BIT 6113

Database Management System

Saroj Ghimire

saroj.ghimire2@texascollege.edu.np

Lincoln University College

IP

• IP Address

• IP Addressing

• IP Addressing Classes

• Netmask

• Subnet Addressing

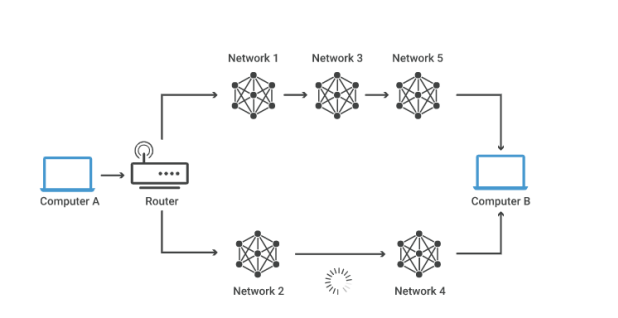
(See these topics for the reference materials)

IP Routing

• **What is routing?**

• Network routing is the process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public transportation. In packet-switching networks, such as the Internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.

• Consider the image, For a data packet to get from Computer A to Computer B, should it pass through networks 1, 3, and 5 or networks 2 and 4? The packet will take a shorter path through networks 2 and 4, but networks 1, 3, and 5 might be faster at forwarding packets than 2 and 4. These are the kinds of choices network routers constantly make.



**How does routing work?**

• Routers refer to internal routing tables to make decisions about how to route  packets along network paths. A routing table records the paths that packets should take to reach every destination that the router is responsible for. Think of train timetables, which train passengers consult to decide which train to catch. Routing tables are like that, but for network paths rather than trains.

• Routers work in the following way: when a router receives a packet, it reads the  headers\* of the packet to see its intended destination, like the way a train conductor may check a passenger's tickets to determine which train they should go on. It then determines where to route the packet based on information in its routing tables.

• Routers do this millions of times a second with millions of packets. As a packet  travels to its destination, it may be routed several times by different routers.

• Routing tables can either be static or dynamic. Static routing tables do not  change. A network administrator manually sets up static routing tables. This essentially sets in stone the routes data packets take across the network, unless the administrator manually updates the tables.

• Dynamic routing tables update automatically. Dynamic routers use various routing  protocols (see below) to determine the shortest and fastest paths. They also make this determination based on how long it takes packets to reach their destination — similar to the way Google Maps, Waze, and other GPS services determine the best driving routes based on past driving performance and current driving conditions.

• Dynamic routing requires more computing power, which is why smaller networks  may rely on static routing. But for medium-sized and large networks, dynamic routing is much more efficient.

**What are the main routing protocols?**

• In networking, a protocol is a standardized way of formatting data so that any connected computer can understand the data. A routing protocol is a protocol used for identifying or announcing network paths.

• The following protocols help data packets find their way across the Internet: • **IP:** The Internet Protocol (IP) specifies the origin and destination for each data packet. Routers inspect each packet's IP header to identify where to send them.

• **BGP:** The Border Gateway Protocol (BGP) routing protocol is used to announce which networks control which IP addresses, and which networks connect to each other. (The large networks that make these BGP announcements are called autonomous systems.) BGP is a dynamic routing protocol.

The below protocols route packets within an AS:

• **OSPF:** The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

• **RIP:** The Routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way. (When a packet goes from one network to another, this is known as a "hop.")

• Other interior routing protocols include EIGRP (the Enhanced Interior Gateway Routing Protocol, mainly for use with Cisco routers) and IS-IS (Intermediate System to Intermediate System).

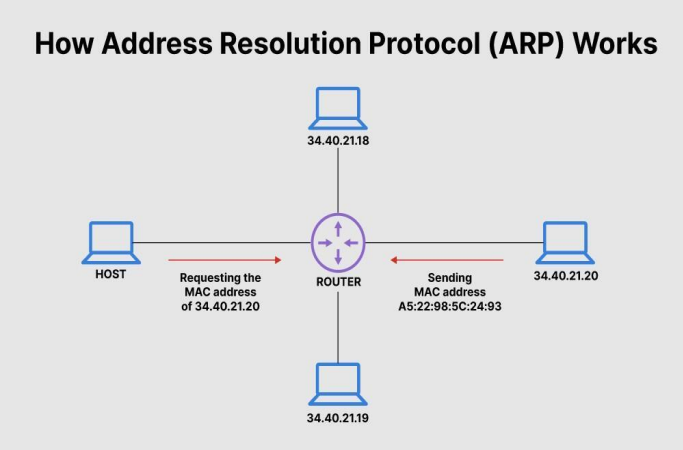
ARP

• Address Resolution Protocol (ARP) is a protocol or procedure that connects an  ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

• This mapping procedure is important because the lengths of the IP and MAC  addresses differ, and a translation is needed so that the systems can recognize one another. The most used IP today is IP version 4 (IPv4). An IP address is 32 bits long. However, MAC addresses are 48 bits long. ARP translates the 32-bit address to 48 and vice versa.

