Welcome to CITS3002 Computer Networks

This unit introduces students to the design and implementation of contemporary wired and wireless computer networks, the systems- and application-level software necessary to support their efficient operation, and the security and privacy factors introduced and enabled by networks and their applications.

Today it is far more likely that a computer is connected to a computer network than not. As computer networks become increasingly faster, more reliable, and more pervasive, the way in which we view computer systems and computing is rapidly changing. This unit takes a bottom-up approach to explaining how current networking technologies work and the security threats and challenges that their use introduces. The unit is presented in two parts:

Data Communications:

- Starting with an explanation of how data is packaged on physical media, such as on copper or optical cables, we follow with an explanation of how errors are introduced and how they can be both detected and corrected.
- We introduce a series of increasingly reliable and efficient network protocols which provide guaranteed, reliable message delivery on error-prone network connections.
- We next introduce local-area Ethernet, wireless, and mobile networks, and examine the security implications of the use of shared-media networks.
- We next examine the subject of routing protocols which enable messages to be both correctly and efficiently delivered between computers not directly connected.

Internetworking:

- We next examine the motivation for and design of the Internet, and its most frequently used protocols and applications, examining the general design of the TCP/IP protocol suite, the impact of the lack of a fundamental security model, and some common vulnerabilities and defences in using its protocols.
- We examine the basic building blocks of cryptography, followed by examples of how and where these techniques are often employed to secure network protocols and network-based applications.
- We continue with a discussion of the design and implementation of client/server applications using the Berkeley sockets API, synchronous and asynchronous I/O, iterative and concurrent servers, and partially automated approaches to developing network applications.

Unit Timeline

Showing the growth (and renaming) of related CSSE units:

Jurassic era	IT312 Computer Networks
2000	IT312 Computer Networks IT410 Internet Technologies
2002	IT312 Computer Networks IT317 Computer and Network Security IT410 Internet Technologies
2007	CITS3230 Computer Networks CITS3231 Computer and Network Security CITS7219 Mobile and Wireless Computing
2012	CITS3002 Networks and Security CITS7219 Mobile and Wireless Computing
2016	CITS3002 Networks and Security CITS4419 Mobile and Wireless Computing CITS5503 Cloud Computing CITS5506 Internet of Things
2018	CITS3002 Networks and Security CITS3004 Cybersecurity CITS4419 Mobile and Wireless Computing CITS5503 Cloud Computing CITS5506 Internet of Things
2020	CITS3002 Computer Networks CITS3004 Cybersecurity CITS4419 Mobile and Wireless Computing CITS5503 Cloud Computing CITS5506 Internet of Things

Some basic networking definitions

- **A computer network** is an *interconnected* collection of *autonomous* computers.
- Computers are **interconnected** if they are capable of exchanging information. The connections can be over copper wire, radio frequencies, optical fibre, infra-red, satellite, microwaves, or a sequence of these.
- Computers are **autonomous** if there is not a permanent master/slave relationship between them. Hence, a mainframe computer and its traditional peripherals do not constitute a computer network, but a desktop computer able to interogate a more modern printer does.

Physically, a network is the computers and physical media connecting them.

Logically (and more interesting and relevant, here), a network is the software which connects and secures the computers their data, and services.

This unit focuses on computer networking software and its support by operating systems and programming languages.

Why do users value computer networks?

- Users can access and create **shared, distributed and replicated data**; e.g. the WWW, e-Commerce, B2B, airline reservation systems, from a variety of locations, including mobile and wireless services.
- Users can have their own (limited) computer and access **shared** and possibly distant physical **resources** (such as a local printer, cloud-based applications and services, cloud-based backup, local NAS music server).
- Networks can provide **fault tolerance** and **load balancing** - if some hardware fails or network connectivity is intermittent, then *logical shadowing* and *delay-tolerant networking* enables data recovery and continued performance (again, cloud-based services are good examples).
- Permit **centralized** facilties and **remote collaboration** - user-administration and file-management, windowing systems, remote desktops, distributed file services with versioning, software development with continuous integration, and tasks to minimize administration of these services.

Can you add to this list?

