Lecture 5: Introduction to Networking

AP Computer Science Principles

Local Area Network (LAN)

LAN

- **local area network**(LAN): a group of interconnected computers that share resources in a small geographic area.
  - Smallest example of a LAN is two computers connected by an CAT6(ethernet cable).

Image:Michael Lamont; www.slideshare.net/MichaelLamont

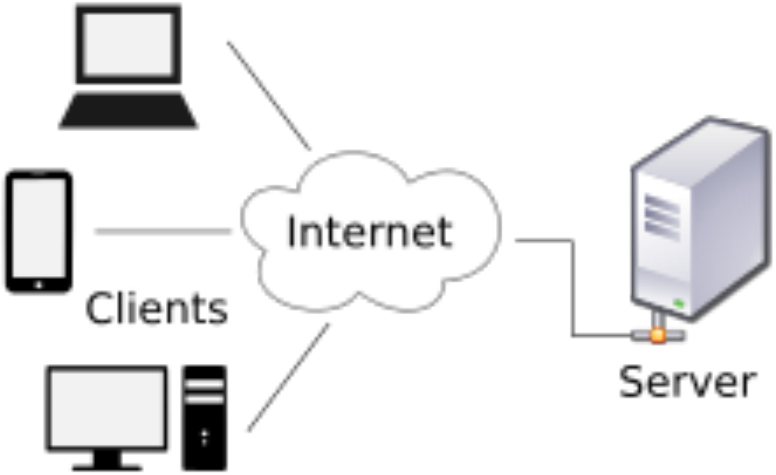
  - A **host** is a computer on a network.

- A **network protocol** is a set of rules for how applications intercommunicate.

Server-Client

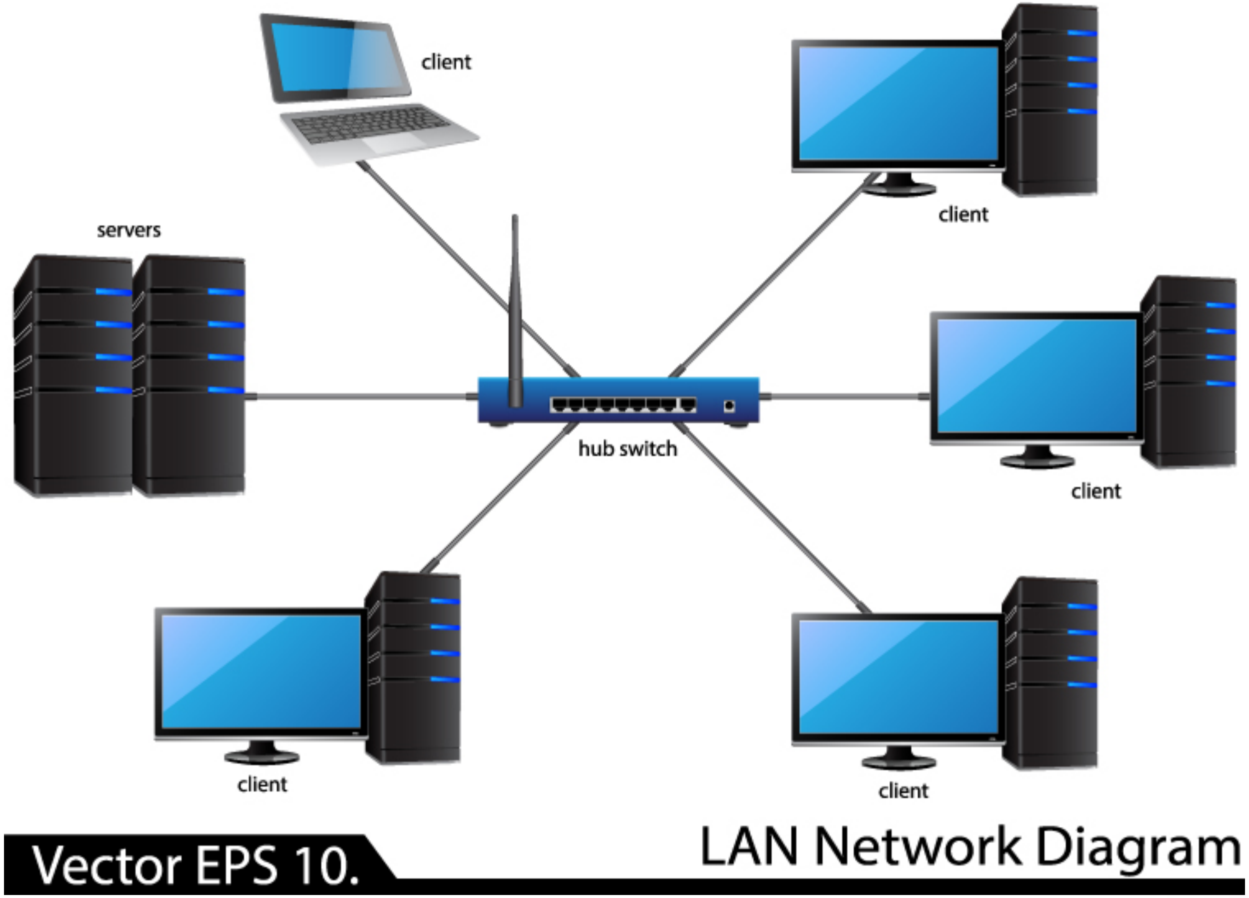
- A **client** is a computer that is requesting a resource or service.

- A **server** is a computer that provides a resource or service.
  - Print servers provides printing service, web servers serves webpages, email servers, file servers, etc…



Hubs and Switches

- **Hubs** and **switches** allow computers on a LAN to communicate with one another.



Hubs vs Switches

- a **hub** is a **multiport repeater**, that is, the data it receives is broadcast and seen by all devices connected to its ports. **Hubs are currently obsolete.**
  - E.g. a computer sent a request to a printer via a hub. All computers connected to that hub see that request.
  - A port is the a physical input/output interface to a networking device.

- a **switch** is a networking device can forward data directly to computers connected to its ports using the destination physical or **hardware address**(MAC address).
  - E.g. a computer sent a request to a printer via a switch; only the printer sees the request.

MAC Address

- A **network interface card**(NIC) on a computer contains a unique hardware address or physical address called the **MAC(media access control) address**.
  - Every device that can make Wifi, ethernet or bluetooth connections has a MAC address, e.g., laptops, phones, bluetooth speakers, smart fridge, tablets, etc…
- A MAC address is 6 bytes or 48 bits in length. It is displayed in 12 hexadecimal digits.
  - Example of a MAC address: 00-AA-00-B6-7A-50. The first six digits identify the vendor; in this case 00-AA-00 belongs to Intel.

IP Address

- The MAC address provides the physical address for the NIC but provides no information as to its network location, LAN or in which building, city or country the network resides.

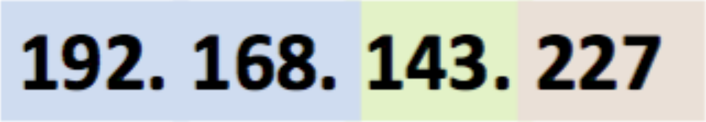
- The **Internet Protocol**(IP) address provide worldwide addressing that identifies the computer’s local network.
  - An IP address is a network address or logical address of a computer.
  - Can be IPv4 or IPv6. Although IPv6 is becoming more popular, IPv4 is still the addressing technique of the internet.

IP Address(IPv4)

- The **IP address** is a unique 32-bit that identifies on which network the computer is located as well as differentiates the computer from all other devices on the same network.

- The address is divided into four 8-bit parts. The format is A.B.C.D, where A,B,C,D are decimal equivalent of the 8-bit binary value. Each value is in the range 0-255.

