ISO Reference Model for Open Systems Interconnection (OSI)

In this report:

Note: This report explains the OSI Seven-Layer Reference Model at all layers; compares OSI to other architectures; rationalizes the need for standards testing and verification; examines the case for OSI; profiles major testing organizations; and outlines OSI Management standards and status.

Datapro Summary

The goal of Open Systems Interconnection (OSI) was designed to enable dissimilar computers in multivendor environments to share information transparently. The OSI structure calls for cooperation among systems of different manufacture and design. There are seven layers of the OSI model that communicate between one end system and another. The layers cover nearly all aspects of information flow, from applications-related services provided at the Application Layer to the physical connection of devices to the communications medium at the Physical Layer. All seven layers have long since been defined and ISO protocols ratified for each layer, though extensions have been made occasionally. Although the model has changed the way we look at networking, the dream of complete OSI-compliance has not come to fruition. The causes are varied, but this is essentially because OSI protocols are too expensive and too complex compared with other protocols that have become *de facto* standards in their own right. Even so, it is important to understand the model because, although the complete stack of protocols is not much used today, the model has formed the way we think of the structure of networks, and the model itself is always referred to in internetworking matters.

Analysis

The proliferation of computerized data processing systems in the late 1960s produced a need for compatible data communications networks in the 1970s. Several proprietary network architectures were developed for mainframe-to-terminal communications, including IBM's SNA in 1974. Although many of these proprietary architectures were based on a layered model, none was compatible with any other. The CCITT's X.25 host interface to the packet networks standard was ratified in 1976 but this is not a complete network architecture. In 1977 the International Organization for Standardization (ISO) formed ISO Technical Committee 97 (TC97), Subcommittee 16 (SC16), to embark on a worldwide standardization effort and confront the issue of incompatibility head-on. The purpose of TC97/SC16 was to develop a model and define the protocols and interfaces required to support an *open system*. The goal of OSI was, and still is, to enable dissimilar computers in multivendor environments to share information transparently. With this capability, it was thought that global digital networks could become a reality. As we shall see, however, much of the OSI goal has in fact come about through widespread use of *de facto* protocols such as TCP/IP and from multivendor initiatives formed to ensure interoperability such as the ATM Forum, a standards-setting body in its own right.

—By Marina Smith
Senior Analyst
email: smithma@mcgraw-hill.com

The Open System

The ISO defines a *system* as a set of one or more computers and associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., which form an autonomous whole capable of performing information processing and/or information transfer. An *open system* is one that obeys OSI standards in its communication with other systems.

An *application process* is an element within a system that performs information processing for a particular application. The application process can be manual (a person operating a banking terminal), computerized (a program executing in a computer center and accessing a remote database), or physical (a process control program executing in a dedicated computer attached to industrial equipment and linked to a plant control system).

The OSI structure calls for cooperation among systems of different manufacture and design. This includes coordinating activities such as the following:

- Interprocess communications—the synchronization between OSI application processes and the exchange of information
- Data representation—the creation and maintenance of data descriptions and transformations for reformatting data exchanged between systems
- Data storage—storage media, file systems, and database systems for providing access to and management of stored data
- Process and resource management—how application processes are declared, initiated, controlled, and acquired
- Integrity and security—information processing constraints that must be ensured during open systems operations
- Program support—the definition, compilation, testing, linking, storage, and transfer of and access to programs executed by the application processes

The OSI model is concerned only with the exchange of information between open systems.

The Layering Concept

Layering is a basic structuring technique used in the OSI model. Each layer is composed of an ordered set of subsystems, with logically related functions grouped together. The OSI model breaks down internetworking activities between systems into two distinct groups. Communications-oriented functions are separated from user-oriented functions; features which move information across a network are distinct from features which handle and format information.

There are seven layers of the OSI model that communicate between one end system and another end system. The layers cover nearly all aspects of information flow, from applications-related services provided at the Application Layer to the connection of devices to the communications medium at the Physical Layer. Below the Physical Layer, the media itself corresponding to "Layer 0"—such as wire, cable, or through-the-air communication—is not addressed by the model. Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers have been defined (see *Table* "The Seven Layers of OSI"). The table describes the OSI model's seven layers and their purposes. In the model, information flows down from Layer 7 to Layer 1, and then out over a physical transmission medium. At the receiving end, the information flows into another end system and up from Layer 1 to Layer 7, until it is received by a user.

The seven layers can be divided into two functional groups: the Transport Platform (Layers 1 to 4) and the Application Platform (Layers 5 to 7). The Transport Platform's function is to get data from one system to another without errors. The Application Platform's function is to interpret the data stream and present it to the user in a usable form (see Figure *"Application and Transport Division"*).

Each layer contributes functions to the communications task. For example, the Link Layer enables communications across a single physical connection, while the Network Layer provides end-to-end routing and data relay. Services at the upper-layer interface—providing communications to the next-higher layer—are provided by each layer, usually described by a service specification for the layer. Services at each layer are provided by a layer entity. Each layer entity communicates with its peer at the same layer on another system, providing services specified in the service specification.

The Seven Layers of OSI

Layer	Name	Purpose
7	Application	Applications and application interfaces for OSI networks. Provides access to lower-layer functions and services.
6	Presentation	Negotiates syntactic representation for the Presentation Layer and performs data transformations.
5	Session	Coordinates connection and interaction between applications. Establishes a dialog, manages and synchronizes the direction of data flow.
4	Transport	Ensures end-to-end data transfer between applications, data integrity, and service quality. Assembles data packets for routing by Layer 3.
3	Network	Routes and relays data units among network nodes.
2	Data Link	Transfers data units from one network node to another over a transmission circuit. Ensures data integrity between nodes.
1	Physical	Delimits and encodes the bits onto the physical medium.

Standards Organizations

Several standards testing and verification bodies have been organized by vendor consortiums, government agencies, and independent organizations. They have found that developing conformance specifications, producing testing suites, and conducting comprehensive testing are complicated, expensive, and time consuming. Regional differences can stymie attempts at verification. The trend for these organizations, therefore, is to cooperate with each other, sharing resources and expertise. A primary objective is demonstrating interoperability among different vendors; i.e., proving that standards really work and fostering end-user interest. Many agencies have tried vainly to involve more end users but are backed primarily by the vendors.

ANSI (American National Standards Institute)

ANSI
11 W.42nd Street
New York NY 10036, U.S.A.
Tel: +1 212 642 4900
Fax: +1 212 398 0023
http://www.ansi.org

ATM Forum

World Headquarters
2570 West El Camino Real
Suite 304
Mountain View, CA 94040-1313, U.S.A.
Phone: +1 415 949 6700
Fax: +1 415 949 6705
http://www.atmforum.com

European Office
Boulevard Saint-Michel 78
1040 Brussels, BELGIUM
Phone: +32 2 732 8505
Fax: +32 2 732 8485
Asia-Pacific Office
Hamamatsucho Suzuki Bldg. 3F
1-2-11 Hamamatsucho, Minato-ku
Tokyo 105, JAPAN
Phone: +81 3 3438 3694
Fax: +81 3 3438 3698

IEEE (The Institute Of Electrical And Electronics Engineers)

The Institute Of Electrical And Electronics Engineers, Inc.
1828 L Street NW, Suite 1202
Washington DC 20036-5104, U.S.A.
Tel: +1 908 981 0060
Fax: +1 908 981 0027
http://www.ieee.org

IEEE Corporate Office
345 E. 47th Street
New York, NY, 10017, U.S.A.
Tel: +1 212 705 7900

IEEE Operations Center
445 Hoes Lane
Piscataway, NJ, 08855-1331, U.S.A.
Tel: +1 908 981 0060

IEEE European Operations Center (Brussels)
Tel: +32 2 770 2242
Fax: 32 2 770 8505
E-mail: memservice-europe@ieee.org

ISO (International Organization for Standardization)

ISO Central Secretariat
1, rue de Varembe
Case Postale 56
CH-1211 Geneva 20
Switzerland
Tel: + 41 22 749 01 11
Fax: + 41 22 733 34 30
E-mail:
INTERNET: central@iso.ch
X.400: c=ch; a=400net; p=iso; o=isocs; s=central
http://www.iso.ch

Please note: Copies of ISO standards can be ordered from local standards offices.

ITU (International Telecommunications Union)

Place des Nations
CH - 1211 Geneva 20
Switzerland
Tel: +41 22 730 51 11
Fax (Group 3): +41 22 733 7256
Fax: (Group 4): +41 22 730 6500
http://www.itu.ch

European Computer Manufacturers Association (ECMA)

Rue du Rhone 114
CH-1204 Geneva, Switzerland
Tel: +41 22 849 6000
Fax: +41 22 849 6001
Telex: 413237 ECMA CH
http://www.ecma.ch

Electronic Industries Association (EIA)

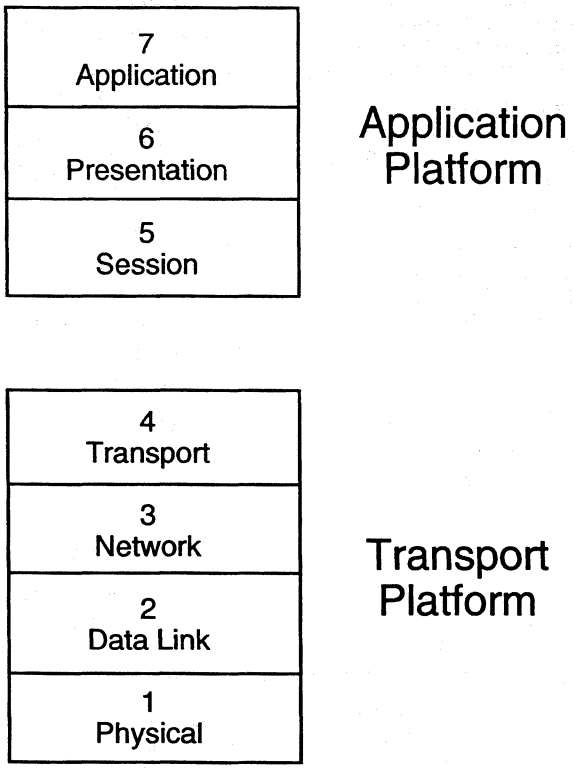
Electronic Industries Association
2500 Wilson Boulevard
Arlington, VA 22201-3834
Tel: +1 703 907 7500
Fax: +1 703 907 7501
http://www.eia.org

IBM's SNA is also a layered architecture, following rules of layering similar to OSI and other layered architectures. There are good reasons for layering: layering simplifies change; components inside a layer can be changed without affecting any other layers in that node. Layers are like structured programming—but for teleprocessing systems. Because there are rigid interfaces between levels, fewer people need to react to changes, allowing them to be implemented faster. There is no better way of achieving complex functions. Layering allows each network function to be made "transparent," unaware and independent of other functions at other layers, thus enabling any layer to be modified without changing the entire monolithic architecture.

Each layer may support one of several different protocols designed for specific network applications; the choice of a specific protocol is optional, allowing users to tailor networks to their own design. Each layer defines functions crucial to the communications process at that layer, independent of the other layers. However, a layer may perform functions hinging on functions performed in the layers immediately above or below. A layer can only communicate with another device or network node at its peer layer. Messages exchanged between peer layers are "enveloped" with messages from other layers and passed through these other layers on the way to their destination, picking up and then shedding these other protocol layers along the way. For example, if layer seven at one end system must send a message to layer seven at another, it must travel down through six layers at its own end and then up through six layers at the other, until it reaches layer seven at its opposite (peer) layer.

Each network node (a network user, computer, terminal) is equipped with this layer mechanism. However, not all intermediate nodes need all seven layers. Network nodes, in particular, must only route and transmit data packets—functions at the bottom three layers of the OSI model. Layer 4 through 7 functions are not required and, therefore, not included in network node software. Data packets processed in these nodes reach only Layer 3 and are then routed elsewhere (see Figure *"Message Movement Among OSI Layers"*). A node communicates with its peer in another node sending or receiving data. Data transfer is routed from Layer 7 down to Layer 1 at the transmitting node, then along the network to Layer 1 at the receiving node, and finally from Layer 1 up to Layer 7. Peer layers communicate by the same method.

Figure
Application and Transport Division



The seven layers are divided into two functional groups.

The message initiated at the Application Layer is passed from layer to layer, through the various OSI layers, encapsulating control information in the process. A fully encapsulated message enters the cable at Layer 1. The procedure is reversed at the receiving end. Each item of control information is processed at its appropriate layer, and the message itself passes up to Layer 7. Data transfer essentially is a packaging process at the transmitting node and an unpackaging process at the receiving node.

The Layers

A number of objectives were considered by the reference model's designers: to limit the number of layers to make the system engineering task of describing and integrating the layers as simple as possible; to create boundaries between layers at points where the description of services can be small and the number of interactions across each boundary is minimized; and to collect similar functions in the same layer. Table "The Seven Layers of OSI" summarizes the OSI Reference Model's layers; more detailed descriptions follow for each layer.

The Application Layer

The Application Layer (Layer 7) is the highest layer, providing the means for the application process to access the OSI environment. Its function is to serve as the passageway between application processes using Open Systems Interconnection to exchange information; consequently, all application process parameters are made known to the OSI environment through this layer.

All services directly usable by the application process (i.e., systems and applications management functions) are provided by the Application Layer. It differs from the other layers in that it does not provide services to a layer above it. Some of the services provided by this layer, other than information transfer, are the following:

- Identifying intended communications partners
- Determining current availability of the intended partners
- Establishing the authority to communicate
- Agreeing on responsibility for error recovery
- Agreeing on procedures for controlling data integrity

The Presentation Layer

The Presentation Layer (Layer 6) allows an application to interpret the meaning of information exchanged. Information is formatted and translated at this layer. Aspects of Layer 6 include data syntax, which is the data to be transferred between layers, and the presentation image syntax, which is the data structure that application entities refer to in their dialog, or the set of actions that may be performed on the data structure.

Services provided to the Presentation Layer include the following:

- Transforming data syntax, primarily code and character set conversion
- Transforming and selecting the presentation syntax, the adaptation and modification of the presentation data (the OSI view)

Functions within the Presentation Layer include session establishment request; data transfer; negotiation and renegotiation of data syntax and presentation image syntax; and session termination request.

The Session Layer

The Session Layer (Layer 5) allows cooperating presentation entities to organize and synchronize their dialog and to manage data exchange. It provides the following services:

- Session-connection establishment—creation of an exchange between presentation entities
- Session-connection release
- Normal data exchange
- Expedited data exchange
- Interaction management—allowing presentation entities to take turns exercising control functions
- Session-connection synchronization
- Exception reporting—permitting the presentation entities to be notified of exceptional situations
- Activity management

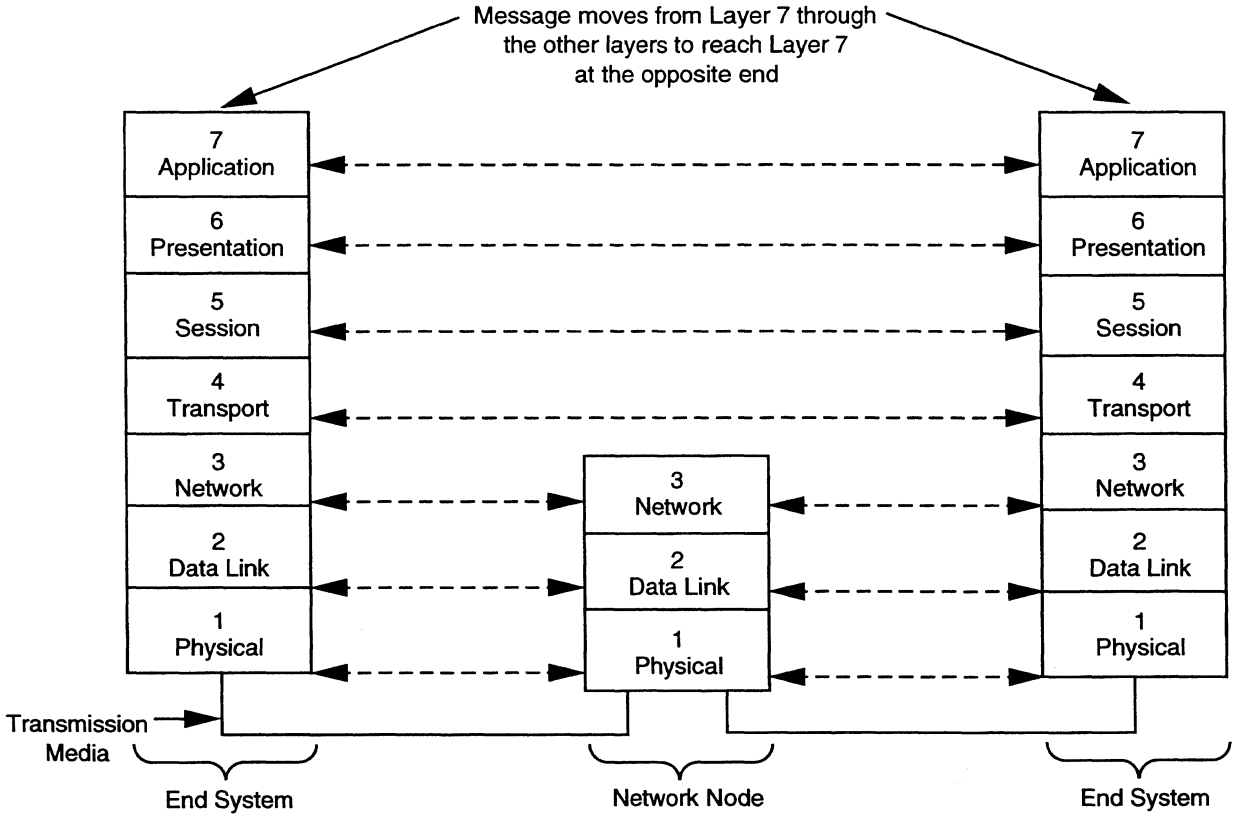
The Transport Layer

The Transport Layer (Layer 4) provides transparent data flow between session entities, freeing the Session Layer from responsibility for cost-effective and reliable data transfer. Layer 4 provides information interchange according to a user-specified reliability level and end-to-end control. Transport protocols transfer information from one end of a physical connection to another and ensure that it is delivered correctly. Layer 4 protocols are used after a route has been established through the network by the network-layer protocol.

The services provided by this layer include the following:

- Transport-connection establishment to complete a connection between session entities

Figure
Message Movement Among OSI Layers



Intermediate nodes in an OSI network require only bottom-layer functions of the OSI model. Note how peer layers communicate only with their peers; i.e., Layer 1 talks to other Layer 1s but not to Layer 2s.

- Data transfer, in accordance with the agreed quality of service
- Transport-connection release

The European Computer Manufacturers Assn. (ECMA) has defined this layer in its Transport Protocol standard, ECMA-72.

In the early 1990s, as the popularity of the OSI protocols began to wane and TCP/IP began to take over, a number of hybrid stacks were developed whereby data streams could "cross over" from one type of stack to another, in either direction. The cross-over point was at the Transport Layer in all cases. This allowed applications to reach their intended destinations whichever system they were using, and encouraged interoperability. Although this was in keeping with the aims of the ISO, it made possible migration to the newly-popular TCP/IP stack, and aided the eventual near-demise of the OSI stack as a complete set of protocols.

The Network Layer

The Network Layer (Layer 3) provides the means to establish, maintain, and terminate connections between systems. Its basic service is providing transparent data transfer between transport entities.

