NETWORK PROGRAMMING AND PROTOCOL COMP 416

INTRODUCTION

PRE – TEST (15MINUTES)

- Define network routing.
- What is the function of a router?
- Differentiate between a network ID and a host ID.
- What is IP addressing?
- Differentiate between IPv4 and IPv6
- Define the bandwidth and the capacity of a link.

COVERAGE

- An Introduction
- Addressing and Internet Service: Overview
- Network Routing: Overview
- IP Addressing
- On Architectures
- Protocol Stack Architecture
- Routing Architecture

AN INTRODUCTION

- If anyone were to send a postcard with minimal address information such as “Jack Ma, China” or “Donald Trump, USA,” it would be routed to them due to their fame; no listing of the street address or the city name would be necessary.
- The postal system can do such routing to famous personalities usually on a case-by-case basis, relying on the name alone.
- In an electronic communication network, a similar phenomenon is possible to reach *any* website or to contact *any person by telephone anywhere in the world without knowing where* the site or the person is currently located.

AN INTRODUCTION

- Not only that, it is possible to do so very efficiently, within a matter of a few seconds.
- How is this possible in a communication network, and how can it be done so quickly?
- At the heart of the answer to this question lies *network routing*.
- **Network routing** refers to the ability of an electronic communication network to send a unit of information from point A to point B by *determining a path* through the network, and by doing so efficiently and quickly.

AN INTRODUCTION

- In a communication network, *addressing* and how it is structured and used plays a critical role.
- In many ways, addressing in a communication network has similarities to postal addressing in the postal system.
- A typical postal address that we write on a postcard has several components—the name of the person, followed by the street address with the house number ("house address"), followed by the city, the state name, and the postal code.

AN INTRODUCTION

- Take the processing view to route the postcard to the right person, we essentially need to consider this address in the reverse order of listing, i.e., start with the postal code, then the city or the state name, then the house address, and finally the name of the person.
- We can reduce this information somewhat; that is, you can just use the postal code and leave out the name of the city or the name of the state, since this is redundant information.
- This means that the information needed in a postal address consists of three main parts: the postal code, the street address (with the house number), and the name.

AN INTRODUCTION

- If we look at it in another way, the place where the postcard originated in fact does not need to know the detailed information of the street or the name to start with; the postal code is sufficient to determine to which geographical area or city to send the card.
- Thus, we can see that postal routing uses *address hierarchy* for routing decisions.
- An important requirement of this hierarchical view is that there must be a way to divide the complete address into multiple distinguishable parts to help with the routing decision.

AN INTRODUCTION

- Now consider an electronic communication network; for example, a critical communication network of the modern age is the Internet.
- Naturally, the first question that arises is: how does addressing work for routing a unit of information from one point to another, and is there any relation to the postal addressing hierarchy that we have just discussed?
- Second, how is service delivery provided? In the next section, we address these questions.

ADDRESSING AND INTERNET SERVICE: AN OVERVIEW

- The addressing in the Internet is referred to as *Internet Protocol (IP) addressing*.
- An IP address defines two parts: one part that is similar to the postal code and the other part that is similar to the house address; in Internet terminology, they are known as the *netid* and the *hostid,* to identify a network and a host address, respectively.
- Thus, a host is the end point of communication in the Internet and where a communication starts.

ADDRESSING AND INTERNET SERVICE: AN OVERVIEW

- A host is a generic term used for indicating many different entities; the most common ones are a web-server, an email server, and certainly the desktop, laptop, or any computer we use for accessing the Internet.
- A netid identifies a contiguous block of addresses.
- Like any service delivery system, we also need a delivery model for the Internet.
- For example, in the postal system, one can request guaranteed delivery for an additional fee.
- The Internet’s conceptual framework, known as *TCP/IP (Transmission Control Protocol/Internet Protocol),* relies on a delivery model in which TCP is in charge of the reliable delivery of information, while IP is in charge of routing, using the IP addressing mechanism.

ADDRESSING AND INTERNET SERVICE: AN OVERVIEW

- IP, however, does not worry about whether the information is reliably delivered to the address or is lost during transit.
- A key difference in the Internet as opposed to the postal system is that the sending host first sends a beacon to the destination address (host) to see if it is reachable, and waits for an acknowledgment *before* sending the actual message.
- Since the beacon also uses the same transmission mechanism, i.e., IP, it is possible that it may not reach the destination. In order to allow for this uncertainty to be factored in, another mechanism known as a *timer* is used.

