PRACTICAL
Radio Comms

- One of many modules from:

The Practical SCADA training suite

Ron Southworth
F. Inst. M. Sci., eEng.

SCADA PERSPECTIVE
Developing
Gap Training Capabilities

first published in paper form

March 2009

Ron Southworth
F. Inst. M. Sci., eEng.

Practical Radio Comms

Developing Gap Training Capabilities

Always Continual Improvements
First version March 2009 – most recent changes December 2020

Prepared for use as part of the turnkey training package for people seeking a SCADA Perspective

ABSTRACT

The intent of this body of work is to help address and close information knowledge and learning gaps in the field of radio frequency communications by providing practical material resources for knowledge and experiences to be better shared exchanged and applied.

EXECUTIVE SUMMARY

This manual provides practical information for those interested in the design, installation, maintenance and safe & secure operation of Radio Communications Systems.

ACKNOWLEDGEMENTS

A special thanks to Perry Pederson for suggesting the idea of the need for gap training to be developed to help centers of excellence to achieve great/greater deeds and outcomes.

The need still exists, now, more than ever there is a great divide that continues to be divisive,

science and it's application is being touted as here-say, irrelevant, unnecessary, something to be taken for granted, no longer a requisite.

The Author would like to thank many friends, peers, colleagues, & numerous vendors thought contributors from the SCADA Mail list, the that have provided practical advice, assistance, moral support, ideas, concepts and original material to turn this manual from a pipe dream into a reality.

Mostly with eternal thanks to a cobber, Ted Mulholland (OAM), Joe Ellis "The" Baron of Burnside who's Callsign I now carry forward with me as it's present custodian, Roy "Sticky Fingers" Hudson and finally Doug Rickard (all sadly "silent key").

- For your guidance, mentoring support, and stedfast friendships,

and to be considered a peer, a mate and a cobber !

Within such seemingly small deeds and actions – always it is the wee things in the life.

Hopefully from the formation of these texts and courses somehow the author hopes to make it so all the pearls of wisdom you all have shown me in the times and adventures we shared, what we learned together, may it never be truly and completely lost.

CONTENTS

FIGURES

TABLES

KEYWORDS

Communications, Radio, RF, HF, Microwave, Satellite, Analogue Radio, Digital Radio, Telemetry.

PRACTICAL RADIO COMMS

1. DEVELOPING GAP TRAINING CAPABILITIES

1.1 Introduction

These pages are gathered here as an enduring reference resource manual which ultimately form part of a comprehensive set of practical and applied research based education resources and training course materials. When consolidated it is hoped that it will enable readers to narrow or eliminate their knowledge gaps when working in, on, and around Radio Communications Systems. A general assumption has been that also the reader has attained other entry level general electronics and electrotechnical skills before attempting to understand this course material for the sake of brevity.

1.2 Background

Communications Technologies underpin the fabric of modern human society and are increasingly leveraged to achieve an outcome. Radio Communications Technologies are considered a part of Modern Information Systems Technologies. The author wants to remind readers that Information Technology (IT) and much more than what IT encompasses requires a wealth of traditional Engineering Disciplines to realise working robust solutions for people to take for granted.

Supervisory Control and Data Acquisition (SCADA) systems have been in use in various forms for well over forty years. The terms SCADA, Distributed Control Systems (DCS) Process Control Systems (PCS), Telemetry Systems and Industrial Control Systems (ICS) are often used interchangeably and can lead to a large amount of debate as to what is the best term to use to describe the particular variation of what is the same general theme. The SCADA & ICS are generally defined to include Process Control Systems (PCS), and Distributed Control Systems (DCS). Other regulatory guidance & appended documents may also mention Industrial Automation and Control Systems (IACS) all of which will be referred to generally as SCADA systems for the purposes of this series of manuals.

1.3 Audience and Scope

This resource was written in order for technically focused people to collaborate effectively and efficiently to improve the overall system resilience of Radio Communications environments. This scope includes people from areas such as operations, plant managers, process, electrical engineers, network administrators, electrical and instrumentation technicians, security professionals & reverse engineering skilled people, to other professionals working (or playing) in other associated disciplines of science. Such a team may be small in some organizations, with those involved having varied responsibilities, or it may include a large group of specialists whose only job is to focus on a certain aspect of the system or enterprise.

