Final exam revision for Fundamental of Network – course IETC1310
By Ahmed Farouk – 77275783

NO	Topic	
1	Protocol, Topology, Switch & Hub, Ports	
	protocols define format, order of messages sent and received among network entities, and actions taken on msg transmission, receipt. **Topology** bus: popular through mid 90s all nodes in same collision domain – can collide star: prevails today - active switch in center – no collide **routers**: network-layer devices – using IP **Switch** : layer two device – communicate using mac (both router and switch have forward table) **Hub** : is a physical-layer device that acts on individual bits rather than frames	1-8 5-38 532
2	Network Interface Card (NIC)and Bandwidth	
	bandwidth is the maximum rate of data transfer across a given path. Applications with throughput requirements such as video and audio are **bandwidth-sensitive applications**	
	TCP/IP Layers/Model verses OSI Model	
	1. **Physical layer** - provides the electrical and mechanical connection to the network. Flow of bits. 2. **Data Link layer** - handles error recovery, flow control , it is the media access control layer" and is where the MAC addressing is defined 3. **Network layer** - accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information (addressing and routing) 4. **Transport layer** - is concerned with message integrity between the source and destination (delivery) 5. **Session layer** - provides the control functions necessary to establish, manage, and terminate the connections as required to satisfy the user request. 6. **Presentation layer** - accepts and structures the messages for the application. It translates the message from one code to another if necessary. This layer is responsible for data compression and encryption. 7. **Application layer** - application programs such as word processing, spreadsheets, and email log the message in, interpret the request, and determine what information is needed to support the request.	
	Application, Transport, Internet, Network, and Interface Layers	
	Same as above	

IP protocol, TCP, ICMP, ARP, Ethernet, Token Ring, IGMP and HTTP Protocols

1. **The Internet Protocol (IP)** is network layer protocol , it is the principal communications protocol in the Internet.
2. **The Transmission Control Protocol (TCP)** is transport layer protocol
3. **ICMP**, **the Internet Control Message Protocol** is used to control the flow of data in the network , reporting errors, and for performing diagnostics.
4. **ARP**, **the Address Resolution Protocol**, is used to resolve an IP address to a hardware address (MAC) for final delivery of data packets to the destination
5. **IGMP** is **the Internet Group Message Protocol**. IGMP is used when one host needs to send data to many destination hosts. This is called multicasting.
6. **The Hypertext Transfer Protocol (HTTP)** is an application layer protocol for distributed, collaborative, hypermedia information systems (web pages)

Port number for FTP, HTTP, DNS, and SMTP

FTP	20, 21
HTTP	80
DNS	53
SMTP	25

Connection-oriented vs. connectionless-oriented

connection-oriented transport(TCP) Three Handshake reliable data transfer flow control connection management bigger header size	connectionless: UPD no connection establishment simple: no connection state small header size no congestion control: UDP can blast away as fast as desired unreliable data transfer

Properties of UDP Protocol

TCP services: reliable transport between sending and receiving process flow control: sender won't overwhelm receiver congestion control: throttle sender when network overloaded does not provide: timing, minimum throughput guarantee, security connection-oriented: setup required between client and server processes.	UDP services: unreliable data transfer between sending and receiving process does not provide: reliability, flow control, congestion control, throughput guarantee, security, connection setup,

TCP data Packets

1. **Version** − Version no. of Internet Protocol used (e.g. IPv4).
2. **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
3. **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
4. **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
5. **Source Address** – **Destination Address**
6. **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

digital subscriber line (DSL)

DSL stands for Digital Subscriber Line. Users get a high speed bandwidth connection from a phone .you can use the Internet while making phone calls.

Ethernet, transmission rate R

The transmission rates of Ethernet LANs can be 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps.

Protocol layers, service models

Link layer services:
flow control: pacing between adjacent sending and receiving nodes
error detection: errors caused by signal attenuation, noise.
receiver detects presence of errors: signals sender for retransmission or drops frame
error correction: receiver identifies and corrects bit error(s)
half-duplex and full-duplex with half duplex, nodes at both ends of link can transmit, but not at same time

End systems, access networks, links

all nontraditional Internet “things” such as laptops, smartphones, tablets, TVs, gaming consoles, thermostats, home security systems, home appliances, watches, eye glasses,
cars, traffic control systems and more are being connected to the Internet.

