***Chapter – II***

***Packet***

A block of data with a “header” attached that can indicate what the packet contains and where it is headed. Think of a packet as a “data envelope,” with the header acting as an address.

***Mbps***

The “data-carrying” capacity of a network connection, used as an indication of speed. For example, an Ethernet link is capable of moving 10 million bits of data per second. A Fast Ethernet link can move 100 million bits of data per second—10 times more bandwidth.

***Collision***

In Ethernet, the result of two nodes transmitting simultaneously.

The frames from each device impact and are damaged when they meet on the physical media.

**Rules of data transfer**

1. Simple communications: data only travel in one direction (Tx & Rx) at the same frequencies.
2. Half-duplex (semi-duplex) communications

Data can travel in either direction but not simultaneously (Tx frequency differs from Rx frequency).

1. Full – duplex communications

Data can travel in both direction simultaneously (Tx freq. differ from Rx freq.).

**NIC (network interface card):**

### Ethernet Cards

**Ethernet cards are usually purchased separately from a computer. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card.**

**Base band:**

Base band provide a single path for transmitting text, graphics ,voice- video data and apply one type can be transmitted at a time in a base band system .

**Broad band :**

Broad band provide several paths so that different types of data can be transmitted simultaneously.

**Band width** : the range of frequencies that a communications medium can carry , for baseband networking media , the bandwidth also indicates the theoretical maximum amount of data that the medium can transfer.

**FDDI**

A Fiber Distributed Data Interface. A LAN technology based on a 100-Mbps token-passing network running over fiber-optic cable. Usually reserved for network backbones in larger organizations.

**Bottleneck**

It’s the congestion of data traffic at one single node segment of network because of the huge amount of data that wants to pass this point.

**Point to point network**

It’s the network that consist of many connections between individual pairs of machines . In this type rooting algorithm play an important role in normally small geographical size network.

**Protocol**

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer.

Protocols can be calcified as:

1. Transport protocol
2. Application protocol

The most common transport protocol are:

* [**Ethernet**](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\chap2.htm#Ethernet#Ethernet)
* **TCP/IP**
* [**FDDI**](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\chap2.htm#FDDI#FDDI)
* [**ATM**](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\chap2.htm#ATM#ATM)
* **IPX/SPX**
* **NetBiue** 
  1. Transport protocol

Ethernet

It is the most popular network architecture its encompasses many different medias. It’s the packing the data into frames ,use baseband signaling, and most use the CSMA/CD access method. the newer standers supports transmission at 100Mbps.

All Ethernet standers use the hardware address of the NIC to address packets. This hardware address is "burned in” to the read only memory (ROM) on the NIC when it is created and is universally unique .Ethernet is divided into two categories based on transmission speed and media use:-

10Mbps IEEE standards

There are four major implementations of Mbps Ethernet:

1. 10Base5: Ethernet using Thicknet coaxial cable
2. 10Base2: Ethernet using Thicknet coaxial cable
3. 10Base-T: Ethernet over unshided twisted pair (UTP)cable
4. 10Base F: Ethernet over fiber optic cable

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preamble 8 byte | Destination address  6 b | Source address  6b | Type  2b | Data  46-1500 b | Crc  4b |

Fig ( ) Ethernet II frame

CSMA/CD:(Carrier – Sense Multiple Access with Collision Detection)

Is one of the most popular ways to regulate network traffic. Used by Ethernet, this access method prevents collisions by listening to the channel to see if another computer is sending data. If the computer dose not sense data on the line, it sends its massage .if another computer is using the channel, the computer waits a random amount of time and then checks again. This process is continued until the channel is free and the computer can send its data.

Delay caused by collisions and retransmitting is very small and does not normally affect the speed of transmission on the network.

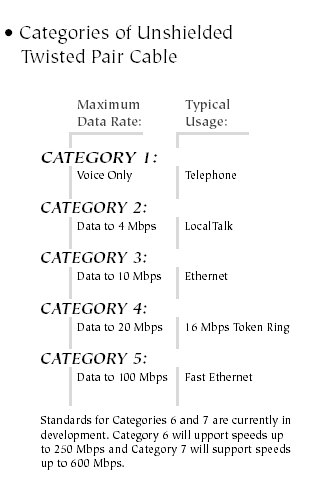
CSMA/CD does not allow traffic from a server to take precedence over traffic from a workstation. All computers on the network are given an equal chance at controlling the channel.

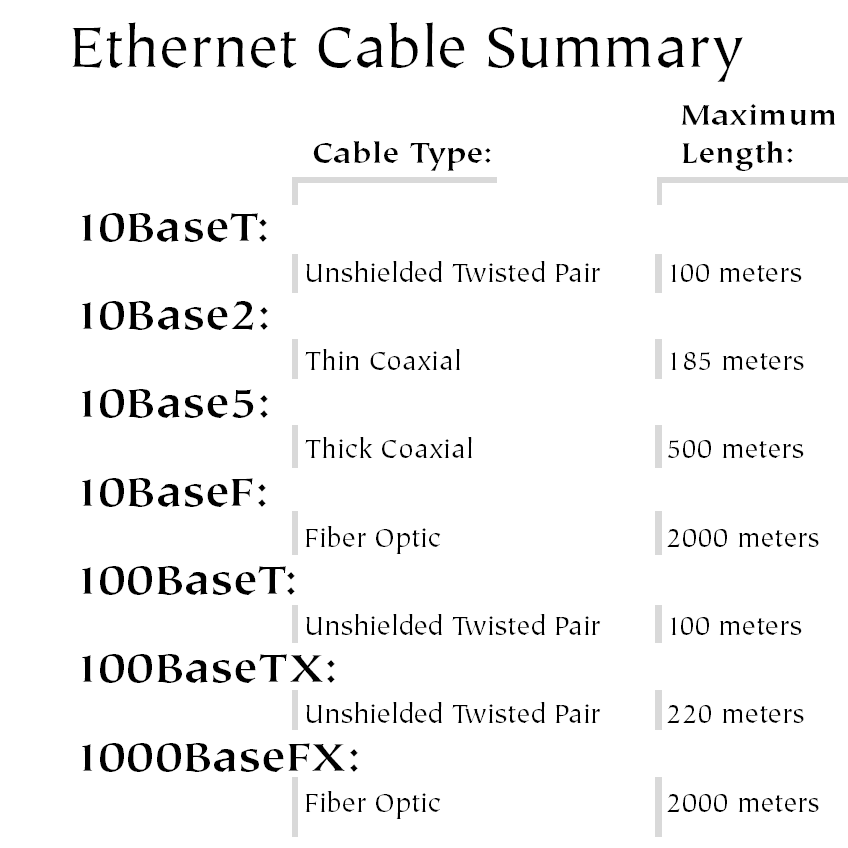
The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps.

