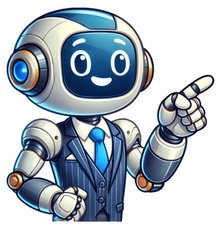
Continue



The OSI (Open Systems Interconnection) Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the International Organization for Standardization (ISO). The OSI Model consists of 7 layers and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together. OSI Model provides a clear structure for data transmission and managing network issues. The OSI Model is widely used as a reference to understand how network systems function.Layers of the OSI ModelThere are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:Layer 1: Physical LayerThe lowest layer of the OSI reference model is the Physical Layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. Physical Layer is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. Common physical layer devices are Hub, Repeater, Modem, and Cables.Physical LayerFunctions of the Physical Layer Bit Synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level. Bit Rate Control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second. Physical Topologies: Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus topology, star topology, or mesh topology. Transmission Mode: Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full duplex. The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame. Switches and Bridges are common Data Link Layer devices. The Data Link Layer is divided into two sublayers: Logical Link Control (LLC)Media Access Control (MAC)The packet received from the Network layer is further divided into frames depending on the frame size of the NIC (Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header. The Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. Physical Addressing: After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame. Error Control: The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment. Access Control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time. Layer 3: Network Layer The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP addresses are placed in the header by the network layer. Segment in the Network layer is referred to as Packet. Network layer is implemented by networking devices such as routers and switches. Functions of the Network Layer Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing. Logical Addressing: To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally. Layer 4: Transport Layer The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.At the sender's side, the transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow and error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data. Functions of the Transport Layer Segmentation and Reassembly: This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message. Service Point Addressing: To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process. Services Provided by Transport Layer Connection-Oriented ServiceConnectionless ServiceLayer 5: Session LayerSession Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP. Functions of the Session Layer Session Establishment, Maintenance, and Termination: The layer allows the two processes to establish, use, and terminate a connection. Synchronization: This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided. Dialog Controller: The session layer allows two systems to start communication with each other in half-duplex or full duplex. Example Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted. Communication in Session LayerThe presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are TLS/SSL (Transport Layer Security / Secure Sockets Layer).JPEG, MPEG, GIF, are standards or formats used for encoding data, which is part of the presentation layer's role. Functions of the Presentation Layer Translation: For example, ASCII to EBCDIC. Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext, and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data. Compression: Reduces the number of bits that need to be transmitted on the network. Layer 7: Application LayerAt the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Protocols used in the Application layer are SMTP, FTP, DNS, etc.Application LayerFunctions of the Application Layer The main functions of the application layer are given below. Network Virtual Terminal (NVT): It allows a user to log on to a remote host. File Transfer Access and Management (FTAM): This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer. Mail Services: Provide email service. Directory Services: This application provides distributed database sources and access for global information about various objects and services. How Data Flows in the OSI Model?When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end. Data flows through the OSI model in a step-by-step process: Application Layer: Applications create the data. Presentation Layer: Data is formatted and encrypted. Session Layer: Connections are established and managed. Transport Layer: Data is broken into segments for reliable delivery. Network Layer: Segments are packaged into packets and routed. Data Link Layer: Packets are framed and sent to the next device. Physical Layer: Frames are converted into bits and transmitted physically. Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival. We can understand how data flows through OSI Model with the help of an example mentioned below.Let us suppose, Person A sends an e-mail to his friend Person B. Step 1: Person A interacts with e-mail application like Gmail, outlook, etc. Writes his email to send. (This happens at Application Layer).Step 2: At Presentation Layer, Mail application prepares for data transmission like encrypting data and formatting it for transmission.Step 3: At Session Layer, there is a connection established between the sender and receiver on the internet.Step 4: At Transport Layer, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information.Step 5: At Network Layer, addressing of packets is done in order to find the best route for transfer.Step 6: At Data Link Layer, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.Step 7: At Physical Layer, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi. After the email reaches the receiver i.e. Person B, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Person B email client.Please refer the below animation for detailed flow. Protocols Used in the OSI LayersLayerWorking Protocol Data Unit Protocols1: Physical LayerEstablishing Physical Connections between Devices.BitsUSB, SONET/SDH, etc. 2: Data Link LayerNode to Node Delivery of Message.FramesEthernet, PPP, etc.3: Network LayerTransmission of data from one host to another, located in different networks.PacketsIP, ICMP, IGMP, OSPF, etc.4: Transport LayerTake Service from Network Layer and provide it to the Application Layer.Segments (for TCP) or Datagrams (for UDP) TCP, UDP, SCTP, etc.5: Session LayerEstablishes Connection, Maintenance, Ensures Authentication and Ensures security.DataNetBIOS, RPC, PPTP, etc.6: Presentation Layer Data from the application layer is extracted and manipulated in the required format for transmission. DataTLS/SSL, MIME, etc. 7: Application LayerHelps in identifying the client and synchronizing communication. DataFTP, SMTP, DNS, DHCP, etc.Why Does the OSI Model MatterThe OSI Model matters because it provides