Research interests and networking

The combination of some significant problems provides a very rich body of investigation, some deep theoretical problems, and some important research results passed on to industry.

- **Unreliable communication** - messages sent over physical media are often garbled or lost. Programming (sequential and parallel) assumes reliable communication and this must be provided. Alternatively, if we accept that errors *do* occur, can we still manage to communicate with data loss (consider Mars probes, mobile communication, satellite TV and digital telephony)?
- The support and study of **temporal and spatial decoupling** of work patterns and communities. Sociologists are interested in communication and observation at a distance.
- **Privacy and security** (they are not the same thing) - industry's desire for electronic commerce and invasive marketing have driven the fields of authentication (and anonymity?) and encryption, and governments' desire for surveillance has driven the fields of identity and communication hiding.
- **Parallel programming** - as most recently seen in Hadoop and Map/Reduce models of processing distributed, and "big-data". Unlike sequential programming, writing, modelling and imagining the execution of parallel programs is very difficult. Parallel "activities" which must be resolved in parallel programs include distributed resource sharing and deadlock detection.

Can you add to this list?

Discussion question 1

> *It's tough to make predictions, especially about the future.*
>
> *— Yogi Berra - US professional baseball catcher, manager, coach*

Make three clear predictions for network technologies, and their affect on the ways we work and live, in the near future (say, 2 years), and longer-term (say, 10 years).

Base your predictions on specific examples or current trends in networking.

For this question, and in future discussions and assessments, provide answers with technical sophistication.

Answers of the form *"things will be faster"*, or *"things will be bigger"*, or *"things will be smaller"*, or *"things will be cheaper"* are insufficient.

Similarly, try to remember *where* you find information - not just *"I read it somewhere"*.

Discussion question 2

Hypothesis: Once hardware speeds have become sufficiently fast (do you believe that that will ever happen?), hardware (and bandwidth) will become free, and we'll just be paying for services.

Are there any precedences for this hypothesis?

What current technolgies will disappear within 3 years, to be replaced by currently emerging network technologies?

The Need for Network Protocols

Definition: A computer *protocol* consists of an agreed format for messages, expressed by a *packet header*, an optional *message component*, and a *set of rules* for the exchange of messages between computers.

We see the use of protocols in Computer Science in almost every activity:

- World Wide Web servers (Microsoft's *IIS*, and The Apache Software Foundation's *apache*) communicate with Web clients/browsers such as *Firefox*, *Chrome*, and *Edge* using the Hyper Text Transfer Protocol (HTTP),
- electronic mail and news articles are delivered and exchanged using the Simple Mail Transfer Protocol (SMTP) and the Network News Transfer Protocol (NNTP),
- some operating systems (such as Linux) display their windows and graphics using the X-Windows Protocol or the impressive Virtual Network Computing (VNC) remote display system, and
- computers share their local disks using the Network File Systems (NFS), *samba/SMB*, or the Windows-NT File System (NTFS) and Resilient File System (ReFS) protocols.

Most importantly the protocol messages must -

- happen in an agreed to order,
- travel from the sender to the correct receiver, and
- contain the correct, unambiguous, data.

The ISO/OSI Reference Model

With computer networks we require *protocols* to "meet" new computers, ask for information, agree to share data, etc.

The complexity of protocols can be simplified by separating some of the functions required into different protocols, and isolating "layers of responsibility" into different protocol modules.

e.g. at the lowest level we are concerned with correctly transmitting bits (0's and 1's) of data.

At another level we may be interested in transferring files between different computers which support different data type representations.

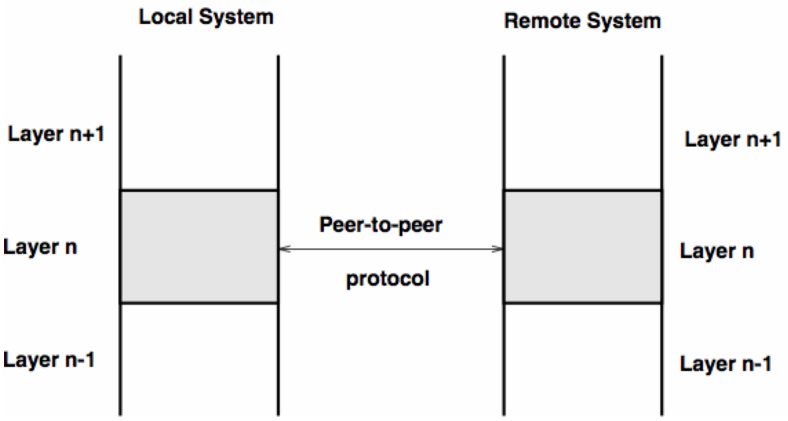
One solution to such separation of responsibilities is provided by the ISO (International Standards Organization) OSI (Open Systems Interconnection) reference model.
(This model was finally agreed upon and standardized in 1983).

Until about fifteen years ago, the OSI protocol suite was still actively sought in all tender specifications by the Australian and U.S. governments.

Today, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite meets nearly all of our networking needs. While TCP/IP employs a 4-layer model, in contrast to the 7-layer ISO/OSI model, many identical concepts may be observed.

The ISO/OSI Reference Model, *continued*

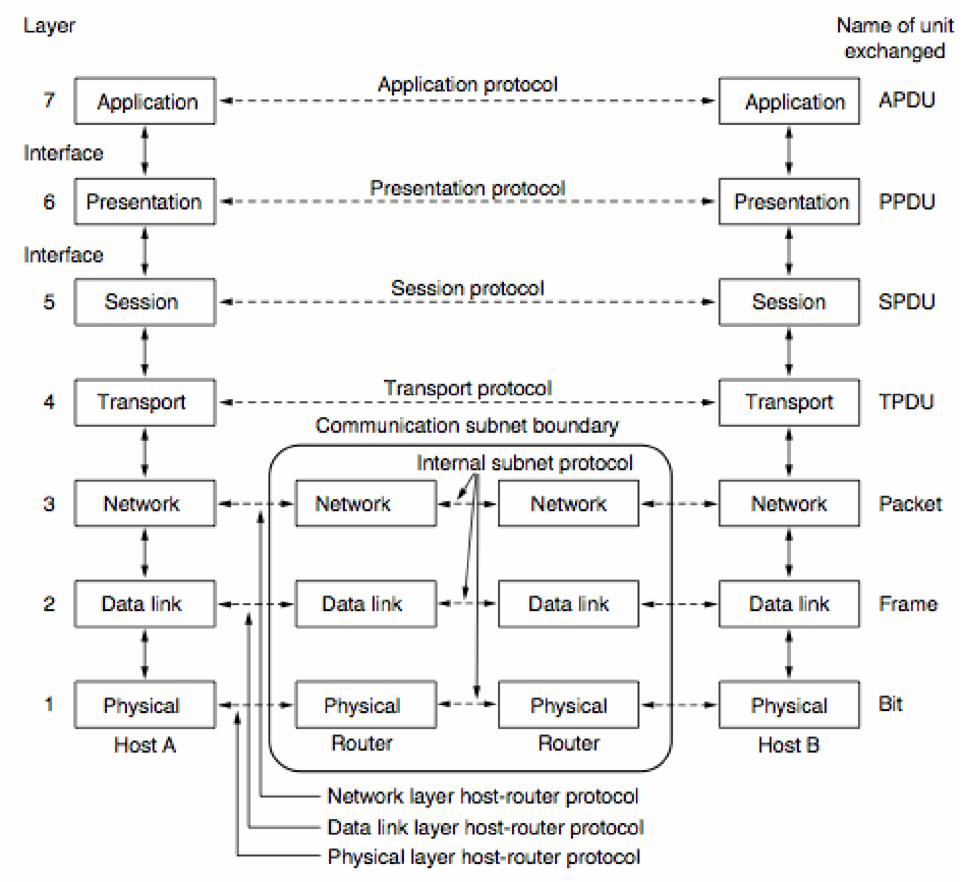
> *While [the ISO/OSI] model may or may not be a good way to organize real, live computer networks, it makes an excellent framework for organizing a book about them.*
>
> — *Andrew Tanenbaum, Computer Networks (2/e), 1988*



The deployment and acceptance of networking standards can be difficult, as evidenced by the irony of this early marketing literature:

> *IBM is the only company that's shipping end-user networking software that conforms to OSI standards. The OSI stamp is important because it assures corporate users that the networking software will easily connect to other vendors' systems and software.*
>
> — *IBM marketing literature, 1987*

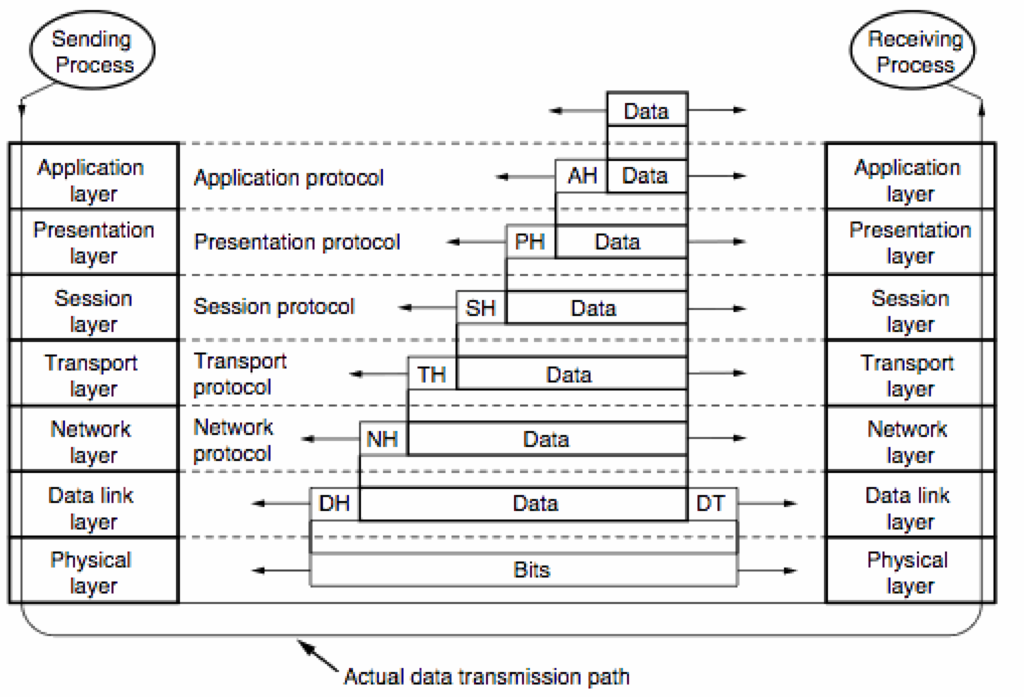
Why a Layered Model?



Why seven layers, why not 3, why not 10? The following principles were followed :

1. A layer corresponds to a different level of abstraction.
2. Each layer provides a well defined, independent function.
3. Within each layer unique protocol standards should be enforceable.
4. There should be a minimum of traffic between layers/across interfaces.
5. The number of layers should be sufficiently large that distinct functions are in different layers and that there are not too many layers for the whole model to become unmanageable.

The ISO/OSI Reference Model - layer-upon-layer

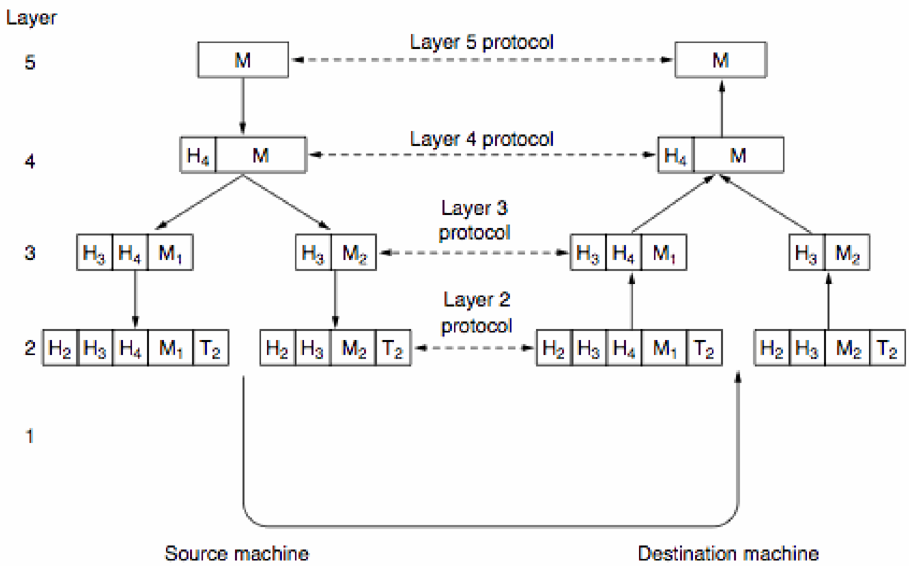


1. The Physical Layer

is responsible for transmitting a (raw) bit stream over the physical communication medium. As such it is concerned with the electrical and mechanical interface between the data and the physical medium.

The physical layer presents a bit stream to the layer above.

The ISO/OSI Reference Model, *continued*

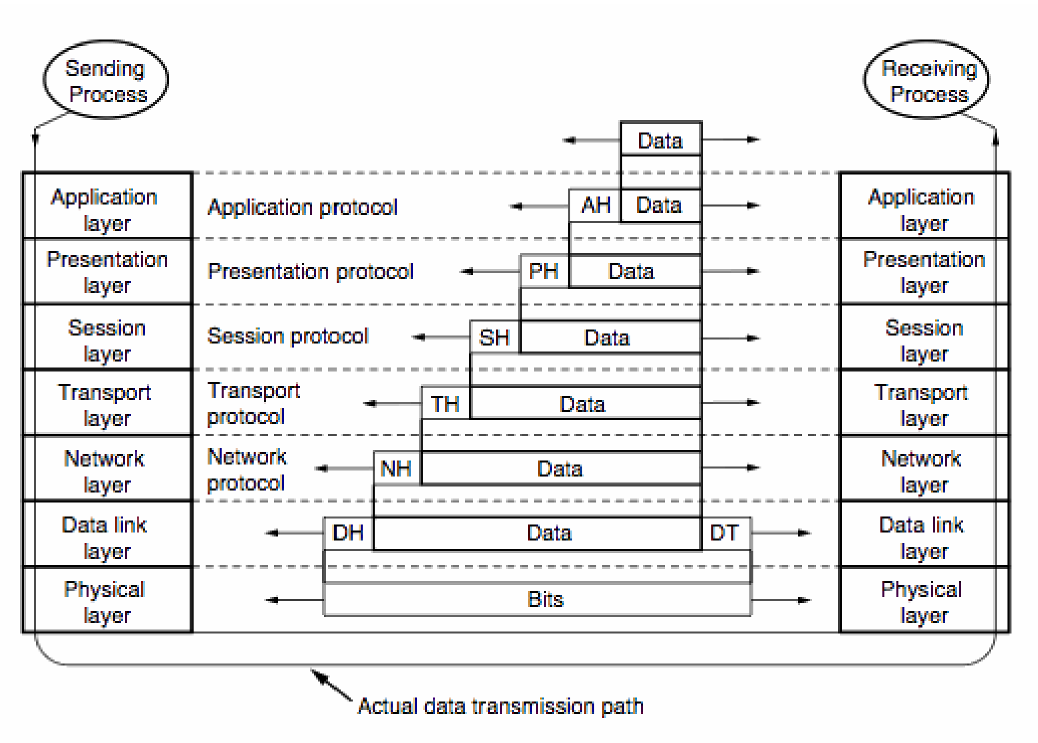


2. The Data-Link Layer

takes the bit stream from the physical layer and constructs logical chunks of data termed *frames*.

The purpose of *framing* is to ensure the reliable transmission of information by performing limited error detection and recovery.

