SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

ICT259 Computer Networking

Seminar 6: Transport and Application Layers

Ms Wong Yoke Moon

Transport Layer

Transport Layer

Objectives:

- Explain the role of the transport layer in end-to-end communication.
- Compare the characteristics of TCP and UDP.
- Explain port number and its usage.
- Summarizes the processes used by TCP for connection establishment and session termination.
- Explain how TCP segments are transmitted and acknowledged to guarantee delivery.
- Outline the processes used by UDP to establish communications with a server.
- Identify the applications best suited to use TCP or UDP as the transport layer protocol.

Transport Layer

Why we need a Transport Layer?

- **Layer 1** allows **bit streams** to be created and to travel.
- **Layer 2** packages those data packets **into frames** to be converted to bit streams and makes data-link delivery possible.
- **Layer 3** packages data from upper layers in **packets** and makes **routing** and network delivery possible.
- But they made no provision for assuring our data **reliably travels end-to-end** across the often vast network path.

Purpose of the Transport Layer

- **Transports and regulates the flow** of information from **source to destination**, **reliably and accurately.**

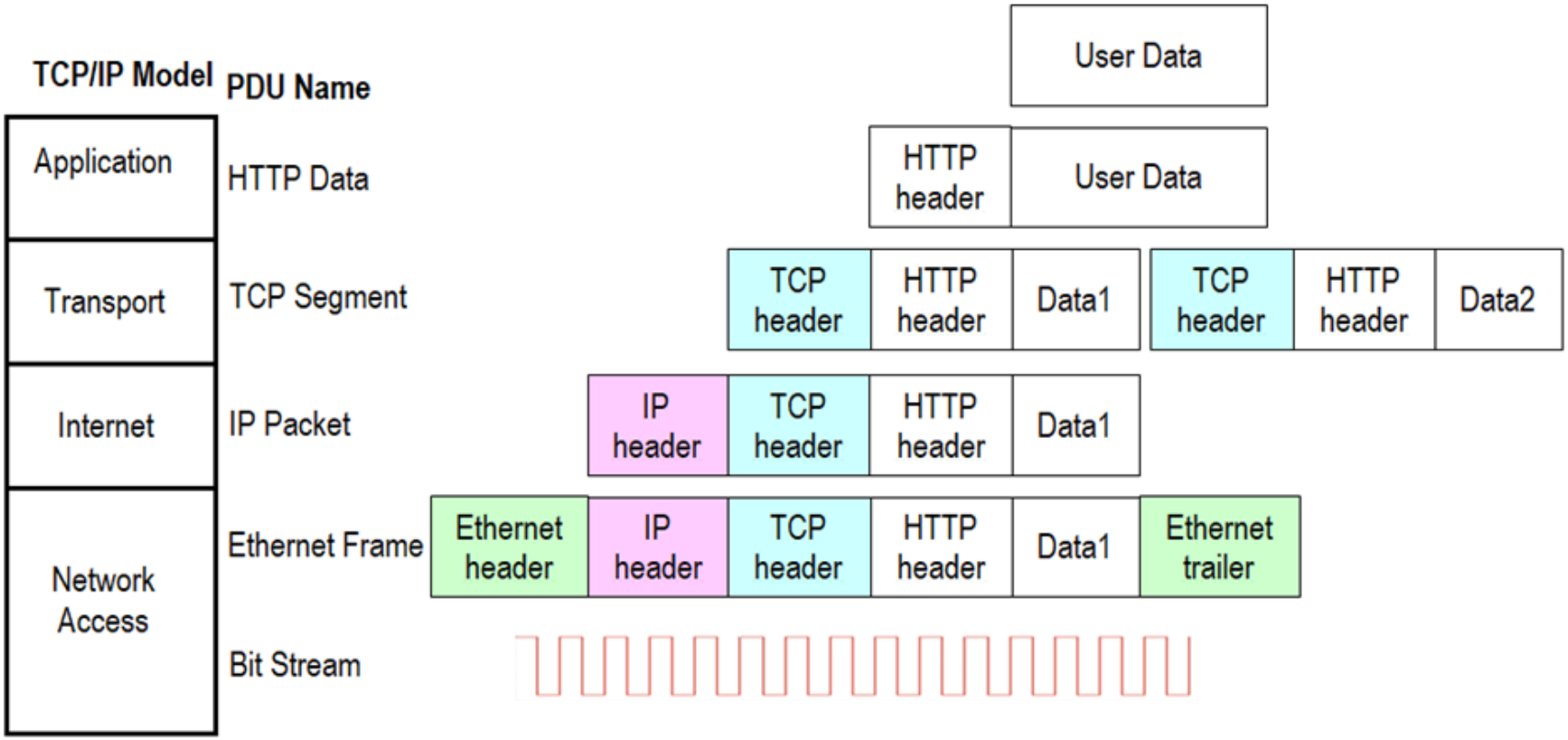
Transport Layer Responsibilities

1. **Tracking Individual Application Processes**
   - An application process refers to the flow of data between a source application and a destination application.
   - A device may have multiple applications running simultaneously across the network.
   - The transport layer protocol needs to maintain and track each individual application process.
2. **Segmenting Data and Reassembling Segments**
   - Some protocols set a limit on the size of the packet that can be transmitted across the network.
   - If the application data is too long, the transport layer protocol needs to segment the application data into segments of appropriate size.
   - At the receiving end, the transport layer protocol needs to reassemble the segments into application data.

Transport Layer Responsibilities

2. Segmenting Data and Reassembling Segments

- Figure below shows the encapsulation process of the previously mentioned **web server example**. Note: The segmentation at the Transport layer.



Transport Layer Responsibilities

3. Identifying the Applications

- Since there can be many applications running on a target device, the transport layer must be able to identify the target application.
- To do this, the transport layer protocol assigns each application an unique ***port number***.
- If a process needs to access the network, the source device will dynamically assign a source port number to the application.
- The port number is a16-bit number and ranging from 0 to 65 535.

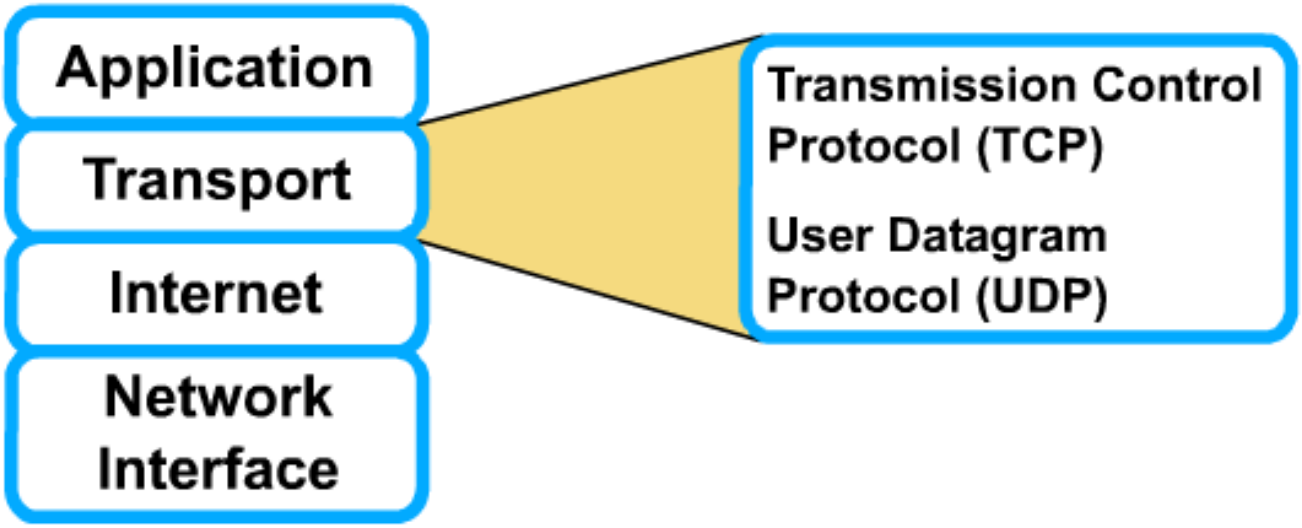
4. Application Process Multiplexing

- Data from each application process running on a device is divided into smaller segments.
- These segments from different processes are to be interleaved or multiplexed on the same network.
- Each segment is differentiated by their port numbers, which is added to the header of the transport layer.