Addressing and Internet service: an overview

- That is, the sending host sends the beacon, then waits for a certain amount of time to see if it receives any response.
- If it does not hear back, it tries to send the beacon a few more times, waiting for a certain amount of time before each attempt, until it stops trying after reaching the limit on the maximum number of attempts.
- The basic idea, then, requires that the receiving host should *also* know the address of the sender so that it can acknowledge the receipt of the beacon. As you can see, this means that when the sending host sends its beacon, it must also include its source IP address.

Addressing and internet service: an overview

- The actual transmission of the content transpires once the connectivity is established.
- Transport system analogy:
- A group of 100 friends wanting to go to a game, a car can hold five people, 20 cars needed to transport them.
- A document that we want to download from a host (web-server) is 2 MB.
- It cannot be accommodated entirely into a single fundamental unit of IP, known as *packet or datagram*, due to a limitation imposed by the *Maximum Transmission Unit* (MTU).

ADDRESSING AND INTERNET SERVICE: AN OVERVIEW

- The document would need to be broken down into smaller units that fit into packets.
- Each packet is then labeled with both the destination and the source address, which is then routed through the Internet toward the destination.
- The IP delivery mechanism is assumed to be unreliable, any such packet can possibly get lost during transit, and would need to be retransmitted if the timer associated with this packet expires.
- Content that has been broken down into smaller packets, once it arrives at the destination, needs to be reassembled in the proper order before delivering the document.

Network Routing: Overview

- Packets are to be routed from a source to a destination.
- Such packets may need to traverse many cross-points, similar to traffic intersections in a road transportation network.
- Cross-points in the Internet are known as *routers*.
- A router's functions are to read the destination address marked in an incoming IP packet, to consult its internal information to identify an outgoing link to which the packet is to be forwarded, and then to forward the packet.

Network Routing: Overview

- A network link that connects two routers is limited by how much data it can transfer per unit of time, commonly referred to as the *bandwidth* or *capacity* of a link; it is generally represented by a data rate, such as 1.54 megabits per second (Mbps).
- A network then carries *traffic* on its links and through its routers to the eventual destination; traffic in a network refers to packets generated by different applications, such as web or email.

NETWORK ROUTING: OVERVIEW

- Suppose that traffic suddenly increases, for example, because of many users trying to download from the same website; then, packets that are generated can possibly be queued at routers or even dropped.
- Since a router maintains a finite amount of space, known as a *buffer*, to temporarily store backlogged packets, it is possible to reach the buffer limit.
- The basic principle of TCP/IP allows the possibility of an IP packet not being delivered or being dropped enroute, the finite buffer at a router is not a problem.

Network Routing: Overview

- From an efficient delivery point of view, it is desirable not to have any packet loss (or at least, minimize it) during transit.
- This is because the reliable delivery notion works on the principle of retransmission and acknowledgment and any drop would mean an increase in delay due to the need for retransmission.
- In addition, during transit, it is also possible that the content enclosed in a data packet is possibly corrupted due to, for example, an electrical signaling problem on a communication link.

Network Routing: Overview

- This then results in garbling of a packet. From an end-to end communication point of view, a garbled packet is the same as a lost packet.
- For efficient delivery of packets, there are several key factors to consider:
- (1) routers with a reasonable amount of buffer space,
- (2) links with adequate bandwidth,
- (3) actual transmission with minimal error (to minimize packets being garbled), and
- (4) the routers' efficiency in switching a packet to the appropriate outgoing link.

Network Routing: Overview

- A packet is to be routed based on the IP address of the destination host there are far too many possible hosts; it is impossible and impractical to store *all* host addresses at any router.
- For example, for a 32-bit address, theoretically a maximum of 2^{32} hosts are possible.
- A router needs to consider a coarser level of address information, i.e., the netid associated with a host, so that an outgoing link can be identified quickly just by looking up the netid.
- Netids do not have any geographical proximity association as with postal codes.

Network Routing: Overview

- Why is IP address numbering not geographic?
- To give a short answer, an advantage of a non-geographic address is that an organization that has been assigned an IP address block can keep its address block even if it moves to a different location or if it wants to use a different provider for connectivity to the Internet.
- A geographically based address system usually has limitations in regard to providing location-independent flexibility.