Fast Ethernet

To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet is becoming common in schools that have been recently wired.

Gigabit Ethernet

The most recent development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably be used for workstation and server connections also. It can be used with both fiber optic cabling and copper. The 1000BaseTX, the copper cable used for Gigabit Ethernet, is expected to become the formal standard in 1999.



**Throughput** : is the pure amount of information in bits that actually transfer between two computers .

There are two key points to consider when comparing throughput to Bandwidth :

1. The throughput rate may vary over time based on the current conditions in the network, where as bandwidth does not change over time.
2. Bandwidth defines the speed of a single link , and throughput refers to the speed of data transfer between two computers – computers may be, and typically are ,separated by several networking devices and several cables.

Interface:

The major network component that added to make it better

1. Repeaters:
2. Routers
3. Bridges
4. Gateways

**Repeaters**

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can "listen" to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or [physical topologies](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#physical_topology). They must, however, be used between networks with the same [protocol](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#protocol).

Routers

A router translates information from one network to another; it is similar to a superintelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even "listen" to the entire network to determine which sections are busiest -- they can then redirect data around those sections until they clear up.

If you have a school LAN that you want to connect to the [Internet](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#internet), you will need to purchase a router. In this case, the router serves as the translator between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet. Routers can:

* Direct signal traffic efficiently
* Route messages between any two protocols
* Route messages between [linear bus](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#linear_bus), [star](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#star), and [star-wired ring](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#star_wired_ring) topologies
* Route messages across [fiber optic](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#fiber), [coaxial](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#coaxial), and [twisted-pair](file:///C:\Documents%20and%20Settings\Ammar\My%20Documents\Networking%20Book\glossary.htm#twisted) cabling

Gateways :

a gateway is an intricate piece of networking equipment that translates information between two different network architectures or data formats. for example, a gateway can be used to allow network communication between a TCP/IP LAN and an IBM mainframe system using (SNA) System Network Architecture. Another example of a gateways is a system that converts Microsoft Mail to SMTP for transmission over the internet.

**Hub**

A device that interconnects clients and servers, repeating

(or amplifying) the signals between them. Hubs act

as wiring “concentrators” in networks based on star

topologies (rather than bus topologies, in which

computers are daily-chained together).

**Switch**

A device that improves network performance by

Segmenting the network and reducing competition for

Bandwidth. When a switch port receives data packets,

It forwards those packets only to the appropriate port

**Server**

A computer or even a software program that provides

Clients with services—such as file storage (file server),

Programs (application server), printer sharing (print

Server), fax (fax server) or modem sharing (modem

Server).

**FTP**

File Transfer Protocol. A part of the chief Internet

protocol “stack” or group (TCP/IP) used for transferring

files from Internet servers to your computer.

**HTTP**

Hyper Text Transmission Protocol. Protocol that governs

Transmission of formatted documents over the Internet.

**Chapter - III**

The **OSI** reference mode:(Open system internetworking)

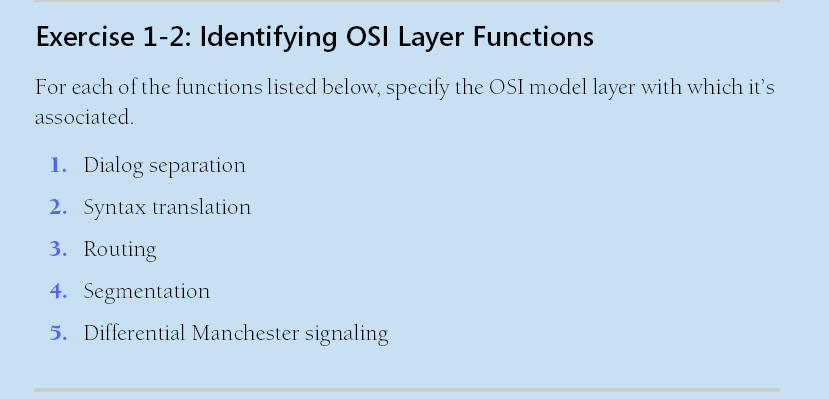
It’s the description of the communications between the computers in the network designed by **(ISO)** international Standards Organization putting the standards for the computer protocols , overcoming all the architectural differences ,OS, and software applications.

OSI identified precisely the type of service and the activity of the protocol in each layer and what must each one do.

Each layer do a especial action different from others and each one provide a service to the above layer and requiring another service from

the lower one , knowing that each layer add its header segment

Functions of OSI can be listed as:



|  |
| --- |
| **Application Layer**  software |
| **Presentation Layer**  JPG-ASCII-data compression-encryption – redirect request to net |
| **Session Layer**  Computer recognition –data synch-rules of comm. |
| **Transport Layer**  Connection-continuation |
| **Network Layer**  Router-IP |
| **Data Link Layer**  MAC-Switch |
| **Physical Layer**  HUB |

Fig ( )The seven layer OSI reference mode standard

1. **Physical layer :**

Layer 1 is the physical layer, its job is to convert bits into signals for outgoing massage, and signals into bits for incoming ones .

The physical layer manage the computer's interface to the network medium and instructs the driver software and the network interface on what to send across the medium.

Its where all the details for creating a network connection are specified: this includes how the medium attaches to (or communicates with) the NIC also it governs the type of connector used and regulates the transmission technique used to send signals across the networking medium.

1. Data Link Layer :

The function of this layer is to provide services to network layer.