Transport Layer Responsibilities

5. Transport layer Reliability

- Transport layer reliability requirements vary from application to application.
- The transport layer of the TCP/IP model has 2 protocols, namely **TCP** and **UDP**.
- **TCP** is a **reliable** and full-featured transport layer protocol. As such it has more fields in the TCP header, which increases the packet size and delivery time.
- **UDP** is an **unreliable** and simple transport layer protocol. It has less fields in the TCP header and is faster than TCP.



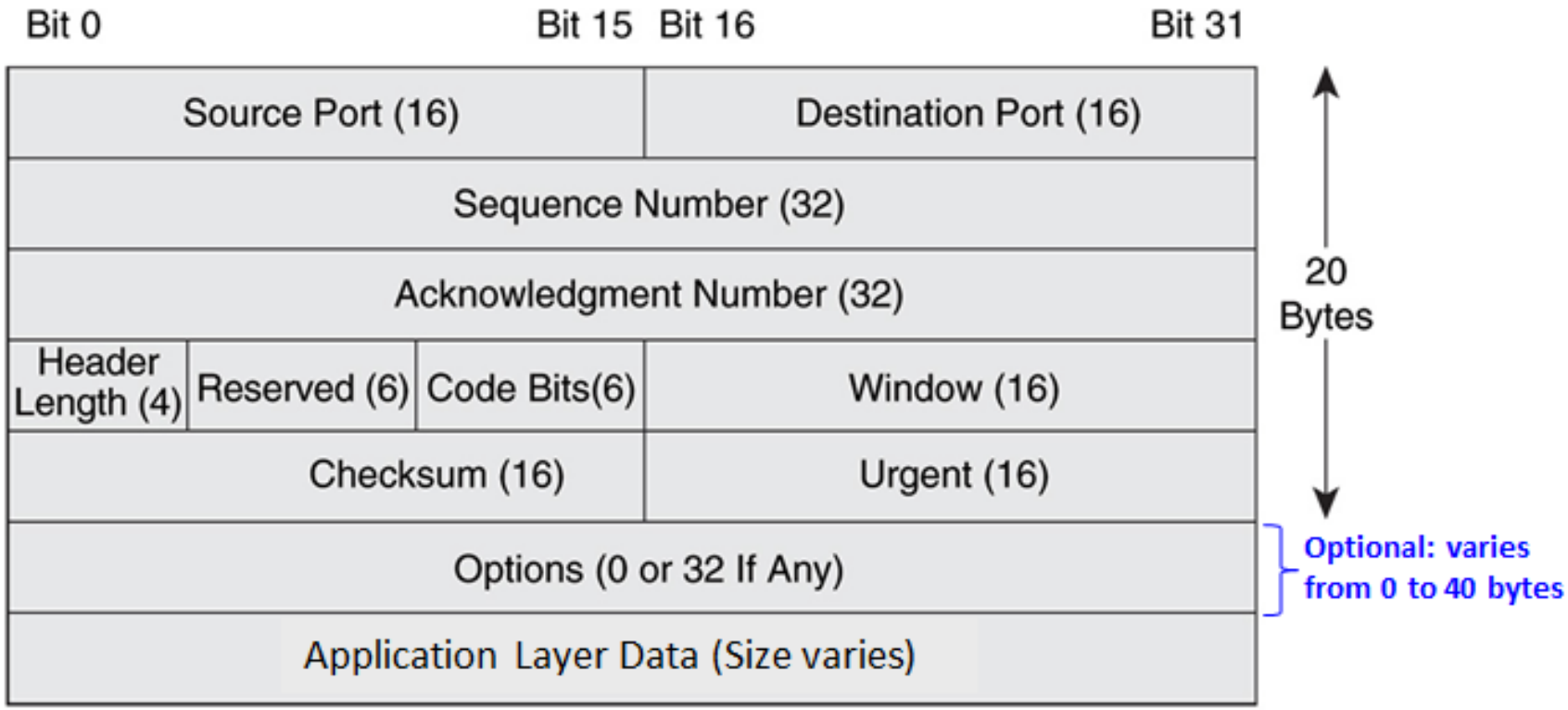
Transmission Control Protocol (TCP)

Characteristics of TCP

- **Connection-oriented** - builds a virtual circuit between source and destination end devices.
  - In virtual circuit , a virtual connection between source and destination end devices is established before transmission. Data is delivered in order.
- **Reliable** delivery
- TCP packet is called **segment**
- **Divides** outgoing data into segments
- **Reassembles** segments into data at the destination device
- **Acknowledges** received data
- **Retransmits** lost data (Error recovery)
- Delivers data in **sequential order**

TCP Header Format

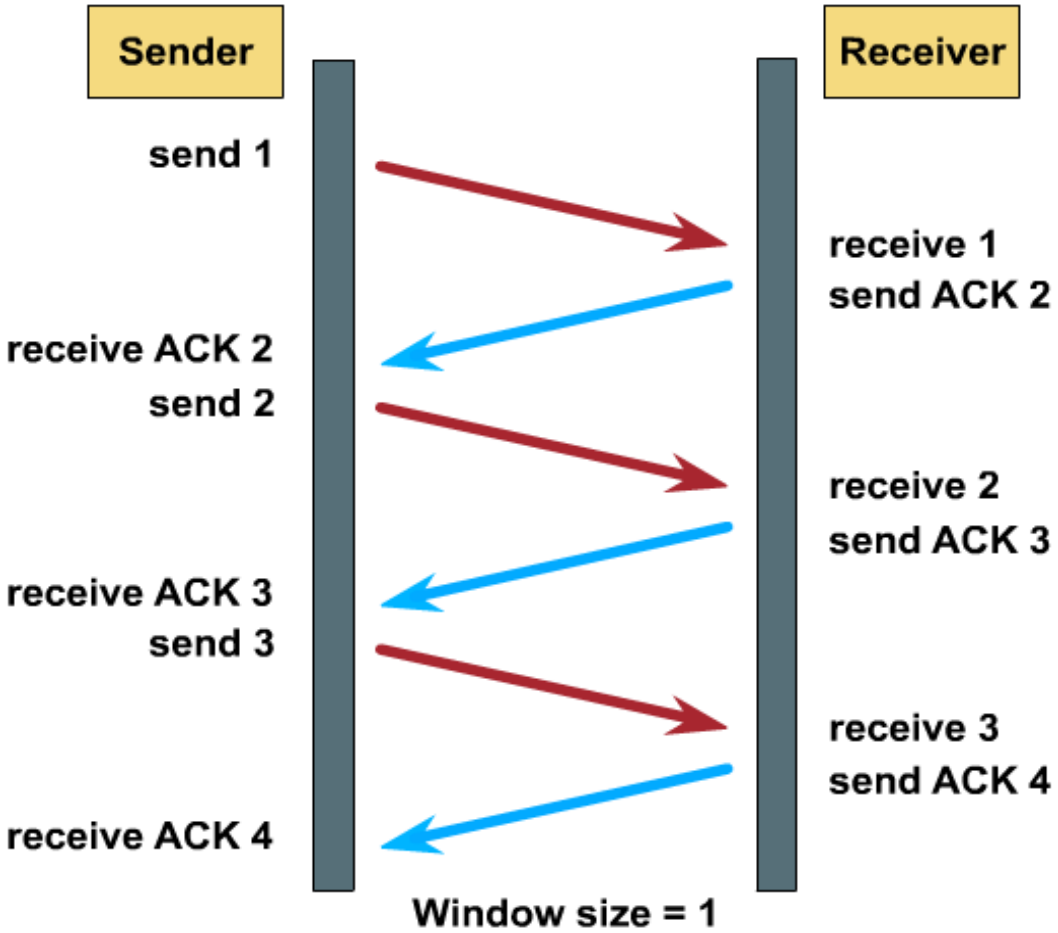
- The TCP header has a **minimum length of 20 bytes** to a **maximum** length of **60 bytes**.