NETWORK ROUTING: OVERVIEW

- To minimize switching time at a router, efficient mechanisms are needed that can look up an address, identify the appropriate outgoing link (direction), and process the packet quickly so that the processing delay can be as minimal as possible.
- The updating of a table in the router, known as the *routing table,* that contains the identifier for the next router, known as the *next hop*, for a given destination netid is an important phase that works in tandem with the lookup process at a router.

NETWORK ROUTING: OVERVIEW

- The routing table is in fact updated ahead of time.
- In order to update such a table, the router would need to store all netids it has learned about so far;
- Second, if a link downstream is down or congested or a netid is not reachable for some reason, it needs to know so that an alternate path can be determined as soon as possible.
- This means that a mechanism is required for *communicating* congestion or a failure of a link or non reachability of a netid. This mechanism is known as the *routing protocol* mechanism.

NETWORK ROUTING: OVERVIEW

- The information learned through a routing protocol is used for generating the routing table ahead of time.
- If new information is learned about the status of links or nodes, or the reachability of a netid through a routing protocol, a *routing* algorithm is then invoked at a router to determine the best possible next hop for each destination netid in order to update the routing table.
- For efficient packet processing, another table, known as the *forwarding table*, is derived from the routing table that identifies the outgoing link interfaces.

IP Addressing

- An IP address assigned to a host is 32 bits long and should be unique.
- This addressing, known as IPv4 addressing, is written in the bit format, from left to right, where the left-most bit is considered the most significant bit.
- The hierarchy in IP addressing is reflected through two parts, a network part and a host part referred as the pair *(netid, hostid)*.
- We can think of the Internet as the *interconnection of networks* identified through netids where each netid has a collection of hosts.