1.4 A High level definition of a SCADA system

A Supervisory Control and DATA Acquisition (SCADA) system is:

A combination and configuration of technologies comprising of Computers (microprocessor based logic resolvers and human machine interfaces), Programmable Logical Controllers (PLC's /RTU's embedded field distributed microprocessors), structured communications devices and medium, instrumentation (sensors), final control elements, valves, relays, contacts pumps, motors transformers etc.

Collectively this technology directly (or indirectly) act or react upon the process material being manipulated, such that the outcome of the manipulation provides a delivered product or products to a known quality and standard in order to consistently and reliably meet the expectations of a consumer.

1.5 What is a SCADA system comprised of

The term SCADA by its definition implies that there are two activities are necessary:

1. The acquisition of data and subsequent transfer to some location (or group of locations); and
2. The control of some process or equipment from these locations.

There are essentially four components to a SCADA system:

1. A site which is the controlling station for the entire system, providing an operator interface or Human Machine Interface (HMI) for display of information and control of remote sites. The master station (or stations) which gather data from the various sites and which can also act as an operator control interface or agent for display of information and control of remote sites or Outstations;
2. The communications system which provides the pathway or medium for communications between the master station and the remote sites;
3. The RTU (PLC or IED) which provides an interface to the field equipment situated at each remote site; and
4. The measurement and control interface equipment. These are the devices which measure and control the processes, usually directly acting with the process medium.

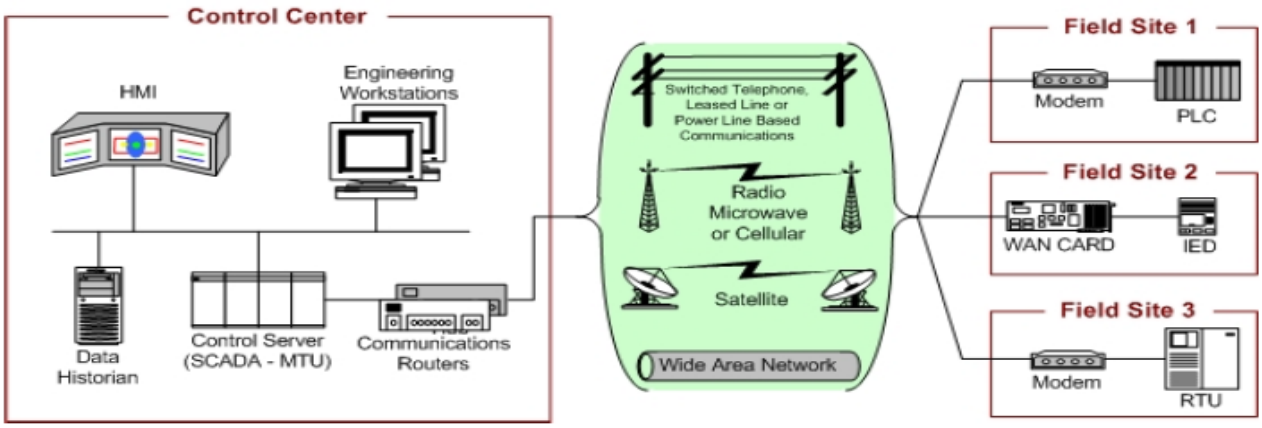

Figure 1. Technologies that make up a SCADA system (from NIST SP800-82)