TCP Sliding Window Flow Control

Simple Acknowledgement

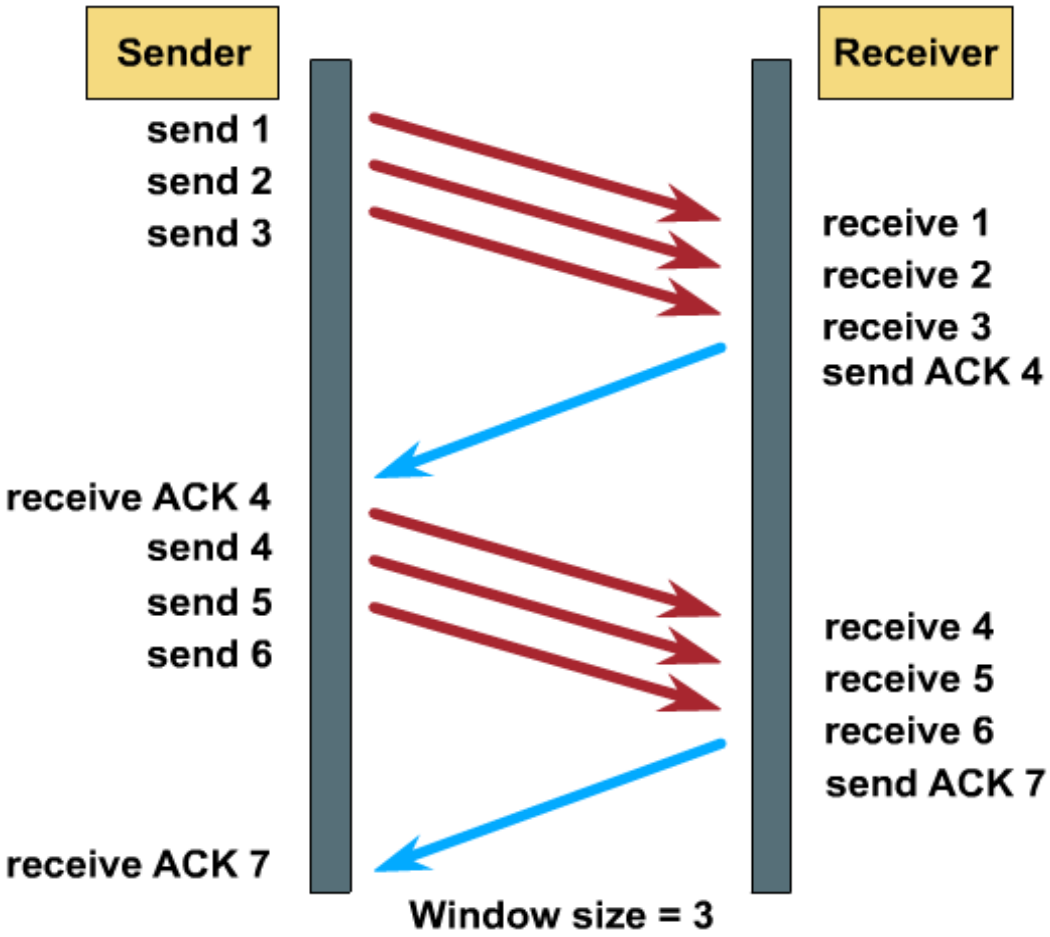
- **Window size** indicates the **maximum number of bytes** that can be **sent before receiving an ACK**.
- The **number after ACK** indicates the **next sequence number expected** to receive.



TCP Sliding Window Flow Control

Sliding Acknowledgement

- **Window size** indicates the **maximum number of bytes** that can be **sent before receiving an ACK**.
- The **number after ACK** indicates the **next sequence number expected** to receive.



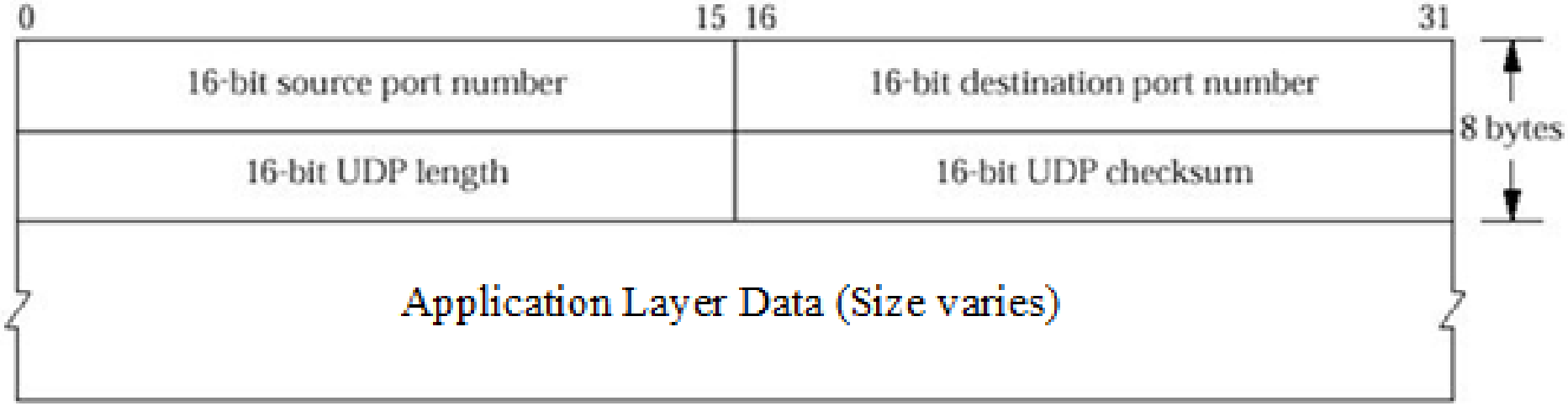
User Datagram Protocol (UDP)

Characteristics of UDP

- **Connectionless** - does not establish a connection before transmitting data.
  - Packets do not follow a fixed path. Thus packets received can be out of sequence.
  - Source device does not check whether destination device is available and ready to receive the data. It just sends.
- UDP packet is called **User Datagram**
- **Unreliable** – no software checking for data delivery
  - **Does not require acknowledgements**
  - **Does not retransmit** lost data (No error recovery)
  - **No flow control**
  - **Does not reassemble** received user datagram (done at the application layer)
- **Fast**
- **Low overhead**
- Delivers data **as it arrives**

UDP Header Format

- UDP header has a **length of 8 bytes**, which is relatively short compared with TCP.