- IP address has three parts: network number(identifies the network), subnet and host ID number(identifies the particular computer or host). For example:



192. 168. 143. 227

IP Address(IPv4)

- For IPv4, with 32-bits, there are a total of 4,294,967,296 addresses.
  - Not a lot of addresses considering the number of tablets, smartphones, smart TVs, Rokus, laptops in each home!

- To conserve the public IP address space, **private IP addresses** are used within private networks. These private addresses are not valid addresses for Internet use.

- The three address blocks for private IP addresses are:

  10.0.0.0 – 10.255.255.255

  172.16.0.0 – 172.31.255.255

  192.168.0.0 – 192.168.255.255

Private IP Addresses

- In a small LAN, computers/hosts are assigned private IP addresses that can identified them locally.
  - These private IP addresses are not unique; two hosts from two different LAN can have the same private IP address.

- When a computer make a request for a resource outside of its LAN, e.g. CNN's webpage, the request passes through the router that is responsible for data packets leaving/entering the network.
  - This router is known as the **default gateway.**
  - The **Internet Service Provider**(ISP) assigns one public IP address to the entire network. Any outside traffic to and from computers inside the network is routed to this public IP address.

Private IP Addresses

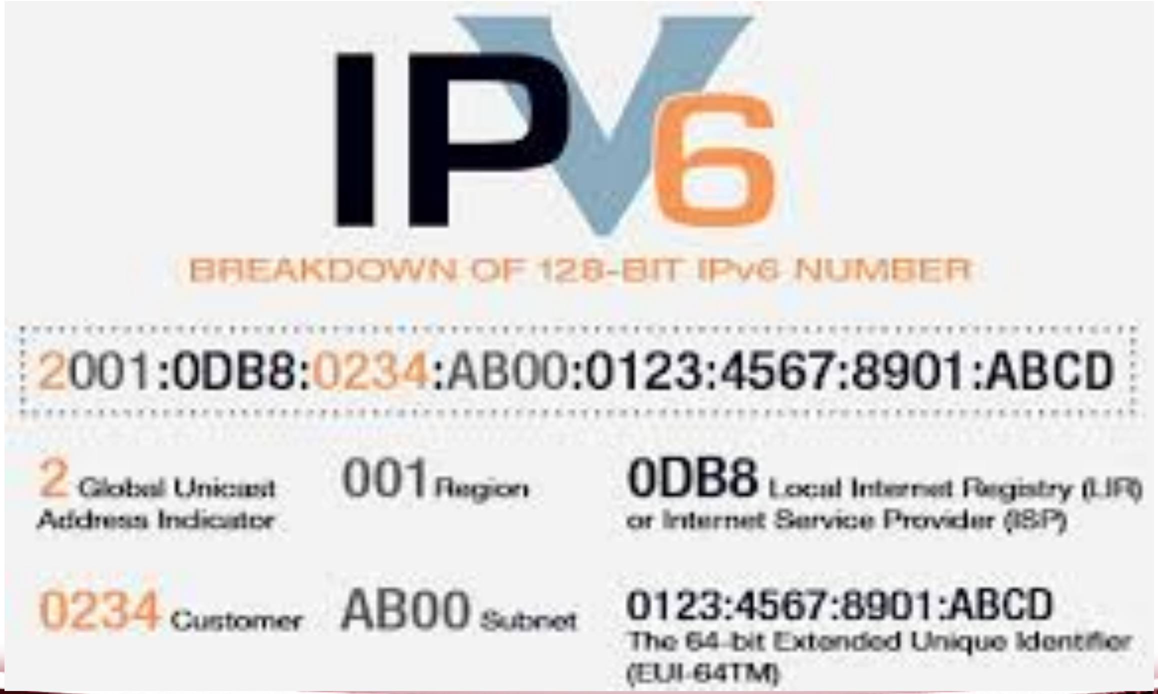
- When you try opening a website from your computer, the request is sent from your computer with a private IP address to your router, after which your router requests the website from your ISP using the public IP address assigned to your network.

- Once the request has been made, the operations are reversed - the ISP sends the contents of the website to the public IP address of your router, which forwards the address to the computer that asked for it.

IP Address(IPv6)

- For **IPv6** uses 128-bits for a total of approximately 3.4x10^{38} addresses.

- The address is divided into eight 16-bit parts. The format is 8 groups of four hexadecimal digits.



BREAKDOWN OF 128-BIT IPv6 NUMBER

2001:0DB8:0234:AB00:0123:4567:8901:ABCD

2 Global Unicast Address Indicator

001 Region

0DB8 Local Internet Registry (LIR) or Internet Service Provider (ISP)

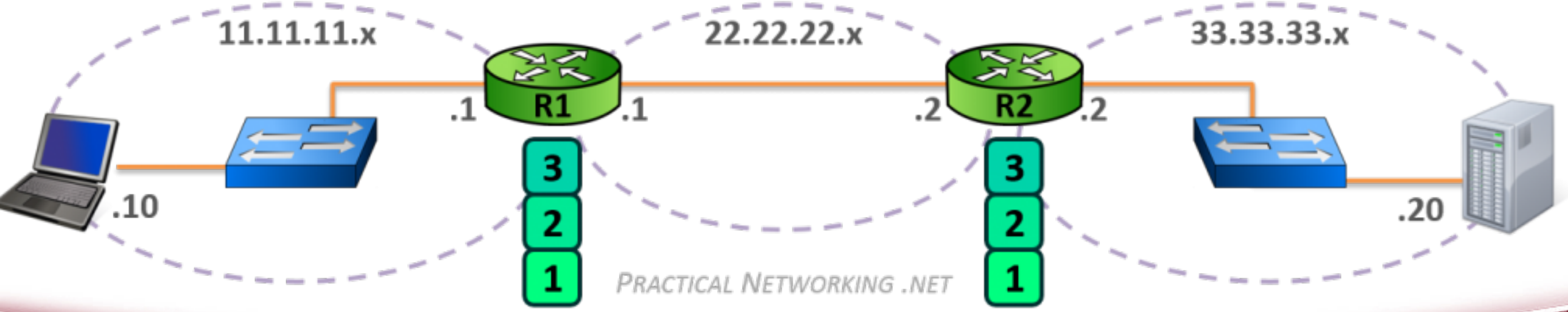
0234 Customer

AB00 Subnet

0123:4567:8901:ABCD The 64-bit Extended Unique Identifier (EUI-64TM)

Switch vs. Router

- A **switch** is a networking device that facilitates communication within a local area network using source and destination MAC addresses.
  - A switch is responsible for hop-to-hop delivery
  - A data unit sent by a switch is a frame.
- A **router** is a networking device that facilitates communication between networks using source and destination IP addresses.
  - A router is responsible for end-to-end delivery
  - A data unit sent by a router is a **packet**.



