Source Port #
192.168.1.101	54,847	=	65.96.14.76	1
--	--	=	--	--



8. Forward frame to DNS server

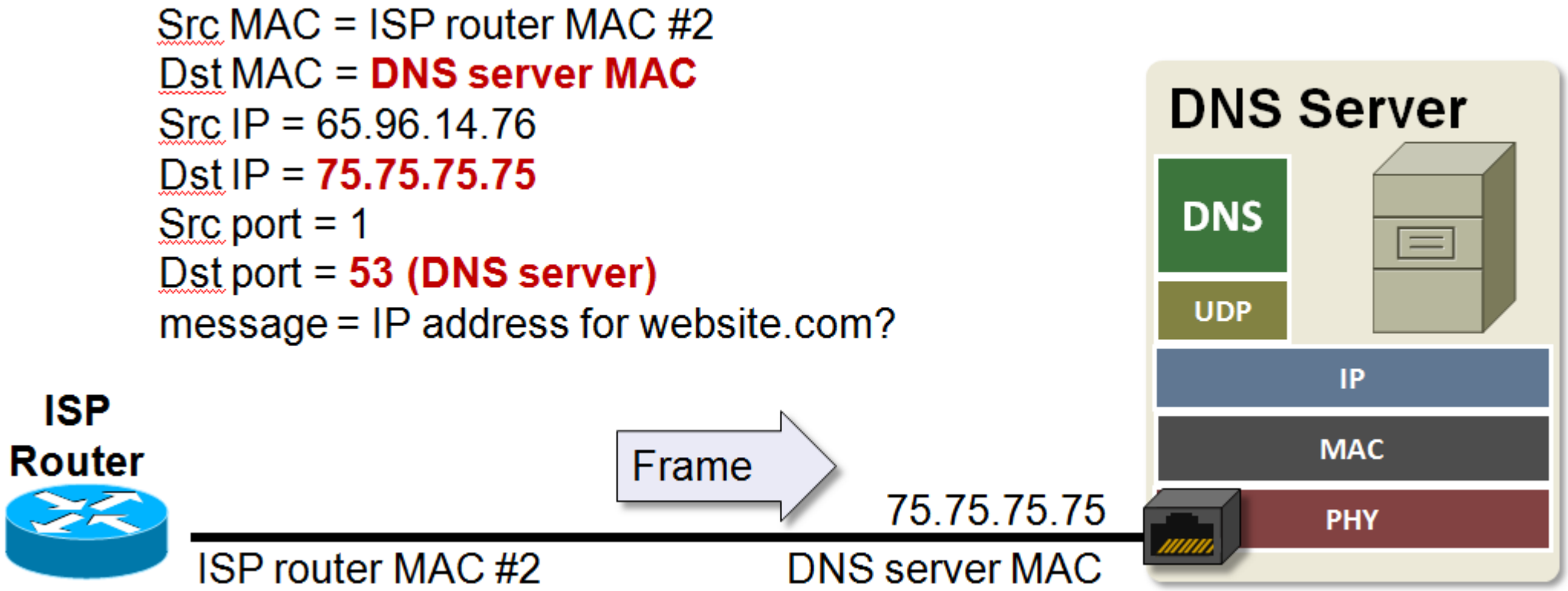
The router at the ISP receives the frame and opens the packet to find the destination IP address. It determines the destination IP address belongs to its DNS server. The router's Network layer sends the packet back to its Link layer to generate a new frame header.
The source MAC address is its own and the destination MAC address is the DNS server's. Note that the source and destination IP addresses remain the same.
The new frame is sent to the DNS server.

Src MAC = **ISP router MAC #2**
Dst MAC = **DNS server MAC**
Src IP = 65.96.14.76
Dst IP = 75.75.75.75
Src port = 1
Dst port = 53 (DNS server)
message = IP address for website.com?



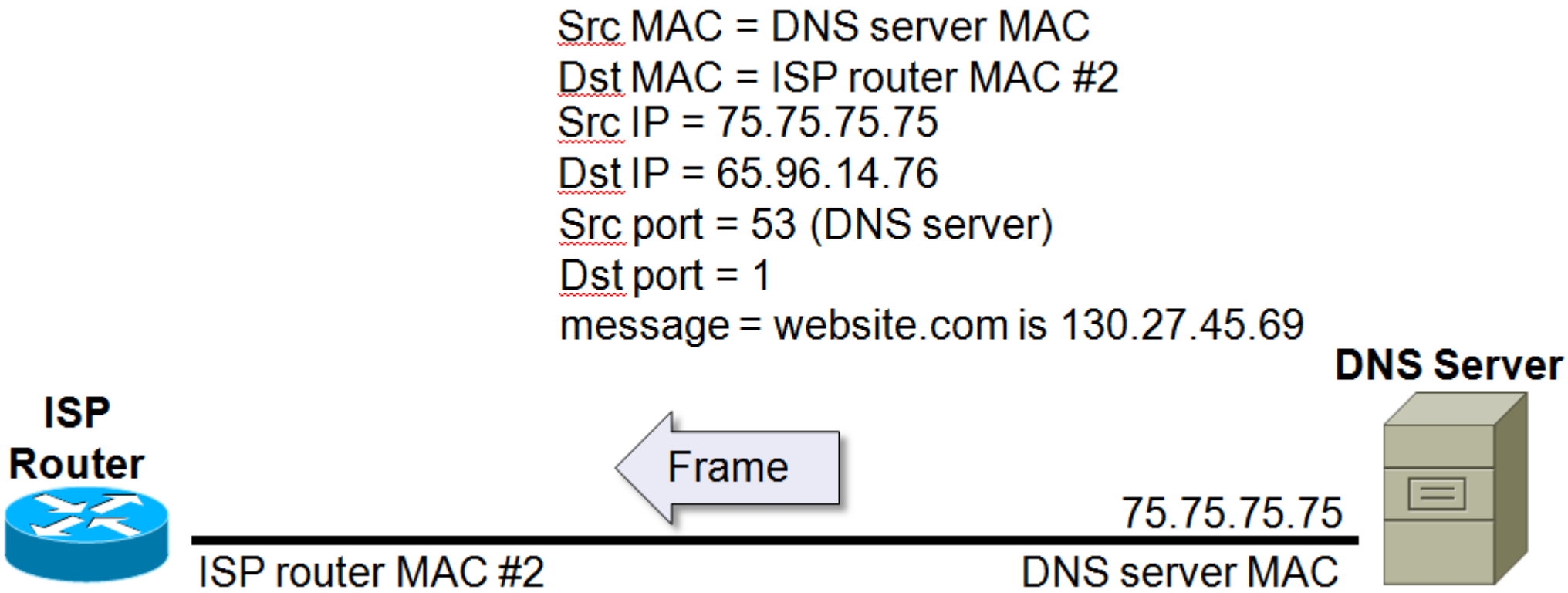
9. DNS server receives frame

The DNS server's PHY receives the bits and forwards the frame to the Link layer.
The Link layer finds its MAC address as the destination so it forwards the packet to the Network layer.
The Network layer opens the packet and finds its IP address as the destination. It still needs to pay attention to the message, so it forwards it up to the Transport layer.
The Transport layer opens the datagram and finds it is being sent to port 53. The DNS server has a process running and listening for traffic on this port, so the message is forwarded to it.



10. DNS translates and generates reply

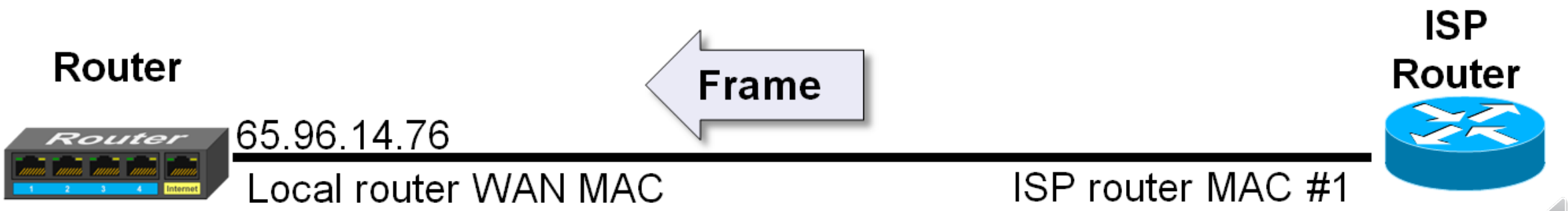
The DNS Server determines the IP address for website.com and generates a reply message containing it. The message is sent back to the Transport layer.
The Transport layer adds the port information and creates the datagram.
The Network layer adds the IP information and creates the packet.
The Link layer adds the MAC information and creates the frame.
The Physical layer transmits the frame's bits to the router.