Port Number Groups

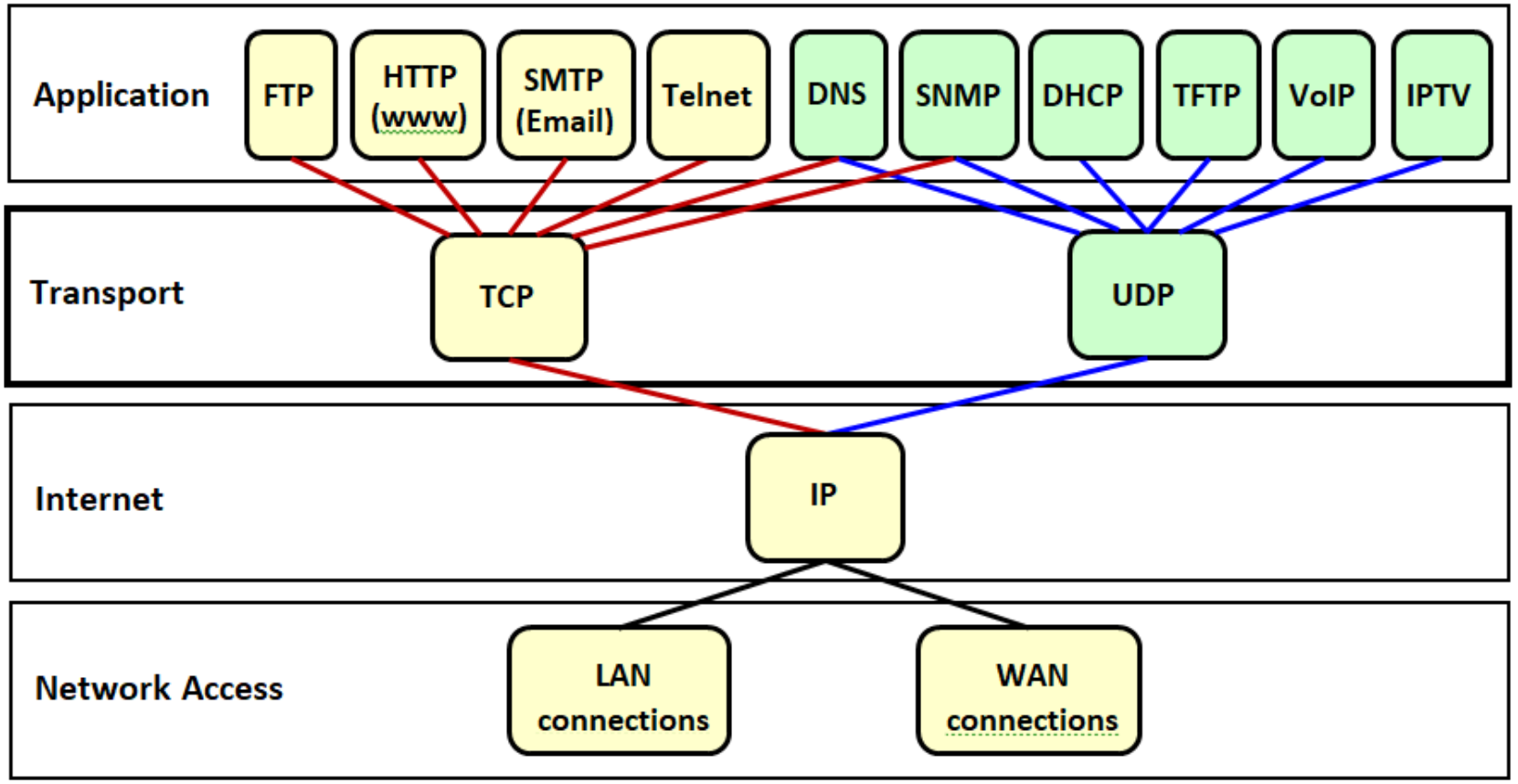
- **Well-Known Ports (Numbers 0 to 1023)** – These are reserved for applications such as web browsers (HTTP, port 80), email clients (SMTP, port 25), file transfer (FTP, port 21), domain name services (DNS, port 53) and etc.
- **Registered Ports (Numbers 1024 to 49 151)** – Organisations can request port numbers from Internet Assigned Numbers Authority (IANA) to be used with specific or less common applications.
- **Dynamic or Private Ports (Numbers 49 152 to 65 535)** – These are used by any device application program to communicate with any other application program without registration requirement. These ports are usually assigned dynamically by the device's OS when a communication is initiated.

Well-Known Port Numbers

Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	-
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67, 68	UDP	Dynamic Host Configuration Protocol	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypetext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP, TCP	Simple Network Management Protocol	SNMP
443	TCP	Hypetext Transfer Protocol Secure	HTTPS

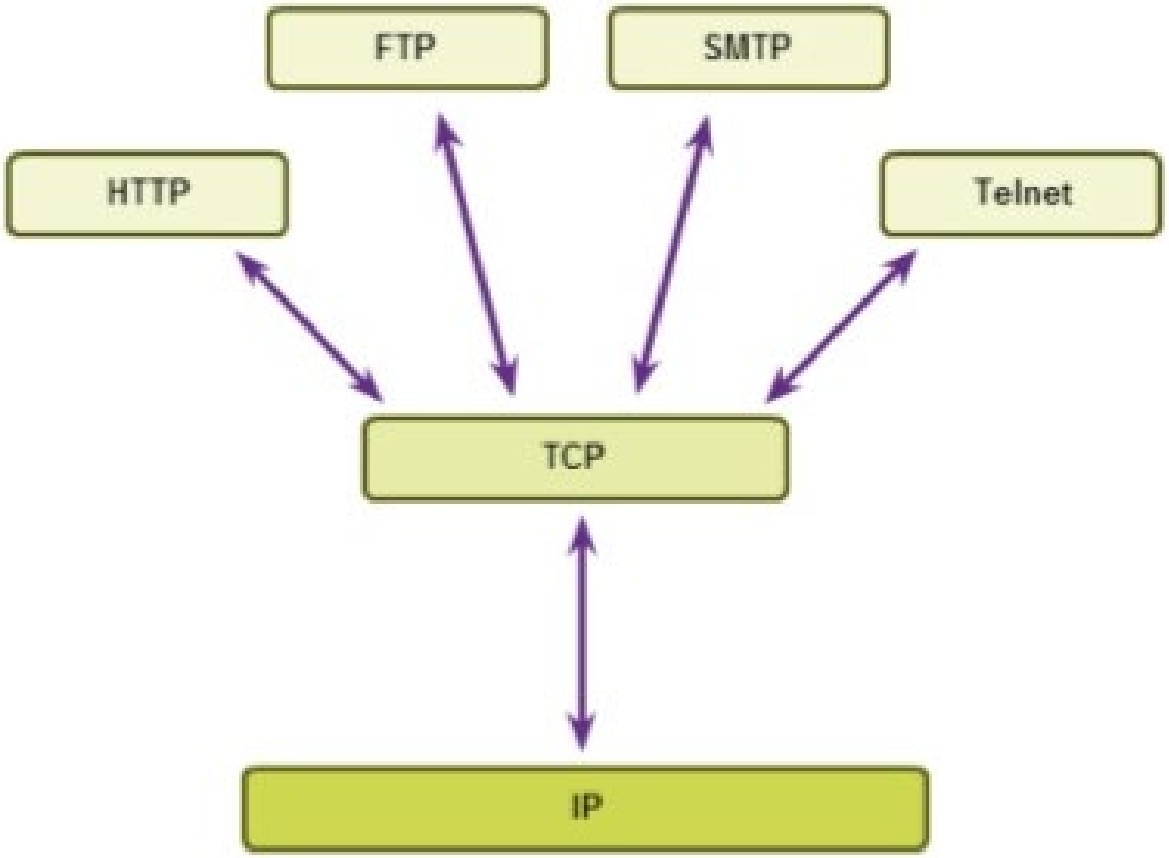
Protocols of the TCP/IP Model

Each transport layer protocol has unique characteristics. **Application developers** must **decide** on the suitability of each transport layer protocol **based on the requirements of the applications**.



Applications that Use TCP

- Applications such as World Wide Web, file transfer, email and remote administration that require data to be received in the same original condition when it was sent.