Host to Host

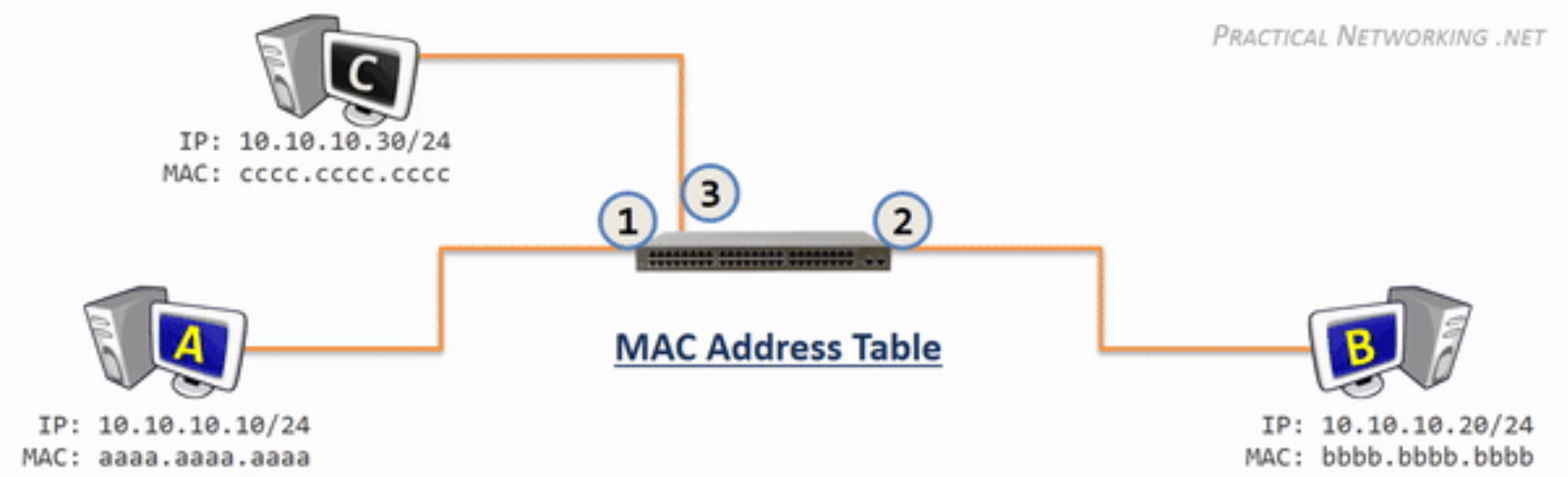
- Typically, when a computer tries to communicate with another computer, it knows the destination IP address.
  - E.g. the IP address of a shared printer is known to everyone in an office.
- However, it does not know the MAC address of the destination computer. A MAC address is needed for communication between two computers even if they are directly connected.
- To do this, it issues an **ARP(Address Resolution Protocol)** request.
- ARP uses an known IP address to discover an unknown MAC address.
  - Once discovered, the computer stored this information inside of an ARP table.
- The ARP request is send to all connected devices.

Switch

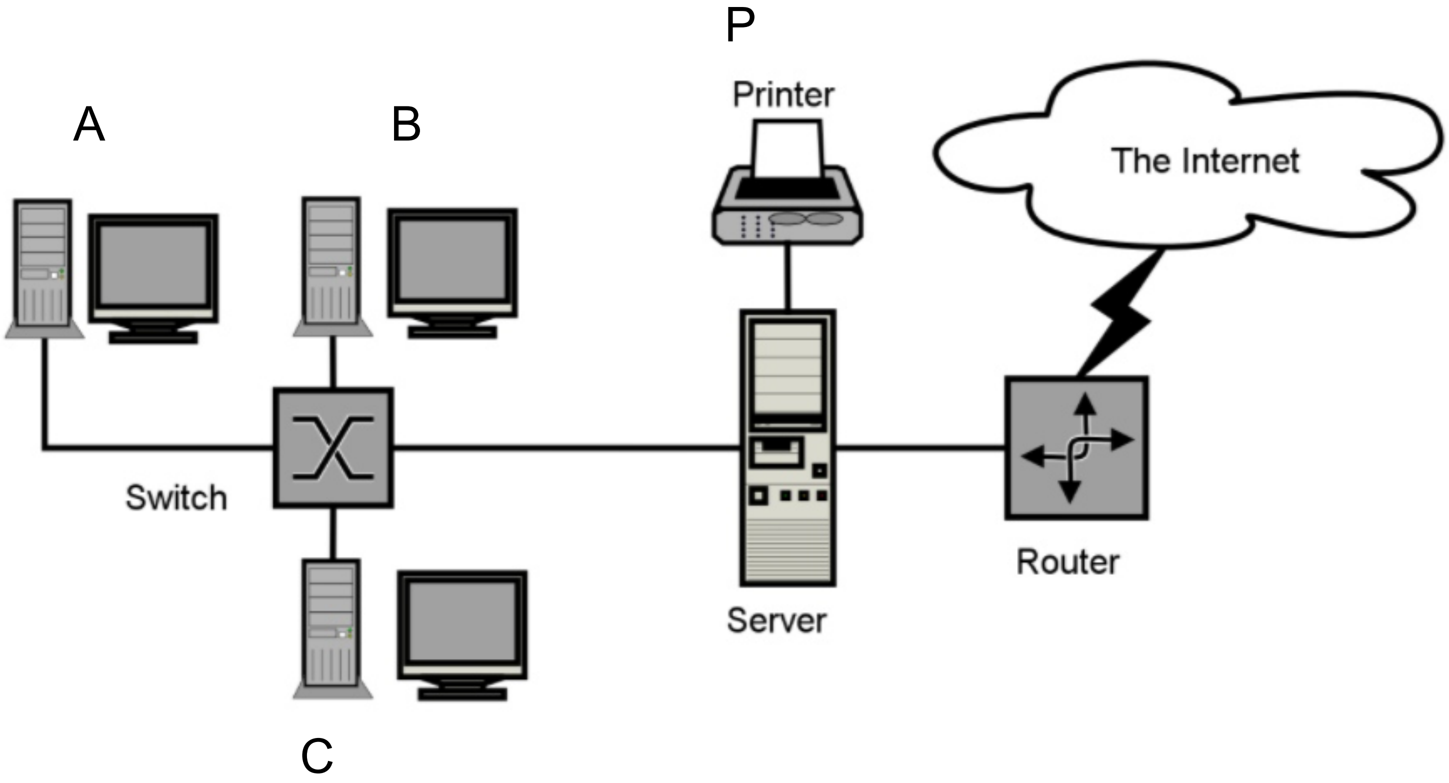
- A switch can forward frames locally within a LAN and makes forwarding decisions based on the source/destination MAC address found on the frame.
- It creates a **MAC address table**, mapping its **switchports** to MAC addresses of its connecting devices.
- The MAC address table starts out empty, and every time a Switch receives anything, it takes a look at the Source MAC address field of the incoming frame. It uses the Source MAC and the switchport the frame was received on to build an entry in the MAC Address Table.

Switch

- If a switch receives a frame with a unknown destination MAC address, it will duplicate the frame and send it out to all ports. (**flooding**)
- All computers connected to the switch will receive the frame. If a computer is not the intended destination, it will drop the frame.
- When the intended device receive the frame, it will generate a response and send it back to the switch.
- The switch then add this MAC address to its table.



How a packet travels within a LAN



How a packet travels within a LAN

- A client A computer wants to use a shared printer P in a LAN.
  - The client examines the IP address of the printer and recognizes that it is on the same LAN. If this IP address is on a different network, the client would forward the request through the default gateway which is the router.

- The client knows the IP address of the printer but doesn’t know its MAC address.

- It issues an ARP request that is sent to all connecting devices, in this case through the switch and to all devices connected to the switch.
  - This request essentially is the message “If you have this IP address, send me your MAC address.”