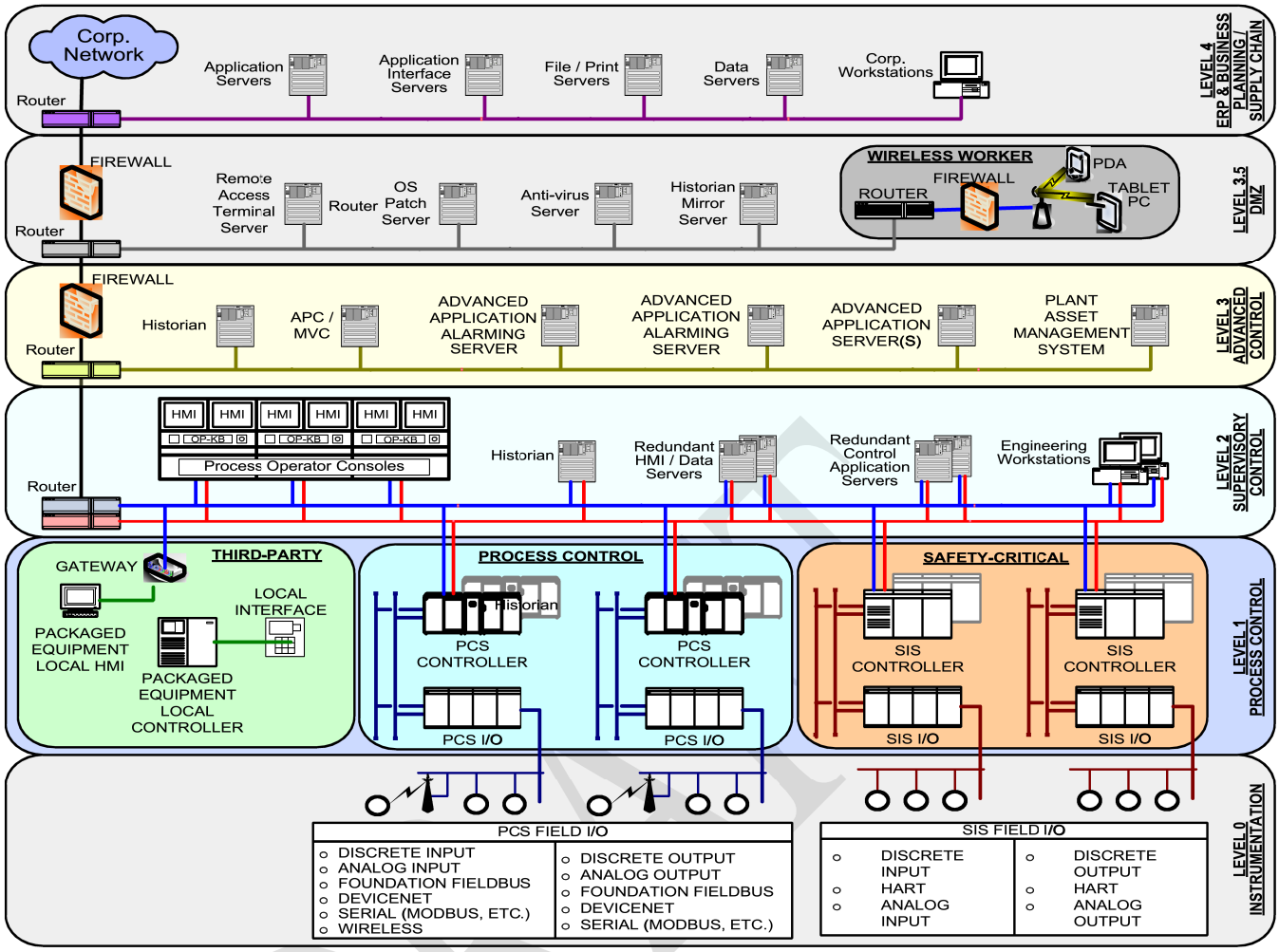

Figure 2 The SCADA System by function (From ISA SP99)

This manual will begin the journey by looking at communications, the "stuff" that glue's all the different elements of the system together. The representation of a SCADA system depicted below in Figure 3 you will see highlighted, the plant and outstation layer. We will build upon this information as we develop or revisit our knowledge base, as the case may be, using the information contained in this training material.

At the heart of this material is the need for us to leverage upon each others experiences utilising this resource to grow our knowledge together collaboratively as we continue on our exploration of this collective technology toward the board room.