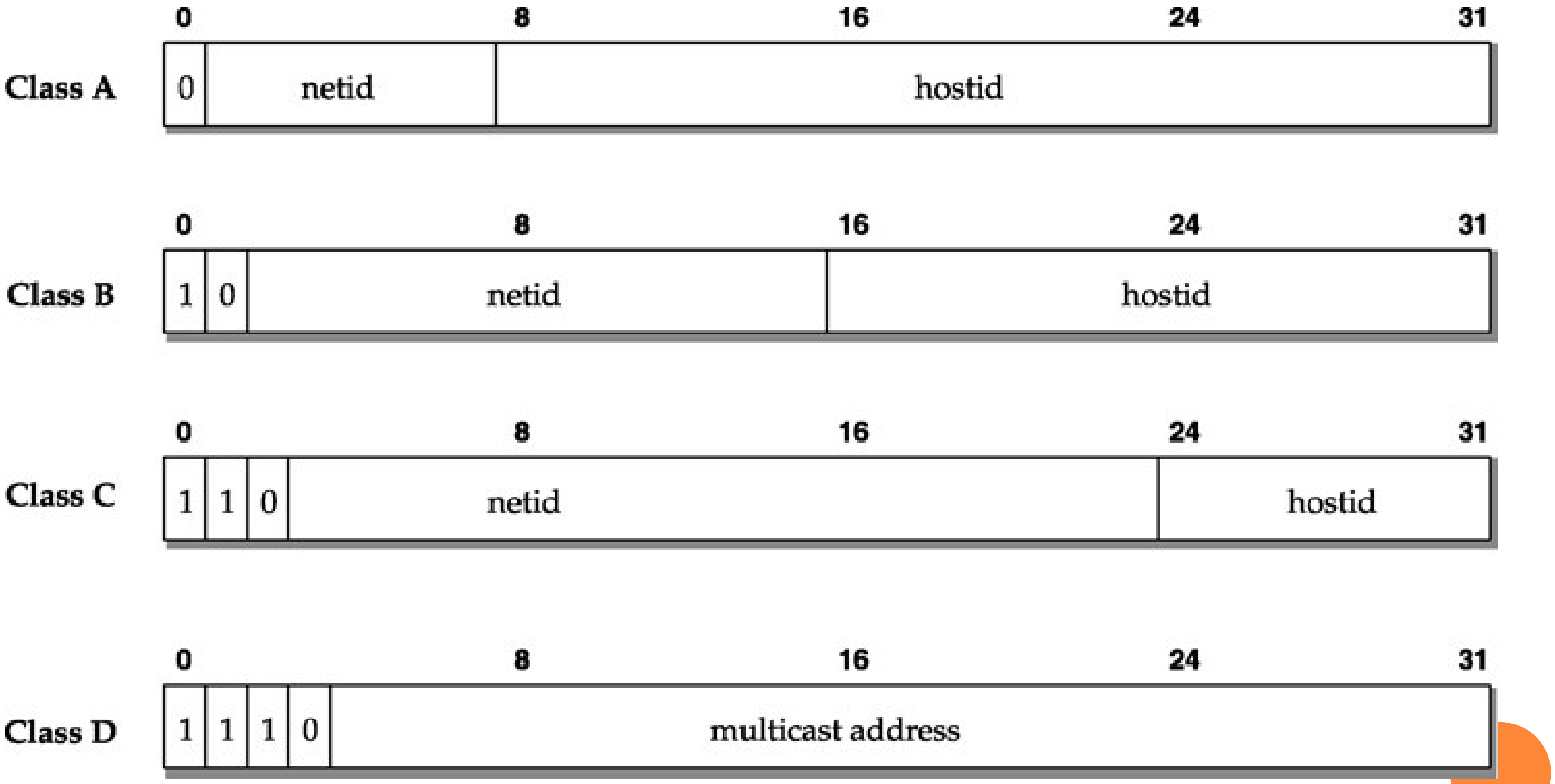
IP ADDRESSING

- The network part (netid) identifies the network to which the host is attached, and the host part (hostid) identifies a host on that network.
- The network part is also referred as the *IP prefix*.
- All hosts attached to the same network share the network part of their IP addresses but must have a unique host part.
- How to partition the total IP address space of 2^{32} addresses was needed, that is, how many network addresses will be allowed and how many hosts each of them will support.

IP Addressing

- Thus, the IP address space was originally divided into three different classes, Class A, Class B, and Class C, as shown in Figure 1 for networks and hosts.
- Each class was distinguished by the first few initial bits of a 32-bit address.
- For readability, IP addresses are expressed as four decimal numbers, with a dot between them.
- This format is called the *dotted decimal notation*.
- The notation divides the 32-bit IP address into 4 groups of 8 bits and specifies the value of each group independently as a decimal number separated by dots.

IP ADDRESSING



IP Addressing

- Because of 8-bit breakpoints, there can be at most 256 (= 2^8) decimal values in each part.
- Since 0 is an assignable value, no decimal values can be more than 255.
- Thus, an example of an IP address is 10.5.21.90 consisting of the four decimal values, separated by a dot or period.
- Each Class A address has the first bit set to 0 and is followed by 7 bits for the network part, resulting in a maximum of 128 (= 2^7) networks; this is then followed by a 24-bit host part.
- Thus, Class A supports a maximum of $2^{24} - 2$ hosts per network.

IP Addressing

- This calculation subtracts 2 because 0s and 1s in the host part of a Class A address may not be assigned to individual hosts; rather, all 0s that follows a netid such as 10.0.0.0 identify the network, while all 1s that follow a netid such as 10.255.255.255 are used as the broadcast address for this network.
- Each Class B network address has the first two bits set to "10," followed by a 14-bit network part, which is then followed by a 16-bit host part. A maximum of 2^{14} networks can be defined with up to $2^{16} - 2$ hosts per network.

IP ADDRESSING

- Finally, a Class C network address has the first three bits set as “110” and followed by a 21-bit network part, with the last 8 bits to identify the host part. Class C provides support for a maximum of 2^{21}*(= 2,097,152)* networks with up to 254 ($2^8 - 2$) hosts.

IP Addressing

- Three address classes discussed so far are used for unicasting in the Internet, that is, for a host-to-host communication.
- There is another class of IP addresses, known as Class D addressing, that is used for *multicasting* in the Internet; in this case, the first four bits of the 32-bit address are set to “1110” to indicate that it is a multicast address.
- A host can use a multicast address as the destination address for a packet generated to indicate that the packet is meant for any hosts on the Internet; in order for any hosts to avail this feature, they must use another mechanism to tune into this address.