The services provided by this layer encompass the following:

- Establishing network connections for transporting data between transport entities through network addresses
- Identifying connection endpoints
- Transferring network service data units
- Noting errors for reporting unrecoverable errors to the transport layer
- Sequencing network control data units
- Flow control
- Releasing the network connection

The Network Layer is where routers and, nowadays, some LAN switches operate. They are indifferent to the type of network and can therefore be used to pass data from one type of network to another, for example from Ethernet to Token-Ring. Although many routers have OSI protocol support, in fact it is little used, IP being by far the preferred protocol for this layer. Given the importance of the Internet, which today runs almost entirely on IP, this can only increase. However, the remarks made earlier as to how the model has formed the way we think about networks holds particularly true for this layer and Layer 2—nobody can talk coherently about networking without mentioning these layers.

The Data Link Layer

Data Link Layer 2 provides the procedural and functional means to establish, maintain, and release data link connections between two network nodes or network entities and to transfer data frames (or packets). This layer also detects and may correct errors that occur in the Physical Layer.

Services provided by the Data Link Layer to the Network Layer include data link connection, sequencing, error notification, flow control, and data unit transfer.

Layers are sometimes divided into sublayers, for several reasons. Layer functions are often divided into separate modules to handle the service interface of the layer beneath it. This avoids "rewriting" the entire layer. The Data Link Layer of the IEEE 802 Local Area Network (LAN) standards is divided into a Logical Link Control (LLC) sublayer and a Media Access Control (MAC) sublayer. The MAC sublayer depends on characteristics of the underlying Physical Layer. Any layer may originate a message to fulfill its responsibilities. The message may not bypass any layer en route to its destination. If a message leaves the node, it will end up in another node at the same layer that originated the message.

It is at Layer 2 that bridges and most LAN switches reside. All such devices have a MAC address table for all the end stations (which all have MAC addresses).

The Physical Layer

The lowest of the OSI layers is Physical Layer 1. It provides the electrical, mechanical, functional, and procedural characteristics for activation, maintenance, and deactivation of a physical connection. Physical Layer standards specify physical interfaces (connectors) connected by a physical medium.

Services provided by this layer include the following:

- Activating and deactivating physical connections
- Data circuit identification
- Sequencing
- Transmitting physical service data units either synchronously or asynchronously
- Fault condition notification

Abstract Syntax Notation One (ASN.1)

ASN.1 is a *specification language* adopted for the OSI Reference Model, giving standards developers a common method for defining syntax. ASN.1 is somewhat analogous to grammatical rules defining the English language, with the exception that it is not procedural. Just as English grammar specifies notation (punctuation symbols) and word classifications (such as nouns and verbs), ASN.1 specifies the rules that help standards developers define complex data types in terms of simple building blocks.

ASN.1 was first formally described and published in 1984, in the ITU-T X.409 standard entitled "Message Handling Systems: Presentation Syntax and Notation." It is now described (in less readable fashion) in two later documents: ITU-T X.208 (ISO 8824), entitled "Specification of Abstract Syntax Notation One (ASN.1)," and X.209 (ISO 8825), "Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)."

According to ASN.1, each fragment of information must possess a type and a value. For example:

- Device-Status could be a type (in this case, it is a Boolean type)
- Zero or One are the possible values

This is specified in ASN.1 notation as such:

```
Device-Status ::= Boolean
Boolean ::= 1 (or 0)
```

This is a very simple example; ASN.1 is a powerful grammar, capable of specifying very complex data types. Hence, it will continue to be the grammar of choice for specifying open systems standards and protocols.

OSI Standards Progress

There are four stages in the development cycle: working paper; committee draft (CD), previously known as a draft proposal; draft international standard (DIS); and international standard (IS). A working paper is developed in the first stage. When it matures and contains well-developed technical concepts, it is registered as a CD. Passage advances the CD to the DIS level, and the document is considered sufficiently stable to serve as the basis of initial implementations. At the DIS level, the document is distributed for a 180-day ballot. The DIS may require multiple ballots. A successful ballot elevates the DIS to the level of IS and completes ISO's process.

The entire process usually takes between four and eight years. Here we can see one of the reasons for the lack of popularity for the protocols involved. The ITU-T was formerly the CCITT, under whose aegis these standards were set. The CCITT has now been devolved into the International Telecommunications Union (ITU). Telecommunications standards can be set over a long period of time as the voice and WAN world needs to ensure high quality and complete interoperability between systems. Data networking, on the other hand, in many cases exists in isolated LANs, and though these are almost always today connected to the outside world in some manner, a gateway of some sort, often IP, gives enough connectivity. For Wide Area Networks (WANs) the same needs may apply as for voice but there is a lot of crossover between the types of device used and the WAN manufacturers have adopted the same standards as are used in LANs in many cases. With the new standard, Asynchronous Transfer Mode (ATM), the standard was set for WANs, but became developed by the LAN vendors far more quickly. Given the fast-moving nature of LAN developments, with low-cost high-volume products appearing in ever greater numbers and new high-specification models ensuring replacements in ever-shorter times, it is easy to see that a standards process that takes up to eight years to complete is not workable. LAN standards today are proposed one year and a first version out the next. Again, the ISO process that demands a complete standard before the first release is ignored. as soon as a halfway working standard can be given out, it is, with a further release the year after. A case in point is the new LAN standard for virtual LANs, being developed by the IEEE 802.1q working group—the first release, planned for mid- to late 1997, has only the facilities for port-switching LANs, whereas the idea of completely separating the logical from the physical LAN (which is what a virtual LAN can do) needs far more than that to be efficient.

A list of standards organizations, together with contact details, associated with the OSI Reference Model and other standards mentioned here is given at the end of this report.

OSI Applications Standards

In the early 1990s, applications at Layer 7 were considered the driving force of OSI acceptance. In particular, the ISO electronic mail standard for message handling systems (MHSs)—or X.400—was becoming popular in commercial implementations. Two versions, one in 1984, and another in 1988, were unratified draft international standards. The standard was given a big boost in 1989, when the Aerospace Industry Assn. (AIA) adopted X.400 to interconnect its diverse electronic mail networks. Gateways to proprietary E-Mail systems were also developed that year, and dozens of vendors rolled out X.400-based products. In addition, the ISO adapted X.400 as the message medium for electronic data interchange (EDI). In this context, X.400 was to be used as the communications method to store and forward trade documents and business forms conforming to ANSI X12, the European EDIFACT, and de facto EDI standards. Alas, MHS/X.400 proved

costly and complicated to implement, and was overtaken by other, simpler, electronic mail standards, particularly, since the mid-1990s, Internet mail based on IP.

One component of successful E-Mail internetworking is directory services (DS), with the ISO version known as X.500. Again, this seems to be unworkable and, while no international standard has taken over, Novell's NDS and Banyan's StreetTalk provide most of the directory functionality in use today. Microsoft is also in the process of developing a similar function. In today's open networking environment, reliance on proprietary software is unusual (unless as pre-standard releases) and it can only be concluded that X.500 proved more or less unworkable, although Banyan declared its StreetTalk to be based very much upon X.500 and obviously drew upon it for a lot of the ideas.

X.500 specifies an on-line directory for message communications, ultimately allowing network providers to map a common, interconnected directory of worldwide users. X.500 dictates naming conventions, how users access directory information, and what services are available.

The OSI protocol pair for office automation, Office Document Architecture (ODA) and Office Document Interchange Format (ODIF), has been an international standard since 1988 (ISO 8613). It was also specified in the various governments' GOSIP procurement standards until the demise of GOSIP worldwide in the early 1990s. ODA and ODIF facilitate the exchange of office documents—such as letters, memoranda, and business reports—among dissimilar systems. Moreover, the standard specifies the formatting and exchange of compound documents—those containing combinations of text, images, and graphics. Several ISO working groups are attempting to strengthen and extend the standard in such areas as the inclusion of audio, spreadsheet data, color graphics, document security, and various layout and presentation styles.

The OSI standard for sending and sharing data files—File Transfer, Access, and Management (FTAM)—is also a finalized international standard. It is a Layer 7 component of the Manufacturing Automation Protocol (MAP), which was developed from networking efforts in the manufacturing industry. It spread quickly in Europe and made significant progress in domestic business applications, but the file protocol used with Transmission Control Protocol/Internet Protocol (TCP/IP)—File Transfer Protocol (FTP)—was also well established in the U.S., however, and generally more popular than FTAM. FTP has since taken over from FTAM for most file transfer and is the established way of downloading large files from Internet sites. It was thought that FTAM would become the standard for EDI transfers but, again, it became apparent that it was too cumbersome, and that was when X.400 became popular for that. The difference in use between X.400 (or any messaging system) and FTAM (or any other file transfer protocol such as FTP), is that file transfer is real time while X.400 is store and forward. With any store-and-forward system, there can be long delays while the information gets through the network—with FTAM and FTP any delays during transmission are usually brief, but are variable depending upon bottlenecks on a large system such as the Internet.

The Layer 7 protocol for network management, Common Management Information Protocol (CMIP), is now an International Standard. CMIP is a communications protocol between the agent process, and management agents at each managed OSI node. The real work of managing network processes is located within each node's managed objects at individual OSI layers. In other words, each layer must have its own network management system, which OSI does not specify. CMIP allows a centralized management process to either modify the value of an attribute, or request its value (read its status) at each of the layers. While CMIP has been more or less superseded by the Simple Network Management Protocol (SNMP) in the LAN, CMIP is still popular for WAN management, showing once again how different the two worlds can be. SNMP has taken up the structure for management that OSI set up with CMIP and now does the job of managing networks perfectly well. (For more information, see the OSI Management section featured later in this report.)

Other Layer 7 protocols include distributed Transaction Processing (TP), designed to interconnect different transaction computing systems across OSI networks; Remote Database Access (RDA), a protocol for integrating database management systems; and Manufacturing Message Specification (MMS), ISO 9506, a manufacturing protocol that requires extensions for specific manufacturing device types.

Connection Methods

Every layer of the OSI Reference Model, except the Physical Layer, supports both connection and connectionless mode (this is one of the reasons the protocols are so complex and expensive to implement—other technologies are one or the other). Connection-oriented service requires a connection establishment phase, a data transfer phase, and a connection termination phase; a logical connection is set up between end systems prior to data exchange. These phases define the necessary sequence of events for successful data transmission. Connection-oriented service capabilities include data sequencing, flow control, and transparent error handling.

In a connectionless service, such as Switched Multi-megabit Data Service (SMDS), each Protocol Data Unit (PDU) is independently routed to the destination; no connection establishment activities are required, since each data unit is independent of the previous or subsequent one. Connectionless-mode service transfers data units without regard to establishing or maintaining connections. In connectionless mode, transmission delivery is uncertain due to the possibility of errors. This appears contrary to the goal of network design—users want to ensure that messages reach their destination. In reality, connectionless-mode communication simply shifts responsibility for message integrity to a higher layer, which checks integrity only once, rather than requiring checks at each lower layer. Alternatively, each data unit might contain the error recovery mechanism.

In connection-oriented networking, such as ATM, a connection is established for the whole data stream just once, and all packets or cells follow that path. There is now also what might be thought of as a hybrid never dreamed of in OSI—IP switching, where the first packet is examined but the rest follow the path of the first through the switch, despite the connectionless nature of the protocols involved. This depends on having a switched network. Multiprotocol Over ATM (MPOA) will perform the same function when standardized late in 1997.

Lower-Layer Protocols

Lower-layer OSI protocols for Layers 1 through 3 are well-defined veterans and in many cases borrowed from existing EIA, IEEE, or ITU-T standards. Connectionless communications at the lower layers of the OSI model is well established and is found, for example, in LANs and metropolitan area networks (MANs). While the original OSI model—described in ISO 7498—was connection oriented, the ISO foresaw the need for connectionless service and issued an addendum to that protocol (ISO 7498/AD1). The ISO standard for Network Layer service, ISO 8348, contains connectionless service (in AD1) in addition to the connection mode.

OSI Security

By definition, an open system is one that encourages communications between different applications or users. Unfortunately, an

open system can also encourage illegal eavesdropping and information theft or destruction. Notorious examples of white-collar crime, corporate espionage, and network intrusions by computer worms and viruses have alarmed information processing professionals, and raised a general awareness of computer security issues. The concepts of information security and open systems are antithetical; nevertheless, the ISO has taken steps to provide a secure environment within the OSI Reference Model.

International Standard 7498, Part 2 addresses a security architecture within the general OSI model. It describes security measures that can be provided by specific layers in the model. Specific security standards are not yet defined, however, but are under study by working group JTC1, Subcommittee 27 for Information Technology Security Standards, plus other subcommittees.

SC21, concerned with maintaining and defining the upper three layers of the OSI Reference Model, stabilized several network management and security standards in 1991. The Security model is composed of six frameworks that work together across all seven layers of the OSI Reference Model: authentication, access control, security audit, nonrepudiation, confidentiality, and integrity.

OSI and MAP/TOP

The Manufacturing Automation Protocol and Technical Office Protocol (TOP) were originally developed by General Motors and Boeing Computer Services, respectively, to automate manufacturing functions on the factory floor and in the "back office." Both are based on the OSI Reference Model, using formal standards for each layer where possible. MAP, in particular, is probably the best-known example of a formal multilevel OSI implementation and is achieving substantial industry acceptance.

Version 3.0 added a Presentation Layer to the profile and implemented a version of the Manufacturing Message Specification (MMS), the protocol for transferring factory and robotics information, ISO 9506. Other Layer 7 protocols specified are FTAM, Network Management, and Directory Service. Middle layers implement ISO connection-oriented protocols, although these must be bypassed for time-critical applications. At the lower transport layers, MAP specifies the IEEE 802.4 token bus system employing a Type F coaxial connection to a 75-ohm cable. Although MAP was taken up widely in some countries, notably Japan, it has not been further pursued generally. LANs have moved on and few new LANs use token bus or coaxial cable now (except that in the new field of home LANs, coaxial cable is often employed for its ease of use, but standard Ethernet is universally installed here).

OSI and TCP/IP

Transmission Control Protocol/Internet Protocol was developed by the U.S. government's Defense Advanced Research Projects Agency (DARPA) for its research network, ARPANET. By 1986, TCP/IP had gained a following of commercial users seeking a protocol that could be used as a common denominator for multivendor computer networks. TCP and IP are actually two separate protocols, occupying middle layers number Four (Transport) and number Three (Network), respectively, of the OSI Reference Model.

TCP/IP has been implemented on almost every type of computer and is especially successful in commercial Ethernet LAN environments. The reason TCP/IP is so popular is because it is free and its development was paid for by the U.S. government. It avoids the connection-oriented/connectionless dilemma by essentially avoiding it. OSI provides a richer set of network options, but these may not be compatible in different networks. Users cannot communicate across different networks if they implement different options at these layers.

Despite OSI's early promise, a majority of networks now use TCP/IP for LAN interconnectivity. The Internet, the tool and plaything of the 1990s that is ARPANET's grandchild, runs almost exclusively on IP, though ATM is hidden now in the infrastructure, and we can expect this to increase as ever more bandwidth is needed. TCP/IP is also used for Ethernet LANs, and Novell has recently withdrawn its proprietary IPX from new NetWare installations, preferring instead to migrate customers to pure IP.

OSI Management

Since the first draft of the seven-layer ISO model was produced in 1978, extensions to the basic model have been developed to more adequately represent all of the functions required by large-scale, multivendor networking environments. OSI Management is an extension to the original reference model that specifies transfer of network management information in the Application Layer and support for network management functions at Layers 4, 5, and 6.

Advantages and Disadvantages to OSI-Based Network Management

In addition to solving the problem of managing heterogeneous environments, OSI-based network management played a part in bringing about a new phenomenon—the unbundling of network management from network products. In a proprietary environment, a given vendor's products are primarily manageable only by products developed by that vendor. The promise of OSI helped to split that one-to-one relationship, making it possible for any OSI-based network management system (NMS) to manage any OSI Management-conformant device. Despite being widely supported, CMIP has in the end lost out to SNMP in the LAN environment, but the initiative encouraged the widespread publication of private Management Information Bases (MIBs) so that heterogeneous networks could be managed under SNMP. In the WAN, CMIP is both widespread and popular. Here, there is not such an open environment due to lack of customer demand for it, and such interoperability as there is must be reliable. WAN management is vital—LAN management is still often, wrongly, treated as a luxury.

The market (both vendors and users) widely criticized ISO for moving too slowly in its efforts to ratify OSI Management standards. Vendors are wisely unwilling to develop products based on standards that are not yet final. In an effort to open the door to new OSI-based network management system products, SC21 WG4 defined groups of network management functions that were to be covered within OSI-based network management: fault, configuration, performance, accounting, and security management specifications. These principles, if not the actual protocols, have been established as the expected field to be covered by any network management system (NMS), and this is one of the areas that OSI has changed networking profoundly.

Another disadvantage of standards-based network management is that OSI standards merely provide a menu of options. There are numerous gaps and ambiguities in OSI Management standards that could be interpreted differently, leading to incompatible implementations.

Standards Documents

OSI Management standards can be broadly categorized into four areas:

1. Functions—*what* network management is, according to OSI
2. Services—*how* network management functions are accomplished

3. Information Structure—terms and categories describing *what is managed* (e.g., "management information")
4. Protocols—describe *means of transporting* network management information

Taken together, these four areas describe a generic package for network management systems, and how these products relate to the network devices they manage (called *managed objects* in OSI terminology).

A blueprint document, Management Framework OMNI*Point*, places the OSI Management environment in perspective by describing terms and the scope of OSI network management.

OSI Management Functions

OSI Management functions are described in the Systems Management standards (IS 10040, IS 10164-1 through 10164-7, and N 10164-8 through 10164-12). Management using three models:

1. The Organizational Model—describes ways OSI Management can be distributed administratively
2. The Information Model—provides guidelines for defining managed objects and their interrelationships, classes, and names
3. The Functional Model—describes network management functions

The Functional Model outlines how ISO has partitioned network management into five functional areas: fault management, configuration and name management, performance management, accounting management, and security management. ISO originally described each of these areas in its own standard. Further studies revealed that functions overlapped; therefore, ISO reorganized the documents in December 1988 into their present Systems Management form.

Fault management provides the detection, isolation, and correction of abnormalities in network operation. Configuration and name management facilities permit network managers to control the configuration of the system, network, or layer entities. Changed configurations may isolate faults, alleviate congestion, or meet changing user needs. Performance management enables the network manager to monitor and evaluate the performance of the system, network, and layer entities. Data from performance management may be used to initiate configuration changes and diagnostic testing to allow a satisfactory level of performance. Accounting management facilities help determine and allocate costs for the use of a network manager's communications resources. Security management facilities permit the management of those services providing access protection of communications resources.

Services

Services are described, in part, in the Common Management Information Protocol (CMIP) standard, IS 9596. Services use *primitives*, or command types, to accomplish network management functions. Examples of CMIP commands include GET, SET, GET REPORT, CREATE, and DELETE. While service primitives are somewhat abstract, they are important building blocks for composite commands used by network management applications to obtain vital data on the status and activity of network devices.

Common Management Information Services (CMIS) include a detailed abstract model of open systems management services. These fall into three categories—event notification, information transfer, and control. Event notification allows one system to notify another that some event of importance has occurred.

Information Structure

The most important standards in this category are Structure of Management Information (SMI), Parts 1, 2, and 4 (CD 10165-1, -2, and -4). (Part 3 is not missing; rather, ISO merged Part 3 into Part 4.) Included in these standards is an explanation of the *object-oriented* paradigm, used to model a network in terms of object classes and attributes. In object-oriented environments, a variable (for example, a variable called Bridge) is defined both in terms of the operations that can be performed on it and the values of attributes it can possess. For example, Bridge can have an attribute such as Status, which may have a value of Busy; a network management system may obtain this value via a Get operation, or alter it via a Set operation.

Objects (including their attributes and operations) are stored in a MIB, sometimes called an Object Library. The SMI documents just listed provide syntax and semantics for information in the MIB; however, no single ISO standard defines exactly what the OSI MIB will contain, nor how vendors and users can register objects in the standard MIB.