11. Forward frame to local router

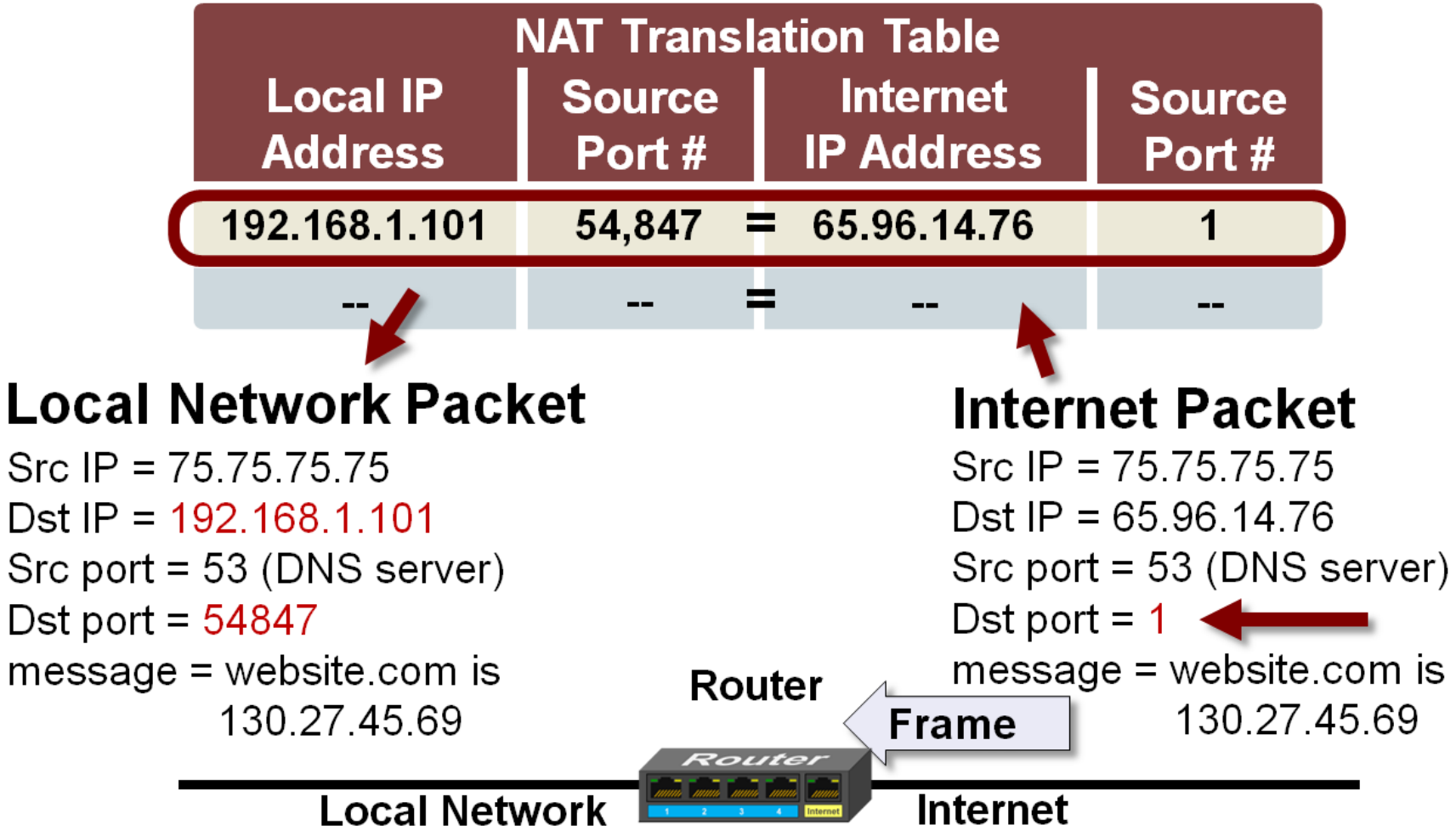
The ISP's router receives the frame, finds its MAC address, and sends it to its Network layer to determine the destination IP address. It finds that the packet belongs to our local router's IP address, so it sends the packet back down to its Link layer.
The Link layer attaches new source and destination MAC addresses to the packet then sends the frame to our local router.