How a packet travels within a LAN

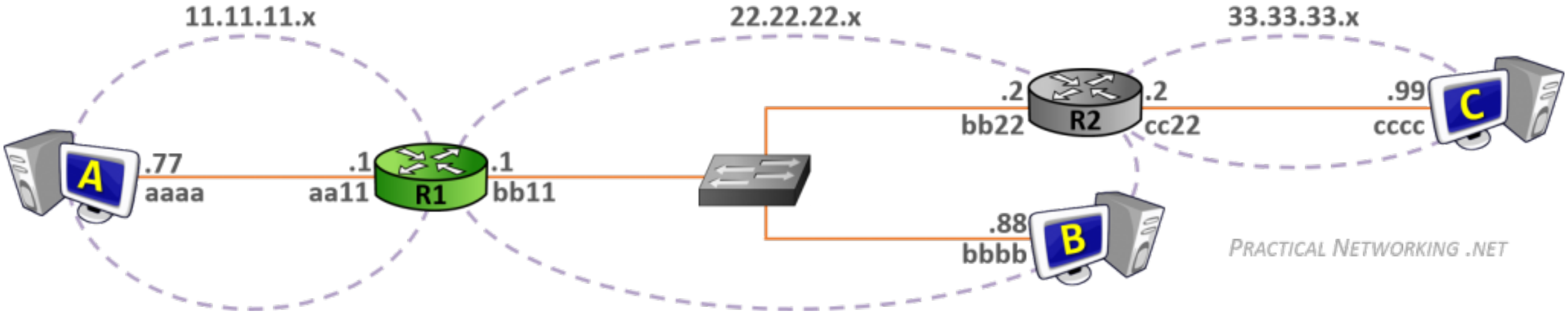
- Clients B and C drop the frame. Printer P realizes it is the intended recipient and generates a response with its MAC address.
- Once client A receives it, it starts sending the print job with the printer’s MAC address as the destination address.
- The switch can use the destination MAC address and forward the print job directly to the printer.

Router

- A router facilitates communication between networks.
- A router accomplishes all this by maintaining what is known as a **Routing Table**. This is a table that contains paths to all the networks a Router knows how to reach.
- These paths are sometimes known as Routes, and each entry contains either an interface or the IP address of the next router in the path to the target.

Router

- Every router populates and maintains a Routing Table and an ARP Table.
- From the perspective of each Router, the Routing Table is the map of all networks in existence.
- If a router receives a packet destined to a network it does not know about, then as far as that router is concerned, that network must not exist and that packet is discarded.



Network Applications

- A **network application** lets a computer interact with other computers by performing a specific set of tasks.
  - Browsers, email clients, etc…
- The application is responsible for managing the transmitting and receiving of data required to perform its tasks .
- The application has to be able to communicate with applications on other networked computers for it to be useful.

Network Applications

- A **network protocol** is a set of rules for how applications intercommunicate.
- Common protocols/applications include:
  - **Simple Mail Transfer Protocol**(SMTP), IMAP, and POP for email
  - **Hypertext Transfer Protocol**(HTTP) for sending/receiving webpages
  - **HTTPS(HTTP Secure)**
    - Encrypted with **SSL(Secure Socket Layer)** or the new **TLS(Transport Layer Security)**
  - **Telnet**
  - **Secure Shell Access**(SSH)
  - **File Transfer Protocol**(FTP)

TCP/IP

- **Transmission Control Protocol**(TCP) is the protocol that is responsible for sending data packets across the internet.

- TCP is a host-to-host protocol that provides **reliable**, **connection-oriented** communication over IP networks between two endpoints.
  - A TCP packet is sent using IP addresses, hence the term TCP/IP.
  - **reliable**: data received is intact, error-free and assembled in the correct order. Any lost data is retransmitted.
  - **Connection-oriented**: Using a system of acknowledgements called the Three-Way-Handshake, two computers confirm the connection before data transmission.

TCP/IP

- The suite of protocols that make up **TCP/IP(Transmission Control Protocol/Internet Protocol)** define:
  - How data is transmitted across a network
  - How data should be formatted so other networked systems can understand it

- TCP/IP is the standard for modern data communications across all networks.

- Another protocol similar to TCP is **User Datagram Protocol(UDP)**, which is a connectionless protocol.
  - Unlike TCP, UDP has no guarantee of delivery or correct assembly. It requires less overhead and is faster. (Skype uses UDP)

TCP/IP

- TCP/IP came out of ARPAnet the Department Of Defense(DoD)’s attempt to create a decentralized, no single point of failure network.
  - There were many network protocols in the 1990’s. The “Protocol Wars” ensued and TCP/IP won the war.

- Two key features TCP/IP features that support decentralization:
  - **End node verification**: the two endpoints of any data transfer are responsible for making sure it was successful – no centralized control scheme
  - **Dynamic routing**: End nodes can transfer data over multiple paths, and the network chooses the best (fastest, most reliable) path for each individual data transfer

Name Resolution

- Logical IP addresses are “friendlier” than physical MAC addresses, but still aren’t really human readable.

- **Domain Names**: structured, user friendly system names provided by TCP/IP. Examples of **top-level domain names**:
  - .com, .org, .edu, .gov, etc…

- **Name Resolution**: the process of mapping logical addresses back and forth into domain names
  - 172.217.10.46 is mapped to www.google.com
  - Special name servers store the mapping information in databases
  - TCP/IP’s Domain Name Service (DNS) provides a hierarchy of name servers that handle name resolution for the Internet.

Port Numbers

- An IP address identifies a computer on the internet; a **port number** is a 16-bit number identifies the application or service on a computer/server.

- A **port** is a logical connection used by programs to exchange information. There are 65536 TCP ports on a computer; each with a 16-bit port number from 0 to 65535. (There are also 65536 UDP ports)
  - This allows a computer to use different network applications simultaneously. Data packets from different applications use different ports.
  - E.g. if I have a browser and an email client such as Apple Mail or Microsoft Outlook, then at least two ports are needed for data transfer.
  - Even within the same webpage request, multiple ports can be used to download the html, images, javascript files, etc… simultaneously.

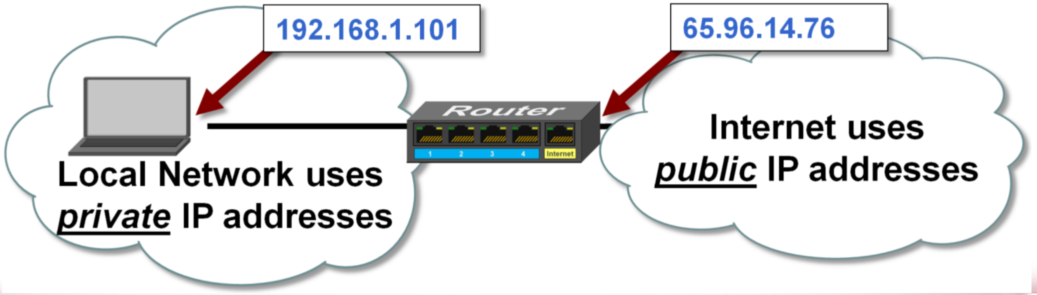
Port Numbers

- The port numbers in the range from 0 to 1023 are the **well-known ports**. They are used to identify widely used types of network services.
  - Port 80 for HTTP, Port 21 for FTP, port 25 SMTP, port 23 for Telnet.

- To make a HTTP request for a website, a TCP connection is established.
  - This connection includes among other things the IP address and port number of the client and the IP address and the port number of the server.
  - The port number of the client is dynamically assigned to a random port above 1023**(ephemeral ports)**. The port number of the server is one of the well-known port.