In the TCP/IP world, an Internet Standard MIB exists for objects managed using SNMP. This MIB functions in an analogous role to the proposed OSI MIB, although the administration and rules governing the two are sure to differ.

MIB includes all information needed to make management decisions. MIB is a conceptual repository of all OSI management data in an OSI environment. The MIB concept does not imply any form of physical or logical storage for management information, however, and its implementation is outside the scope of OSI standards. Rather, the SMI defines the abstract syntax and the semantics of information, so that it can be represented in OSI protocol exchanges.

Protocols

Common Management Information Protocol, IS 9596, is the primary OSI Management protocol. CMIP specifies procedures for the exchange of basic management information between open systems interconnected by OSI protocols.

X.500—The Directory

The Directory is a related standard designed to manage name-related information concerning protocol layers and network nodes. These services connect the actual names used in the network with names and addresses understood by human users. The Directory is defined in CD 9594.

OSI and the Future

The world needs a network of computers, similar to standards for international telephony, to link users across oceans and continents. A few years ago, most industry analysts perceived OSI as the answer. Although endorsed by such prominent vendors as IBM, DIGITAL, and Hewlett-Packard, OSI's once-bright future as the premier means of interconnecting multivendor computer networks is now dimmed. Where OSI was too complex, slow, and expensive, TCP/IP stepped in to fill the gaps. The OSI Reference Model also had some technical glitches and holes that prevented it from being widely implemented. These will probably never now be repaired. As an internetworking protocol, TCP/IP has proved its worth and is a popular and commercially successful method of linking users across diverse networks. OSI middle-layer protocols 3 through 5, the alternatives to TCP/IP, are not as simple to implement in the real world. SNMP, the network management protocol for TCP/IP networks, is also a proven, commercially successful solution. As long as vendors and users require practical networking products, they will continue using TCP/IP-based protocols—standard or not.

In reality, OSI and other layered architectures do not serve every application and are not a panacea. Proprietary architectures will continue to thrive alongside both *de facto* and *de jure* standards-based networks, especially for closed user groups (where internetworking is not a requirement) or in time-sensitive applications intolerant of layered protocols' high overhead.

All others who desire internetworking must realize that the associated protocols are still evolving—nothing is truly cast in iron. In market-based economies, products that do not satisfy market needs will not gain widespread favor. Therefore, prospective users must evaluate OSI protocols and their adoption with an eye toward future standards developments. As it stands now, OSI will not be the interconnection standard of the future. Significant portions of it, however, have most certainly contributed to the evolution of international standards. The OSI 7-Layer model itself, however, has proved itself over and over. This view of data communication has become universally accepted, with even SNA—which is layered differently—often explained in the OSI model's terms. While the standards and protocols may not develop, the structure has added greatly to a common understanding of networking and has now also stood the test of time. ■

ISO Reference Model for Open Systems Interconnection (OSI)

In this report:

Note: This report updates the OSI's status at all seven layers; compares OSI to other architectures; rationalizes the need for standards testing and verification; profiles major testing organizations; and outlines OSI Management standards and status.

Datapro Summary

The goal of Open Systems Interconnection (OSI) is to enable dissimilar computers in multivendor environments to share information transparently. The OSI structure calls for cooperation among systems of different manufacture and design. With this capability, global digital networks can become a reality. There are seven layers of the OSI model that communicate between one end system and another. The layers cover nearly all aspects of information flow, from applications-related services provided at the Application Layer to the physical connection of devices to the communications medium at the Physical Layer. Although all seven layers have long since been defined and ISO protocols ratified for each layer, the ISO committees must keep refining and extending specific sections of the model by rewriting existing definitions and adding new protocols.

Analysis

The proliferation of computerized data processing systems in the late 1960s produced a need for compatible data communications networks in the 1970s. Several proprietary network architectures were developed for mainframe-to-terminal communications, including IBM's SNA in 1974. Although many of these proprietary architectures were based on a layered model, none were compatible with any other. The CCITT's X.25 host interface to the packet networks standard was ratified in 1976 but is not a complete network architecture. In 1977 the International Organization for Standardization (ISO) formed ISO Technical Committee 97 (TC97), Subcommittee 16 (SC16), to embark on a worldwide standardization effort and confront the issue of incompatibility head-on. The purpose of TC97/SC16 was to develop a model and define the protocols and interfaces required to support an *open system*. The goal of OSI was, and still is, to enable dissimilar computers in multivendor environments to share information transparently. With this capability, global digital networks can become a reality.

The Open System

The ISO defines a *system* as a set of one or more computers and associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., which form an autonomous whole capable of performing information processing and/or information transfer. An *open system* is one that obeys OSI standards in its communication with other systems.

An *application process* is an element within a system that performs information processing for a particular application. The application process can be manual (a person operating a banking terminal), computerized (a program executing in a computer center and accessing a remote database), or physical (a process control program executing in a dedicated computer attached to industrial equipment and linked to a plant control system).

The OSI structure calls for cooperation among systems of different manufacture and design. This includes coordinating activities such as the following:

- Interprocess communications—the synchronization between OSI application processes and the exchange of information
- Data representation—the creation and maintenance of data descriptions and transformations for reformatting data exchanged between systems

- Data storage—storage media, file systems, and database systems for providing access to and management of stored data
- Process and resource management—how application processes are declared, initiated, controlled, and acquired
- Integrity and security—information processing constraints that must be ensured during open systems operations
- Program support—the definition, compilation, testing, linking, storage, and transfer of and access to programs executed by the application processes

The OSI model is concerned only with the exchange of information between open systems.

The Layering Concept

Layering is a basic structuring technique used in the OSI model. Each layer is composed of an ordered set of subsystems, with logically related functions grouped together. The OSI model breaks down internetworking activities between systems into two distinct groups. Communications-oriented functions are separated from user-oriented functions; features which move information across a network are distinct from features which handle and format information.

There are seven layers of the OSI model that communicate between one end system and another end system. The layers cover nearly all aspects of information flow, from applications-related services provided at the Application Layer to the connection of devices to the communications medium at the Physical Layer. Below the Physical Layer, the media itself corresponding to "Layer 0"—such as wire, cable, or through-the-air communication—is currently not addressed by the model. Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers have been defined (see Table 1). The model described in Table 1 is OSI's seven layers with their purposes. In Table 1, information flows down from Layer 7 to Layer 1, and then out over a physical transmission medium. At the receiving end, the information flows into another end system and up from Layer 1 to Layer 7, until it is received by a user.

The seven layers can be divided into two functional groups: the Transport Platform (Layers 1 to 4) and the Application Platform (Layers 5 to 7). The Transport Platform's function is to get data from one system to another without errors. The Application Platform's function is to interpret the data stream and present it to the user in a usable form (see Figure 1).

Each layer contributes functions to the communications task. For example, the Link Layer enables communications across a single physical connection, while the Network Layer provides end-to-end routing and data relay. Services at the upper-layer interface—providing communications to the next-higher layer—are provided by each layer, usually described by a service specification for the layer. Services at each layer are provided by a layer entity. Each layer entity communicates with its peer at the same layer on another system, providing services specified in the service specification.

Layers are sometimes divided into sublayers, for several reasons. Layer functions are often divided into separate modules to handle the service interface of the layer beneath it. This avoids "rewriting" the entire layer. For example, the Link Layer of the IEEE 802 Local Area Network (LAN) standards is divided into a Logical Link Control (LLC) sublayer and a Media Access Control (MAC) sublayer. The MAC sublayer depends on characteristics of the underlying Physical Layer. Any layer may originate a message to fulfill its responsibilities. The message may not bypass any layer en route to its destination. If a message leaves the node, it will end up in another node at the same layer that originated the message.

IBM's SNA is also a layered architecture, following rules of layering similar to OSI and other layered architectures. There are good reasons for layering: layering simplifies change; components inside a layer can be changed without affecting any other layers in that node. Layers are like structured programming—but for teleprocessing systems. Because there are rigid interfaces between levels, fewer people need to react to changes, allowing them to be implemented faster. There is no better way of achieving complex functions. Layering allows each network function to

Table 1. The Seven Layers of OSI

Layer	Name	Purpose
7	Application	Applications and application interfaces for OSI networks. Provides access to lower-layer functions and services.
6	Presentation	Negotiates syntactic representation for the Presentation Layer and performs data transformations.
5	Session	Coordinates connection and interaction between applications. Establishes a dialog, manages and synchronizes the direction of data flow.
4	Transport	Ensures end-to-end data transfer between applications, data integrity, and service quality. Assembles data packets for routing by Layer 3.
3	Network	Routes and relays data units among network nodes.
2	Data Link	Transfers data units from one network node to another over a transmission circuit. Ensures data integrity between nodes.
1	Physical	Delimits and encodes the bits onto the physical medium.

Standards Organizations and Testing Agencies

Although standards are indispensable for computer internetworking, they are useless unless vendor claims of compatibility can be tested and users can be ensured of acquiring products that comply fully with the standards. In general, vendor claims of standards compatibility are suspect unless verified by an impartial testing agency. Additionally, compatibility claims can mean different things to different people. For users, it is a good idea to probe vendor claims of standards compatibility to determine what is compatible with what, and at what levels.

Several standards testing and verification bodies have been organized both here and abroad by vendor consortiums, government agencies, and independent organizations. They have found that developing conformance specifications, producing testing suites, and conducting comprehensive testing are complicated, expensive, and time consuming. Regional differences can stymie attempts at verification. The trend for these organizations, therefore, is to cooperate with each other, sharing resources and expertise. A primary objective is demonstrating interoperability among different vendors; i.e., proving that standards really work and fostering end-user interest. Many agencies have tried vainly to involve more end users but are backed primarily by the vendors.

In the U.S., primary testing and certification agencies include the Corporation for Open Systems (COS), the National Institute of Science and Technology (NIST), and Bell Communications Research (Bellcore). Several smaller organizations and certain vendors, however, also offer testing services. Europe is represented by the Standards Promotion & Application Group (SPAG); Japan by the Promoting Conference for OSI (POSI). Standards organizations are listed below:

American National Standards Institute (ANSI)
1430 Broadway
New York, NY 10018
(212) 642-4900

ANSI X3 Secretariat
Computer and Business Equipment Manufacturers Assn. (CBEMA)
Suite 500, 311 First Street, NW
Washington, DC 20001-2178
(202) 737-8888

Bell Communications Research (Bellcore)
60 New England Avenue
Piscataway, NJ 08854-4196
(908) 699-2000
Customer Service Hot Line:
(800) 521-CORE

Corporation for Open Systems (COS)
Suite 400, 1750 Old Meadow Road
McLean, VA 22102-4306
(703) 883-2700
Telex: WUI 6503157578 MCI UW

European Computer Manufacturers Assn. (ECMA)
Rue du Rhone 114
CH-1204 Geneva, Switzerland
(+41) 22 735 36 34
Telex: 413237 ECMA CH

Electronic Industries Assn. (EIA)
1722 Eye Street NW, Suite 300
Washington, DC 20006
(202) 457-4900

International Organization for Standardization (ISO)
1, Rue de Varembe
Case Postale 56
CS-1211 Geneva 20, Switzerland
(+41) 22 33 34 30

International Telegraph and Telephone Consultative Committee (CCITT)
General Secretariat
International Telecommunications Union (ITU)
Place des Nations
CH-1211 Geneva 20, Switzerland
(+41) 22 99 51 11
Fax: (+41) 22 33 72 56
Telex: 421 000 UIT CH

Institute of Electrical and Electronics Engineers (IEEE)
Headquarters
345 E. 47th Street
New York, NY 10017
(212) 705-7900
Fax (publications): (212) 705-7682

IEEE Service Center
(published standards):
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331
(908) 981-1393
Fax: (908) 981-9667
Telex: 833-233

OSINET
Mr. Jerry Mulvenna, Chairman
OSINET Steering Committee
NIST Building 225, Room B217
Clopper Road
Gaithersburg, MD 20899

Standards Promotion & Application Group SA (SPAG)
Avenue Louise 149, Box 7
1050 Brussels, Belgium
(+32) 2 535 08 11
Telex: 20307 SPAG B

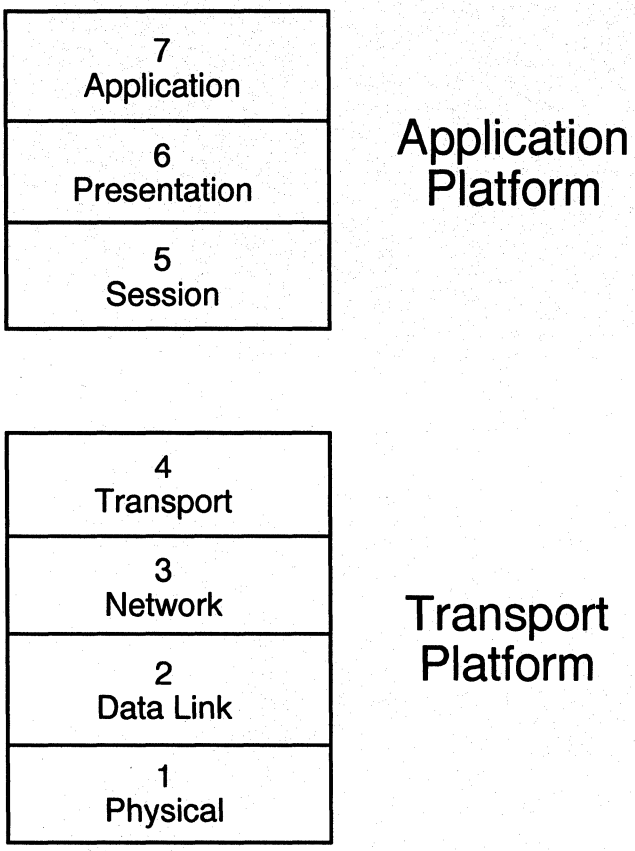
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
Gaithersburg, MD 20899
(301) 975-2000

be made "transparent," unaware and independent of other functions at other layers, thus enabling any layer to be modified without changing the entire monolithic architecture.

Each layer may support one of several different protocols designed for specific network applications; the choice of a specific protocol is optional, allowing users to tailor networks to their own design. Each layer defines functions crucial to the communications process at that layer, independent of the other layers. However, a layer may perform functions hinging on functions performed in the layers immediately above or below. A layer can only communicate with another device or network node at its peer layer. Messages exchanged between peer layers are "enveloped" with messages from other layers and passed through these other layers on the way to their destination, picking up and then shedding these other protocol layers along the way. For example, if layer seven at one end system must send a message to layer seven at another, it must travel down through six layers at its own end and then up through six layers at the other, until it reaches layer seven at its opposite (peer) layer.

Each network node (a network user, computer, terminal) is equipped with this layer mechanism. However, not all intermediate nodes need all seven layers. Network nodes, in particular, must only route and transmit data packets—functions at the bottom three layers of the OSI model. Layer 4 through 7 functions are not required and, therefore, not included in network node software. Data packets processed in these nodes reach only Layer 3 and are then routed elsewhere (see Figure 2). A node communicates with its peer in another node sending or receiving data. Data transfer is routed from Layer 7 down to Layer 1 at the transmitting node, then along the network to Layer 1 at the receiving node, and finally from Layer 1 up to Layer 7. Peer layers communicate by the same method.

Figure 1.
Application and Transport Divisions



The seven layers are divided into two functional groups.

The message initiated at the Application Layer is passed from layer to layer, through the various OSI layers, encapsulating control information in the process. A fully encapsulated message enters the cable at Layer 1. The procedure is reversed at the receiving end. Each item of control information is processed at its appropriate layer, and the message itself passes up to Layer 7. Data transfer essentially is a packaging process at the transmitting node and an unpackaging process at the receiving node.

The Layers

A number of objectives were considered by the reference model's designers: to limit the number of layers to make the system engineering task of describing and integrating the layers as simple as possible; to create boundaries between layers at points where the description of services can be small and the number of interactions across each boundary is minimized; and to collect similar functions in the same layer. Table 1 summarizes the OSI Reference Model's layers; more detailed descriptions follow for each layer.

The Application Layer

The Application Layer (Layer 7) is the highest layer, providing the means for the application process to access the OSI environment. Its function is to serve as the passageway between application processes using Open Systems Interconnection to exchange information; consequently, all application process parameters are made known to the OSI environment through this layer.

All services directly usable by the application process (i.e., systems and applications management functions) are provided by the Application Layer. It differs from the other layers in that it does not provide services to a layer above it. Some of the services provided by this layer, other than information transfer, are the following:

- Identifying intended communications partners
- Determining current availability of the intended partners
- Establishing the authority to communicate
- Agreeing on responsibility for error recovery
- Agreeing on procedures for controlling data integrity

The Presentation Layer

The Presentation Layer (Layer 6) allows an application to interpret the meaning of information exchanged. Information is formatted and translated at this layer. Aspects of Layer 6 include data syntax, which is the data to be transferred between layers, and the presentation image syntax, which is the data structure that application entities refer to in their dialog, or the set of actions that may be performed on the data structure.

Services provided to the Presentation Layer include the following:

- Transforming data syntax, primarily code and character set conversion
- Transforming and selecting the presentation syntax, the adaptation and modification of the presentation data (the OSI view)

Functions within the Presentation Layer include session establishment request; data transfer; negotiation and renegotiation of data syntax and presentation image syntax; and session termination request.

The Session Layer

The Session Layer (Layer 5) allows cooperating presentation entities to organize and synchronize their dialog and to manage data exchange. It provides the following services:

- Session-connection establishment—creation of an exchange between presentation entities
- Session-connection release
- Normal data exchange
- Expedited data exchange
- Interaction management—allowing presentation entities to take turns exercising control functions
- Session-connection synchronization
- Exception reporting—permitting the presentation entities to be notified of exceptional situations
- Activity management

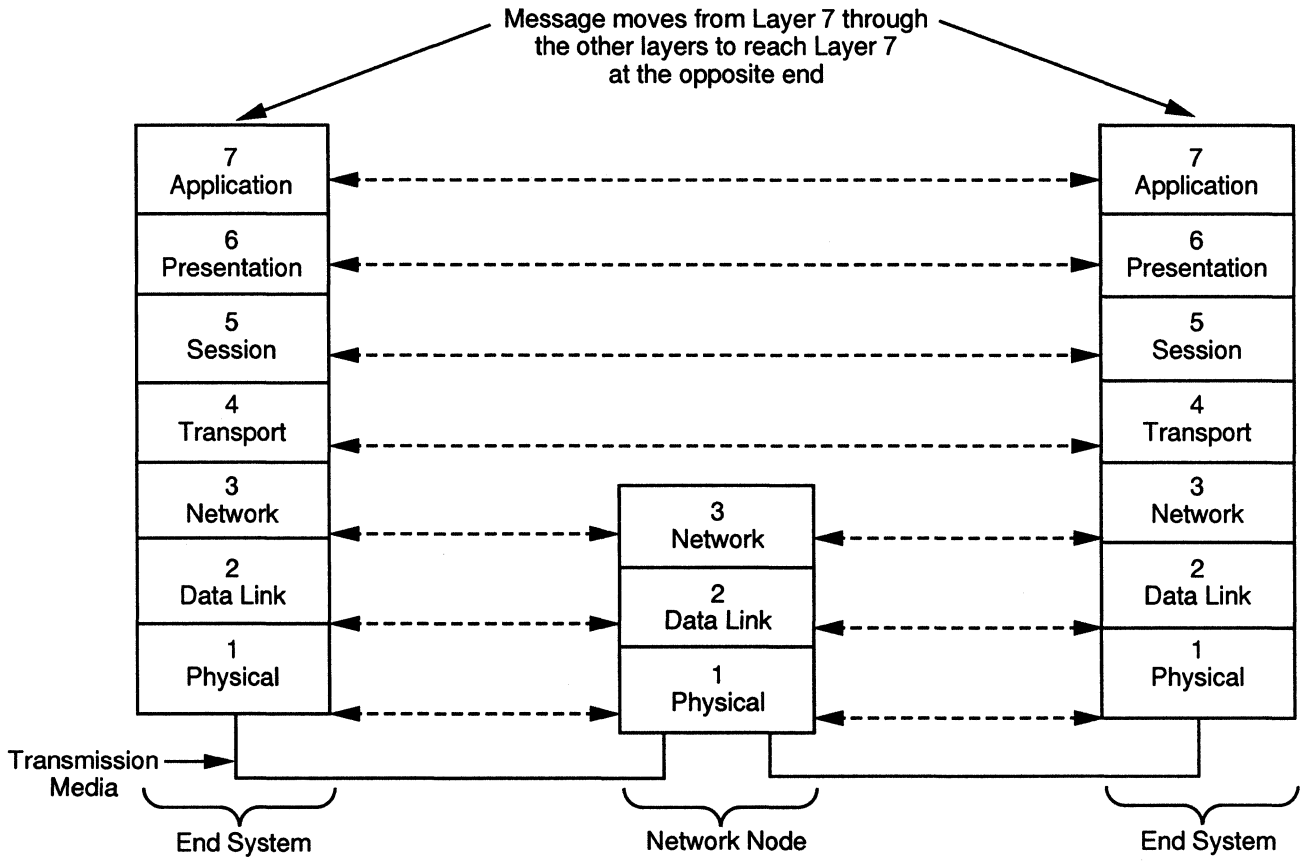
The Transport Layer

The Transport Layer (Layer 4) provides transparent data flow between session entities, freeing the Session Layer from responsibility for cost-effective and reliable data transfer. Layer 4 provides information interchange according to a user-specified reliability level and end-to-end control. Transport protocols transfer information from one end of a physical connection to another and ensure that it is delivered correctly. Layer 4 protocols are used after a route has been established through the network by the network-layer protocol.

The services provided by this layer include the following:

- Transport-connection establishment to complete a connection between session entities

Figure 2.
Message Movement Among OSI Layers



Intermediate nodes in an OSI network require only bottom-layer functions of the OSI model. Note how peer layers communicate only with their peers; i.e., Layer 1 talks to other Layer 1s but not to Layer 2s.

- Data transfer, in accordance with the agreed quality of service
- Transport-connection release

The European Computer Manufacturers Assn. (ECMA) has defined this layer in its Transport Protocol standard, ECMA-72. This standard has gained the support of a number of North American and European computer manufacturers.

The Network Layer

The Network Layer (Layer 3) provides the means to establish, maintain, and terminate connections between systems. Its basic service is providing transparent data transfer between transport entities.

The services provided by this layer encompass the following:

- Establishing network connections for transporting data between transport entities through network addresses
- Identifying connection endpoints
- Transferring network service data units
- Noting errors for reporting unrecoverable errors to the transport layer
- Sequencing network control data units
- Flow control
- Releasing the network connection

The Data Link Layer

Data Link Layer 2 provides the procedural and functional means to establish, maintain, and release data link connections between two network nodes or network entities and to transfer data frames (or packets). This layer also detects and may correct errors that occur in the Physical Layer.

Services provided by the Data Link Layer to the Network Layer include data link connection, sequencing, error notification, flow control, and data unit transfer.

The Physical Layer

The lowest of the OSI layers is Physical Layer 1. It provides the electrical, mechanical, functional, and procedural characteristics for activation, maintenance, and deactivation of a physical connection. Physical Layer standards specify physical interfaces (connectors) connected by a physical medium.

Services provided by this layer include the following:

- Activating and deactivating physical connections
- Data circuit identification
- Sequencing
- Transmitting physical service data units either synchronously or asynchronously
- Fault condition notification

Abstract Syntax Notation One (ASN.1)

ASN.1 is a *specification language* adopted for the OSI Reference Model, giving standards developers a common method for defining syntax. ASN.1 is somewhat analogous to grammatical rules defining the English language, with the exception that it is not procedural. Just as English grammar specifies notation (punctuation symbols) and word classifications (such as nouns and verbs), ASN.1 specifies the rules that help standards developers define complex data types in terms of simple building blocks.

ASN.1 was first formally described and published in 1984, in the CCITT X.409 standard entitled "Message Handling Systems: Presentation Syntax and Notation." It is now described (in less readable fashion) in two later documents: CCITT X.208 (ISO 8824), entitled "Specification of Abstract Syntax Notation One (ASN.1)," and X.209 (ISO 8825), "Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)."

According to ASN.1, each fragment of information must possess a type and a value. For example:

- **Device-Status** could be a type (in this case, it is a Boolean type)
- **Zero** or **One** are the possible values

This is specified in ASN.1 notation as such:

```
Device-Status ::= Boolean
Boolean ::= 1 (or 0)
```

This is a very simple example; ASN.1 is a powerful grammar, capable of specifying very complex data types. Hence, it will continue to be the grammar of choice for specifying open systems standards and protocols.

OSI Standards Progress

There are four stages in the development cycle: working paper; committee draft (CD), previously known as a draft proposal; draft international standard (DIS); and international standard (IS). A working paper is developed in the first stage. When it matures and contains well-developed technical concepts, it is registered as a CD. Passage advances the CD to the DIS level, and the document is considered sufficiently stable to serve as the basis of initial implementations. At the DIS level, the document is distributed for a 180-day ballot. The DIS may require multiple ballots. A successful ballot elevates the DIS to the level of IS and completes ISO's process.

The entire process usually takes between four and eight years. A list of standards organizations associated with the OSI Reference Model is given at the end of this report.

The Evolution of OSI Committees

In the spring of 1977, ISO Technical Committee 97 (TC97) formed a special subcommittee (SC16) charged with developing an architectural model that would extend from applications-layer communications clear down to the connection with the physical interface. The first draft of the seven-layer OSI Reference Model was completed in 1978. Between 1978 and 1983, the Basic Reference Model and many of the standards for the individual layers approached or attained draft international standard status. By the end of 1984, SC16 was reorganized to form Subcommittee 21 (SC21). Working groups within SC16 were also realigned.

The OSI Basic Reference Model became an international standard in 1984. During 1985 a number of vendors demonstrated products that implemented these standards and, by the end of 1986, many of these products were commercially introduced.

In July 1987 the Joint Technical Committee for Information Technology (JTC1) was formed when ISO/TC97 joined forces with Technical Committee 83 (TC83) of the International Electrotechnical Commission (IEC). The IEC is a coalition of industrial standards bodies that is co-located with the ISO in Geneva, Switzerland. The new JTC1 held its first meeting in 1987. The standardization activities of SC21 report to JTC1.

SC21 is composed of member bodies (MBs) from 23 different countries. Each MB has its own national standards organization; for example, ANSI represents the United States in JTC1. The individuals or "national correspondents" comprising the MB delegations come from different groups including user organizations, manufacturing firms, government agencies, and common carriers or PTTs. As such, they bring varying perspectives and concerns to the committee sessions.

When an OSI committee or working group produces a document such as a CD, the document is circulated among the MBs for a vote and to the liaison organizations (LOs) for review. LOs are independent organizations which also have a vested interest in OSI development. LOs provide comments on the content of OSI documents but do not have voting privileges.

Status of OSI Protocols

Protocol standards for all seven layers of the OSI model have been approved; however, OSI committees are refining and extending some standards as required and may add new standards at specific layers (particularly Layer 7). Additionally, other standards groups—such as the CCITT, ANSI, and IEEE—may adopt OSI protocol standards as their own and vice versa. Consequently, many OSI standards are known by more than one standard designation. Table 2 shows some major ISO protocols approved for each OSI layer and lists corresponding appellations from ANSI, the CCITT, and the ECMA, where applicable.

OSI Applications Standards

ISO committees are working hard at Layer 7, the Application Layer. In fact, OSI application standards are perceived as potentially powerful and versatile and are the driving force for OSI market acceptance. We devote considerable space reviewing some of the most important ones here.

In particular, the ISO electronic mail standard for message handling systems (MHSs)—or CCITT X.400—is becoming popular in commercial implementations. Two versions, one in 1984, and another in 1988, are draft international standards that have not been ratified. The standard was given a big boost in 1989, when the Aerospace Industry Assn. (AIA) adopted X.400 to interconnect its diverse electronic mail networks. Gateways to proprietary E-Mail systems were also developed that year, and dozens of vendors have rolled out X.400-based products. Most public E-Mail carriers have also adopted the standard and are migrating to the 1988 version.

In addition, the ISO is adapting X.400 as the message medium for electronic data interchange (EDI). In this context, X.400 would be used as the communications method to store and forward trade documents and business forms conforming to ANSI X12, the European EDIFACT, and de facto EDI standards.

One component of successful E-Mail internetworking is directory services (DS), commonly known as CCITT X.500. X.500 specifies an on-line directory for message communications, ultimately allowing network providers to map a common, interconnected directory of worldwide users. X.500 dictates naming conventions, how users access directory information, and what services are available.

Since the 1988 standard is not flexible, SC21 WG4 is working to ease the transition to the new 1992 version. Older 1988 X.500 systems will require a software modification to work with the 1992 version. Realistically, the vision of a worldwide messaging directory probably will not be realized until the late 1990s.

Table 2. ISO Protocols and Equivalent Standards

Layer	ISO	CCITT	ANSI *(1)*	ECMA
7	8571 (FTAM)	—	—	—
Application	10021 (MHS)	X.400	—	—
	9041 (VT)	—	—	—
	10026 (DTP)	—	—	—
	9594 (DS)	X.500	—	—
	8613 (ODA)	T.410 Series, T.73	—	ECMA-101
	9579 (RDA)	—	—	—
	9596 (CMIP)	—	—	—
6	8823 (connection)	X.226	—	—
Presentation	9596 (connectionless)	—	—	—
5	8327 (connection)	X.225	X3.153	ECMA-75
Session	9548 (connectionless)	—	—	—
4	8073 (TP0-TP4) (connection)	X.224	X3.140	ECMA-72
Transport	8602/8072 (connectionless)	—	—	—
3	8208 (Layers 1-3)	X.25	—	—
Network	8348 (connection)	X.213	—	—
	8473 (connectionless)	—	—	ECMA-92
	9542 (IS-IS)	—	—	—
	8878 (use w/8208)	(X.25)	—	—
	8880 (LAN)	—	—	—
	8881 (X.25 on LANs)	—	—	—
2	7776 (LAPB)	X.25	—	—
Data Link	3309 (HDLC)	—	X3.66	ECMA-40
	8802.2-.7 (LAN) (IEEE 802.2-.7)	—	—	ECMA-82, -81, -90, -89
1	9314 (FDDI)	—	X3.148, X3.139, X3.166	—
Physical	2110 (EIA-232D)	V.24, V.28	—	—
	4902 (EIA-449)	V.24, V.28	—	—
	2593	V.35	—	—
	4903	X-Series interfaces, Other V-Series	—	—

(1) No ANSI standards exist by policy in most instances, as U.S. follows International standards.

The OSI protocol pair for office automation, Office Document Architecture (ODA) and Office Document Interchange Format (ODIF), has been an international standard since 1988 (ISO 8613). It is also specified in the U.S. government's GOSIP standard. ODA and ODIF facilitate the exchange of office documents—such as letters, memoranda, and business reports—among dissimilar systems. Moreover, the standard specifies the formatting and exchange of compound documents—those containing combinations of text, images, and graphics. Several ISO working groups are attempting to strengthen and extend the standard in such areas as the inclusion of audio, spreadsheet data, color graphics, document security, and various layout and presentation styles.

The OSI standard for sending and sharing data files—File Transfer, Access, and Management (FTAM)—is also a finalized international standard. It is a Layer 7 component of the Manufacturing Automation Protocol (MAP), which was developed from networking efforts in the manufacturing industry. FTAM has spread quickly in Europe and has made significant progress in domestic business applications. The file protocol used with

Transmission Control Protocol/Internet Protocol (TCP/IP)—File Transfer Protocol (FTP)—is also well established in the U.S., however, and generally more popular than FTAM.

The Layer 7 protocol for network management, Common Management Information Protocol (CMIP), is now an International Standard. CMIP is a communications protocol between the agent process and management agents at each managed OSI node. The real work of managing network processes is located within each node's managed objects at individual OSI layers; in other words, each layer must have its own network management system, which OSI does not specify. CMIP allows a centralized management process to either modify the value of an attribute or request its value (read its status) at each of the layers. Definitions and descriptions of management structures and managed information are contained in other OSI standards yet to be completed. (For more information, see the OSI Management section featured later in this report.)

Other Layer 7 protocols include distributed Transaction Processing (TP), designed to interconnect different transaction computing systems across OSI networks; Remote Database Access (RDA), a protocol for integrating database management systems; and Manufacturing Message Specification (MMS), ISO 9506, a manufacturing protocol that requires extensions for specific manufacturing device types.

Connection Methods

Every layer of the OSI Reference Model, except the Physical Layer, supports connection and connectionless mode. Connection-oriented service requires a connection establishment phase, a data transfer phase, and a connection termination phase; a logical connection is set up between end systems prior to data exchange. These phases define the necessary sequence of events for successful data transmission. Connection-oriented service capabilities include data sequencing, flow control, and transparent error handling.

In a connectionless service, such as new Switched Multimegabit Data Service (SMDS), each Protocol Data Unit is independently routed to the destination; no connection establishment activities are required, since each data unit is independent of the previous or subsequent one. Connectionless-mode service transfers data units without regard to establishing or maintaining connections. In connectionless mode, transmission delivery is uncertain due to the possibility of errors. This appears contrary to the goal of network design—users want to ensure that messages reach their destination. In reality, connectionless-mode communication simply shifts responsibility for message integrity to a higher layer, which checks integrity only once, rather than requiring checks at each lower layer. Alternatively, each data unit might contain the error recovery mechanism.

Lower-Layer Protocols

Lower-layer OSI protocols for Layers 1 through 3 are well-defined veterans and in many cases borrowed from existing EIA, IEEE, or CCITT standards. Connectionless communications at the lower layers of the OSI model is well established and is found, for example, in LANs and metropolitan area networks (MANs). While the original OSI model—described in ISO 7498—was connection oriented, the ISO foresaw the need for connectionless service and issued an addendum to that protocol (ISO 7498/AD1). The ISO is now working to update the Connectionless Addendum, and CCITT SG VII pursues a parallel process. The CCITT, however, has been reluctant to insert connectionless-mode data transmission concepts into CCITT X.200—its version of the OSI model. The ISO standard for Network Layer service, ISO 8348, contains connectionless service (in AD1) in addition to the connection mode.

OSI Security

By definition, an open system is one that encourages communications between different applications or users. Unfortunately, an open system can also encourage illegal eavesdropping and information theft or destruction. Recently, notorious examples of white-collar crime, corporate espionage, and network intrusions by computer worms and viruses have alarmed information processing professionals and raised a general awareness of computer security issues. The concepts of information security and open systems are antithetical; nevertheless, the ISO has taken steps to provide a secure environment within the OSI Reference Model.

International Standard 7498, Part 2 addresses a security architecture within the general OSI model. It describes security measures that can be provided by specific layers in the model. Specific security standards are not yet defined, however, but are under study by working group JTC1, Subcommittee 27 for Information Technology Security Standards, plus other subcommittees.

SC21, concerned with maintaining and defining the upper three layers of the OSI Reference Model, stabilized several network management and security standards in 1991. The Security model is composed of six frameworks that work together across all seven layers of the OSI Reference Model: authentication, access control, security audit, nonrepudiation, confidentiality, and integrity. SC21 is working to establish two of the six security standards as Draft International Standards (DISs), and the remaining four standards, which are working drafts, will progress to CD status.

OSI and MAP/TOP

The Manufacturing Automation Protocol and Technical Office Protocol (TOP) were originally developed by General Motors and Boeing Computer Services, respectively, to automate manufacturing functions on the factory floor and in the "back office." Both are based on the OSI Reference Model, using formal standards for each layer where possible. MAP, in particular, is probably the best-known example of a formal multilevel OSI implementation and is achieving substantial industry acceptance. Many vendors now offer MAP 3.0 products, which have nearly eliminated proprietary "shop floor" automated factory solutions.

Today, manufacturing networking standards are directed by the MAP/TOP users group. MAP Version 3.0 was released in June 1988 and will remain free from major changes until 1994. Version 3.0 added a Presentation Layer to the profile and implemented a version of the Manufacturing Message Specification (MMS), the protocol for transferring factory and robotics information, ISO 9506. The ISO is currently working to extend MMS in support of realtime applications. Other Layer 7 protocols specified are FTAM, Network Management, and Directory Service. Middle layers implement ISO connection-oriented protocols, although these must be bypassed for time-critical applications. At the lower transport layers, MAP specifies the IEEE 802.4 token bus system employing a Type F coaxial connection to a 75-ohm cable.

OSI and TCP/IP

Transmission Control Protocol/Internet Protocol was developed by the U.S. government's Defense Advanced Research Projects Agency (DARPA) for its research network, ARPANET. By 1986, TCP/IP had gained a following of commercial users seeking a protocol that could be used as a common denominator for multivendor computer networks. TCP and IP are actually two separate protocols, occupying middle layers number Four (Transport) and number Three (Network), respectively, of the OSI Reference Model.

TCP/IP has been implemented on almost every type of computer and is especially successful in commercial Ethernet LAN environments. The reason TCP/IP is so popular is because it is free and its development was paid for by the U.S. government. In fact, it is actually more complex than TP4. It avoids the connection-oriented/connectionless dilemma by essentially avoiding it. OSI provides a richer set of network options, but these may not be compatible in different networks. Users cannot communicate across different networks if they implement different options at these layers.

Already, some proprietary stripped-down versions of OSI have been developed to operate over TCP/IP, and some pundits believe that TCP/IP will evolve to resemble OSI in the future. TCP/IP's future could have been jeopardized, since the U.S. government mandated OSI compliance in government procurements, had it not been for Novell's introduction earlier this year of a new version of its NetWare network operating software that supports TCP/IP.

A majority of users still use TCP/IP networks for LAN interconnectivity. However, the consensus is that TCP/IP is not the ultimate solution—a feat attributed to OSI. The trend is toward a migration to OSI-based applications running on a TCP/IP infrastructure. As a result, more vendors, including Unisys and Amdahl, are introducing products that support multiple protocols.

OSI Management

Since the first draft of the seven-layer ISO model was produced in 1978, extensions to the basic model have been developed to more adequately represent all of the functions required by large-scale, multivendor networking environments. OSI Management is an extension to the original reference model that specifies transfer of network management information in the Application Layer and support for network management functions at Layers 4, 5, and 6.

Advantages to OSI-Based Network Management

OSI-based network management continues to capture attention as the premier solution for multivendor network management. Vendors such as AT&T, Digital Equipment, Hewlett-Packard, and NCR are now designing their network management architectures to accommodate OSI Management standards and protocols.

In addition to solving the problem of managing heterogeneous environments, OSI-based network management will bring about a new phenomenon—unbundling network management from network products. In a proprietary environment, a given vendor's products are primarily manageable only by products developed by that vendor. Widespread use of OSI will split that one-to-one relationship, making it possible for any OSI-based network management system (NMS) to manage any OSI Management-conformant device.

Disadvantages to OSI-Based Network Management

The market (both vendors and users) has widely criticized ISO for moving too slowly in its efforts to ratify OSI Management standards. Indeed, the greatest disadvantage to OSI-based network management is that the demand for it far exceeds the available products—and vendors are wisely unwilling to develop products based on standards that are not yet final. In an effort to open the door to new OSI-based network management system products, SC21 WG4 is currently working to finalize fault, configuration, performance, accounting, and security management specifications. These standards will assist in differentiating OSI-based systems from Simple Network Management Protocol (SNMP)-based products.