IP Addressing

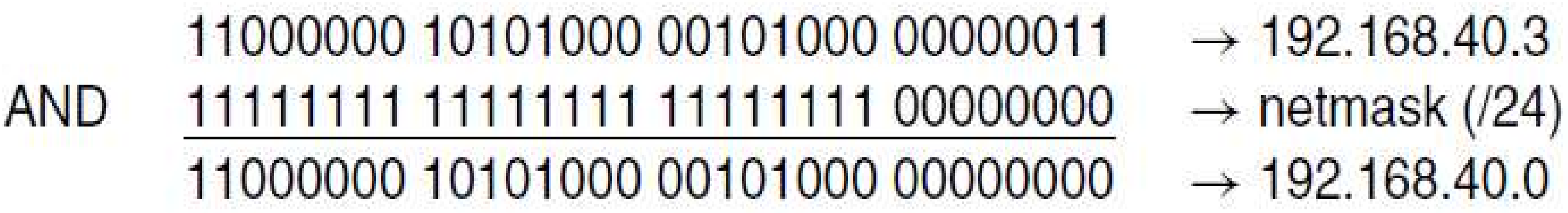
- The original rationale behind classes of different sizes was to provide the flexibility to support different sized networks, with each network containing a different number of hosts.

IP Addressing

- Subnetting/Netmask:
- Consider the IP address 192.168.40.3 that is part of Class C network 192.168.40.0.
- A subnet or sub-network is defined through a network mask boundary using the specified number of significant bits as 1s.
- Since Class C defines networks with a 24-bit boundary, we can then consider that the most significant 24 bits are 1s, and the lower 8 bits are 0s.
- This translates to the dotted decimal notation 255.255.255.0, which is also compactly written as

IP ADDRESSING

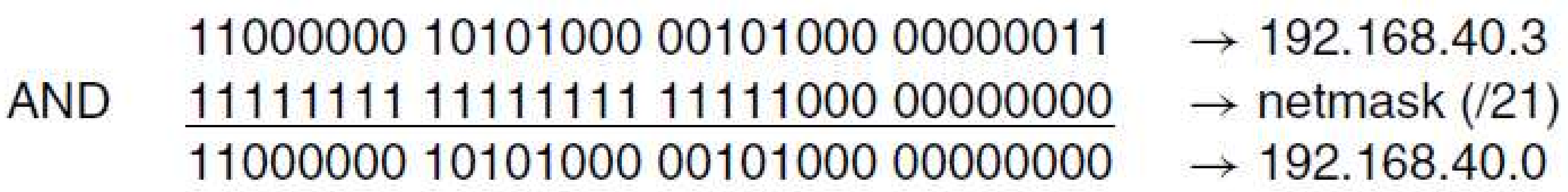
- “/24” to indicate how many most significant bits are 1s.
- We can then do a bit-wise logical “AND” operation between the host address and the netmask to obtain the Class C network address as shown below:



```
      11000000 10101000 00101000 00000011   → 192.168.40.3
AND   11111111 11111111 11111111 00000000   → netmask (/24)
      -----------------------------------
      11000000 10101000 00101000 00000000   → 192.168.40.0
```

IP ADDRESSING

- Now consider that we want to change the netmask *explicitly* to /21 to identify a network larger than a 24-bit subnet boundary.
- If we now do the bit-wise operation we note that the network address is again 192.168.40.0.
- However, in the latter case, the network boundary is 21 bits.



```
      11000000 10101000 00101000 00000011   → 192.168.40.3
AND   11111111 11111111 11111000 00000000   → netmask (/21)
      ___________________________________
      11000000 10101000 00101000 00000000   → 192.168.40.0
```

IP Addressing

- Thus, to be able to clearly distinguish between the first and the second one, it is necessary to explicitly mention the netmask.
- This is commonly written for the second example as 192.168.40.0/21, where the first part is the netid and the second part is the mask boundary indicator.
- In this notation, we could write the original Class C address as 192.168.40.0/24 and thus, there is no ambiguity with 192.168.40.0/21.