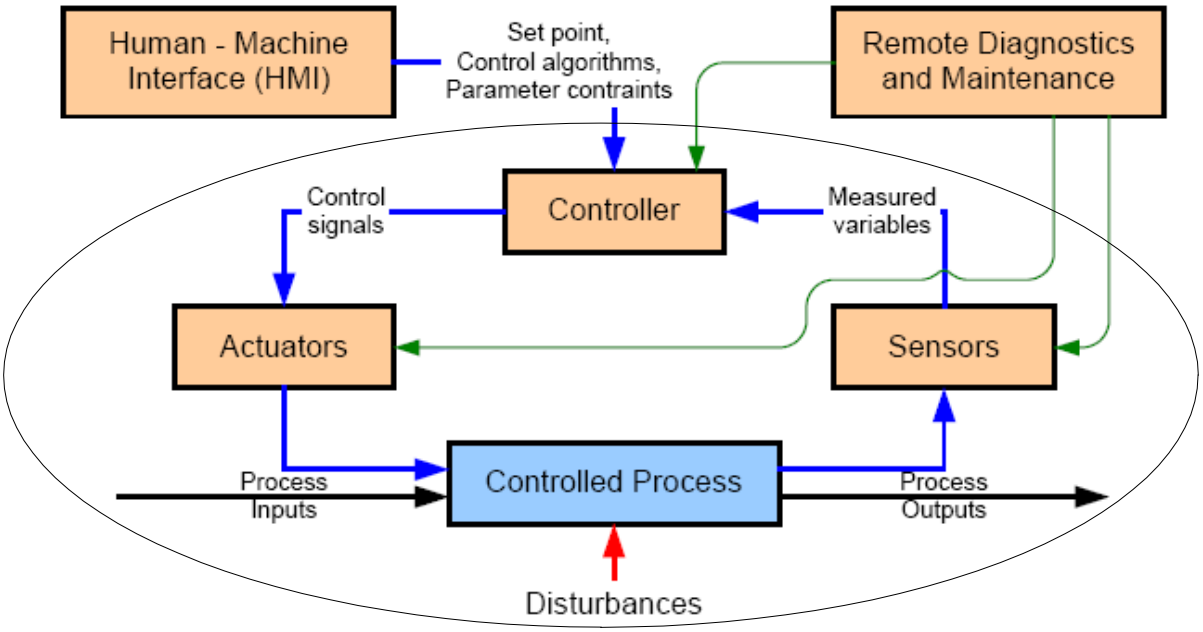

Figure 3 Process interfacing equipment (from SP800-82)

Technical Communications

2. THE COMMUNICATIONS PROCESS

(Transmitters, receivers and communication channels)

A communications process requires the following components for successful communication:

1. A source of the information;
2. A transmitter to convert the information into data signals compatible with the communications channel;
3. A communications channel;
4. A receiver to convert the data signals back into a form the destination can understand; and
5. The destination of the information.

Figure 4 below, shows the communications process.

Figure 4. The Communications Process

Encoding is the process of converting data to code, and decoding is the process of converting code back to data. The codes that represent the data can exist in many different forms.

The transmitter encodes the information into a suitable form to be transmitted over the communications channel. The communications channel moves this signal as electro-magnetic energy from the source to one or more destination receivers. The channel may convert this energy from one form to another, such as electrical to optical signals, while maintaining the integrity of the information so that the recipient can understand the message sent by the transmitter.

For the communications to be successful, the source and destination must use a mutually agreed method of conveying the data. The main factors that must be considered are:

1. The form of signalling and the magnitude(s) of the signals to be used;
2. The type of communications link (twisted pair, coaxial, optic Fiber, radio etc.);
3. The arrangement of signals to form character codes from which the message can be constructed;
4. The methods of controlling the flow of data; and
5. The procedures for detecting and correcting errors in the transmission.

The form of physical connections is defined by interface standards**.** Some agreed coding is applied to the message and the rules controlling the data flow and detection and correction of errors are known as protocol.