Physical media – Guided Vs Wireless

Physical media fall into two categories: guided media and unguided media. With guided
media, the waves are guided along a solid medium, such as a fiber-optic cable, a twisted-pair copper wire, or a coaxial cable. With unguided media, the waves propagate in the atmosphere and in outer space, such as in a wireless LAN or a digital satellite channel.

Packet vs circuit switching

	Circuit switching is defined as the method of switching which is used for establishing a dedicated communication path between the sender and the receiver. FDM versus TDM	Packet switching is defined as the connectionless network where the messages are divided and grouped together and, this is known as a packet. Each packet is routed from the source to the destination as individual packets. great for bursty data , resource sharing simpler, no call setup excessive congestion possible: packet delay and loss protocols needed for reliable data transfer, congestion control	

ISP, IXP

An Internet service provider (ISP) is an organization that provides a myriad of services for accessing, using, or participating in the Internet.

An Internet exchange point (IX or IXP) is the physical infrastructure through which Internet service providers (ISPs) and content delivery networks (CDNs) exchange Internet traffic among their networks (autonomous systems) and peer together

Four sources of packet delay

1. **nodal processing** : check bit errors and determine output link .
2. **queueing delay**: time waiting at output link for transmission depends on congestion level of router.
3. **transmission delay**: L: packet length (bits) R: link bandwidth (bps)
4. **propagation delay**: d: length of physical link s: propagation speed in medium

Caravan analogy

assume that whenever the first car of the caravan arrives at a tollbooth, it must wait at the entrance to the tollbooth until all of the other cars in its caravan have arrived, and lined up behind it before being serviced at the toll booth. (That is, the entire caravan must be stored at the tollbooth before the first car in the caravan can pay its toll and begin driving towards the next tollbooth)

Packet loss, Throughput

Throughput refers to how much data can be transferred from one location to another in a given amount of time.

Network Congestion

Just like in road congestion, Network Congestion occurs when a network is not able to adequately handle the traffic flowing through it. (temporary)

Encapsulation

During encapsulation, each layer builds a protocol data unit (PDU) by adding a header (and sometimes trailer) containing control information to the PDU from the layer above

Application Structure: Client/Server

server:	clients:
always-on host permanent IP address data centers for scaling	communicate with server may be intermittently connected may have dynamic IP addresses do not communicate directly with each other

P2P

no always-on server
arbitrary end systems directly communicate
peers request service from other peers, provide service in return to other peers
self scalability – new peers bring new service capacity, as well as new service demands
peers are intermittently connected and change IP addresses
complex management

principles of network applications

run on (different) end systems
communicate over network
e.g., web server software communicates with browser software
no need to write software for network-core devices
network-core devices do not run user applications
applications on end systems allows for rapid app development, propagation

Web and HTTP Persistent HTTP

persistent HTTP	non-persistent HTTP
multiple objects can be sent over single TCP connection between client, server server leaves connection open after sending response subsequent HTTP messages between same client/server sent over open connection client sends requests as soon as it encounters a referenced object as little as one RTT for all the referenced objects	at most one object sent over TCP connection connection then closed downloading multiple objects required multiple connections requires 2 RTTs per object OS overhead for each TCP connection browsers often open parallel TCP connections to fetch referenced objects

HTTP request message and Method types

two types of HTTP messages: request, response

URL method:

uses GET method
input is uploaded in URL field of request line.

POST method:

web page often includes form input
input is uploaded to server in entity body

Web caching

satisfy client request without involving origin server.
why Web caching?
reduce response time for client request
reduce traffic on an access link

electronic mail and its components; SMTP, POP3, IMAP

SMTP: simple message transfer protocol
POP: post office protocol
IMAP: internet message access

DNS and its services

DNS: domain name system.
DNS services

1. hostname to IP address translation
2. host aliasing
3. canonical, alias names
4. mail server aliasing
5. load distribution
6. replicated Web servers: many IP addresses correspond to one name

TCP vs UDP services

Above

transport-layer services vs network layer

multiplexing and demultiplexing

multiplexing at sender handle data from multiple sockets, add transport header FDM – TDM	demultiplexing at receiver use header info to deliver received segments to correct socket

connectionless transport: UDP

Above

principles of reliable data transfer (rdt)

important in application, transport, link layers
incrementally develop sender
use finite state machines (FSM) to specify sender, receiver

Segments

breaking the application messages into smaller chunks and adding a transport-layer header to each chunk to create the transport-layer segment

Pipelined protocols

Same as rdt
*consider only unidirectional data transfer

Router architecture

1. Input ports. Receiving data from senders.
2. Switching fabric connects the router's input ports to its output ports
3. Output ports store packets received from the switching fabric and transmits these packets on the outgoing link
4. Routing processor. The routing processor performs control-plane functions. In traditional routers, it executes the routing