the user a clear structure of "how the data moves in the network?". As the OSI Model consists of 7 layers, each layer has its specific role, and due to which it helps in understanding, identifying and solving the complex network problems easily by focusing on one of the layers not the entire network.As the modern Internet does not prefer the OSI Model, but still, the OSI Model is still very helpful for solving network problems. It helps people understanding network concepts very easily.Difference Between OSI and TCP/IP ModelOSI Model TCP/IP ModelOSI stands for Open Systems Interconnection.TCP/IP stands for Transmission Control Protocol/Internet Protocol.OSI model has 7 layers.TCP/IP model consists of 4 layers.Package delivery is guaranteed in OSI Model.Package delivery is not guaranteed in the TCP/IP Model.In the OSI model, only layers 1,2 and 3 are necessary for data transmission.All layers of the TCP/IP model are needed for data transmission.Protocols at each layer is independent of the other layer.Layers are integrated; some layers are required by other layers of TCP/IP model.OSI Model is a conceptual framework, less used in practical applications.Widely used in actual networks like Internet and Communication Systems.OSI vs TCP/IPAdvantages of OSI Model The OSI Model defines the communication of a computing system into 7 different layers. Its advantages include: It divides network communication into 7 layers which makes it easier to understand and troubleshoot.It standardizes network communications, as each layer has fixed functions and protocols.Diagnosing network problems is easier with the OSI model. It is easier to improve with advancements as each layer can get updates separately.Disadvantages of OSI Model The OSI Model has seven layers, which can be complicated and hard to understand for beginners.In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model is not always directly applicable.Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.The OSI Model is more of a theoretical framework, meaning it's great for understanding concepts but not always practical for implementation. Model of communication of seven abstraction layers OSI modelby layer 7. Application layer NNTP SIP SSI DNS FTP Gopher HTTP (HTTP/3) NFS NTP SMPP SSH SMTP SNMP Telnet DHCP NETCONF more.... 6. Presentation layer MIME XDR ASN.1 ASCII TLS PGP 5. Session layer Named pipe NetBIOS SAP PPTP RTP SOCKS X.225[1] 4. Transport layer TCP UDP SCTP DCCP QUIC SPX 3. Network layer IP IPv4 IPv6 ICMP (ICMPv6) IPsec IGMP IPX IS-IS AppleTalk X.25 PLP 2. Data link layer ATM ARP SDLC HDLC CSLIP SLIP GFP PLIP IEEE 802 LLC MAC L2TP Frame Relay ITU-T G.hn DLL PPP X.25 LAPB Q.922 LAPF 1. Physical layer RS-232 RS-449 ITU-T V-Series I.430 I.431 PDH SONET/SDH PON OTN DSL IEEE 802 IEEE 1394 ITU-T G.hn PHY USB Bluetooth X.21 vte The Open Systems Interconnection (OSI) model is a reference model developed by the International Organization for Standardization (ISO) that "provides a common basis for the coordination of standards development for the purpose of systems interconnection."[2] In the OSI reference model, the components of a communication system are distinguished in seven abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.[3] The model describes communications from the physical implementation of transmitting bits across a transmission medium to the highest-level representation of data of a distributed application. Each layer has well-defined functions and semantics and serves a class of functionality to the layer above it and is served by the layer below it. Established, well-known communication protocols are decomposed in software development into the model's hierarchy of function calls. The Internet protocol suite as defined in RFC 1122 and RFC 1123 is a model of networking developed contemporarily to the OSI model, and was funded primarily by the U.S. Department of Defense. It was the foundation for the development of the Internet. It assumed the presence of generic physical links and focused primarily on the software layers of communication, with a similar but much less rigorous structure than the OSI model. In comparison, several networking models have sought to create an intellectual framework for clarifying networking concepts and activities,[citation needed] but none have been as successful as the OSI reference model in becoming the standard model for discussing and teaching networking in the field of information technology. The model allows transparent communication through equivalent exchange of protocol data units (PDUs) between two parties, through what is known as peer-to-peer networking (also known as peer-to-peer communication). As a result, the OSI reference model has not only become an important piece among professionals and non-professionals alike, but also in all networking between one or many parties, due in large part to its commonly accepted user-friendly framework.[4] Communication in the OSI model (example with layers 3 to 5) The development of the OSI model started in the late 1970s to support the emergence of the diverse computer networking methods that were competing for application in the large national networking efforts in the world (see OSI protocols and Protocol Wars). In the 1980s, the model became a working product of the Open Systems Interconnection group at the International Organization for Standardization (ISO). While attempting to provide a comprehensive description of networking, the model failed to garner reliance during the design of the Internet, which is reflected in the less prescriptive Internet Protocol Suite, principally sponsored under the auspices of the Internet Engineering Task Force (IETF). In the early- and mid-1970s, networking was largely either government-sponsored (NPL network in the UK, ARPANET in the US, CYCLADES in France) or vendor-developed with proprietary standards, such as IBM's Systems Network Architecture and Digital Equipment Corporation's DECnet. Public data networks were only just beginning to emerge, and these began to use the X.25 standard in the late 1970s.[5][6] The Experimental Packet Switched System in the UK c. 1973–1975 identified the need for defining higher-level protocols.[5] The UK National Computing Centre publication, Why Distributed Computing, which came from considerable research into future configurations for computer systems,[7] resulted in the UK presenting the case for an international standards committee to cover this area at the ISO meeting in Sydney in March 1977.[8][9] Beginning in 1977, the ISO initiated a program to develop general standards and methods of networking. A similar process evolved at the International Telegraph and Telephone Consultative Committee (CCITT, from French: Comité Consultatif International Téléphonique et Télégraphique). Both bodies developed documents that defined similar networking models. The British Department of Trade and Industry acted as the secretariat, and universities in the United Kingdom developed prototypes of the standards.[10] The OSI model was first defined in raw form in Washington, D.C., in February 1978 by French software engineer Hubert Zimmermann, and the refined but still draft standard was published by the ISO in 1980.