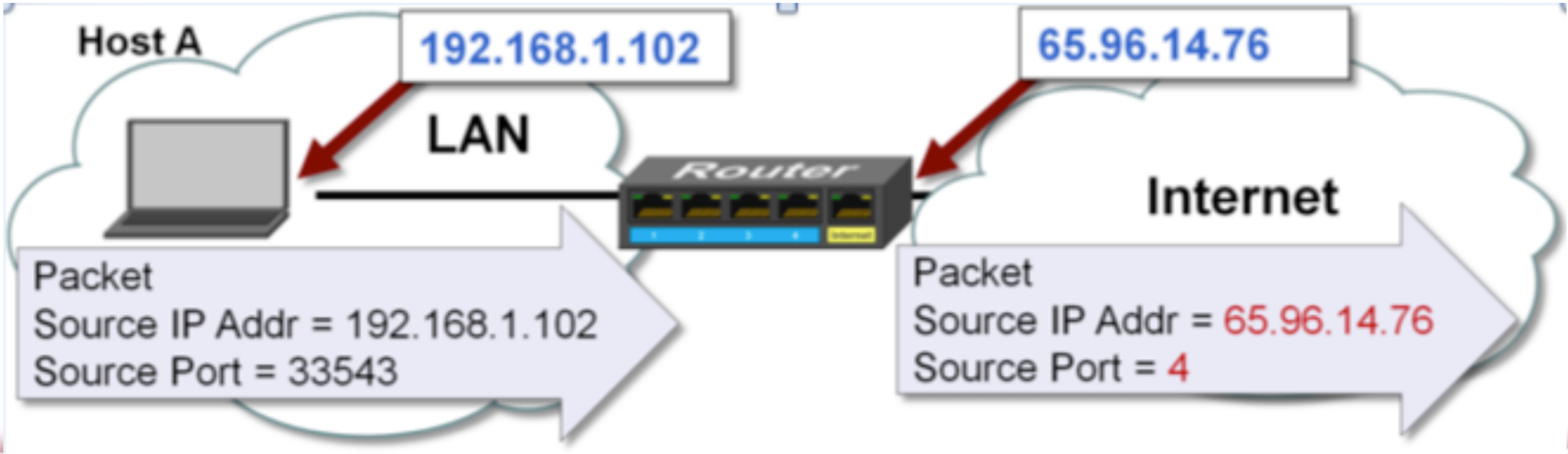
Network Address Translation(NAT)

- **Network address translation**(NAT) translates local, private IP addresses to public IP addresses. NAT helps conserve the limited IPv4 address space.
- All hosts that connect to the local network are assigned with local network IP addresses by the **Dynamic Host Configuration Protocol**(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.
  - In your home network, your tablets, laptops, smart TV, etc… all share one public IP address.



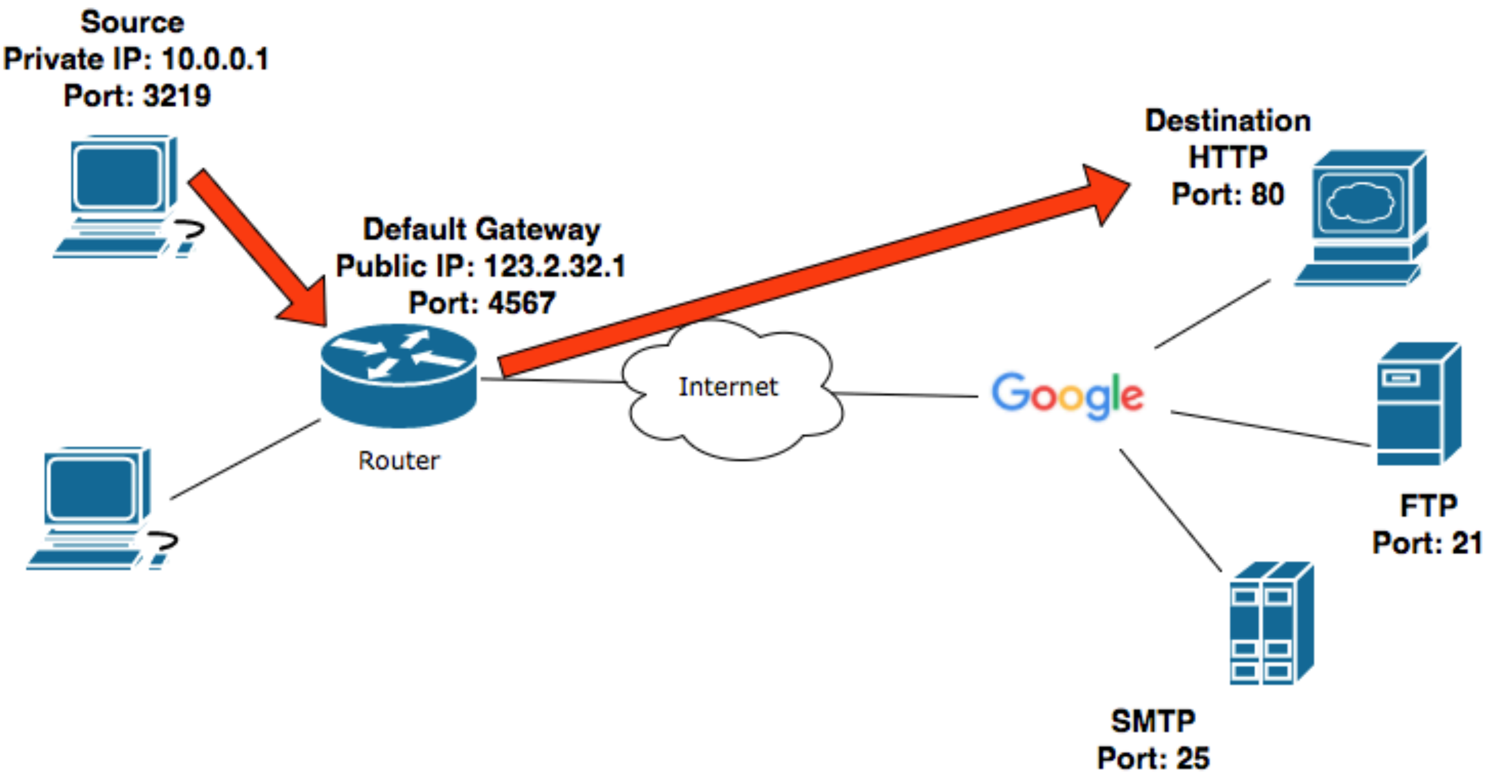
Network Address Translation(NAT)

- 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.



Port Numbers

- A webpage(HTTP) request from a computer.