Another disadvantage to standards-based network management is that OSI standards merely provide a menu of options. There are numerous gaps and ambiguities in OSI Management standards that could be interpreted differently, leading to incompatible implementations. Industry consensus is the only hope for interoperable implementations. Currently, this consensus is building around the Network Management Forum and the Network Management Special Interest Group (NMSIG) of the OIW, sponsored by NIST and the IEEE. The NMSIG is developing Implementation Agreements (IAs) based on emerging network management standards. IAs are being introduced in phases that coincide with ISO/IEC standards as they progress from CD to international standards. The OIW NM Phase I IA became stable in December 1990.

To further simplify government procurement of network management products, NIST introduced a proposal in 1991, called the Government Network Management Profile (GNMP). GNMP will also be introduced in phases that will cross-reference the latest GOSIP versions. GNMP Phase I, II, and III will address the following categories of management information:

- Phase I—IEEE 802 LAN standards, X.25, ISDN, FDDI, modems, multiplexers, bridges, and the physical link of the OSI model.
- Phase II—protocol software operating in Layers 3 to 7, routers, terminal servers, MTAs, PBX, and circuit switches.
- Phase III—applications, services, operating systems, computers, networks, and database management systems.

GNMP Phase I specifies CMIS/P, management definitions in GNMP section 4, and five systems management functions: object management function, state management function, attributes for representing relationships, alarm reporting, and event reporting.

Since SNMP is already widely implemented, it is likely that SNMP will be deployed to manage routers. Future versions of GNMP will specify a network management architecture incorporating both SNMP and GNMP protocols.

Standards Documents

OSI Management standards can be broadly categorized into four areas:

1. Functions—*what* network management is, according to OSI
2. Services—*how* network management functions are accomplished
3. Information Structure—terms and categories describing *what is managed* (e.g., "management information")
4. Protocols—describe *means of transporting* network management information

Taken together, these four areas describe a generic package for network management systems, and how these products relate to the network devices they manage (called *managed objects* in OSI terminology).

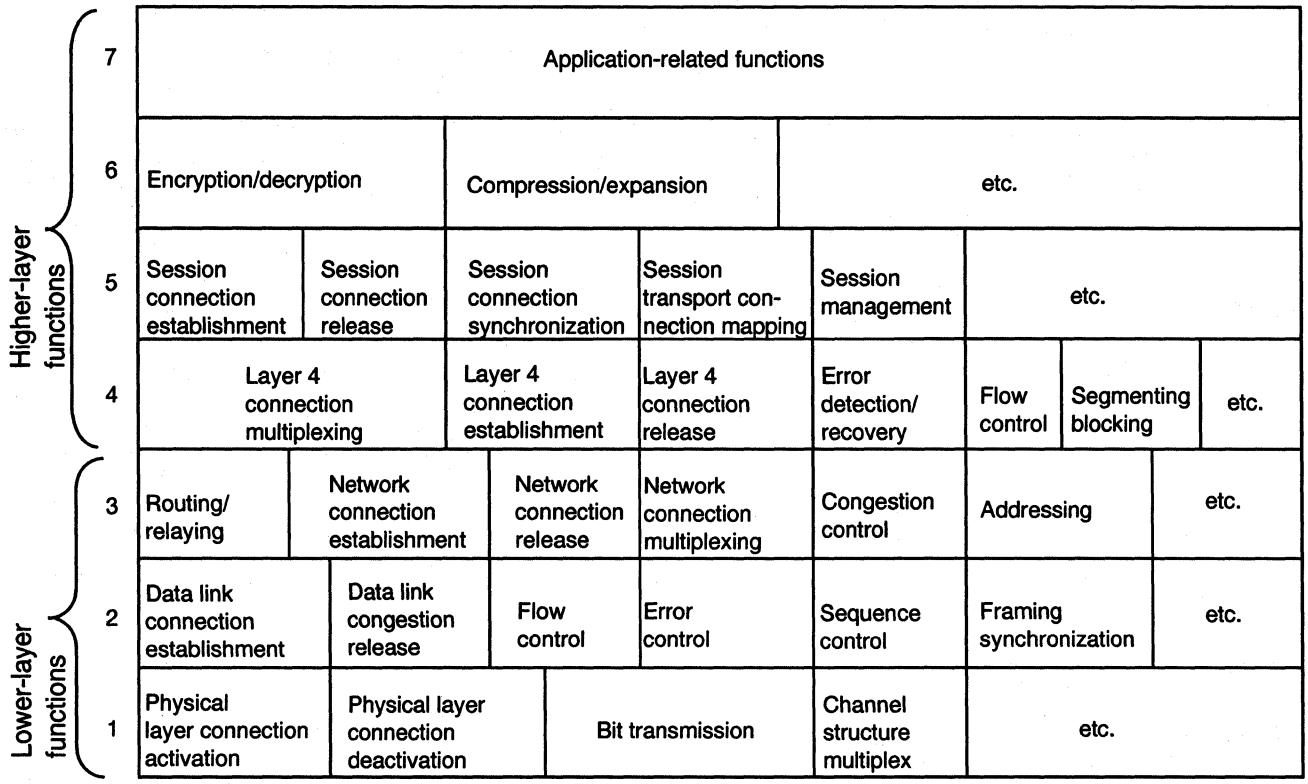
A blueprint document, Management Framework OMNI*Point*, places the OSI Management environment in perspective by describing terms and the scope of OSI network management.

OSI Management Functions

OSI Management functions are described in the Systems Management standards (IS 10040, IS 10164-1 through 10164-7, and N 10164-8 through 10164-12). Management using three models:

1. The Organizational Model—describes ways OSI Management can be distributed administratively

Figure 3.
ISDN Through OSI Eyes



ISDN functions allocated according to layering principles of Recommendation X.200.

2. The Information Model—provides guidelines for defining managed objects and their interrelationships, classes, and names
3. The Functional Model—describes network management functions

The Functional Model outlines how ISO has partitioned network management into five functional areas: fault management, configuration and name management, performance management, accounting management, and security management. ISO originally described each of these areas in its own standard. Further studies revealed that functions overlapped; therefore, ISO reorganized the documents in December 1988 into their present Systems Management form.

Fault management provides the detection, isolation, and correction of abnormalities in network operation. Configuration and name management facilities permit network managers to control the configuration of the system, network, or layer entities. Changed configurations may isolate faults, alleviate congestion, or meet changing user needs. Performance management enables the network manager to monitor and evaluate the performance of the system, network, and layer entities. Data from performance management may be used to initiate configuration changes and diagnostic testing to allow a satisfactory level of performance. Accounting management facilities help determine and allocate costs for the use of a network manager's communications resources. Security management facilities permit the management of those services providing access protection of communications resources.

Services

Services are described, in part, in the Common Management Information Protocol (CMIP) standard, IS 9596. Services use *primitives*, or command types, to accomplish network management functions. Examples of CMIP commands include GET, SET, GET REPORT, CREATE, and DELETE. While service primitives are somewhat abstract, they are important building blocks for composite commands used by network management applications to obtain vital data on the status and activity of network devices.

Common Management Information Services (CMIS) include a detailed abstract model of open systems management services. These fall into three categories—event notification, information transfer, and control. Event notification allows one system to notify another that some event of importance has occurred.

Information Structure

The most important standards in this category are Structure of Management Information (SMI), Parts 1, 2, and 4 (CD 10165-1, -2, and -4). (Part 3 is not missing; rather, ISO merged Part 3 into Part 4.) Included in these standards is an explanation of the *object-oriented* paradigm, used to model a network in terms of object classes and attributes. In object-oriented environments, a variable (for example, a variable called Modem) is defined both in terms of the operations that can be performed on it and the values of attributes it can possess. For example, Modem can have an attribute such as Status, which may have a value of On-Line or Off-Line; a network management system may obtain this value via a Get operation or alter it via a Set operation.

Objects (including their attributes and operations) are stored in a Management Information Base (MIB), sometimes called an Object Library. The SMI documents just listed provide syntax

and semantics for information in the MIB; however, as yet no single ISO standard defines exactly what the OSI MIB will contain, nor how vendors and users will register objects in the standard MIB. SC21 WG4 is currently working to finalize the SMI, providing guidelines that can be used to define management objects and their attributes. The final SMI will ensure interoperability among OSI-based network management systems.

In the TCP/IP world, an Internet Standard MIB exists for objects managed using SNMP. This MIB functions in an analogous role to the proposed OSI MIB, although the administration and rules governing the two are sure to differ.

MIB includes all information needed to make management decisions. MIB is a conceptual repository of all OSI management data in an OSI environment. The MIB concept does not imply any form of physical or logical storage for management information, however, and its implementation is outside the scope of OSI standards. Rather, the SMI defines the abstract syntax and the semantics of information so that it can be represented in OSI protocol exchanges.

Protocols

Common Management Information Protocol, IS 9596, is the primary OSI Management protocol. CMIP specifies procedures for the exchange of basic management information between open systems interconnected by OSI protocols. CMIP is intended to be a general-purpose management protocol suitable for the management of both OSI resources and the real resources used to provide communications services.

X.500—The Directory

The Directory is a related standard designed to manage name-related information concerning protocol layers and network nodes. These services connect the actual names used in the network with names and addresses understood by human users. The Directory is defined in CD 9594 and several other OSI working drafts. CD 9594 attained DIS in March 1988.

OSI and the Future

The world needs a network of computers, similar to standards for international telephony, to link users across oceans and continents. A few years ago, most industry analysts perceived OSI as the answer. Although endorsed by such prominent vendors as IBM, Digital, and Hewlett-Packard, OSI's future as the premier means of interconnecting multivendor computer networks is now uncertain. The tremendous growth of the Internet has given TCP/IP a firm base in the United States and the protocol has also been making significant strides in Europe. OSI applications protocols, such as CCITT X.400, X.500, and EDI, are still very popular, however, and lend support to OSI.

The OSI Reference Model has some glitches and holes that prevent it from being widely implemented. In the U.S., OSI and TCP/IP proponents are badly divided. As an internetworking protocol, TCP/IP has proved its worth and is a popular and commercially successful method of linking users across diverse networks—particularly LANs. OSI middle-layer protocols 3 through 5, the alternatives to TCP/IP, are not as simple to implement in the real world. SNMP, the network management protocol for TCP/IP networks, is also a proven, commercially successful solution. As long as vendors and users require practical networking products, they will continue using TCP/IP-based protocols—standards or not.

OSI will most likely evolve to better serve user needs, with an OSI-TCP/IP hybrid a likely compromise. A possible scenario for wider OSI acceptance is that TCP/IP middle layers will migrate to resemble OSI, at least functionally. In many commercial networking applications, however, vendors are blending different protocol stacks from different sources to match user needs. For instance, one vendor's network protocol might graft together different layers from OSI, TCP/IP, and IBM's SNA.

In reality, OSI and other layered architectures do not serve every application and are not a panacea. Proprietary architectures will continue to thrive alongside OSI-based networks, especially for closed user groups (where internetworking is not a requirement) or in time-sensitive applications intolerant of layered protocols' high overhead.

All others who desire internetworking must realize that the associated protocols are still evolving—nothing is truly cast in iron. In market-based economies, products that do not satisfy market needs will not gain widespread favor. Therefore, prospective users must evaluate OSI protocols and their adoption with an eye toward future standards developments. As it stands now, OSI will not be the interconnection standard of the future. Significant portions of it, however, will most certainly contribute to the evolution of an international standard. ■

ISO Reference Model for Open Systems Interconnection (OSI)

In this report:

Synopsis

Editor's Note
The goal of Open Systems Interconnection (OSI) is to enable dissimilar computers in multivendor environments to share information transparently. The OSI structure calls for cooperation among systems of different manufacture and design. With this capability, global digital networks can become a reality.

There are seven layers of the OSI model that communicate between one end system and another. The layers cover nearly all aspects of information flow, from applications-related services provided at the Application Layer to the physical connection of devices to the communications medium at the Physical Layer.

Although all seven layers have long since been defined and ISO protocols ratified for each layer, the ISO committees must keep refining and redefining specific sections of the model by rewriting existing definitions and adding new protocols.

Report Highlights
This report updates the OSI's status at all seven layers; gives the status of OSI standards progress; compares OSI to other architectures, including ISDN, SNA, DECnet, MAP/TOP, and TCP/IP; rationalizes the need for standards testing and verification; profiles major testing organizations; and outlines OSI Management standards and status.

Analysis

The proliferation of computerized data processing systems in the late 1960s produced a need for compatible data communications networks in the 1970s. Several proprietary network architectures were developed for mainframe-to-terminal communications, including IBM's SNA in 1974. Although many of these proprietary architectures were based on a layered model, none were compatible with any other. The CCITT's X.25 host interface to the packet networks standard was ratified in 1976 but is not a complete network architecture. In 1977, the International Organization for Standardization (ISO) formed ISO Technical Committee 97 (TC97), Subcommittee 16 (SC16), to embark on a worldwide standardization effort and confront the issue of incompatibility head-on. The purpose of TC97/SC16 was to develop a model and define the protocols and interfaces required to support an *open system*. The goal of Open Systems Interconnection (OSI) was, and still is, to enable dissimilar computers in multivendor environments to share information transparently. With this capability, global digital networks can become a reality.

The Open System

The ISO defines a *system* as a set of one or more computers and associated software, peripherals, terminals, human operators, physical processes, information transfer means, etc., which form an autonomous whole capable of performing information processing and/or information transfer. An *open system* is one that obeys OSI standards in its communication with other systems.

An *application process* is an element within a system that performs information processing for a particular application. The application process can be manual (a person operating a banking terminal), computerized (a program executing in a computer center and accessing a remote database), or physical (a process control program executing in a dedicated computer attached to industrial equipment and linked to a plant control system).

The OSI structure calls for cooperation among systems of different manufacture and design. This includes coordinating activities such as the following:

- Interprocess communications—the synchronization between OSI application processes and the exchange of information
- Data representation—the creation and maintenance of data descriptions and transformations for reformatting data exchanged between systems
- Data storage—storage media, file systems, and database systems for providing access to and management of stored data
- Process and resource management—how application processes are declared, initiated, controlled, and acquired
- Integrity and security—information processing constraints that must be ensured during open systems operations
- Program support—the definition, compilation, testing, linking, storage, and transfer of and access to programs executed by the application processes

The OSI model is concerned only with the exchange of information between open systems.

The Layering Concept

Layering is a basic structuring technique used in the OSI model. Each layer is composed of an ordered set of subsystems, with logically related functions grouped together. The OSI model breaks down internetworking activities between systems into two distinct groups. Communications-oriented functions are separated from user-oriented functions; features which move information across a network are distinct from features which handle and format information.

There are seven layers of the OSI model that communicate between one end system and another end system. The layers cover nearly all aspects of information flow, from applications-related services provided at the Application Layer to the connection of devices to the communications medium at the Physical Layer. Below the Physical Layer, the media itself corresponding to "Layer 0"—such as wire, cable, or through-the-air communication—is currently not addressed by the model. ▶

Standards Organizations and Testing Agencies

Although standards are indispensable for computer internetworking, they are useless unless vendor claims of compatibility can be tested and users can be assured of acquiring products that comply fully with the standards. In general, vendor claims of standards compatibility are suspect unless verified by an impartial testing agency. Additionally, compatibility claims can mean different things to different people. For users, it is a good idea to probe vendor claims of standards compatibility to determine what is compatible with what, and at what levels.

Several standards testing and verification bodies have been organized both here and abroad by vendor consortiums, government agencies, and independent organizations. They have found that developing conformance specifications, producing testing suites, and conducting comprehensive testing is complicated, expensive, and time consuming. Regional differences can stymie attempts at verification. The trend for these organizations, therefore, is to cooperate with each other, sharing resources and expertise. A primary objective is demonstrating interoperability among different vendors; i.e., proving that standards really work and fostering end-user interest. Many agencies have tried vainly to involve more end users but are backed primarily by the vendors.

In the U.S., primary testing and certification agencies include the Corporation for Open Systems (COS), the National Institute of Science and Technology (NIST), and Bell Communications Research (Bellcore). Several smaller organizations and certain vendors, however, also offer testing services. Europe is represented by the Standards Promotion & Application Group (SPAG); Japan by the Promoting Conference for OSI (POSI). Standards organizations are listed below:

American National Standards Institute (ANSI)
1430 Broadway
New York, NY 10018
(212) 642-4900

ANSI X3 Secretariat
Computer and Business Equipment Manufacturers Association (CBEMA)
Suite 500, 311 First Street, NW
Washington, DC 20001-2178
(202) 737-8888

Bell Communications Research (Bellcore)
60 New England Avenue
Piscataway, NJ 08854-4196
(908) 699-2000
Customer Service Hot Line:
(800) 521-CORE

Corporation for Open Systems (COS)
Suite 400, 1750 Old Meadow Road
McLean, VA 22102-4306
(703) 883-2700
Telex: WUI 6503157578 MCI UW

European Computer Manufacturers Association (ECMA)
Rue du Rhone 114
CH-1204 Geneva, Switzerland
(+41) 22 735 36 34
Telex: 413237 ECMA CH

Electronic Industries Association (EIA)
1722 Eye Street NW, Suite 300
Washington, DC 20006
(202) 457-4900

International Organization for Standardization (ISO)
1, Rue de Varembe
Case Postale 56
CS-1211 Geneva 20, Switzerland
(+41) 22 33 34 30

International Telegraph and Telephone Consultative Committee (CCITT)
General Secretariat
International Telecommunications Union (ITU)
Place des Nations
CH-1211 Geneva 20, Switzerland
(+41) 22 99 51 11
Fax: (+41) 22 33 72 56
Telex: 421 000 UIT CH

Institute of Electrical and Electronics Engineers (IEEE)
Headquarters
345 E. 47th Street
New York, NY 10017
(212) 705-7900
Fax (publications): (212) 705-7682

IEEE Service Center
(published standards:)
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331
(908) 981-1393
Fax: (908) 981-9667
Telex: 833-233

OSINET
Mr. Jerry Mulvenna, Chairman
OSINET Steering Committee
NIST Building 225, Room B217
Clopper Road
Gaithersburg, MD 20899

Standards Promotion & Application Group sa (SPAG)
Avenue Louise 149, Box 7
1050 Brussels, Belgium
(+32) 2 535 08 11
Telex: 20307 SPAG B

National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
Gaithersburg, MD 20899
(301) 975-2000

▶ *(Analysis continued)*

model. Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers have been defined (see Table 1). The model represented by Table 1 is only one end system, in this case the transmitting end; most networks have at least two end systems. In Table 1, information flows down from Layer 7 to Layer 1, and then out over a physical transmission medium. At the receiving end, the information flows into another end system and up from Layer 1 to Layer 7, until it is received by a user.

The seven layers can be divided into two functional groups: the Transport Platform (Layers 1 to 4) and the Application Platform (Layers 5 to 7). The Transport Platform's function is to get data from one system to another without errors. The Application Platform's function is to interpret the datastream and present it to the user in a usable form (see Figure 1).

Each layer contributes functions to the communications task. For example, the Link Layer enables communications across a single physical connection, while the Network Layer provides end-to-end routing and data relay. Services at the upper layer interface—providing connection to the next-higher layer—are provided by each layer, usually described by a service specification for the layer. Services at each layer are provided by a layer entity. Each layer entity communicates with its peer at the same layer on another system, providing services specified in the service specification.

