Computer Networking

Reference Models

Reference Models

- Two important network architectures, the
- ❑ OSI (Open Systems Interconnection) reference model
- ❑ TCP/IP (Transmission Control Protocol/Internet Protocol) reference model
- The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology.
- The **OSI Model** is a conceptual framework used to describe the functions of a networking system.
- **TCP/IP Model** is a suite of communication protocols used to interconnect network devices on the internet.

- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- The OSI model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers. It was revised in 1995.
- The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems. We will just call it the OSI model for short.
- Although the protocols associated with the OSI model are rarely used any more, the model itself is actually quite general and still valid, and the features discussed at each layer are still very important.
- The TCP/IP model has the opposite properties: the model itself is not of much use but the protocols are widely used.

OSI Reference Model

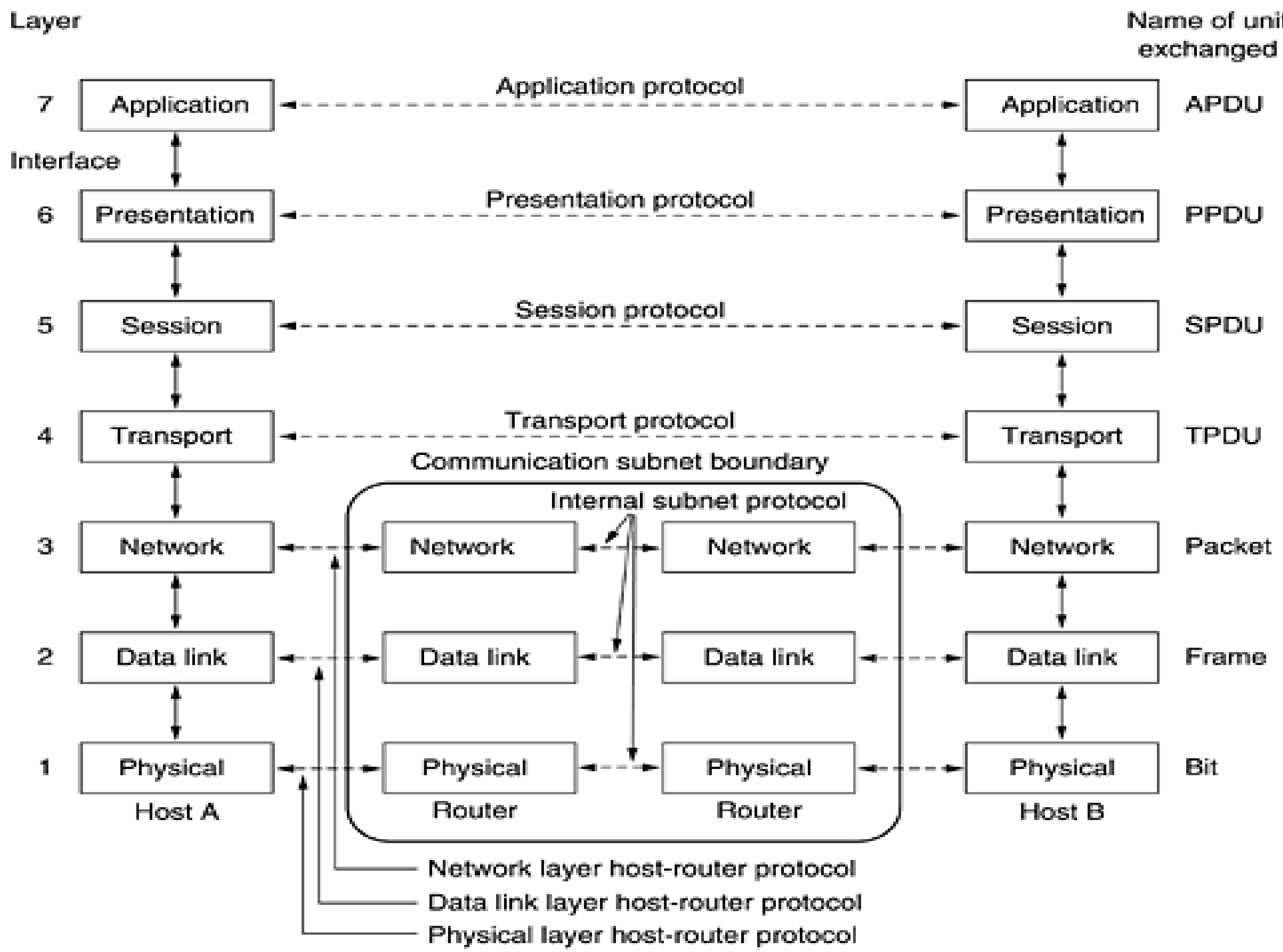
- The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:
    1. A layer should be created where a different abstraction is needed.
    2. Each layer should perform a well-defined function.
    3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
    4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
    5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

- The OSI model has seven layers:

- ❑ Physical Layer
- ❑ Data Link Layer
- ❑ Network Layer
- ❑ Transport Layer
- ❑ Session Layer
- ❑ Presentation Layer
- ❑ Application Layer

- It's easy to remember the sequence of OSI Model 7 Layers using this simple sentence:
  - “**P**lease **D**o **N**ot **T**hrow **S**eafood **P**izza **A**way”
  - "**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing."

The OSI reference model



The Physical Layer

- The physical layer is concerned with transmitting raw bits over a communication channel.
- Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism.
- Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations.
- Converts data from the upper layers into 1s and 0s for transmission over media.
- Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data. The binary data is then sent over the wired or wireless media.
- Defined on this layer: Cable standards, wireless standards, and fiber optic standards.
- Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the Physical layer of the OSI Model.

The Physical Layer

- The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.
- Typical questions here are
  - how many volts should be used to represent a 1 and how many for a 0,
  - how many nanoseconds a bit lasts, whether transmission may proceed simultaneously in both directions,
  - how the initial connection is established and how it is torn down (disassemble or disintegrate) when both sides are finished, and
  - how many pins the network connector has and what each pin is used for.
- The design issues here largely deal with mechanical, electrical, and timing interfaces, and the physical transmission medium, which lies below the physical layer.

The Data Link Layer

- Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.
- At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.
- Data link layer Transforms the raw data bits to a data frame (few hundred/thousand bits).
- It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially.
- Is responsible for moving frames from node to node or computer to computer.
- Protocols defined include **Ethernet Protocol** and **Point-to-Point Protocol (PPP)**

The Data Link Layer

- Two sublayers: Logical Link Control (LLC) and the Media Access Control (MAC)

Logical Link Control (LLC)

–Data Link layer addressing, flow control, address notification, error control

Media Access Control (MAC)

–Determines which computer has access to the network media at any given time

–Determines where one frame ends and the next one starts, called frame synchronization

- One issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data.
- Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel. A special sublayer of the data link layer, the media access control sublayer, deals with this problem.

The Network Layer

- The network layer controls the operation of the subnet.
- Responsible for moving packets (data) from one end of the network to the other, called *end-to-end communications*
- Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.
- Handles the issues raised due to different physical addresses of machines belonging to different networks
- A key design issue is determining how packets are routed from source to destination.
- If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer.
- More generally, the quality of service provided (delay, transit time, etc.) is also a network layer issue.

The Network Layer

- When a packet has to travel from one network to another to get to its destination, many problems can arise.
- The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large.
- The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.
- Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other.
- Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

The Transport Layer

- Accepts data from higher levels and splits it into smaller segments that can be sent to network layer.
- Transport layer takes data from upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to lower layer (Network Layer) for delivery.
- This Layer is the first one which breaks the information data, supplied by Application layer in to smaller units called segments.
- Also, reassembles data segments into data for the use of higher layers
- Puts segments in correct order (called sequencing) so they can be reassembled in correct order at destination.
- This layer ensures that data must be received in the same sequence in which it was sent.
- Concerned with the reliability of the transport of sent data.
- May use a *connection-oriented protocol* such as TCP (Transmission Control Protocol) to ensure destination received segments
- May use a *connectionless protocol* such as UDP (User Datagram Protocol) to send segments without assurance of delivery

The Session Layer

- The session layer allows users on different machines to establish active communication sessions between them.
- It's main aim is to establish, manage, terminate, maintain and synchronize the interaction between communicating systems.
- Provides duplex, half-duplex, or simplex communications between devices
- Sessions offer various services, including
  - Dialog control
  - Token management
  - Synchronization

- **Dialog control** :keeping track of whose turn it is to transmit. This layer allows two systems to start communication with each other.
- **Token management:** preventing two parties from attempting the same critical operation at the same time.
- **Synchronization:** checkpointing long transmissions to allow them to continue from where they were after a crash. This layer allows a process to add checkpoints which are considered as synchronization points into stream of data.

The Presentation Layer

- The primary goal of this layer is to take care of the **syntax** and **semantics** of the information exchanged between two communicating systems.
- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
- Since different computer may deal with different data representations a standard encoding is done, thus handles three primary tasks:

–Translation , –Compression , –Encryption

- **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
- **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
- **Compression:** The primary role of Data compression is to reduce the number of bits to be transmitted.

The Application Layer

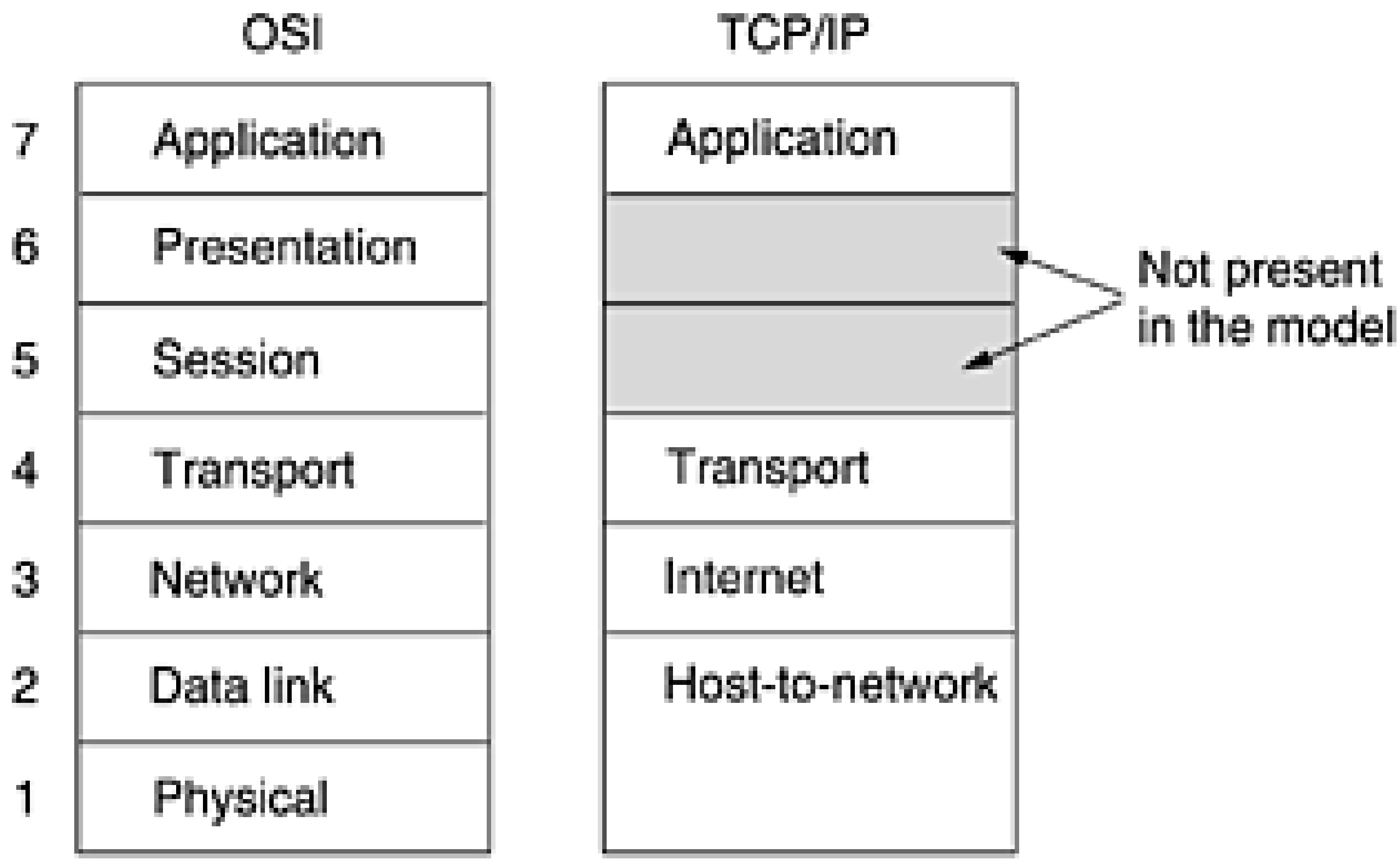
- The application layer contains a variety of protocols that are commonly needed by users. This layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc.
- One widely-used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web.
- Other Application protocols that are used are: File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), TELNET, Domain Name System (DNS) etc.
- Functions of Application Layer
  - Mail Services
  - Network Virtual Terminal
  - Directory Services
  - File Transfer, Access and Management (FTAM)

- **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
- **Network Virtual Terminal:** It allows a user to log on to a remote host.
- **Directory Services:** This layer provides access for global information about various services.
- **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

The TCP/IP Reference Model

- This model was proposed earlier to OSI model.
- The main aim behind the development of this protocol suite is to support/interconnect different types of network (e.g. interconnection of radio network and computer network).
- Another major goal is connections to remain intact as long as the source and destination machines were functioning, even if some of the machines or transmission lines in between were suddenly put out of operation.
- The original TCP/IP protocol suite was defined having four protocol layers: **Host-to-network, internet, transport and application**.
- When TCP/IP is compared to OSI it can be seen that the host-to-network layer is equivalent to the combination of physical and data link layer. Also, the internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers.

The TCP/IP reference model.



The Host-to-Network Layer

- The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it.
- This protocol is not defined and varies from host to host and network to network. Books and papers about the TCP/IP model rarely discuss it.
- At the physical and data link layers, *TCP/IP* does not define any specific protocol. It supports all the standard and proprietary protocols.

The Internet Layer

- All these requirements led to the choice of a packet-switching network based on a connectionless internetwork layer. This layer, called the internet layer.
- The job of this layer is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network).
- They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.

The Internet Layer

- The internet layer defines an official packet format and protocol called **IP (Internet Protocol)**. The job of the internet layer is to deliver IP packets where they are supposed to go.
- Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer.

Transport Layer

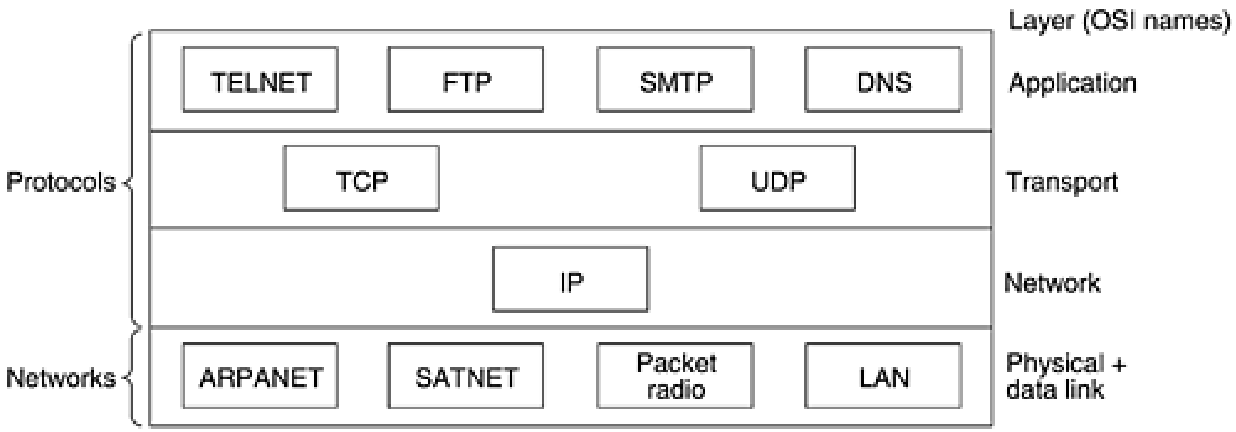
- Allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Makes the use of either of the two types of transport protocol **TCP(Transmission Control Protocol) , UDP(User Datagram Protocol).**
- **TCP(Transmission Control Protocol) :**

  - A reliable connection-oriented protocol.
  - Allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.
  - It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer.
  - At the destination, the receiving TCP process reassembles the received messages into the output stream.
  - TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

Transport Layer

- **UDP(User Datagram Protocol):**
  - An unreliable, connectionless protocol for applications that do not want sequencing or flow control and wish to provide their own.
  - Also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.
  - The relation of IP, TCP, and UDP is shown in figure.

(Fig: Protocols and networks in the TCP/IP model initially)



The Application Layer

- Application layer protocols define the rules when implementing specific network applications
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
  - FTP – File Transfer Protocol (For file transfer)
  - Telnet – Remote terminal protocol (For remote login on any other computer on the network)
  - SMTP – Simple Mail Transfer Protocol (For mail transfer)
  - HTTP – Hypertext Transfer Protocol (For Web browsing)
  - NNTP-Network News Transfer Protocol (For transfer newsgroup articles between systems over the Internet)

A Comparison of the OSI and TCP/IP Reference Models

- Since both OSI and TCP/IP reference models have developed looking at the operation of communication between users of a computer network they support some similar characteristics as listed below.

Similarities :

- Both lie on the concept of a stack of independent protocols.
- Functionality of the layers is roughly similar

Differences :

OSI reference model	TCP/IP reference model
uses 7 different layers.	Uses 4 different layers.
Supports both connectionless & connection oriented service in the network layer but only connection oriented service in transport layer.	Supports only connectionless service in the network layer but both connectionless & connection oriented service in transport layer.
Clearly distincts service, interface & protocol.	Doesn't clearly distinguish service, interface & protocol.
Protocols are better hidden and can be replaced relatively easily as the technology changes.	Protocols are not hidden and can not be replaced easily as the technology changes (e.g. Replacing IP with a different protocol is virtually impossible).
The reference model was devised before the corresponding protocols were invented.	The protocols came first, and the model was really just a description of the existing protocols since the prtocols fit perfectly.