[9] The drafters of the reference model had to contend with many competing priorities and interests. The rate of technological change made it necessary to define standards that new systems could converge to rather than standardizing procedures after the fact; the reverse of the traditional approach to developing standards.[11] Although not a standard itself, it was a framework in which future standards could be defined.[12] In May 1983,[13] the CCITT and ISO documents were merged to form The Basic Reference Model for Open Systems Interconnection, usually referred to as the Open Systems Interconnection Reference Model, OSI Reference Model, or simply OSI model. It was published in 1984 by both the ISO, as standard ISO 7498, and the renamed CCITT (now called the Telecommunications Standardization Sector of the International Telecommunication Union or ITU-T) as standard X.200. OSI had two major components: an abstract model of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocols. The OSI reference model was a major advance in the standardisation of network concepts. It promoted the idea of a consistent model of protocol layers, defining interoperability between network devices and software. The concept of a seven-layer model was provided by the work of Charles Bachman at Honeywell Information Systems.[14] Various aspects of OSI design evolved from experiences with the NPL network, ARPANET, CYCLADES, EIN, and the International Network Working Group (IFIP WG6.1). In this model, a networking system was divided into layers. Within each layer, one or more entities implement its functionality. Each entity interacted directly only with the layer immediately beneath it and provided facilities for use by the layer above it. The OSI standards documents are available from the ITU-T as the X.200 series of recommendations.[15] Some of the protocol specifications were also available as part of the ITU-T X series. The equivalent ISO/IEC standards for the OSI model were available from ISO. Not all are free of charge.[16] OSI was an industry effort, attempting to get industry participants to agree on common network standards to provide multi-vendor interoperability.[17] It was common for large networks to support multiple network protocol suites, with many devices unable to interoperate with other devices because of a lack of common protocols. For a period in the late 1980s and early 1990s, engineers, organizations and nations became polarized over the issue of which standard, the OSI model or the Internet protocol suite, would result in the best and most robust computer networks.[9][18][19] However, while OSI developed its networking standards in the late 1980s,[20][page needed][21][page needed] TCP/IP came into widespread use on multi-vendor networks for internetworking. The OSI model is still used as a reference for teaching and documentation;[22] however, the OSI protocols originally conceived for the model did not gain popularity. Some engineers argue the OSI reference model is still relevant to cloud computing.[23] Others say the original OSI model does not fit today's networking protocols and have suggested instead a simplified approach.[24][25] This section needs additional citations for verification. Please help improve this article by adding citations to reliable sources in this section. Unsourced material may be challenged and removed. (November 2019) (Learn how and when to remove this message) Communication protocols enable an entity in one host to interact with a corresponding entity at the same layer in another host. Service definitions, like the OSI model, abstractly describe the functionality provided to a layer N by a layer N−1, where N is one of the seven layers of protocols operating in the local host. At each level N, two entities at the communicating devices (layer N peers) exchange protocol data units (PDUs) by means of a layer N protocol. Each PDU contains a payload, called the service data unit (SDU), along with protocol-related headers or footers. Data processing by two communicating OSI-compatible devices proceeds as follows: The data to be transmitted is composed at the topmost layer of the transmitting device (layer N) into a protocol data unit (PDU). The PDU is passed to layer N−1, where it is known as the service data unit (SDU). At layer N−1 the SDU is concatenated with a header, a footer, or both, producing a layer N−1 PDU. It is then passed to layer N−2. The process continues until reaching the lowermost level, from which the data is transmitted to the receiving device. At the receiving device the data is passed from the lowest to the highest layer as a series of SDUs while being successively stripped from each layer's header or footer until reaching the topmost layer, where the last of the data is consumed. The OSI model was defined in ISO/IEC 7498 which consists of the following parts: ISO/IEC 7498-1 The Basic Model ISO/IEC 7498-2 Security Architecture ISO/IEC 7498-3 Naming and addressing ISO/IEC 7498-4 Management framework ISO/IEC 7498-1 is also published as ITU-T Recommendation X.200. The recommendation X.200 describes seven layers, labelled 1 to 7. Layer 1 is the lowest layer in this model. OSI model Layer Protocol data unit (PDU) Function[26] Hostlayers 7 Application Data High-level protocols such as for resource sharing or remote file access, e.g. HTTP. 6 Presentation Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption 5 Session Managing communication sessions, i.e., continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes 4 Transport Segment Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing Medialayers 3 Network Packet, Datagram[27] Structuring and managing a multi-node network, including addressing, routing and traffic control 2 Data link Frame Transmission of data frames between two nodes connected by a physical layer 1 Physical Bit, Symbol Transmission and reception of raw bit streams over a physical medium Main article: Physical layer The physical layer is responsible for the transmission and reception of unstructured raw data between a device, such as a network interface controller, Ethernet hub, or network switch, and a physical transmission medium. It converts the digital bits into electrical, radio, or optical signals (analogue signals). Layer specifications define characteristics such as voltage levels, the timing of voltage changes, physical data rates, maximum transmission distances, modulation scheme, channel access method and physical connectors. This includes the layout of pins, voltages, line impedance, cable specifications, signal timing and frequency for wireless devices. Bit rate control is done at the physical layer and may define transmission mode as simplex, half duplex, and full duplex. The components of a physical layer can be described in terms of the network topology. Physical layer specifications are included in the specifications for the ubiquitous Bluetooth, Ethernet, and USB standards. An example of a less well-known physical layer specification would be for the CAN standard. The physical layer also specifies how encoding occurs over a physical signal, such as electrical voltage or a light pulse. For example, a 1 bit might be represented on a copper wire by the transition from a 0-volt to a 5-volt signal, whereas a 0 bit might be