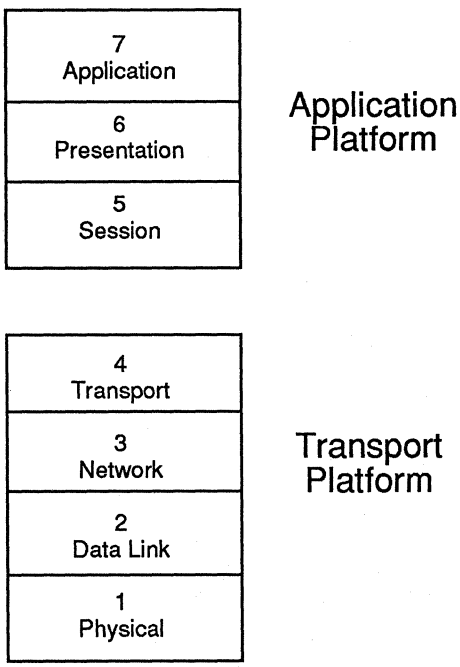
Layers are sometimes divided into sublayers, for several reasons. Layers often need sublayers to handle the service interface of the layer beneath it. This avoids "rewriting" the entire layer. For example, the Link Layer of the IEEE 802 Local Area Network (LAN) standards is divided into a Logical Link Control (LLC) sublayer and a Media Access Control (MAC) sublayer. The MAC sublayer depends on characteristics of the underlying physical layer. Layer independence and modularity are promoted by ensuring that layer entities on one system are not permitted to communicate with nonpeers on another OSI system.

IBM's SNA is also a layered architecture, following rules of layering common to OSI and other layered architectures. Any layer may originate a message to fulfill its responsibilities. The message may not bypass any layer en route to its destination. If a message leaves the node it will end up in another node at the same layer that originated the message.

There are good reasons for layering: layering simplifies change; components inside a layer can be changed without affecting any other layers in that node. Layers are like structured programming—but for teleprocessing systems. Because there are rigid interfaces between levels, fewer people need to react to changes, allowing them to be implemented faster. There is no better way of achieving complex functions. Layering allows each network function to be made "transparent," unaware and independent of other functions at other layers, thus enabling any layer to be modified without changing the entire monolithic architecture.

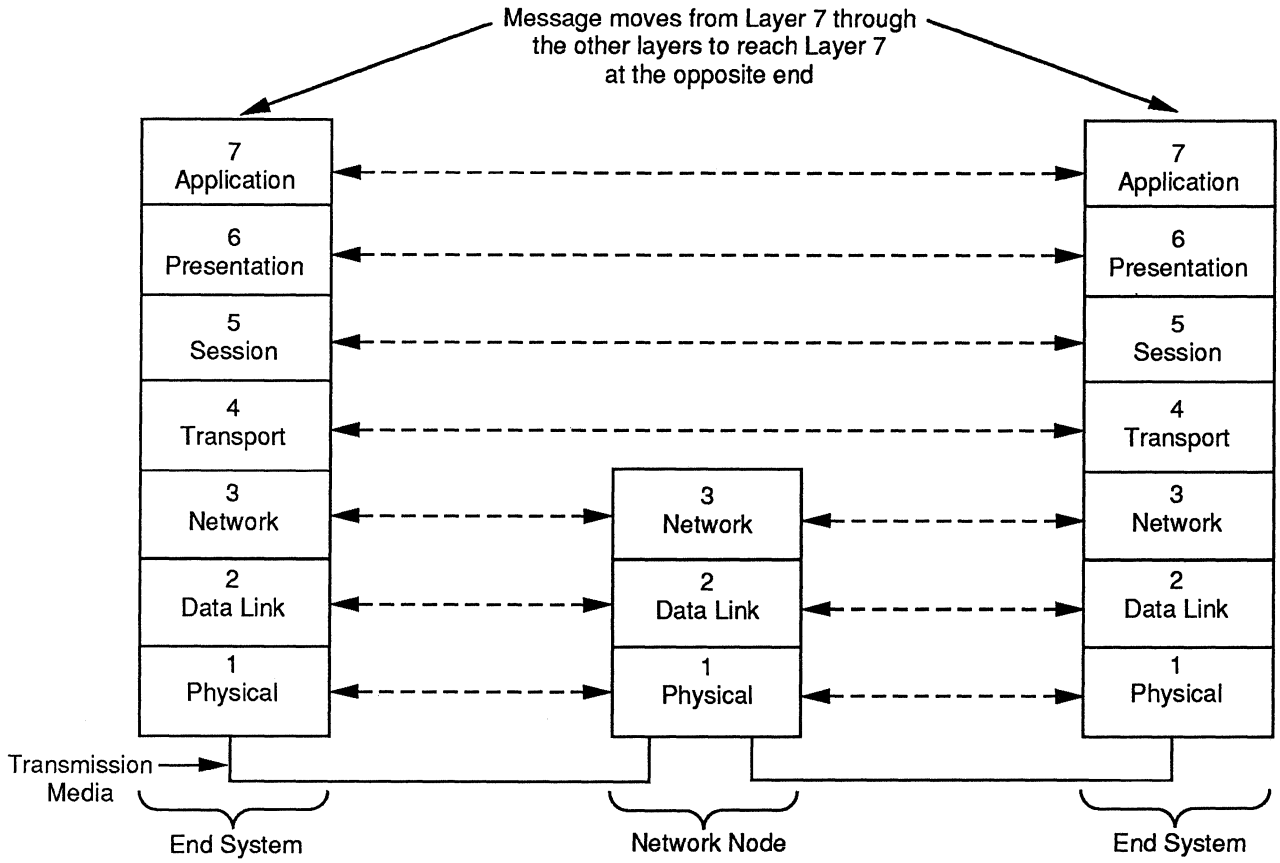
Each layer may support one of several different protocols designed for specific network applications; the choice of a specific protocol is optional, allowing users to tailor networks to their own design. Each layer defines functions crucial to the communications process at that layer, independent of the other layers. However, a layer may perform functions hinging on functions performed in the layers immediately above or below. A layer can

Figure 1.
Application and Transport Divisions



The seven layers are divided into two functional groups.

Figure 2.
Message Movement among OSI Layers



Intermediate nodes in an OSI network require only bottom-layer functions of the OSI model. Note how peer layers communicate only with their peers; i.e., Layer 1 talks to other Layer 1s but not to Layer 2s.

only communicate with another device or network node at its peer layer. Messages exchanged between peer layers are "enveloped" with messages from other layers and passed through these other layers on the way to their destination, picking up and then shedding these other protocol layers along the way. For example, if layer seven at one end system must send a message to layer seven at another, it must travel down through six layers at its own end and then up through six layers at the other, until it reaches layer seven at its opposite (peer) layer.

Each network node (a network user, computer, terminal) is equipped with this layer mechanism. However, not all intermediate nodes need all seven layers. Network nodes, in particular, must only route and transmit data packets—functions at the bottom three layers of the OSI model. Layer four through seven functions are not required and therefore not included in network node software. Data packets processed in these nodes reach only Layer 3 and are then routed elsewhere (see Figure 2). A node communicates with its peer in the node sending or receiving data. Interfaces within nodes allow them to accept, process, and route data. Data transfer is routed from Layer 7 down to Layer 1 at the transmitting node, then along the network to Layer 1 at the receiving node, and finally from Layer 1 up to Layer 7. Peer layers communicate by the same route.

The message initiated at the transmitting node (Layer 7) is passed from layer to layer, each layer adding control information, if required, and acting in accord with control information from its peer in the receiving node. A fully prepared message enters the cable at Layer 1. The procedure is reversed at the receiving end. Each item of control information stops at its appropriate layer, and the message itself passes up to Layer 7. Data transfer essentially is a cumulating process at the transmitting node and a diminishing process at the receiving node.

Table 1. The Seven Layers of OSI

Layer	Name	Purpose
7	Application	Applications and application interfaces for OSI networks. Provides access to lower layer functions and services.
6	Presentation	Formats data received from Layer 7; includes terminal standards, display rules.
5	Session	Coordinates connection and interaction between applications. Establishes a dialog, manages and synchronizes the direction of data flow, and terminates the session.
4	Transport	Ensures end-to-end data transfer between applications, data integrity, and service quality. Assembles data packets for routing by Layer 3.
3	Network	Routes and relays data units among network nodes.
2	Data Link	Transfers data units from one network node to another over a transmission circuit. Ensures data integrity between nodes.
1	Physical	Sends the bit stream to the transmission medium.

The Layers

A number of objectives were considered by the reference model's designers: to limit the number of layers to make the system engineering task of describing and integrating the layers as simple as possible; to create boundaries between layers at points where the description of services can be small and the number of interactions across each boundary is minimized; and to collect similar functions in the same layer. Table 1 summarizes the OSI Reference Model's layers; more detailed descriptions follow for each layer.

The Application Layer

The Application Layer (Layer 7) is the highest layer, providing the means for the application process to access the OSI environment. Its function is to serve as the passageway between application processes using Open Systems Interconnection to exchange information; consequently, all application process parameters are made known to the OSI environment through this layer.

All services directly usable by the application process (i.e., systems and applications management functions) are provided by the Application Layer. It differs from the other layers in that it does not provide services to a layer above it nor is it associated with a service-access point. Some of the services provided by this layer, other than information transfer, are the following:

- Identifying intended communications partners
- Determining current availability of the intended partners
- Establishing the authority to communicate
- Agreeing on responsibility for error recovery
- Agreeing on procedures for controlling data integrity

The Application Layer actually consists of two sublayers. The uppermost sublayer consists of Specific Application Service Elements (SASEs), such as message handling system (X.400), FTAM, Directory Services (X.500), DTP, and Virtual Terminal (VT). The lower sublayer consists of Common Application Service Elements (CASEs), which provide specific services for the upper applications. Examples of CASE protocols include Commitment Concurrency and Recovery Service Element (CCR) and Remote Operation Service Element (ROSE).

The Presentation Layer

The Presentation Layer (Layer 6) allows an application to interpret the meaning of information exchanged. Information is formatted and translated

Table 2. ISO Protocols and Equivalent Standards

Layer	ISO	CCITT	ANSI	ECMA
7	8571 (FTAM)	—	—	—
Application	10021 (MHS)	X.400	—	—
	9041 (VT)	—	—	—
	10026 (DTP)	—	—	—
	9594 (DS)	X.500	—	—
	8613 (ODA)	T.410 Series, T.73	—	ECMA-101
	9579 (RDA)	—	—	—
	9596 (CMIP)	—	—	—
6	8823 (connection)	X.226	—	—
Presentation	9596 (connectionless)	—	—	—
5	8327 (connection)	X.225	X3.153	ECMA-75
Session	9548 (connectionless)	—	—	—
4	8073 (TP0-TP4) (connection)	X.224	X3.140	ECMA-72
Transport	8602/8072 (connectionless)	—	—	—
3	8208 (Layers 1-3)	X.25	—	—
Network	8348 (connection)	X.213	—	—
	8473 (connectionless)	—	—	ECMA-92
	9542 (IS-IS)	—	—	—
	8878 (use w/8208)	(X.25)	—	—
	8880 (LAN)	—	—	—
	8881 (X.25 on LANs)	—	—	—
2	7776 (LAPB)	X.25	—	—
Data Link	3309 (HDLC)	—	X3.66	ECMA-40
	8802.2-.7 (LAN) (IEEE 802.2-.7)	—	—	ECMA-82, -81, -90, -89
1	9314 (FDDI)	—	X3.148, X3.139, X3.166	—
Physical	2110 (EIA-232D)	V.24, V.28	—	—
	4902 (EIA-449)	V.24, V.28	—	—
	2593	V.35	—	—
	4903	X-Series interfaces, Other V-Series	—	—

at this layer. Aspects of Layer 6 include data syntax, which is the data to be transferred between layers, and the presentation image syntax, which is the data structure that application entities refer to in their dialog, or the set of actions that may be performed on the data structure.

Services provided to the Presentation Layer include the following:

- Transforming data syntax, primarily code and character set conversion
- Transforming and selecting the presentation image syntax, the adaptation and modification of the presentation image (the OSI view of the data structure)

Functions within the Presentation Layer include session establishment request; data transfer; negotiation and renegotiation of data syntax and presentation image syntax; special data transformations, such as compression; and session termination request.

The Session Layer

The Session Layer (Layer 5) allows cooperating presentation entities to organize and synchronize their dialog and to manage data exchange. It provides the following services:

- Session-connection establishment—creation of an exchange between presentation entities
- Session-connection release
- Normal data exchange
- Quarantine service—in which data units sent by a presentation entity are withheld from the receiving presentation entity until released by the sending presentation entity
- Expedited data exchange
- Interaction management—allowing presentation entities to take turns exercising control functions
- Session-connection synchronization

Table 3. OSI Network Management Standards

Title	Current Status	Finalization Date
CMIS/CMIP		
Common Management Information Service (CMIS) (IS 9595)	International Standard	Final 11/89
CMIS CancelGet Addendum (AD 9595-1)	Addendum	Final 11/90
CMIS Add/Remove Addendum (AD 9595-2)	Addendum	Final 11/90
Support for Allomorphism (Amendment to CMIS) (CD 9595)	New Work Items	DIS expected in 11/91; IS expected in 11/92
Access Control (Amendment to CMIS) (CD 9595)	New Work Items	DIS expected in 11/91; IS expected in 11/92
Common Management Information Protocol (CMIP) (IS 9596)	International Standard	Final 11/89
CMIP CancelGet Addendum (AD 9596-1)	Addendum	Final 11/90
CMIP Add/Remove Addendum (AD 9596-2)	Addendum	Final 11/90
Support for Allomorphism (Amendment to CMIP) (CD 9596)	New Work Items	DIS expected in 11/91; IS expected in 11/92
PICS Proforma (Amendment to CMIP) (CD 9596)	New Work Items	DIS expected in 11/91; IS expected in 11/92
OSI Systems Management Functions		
OSI Systems Management Overview (DIS 10040)	Draft International Standard	IS 5/91
Object Management Function (DIS 10164-1)	Draft International Standard	IS 5/91
State Management Function (DIS 10164-2)	Draft International Standard	IS 5/91
Attributes for Representing Relationships (DIS 10164-3)	Draft International Standard	IS 5/91
Alarm Reporting Function (DIS 10164-4)	Draft International Standard	IS 5/91
Event Management Function (DIS 10164-5)	Draft International Standard	IS 5/91
Log Control Function (DIS 10164-6)	Draft International Standard	IS 5/91
Security Alarm Reporting Function (DIS 10164-7)	Draft International Standard	IS 5/91
Security Audit Trail Function (CD 10164-8)	Committee Draft*	DIS 4/91
Objects and Attributes for Access Control (CD 10164-9)	Committee Draft*	DIS 4/91
Accounting Meter Function (CD 10164-10)	Committee Draft*	DIS 4/91
Workload Monitoring Function (CD 10164-11)	Committee Draft*	DIS 4/91
Confidence and Diagnostic Testing Classes, Test Management Function (N4078, 10164-X)	Committee Draft*	DIS expected 8/91; IS expected 8/92
Measurement Summarization (N4081, 10164-X)	Committee Draft*	DIS expected 8/91; IS expected 8/92
Response Time Monitoring (N4079, 10164-X)	Committee Draft*	DIS expected 8/91; IS expected 8/92
Software Management Function (10164-X)	New Work Item	DIS expected 7/92; IS expected 7/93
Time Management Function (10164-X)	New Work Item	DIS expected 8/92; IS expected 8/93
Structure of Management Information (SMI)		
Management Information Model (DIS 10165-1)	Draft International Standard	IS 5/91
Definition of Management Information (DIS 10165-2)	Draft International Standard	IS 5/91
Guidelines for Definition of Managed Objects (DIS 10165-4**)	Draft International Standard	IS 5/91
Generic Managed Objects (N4075)	Working Draft	DIS registration dates to be determined

**Draft proposals (DPs) are now referred to as Committee Drafts (CDs).*
***Document DIS 10165-3 was merged with DIS 10165-2 and will not appear in future standards listings.*

- Exception reporting—permitting the presentation entities to be notified of exceptional situations

An example of a working Layer 5 protocol outside the scope of OSI is the Department of Defense Transmission Control Protocol (TCP).

Table 3. OSI Network Management Standards (Continued)

Title	Current Status	Finalization Date
Specific Management Functional Areas (SMFAs)		
Performance Management (N4981)	Working Draft	Next milestone to be determined
Accounting Management (N875R)	Working Draft	Next milestone to be determined
Security Management (N4091)	Working Draft	Next milestone to be determined
Fault Management (N4077)	Working Draft	Next milestone to be determined
Configuration Management (N3311)	Working Draft	Next milestone to be determined
Related Upper Layer Standards		
OSI Management Framework (IS 7498/4)	International Standard	Final 4/89
File Transfer, Access and Management (FTAM) (ISO 8571)	International Standard	Final 10/88
Association Control Service Element (ACSE) (ISO 8649, plus addendums)	International Standard	Final 12/88
Remote Operations Service Element (ROSE) (IS 9072-1&2)	International Standard	Final 11/89

The Transport Layer

The Transport Layer (Layer 4) provides transparent data flow between session entities, freeing the Session Layer from responsibility for cost-effective and reliable data transfer. Layer 4 provides information interchange according to a user-specified reliability level and end-to-end control. Transport protocols transfer information from one end of a physical connection to another and ensure that it is delivered correctly. Layer 4 protocols are used after a route has been established through the network by the network-layer protocol.

The services provided by this layer include the following:

- Transport-connection establishment to complete a connection between session entities
- Data transfer, in accordance with the agreed quality of service
- Transport-connection release

The Transport Layer is the most defined of the upper four layers. The European Computer Manufacturers Association (ECMA) has defined this layer in its Transport Protocol standard, ECMA-72. This standard has gained the support of a number of North American and European computer manufacturers. An end-to-end data transport protocol outside the scope of OSI is the Department of Defense Internet Protocol (IP).

The Network Layer

The Network Layer (Layer 3) provides the means to establish, maintain, and terminate connections between systems. Its basic service is providing transparent data transfer between transport entities.

The services provided by this layer encompass the following:

- Establishing network connections for transporting data between transport entities through network addresses
- Identifying connection endpoints
- Transferring network service data units
- Noting errors for reporting unrecoverable errors to the transport layer
- Sequencing network control data units
- Flow control
- Releasing the network connection

The Data Link Layer

Data Link Layer 2 provides the procedural and functional means to establish, maintain, and release data link connections between two network nodes or network entities and to transfer data frames (or packets). This layer also detects and may correct errors that occur in the physical layer.

Services provided by the Data Link Layer to the Network Layer include data link connection, sequencing, error notification, flow control, and data unit transfer.

The Physical Layer

The lowest of the OSI layers is Physical Layer 1. It provides the electrical, mechanical, functional, and procedural characteristics for activation, maintenance, and deactivation of a physical connection. Physical Layer standards specify physical interfaces (connectors) connected by a physical medium.

Services provided by this layer include the following:

- Activating and deactivating physical connections
- Data circuit identification
- Sequencing
- Transmitting physical service data units either synchronously or asynchronously
- Fault condition notification

Abstract Syntax Notation One (ASN.1)

ASN.1 is a *specification language* adopted for the OSI Reference Model, giving standards developers a common method for defining protocols and related standards. ASN.1 is somewhat analogous to grammatical rules defining the English language. Just as English grammar specifies notation (punctuation symbols) and word classifications (such as nouns and verbs), ASN.1 specifies a "grammar" and rules that help standards developers define complex data types in terms of simple building blocks.

ASN.1 was derived from the Backus-Naur Form, used to describe programming languages such as Pascal and Ada. ASN.1 was first formally described and published in 1984, in the CCITT X.409 standard entitled "Message Handling Systems: Presentation Syntax and Notation." It is now described (in less readable fashion) in two later documents: CCITT X.208 (ISO 8824), entitled "Specification of Abstract Syntax Notation One (ASN.1)," and X.209 (ISO 8825), "Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)."