The main service is transferring data from network layer on the source machine to the network later on destination machine

Data link layer jobs is to:-

1. Take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer.

It accomplishes this task by having the sender break the input data up into data frames, transmit the frames sequentially, and process the acknowledgement frames sent back by the receiver.

b- Create and recognize frame boundaries, it accomplish by attaching special bit patterns to the beginning and end of the frame

c- Retransmit the frame if it is destroyed.

d- Employed traffic regulation mechanism.

e- Error detection and correction using error detection codes and error correcting codes.

f- Provide services to the network layer.

1. Network Layer:

The network layer routed information from one computer to another. The computers may be physically connected with in the same network or within another network.

The layer 3 ,handles addresses and names into their physical counterparts. The network layer is also responsible for deciding how to route transmissions from sender to receiver. To determine how to get from point a to point b, the network layer considers factors based on network conditions, quality of service information, cost of alternative routes, and delivery priorities.

This layer is also the traffic cop for network activity and handles (packet switching), data routing, and (congestion control).

When moving data from one kind of network medium to another, the network layer also handles segmentation and reassembly functions based on disparities between dissimilar media.

*Where:*PDU: (Packet Data Unit) is a data unit associated with processing at any layer in the OSI. in another word it’s a unit of information passed as a self-contained data structure from one layer to another up or down the stack. In the preceding discussion, it would have been more accurate to say that, within reason, an outgoing PDU for the sender at given layer should substantially agree with the incoming version of that same PDU on the receiver.

At each layer in the stack, the software its own special formatting or addressing to the PDU to allow delivery of its payload across the network successfully when data shows up on the receiving end, the basket travels up the stack from the physical layer through the application layer .at each layer, the software reads it specific PDU data and performs whatever additional processing may be required . it then strips that information of the PDU and passes it the next – higher layer . when the basket leaves the application layer , the data is in from that readable to the receiving application and has been stripped of all the network addressing and packaging in instruction necessary to move the data from sender to receiver.

**Payload :** Thedata content within a PDU

**Connectionless protocol :** is a type of protocol that sends the data across the network to its destination without guaranteeing receipt.

**Connection- Oriented Protocol** : this one establishes a formal connection between two computers, guaranteeing the data reaches its destination.

**4- Transport Layer :**

This layer is the heart of all protocol hiericaly it’s the tasks to provide reliable cost effective data transport from source machine to destination machine independent of physical network. The primary function is enhancing the quality of service (QoS) provided by network layer.

The quality of service parameters are:\_

1. Connection establishment delay.
2. Connection establishment failure probability.
3. Throughput (no. of bytes per second)
4. Residual error ratio (No. of lost massages per total Snet)
5. Protection
6. Priority
7. Resilience

(Probability of transport layer terminated the connection Due to internal problem).

The quality of service is specified by T.L when connection is requested

Note: the option negotiation such as about the speed of throughput is done by transport Layer.

Some tasks of transport Layer:-

1. Basic function of this layer is to accept data from session layer, split it up into smaller units if needed, pass these to the network layer and ensure that all pieces arrived correctly at the other end.
2. Determines what type of service to provide to session layer (connection oriented or connectionless).
3. Multiplexing several massage streams onto 1 channel.
4. Take care of establishing and deleting connections across the network**.**
5. **Session Layer :**

Permits two parties to hold ongoing communications – called a session-across a network. This means applications on either end of the session can exchange data for as long as the session lasts.

The session layer is capable of:-

1- Is conceder the user interface into the network tasks:-

2-allow users on different machine to establish session between them.

3-Manage the dialog control.

4-Synchronization

5- Provide check point into data streams.

1. **Presentation Layer**

Concerned with syntax and semantics of the information because in this layer massages are translated into form the format used in the network to a format used inside the computer

7- Application layer :-

This layer is the last layer contained different protocols that are commonly need (for ex:- there are hundreds of incompatible terminal types in the world that need to be compatible),also application layer activities to user such as file transfer ,handling massages and providing security.

PDU: ( Packet Data Unit) a data unit associated with processing at any layer in the OSI .

**Some network transport protocols:**

1. **ATM**

Asynchronous Transfer Mode. Under ATM, multiple traffic types (such as voice, video, or data) are length “packets” moved by technologies such as Ethernet and FDDI Fiber Distributed Data Interface. This feature enables very high speeds, making ATM popular for demanding network backbones. With networking equipment that has recently become available, ATM will also support WAN transmissions. This feature makes ATM valuable for large, dispersed organizations.

1. IPX/SPX : ( Internetwork Packet eXchange) is a protocol designed and developed by Novell, its network and transport layer protocol this protocol is the most commonly associated with NetWare networks.

SPX : (sequence Packet eXchange) this protocol functions in transport layer SPX is responsible of segmenting data into packets and maintaining a sequence number for each packet. The receiving computer uses the number to reassemble the data.

1. **NetBEUI :**

Network Enhanced User Interface is a computer network working with small office networks (un routable protocol) not routable protocol, up to 200 pc can be controlled by this protocol.

1. **Telnet:** Is a route Terminal emulation protocol. Also operating at all upper layers, which are mostly used to provide connectivity between dissimilar system (e.g. Pc and router). Through telnet, remote equipment (such as routers and switches) can be monitored and configured thus remote system can be troubleshooted.
2. **TCP/IP**(Transmission Control Protocol/ Internet Protocol): it is designed by DoD consists of many protocols ,it’s a connection oriented protocol and defines the set of networking standards and protocols used to build most networks today. it’s the commonly used protocol because it allows for easy cross-platform communications and it’s the base of Internet.

TCP/IP gained popularity when it was adopted as the protocol for UNIX system. Its scalability and superior functionality over Wan,s has made it the standard for connecting different types of computers and networks .