represented by the transition from a 5-volt to a 0-volt signal. As a result, common problems occurring at the physical layer are often related to the incorrect media termination, EMI or noise scrambling, and NICs and hubs that are misconfigured or do not work correctly. Main article: Data link layer The data link layer provides node-to-node data transfer—a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the physical layer. It defines the protocol to establish and terminate a connection between two physically connected devices. It also defines the protocol for flow control between them. IEEE 802 divides the data link layer into two sublayers:[28] Medium access control (MAC) layer – responsible for controlling how devices in a network gain access to a medium and permission to transmit data. Logical link control (LLC) layer – responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization. The MAC and LLC layers of IEEE 802 networks such as 802.3 Ethernet, 802.11 Wi-Fi, and 802.15.4 Zigbee operate at the data link layer. The Point-to-Point Protocol (PPP) is a data link layer protocol that can operate over several different physical layers, such as synchronous and asynchronous serial lines. The ITU-T G.hn standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer that provides both error correction and flow control by means of a selective-repeat sliding-window protocol. Security, specifically (authenticated) encryption, at this layer can be applied with MACsec. Main article: Network layer The network layer provides the functional and procedural means of transferring packets from one node to another connected in "different networks". A network is a medium to which many nodes can be connected, on which every node has an address and which permits nodes connected to it to transfer messages to other nodes connected to it by merely providing the content of a message and the address of the destination node and letting the network find the way to deliver the message to the destination node, possibly routing it through intermediate nodes. If the message is too large to be transmitted from one node to another on the data link layer between those nodes, the network may implement message delivery by splitting the message into several fragments at one node, sending the fragments independently, and reassembling the fragments at another node. It may, but does not need to, report delivery errors. Message delivery at the network layer is not necessarily guaranteed to be reliable; a network layer protocol may provide reliable message delivery, but it does not need to do so. A number of layer-management protocols, a function defined in the management annex, ISO 7498/4, belong to the network layer. These include routing protocols, multicast group management, network-layer information and error, and network-layer address assignment. It is the function of the payload that makes these belong to the network layer, not the protocol that carries them.[29] Main article: Transport layer The transport layer provides the functional and procedural means of transferring variable-length data sequences from a source host to a destination host from one application to another across a network while maintaining the quality-of-service functions. Transport protocols may be connection-oriented or connectionless. This may require breaking large protocol data units or long data streams into smaller chunks called "segments", since the network layer imposes a maximum packet size called the maximum transmission unit (MTU), which depends on the maximum packet size imposed by all data link layers on the network path between the two hosts. The amount of data in a data segment must be small enough to allow for a network-layer header and a transport-layer header. For example, for data being transferred across Ethernet, the MTU is 1500 bytes, the minimum size of a TCP header is 20 bytes, and the minimum size of an IPv4 header is 20 bytes, so the maximum segment size is 1500−(20+20) bytes, or 1460 bytes. The process of dividing data into segments is called segmentation; it is an optional function of the transport layer. Some connection-oriented transport protocols, such as TCP and the OSI connection-oriented transport protocol (COTP), perform segmentation and reassembly of segments on the receiving side; connectionless transport protocols, such as UDP and the OSI connectionless transport protocol (CLTP), usually do not. The transport layer also controls the reliability of a given link between a source and destination host through flow control, error control, and acknowledgments of sequence and existence. Some protocols are state- and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail delivery through the acknowledgment hand-shake system. The transport layer will also provide the acknowledgement of the successful data transmission and sends the next data if no errors occurred. Reliability, however, is not a strict requirement within the transport layer. Protocols like UDP, for example, are used in applications that are willing to accept some packet loss, reordering, errors or duplication. Streaming media, real-time multiplayer games and voice over IP (VoIP) are examples of applications in which loss of packets is not usually a fatal problem. The OSI connection-oriented transport protocol defines five classes of connection-mode transport protocols, ranging from class 0 (which is also known as TP0 and provides the fewest features) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries. Detailed characteristics of TP0–4 classes are shown in the following table:[30] Feature name TP0 TP1 TP2 TP3 TP4 Connection-oriented network Yes Yes Yes Yes Yes Connectionless network No No No No Yes Concatenation and separation No Yes Yes Yes Yes Segmentation and reassembly Yes Yes Yes Yes Yes Error recovery No Yes Yes Yes Yes Reinitiate connectiona No Yes No Yes No Multiplexing / demultiplexing over single virtual circuit No No Yes Yes Yes Explicit flow control No No Yes Yes Yes Retransmission on timeout No No No No Yes Reliable transport service No Yes No Yes Yes a If an excessive number of PDUs are unacknowledged. An easy way to visualize the transport layer is to compare it with a post office, which deals with the dispatch and classification of mail and parcels sent. A post office inspects only the outer envelope of mail to determine its delivery. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, tunnelling protocols operate at the transport layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPsec. While Generic Routing Encapsulation (GRE) might seem to be a network-layer protocol, if the encapsulation of the payload takes place only at the endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete Layer 2 frames or Layer 3 packets to deliver to the endpoint. L2TP carries PPP frames inside transport segments. Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the transport layer, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite are commonly categorized as layer 4 protocols within OSI. Transport Layer Security (TLS) does not strictly fit inside the model either. It contains characteristics of the transport and presentation layers.[31][32] Main article: Session layer The session layer creates the setup, controls the connections, and ends the teardown, between two or more computers, which is called a "session". Common functions of the session layer include user logon (establishment) and user logoff (termination) functions. Including this matter, authentication methods are also built into most client software, such as FTP Client and NFS Client for Microsoft Networks. Therefore, the session layer establishes, manages and terminates the connections between the local and remote applications. The session layer also provides for full-duplex, half-duplex, or simplex operation,[citation needed] and establishes procedures for checkpointing, suspending, restarting, and terminating a session between two related streams of data, such as an audio and a video stream in a web-conferencing application. Therefore, the session layer is commonly implemented explicitly in application environments that use remote procedure calls. Main article: Presentation layer The presentation layer establishes data formatting and data translation into a format specified by the application layer during the encapsulation of outgoing messages while being passed down the protocol stack, and possibly reversed during the deencapsulation of incoming messages when being passed up the protocol stack. For this very reason, outgoing messages during encapsulation are converted into a format specified by the application layer, while the conversion for incoming messages during deencapsulation are reversed. The presentation layer handles protocol conversion, data encryption, data decryption, data compression, data decompression, incompatibility of data representation between operating systems, and graphic commands. The presentation layer transforms data into the form that the application layer accepts, to be sent across a network. Since the presentation layer converts data and graphics into a display format for the application layer, the presentation layer is sometimes called the syntax layer.[33] For this reason, the presentation layer negotiates the transfer of syntax structure through the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.[4] Main article: Application layer The application layer is the layer of the OSI model that is closest to the end user, which means both the OSI application layer and the user interact directly with a software application that implements a component of communication between the client and server, such as File Explorer and Microsoft Word. Such application programs fall outside the scope of the OSI model unless they are directly integrated into the application layer through the functions of communication, as is the case with applications such as web browsers and email programs. Other examples of software are Microsoft Network Software for File and Printer Sharing and Unix/Linux Network File System Client for access to shared file resources. Application-layer functions typically include file sharing, message handling, and database access, through the most common protocols at the application layer, known as HTTP, FTP, SMB/CIFS, TFTP, and SMTP. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. The most important distinction in the application layer is the distinction between the application entity and the application. For example, a reservation website might have two application entities: one using HTTP to communicate with its users, and one for a remote database protocol to record reservations. Neither of these protocols have anything to do with reservations. That logic is in the application itself. The application layer has no means to determine the availability of resources in the network.[4] Further information: Cross-layer optimization Cross-layer functions are services that are not tied to a given layer, but may affect more than one layer.[34] Some orthogonal aspects, such as management and security, involve all of the layers (See ITU-T X.800 Recommendation[35]). These services are aimed at improving the CIA triad—confidentiality, integrity, and availability—of the transmitted data. Cross-layer functions are the norm, in practice, because the availability of a communication service is determined by the interaction between network design and network management protocols. Specific examples of cross-layer functions include the following: Security service (telecommunication)[35] as defined by ITU-T X.800 recommendation. Management functions, i.e. functions that permit to configure, instantiate, monitor, terminate the communications of two or more entities: there is a specific application-layer protocol, Common Management Information Protocol (CMIP) and its corresponding service, Common Management Information Service (CMIS), they need to interact with every layer in order to deal with their instances. Multiprotocol Label Switching (MPLS), ATM, and X.25 are 3a protocols. OSI subdivides the Network Layer into three sublayers: 3a) Subnetwork Access, 3b) Subnetwork Dependent Convergence and 3c) Subnetwork Independent Convergence.[36] It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram-based service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames. Sometimes one sees reference to a Layer 2.5. Cross MAC and PHY Scheduling is essential in wireless networks because of the time-varying nature of wireless channels. By scheduling packet transmission only in favourable channel conditions, which requires the MAC layer to obtain channel state information from the PHY layer, network throughput can be significantly improved and energy waste can be avoided.[37][page needed] Neither the OSI Reference Model, nor any OSI protocol specifications, outline any programming interfaces, other than deliberately abstract service descriptions. Protocol specifications define a methodology for communication between peers, but the software interfaces are implementation-specific. For example, the Network Driver Interface Specification (NDIS) and Open Data-Link Interface (ODI) are interfaces between the media (layer 2) and the network protocol (layer 3). The table below presents a list of OSI layers, the original OSI protocols, and some approximate modern matches. This correspondence is rough: the OSI model contains idiosyncrasies not found in later systems such as the IP stack in modern Internet.