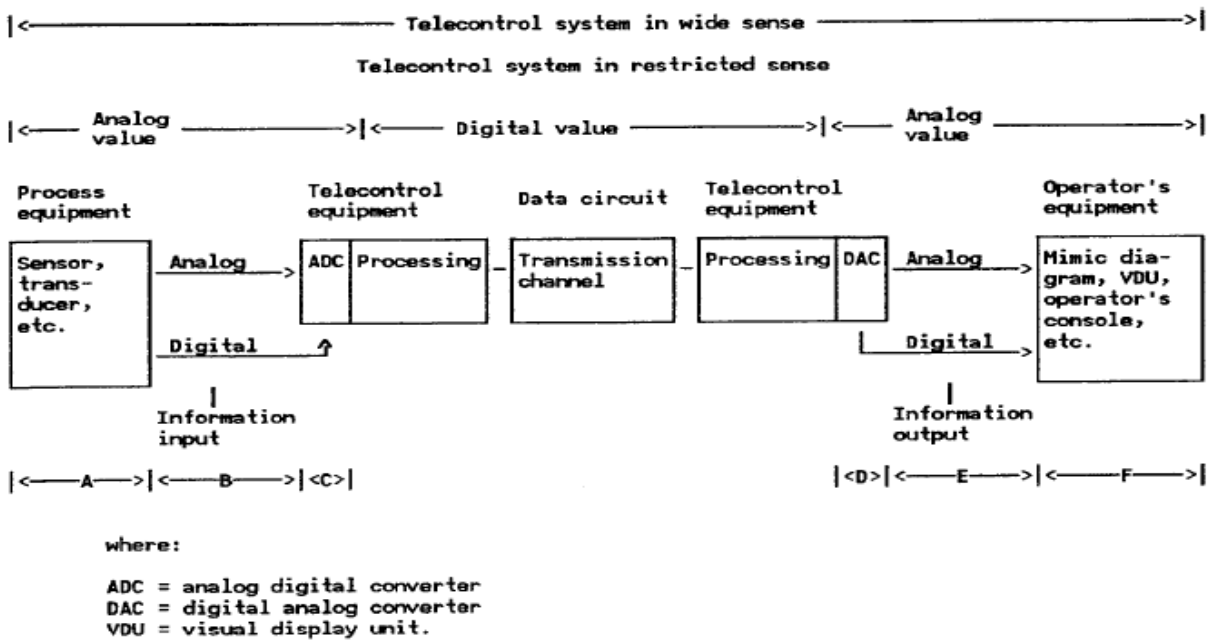

Figure 5. IEC AS16850 description of a SCADA System

2.1 ISO 7 LAYER MODEL

A framework that has had a tremendous impact on the design of communications systems is the Open Systems Interconnection (OSI) model developed by the International Standards Organization (ISO). The objective of the model is to provide a foundation for the coordination of standards development that allows both existing and evolving standards activities to be set within that common understanding.

The interconnection of two or more devices with digital communication is the first step towards establishing a network. In addition to the hardware requirements, the software problems of communication must also be overcome. Where all the devices on a network are from the same manufacturer, the hardware and software problems are usually easily solved because the system is usually designed within the same guidelines and specifications.

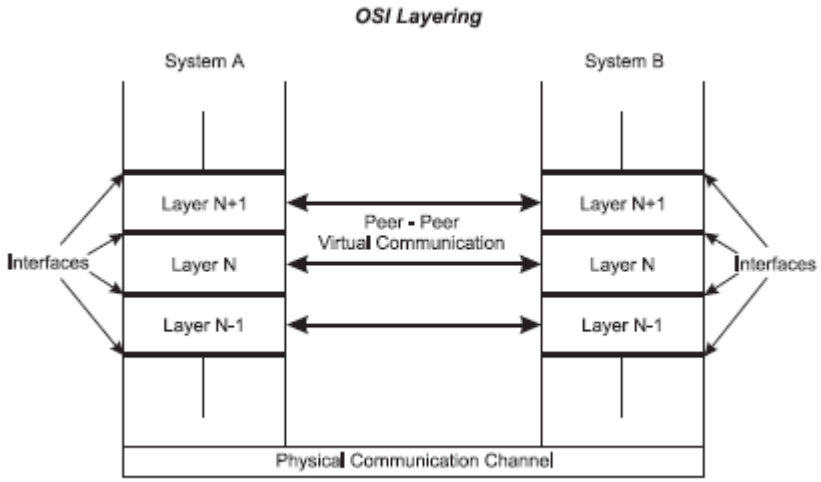

Figure 6. OSI Layering

Open Systems are those that conform to specifications and guidelines which are "open" to all. This allows equipment from any manufacturer, who complies with that standard, to be used interchangeably on the network. The benefits of Open Systems include multiple vendors and hence wider availability of equipment, lower prices and easier integration with other components.