The ISO/OSI Reference Model, *continued*



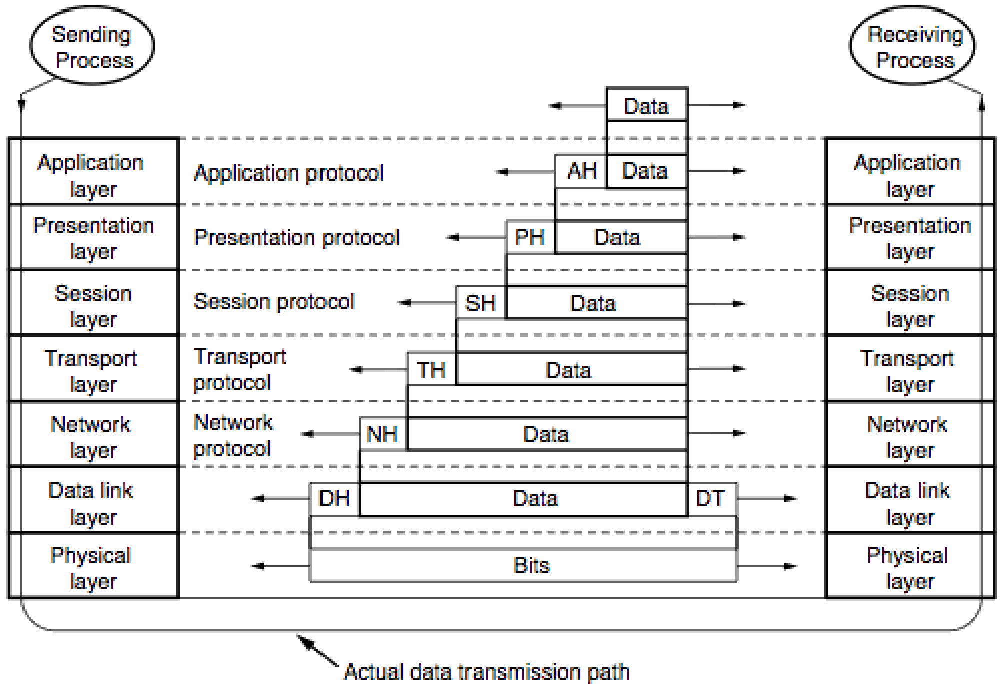
3. The Network Layer

is responsible for providing the connection between "end systems" across a network. These connections might include multiple, intermediate links and are intended to be independent of the (sub)networks used to transmit the data.

Network layer functions include:

- routing: deciding how to transmit frames between source and destination using addresses.
- relaying: enables data transfer (transparently) across intermediate (sub)networks.
- flow control: matches traffic flow with the physical capacity of a transmission path.
- sequencing: control ordering of frames across a network.

The ISO/OSI Reference Model, *continued*

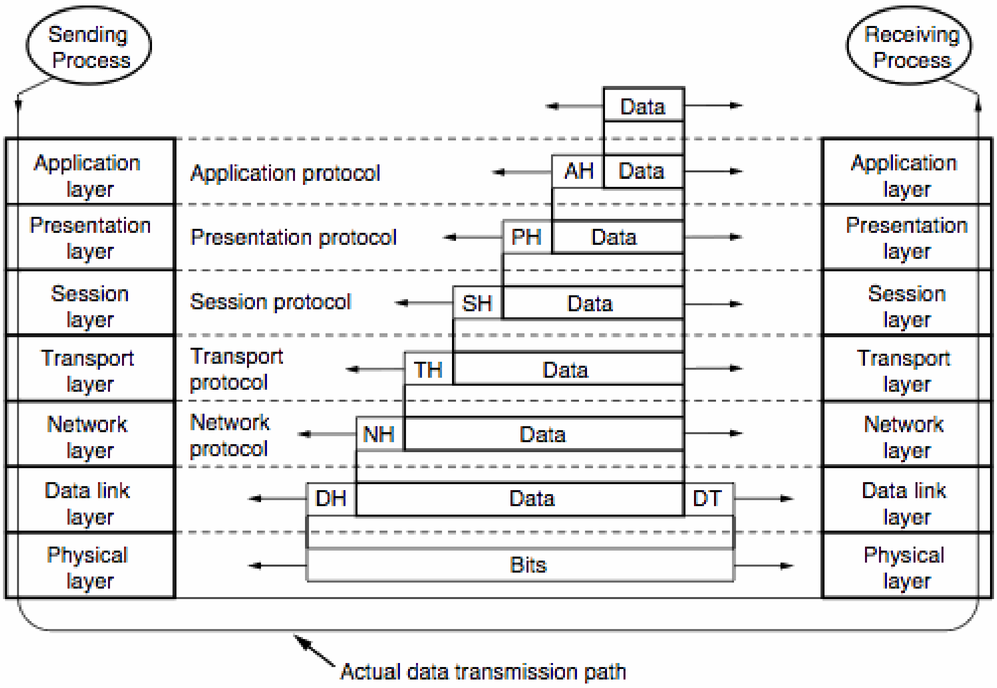


4. The Transport Layer

provides a reliable end-to-end service independent of the network topology. This is achieved by splitting messages into network sized *packets* and joining them back together again at the other end.