[25] Layer OSI protocols TCP/IP protocols SignalingSystem 7[38] AppleTalk IPX SNA UMTS HTTP-based protocols Miscellaneous examples No. Name 7 Application FTAMX.400X.500DAPROSERTSEACSE[39][40]CMIP[41][42][43][44] HTTPHTTPSFTPSMTP INAPMAPTCAPISUPTUP AFPZIPRTMPNBP SAP Transaction ServicesPresentation Services Web BrowserWebDAVSOAPOpenIDREST APIOAuthGraphQLActivityPubGitDNS over HTTP HL7ModbusWebSocketCoAP 6 Presentation ISO/IEC 8823X.226ISO/IEC 9576-1X.236 MIMESSL/TLSXDR AFP Presentation Services XMLJSONMIMEPercent-encodingbase64gzipbrotli TDIASCIIEBCDICMIDIMPEG 5 Session ISO/IEC 8327X.225ISO/IEC 9548-1X.235 Sockets (session establishment in TCP / RTP / PPTP) ASPADSPPAP NWLink Presentation ServicesData Flow Control HTTP headers, including cookiesCSRF tokensWebSocket Named pipesNetBIOSSAPRPCSOCKS 4 Transport ISO/IEC 8073TP0TP1TP2TP3TP4 (X.224)ISO/IEC 8602X.234 TCPUDPSCTPQUICDCCP DDP SPX Data Flow ControlTransmission Control HTTP/HTTP/2/HTTP/3WebSocketDTLS Port number can be specified. NBF 3 Network ISO/IEC 8208X.25 (PLP) ISO/IEC 8878X.223ISO/IEC 8473-1CLNP X.233ISO/IEC 10589IS-IS IPIPsecICMPIGMPOSPFRIP SCCPMTP ATP (TokenTalk / EtherTalk) IPX Transmission ControlPath Control RRC / BMC Out of scope. IP addresses can be used instead of domain names in URLs. NBFQ.931 2 Data link ISO/IEC 7666X.25 (LAPB)Token BusX.222ISO/IEC 8802-2LLC (type 1 / 2)[45] PPPSBTVSLIP MTPQ.710 LocalTalkARAPPP IEEE 802.3 framingEthernet II framing Path ControlData Link Control PDCP[46]LLCMAC Out of scope. ARPNDP (Neighbor Discovery Protocol)ARQATMBit stuffingCDPDOCSISFDDIFDPFibre ChannelFrame RelayHDLCIEEE 802.3 MACIEEE 802.11 MACIEEE 802.1QISLITU-T G.hn DLLLinux interface bondingPPPQ.921Token RingNDP (Nortel Discovery Protocol)IS-IS 1 Physical X.25 (X.21bisEIA/TIA-232EIA/TIA-449EIA-530G.703)[45] TCP/IP stack does not care about the physical medium, as long as it provides a way to communicate octets MTPQ.710 RS-232RS-422PhoneNet Physical UMTS air interfaces Out of scope. RS-232RJ45 (8P8C)V.35V.34I.430I.431T1E1IEEE 802.3 PHY (10BASE-T100BASE-TX1000BASE-T)POTSSONETBluetoothSDHDSLIEEE 802.11 PHYITU-T G.hn PHYDOCSISDWDMOTN See also: Internet protocol suite § Comparison of TCP/IP and OSI layering The design of protocols in the TCP/IP model of the Internet does not concern itself with strict hierarchical encapsulation and layering. RFC 3439 contains a section entitled "Layering considered harmful".[47] TCP/IP does recognize four broad layers of functionality which are derived from the operating scope of their contained protocols: the scope of the software application; the host-to-host transport path; the internetworking range; and the scope of the direct links to other nodes on the local network.[48] Despite using a different concept for layering than the OSI model, these layers are often compared with the OSI layering scheme in the following manner: The Internet application layer maps to the OSI application layer, presentation layer, and most of the session layer. The TCP/IP transport layer maps to the graceful close function of the OSI session layer as well as the OSI transport layer. The internet layer performs functions as those in a subset of the OSI network layer. The link layer corresponds to the OSI data link layer and may include similar functions as the physical layer, as well as some protocols of the OSI's network layer. These comparisons are based on the original seven-layer protocol model as defined in ISO 7498, rather than refinements in the internal organization of the network layer. The OSI protocol suite that was specified as part of the OSI project was considered by many as too complicated and inefficient, and to a large extent unimplementable.[49][page needed] Taking the "forklift upgrade" approach to networking, it specified eliminating all existing networking protocols and replacing them at all layers of the stack. This made implementation difficult and was resisted by many vendors and users with significant investments in other network technologies. In addition, the protocols included so many optional features that many vendors' implementations were not interoperable.[49][page needed] Although the OSI model is often still referenced, the Internet protocol suite has become the standard for networking. TCP/IP's pragmatic approach to computer networking and to independent implementations of simplified protocols made it a practical methodology.[49][page needed] Some protocols and specifications in the OSI stack remain in use, one example being IS-IS, which was specified for OSI as ISO/IEC 10589:2002 and adapted for Internet use with TCP/IP as RFC 1142.[50] Government Open Systems Interconnection Profile Hierarchical internetworking model History of the Internet Layer 8 List of information technology initialisms Management plane Recursive Internetwork Architecture Service layer Session multiplexing ^ "X.225 : Information technology – Open Systems Interconnection – Connection-oriented Session protocol: Protocol specification". Archived from the original on 1 February 2021. Retrieved 10 March 2023. ^ ISO/IEC 7498-1:1994 Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. June 1999. Introduction. Retrieved 26 August 2022. ^ "What is the OSI Model?". Forcepoint. 10 August 2018. Retrieved 20 May 2022. ^ a b c Tomsho, Greg (2016). Guide to Networking Essentials (7th ed.). Cengage. Retrieved 3 April 2022. ^ a b Davies, Howard; Bressan, Beatrice (26 April 2010). A History of International Research Networking: The People who Made it Happen. John Wiley & Sons. pp. 2–3. ISBN 978-3-527-32710-2. ^ Roberts, Dr. Lawrence G. (November 1978). "The Evolution of Packet Switching" (PDF). IEEE Invited Paper. Retrieved 26 February 2022. ^ Down, Peter John; Taylor, Frank Edward (1976). Why distributed computing?: An NCC review of potential and experience in the UK. NCC Publications. ISBN 9780850121704. ^ Radu, Roxana (2019). "Revisiting the Origins: The Internet and its Early Governance". Negotiating Internet Governance. Oxford University Press. pp. 43–74. doi:10.1093/oso/9780198833079.003.0003. ISBN 9780191871405. ^ a b c Andrew L. Russell (30 July 2013). "OSI: The Internet That Wasn't". IEEE Spectrum. Vol. 50, no. 8. ^ Campbell-Kelly, Martin; Garcia-Swartz, Daniel D (2013). "The History of the Internet: The Missing Narratives". Journal of Information Technology. 28 (1): 18–33. doi:10.1057/jit.2013.4. ISSN 0268-3962. S2CID 41013. SSRN 867087. ^ Sunshine, Carl A. (1989). Computer Network Architectures and Protocols. Springer Science & Business Media. p. 35. ISBN 978-1-4613-0809-6. ^ Hasman, A. (1995). Education and Training in Health Informatics in Europe: State of the Art, Guidelines, Applications. IOS Press. p. 251. ISBN 978-90-5199-234-2. ^ "ISO/OSI (Open Systems Interconnection): 1982 - 1983 | History of Computer Communications". historyofcomputercommunications.info. Retrieved 12 July 2024. ^ J. A. N. Lee. "Computer Pioneers by J. A. N. Lee". IEEE Computer Society. ^ "ITU-T X-Series Recommendations". ^ "Publicly Available Standards". Standards.iso.org. 30 July 2010. Retrieved 11 September 2010. ^ Russell, Andrew L. (28 April 2014). Open Standards and the Digital Age: History, Ideology, and Networks. Cambridge University Press. ISBN 978-1-139-91661-5. ^ Russell, Andrew L. (July–September 2006). "Rough Consensus and Running Code' and the Internet-OSI Standards War" (PDF). IEEE Annals of the History of Computing. 28 (3): 48–61. doi:10.1109/MAHC.2006.42. ^ "Standards Wars" (PDF). 2006. ^ Network World. IDG Network World Inc. 15 February 1988. ^ Network World. IDG Network World Inc. 10 October 1988. ^ Shaw, Keith (22 October 2018). "The OSI model explained: How to understand (and remember) the 7 layer network model". Network World. Archived from the original on 4 October 2020. Retrieved 16 May 2020. ^ "An OSI Model for Cloud". Cisco Blogs. 24 February 2017. Retrieved 16 May 2020. ^ Taylor, Steve; Metzler, Jim (23 September 2008). "Why it's time to let the OSI model die". Network World. Retrieved 16 May 2020. ^ a b Crawford, JB (27 March 2021). "The actual OSI model". ^ "Windows Network Architecture and the OSI Model". Microsoft Documentation. Retrieved 24 June 2020. ^ "What is a packet? | Network packet definition". Cloudflare. ^ "5.2 RM description for end stations". IEEE Std 802-2014, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture. ieee. doi:10.1109/IEEESTD.2014.6847097. ISBN 978-0-7381-9219-2. ^ International Organization for Standardization (15 November 1989). "ISO/IEC 7498-4:1989 – Information technology – Open Systems Interconnection – Basic Reference Model: Management framework". ISO Standards Maintenance Portal. ISO Central Secretariat. Retrieved 16 November 2024. ^ "ITU-T Recommendation X.224 (11/1995) ISO/IEC 8073, Open Systems Interconnection – Protocol for providing the connection-mode transport service". ITU. ^ Hooper, Howard (2012). CCNP Security VPN 642-648 Official Cert Guide (2 ed.). Cisco Press. p. 22. ISBN 9780132966382. ^ Spott, Andrew; Leek, Tom; et al. "What layer is TLS?". Information Security Stack Exchange. ^ Grigonis, Richard (2000). "Open Systems Interconnection (OSI) Model". Computer Telephony Encyclopedia. New York: CMP Books. p. 331. ISBN 978-1-929629-51-0. OCLC 48138823. ^ Mao, Stephen (2009). "Chapter 8: Fundamentals of communication networks". In Wyglinski, Alexander; Nekovee, Maziar; Hou, Thomas (eds.). Cognitive Radio Communications and Networks: Principles and Practice. Elsevier. p. 201. ISBN 978-0-08-087932-1. OCLC 635292718, 528550718. Partial preview at Google Books. ^ a b "ITU-T Recommendation X.800 (03/91), Security architecture for Open Systems Interconnection for CCITT applications". ITU. Retrieved 14 August 2015. ^ Hegering, Heinz-Gerd; Abeck, Sebastian; Neumair, Bernhard (1999). "Fundamental Structures of Networked Systems". Integrated management of networked systems: concepts, architectures, and their operational application. San Francisco, Calif.: Morgan Kaufmann. p. 54. ISBN 978-1-55860-571-8. OCLC 1341886747 – via Internet Archive. ^ Miao, Guowang; Song, Guocong (2014). Energy and spectrum efficient wireless network design. New York: Cambridge University Press. ISBN 978-1-139-62677-4. OCLC 898138775 – via Internet Archive. ^ "ITU-T Recommendation Q.1400 (03/1993)], Architecture framework for the development of signaling and OA&M protocols using OSI concepts". ITU. pp. 4, 7. ^ "ITU-T X.227 (04/1995)". ITU-T Recommendations. 10 April 1995. Retrieved 12 July 2024. ^ "ITU-T X.217". Open Systems Interconnection. 10 April 1995. Retrieved 12 July 2024. ^ "X.700: Management framework for Open Systems Interconnection (OSI) for CCITT applications". ITU. 10 September 1992. Retrieved 12 July 2024. ^ "X.711". Open Systems Interconnection. 15 May 2014. Retrieved 12 July 2024. ^ "ISO/IEC 9596-1:1998(en)". ISO. Retrieved 12 July 2024. ^ "ISO/IEC 9596-2:1993(en)". ISO. Retrieved 12 July 2024. ^ a b "Internetworking Technology Handbook – Internetworking Basics [Internetworking]". Cisco. 15 January 2014. Retrieved 14 August 2015. ^ "3GPP specification: 36.300". 3gpp.org. Retrieved 14 August 2015. ^ "Layering Considered Harmful". Some Internet Architectural Guidelines and Philosophy. December 2002. sec. 3. doi:10.17487/RFC3439. RFC 3439. Retrieved 25 April 2022. ^ Walter Goralski (2009). The Illustrated Network: How TCP/IP Works in a Modern Network (PDF). Morgan Kaufmann. p. 26. ISBN 978-0123745415. ^ a b c Tanenbaum, Andrew S. (2003). Computer networks. Upper Saddle River, NJ: Prentice Hall PTR. ISBN 978-0-13-066102-9. OCLC 50166590. ^ "OSI IS-IS Intra-domain Routing Protocol". IETF Datatracker. doi:10.17487/RFC1142. RFC 1142. Retrieved 12 July 2024. Day, John D. (2008). Patterns in Network Architecture: A Return to Fundamentals. Upper Saddle River, N.J.: Pearson Education. ISBN 978-0-13-225242-3. OCLC 213482801. Dickson, Gary; Lloyd, Alan (1992). Open Systems Interconnection. New York: Prentice Hall. ISBN 978-0-13-640111-7. OCLC 1245634475 – via Internet Archive. Piscitello, David M.; Chapin, A. Lyman (1993). Open systems networking : TCP/IP and OSI. Reading, Mass.: Addison-Wesley Pub. Co. ISBN 978-0-201-56334-4. OCLC 624431223 – via Internet Archive. Rose, Marshall T. (1990). The Open Book: A Practical Perspective on OSI. Englewood Cliffs, N.J.: Prentice Hall. ISBN 978-0-13-643016-2. OCLC 1415988401 – via Internet Archive. Russell, Andrew L. (2014). Open Standards and the Digital Age: History, Ideology, and Networks. Cambridge University Press. ISBN 978-1-139-91661-5. OCLC 881237495. Partial preview at Google Books. Zimmermann, Hubert (April 1980). "OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection". IEEE Transactions on Communications. 28 (4): 425–432. CiteSeerX 10.1.1.136.9497. doi:10.1109/TCOM.1980.1094702. ISSN 0090-6778. OCLC 5858668034. S2CID 16013989. OSI model at Wikipedia's sister projects Definitions from WiktionaryMedia from CommonsTextbooks from WikibooksResources from Wikiversity "Windows network architecture and the OSI model". Microsoft Learn. 2 February 2024. Retrieved 12 July 2024. "ISO/IEC standard 7498-1:1994 - Service definition for the association control service element". ISO Standards Maintenance Portal. Retrieved 12 July 2024. (PDF document inside ZIP archive) (requires HTTP cookies in order to accept licence agreement) "ITU Recommendation X.200". International Telecommunication Union. 2 June 1998. Retrieved 12 July 2024. "INformation CHanGe Architectures and Flow Charts powered by Google App Engine". infchg.appspot.com. Archived from the original on 26 May 2012. "Internetworking Technology Handbook". docwiki.cisco.com. 10 July 2015. Archived from the original on 6 September 2015. EdXD; Saikot, Mahmud Hasan (25 November 2021). "7 Layers of OSI Model Explained". ByteXD. Retrieved 12 July 2024. Retrieved from " 2Electrical connector commonly used in telephone and computer networks Left to right, modular connectors: 8P8C plug, 6P6C plug, 6P4C plug, 4P4C plug, 6P6C jack. An 8P8C modular plug. This is the common crimp-type plug, of the same kind pictured above crimped onto a cable (with molded sleeve). A modular connector is a type of electrical connector for cords and cables of electronic devices and appliances, such as in computer networking, telecommunication equipment, and audio headsets. Modular connectors were originally developed for use on specific Bell System telephone sets in the 1960s, and similar types found use for simple interconnection of customer-provided telephone subscriber premises equipment to the telephone network. The Federal Communications Commission (FCC) mandated in 1976 an interface registration system, in which they became known as registered jacks. The convenience of prior existence for designers and ease of use led to a proliferation of modular connectors for many other applications. Many applications that originally used bulkier, more expensive connectors have converted to modular connectors. Probably the best-known applications of modular connectors are for telephone and Ethernet. Accordingly, various electronic interface specifications exist for applications using modular connectors, which prescribe physical characteristics and assign electrical signals to their contacts. Modular connectors are often referred to as modular phone jack and plug, RJ connector, and Western jack and plug. The term modular connector arose from its original use in modular wiring components of telephone equipment by the Western Electric Company in the 1960s.