In 1978 the ISO, faced with the proliferation of closed systems, defined a "Reference Model for Communication between Open Systems" (ISO 7498), which has become known as the Open Systems Interconnection model, or simply as the OSI model. OSI is essentially a data communications management structure, which breaks data communications down into a manageable hierarchy of seven layers.

Each layer has a defined purpose and interfaces with the layers above it and below it. By laying down standards for each layer, some flexibility is allowed so that the system designers can develop protocols for each layer independent of each other. By conforming to the OSI standards, a system is able to communicate with any other compliant system, anywhere in the world.

It should be realized at the outset that the OSI Reference Model is not a protocol or set of rules for how a protocol should be written but rather an overall framework in which to define protocols. The OSI Model framework specifically and clearly defines the functions or services that have to be provided at each of the seven layers (or levels).

The diagram below shows the seven layers of the OSI Model.

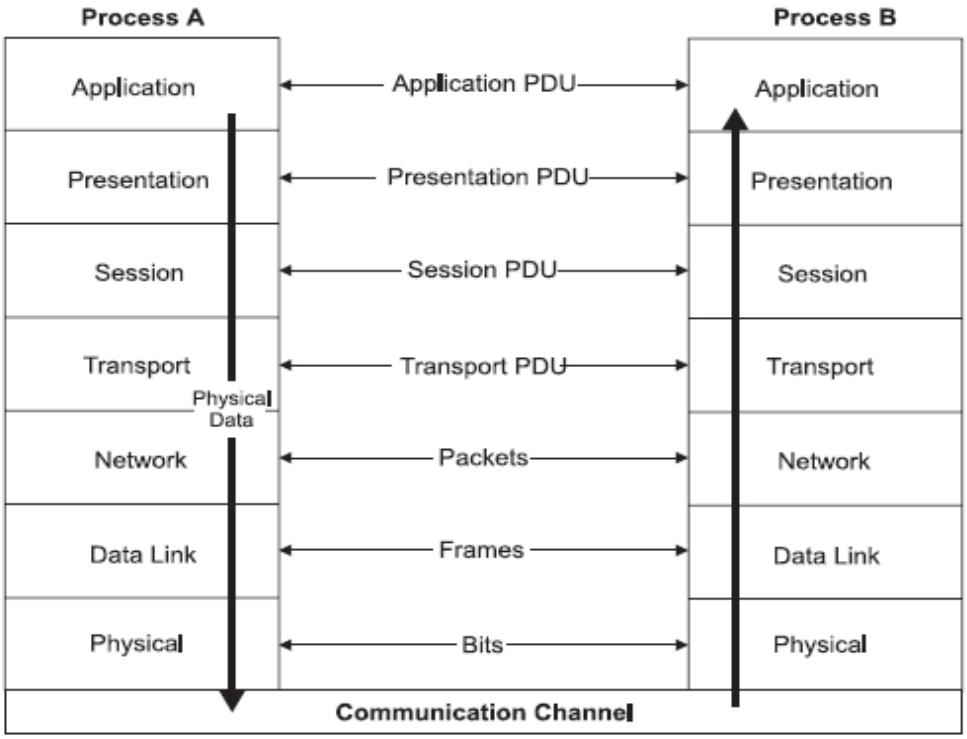

Figure 7. ISO 7 Layer Model

The seven layers are summarised below:

7 The **Application Layer**
The provision of network services to the user's application programs.
Actual application programs do NOT reside here

6 The **Presentation Layer**
Primarily takes care of data representation (including encryption)

5 The **Session Layer**
Control of the communications (sessions) between the users

4 The **Transport Layer**
The management of the communications between the two end systems

3 The **Network Layer**
Primarily responsible for the routing of messages

2 The **Data Link Layer**
Responsible for assembling and sending a frame of data from one system to another

1 The **Physical Layer**
Defines the electrical signals and mechanical connections at the physical level. The figure below gives an idea on how transmission of a message is effected by each layer being encapsulated within the layer below it, before it is sent out on the physical data highway. Similarly once the packet (or more strictly speaking - the frame) is received each layer is then stripped off as the packet is pushed to the top where the message is then extracted.