**Internet Protocol** IP is network layer protocol that provides source and destination addressing and routing in the TCP/IP suite. IP is connectionless datagram protocol that, like all connectionless protocols, is fast but unreliable.

|  |
| --- |
| **Application** |
| **Transport** |
| **Internet** |
| **Network**  **Access** |

**Fig ( ) TCP/IP network Model**

1. Application software (a web server in this case) packages the contents of the web page along with any needed application headers. With web services, the HTTP protocol builds the header, including things like the name of the file that is being sent to the web browser. This process includes the application layer processing, which is typically implemented by the application software.
2. The transport layer software , which is TCP in this case , segments the data into chunks or pieces that are small enough to be accepted in the network.(the data created at step 1 (layer 1) is too big to all be sent at once over the network : in this example , creates two TCP segments). TCP also adds a *transport layer header* to the data given to it from the application layer. (The data structure at this step, which includes the TCP header and data, is called a segment.)
3. The network layer software: IP in this case, adds a header in order to provide destination logical address. The header also includes a source logical address so that the computer receiving data knows to whom to reply. Having the destination address, the data can be routed to the end destination; it’s on the same LAN or on the other side of the Internet. (The data structure at this step, which includes the IP header and data, is called a packet.)
4. The network access layer, specifically the part the more closely matches the OSI data link layer, adds another header, plus a trailer, to the data .because this example uses an Ethernet NIC , this step adds an Ethernet header and trailer to the data . The header includes destination MAC address, which is used for forwarding the data over the Ethernet. (The data structure at this step, which includes the Ethernet header, trailer and data, is called frame).

Also the network access layer specifically the part that matches the OSI physical layer, causes the bits to be physically transmitted over the medium.

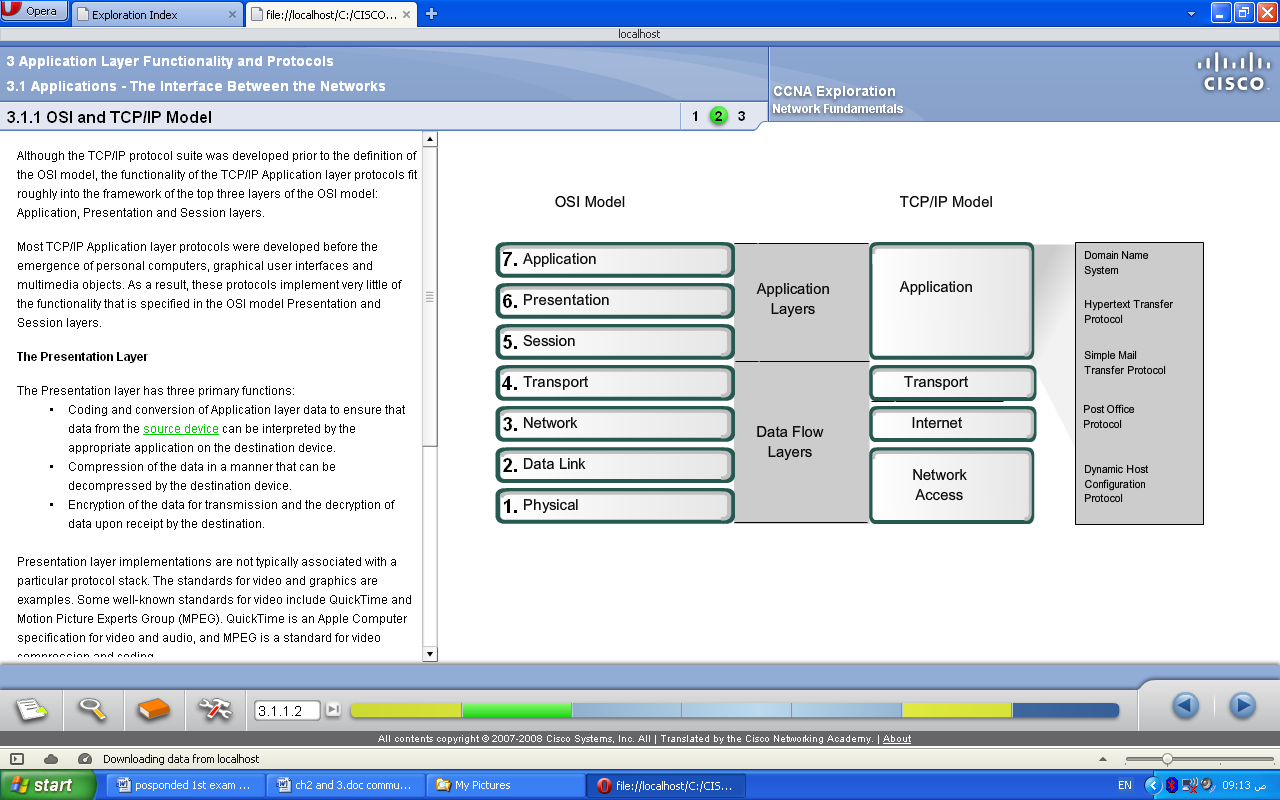


Fig ( ) The comparison of OSI and TCP/IP of DoD Models

**Capsulation :**

Segmentation and enveloping of data as it passes down the protocol stack in the source end device attaching all the required headers according to each layer until reaching the transmission medium.

**Decapsulation**

It’s the reassembly of the data as it passes up the stack of protocol in the destination device until reaches the application file.

**Encapsulation**

As application data is passed down the protocol stack on its way to be transmitted across the network media, various protocols add information to it at each level. This is commonly known as the encapsulation process.

During encapsulation, each succeeding layer encapsulates the PDU that it receives from the layer above in accordance with the protocol being used. At each stage of the process, a PDU has a different name to reflect its new appearance. Although there is no universal naming convention for PDUs, in this course, the PDUs are named according to the protocols of the TCP/IP suite.