The transport layer often supports *multiplexing* to optimize network cost (several transport connections mapped into a single network connection) or *splitting* to enhance services (single transport to multiple connections).

The ISO/OSI Reference Model, *continued*

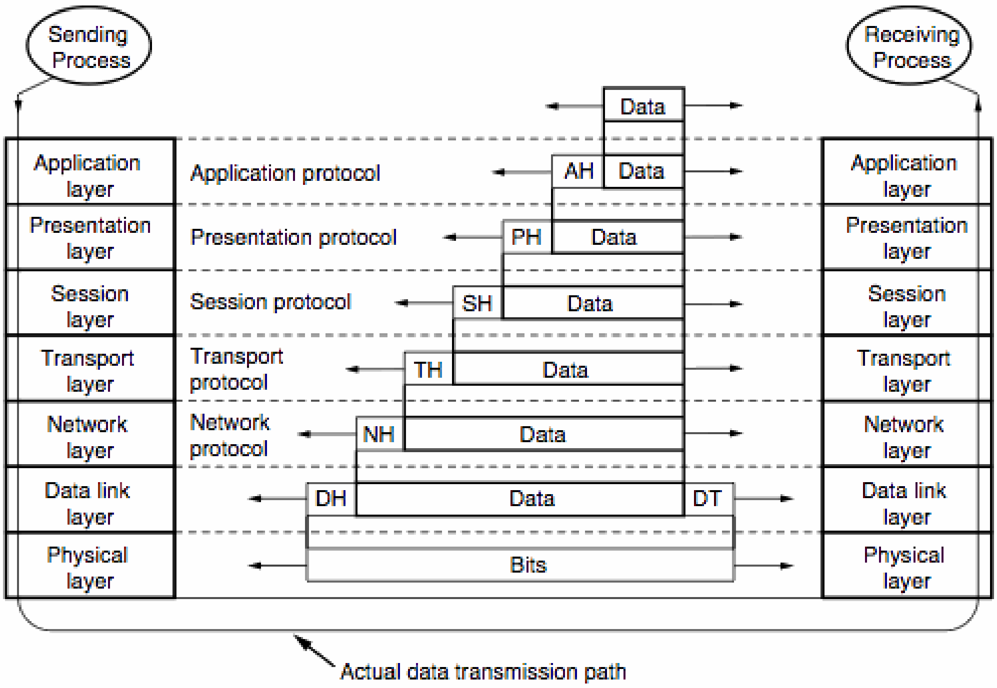


5. The Session Layer

is the first upper layer crucial to *internetworking* and manages the dialogue between end systems. Typically the session layer provides:

- establishment and closing of connections.
- synchronization to allow checking and recovery of data.
- negotiation of full and half duplex communication.