Source
Private IP: 10.0.0.1
Port: 3219

Default Gateway
Public IP: 123.2.32.1
Port: 4567

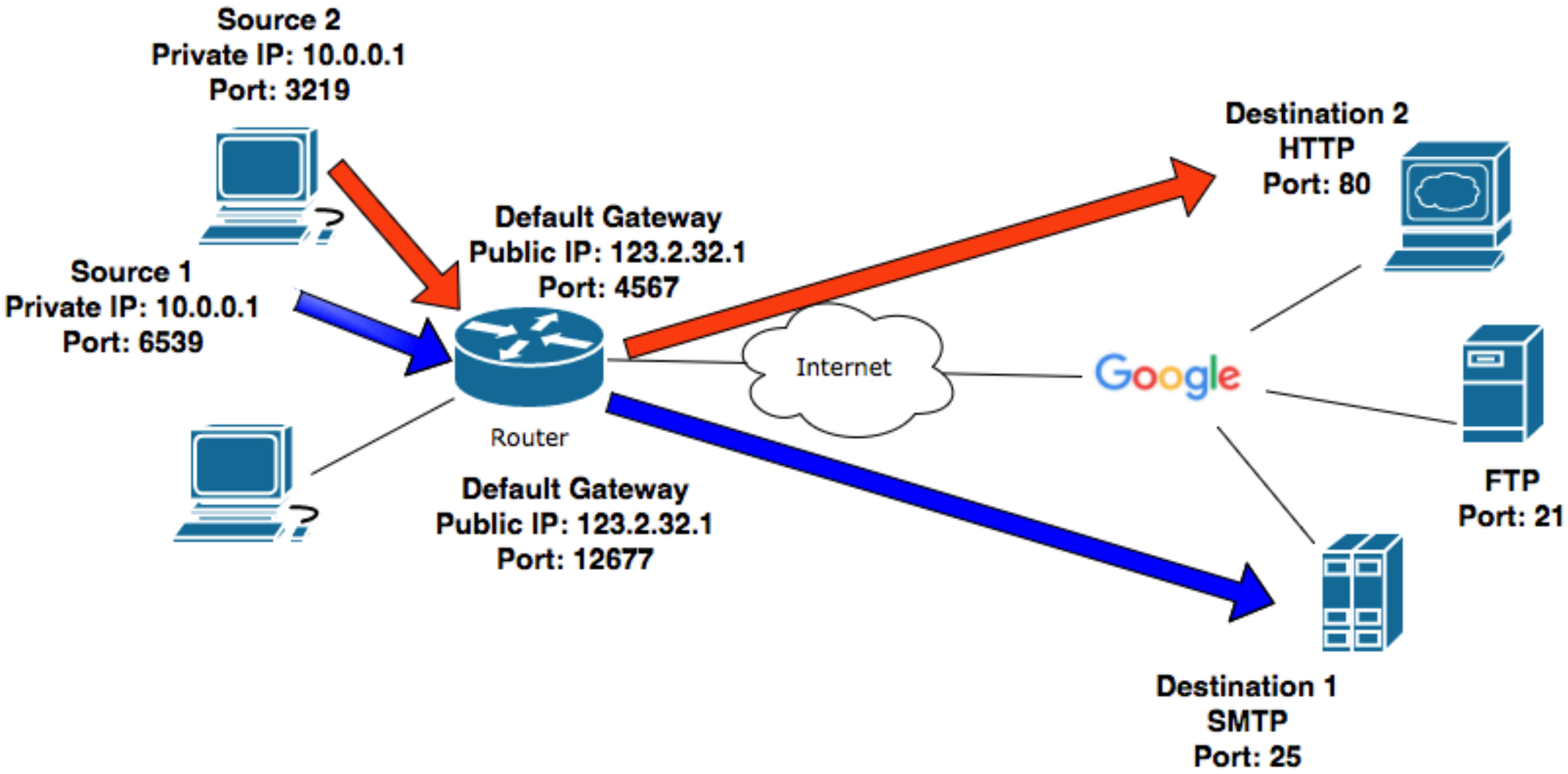
Destination
HTTP
Port: 80

FTP
Port: 21

SMTP
Port: 25

Port Numbers

- A webpage request and sending an email from the same computer.



Source 2
Private IP: 10.0.0.1
Port: 3219

Source 1
Private IP: 10.0.0.1
Port: 6539

Default Gateway
Public IP: 123.2.32.1
Port: 4567

Default Gateway
Public IP: 123.2.32.1
Port: 12677

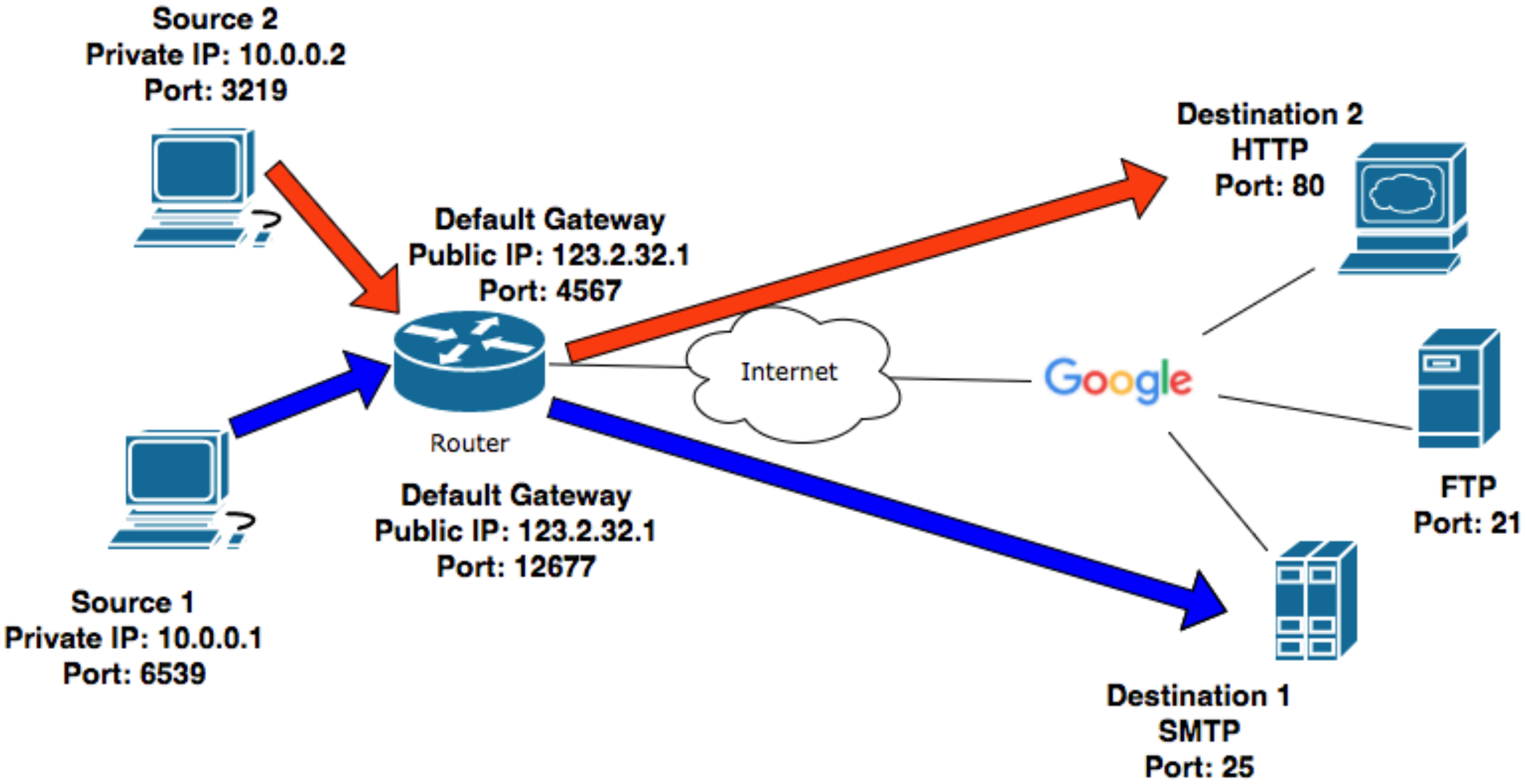
Destination 2
HTTP
Port: 80

FTP
Port: 21

Destination 1
SMTP
Port: 25

Port Numbers

- Computer 1 sending an email. Computer 2 requesting a webpage. Both computers are in the same local area network.



TCP/IP Model

The TCP/IP protocols map to five-layer conceptual model. The four layers are:

1)Application Layer

2)Transport Layer

3)Internet or Network Layer

4)Data Link Layer

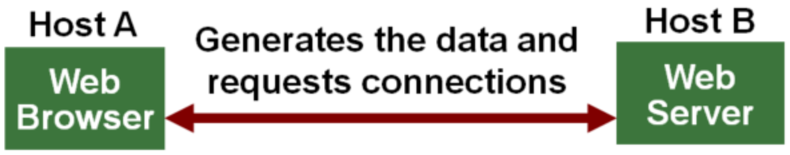
5)Physical Layer

Another popular model used to explain network protocols is the **OSI** model. To be explored in the problem set.