Src MAC = ISP router MAC #1
Dst MAC = Local router WAN MAC
Src IP = 75.75.75.75
Dst IP = 65.96.14.76
Src port = 53 (DNS server)
Dst port = 1
message = website.com is 130.27.45.69



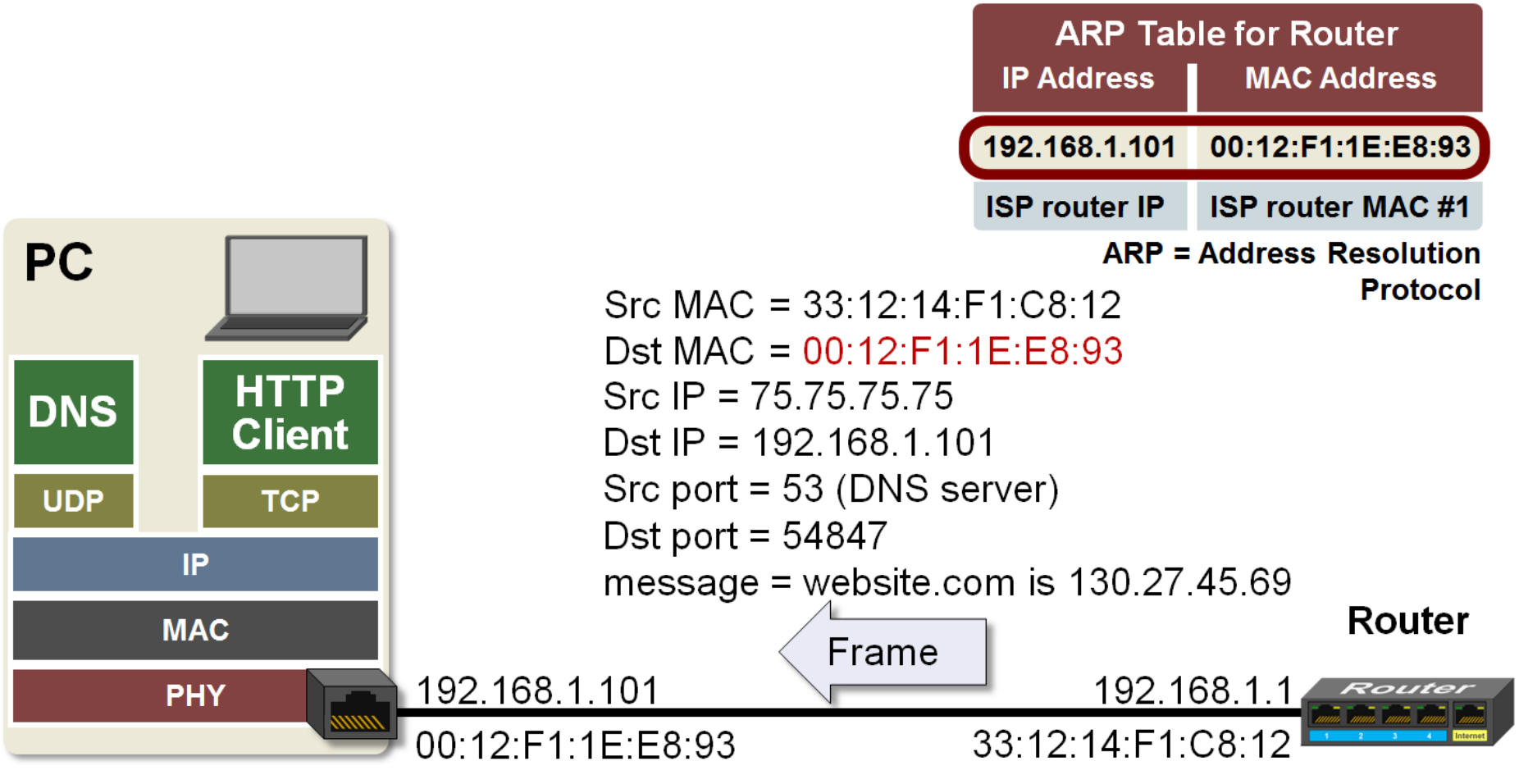
12. NAT translation in local router

When the local router receives the packet from the ISP's router, it consults its NAT table to determine which local host to forward it to. It finds an entry with an internet destination port number of 1 in the translation table.
The corresponding local IP address and port number are substituted into the packet that will be sent to the local network.



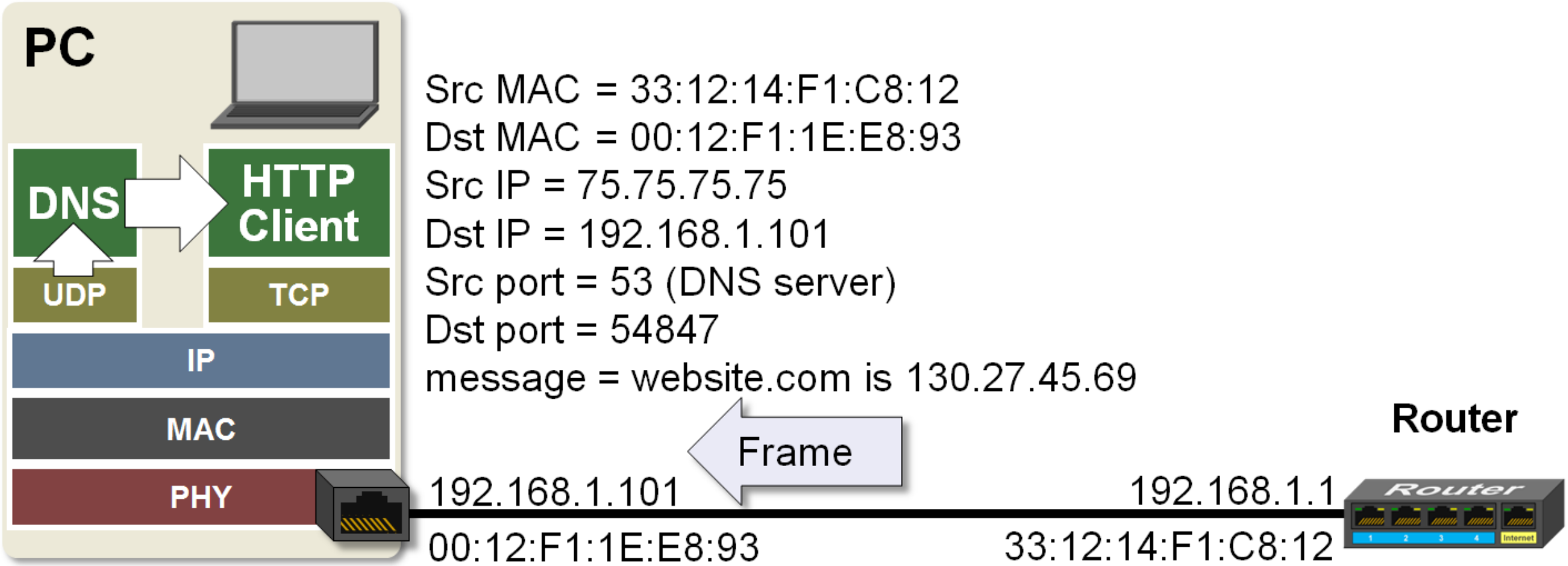
13. Frame forwarded to PC

The new packet is sent to the router's Link layer where the source and destination MAC addresses are added creating the frame.
The router knows the destination MAC address corresponding to the destination IP address by consulting its ARP table.
This frame is then sent to the physical layer to be transmitted on the network.



14. DNS client delivers IP address

When the Frame arrives at the PC the message is sent to the DNS client.
The DNS client then provides the IP address for website.com to the HTTP client.



15. HTTP client creates message

Now that the HTTP client has the IP address for website.com (130:27:45:69) it can generate the message to download the HTML file for this website.