• There is a networking model known as the Open Systems Interconnection (OSI)  model. First developed in the late 1970s, the OSI model uses layers to give IT teams a visualization of what is going on with a particular networking system. This can be helpful in determining which layer affects which application, device, or software installed on the network, and further, which IT or engineering professional is responsible for managing that layer.

• The MAC address is also known as the data link layer, which establishes and  terminates a connection between two physically connected devices so that data transfer can take place. The IP address is also referred to as the network layer or the layer responsible for forwarding packets of data through different routers. ARP works between these layers.



ARP

• **What Does ARP Do and How Does It Work?**

• When a new computer joins a local area network (LAN), it will receive a unique IP address to use for identification and communication.

• Packets of data arrive at a gateway, destined for a particular host machine. The gateway, or the piece of hardware on a network that allows data to flow from one network to another, asks the ARP program to find a MAC address that matches the IP address. The ARP cache keeps a list of each IP address and its matching MAC address. The ARP cache is dynamic, but users on a network can also configure a static ARP table containing IP addresses and MAC addresses.

• ARP caches are kept on all operating systems in an IPv4 Ethernet network. Every time a device requests a MAC address to send data to another device connected to the LAN, the device verifies its ARP cache to see if the IP-to-MAC-address connection has already been completed. If it exists, then a new request is unnecessary. However, if the translation has not yet been carried out, then the request for network addresses is sent, and ARP is performed.

• An ARP cache size is limited by design, and addresses tend to stay in the cache for only a few minutes. It is purged regularly to free up space. This design is also intended for privacy and security to prevent IP addresses from being stolen or spoofed by cyber attackers. While MAC addresses are fixed, IP addresses are constantly updated.

• In the purging process, unutilized addresses are deleted; so is any data related to unsuccessful attempts to communicate with computers not connected to the network or that are not even powered on.

Broadcast

• A broadcast is a data packet destined for all hosts on a particular physical network. Network hosts recognize broadcasts by special addresses.

• Limited broadcast—A packet is sent to a specific network or series of networks. A limited broadcast address includes the network or subnet fields. In a limited broadcast packet destined for a local network, the network identifier portion and host identifier portion of the destination address is either all ones (255.255.255.255) or all zeros (0.0.0.0).

• Flooded broadcast—A packet is sent to every network. • Directed broadcast—A packet is sent to a specific destination address where only the host portion of the IP address is either all ones or all zeros (such as 192.20.255.255 or 190.20.0.0).

Network Socket

• A network socket is defined by the IP address of the machine, the port on which it uses. For example, if we have a website running on IP address 100.1.1.1, the socket corresponding to the HTTP server for that site would be 100.1.1.1:80.

• Sockets are classified into stream sockets, socket.SOCK\_STREAM, or datagram sockets, socket.SOCK\_DGRAM, depending on the underlying protocol we use.

• SOCK\_STREAM: It is associated with the TCP protocol and provides security in the transmission of data and security in the data reception. In connection-oriented communication, there must be a channel established before we transfer data.

• SOCK\_DGRAM: It is associated with the UDP protocol and indicates that packets will travel in the datagram type, which has an asynchronous communication style. For UDP sockets, we can send out data without a connection. So this is called connection-less.

Introduction of TCP Sockets

• TCP sockets provide an open bi-directional connection between two endpoints. Each connection is uniquely identified using the combination of the client socket and server socket, which in turn contains four elements: the client IP address and port, and the server IP address and port. We call this a TCP socket pair.

• For example, we are sending an HTTP request from our client at 120.1.1.1 to the website at 189.1.1.1. The server for that website will use well-known port number 80, so its socket is 189.1.1.1:80, as we saw before. we have been ephemeral port number 3022 for the web browser, so the client socket is 120.1.1.1:3022. The overall connection between these devices can be described using this socket pair: (189.1.1.1:80, 120.1.1.1:3022).

• Advantage of TCP Sockets

• **Is reliable:** packets dropped in the network are detected and retransmitted by the sender.

• **Has in-order data delivery:** data is read by our application in the order it was written by the sender.

• On a TCP/IP network every device must have an IP address. • The **IP address identifies the device** e.g. computer. • However an IP address alone is not sufficient for running

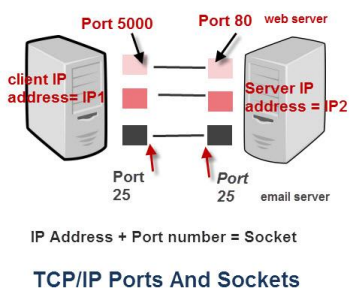
network applications, as a computer can run **multiple applications** and/or **services**.

• Just as the IP address identifies the computer, The network **port** identifies the **application or service** running on the computer.

• **Analogy**

• If you use a house or apartment block analogy the IP address corresponds to the street address.