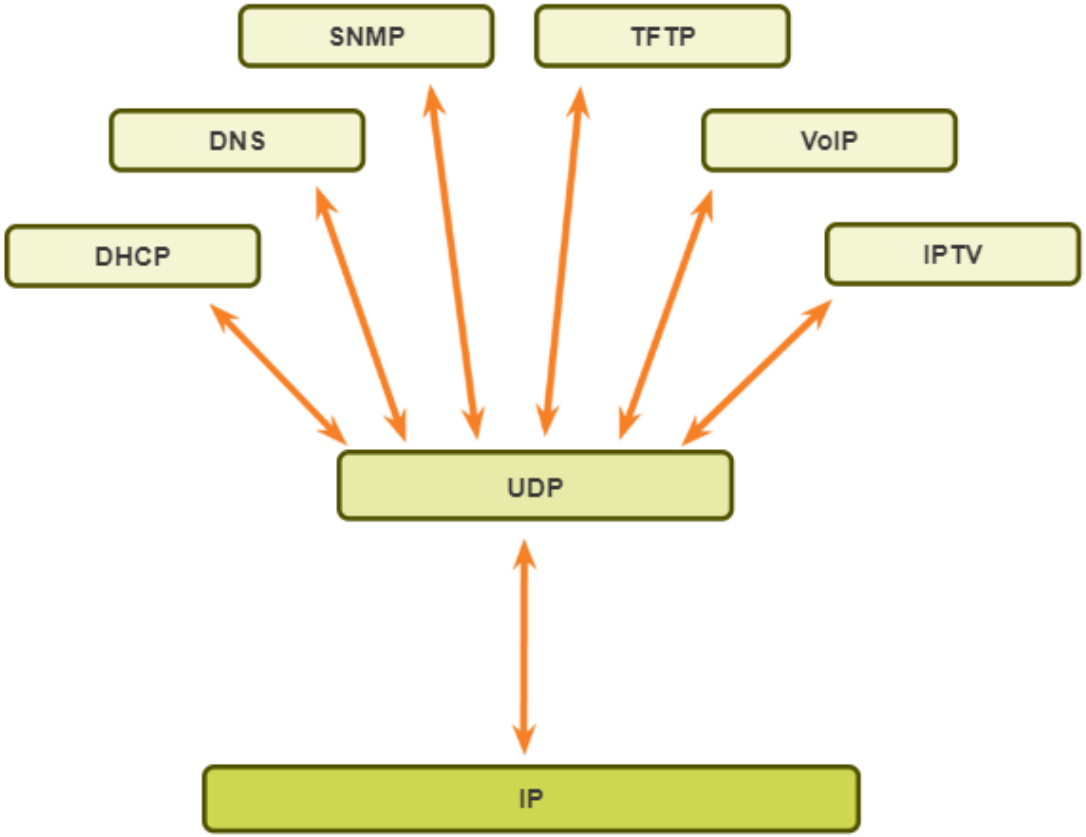
Applications that Use UDP

Applications that are suitable for UDP

- **Live video and multimedia applications** – Since speed of delivery has higher priority, some loss of data can be tolerated. Suitable for applications such as streaming live audio, live video, and Voice over IP (VoIP).
- **Simple request and reply applications** - Applications with simple communications where a device sends a request , but might not receive a reply. E.g. includes DNS, DHCP and electronic financial transactions such as ATM transactions, e-transactions at Point of Sale (POS) counter and etc.
- **Applications that take care of its own reliability** – Applications that do not require reliability or can be handled by the application. E.g. includes SNMP and TFTP. TFTP has its own mechanisms to handle reliability.

Applications that Use UDP

- By default, DNS and SNMP use UDP, but they can also use TCP.
- UDP is used to exchange small information. If information is larger than 512 bytes, TCP must be used.
- If the DNS request or DNS reply is more than 512 bytes, TCP will be used.
- Similarly, under certain circumstances, SNMP will use TCP.



Transport Layer Summary

- The role of the transport layer protocols is to ensure end-to-end delivery.
- TCP and UDP are two transport layer protocols.
- TCP provides high reliability transmissions, whereas UDP transmissions are non-guaranteed.
- TCP uses various mechanisms to achieve reliability.
- The reliability process imposes overhead on the network.
- UDP is best suited for applications that do not require the reliability or want to avoid the overhead.
- Both TCP and UDP have specific applications mapped to them that suited their unique characteristics.

Application Layer

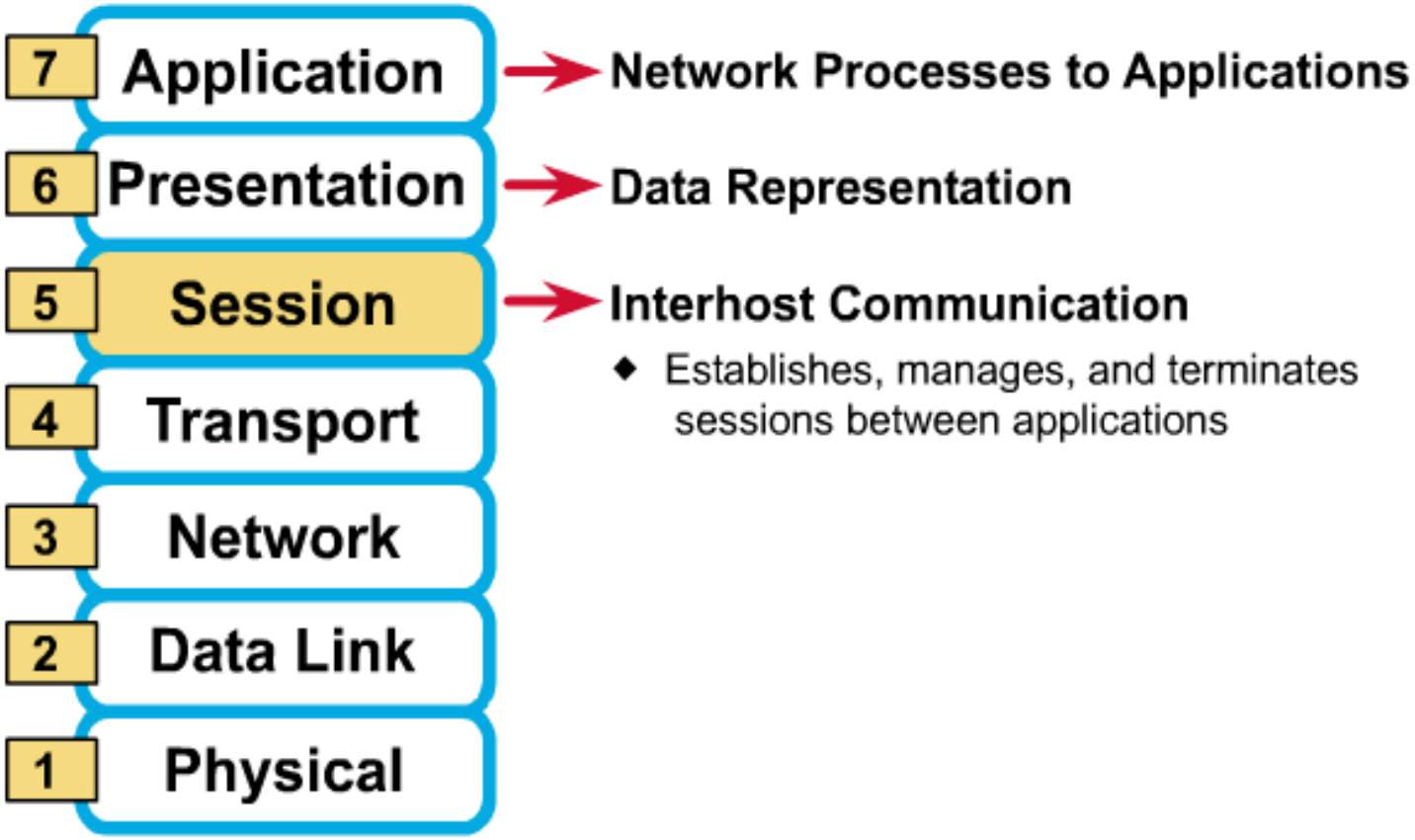
Application Layer

Objectives:

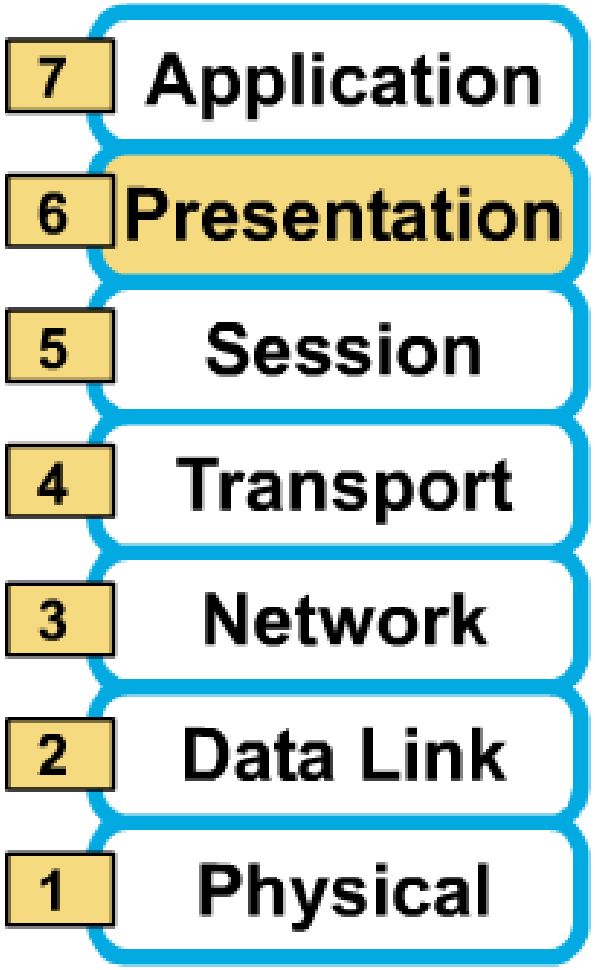
- Explain the functions of the application, presentation and session layers in providing services to end-user applications.
- Describe the interactions between application layer protocols and end-user applications.
- Summarizes the processes application layer protocols use to provide IP Addressing Services.

Functions of Session Layer

- **Creates, manages and terminates dialogs** between source and destination applications. It also restarts dialogs that have been disrupted or idle for a long period of time.



Functions of Presentation Layer



Network Processes to Applications

Data Representation

- Insure data is readable by receiving system
- Format of data
- Data structures
- Negotiates data transfer syntax for application layer

Functions of Presentation Layer

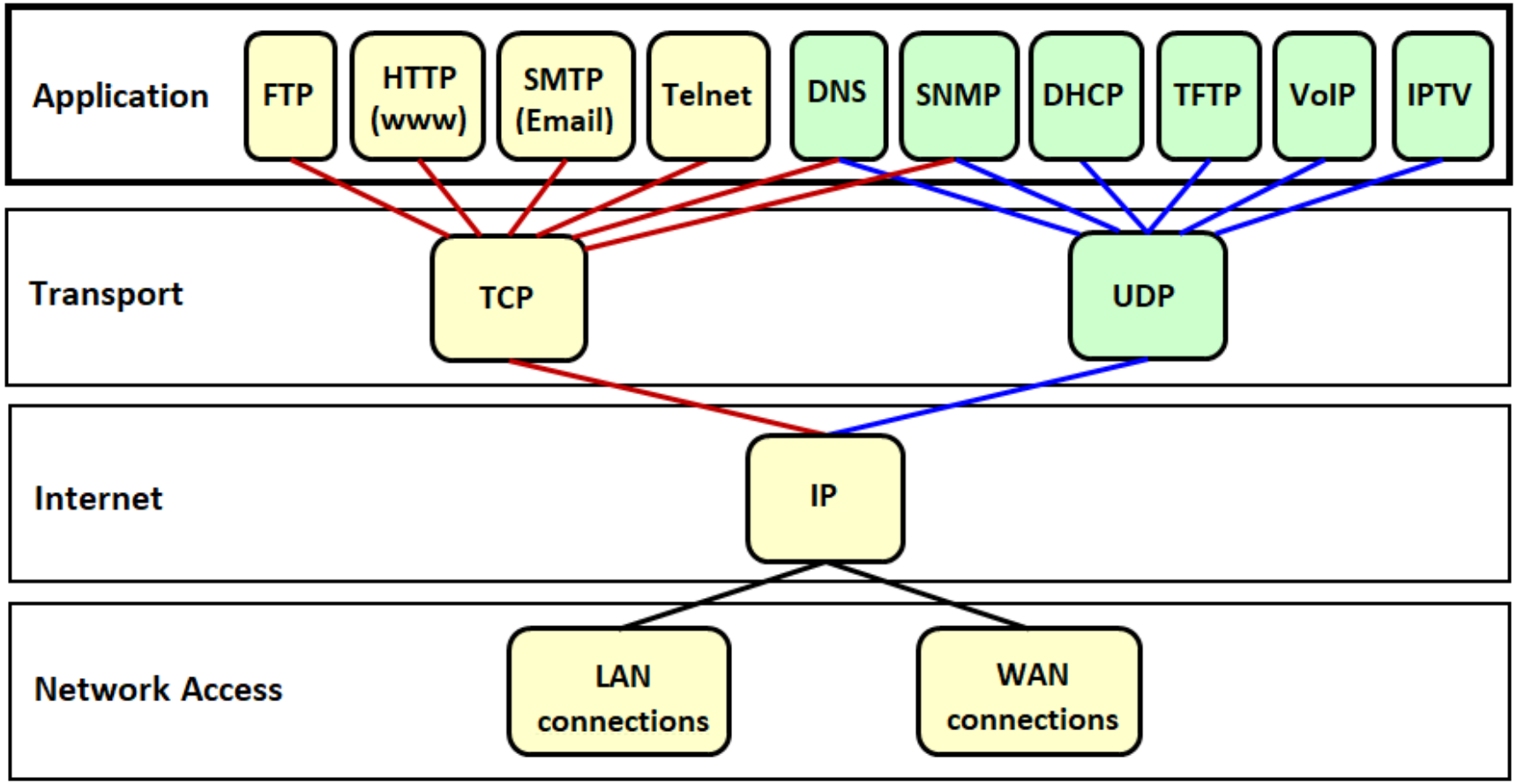
- **Data representation** - Format or represent data at the source device into a form that is readable or acceptable by the destination device. This is needed because different computer architectures use different data representations.
- **Data compression** – Compress data before transmission to improves data throughput. It must also ensure that compressed data can be decompressed by the destination device.
- **Data encryption** – Encrypt data before transmission and decrypt data upon receipt.

Presentation Layer Standards

- Presentation layer sets **standards for file formats**.
- Some well-known standards are:
  - For **text**: ASCII
  - For **graphic image** used on networks:
    - Graphics Interchange Format (GIF)
    - Joint Photographic Experts Group (JPEG)
    - Portable Network Graphics (PNG)
  - For **video**:
    - QuickTime
    - Motion Picture Experts Group (MPEG)

Application Layer Protocols and Services

- Given below are some well-known application layer protocols and services. We will examine DHCP in more details.



Dynamic Host Configuration Protocol (DHCP)

Function of DHCP

- Dynamically assign an IP address to a host at start-up from a determined range of IP addresses for a given network. The address can be released back to the pool for re-assignment when it is no longer needed.

IP Addressing Services

- For a device or **host to function on an IP network**, it requires the following to be configured:
  - IP address
  - Subnet mask
  - Default gateway
  - DNS server (E.g. 152.226.64.11)
  - Domain name (E.g. suss.edu.sg)
- **Two methods** for this to be done
  - Static assignment
  - Dynamic assignment