According to ASN.1, each fragment of information must possess a type and a value. For example:

- **Device-Status** could be a type (in this case, it is a Boolean type)
- **Zero** or **One** are the possible values

This is specified in ASN.1 notation as such:

Device-Status ::= Boolean
Boolean ::= 0 1 1

This is a very simple example; ASN.1 is a powerful grammar, capable of specifying very complex data types. Hence, it will continue to be the grammar of choice for specifying open systems standards and protocols.

OSI Standards Progress

The primary responsibility for developing OSI management standards in the United States rests with American Standards Committee (ASC) X3T5.4. There are four stages in the development cycle: working paper, committee draft (CD), previously known as a draft proposal), draft international standard (DIS), and international standard (IS). A working paper is developed in the first stage. When it matures and contains well-developed technical concepts, it is registered as a CD. Passage advances the CD to the DIS level, and the document is considered sufficiently stable to serve as the basis of initial implementations. At the DIS level, the document is distributed for a 180-day ballot. The DIS may require multiple ballots. A successful ballot elevates the DIS to the level of IS and completes ISO's process.

The entire process usually takes between four and eight years. A list of standards organizations associated with the OSI Reference Model is given at the end of this report.

The Evolution of OSI Committees

In the spring of 1977, ISO Technical Committee 97 (TC97) formed a special subcommittee (SC16) charged with developing an architectural model that would extend from applications-layer communications clear down to the connection with the physical interface. The first draft of the seven-layer OSI Reference Model was completed in 1978. Between 1978 and 1983, the Basic Reference Model and many of the standards for the individual layers

approached or attained draft international standard status. By the end of 1984, SC16 was reorganized to form Subcommittee 21 (SC21). Working groups within SC16 were also realigned.

The OSI Basic Reference Model became an international standard in 1984. During 1985, a number of vendors demonstrated products that implemented these standards and, by the end of 1986, many of these products were commercially introduced.

In July 1987, the Joint Technical Committee for Information Technology (JTC1) was formed when ISO/TC97 joined forces with Technical Committee 83 (TC83) of the International Electrotechnical Commission (IEC). The IEC is a coalition of industrial standards bodies that is colocated with the ISO in Geneva, Switzerland. The new JTC1 held its first meeting in 1987. The standardization activities of SC21 report to JTC1.

SC21 is composed of member bodies (MBs) from 23 different countries. Each MB has its own national standards organization; for example, ANSI represents the United States in JTC1. The individuals or "national correspondents" comprising the MB delegations come from different groups including user organizations, manufacturing firms, government agencies, and common carriers or PTTs. As such, they bring varying perspectives and concerns to the committee sessions.

When an OSI committee or working group produces a document such as a CD, the document is circulated among the MBs for a vote and to the liaison organizations (LOs) for review. LOs are independent organizations which also have a vested interest in OSI development. LOs provide comments on the content of OSI documents but do not have voting privileges.

Status of OSI Protocols

Protocol standards for all seven layers of the OSI model have been approved; however, OSI committees are refining and extending some standards as required and may add new standards at specific layers (particularly Layer 7). Additionally, other standards groups—such as the CCITT, ANSI, and IEEE—may adopt OSI protocol standards as their own and vice versa. Consequently, many OSI standards are known by more than one standard designation. Table 2 shows some major ISO protocols approved for each OSI layer and lists corresponding appellations from ANSI, the CCITT, and the European Computer Manufacturers Association (ECMA), where applicable.

OSI Applications Standards

ISO committees are working hard at Layer 7, the Application Layer. In fact, OSI application standards are perceived as potentially powerful and versatile and are the driving force for OSI market acceptance. We devote considerable space reviewing some of the most important ones here.

In particular, the ISO electronic mail standard for message handling systems (MHSs)—or CCITT X.400—is becoming popular in commercial implementations. Two versions, one in 1984, and another in 1988, are draft international standards that have not been ratified. The standard was given a big boost in 1989, when the Aerospace Industry Association (AIA) adopted X.400 to interconnect its diverse electronic mail networks. Gateways to proprietary E-Mail systems were also developed that year, and dozens of vendors have rolled out X.400-based products. Most public E-Mail carriers have also adopted the standard and are migrating to the 1988 version.

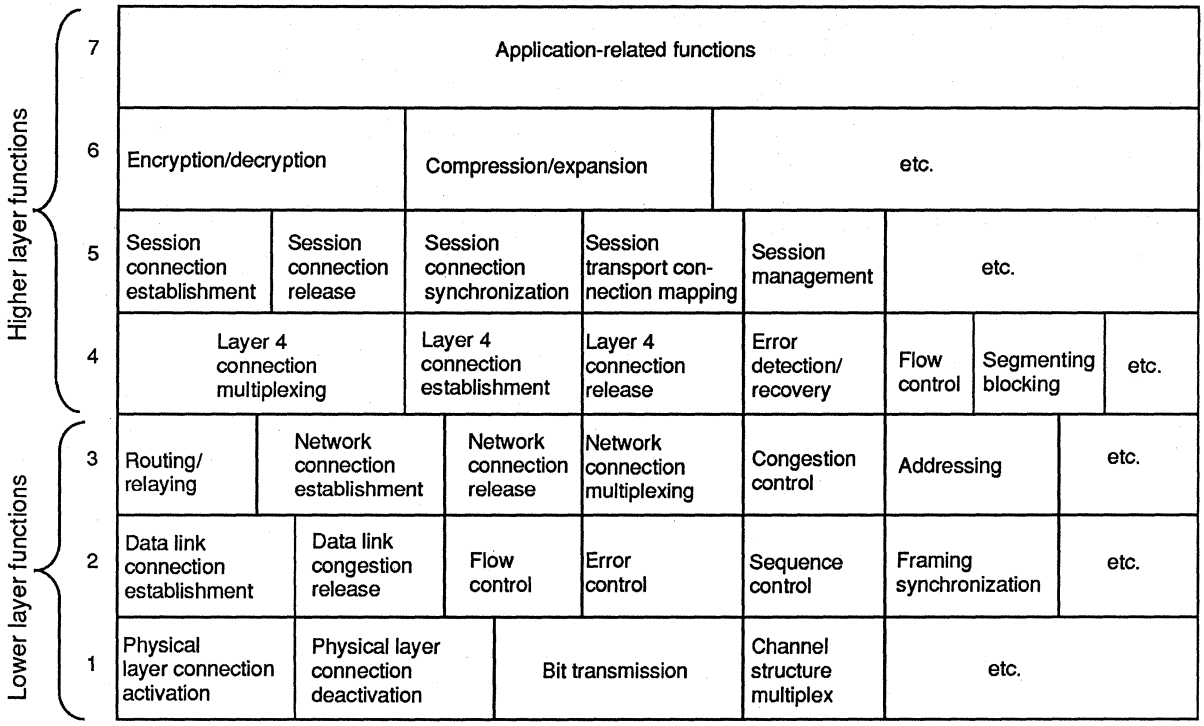
In addition, the ISO is adapting X.400 as the message medium for electronic data interchange (EDI). In this context, X.400 would be used as the communications method to store and forward trade documents and business forms conforming to ANSI X12, the European EDIFACT, and de facto EDI standards.

One component of successful E-Mail internetworking is directory services (DS), commonly known as CCITT X.500. X.500 specifies an online directory for message communications, ultimately allowing network providers to map a common, interconnected directory of worldwide users. X.500 dictates naming conventions, how users access directory information, and what services are available.

Since the 1988 standard is not flexible, SC21 WG4 is working to ease the transition to the new 1992 version. Older 1988 X.500 systems will require a software modification to work with the 1992 version. Realistically, the vision of a worldwide messaging directory probably will not be realized until the late 1990s.

The OSI protocol pair for office automation, Office Document Architecture (ODA) and Office Document Interchange Format (ODIF), has been an international standard since 1988 (ISO 8613). It

Figure 3.
ISDN through OSI Eyes



ISDN functions allocated according to layering principles of Recommendation X.200.

is also specified in the U.S. government's GOSIP standard. ODA and ODIF facilitate the exchange of office documents—such as letters, memoranda, and business reports—among dissimilar systems. Moreover, the standard specifies the formatting and exchange of compound documents—those containing combinations of text, images, and graphics. Several ISO working groups are attempting to strengthen and extend the standard in such areas as the inclusion of audio, spreadsheet data, color graphics, document security, and various layout and presentation styles.

The OSI standard for sending and sharing data files—File Transfer, Access, and Management (FTAM)—is also a finalized international standard. It was developed from networking efforts in the manufacturing industry and is a Layer 7 component of the Manufacturing Automation Protocol (MAP). Although FTAM is spreading quickly in Europe, it is also making some progress in domestic business applications. The file protocol used with TCP/IP—File Transfer Protocol (FTP)—is well established in the U.S., however, and generally more popular than FTAM. SC21 is working on an enhancement to FTAM, and it plans to establish conformance testing guidelines in the near future.

The Layer 7 protocol for network management, Common Management Information Protocol (CMIP), was approved as a draft standard in late 1989. CMIP itself is merely a way of communicating between the "management process" and management agents at each lower layer of the OSI model. The real work of managing network processes is located within the managed objects at individual OSI layers; in other words, each layer must have its own network management system, which OSI does not specify. CMIP allows a centralized management process to either modify the value of an attribute or request its value (read its status) at each of the layers. Definitions and descriptions of management structures and managed information are contained in other OSI standards yet to be completed. (For more information, see the OSI Management section featured later in this report.)

Other Layer 7 protocols in various development stages include distributed Transaction Processing (TP), currently a committee draft designed to interconnect different transaction computing systems across OSI networks; Remote Database

Access (RDA), a committee draft describing a protocol for integrating database management systems; and Manufacturing Message Specification (MMS), ISO 9506, a manufacturing protocol that requires extensions for specific manufacturing device types.

Middle Layer Protocols

During 1987 and 1988, the ISO finalized protocol standards for middle layers 4, 5, and 6. These standards were based on a previous agreement that all connections would conform to a connection-oriented method of establishing circuits.

Every layer of the OSI Reference Model, except the Physical Layer, supports connection and connectionless mode. Connection-oriented service requires a connection establishment phase, a data transfer phase, and a connection termination phase; a logical connection is set up between end systems prior to data exchange. These phases define the necessary sequence of events for successful data transmission. Connection-oriented service capabilities include data sequencing, flow control, and transparent error handling.

In a connectionless service, such as new Switched Multi-megabit Data Service (SMDS), each Protocol Data Unit is independently routed to the destination; no connection establishment activities are required, since each data unit is independent of the previous or subsequent one. Connectionless-mode service transfers data units without regard to establishing or maintaining connections. In connectionless mode, transmission delivery is uncertain due to the possibility of errors. This appears contrary to the goal of network design—users want to ensure that messages reach their destination. In reality, connectionless-mode communication simply shifts responsibility for message integrity to a higher layer, which checks integrity only once, rather than requiring checks at each lower layer. Alternatively, each data unit might contain the error recovery mechanism.

Lower Layer Protocols

Lower layer OSI protocols for layers 1 through 3 are well-defined veterans and in many cases borrowed from existing EIA, IEEE, or CCITT standards. Connectionless communications at the lower layers of the OSI model is well established and is found, for example, in local area networks (LANs) and metropolitan area networks (MANs).

While the original OSI model—described in ISO 7498—was connection oriented, the ISO foresaw the need for connectionless service and issued an addendum to that protocol (ISO 7498/AD1). The ISO is now working to update the Connectionless Addendum, and CCITT SG VII pursues a parallel process. The CCITT, however, has been reluctant to insert connectionless-mode data transmission concepts into CCITT X.200—its version of the OSI model. The ISO standard for Network Layer service, ISO 8348, contains connectionless service (in AD1) in addition to the connection mode.

The Government's GOSIP Standard

In 1979, the National Bureau of Standards (now the National Institute of Standards and Technology—NIST) initiated a program to support U.S. government standards for interoperable data communications. It chose to develop a standard based on the ISO's OSI Reference Model, named the Government OSI Protocol (GOSIP). Since August 1990, NIST has mandated GOSIP as a federal information processing standard (FIPS). All federal agencies must conform to GOSIP in procuring networking products. According to NIST, the standard will be updated every year, and each new version will be compatible with the preceding one.

GOSIP is also expected to accelerate the development of OSI standards and products for the private sector. As the largest user of information processing systems and services in the world, the federal government greatly influences vendors in the computer and communications industries. The need for government GOSIP compliance will spur the development of OSI protocols and software products.

GOSIP Version 1 specifies the following protocols for each OSI layer:

- *Application Layer 7:* File Transfer, Access, and Management (FTAM); X.400 Message Handling System (MHS); and the Association Control Service Element (ACSE)
- *Presentation Layer 6:* ISO 8823/CCITT X.226
- *Session Layer 5:* ISO 8327/CCITT X.225
- *Transport Layer 4:* ISO 8073, Transport Protocol Class 4 (TP4)
- *Network Layer 3:* ISO 8473 Connectionless Network Layer Protocol (CLNP)

- *Data Link Layer 2:* ISO 3309 (HDLC); ISO 8802.2-5/IEEE 802.2-5
- *Physical Layer 1:* GOSIP does not mandate specific physical interface standards but suggests standard interfaces such as EIA RS-232-C for transmission speeds up to 19.2K bps and CCITT V.35 for speeds above 19.2K bps

GOSIP Version 2.0 became mandatory in August 1991. It adds the following protocols to the existing GOSIP model:

- *Application Layer 7:* Basic Class Virtual Terminal (VT), ISO 9040, ISO 9041, ISO 9040 AD1, and ISO 9041. Office Document Architecture (ODA), ISO 8613-8.
- *Transport Layer 4:* Connectionless Transport Service, ISO 8602.
- *Network Layer 3*: Connection-Oriented Network Service for ISDN or X.25 networks, ISO 8348 and 8348/AD1. Intermediate System to Intermediate System (IS-IS) intradomain routing, ISO 9542. Integrated Services Digital Network (ISDN), CCITT I.451 and Q.931.
- *Data Link Layer 2:* ISDN CCITT I.441 and Q.921 (Link Access Protocol D—LAPD).

By supporting ISDN, Version 2.0 will also support CCITT X.25 packet interfaces and IEEE 802.2 to 802.6 LAN networks. GOSIP Version 3.0, which becomes mandatory in August 1992, adds OSI network management, X.500 directory services, the Fiber Distributed Data Interface (FDDI) standard, and Open Document Architecture (ODA). Complete GOSIP details can be obtained from NIST publications *Government Open Systems Interconnection Profile Users' Guide* (SP 500-163) and *Government Open Systems Interconnection Profile* (FIPS PUB 146).

OSI Security

By definition, an open system is one that encourages communications between different applications or users. Unfortunately, an open system can also encourage illegal eavesdropping and information theft or destruction. Recently, notorious examples of white-collar crime, corporate espionage, and network intrusions by computer worms and viruses have alarmed information processing professionals and raised a general awareness of computer security issues. The concepts of information security and open systems are antithetical; nevertheless, the ISO has taken steps to provide a secure environment within the OSI Reference Model.

International Standard 7498, Part 2 addresses a security architecture within the general OSI model. It describes security measures that can be provided by specific layers in the model. Specific security standards are not yet defined, however, but are under study by working group JTC1, Subcommittee 27 for Information Technology Security Standards, plus other subcommittees. The U.S. participant in this process is ANSI's X3 Committee.

SC21, concerned with maintaining and defining the upper three layers of the OSI Reference Model, met in May 1991, in Arles, France, to stabilize several network management and security standards. The Security model is composed of six frameworks that work together across all seven layers of the OSI Reference Model: authentication, access control, security audit, nonrepudiation, confidentiality, and integrity. SC21 is working to establish two of the six security standards as Draft International Standards (DISs), and the remaining four standards, which are working drafts, will progress to CD status.

OSI and Other Network Architectures

OSI and ISDN

Functioning as the international voice of the telephone industry, the CCITT worked independently of ISO to develop its Integrated Services Digital Network (ISDN) technology. On the other hand, CCITT and ISO efforts are closely related because of expanding digital telephone networks and the merging of voice and data.

Increasingly, the OSI Reference Model and ISDN overlap. The ISO has adopted versions of CCITT X.21 and X.25 standards for the lower layers of the OSI model. ISDN functions are described in terms of the seven-layer OSI model in the CCITT's Recommendation X.200 (see Figure 3). Altogether, about 10 standards adopted by both CCITT and ISO are identical, except for introductory paragraphs and identification numbers.

ISDN standards are now mapped to the OSI Reference Model and occupy its lower layers. Specific network applications, such as network management and electronic mail, occupy the higher

OSI layers and can be integrated on top of ISDN protocols in telephony networks. ISDN will provide a more versatile communications medium for integrating telephony and data processing. The U.S. government has already specified ISDN protocol options for its GOSIP network architecture, which is modeled on OSI. NIST has successfully tested ISDN as a transport subnetwork for higher layer OSI protocols. ISDN is expected to be implemented throughout the public telephone network by late 1992. OSI and ISDN are complementary standards that will allow effective internetworking.

OSI and Proprietary Architectures

Until 1976, the only de facto network standards were those developed by IBM for its Systems Network Architecture (SNA). That year, however, CCITT introduced its X.25 standard for host interface-to-packet networks, and Digital Equipment Corp. brought out its Digital Network Architecture (DNA). When the ISO defined its OSI Basic Reference Model (ISO 7498 and 7498/AD1) in 1979, users had a non-IBM alternative for the first time. The purpose of the OSI model—interoperability in a multivendor environment—was fundamentally different from the proprietary nature of SNA.

Although OSI and SNA are both seven-layer network architectures, the layers do not match exactly and are incompatible. At first, IBM paid lip service to customer requests for OSI functionality. The vendor did not embrace OSI within SNA; instead, it provided an OSI gateway between SNA and other non-SNA networks. Like most gateways, this solution proved unwieldy and unsatisfactory. IBM also provided partial OSI solutions at various layers, such as X.25 connectivity at Layer 3 and below. Another interim OSI product was the Open Systems Message Exchange (OSME), an E-Mail package conforming to CCITT X.400.

Increasingly, pressure from customers demanding open, nonproprietary platforms has forced IBM and other major companies, such as Digital Equipment Corp. and NCR, into a mainstream OSI approach.

In 1988, IBM announced OSI/Communications Subsystem, mainframe-based (MVS) software supporting layers 3 to 6 OSI protocols in an SNA environment. In 1989, both IBM and Digital Equipment joined in the OSI/Network Management Forum, a group that was formed to study interoperability among network management systems. In 1990, IBM delivered Release 1.1 of its OSI Communications Subsystem supporting OSI layers 3 to 6 protocols in a multivendor environment and announced SystemView, an OSI-based network and systems management architecture.

IBM now supports three major networking standards: OSI, TCP/IP, and FDDI. However, in early 1991, the company announced that full deployment of its SystemView will be delayed until 1994 or 1995.

This year, after delaying Phase V product introduction, Digital Equipment introduced a new networking architecture for incorporating OSI into DECnet, called Advantage-Networks. Digital designed Advantage-Networks to replace DECnet/OSI Phase V. The new architecture enables users to transmit data from among OSI, TCP/IP, and DECnet applications and network management is supported with Digital's Enterprise Management Architecture (EMA).

In the past, relatively smaller vendors were generally more amenable to adopting OSI standards. Standard Telephone and Cable/International Computers, Ltd. (STC/ICL), for example, was one of the first European manufacturers to ensure that American and European standards efforts are coordinated. STC/ICL is a British information systems firm that perceives adoption of OSI standards as a way to increase the applicability of its own products on an international level.