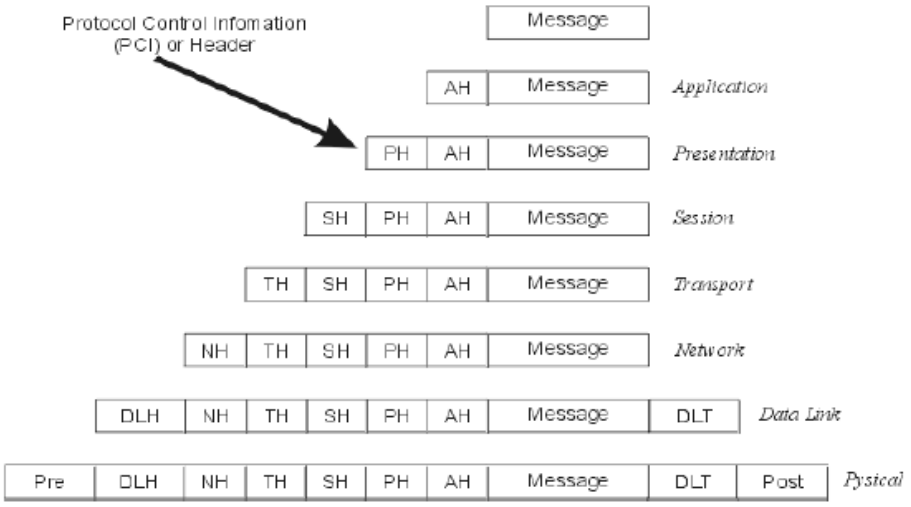

Figure 8. The protocol information header

2.1.1 The open systems interconnection model

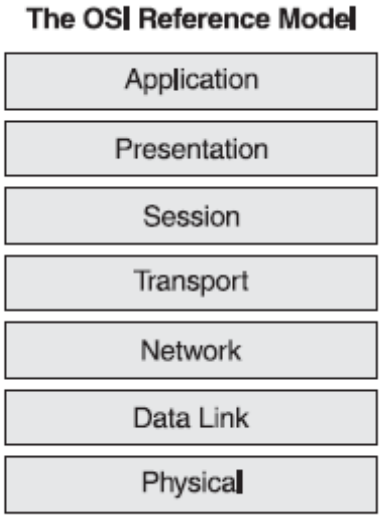

Figure 9. The OSI Reference Model

Typically, each layer on the transmitting side adds header information, or protocol control information (PCI), to the data before passing it on to the next lower layer. In some cases, especially at the lowest level, a trailer may also be added.

At each level, this combined data and header 'packet' is termed a protocol data unit or PDU. The headers are used to establish the peer-to-peer sessions across the sites and some layer implementations use the headers to invoke functions and services at the layers adjacent to the destination layer.
At the receiving site, the opposite occurs with the headers being stripped from the data as it is passed up through the layers. These header and control messages invoke services and a peer-to-peer logical interaction of entities across the sites.

Generally, layers in the same site (i.e. within the same host) communicate in software with parameters passed through primitives, whilst peer layers at different sites communicate with the use of the protocol control information, or headers.
At this stage, it should be quite clear that there is NO connection or direct communication between the peer layers of the network. Rather, all physical communication is across the physical layer, or the lowest layer of the stack. Communication is down through the protocol stack on the transmitting stack and up through the stack on the receiving stack. As will be realised, the net effect of this extra information is to reduce the overall bandwidth of the communications channel, since some of the available bandwidth is used to pass control information.