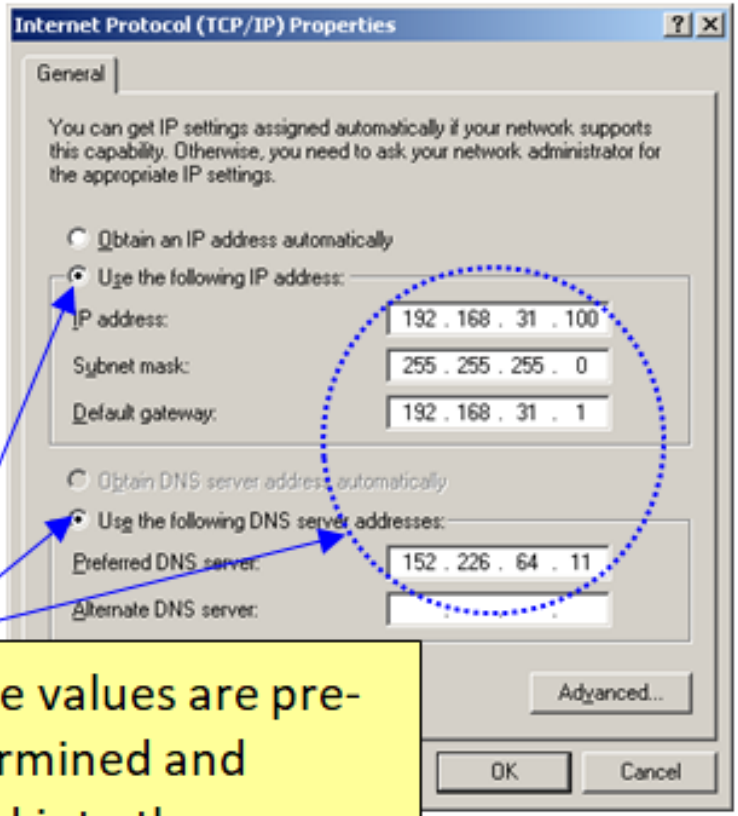
Dynamic Host Configuration Protocol (DHCP)

- **Before IP assignment**, the administrator must first:
  - Determine, by calculation, the range of valid host IP addresses. This includes the subnet mask.
  - Determine the default gateway, domain name and DNS server.

- **Static assignment**
  - Administrator manually keys in the required parameters on to the host's IP configuration window.
- **Dynamic assignment**
  - Administrator selects "automatic" assignment on the host's IP configuration window.

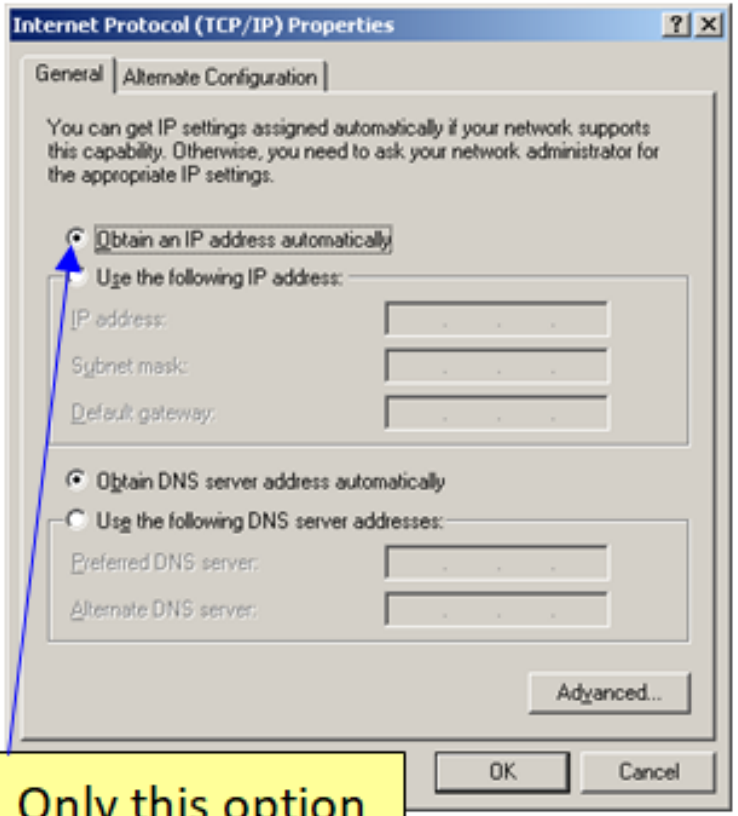
Dynamic Host Configuration Protocol (DHCP)

Static IP Assignment



These values are pre-determined and keyed into the configuration window

Dynamic IP Assignment



Only this option is selected

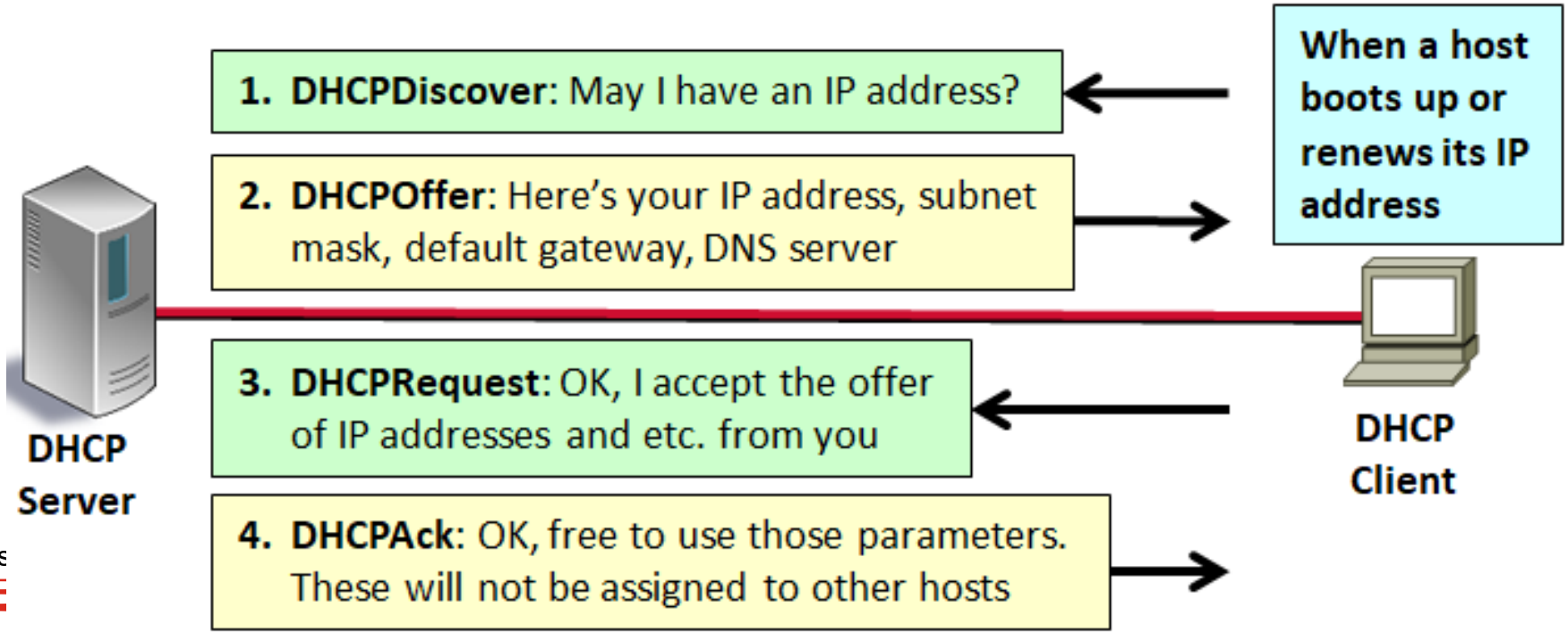
Dynamic Host Configuration Protocol (DHCP)

Comparison between Static and Dynamic Assignment

- **Static assignment**
  - Administrator has to manually key in the parameters on EVERY host - very tedious if there are many hosts.
  - Administrator has to keep a record of the IP address assignment (i.e. which station is given which address) – very tedious.
  - Not suitable for mobile work environment – (e.g. a notebook user moving around in various locations of the company or campus).
  - Good for systems requiring a fixed IP address (e.g. servers and routers).
- **Dynamic assignment**
  - Administrator needs to just set the hosts on “automatic” assignment (note: this is the default setting of the station).
  - Administrator needs to set up a DHCP server in the network.
  - Very good solution for dynamic and large environment.
  - Not suitable for important resources like servers and routers.