TCP/IP 5-Layer Model

5 Application Layer

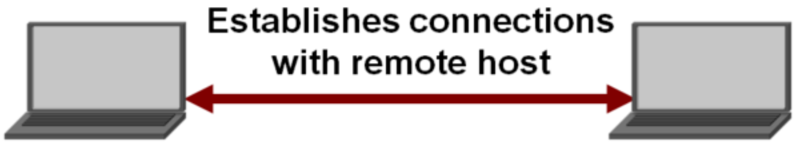
The Application layer is the group of applications requiring network communications.



Generates the data and requests connections

4 Transport Layer (TCP/UDP)

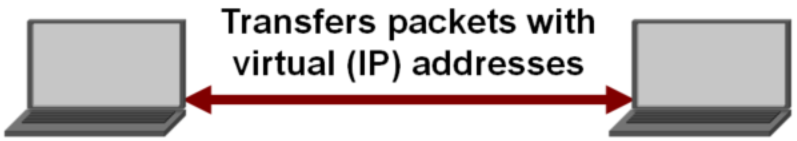
The Transport layer establishes the connection between applications on different hosts.



Establishes connections with remote host

3 Network Layer (IP)

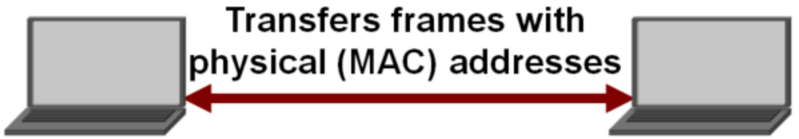
The Network layer is responsible for creating the packets that move across the network.



Transfers packets with virtual (IP) addresses

2 Data Link Layer (MAC)

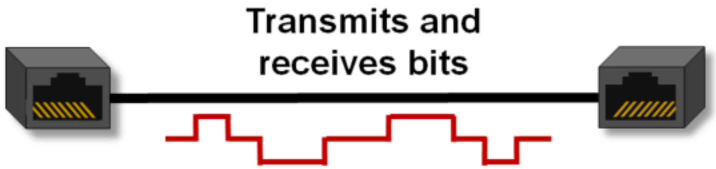
The Data Link layer is responsible for creating the frames that move across the network.



Transfers frames with physical (MAC) addresses

1 Physical Layer

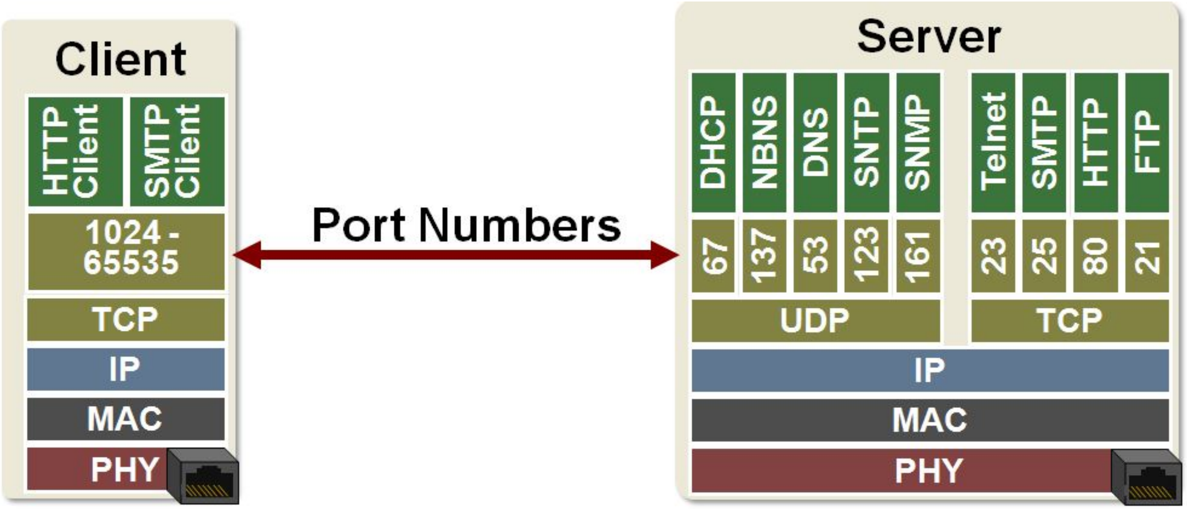
The Physical layer is the transceiver that drives the signals on the network.



Transmits and receives bits

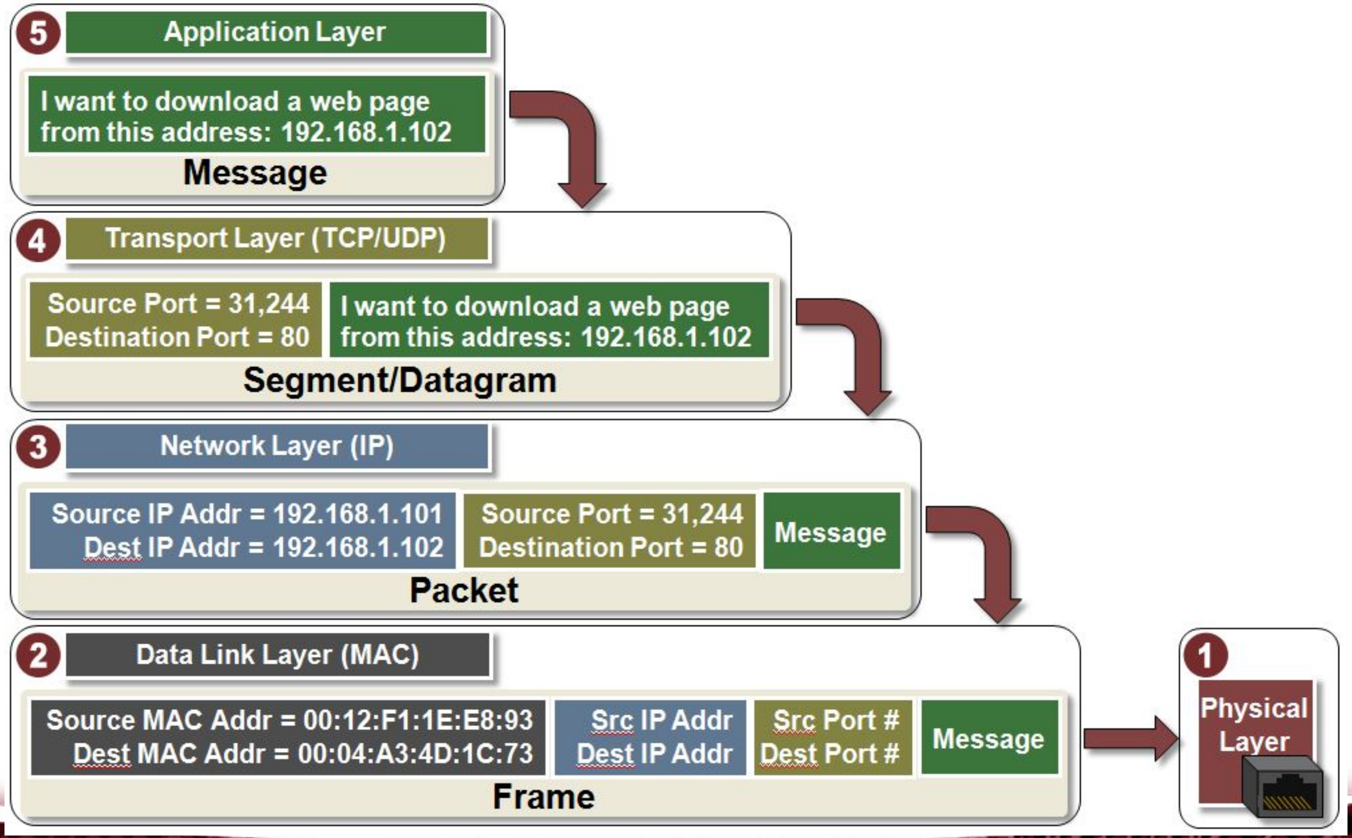
Client-Server

- A client requesting some service from a server is dynamically allocated a high source port(1024-65535). The destination port however has to be a well-known port.
  - E.g. the client HTTP is assigned port 1120 making a request for a webpage must have destination port 80.