Two key network-layer functions

1. accepts outgoing messages and combines messages or segments into packets (addressing)
2. adding a header that includes routing information (routing)

Forwarding and Routing

forwarding: move packets from router's input to appropriate router output

routing: determines source-destination route taken by packets

routing algorithm

goal is to determine good paths (equivalently, routes), from senders to receivers, through the network of routers. Typically, a "good" path is one that has the least cost.

forwarding table

A router forwards a packet by examining the value of one or more fields in the arriving packet's header, and then using these header values to index into its forwarding table

Switching fabrics and its three types

1. **Switching via memory**. The simplest, earliest routers were traditional computers, with switching between input and output ports being done under direct control of the CPU (routing processor). Input and output ports functioned as traditional I/O devices in a traditional operating system.
2. **Switching via a bus**. In this approach, an input port transfers a packet directly to the output port over a shared bus, without intervention by the routing processor.
3. **Switching via an interconnection network**. One way to overcome the bandwidth limitation of a single, shared bus is to use a more sophisticated interconnection network

IP datagram format

32 bit above

Switching via interconnection network

Above

CIDR: Classless InterDomain Routing

Classless Inter-Domain Routing is a method for allocating IP addresses and for IP routing. Its goal was to slow the growth of routing tables on routers across the Internet, and to help slow the rapid exhaustion of IPv4 addresses.

DHCP: Dynamic Host Configuration Protocol

the Dynamic Host Configuration Protocol DHCP allows a host to obtain (be allocated) an IP address automatically

DHCP client-server scenario

1. DHCP server **discovery**. The first task of a newly arriving host is to find a DHCP server with which to interact.
2. DHCP server **offer**(s). A DHCP server receiving a DHCP discover message responds to the client with IP.
3. DHCP **request**. The newly arriving client will choose from among one or more server offers
4. DHCP **ACK**. The server responds to the DHCP request message with a DHCP ACK message,

Framing, link access

Framing. Almost all link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission over the link. A frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields. The structure of the frame is specified by the link-layer protocol.

Link access. A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link. For point-to-point links that have a single sender at one end of the link and a single receiver at the other end of the link, the MAC protocol is simple (or nonexistent)—the sender can send a frame whenever the link is idle

Node and datagram

hosts and routers: nodes

Link layer services

1. *flow control:* pacing between adjacent sending and receiving nodes
2. *error detection*: errors caused by signal attenuation, noise. receiver detects presence of errors: signals sender for retransmission or drops frame
3. *error correction:* receiver identifies *and corrects* bit error(s) without resorting to retransmission
4. *half-duplex and full-duplex*

Error detection (EDC)

At the sending node, data, D, to be protected against bit errors is augmented with error-detection and -correction bits

Single and *two-dimensional bit parity checking*

Single parity check: a single bit is appended to the end of each frame, the bit is 1 if the data portion of the frame has odd number of 1's.

Two Dimensional Parity can detect as well as correct one or more bit errors. If a one or more bit error takes place then the receiver will receive the message with the changed parity bit.

Checksum,

A checksum is a small-sized block of data derived from another block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage.

Collision

collision is the situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant

point-to-point and *broadcast access links, protocols*

point-to-point link consists of a single sender at one end of the link and a single receiver at the other end of the link.

broadcast link, can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel. The term broadcast is used here because when any one node transmits a frame, the channel broadcasts the frame and each of the other nodes receives a copy

Three broad classes of MAC protocols

MAC three broad classes:

1. channel partitioning: divide channel into smaller “pieces” (time slots, frequency, code) allocate piece to node for exclusive use
2. random access: channel not divided, allow collisions “recover” from collisions
3. “taking turns”: nodes take turns, but nodes with more to send can take longer turns

CSMA (carrier sense multiple access) & CSMA/CD

CSMA (carrier sense multiple access). Listen before transmitting.

CSMA/CD

1- Taking turns
2- Polling request
3- Token pass

Channel partitioning MAC protocols: TDMA and FDMA

FDMA: frequency division multiple access. Divide the media in bands like radio
TDMA: time division multiple access. Divide the transmission using time frame (send in round)

Taking turns” MAC protocols

	Above	
	Polling	
	the polling protocol. The polling protocol requires one of the nodes to be designated as a master node. The master node polls each of the nodes in a round-robin fashion. In particular, the master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames	