COMMUNICATIONS AND NETWORK SECURITY

Third Stage

2

The OSI Model

Computer Networks

Introduction

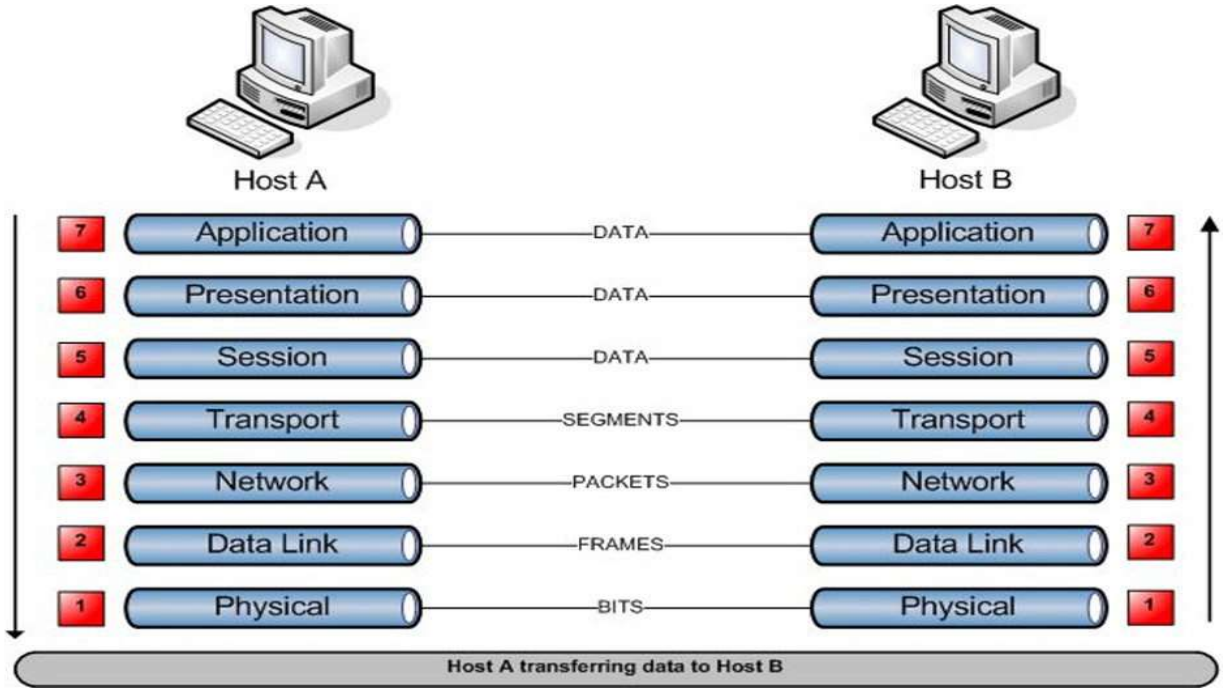
The Open Systems Interconnection (OSI) model is a reference tool for understanding data communications between any two networked systems. It divides the communications processes into seven layers. Each layer both performs specific functions to support the layers above it and offers services to the layers below it. The three lowest layers focus on passing traffic through the network to an end system. The top four layers come into play in the end system to complete the process.

This lecture will provide you with an understanding of each of the seven layers, including their functions and their relationships to each other. This will provide you with an overview of the network process, which can then act as a framework for understanding the details of computer networking.

Since the discussion of networking often includes talk of “extra layers”, this lecture will address these unofficial layers as well.

Finally, this lecture will draw comparisons between the theoretical OSI model and the functional TCP/IP model. Although TCP/IP has been used for network communications before the adoption of the OSI model, it supports the same functions and features in a differently layered arrangement.

An Overview of the OSI Model



A networking model offers a generic means to separate computer networking functions into multiple layers. Each of these layers relies on the layers below it to provide supporting capabilities and performs support to the layers above it. Such a model of layered functionality is also called a “protocol stack” or “protocol suite”.

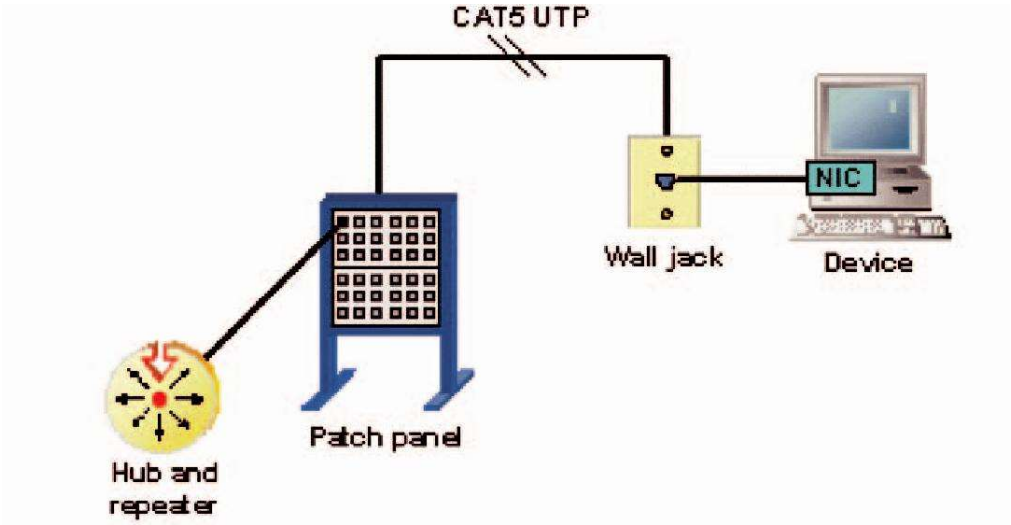
Protocols, or rules, can do their work in either hardware or software or, as with most protocol stacks, in a combination of the two. The nature of these stacks is that the lower layers do their work in hardware or firmware (software that runs on specific hardware chips) while the higher layers work in software.

The Open System Interconnection model is a seven-layer structure that specifies the requirements for communications between two computers. The ISO (International Organization for Standardization) standard 7498-1 defined this model. This model allows all network elements to operate together, no matter who created the protocols and what computer vendor supports them.

The main benefits of the OSI model include the following:

- Helps users understand the big picture of networking
- Helps users understand how hardware and software elements function together
- Makes troubleshooting easier by separating networks into manageable pieces
- Defines terms that networking professionals can use to compare basic functional relationships on different networks
- Helps users understand new technologies as they are developed
- Aids in interpreting vendor explanations of product functionality

Layer 1 – The Physical Layer



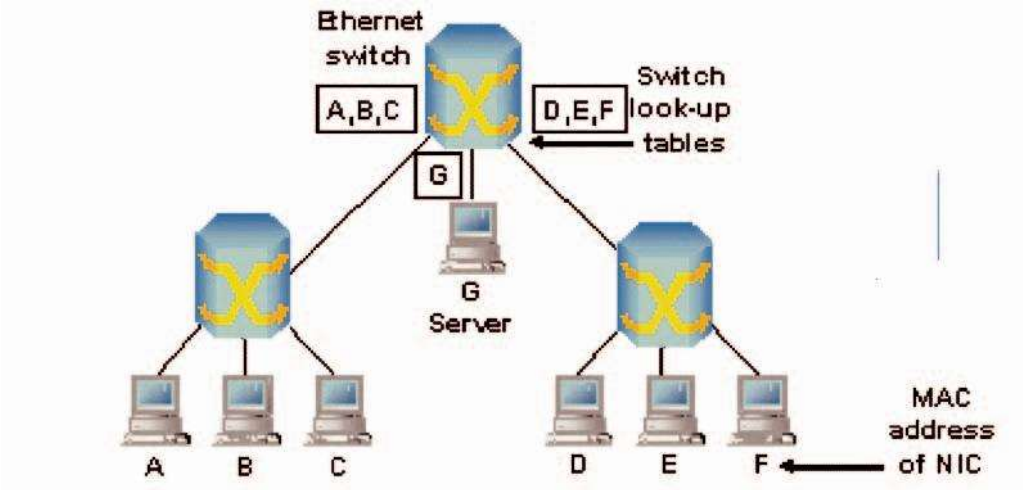
The physical layer of the OSI model defines connector and interface specifications, as well as the medium (cable) requirements. Electrical, mechanical, functional, and procedural specifications are provided for sending a bit stream on a computer network. Components of the physical layer include:

- Cabling system components
- Adapters that connect media to physical interfaces
- Connector design and pin assignments
- Hub, repeater, and patch panel specifications
- Wireless system components
- Parallel SCSI (Small Computer System Interface)
- Network Interface Card (NIC)

In a LAN environment, Category 5e UTP (Unshielded Twisted Pair) cable is generally used for the physical layer for individual device connections. Fiber optic cabling is often used for the physical layer in a vertical or riser backbone link. The IEEE, EIA/TIA, ANSI, and other similar standards bodies developed standards for this layer.

Note: The Physical Layer of the OSI model is only part of a LAN (Local Area Network).

Layer 2 – The Data Link Layer



Layer 2 of the OSI model provides the following functions:

- Allows a device to access the network to send and receive messages
- Offers a physical address so a device's data can be sent on the network
- Works with a device's networking software when sending and receiving messages
- Provides error-detection capability

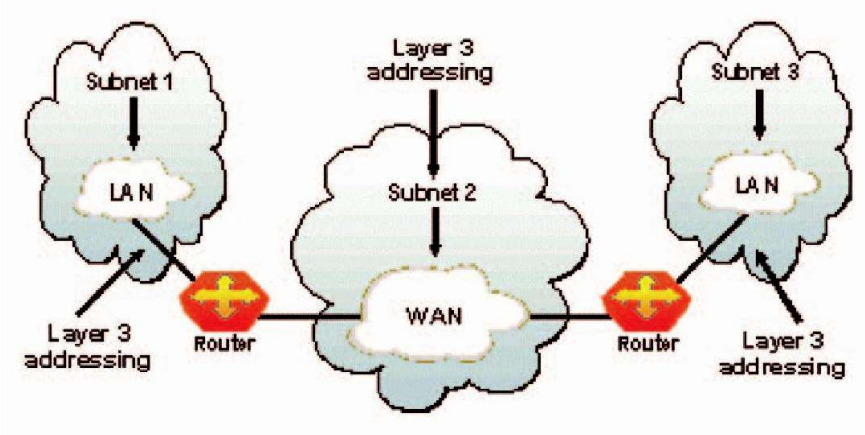
Common networking components that function at layer 2 include:

- Network interface cards
- Ethernet and Token Ring switches
- Bridges

NICs have a layer 2 or MAC address. A switch uses this address to filter and forward traffic, helping relieve congestion and collisions on a network segment.

Bridges and switches function in a similar fashion; however, bridging is normally a software program on a CPU, while switches use Application-Specific Integrated Circuits (ASICs) to perform the task in dedicated hardware, which is much faster.

Layer 3 – The Network Layer



Layer 3, the network layer of the OSI model, provides an end-to-end logical addressing system so that a packet of data can be routed across several layer 2 networks (Ethernet, Token Ring, Frame Relay, etc.). Note that net-work layer addresses can also be referred to as logical addresses.

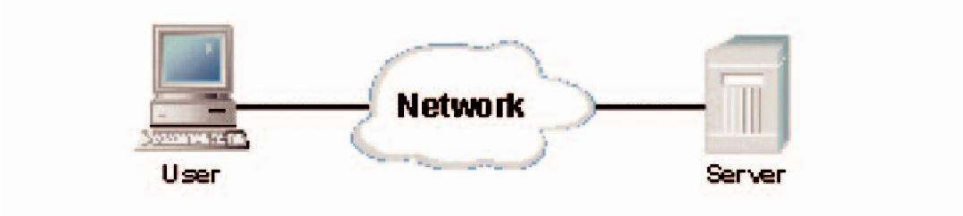
Initially, software manufacturers, such as Novell, developed proprietary layer 3 addressing. However, the net-working industry has evolved to the point that it requires a common layer 3 addressing system. The Internet Protocol (IP) addresses make networks easier to both set up and connect with one another. The Internet uses IP addressing to provide connectivity to millions of networks around the world.

To make it easier to manage the network and control the flow of packets, many organizations separate their network layer addressing into smaller parts known as subnets. Routers use the network or subnet portion of the IP addressing to route traffic between different networks. Each router must be configured specifically for the networks or subnets that will be connected to its interfaces.

Routers communicate with one another using routing protocols, such as Routing Information Protocol (RIP) and Open version of Shortest Path First (OSPF), to learn of other networks that are present and to calculate the best way to reach each network based on a variety of criteria (such as the path with the fewest routers). Routers and other networked systems make these routing decisions at the network layer.

When passing packets between different networks, it may become necessary to adjust their outbound size to one that is compatible with the layer 2 protocol that is being used. The network layer accomplishes this via a process known as fragmentation. A router's network layer is usually responsible for doing the fragmentation. All reassembly of fragmented packets happens at the network layer of the final destination system.

.Layer 4 – The Transport Layer



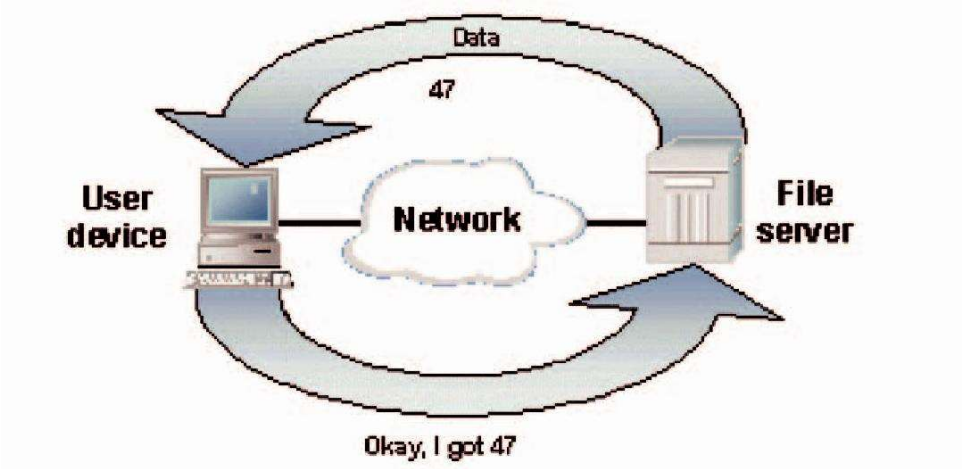
Layer 4, the transport layer of the OSI model, offers end-to-end communication between end devices through a network. Depending on the application, the transport layer either offers reliable, connection-oriented or connectionless, best-effort communications.

Some of the functions offered by the transport layer include:

- Application identification
- Client-side entity identification
- Confirmation that the entire message arrived intact
- Segmentation of data for network transport
- Control of data flow to prevent memory overruns
- Establishment and maintenance of both ends of virtual circuits
- Transmission-error detection
- Realignment of segmented data in the correct order on the receiving side
- Multiplexing or sharing of multiple sessions over a single physical link

The most common transport layer protocols are the connection-oriented TCP Transmission Control Protocol (TCP) and the connectionless UDP User Datagram Protocol (UDP).

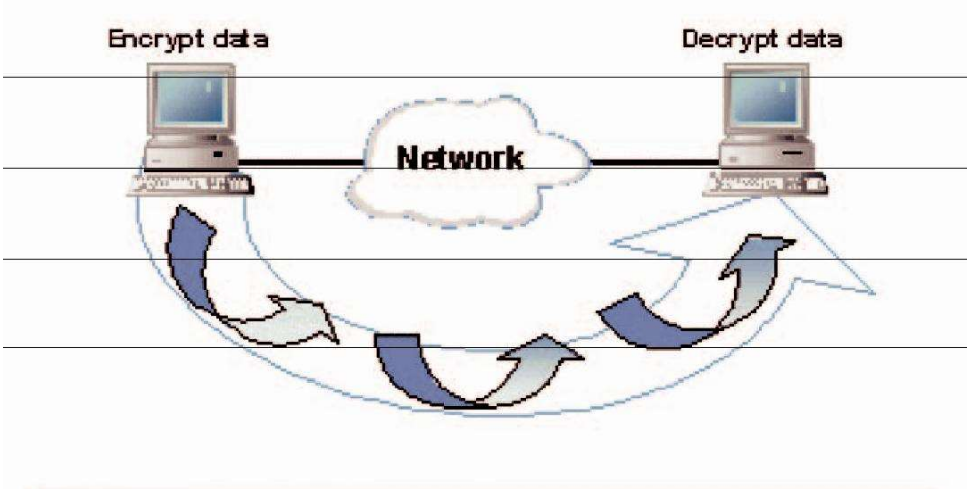
Layer 5 – The Session Layer



Layer 5, the session layer, provides various services, including tracking the number of bytes that each end of the session has acknowledged receiving from the other end of the session. This session layer allows applications functioning on devices to establish, manage, and terminate a dialog through a network. Session layer functionality includes:

- Virtual connection between application entities
- Synchronization of data flow
- Creation of dialog units
- Connection parameter negotiations
- Partitioning of services into functional groups
- Acknowledgements of data received during a session
- Retransmission of data if it is not received by a device

Layer 6 – The Presentation Layer



Layer 6, the presentation layer, is responsible for how an application formats the data to be sent out onto the network. The presentation layer basically allows an application to read (or understand) the message. Examples of presentation layer functionality include:

- Encryption and decryption of a message for security
- Compression and expansion of a message so that it travels efficiently
- Graphics formatting
- Content translation
- System-specific translation

Layer 7 – The Application Layer

Layer 7, the application layer, provides an interface for the end user operating a device connected to a net-work. This layer is what the user sees, in terms of loading an application (such as Web browser or e-mail); that is, this application layer is the data the user views while using these applications.

Examples of application layer functionality include:

- Support for file transfers
- Ability to print on a network
- Electronic mail
- Electronic messaging
- Browsing the World Wide Web