1. Data - The general term for the PDU used at the Application layer
2. Segment - Transport Layer PDU
3. Packet - Internet Layer PDU
4. Frame - Network Access Layer PDU
5. Bits - A PDU used when physically transmitting data over the medium

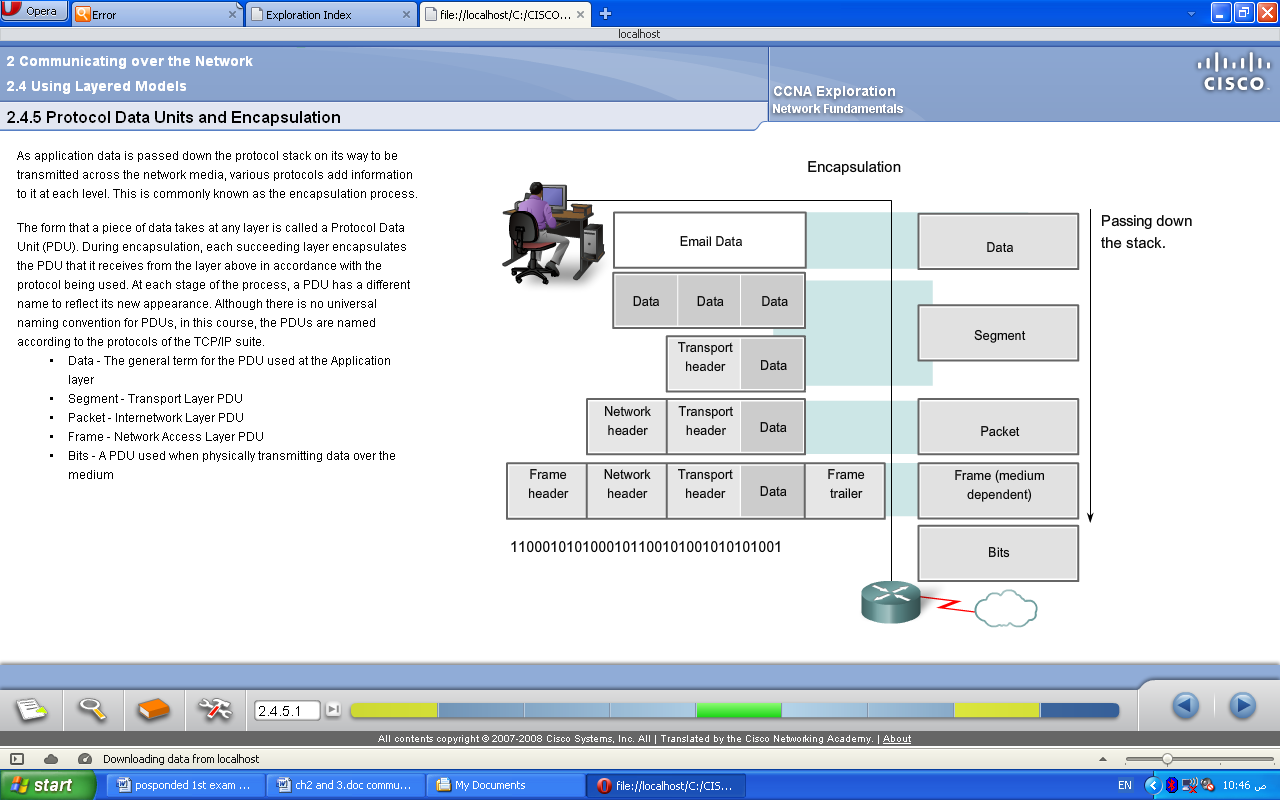


Fig ( ) Encapsulation process with PDU headers

Data (1000 b)

Data (1000 b)

HTTP

Data (1000 b)

TCP

Data (1000 b)

Eth

Data (1000 b)

Eth

IP

Segment

Packet

Frame

Bits 01001011111000011110001010101000000000001101010010100101

1

2

3

4

5

Fig ( ) Encapsulation process

Data (1000 b)

Data (1000 b)

HTTP

Data (1000 b)

TCP

Data (1000 b)

Eth

Data (1000 b)

Eth

IP

Segment

Packet

Frame

Bits 01001011111000011110001010101000000000001101010010100101

5

4

3

2

1

Fig ( ) De-capsulation process

1. UDP (User Data Protocol):

Is a connectionless Transport layer Protocol. And because of reducing its overhead, it’s generally faster, although less reliable than TCP.

Where Overhead is the total amount of Data that transfer over the media at a specific network segment.

**Network factors:**

Many factors influence (throughput). Among these factors are the amount of traffic, the type of traffic, and the number of network devices encountered on the network being measured. In a multi-access topology such as Ethernet, nodes are competing for media access and its use. **Therefore, the throughput of each node is degraded as usage of the media increases**.

In an internetwork or network with multiple segments, throughput cannot be faster than the slowest link of the path from source to destination. Even if all or most of the segments have high bandwidth, it will only take one segment in the path with low throughput to create a bottleneck to the throughput of the entire network.