2.1.2 Application layer

The application layer is the topmost layer in the OSI reference model. This layer is responsible for giving applications access to the network. Examples of application-layer tasks include file transfer, electronic mail (e-mail) services, and network management. Application- layer services are much more varied than the services in lower layers, because the entire range of application possibilities is available here. Application programs can get access to the application-layer services in software through application service elements (ASEs).

There are a variety of such application service elements; each designed for a class of tasks. To accomplish its tasks, the application layer passes program requests and data to the presentation layer, which is responsible for encoding the application layer's data in the appropriate form.

2.1.3 Presentation layer

The presentation layer is responsible for presenting information in a manner suitable for the applications or users dealing with the information. Functions such as data conversion from EBCDIC to ASCII (or vice versa), use of special graphics or character sets, data compression or expansion, and data encryption or decryption are carried out at this layer. The presentation layer provides services for the application layer above it, and uses the session layer below it. In practice, the presentation layer rarely appears in pure form, and it is the least well defined of the OSI layers. Application- or session-layer programs will often encompass some or all of the presentation layer functions.

2.1.4 Session layer

The session layer is responsible for synchronising and sequencing the dialogue and packets in a network connection. This layer is also responsible for making sure that the connection is maintained until the transmission is complete, and ensuring that appropriate security measures are taken during a 'session' (that is, a connection).The session layer is used by the presentation layer above it, and uses the transport layer below it.

2.1.5 Transport layer

In the OSI reference model, the transport layer is responsible for providing data transfer at an agreed-upon level of quality, such as at specified transmission speeds and error rates. To ensure delivery, outgoing packets are sometimes assigned numbers in sequence. These numbers are then included in the packets that are transmitted by lower layers. The transport layer at the receiving end subsequently checks the packet numbers to make sure all have been delivered and to put the packet contents into the proper sequence for the recipient. The transport layer provides services for the session layer above it, and uses the network layer below it to find a route between source and destination. The transport layer is crucial in many ways, because it sits between the upper layers (which are strongly application-dependent) and the lower ones (which are network-based).

The layers below the transport layer are collectively known as the 'subnet' layers. Depending on how well (or not) they perform their function, the transport layer has to interfere less (or more) in order to maintain a reliable connection.

Three types of subnet service (i.e. the service supplied by the underlying physical network between two hosts) are distinguished in the OSI model as:

1. Type A: Very reliable, connection-oriented service
2. Type B: Unreliable, connection-oriented service
3. Type C: Unreliable, possibly connectionless service

To provide the capabilities required for the above service types, several classes of transport layer protocols have been defined in the OSI model:

TP0 (transfer protocol class 0), which is the simplest protocol. It assumes type A service; that is, a subnet that does most of the work for the transport layer. Because the subnet is reliable, TP0 requires neither error detection or error correction. Because the connection is connection-oriented, packets do not need to be numbered before transmission

TP1 (transfer protocol class 1), which assumes a type B subnet; that is, one that may be unreliable. To deal with this, TP1 provides its own error detection, along with facilities for getting the sender to retransmit any erroneous packets

TP2 (transfer protocol class 2), which also assumes a type A subnet. However, TP2 can multiplex transmissions, so that multiple transport connections can be sustained over the single network connection

TP3 (transfer protocol class 3), which also assumes a type B subnet. TP3 can also multiplex transmissions, so that this protocol has the capabilities of TP1 and TP2

TP4 (transfer protocol class 4), which is the most powerful protocol, in that it makes minimal assumptions about the capabilities or reliability of the subnet. TP4 is the only one of the OSI transport-layer protocols that supports connectionless service

2.1.6 Network layer

The network layer is the third lowest layer, or the uppermost subnet layer. It is responsible for the following tasks:

Determining addresses or translating from hardware to network addresses.
These addresses may be on a local network or they may refer to networks located elsewhere on an internetwork. One of the functions of the network layer is, in fact, to provide capabilities needed to communicate on an internetwork

Finding a route between a source and a destination node or between two intermediate devices
Fragmentation of large packets of data into frames which are small enough to be transmitted by the underlying data link layer (fragmentation). The corresponding network layer at the receiving node undertakes re-assembly of the packet.