Packets

- A message that needs to be sent across the internet receives headers from each layer as it travels down the protocol stack. The headers provide routing/addressing information, e.g., port numbers, IP addresses, MAC addresses, etc…



5 Application Layer

I want to download a web page from this address: 192.168.1.102

Message

4 Transport Layer (TCP/UDP)

Source Port = 31,244
Destination Port = 80

I want to download a web page from this address: 192.168.1.102

Segment/Datagram

3 Network Layer (IP)

Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102

Source Port = 31,244
Destination Port = 80

Message

Packet

2 Data Link Layer (MAC)

Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73

Src IP Addr
Dest IP Addr

Src Port #
Dest Port #

Message

Frame

1 Physical Layer

How a packet travels across the internet

- A message(data) that needs to be sent starts at the top of the application layer.
- It travels down the protocol stack to the Transport Layer. The message is broken down into segments and sent separately across the internet using TCP.
- Each segment has a header which contains source/destination port numbers, label number etc…
  - Using UDP, segments are called datagrams.
- Each segment moves down to the Internet or Network Layer and receives a Internet header which contains source/destination IP addresses.(packet)
- The packet then travels down to the Data Link layer where it receives a Data Link header containing for example source/destination MAC addresses.

How a packet travels across the internet

- The headers from the Transport and Network Layers are unchanged during the data’s journey across the internet.
- The header from the Data Link layer, however, will change as the data hops from router to router.
- Suppose we have a packet on its way across the internet and it is currently located at some router R1. R1 will inspect the destination IP address and determines the best hop to the next router R2.
- R1 creates a new frame header containing the source MAC address of R1 and the destination MAC address of R2. Then it sends the entire frame to R2.
- Once R2 receives the frame and inspects it, it realizes that it is the intended recipient and removes the frame header. It examines the destination IP address and from its routing table determines the next hop to R3. This process is repeated until it arrives at the correct LAN of the receiving computer.

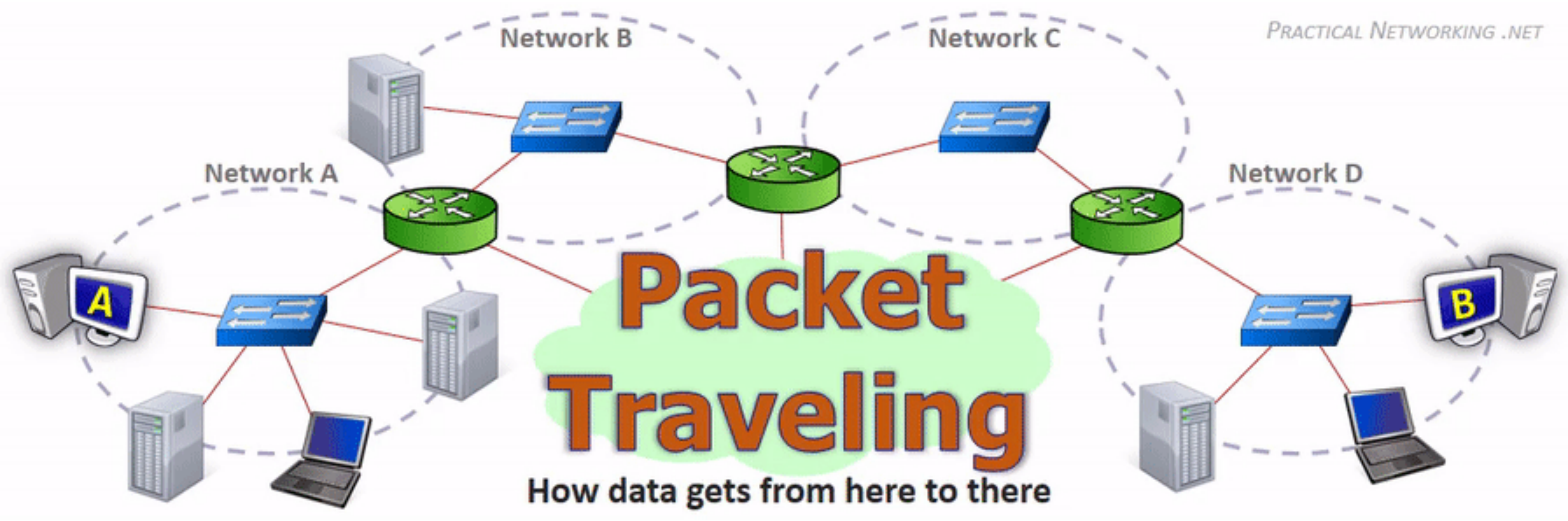
TCP/IP model

- Layers of TCP/IP with protocol examples, protocol data units, addressing and network devices.

Layer	Protocol	Protocol Data Unit	Addressing	Devices
Application	HTTP, SMTP	Message or Data	n/a	VOIP
Transport	TCP/UDP	Segment/Datagram	Port #'s	Firewalls
Internet or Network	IP	Packet	IP Address	Routers
Data Link	Ethernet, WI-FI	Frame	MAC Address	Switchs, Bridges
Physical	10 Base T, 802.11	Bits	n/a	Hubs, Repeaters

Packet Travelling

- The following GIF is from a detailed video explaining how a packet travel across the internet. It provides a good review of many of the concepts covered in this lecture. Please watch it!
- https://www.youtube.com/watch?v=rYodcvhh7b8



TCP/IP Model

- The Physical Layer is the physical medium carrying the 0’s and 1’s bits across the wire.
- The Link Layer is responsible for hop-to-hop delivery and uses MAC addresses.
- The Internet or Network Layer is responsible for end-to-end delivery and uses IP addresses.
- The Transport Layer is responsible for service-to-service delivery and uses port numbers.

Homework

1)Read and reread these lecture notes.

2)Watch the following short videos.(Required)

- Hub vs. Switch vs Router: https://www.youtube.com/watch?v=1z0ULvg_pW8
- Port Forwarding: https://www.youtube.com/watch?v=2G1ueMDgwxw
- TCP vs. UDP: https://www.youtube.com/watch?v=uwoD5YsGACg
- DHCP Explained: https://www.youtube.com/watch?v=e6-TaH5bkjo
- Packet Travelling: https://www.youtube.com/watch?v=rYodcvhh7b8
- OSI Model: https://www.youtube.com/watch?v=LANW3m7UgWs

3)Optional video: This video is about 30 mins but is a nice Prezi presentation on TCP/IP and the OSI Model. Highly recommended!

- https://www.youtube.com/watch?v=e5DEVa9eSN0

References

1) InetDaemon. (2014, September). Networking Tutorials. Retrieved from http://www.inetdaemon.com/tutorials/networking/

2) Allen, Scott. (2012, January). A Software Developer's Guide to HTTP. Retrieved from

https://odetocode.com/Articles/741.aspx

3) Microchip Technology.(2018). Introduction to TCP/IP. Retrieved from

http://microchipdeveloper.com/tcpip:tcpip-intro-video