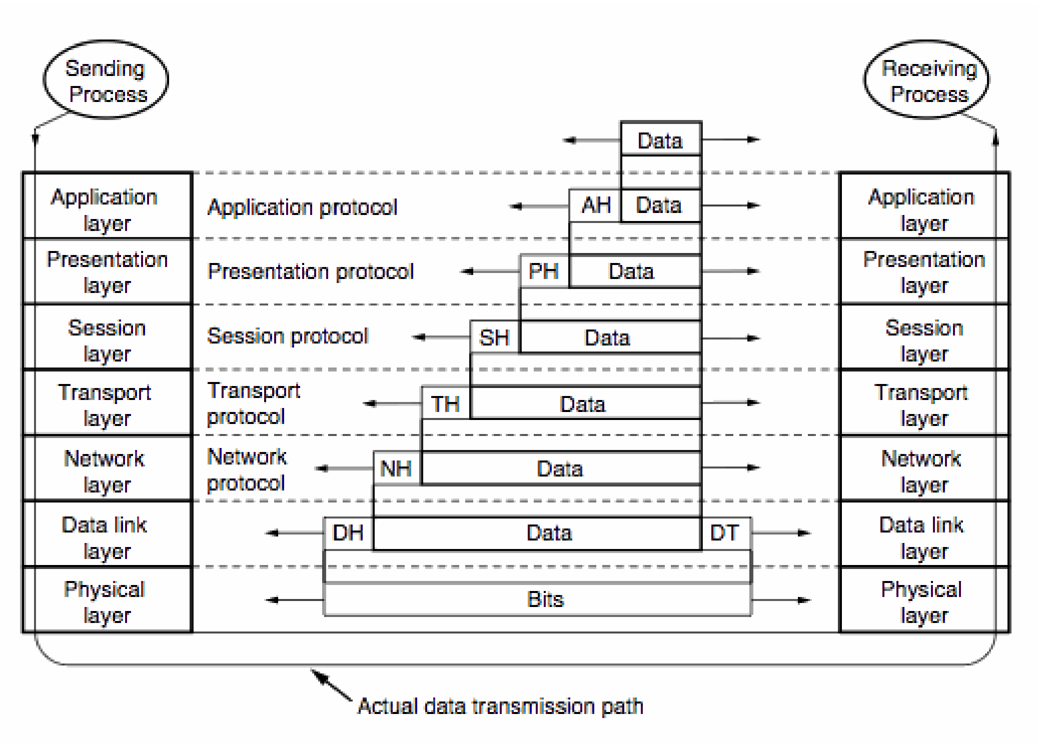
The ISO/OSI Reference Model, *continued*



6. The Presentation Layer

provides a standard format for transferred information by overcoming compatability problems between systems using dissimilar data encoding rules and (possibly) different display (input and output) technologies.

The ISO/OSI Reference Model, *continued*



7. The Application Layer

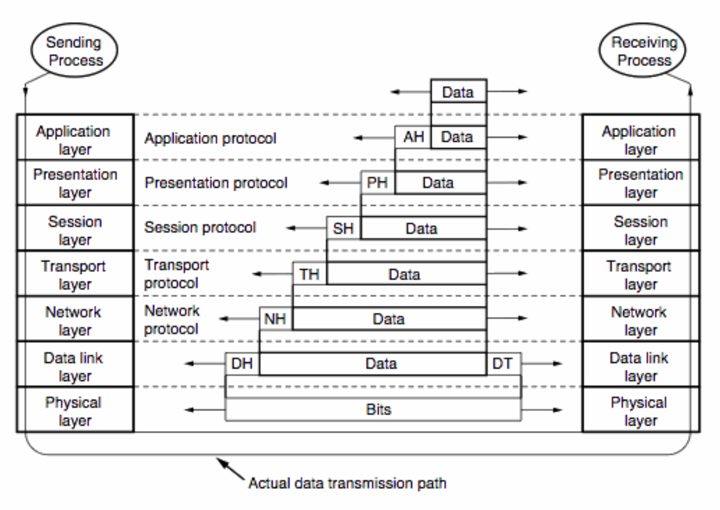
provides the interface between the application processes. In particular, functions such as file transfer, remote job execution (remote procedure calls) and application independent virtual terminal support are provided.

In overview, the application layer provides transparency to the users, load balancing between machines, data bases (banks and airline reservations), and the prospect of distributed operating systems.

Discussion question 3

On 26 March 2015 Australia's controversial Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, was passed into law by the Australian Parliament.

With reference to the ISO/OSI reference model of computer networking, data from which layers would be retained under this Bill?



Consider mobile phones as providing an obvious case-study - the information collected will include:

- who (actually, which device, a phone number or SIM card number) is calling who (another device);
- what time was the call started, and finished;
- how many bytes of data was transfered;
- BUT NOT the words of the conversation itself.

May be of interest:

- How your phone tracks your every move (ABC News).
- What reporter Will Ockenden's metadata reveals about his life (ABC News).