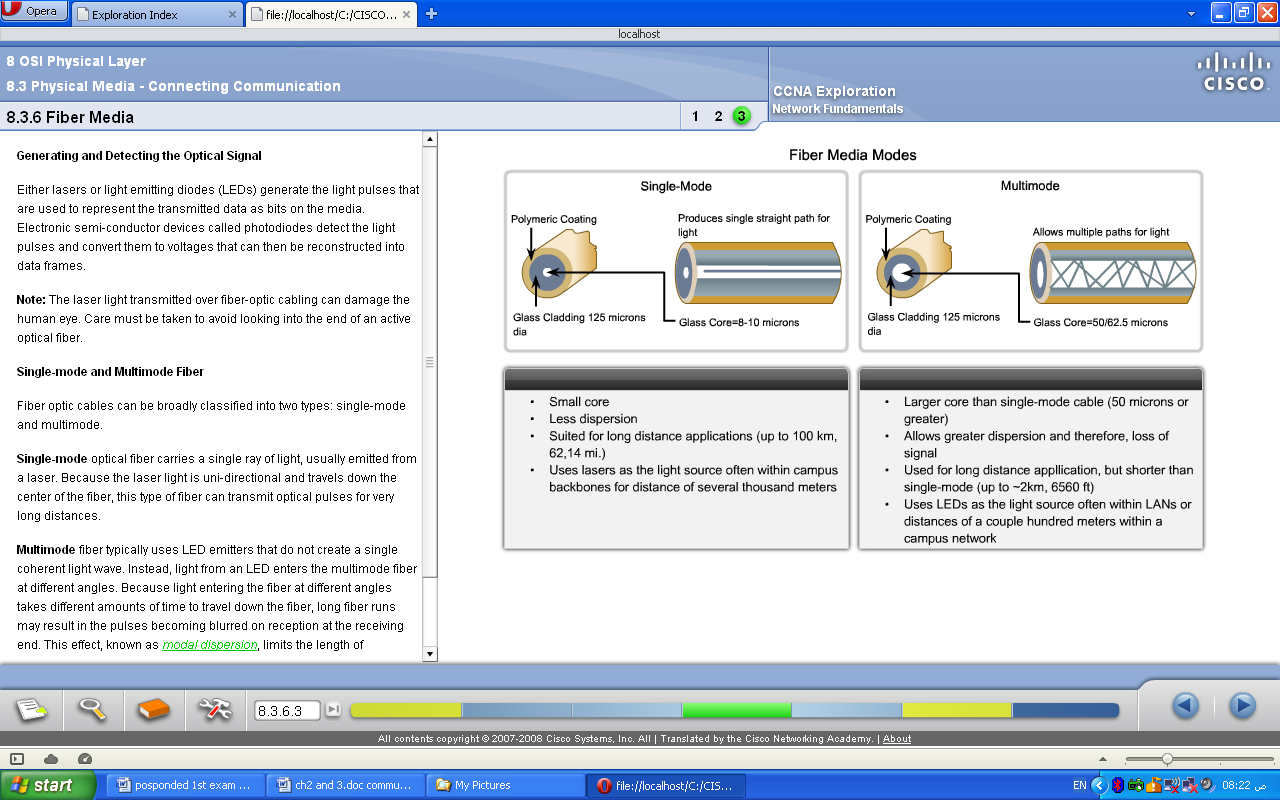
**Goodput:**

A third measurement has been created to measure the transfer of usable data. That measure is known as goodput. Goodput is the measure of usable data transferred over a given period of time, and is therefore the measure that is of most interest to network users.

Goodput measures the effective transfer of user data between Application layer entities, such as between a source web server process and a destination web browser device. Unlike throughput**,** which measures the transfer of **bits** and not the transfer of usable data, goodput accounts for **bits** devoted to protocol overhead.

Generating and Detecting the Optical Signal

Either lasers or light emitting diodes (LEDs) generate the light pulses that are used to represent the transmitted data as bits on the media. Electronic semi-conductor devices called photodiodes detect the light pulses and convert them to voltages that can then be reconstructed into data frames.



Note: The laser light transmitted over fiber-optic cabling can damage the human eye. Care must be taken to avoid looking into the end of an active optical fiber.

* Single-mode and Multimode Fiber

Fiber optic cables can be broadly classified into two types: single-mode and multimode.

Single-mode optical fiber carries a single ray of light, usually emitted from a laser. Because the laser light is uni-directional and travels down the center of the fiber, this type of fiber can transmit optical pulses for very long distances.

Multimode fiber typically uses LED emitters that do not create a single coherent light wave. Instead, light from an LED enters the multimode fiber at different angles. Because light entering the fiber at different angles takes different amounts of time to travel down the fiber, long fiber runs may result in the pulses becoming blurred on reception at the receiving end. This effect, known as modal dispersion, limits the length of multimode fiber segments.

* Multimode fiber, and the LED light source used with it, are cheaper than single-mode fiber and its laser-based emitter technology.

**Common Optical Fiber Connectors**

Fiber-optic connectors come in a variety of types. The figure shows some of the most common:

Straight-Tip (ST) (trademarked by AT&T) - a very common bayonet style connector widely used with multimode fiber.

Subscriber Connector (SC) - a connector that uses a push-pull mechanism to ensure positive insertion. This connector type is widely used with single-mode fiber.

Lucent Connector (LC) - A small connector becoming popular for use with single-mode fiber and also supports multi-mode fiber.

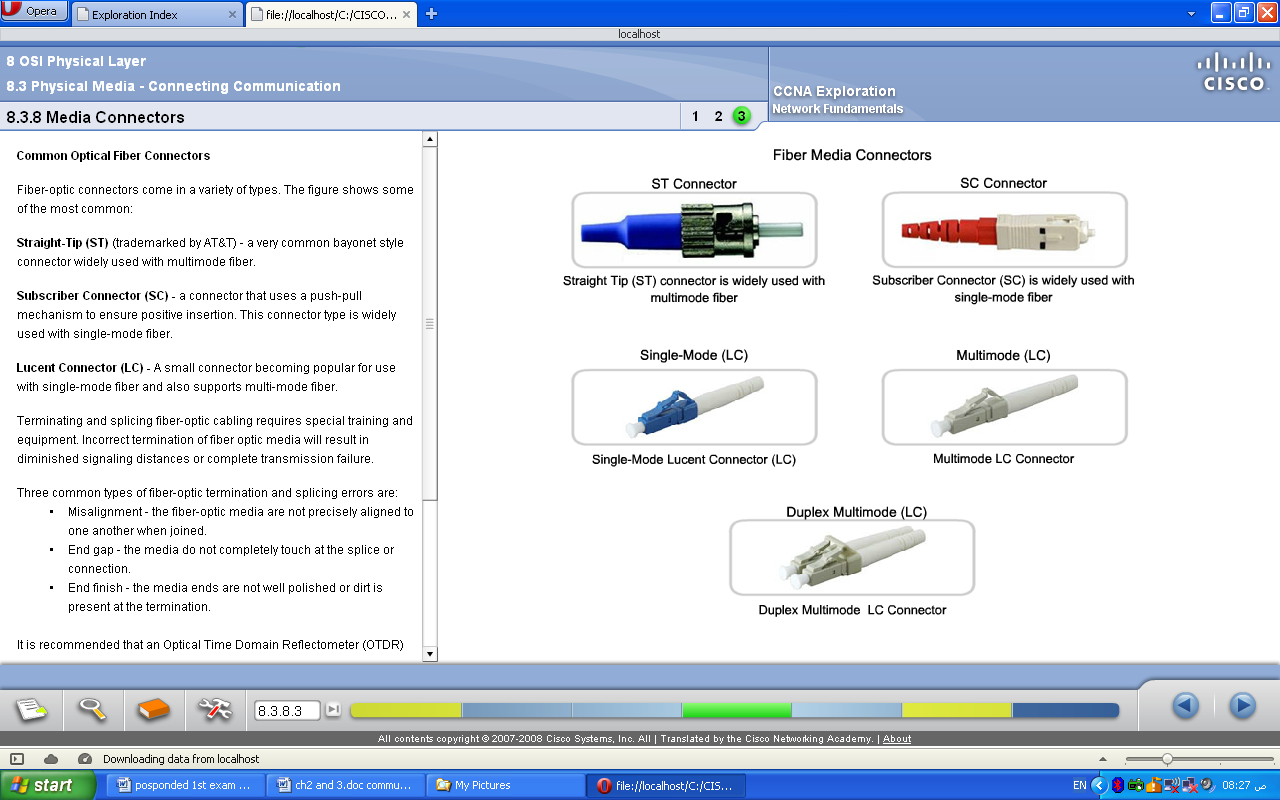
Terminating and splicing fiber-optic cabling requires special training and equipment. Incorrect termination of fiber optic media will result in diminished signaling distances or complete transmission failure.

Three common types of fiber-optic termination and splicing errors are:

Misalignment - the fiber-optic media are not precisely aligned to one another when joined.

End gap - the media do not completely touch at the splice or connection.

End finish - the media ends are not well polished or dirt is present at the termination.



It is recommended that an Optical Time Domain Reflectometer (OTDR) be used to test each fiber-optic cable segment. This device injects a test pulse of light into the cable and measures back scatter and reflection of light detected as a function of time. The OTDR will calculate the approximate distance at which these faults are detected along the length of the cable.

A field test can be performed by shining a bright flashlight into one end of the fiber while observing the other end of the fiber. If light is visible, then the fiber is capable of passing light. Although this does not ensure the performance of the fiber, it is a quick and inexpensive way to find a broken fiber.

# Bit Time

For each different media speed, a period of time is required for a bit to be placed and sensed on the media. This period of time is referred to as the bit time. On 10-Mbps Ethernet, one bit at the MAC layer requires 100 nanoseconds (nS) to transmit. At 100 Mbps, that same bit requires 10 nS to transmit. And at 1000 Mbps, it only takes 1 nS to transmit a bit. As a rough estimate, 20.3 centimeters (8 inches) per nanosecond is often used for calculating the propagation delay on a UTP cable. The result is that for 100 meters of UTP cable, it takes just under 5 bit times for a 10BASE-T signal to travel the length the cable.

Subnet Masks

Having determined the required number of hosts and subnets, the next step is to apply one subnet mask for the entire network and then calculate the following values:

A unique subnet and subnet mask for each physical segment

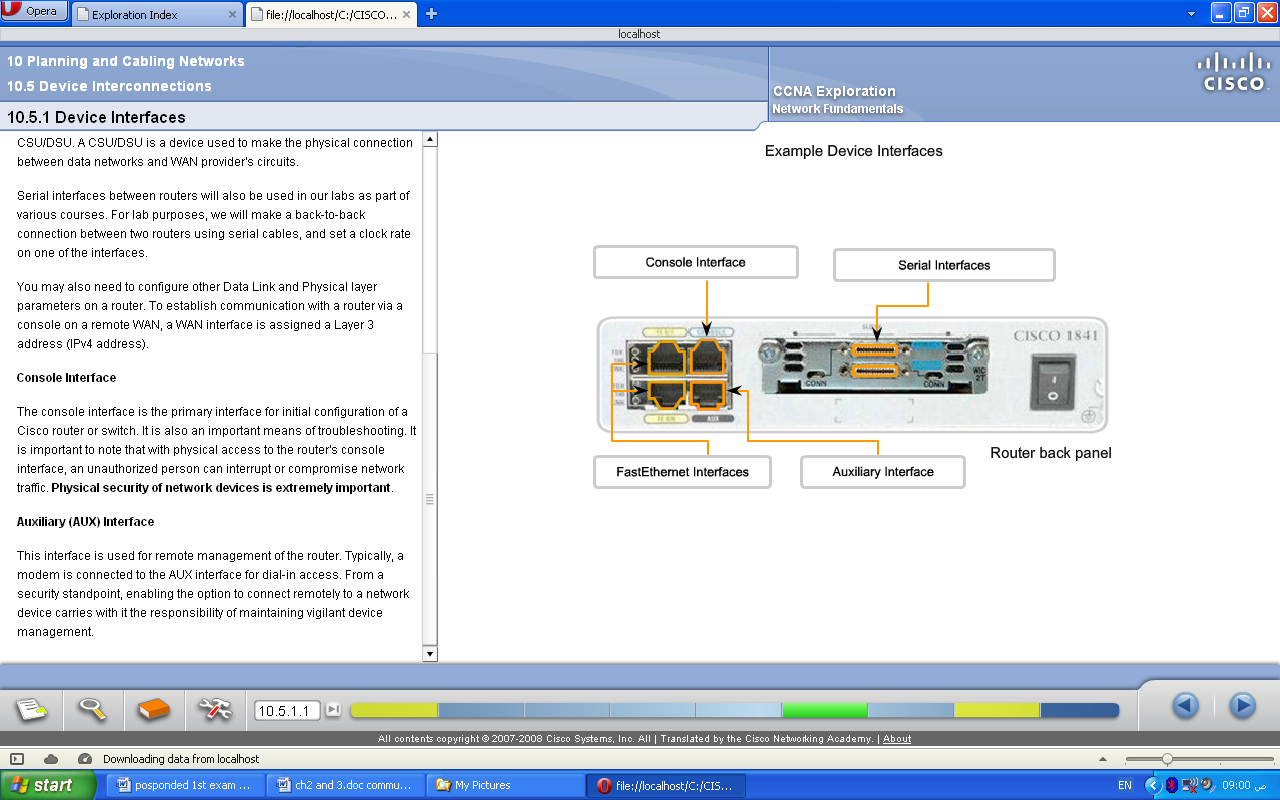
A range of usable host addresses for each subnet

Console Interface

The console interface is the primary interface for initial configuration of a Cisco router or switch. It is also an important means of troubleshooting. It is important to note that with physical access to the router's console interface, an unauthorized person can interrupt or compromise network traffic. Physical security of network devices is extremely important.