ON ARCHITECTURES

- Architectures cover many different aspects of networking environments. Network routing must account for each of the following architectural components. Some aspects of the architectures listed below are critical to routing issues:
- *Service Architecture*: A service model gives the basic framework for the type of services a network offers.
- *Protocol Stack Architecture*: A protocol stack architecture defines how service delivery may require different functions to be divided along well-defined boundaries so that responsibilities can be decoupled

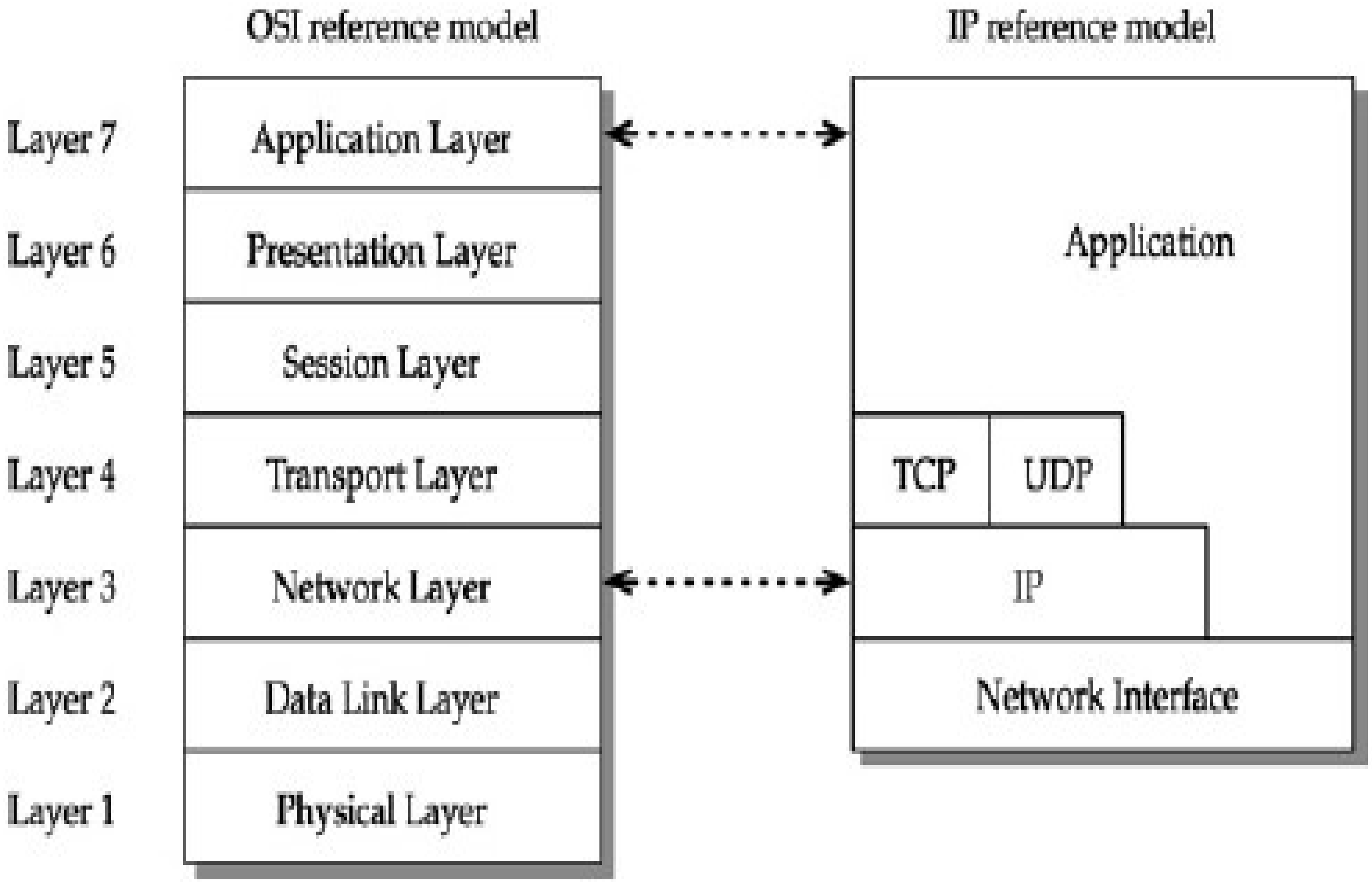
On Architectures

- *Router Architecture*: A router is a specialized computer that is equipped with hardware/ software for packet processing.
- *Network Topology Architecture*: For efficient operation as well as to provide acceptable service to its users, a network is required to be organized based on a network topology architecture that is scalable and allows growth.

Protocol Stack Architecture

- **OSI Reference Model**
- The OSI reference model was developed in the 1980s to present a general reference model for how a computer network architecture should be functionally divided.
- As part of OSI, many protocols have also been developed.
- The OSI reference model uses a layered hierarchy to separate functions, where the layering is strictly enforced.
- That is to say that an *N-layer uses services provided by layer N − 1;* it cannot receive services directly from layer *N − 2.*
- *In the OSI model, a seven-layer architecture* is defined

Protocol Stack Architecture



IP Protocol Stack Architecture

- The IP architectural model can be classified into the following layers: the network interface, the IP layer, the transport layer, and the application layer.
- Actual applications are considered on the top of the application layer, although the IP model does not strictly follow layering boundaries as in the OSI reference model. For example, it allows an application to be built without using a transport layer; *ping* is such an example.
- IP includes both the destination and the source address—this is accomplished through a header part in the IP packet that also contains additional information

IP Protocol Stack Architecture

- The IP addressing is defined at the IP layer, where the delivery mode is assumed to be unreliable.
- The transport layer that is above the IP layer provides transport services, which can be either reliable or unreliable.
- More important, the transport layer provides another form of addressing, commonly known as the *port number*.
- Port numbers are 16 bits long.
- Thus, the unreliable transport layer protocol, known as the User Datagram Protocol (UDP), can be thought of as allowing the extension of the address space by tagging a 16-bit port number to the 32-bit IP address.

IP Protocol Stack Architecture

- The reliable transport counterpart of UDP is known as the Transmission Control Protocol (TCP) which also uses a 16-bit port number, but provides reliable transport layer service by using a retransmission and acknowledgment mechanism.
- To be able to include the port number and other information, both TCP and UDP have well-defined headers.
- Because of two-way communication, similar to an IP packet including both the source and the destination address, TCP and UDP also include port numbers both for the source and the destination side.

IP Protocol Stack Architecture

- Since both TCP and UDP are above IP, a field in the IP header, known as the protocol type field, is used to be able to distinguish them.
- That is, through five pieces of information consisting of the source and the destination IP addresses, the source and the destination port numbers, and the transport protocol type, a connection in the Internet can be uniquely defined.
- This is also known as a microflow.

IP Protocol Stack Architecture

- There are two IP packet formats: IPv4 and IPv6.
- IPv4 uses the 32-bit IP address and is the most widely deployed addressing scheme. IPv6 uses a longer 128-bit address that was developed in the mid-1990s; initially, it was designed anticipating that IPv4 addresses would be running out soon. This did not happen as initially thought, partly because of the proliferation of private IP address usage (see Table 1.1) that has been made possible by mechanisms known as network address translation (NAT) devices, which can map and track multiple private IP addresses to a single IP address.

IP Protocol Stack Architecture

- Information structure at the transport layer is still at the byte level; there is no structured, semantic information considered at this level. However, structural information is needed for a particular application.
- For example, an email requires fields such as “From,” “To” before the body of a message is added; this then helps the receiving end know how to process the structured information.
- Examples of application layer protocols are Simple Mail Transfer Protocol (SMTP), and HyperText Transport Protocol (HTTP), which are used by email and web applications, respectively.

IP Protocol Stack Architecture

- There are other applications that do not require reliable data delivery. Voice over IP protocol, commonly referred to as VoIP, is one such application that can tolerate some packet loss and thus, retransmission of lost packets is not necessary.
- Such an application can then use UDP
- Since UDP does not provide any structural boundaries, and because many real-time communications, such as voice and video, require similar structural formats with the ability to distinguish different encoding mechanisms, Real-time Transport Protocol (RTP) has been defined above UDP.

Router Architecture

- A router provides several important functions in order to ensure proper packet forwarding, and to do so in an efficient manner. A router is a specialized computer that handles three primary functions:
- *Packet Forwarding*: On receiving an incoming packet, a router checks whether the packet is error free. After inspecting the header of a packet for destination address, it performs a table lookup function to determine how to find the appropriate outgoing link.

Router Architecture

- *Routing Protocol Message Processing*: A router also needs to handle routing protocol packets and determine if any changes are needed in the routing table by invoking a routing algorithm, when and if needed.
- *Specialized Services*: In addition, a router is required to handle specialized services that can aid in monitoring and managing a network.

- Questions?
- Comments?
- Contributions?