NCR is expected to roll out its OSI-based router in 1992, as well as its OSI-based Communications Processor software for the 56X5. The company was supposed to have made them available last April, just before the introduction of its new System 3600 parallel processor. However, development problems have delayed delivery until next year. All of NCR's products are based on its Open Cooperative Computing Architecture (OCCA), which provides for the coexistence and information exchange among OSI, SNA, and TCP/IP networks. OCCA will be the platform used by AT&T and NCR to achieve global networking.

OSI and MAP/TOP

The Manufacturing Automation Protocol (MAP) and Technical Office Protocol (TOP) were originally developed by General Motors and Boeing Computer Services, respectively, to automate manufacturing functions on the factory floor and in the

"back office." Both are based on the OSI Reference Model, using formal standards for each layer where possible. MAP, in particular, is probably the best-known example of a formal multilevel protocol and has achieved moderate industry acceptance. Many vendors now offer MAP 3.0 products, but these compete with proprietary "shop floor" automated factory solutions.

Today, manufacturing networking standards are directed by the MAP/TOP users group. MAP Version 3.0 was released in June 1988 and will remain free from major changes until 1994. Version 3.0 added a Presentation Layer to the protocol and implemented a version of the Manufacturing Message Specification (MMS), the protocol for transferring factory and robotics information, ISO 9506. The ISO is currently working to extend MMS in support of realtime applications. Other Layer 7 protocols specified are FTAM, Network Management, and Directory Service. Middle layers implement ISO connection-oriented protocols, although these must be bypassed for time-critical applications. At the lower transport layers, MAP specifies the IEEE 802.4 token bus system employing a Type F coaxial connection to a 75-ohm cable.

OSI and TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) was developed by the U.S. government's Defense Advanced Research Projects Agency (DARPA) for its research network, ARPANET. By 1986, TCP/IP had gained a following of commercial users seeking a protocol that could be used as a common denominator for multivendor computer networks. TCP and IP are actually two separate protocols, occupying middle layers number four (transport) and number three (network), respectively, of the OSI Reference Model.

TCP/IP has been implemented on almost every type of computer and is especially successful in commercial Ethernet LAN environments. The reason for TCP/IP's popularity is that it is a relatively simple, proven system for internetworking. Its handling of the connection-oriented/connectionless dilemma, which can be problematic in OSI, is straightforward and easy to implement. OSI provides a richer set of network options, but these may not be compatible in different networks. Users cannot communicate across different networks if they implement different options at these layers.

Already, some proprietary stripped-down versions of OSI have been developed that resemble TCP/IP, and some pundits believe that OSI itself will evolve to resemble TCP/IP in the future. TCP/IP's future could have been jeopardized, since the U.S. government mandated OSI compliance in government procurements, had it not been for Novell's introduction earlier this year of a new version of its NetWare network operating software that supports TCP/IP.

A majority of users still use TCP/IP networks for LAN interconnectivity. However, the consensus is that TCP/IP is not the ultimate solution—a feat attributed to OSI. The trend is toward a migration to OSI-based applicaions running on a TCP/IP infratsructure. As a result, more vendors, including Unisys and Amdahl, are introducing products that support multiple protocols.

Testing and Verification Agencies

The Corporation for Open Systems (COS)

During the late 1970s and early 1980s, vendor support for the OSI model ranged from wholehearted to indifferent. By 1985, however, it became apparent that cooperation among vendors—and users—would be critical to the success of open standards. That year, major U.S. vendors officially announced their support and formed the Corporation for Open Systems (COS) to promote implementation of OSI standards.

COS is a nonprofit research and development consortium located in McLean, VA, with an annual budget of $10 million. Its stated purpose is to work toward worldwide information systems interoperability. Its mission is to open worldwide markets for new OSI and ISDN products through certification, by developing conformance test products, and by cooperating with other international organizations. COS is not in the business of reinventing standards. It works with existing standards organizations to accelerate the implementation of present standards by testing and certification.

COS currently lists about 60 full-fledged member companies composed primarily of information technology vendors such as Apple Computer, AT&T, Digital Equipment Corp., Hewlett-Packard, IBM, Intel, Sun Microsystems, Texas

Instruments, and several software and LAN vendors. The list also includes several federal government agencies and a few large end users.

Members are committed to accelerate OSI and related standards and to assess how vendors can best supply end users with OSI and ISDN solutions; they are afforded several privileges not available to nonmembers. There are three types of memberships:

1. Regular membership, with an annual fee of $25,000
2. Corporate Research membership, for corporations with revenues in excess of $25 million, with an annual fee of $25,000
3. Senior Research membership, for corporations with revenues in excess of $150 million, with an annual membership fee of $25,000 and an annual research fee of $175,000.

Besides these three categories, COS provides an Affiliate Associate Program currently consisting of over 40 universities, foundations, associations, and nonprofit organizations.

COS' major activity is developing and administering the COS Mark Licensing Program, which is crucial to the COS mission. Informally known as the "gold dot," the COS Mark was developed with the aid of Underwriters Laboratories (UL). It is a "seal of approval," providing impartial verification to users that OSI and ISDN products conform to standards and ensure multivendor interoperability. COS awards the mark to products that meet COS requirements and pass a set of COS conformance tests. Since OSI contains many optional classes, subsets, and parameters, conformance tests are conducted on a COS Stack Specification—a specific profile of optional OSI protocols.

COS conformance tests are available through three avenues: at an on-site COS testing lab, through licenses issued to third-party testing organizations, and through licenses issued to vendors. In addition to OSI, the COS Conformance Testing Laboratory offers conformance test services for the following protocols:

- 802.3 CSMA/CD
- 802.4, Layer 1 and Layer 2
- X.25 (OSI 8882)
- Internet
- Transport
- FTAM
- MHS

Testing services cost $1,000 per day. Conformance test licenses are available for the protocols mentioned above, plus 10 specific MAP/TOP protocols, ranging from $5,500 to $135,000 per protocol (with discounts for multiple licenses).

COS has been unsuccessful in attracting end-user members and is criticized for moving too slowly and for not being impartial. COS members represent diverse interests but "theoretically" share a common vision of worldwide interoperability as well as a recognition of the potential profitability of open systems products. COS member representatives are working together to translate these ideals into several goals. Nevertheless, COS members cannot always reconcile their business interests with support of open standards.

Accordingly, COS has forged partnerships with similar testing and conformance groups in the U.S. and abroad. It has relationships with the MAP/TOP Users Group, NIST, ANSI, SPAG, POSI, and the Interoperability Technology Association for Information Processing (INTAP) of Japan. With ODA becoming mandatory for federal information system procurements after August 1992, the need for OSI conformance testing will increase immensely in the coming years. Recently, COS has shifted emphasis from that of a testing laboratory to producing a model for third-party testers.

In 1991, COS announced an industry-wide consensus to develop and deliver ISDN capabilities in the public switched telephone network by late 1992. ISDN will be deployed based on standard technical specifications and implementation agreements. Known collectively as National ISDN 1, the technical specifications were developed by Bellcore in conjunction with major industry equipment and service providers.

National Institute of Standards and Technology (NIST)

NIST, formerly the National Bureau of Standards (NBS), is a branch of the U.S. Department of Commerce. It develops federal information processing standards for ISDN and OSI and sponsors the OSI Implementers Workshop (OIW) and several OSI special interest groups. In 1979, NIST developed

formal standards description techniques and protocol test methods. It is grappling with the government's role in standardization, and whether that role should be increased to meet the challenges posed by international competition. Unlike other countries, the U.S. does not implement laws for standards conformance—a concept vigorously opposed by U.S. industry.

NIST and IEEE

NIST helps to sponsor an experimental OSI network for OSI product vendors and users, called OSINET. Originally formed in 1984 to test MAP protocols, OSINET is a packet switched network with about 40 U.S. nodes. It allows two vendors to voluntarily perform brief interoperability tests, modeled after OSI standards for conformance testing. Abbreviated test results are registered and made available to end users through an online database. Complete testing details and results can be obtained from OSINET.

OSINET costs are maintained by the participating vendors, including Digital Equipment Corp., Hewlett-Packard, IBM, NCR, and Unisys. NIST is a full member, and the network's chairperson is a NIST employee. In 1989, OSINET and equivalent networks from Europe, Japan, Australia, and Singapore formed a partnership called OSIone, which tests global OSI interoperability and demonstrates OSI internetworking at trade shows and special events around the world.

Bell Communications Research (Bellcore)

Bellcore, the R&D arm owned jointly by the Bell Operating Companies (BOCs), is the U.S.'s largest research consortium. Splintered from AT&T Bell Laboratories when AT&T was divested in 1984, its goal is to help make it possible for people anywhere in the world to communicate easily and securely in any medium or combination of media. Bellcore's domain is the public switched telephone network, for which it devises standards and tests vendor products for compliance. Bellcore's role is extremely important: in the absence of a regulated telephone monopoly (the Bell system), someone or something must maintain a homogeneous nationwide telephone network. In addition, the BOCs are not allowed to manufacture their own equipment and must purchase equipment from a variety of manufacturers.

Bellcore is active in public network specifications for ISDN, fiber optics, network management, the intelligent network concept, and related topics. After Bellcore drafts network standards, it allows them to be reviewed by the industry at large. After modifications, the standards are then published as Technical References (TRs), which are listed in Bellcore's annual *Catalog of Technical Information*. They can be ordered as complete documents at modest prices.

Since its inception, Bellcore has been actively engaged in ISDN research and testing. It produces commercially available testbeds for ISDN protocol compatibility. It also publishes books and videotapes on ISDN concepts, planning, and other ISDN topics.

Standards Promotion & Application Group (SPAG)

SPAG, the European equivalent of COS, was incorporated in 1986. Its stated mission is to pave the way to an open international market for the computer and telecommunications industry, based on harmonized standards and testing and certification of OSI products.

Like COS, SPAG concentrates its efforts on producing conformance testing, accrediting test laboratories, and certifying OSI products. SPAG has signed international agreements with COS and POSI to harmonize tools and testing technology. In 1988, it signed a joint development agreement with COS to produce the Integrated Tool Set (ITS). The agreement also provided for reciprocal cross-licensing and distribution of test tools.

In response to criticism that SPAG and COS were competing with tool developers and that testing was being conducted in a closed environment, SPAG developed the concept of OPEN Integrated Test Specification (OPEN ITS), an open approach to testing open systems.

OSI Management

Since the first draft of the seven-layer ISO model was produced in 1978, extensions to the basic model have been developed to more adequately represent all of the functions required by large-scale, multivendor networking environments. OSI

Management is an extension to the original reference model that specifies transfer of network management information in the Application Layer and support for network management functions at Layers 4, 5, and 6.

Advantages to OSI-Based Network Management

OSI-based network management continues to capture attention as the premier solution for multivendor network management. Vendors such as AT&T, Digital, Hewlett-Packard, and NCR are now designing their network management architectures to accommodate OSI Management standards and protocols.

In addition to solving the problem of managing heterogeneous environments, OSI-based network management will bring about a new phenomenon—unbundling network management from network products. In a proprietary environment, a given vendor's products are primarily manageable only by products developed by that vendor. Widespread use of OSI will split that one-to-one relationship, making it possible for any OSI-based network management system (NMS) to manage any OSI management-conformant device.

Disadvantages to OSI-Based Network Management

The market (both vendors and users) has widely criticized ISO for moving too slowly in its efforts to ratify OSI Management standards. Indeed, the greatest disadvantage to OSI-based network management is that the demand for it far exceeds the available products—and vendors are wisely unwilling to develop products based on standards that are not yet final. In an effort to open the door to new OSI-based network management system products, SC21 WG4 is currently working to finalize fault, configuration, performance, accounting, and security management specifications. These standards will assist in differentiating OSI-based systems from SNMP-based products.

Another disadvantage to standards-based network management is that OSI standards merely provide a menu of options. There are numerous gaps and ambiguities in OSI Management standards that could be interpreted differently, leading to incompatible implementations. Industry consensus is the only hope for interoperable implementations. Currently, this consensus is building around the OSI/Network Management Forum and the Network Management Special Interest Group (NMSIG) of the OIW, sponsored by NIST and the IEEE. The NMSIG is developing Implementation Agreements (IAs) based on emerging network management standards. IAs are being introduced in phases that coincide with ISO/IEC standards as they progress from CD to international standards. The OIW NM Phase I IA became stable in December 1990. To further simplify government procurement of network management products, NIST introduced a new proposal in May 1991, called the Government Network Management Profile (GNMP). GNMP will also be introduced in phases that will cross-reference the latest GOSIP versions. GNMP Phase I, II, and III will address the following categories of management information:

- Phase I—IEEE 802 LAN standards, X.25, ISDN, FDDI, modems, multiplexers, bridges, and the physical link of the OSI model.
- Phase II—protocol software operating in layers 3 to 7, routers, terminal servers, MTAs, PBX, and circuit switches.
- Phase III—applications, services, operating systems, computers, networks, and database management systems.

GNMP Phase I specifies CMIS/P, management definitions in GNMP secion 4, and five systems management functions: object management function, state management function, attributes for representing relationships, alarm reporting, and event reporting.

Since SNMP is already widely implemented, it is likely that SNMP will be deployed to manage routers. Future versions of GNMP will specify a network management architecture incorporating both SNMP and GNMP protocols.

Standards Documents

OSI Management standards can be broadly categorized into four areas:

1. Functions—*what* network management is, according to OSI
2. Services—*how* network management functions are accomplished
3. Information Structure—terms and categories describing *what is managed* (e.g., "management information")

4. Protocols—describe *means of transporting* network management information

Taken together, these four areas describe a generic package for network management systems, and how these products relate to the network devices they manage (called *managed objects* in OSI terminology).

A blueprint document, OSI Management Framework (IS 7498-4), places the OSI Management environment in perspective by describing terms and the scope of OSI network management.

OSI Management Functions

OSI Management functions are described in the Systems Management standards (CD 10040, CD 10164-1 through 10164-7, and N 10164-8 through 10164-12). These documents are listed in Table 3 and describe the scope of OSI Management using three models:

1. The Organizational Model—describes ways OSI Management can be distributed administratively
2. The Information Model—provides guidelines for defining managed objects and their interrelationships, classes, and names
3. The Functional Model—describes network management functions

The Functional Model outlines how ISO has partitioned network management into five functional areas: fault management, configuration and name management, performance management, accounting management, and security management. ISO originally described each of these areas in its own standard. Further studies revealed that functions overlapped; therefore, ISO reorganized the documents in December 1988 into their present Systems Management form.

Fault management provides the detection, isolation, and correction of abnormalities in network operation. Configuration and Name Management facilities permit network managers to control the configuration of the system, network, or layer entities. Changed configurations may isolate faults, alleviate congestion, or meet changing user needs. Performance management enables the network manager to monitor and evaluate the performance of the system, network, and layer entities. Data from performance management may be used to initiate configuration changes and diagnostic testing to allow a satisfactory level of performance. Accounting management facilities help determine and allocate costs for the use of a network manager's communications resources. Security Management facilities permit the management of those services providing access protection of communications resources.

Services

Services are described, in part, in the Common Management Information Services (CMIS) standard, IS 9595. Services use *primitives*, or command types, to accomplish network management functions. Examples of primitives include INITIALIZE, EVENT-REPORT, and TERMINATE. While service primitives are somewhat abstract, they are important building blocks for real commands used by network management applications to obtain vital data on the status and activity of network devices.

CMIS includes a detailed abstract model of open systems management services. These fall into three categories—event notification, information transfer, and control. Event notification allows one system to notify another that some event of importance has occurred. Information transfer consists of a single service element—Get. Control consists of three elements: Set, Action, and Compare.

Information Structure

The most important standards in this category are Structure of Management Information (SMI), Parts 1, 2, and 4 (CD 10165-1, 2, and 4). (Part 3 is not missing; rather, ISO merged Part 3 into Part 4.) Included in these standards is an explanation of the *object-oriented* paradigm, used to model a network in terms of object classes and attributes. In object-oriented environments, a variable (for example, a variable called Modem) is defined both in terms of the operations that can be performed on it and the values of attributes it can possess. For example, Modem can have an attribute such as Status, which may have a value of Up or Down; a network management system may obtain this value via a Get operation or alter it via a Set operation.

Objects (including their attributes and operations) are stored in a Management Information Base (MIB), sometimes called a Management Information Library (MIL). The SMI documents just

listed provide syntax and semantics for information in the MIB; however, as yet no single ISO standard defines exactly what the OSI MIB will contain, nor how vendors and users will register objects in the standard MIB. SC21 WG4 is currently working to finalize the Structure of Management Information (SMI), providing guidelines that can be used to define management objects and their attributes. The final SMI will ensure interoperability among OSI-based network management systems.

In the TCP/IP world, an Internet Standard MIB exists for objects managed using SNMP. This MIB functions in an analogous role to the proposed OSI MIB, although the administration and rules governing the two are sure to differ.

MIB includes all information needed to make management decisions. MIB is a conceptual repository of all OSI management data in an OSI environment. The MIB concept does not imply any form of physical or logical storage for management information, however, and its implementation is outside the scope of OSI standards. Rather, the SMI defines the abstract syntax and the semantics of information so that it can be represented in OSI protocol exchanges.

Protocols

Common Management Information Protocol (CMIP), IS 9596, is the primary OSI Management protocol. CMIP specifies procedures for the exchange of basic management information between open systems interconnected by OSI protocols. CMIP is intended to be a general-purpose management protocol suitable for the management of both OSI resources and the real resources used to provide communications services.

X.500—The Directory

The Directory is a related standard designed to manage name-related information concerning protocol layers and network nodes. These services connect the actual names used in the network with names and addresses understood by human users. The Directory is defined in CD 9594 and several other OSI working drafts. CD 9594 attained DIS in March 1988.

OSI and the Future

OSI's future as the premier means of interconnecting multivendor computer networks is almost a certainty. Too many government agencies, vendors, trade associations, and users have staked their futures on this architecture for it not to succeed. OSI applications protocols, such as CCITT X.400, X.500, and EDI, are catching on and spurring OSI's adoption. The world needs a network of computers, similar to standards for international telephony, to link users across oceans and continents. OSI is perceived as the answer to this need.

The OSI Reference Model has some glitches and holes, however, that prevent it from being widely implemented. In the U.S., OSI and TCP/IP proponents are badly divided. As an internetworking protocol, TCP/IP has proved its worth and is a popular and commercially successful method of linking users across diverse networks—particularly LANs. OSI middle-layer protocols 3 through 5, the alternatives to TCP/IP, are neither as practical nor as simple to implement in the real world. Simple Network Management Protocol (SNMP), the network management protocol for TCP/IP networks, is also a proven, commercially successful solution. As long as vendors and users require practical networking products, they will continue using TCP/IP-based protocols—standards or not.

Although nobody can predict the future, OSI will probably evolve to better serve user needs. A possible scenario for wider OSI acceptance is that OSI middle layers will migrate to resemble TCP/IP, at least in functionality. One such implementation already exists. A product called Xpress Transfer Protocol (XTP), a proprietary networking scheme from Protocol Engines, Inc. (Santa Barbara, CA), is a streamlined version of OSI's middle layers. XTP combines OSI layers 3 and 4 into one protocol and has been officially proposed to ANSI's X3S3 Committee for adoption.

In many commercial networking applications, however, vendors are blending different protocol stacks from different sources to match user needs. For instance, one vendor's network protocol might graft together different layers from OSI, TCP/IP, and IBM's SNA.

In reality, OSI and other layered architectures do not serve every application and are not a panacea. Proprietary architectures will continue to thrive alongside OSI-based networks, especially for closed user groups (where internetworking is not a requirement) or in time-sensitive applications intolerant of layered protocols' high overhead.

All others who desire internetworking must realize that the associated protocols are still evolving—nothing is truly cast in iron. In market-based economies, products that do not satisfy market needs will not gain widespread favor. Therefore, prospective users must evaluate OSI protocols and their adoption with an eye toward future standards developments. ■