DHCP Operations (4 Phases)

- DHCP is a **client-server protocol** where the DHCP server leases out IP addresses and other information to any client that requests them.
- There are **4 DHCP messages** used, shown with their mode of transmission.
- DHCP**Discover**: broadcast
- DHCP**Offer**: unicast
- DHCP**Request**: broadcast
- DHCP**Ack**: unicast



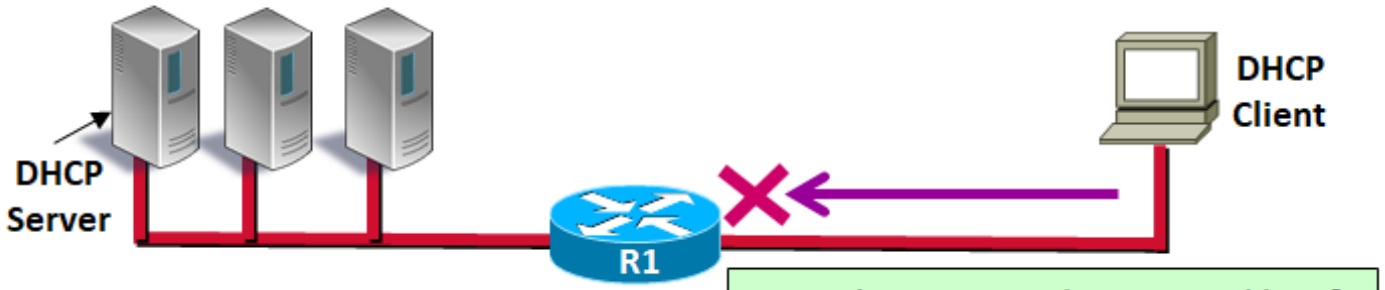
DHCP Operations (4 Phases)

The DHCP client configuration process uses the following steps:

- **Client sends** a request to a server requesting an IP configuration by sending a **broadcast** called a **DHCPDISCOVER**.
- The server receives the broadcast. If it can offer an IP address, the DHCP **server replies** the client with IP configuration information in the form of a **unicast DHCPOFFER** which includes IP address, DNS server address, and lease time.
- If the offer is agreeable, the **client will send** another **broadcast**, a **DHCPREQUEST**, specifically requesting those particular IP parameters. If more than one server makes an offer, the broadcasted DHCPREQUEST allows the other servers to know which offer was accepted. The offer accepted is usually the first offer received.
- The **server** that receives the DHCPREQUEST makes the configuration official by sending a **unicast acknowledgment**, the **DHCPACK**. Receipt of the DHCPACK message enables the client to begin using the assigned address immediately.

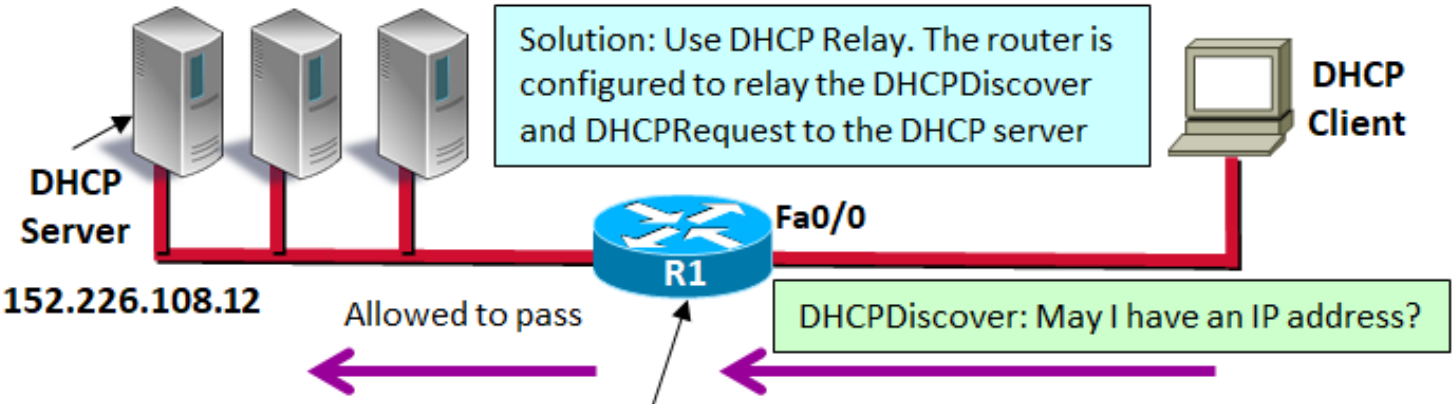
DHCP Relay

Problem: What if the DHCP server is on another subnet?



Recap: **DHCPDiscover** is a broadcast which a router (by default) filters. The router will drop such a packet and it will not reach the DHCP server

Solution: DHCP Relay

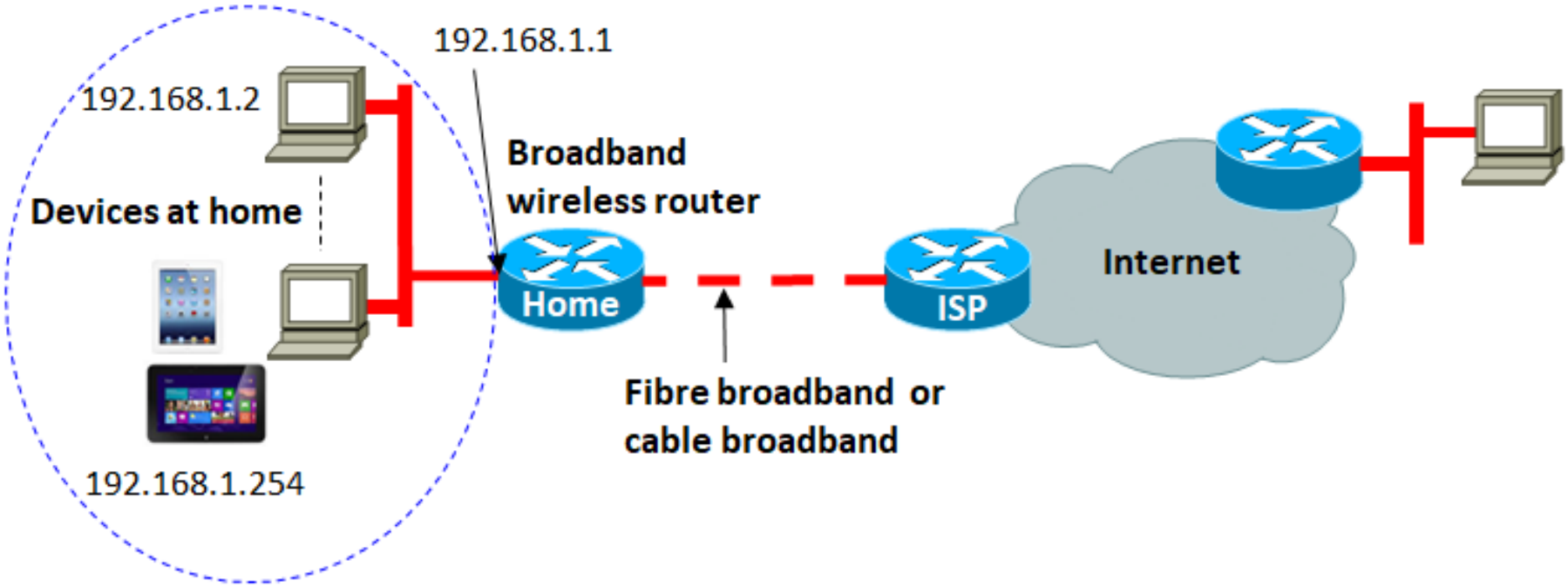



```
R1(config)# int fa0/0
R1(config-if)# ip helper-address 152.226.108.12
```

DHCP Server in Home Network

- Shown below is a typical setup in home network.
- Home devices are on automatic IP address assignment.
- Broadband wireless router functions as **DHCP server**, NAT/PAT (Network Address Translation/Port Address Translation)* server and Web server.

* NAT/PAT is beyond the scope of this course.



Application Layer Summary

- The application layer protocols enable users to access Internet services.
- DHCP provides automatic and central management for the distribution of IP addresses within a network.

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Thank You.