• All of the apartments share the same street address. • However each apartment also has an apartment number which corresponds to the Port number.



**Port Number Ranges and Well Known Ports**

• A port number uses 16 bits and so can therefore have a value from **0** to **65535** decimal

• Port numbers are divided into ranges as follows:

• **Port numbers 0-1023 – Well known ports.** These are allocated to **server services** by the **Internet Assigned Numbers Authority** (IANA). e.g Web servers normally use **port 80** and SMTP servers use **port 25** (see diagram above).

• **Ports 1024-49151- Registered Port** -These can be registered for services with the **IANA** and should be treated as **semi reserved.** User written programs should not use these ports. • **Ports 49152-65535**– These are used by **client programs** and you are free to use these in client programs. When a Web browser connects to a web server the browser will allocate itself a port in this range. Also known as **ephemeral ports**.

Socket

• A connection between two computers uses a socket.

• A socket is the combination of IP address plus port

• Each end of the connection will have a socket.

• Imagine sitting on your PC at home, and you have two browser windows open. • One looking at the Google website, and the other at the Yahoo website.

• The connection to Google would be:

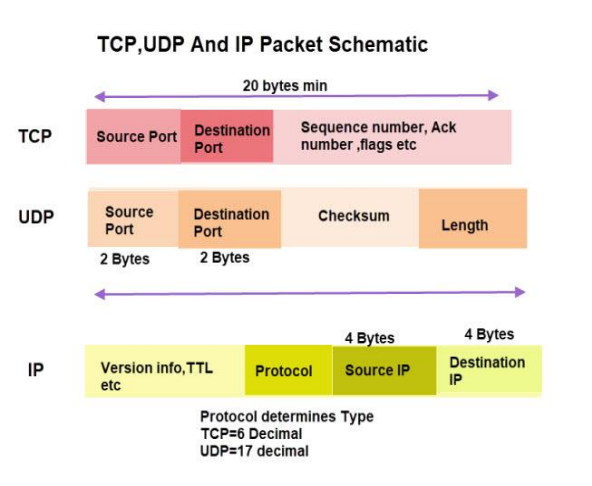
• Your PC – IP1+port 60200 ——– Google IP2 +port 80 (standard port)

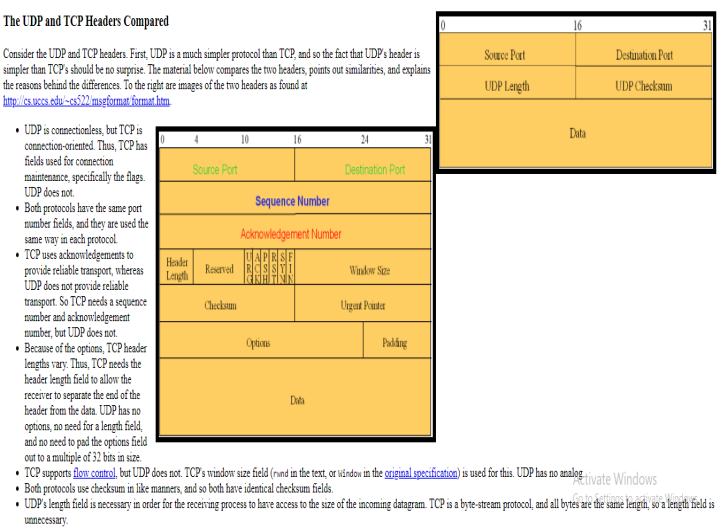
• The combination IP1+60200 = the socket on the client computer and IP2 + port 80 = destination socket on the Google server.

• The connection to Yahoo would be:

• your PC – IP1+port 60401 ——–Yahoo IP3 +port 80 (standard port)

• The combination IP1+60401 = the socket on the client computer and IP3 + port 80 = destination socket on the Yahoo server





Application Layer

• An application layer is the topmost layer in the TCP/IP model. • It is responsible for handling high-level protocols, issues of representation.

• This layer allows the user to interact with the application. • When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

• There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol

**Domain Name System (DNS) in Application Layer**

• DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

• Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

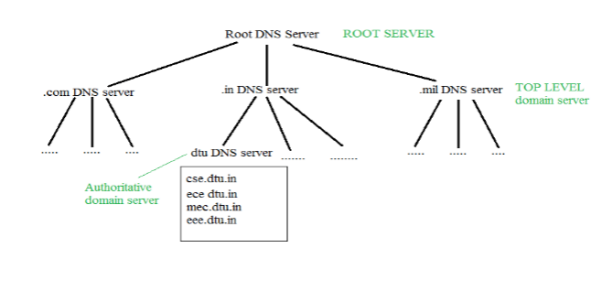
• **Domain :**

There are various kinds of DOMAIN :

• Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain. • Country domain .in (india) .us .uk

• Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

**Organization of Domain**

****

DNS

• It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.

**DNS record** – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

• **Namespace** – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –

• **Name server** – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.