Auxiliary (AUX) Interface

This interface is used for remote management of the router. Typically, a modem is connected to the AUX interface for dial-in access. From a security standpoint, enabling the option to connect remotely to a network device carries with it the responsibility of maintaining vigilant device management.



The most widely-known TCP/IP Application layer protocols are those that provide for the exchange of user information. These protocols specify the format and control information necessary for many of the common Internet communication functions. Among these TCP/IP protocols are:

Domain Name Service Protocol (DNS) is used to resolve Internet names to IP addresses.

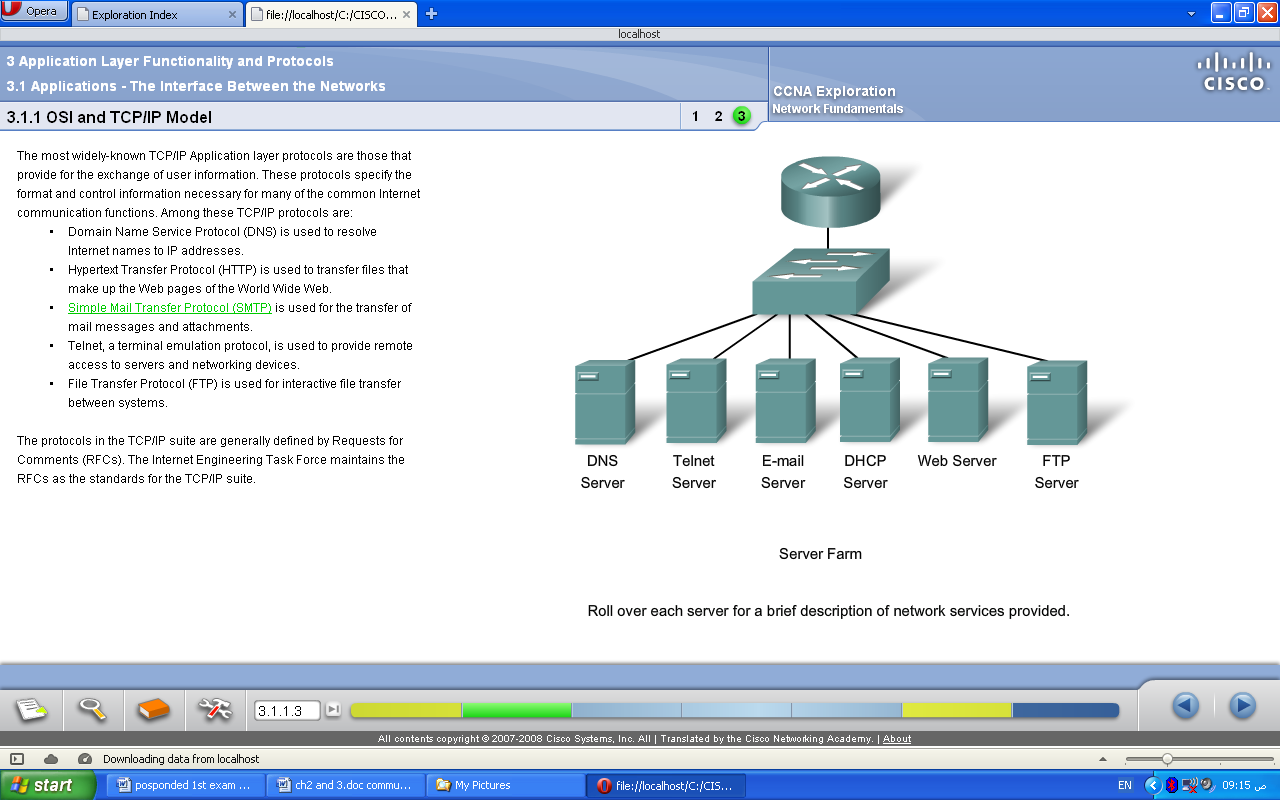
Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.

Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.

Telnet, a terminal emulation protocol, is used to provide remote access to servers and networking devices.

File Transfer Protocol (FTP) is used for interactive file transfer between systems.

The protocols in the TCP/IP suite are generally defined by Requests for Comments (RFCs). The Internet Engineering Task Force maintains the RFCs as the standards for the TCP/IP suite.



Now that we have a better understanding of how applications provide an interface for the user and provide access to the network, we will take a look at some specific commonly used protocols.

As we will see later in this course, the Transport layer uses an addressing scheme called a port number. Port numbers identify applications and Application layer services that are the source and destination of data. Server programs generally use predefined port numbers that are commonly known by clients. As we examine the different TCP/IP Application layer protocols and services, we will be referring to the TCP and UDP port numbers normally associated with these services. Some of these services are:

Domain Name System (DNS) - TCP/UDP Port 53

Hypertext Transfer Protocol (HTTP) - TCP Port 80

Simple Mail Transfer Protocol (SMTP) - TCP Port 25

Post Office Protocol (POP) - UDP Port 110

Telnet - TCP Port 23

Dynamic Host Configuration Protocol - UDP Ports 67 and 68

File Transfer Protocol (FTP) - TCP Ports 20 and 21

DNS

In data networks, devices are labeled with numeric IP addresses, so that they can participate in sending and receiving messages over the network. However, most people have a hard time remembering this numeric address. Hence, domain names were created to convert the numeric address into a simple, recognizable name.

On the Internet these domain names, such as www.cisco.com, are much easier for people to remember than 198.133.219.25, which is the actual numeric address for this server. Also, if Cisco decides to change the numeric address, it is transparent to the user, since the domain name will remain www.cisco.com. The new address will simply be linked to the existing domain name and connectivity is maintained. When networks were small, it was a simple task to maintain the mapping between domain names and the addresses they represented. However, as networks began to grow and the number of devices increased, this manual system became unworkable.

The Domain Name System (DNS) was created for domain name to address resolution for these networks. DNS uses a distributed set of servers to resolve the names associated with these numbered addresses.

The DNS protocol defines an automated service that matches resource names with the required numeric network address. It includes the format for queries, responses, and data formats. DNS protocol communications use a single format called a message. This message format is used for all types of client queries and server responses, error messages, and the transfer of resource record information between servers.