[1] This includes the 6P2C used for telephone line connections and 4P4C used for handset connectors. Registered jack designations describe the signals and wiring used for voice and data communication at customer-facing interfaces of the public switched telephone network (PSTN). It is common to use a registered jack number to refer to the physical connector itself; for instance, the regular 8P8C modular connector type is often labeled RJ45 because the registered jack standard of the similar name RJ45S specified a similar, but modified, 8P8C modular connector. Similarly, various six-position modular connectors may be called RJ11. Likewise, the 4P4C connector is sometimes called RJ9 or RJ22 though no such official designations exist.[citation needed] The first types of small modular telephone connectors were created by AT&T in the mid-1960s for the plug-in handset and line cords of the Trimline telephone.[1] Driven by demand for multiple sets in residences with various lengths of cords, the Bell System introduced customer-connectable part kits and telephones, sold through PhoneCenter stores in the early 1970s.[2] For this purpose, Illinois Bell started installing modular telephone sets on a limited scale in June 1972. The patents by Edwin C. Hardesty and coworkers, US 3699498 (1972) and US 3860316 (1975), followed by other improvements, were the basis for the modular molded-plastic connectors that became commonplace for telephone cords by the 1980s. In 1976, these connectors were standardized nationally in the United States by the Registration Interface program of the Federal Communications Commission (FCC), which designated a series of Registered Jack (RJ) specifications for interconnection of customer-premises equipment to the PSTN.[3][4] Modular connectors have gender: plugs are considered to be male, while jacks or sockets are considered to be female. Plugs are used to terminate cables and cords, while jacks are used for fixed locations on surfaces of walls, panels, and equipment. Other than telephone extension cables, cables with a modular plug on one end and a jack on the other are rare. Instead, cables are usually connected using a female-to-female coupler, having two jacks wired back-to-back. Most modular connectors are designed with a latching mechanism that secures the physical connection. As a plug is inserted into a jack, a plastic tab on the plug locks against a ridge in the socket so that the plug cannot be removed without disengaging the tab by pressing it against the plug body. The standard orientation for installing a jack in a vertical surface is with the tab down. The modular plug is often installed with a boot, a plastic covering over the tab and body, to prevent the latching tab from hooking into other cords or edges, which may cause excessive bending or breaking of the tab. Such snagless cords are usually constructed by installing the protective boot before the modular plug is crimped. 8P8C modular plug contact numbering Modular connectors are designated using two numbers that represent the maximum number of contact positions and the number of installed contacts, with each number followed by P and C, respectively. For example, 6P2C is a connector having six positions and two installed contacts. Alternate designations omit the letters while separating the position and contact quantities with either an x (6x2) or a slash (6/2). When not installed, contacts are usually omitted from the outer positions inward, such that the number of contacts is almost always even. The connector body positions with omitted or unconnected contacts are unused for the electrical connection but ensure that the plug fits correctly. For instance, inexpensive telephone cords often have connectors with six positions and four contacts, to which are attached just two wires, carrying only line 1 from a one-, two-, or three-line jack. The contact positions are numbered sequentially starting from 1. When viewed head-on with the retention mechanism on the bottom, jacks will have contact position number 1 on the left and plugs will have it on the right. Contacts are numbered by the contact position. For example, on a six-position, two-contact plug, where the outermost four positions do not have contacts, the two contacts are numbered 3 and 4. Modular connectors are manufactured in four sizes, with four, six, eight, and ten positions. The insulating plastic bodies of 4P and 6P connectors have different widths, whereas 8P or 10P connectors share an even larger body width. 8P8C plug with contacts for solid wire (left) and stranded wire (right) Contacts for solid wire (top left) and stranded wire (bottom right) Internally, the contacts in the plugs have sharp prongs that, when crimped, displace the wire insulation and connect with the conductors inside—a mechanism known as insulation displacement. Cables have either solid or stranded (tinsel wire) conductors, and a given plug is designed for only one type. The sharp prongs are different in the connectors made for each type of wire, and a mismatch between plug type and wire type results in unreliable connections. A

modular plug for solid (single-strand) wire often has three slightly splayed prongs on each contact to securely surround and grip the conductor while scraping along the outside, and a plug for stranded wire has prongs that are designed to pierce the insulation and go straight through to contact multiple wire strands. Some modular connectors are indexed, meaning their dimensions are intentionally non-standard, preventing connections with connectors of standard dimensions. The means of indexing may be non-standard cross-sectional dimensions or shapes, retention mechanism dimensions or configuration. For example, a Modified Modular Jack using an offset latching tab was developed by Digital Equipment Corporation to prevent accidental interchange of data and telephone cables. Modular connector typical dimensions (millimeters) Connector Length Width Height 4P4C[citation needed] 7.7 6P6C[5] 13.34 9.85 6.60 8P8C[6] 22.48 11.68 8.00 The dimensions of modular connectors are such that a narrower plug can be inserted into a wider jack that has more positions than the plug, leaving the jack's outermost contacts unconnected. The height of the plug's insertion area is 0.260 inches (6.60 mm) and the contacts are 0.040 inches (1.02 mm) apart (contact pitch), so the width is dependent on the number of pin positions.[7][8] However, not all plugs from all manufacturers have this capability, and some jack manufacturers warn that their jacks are not designed to accept smaller plugs without damage. If an inserted plug lacks slots to accommodate the jack's contacts at the outermost extremes, it may permanently deform the outermost contacts of an incompatible jack. Excessive resistance may be encountered when inserting an incompatible plug, as the outermost contacts in the jack are forcibly deformed. Special modular plugs have been manufactured (for example, the Siemon UP-2468[9]) which have extra slots beyond their standard contacts, to accommodate the wider jack's outermost contacts without damage. These special plug connectors can be visually identified by carefully looking for the extra slots molded into the plug. The molded plastic bodies of the special plugs may also be colored with a light blueish tinge to aid in quick recognition. The special plugs are preferred for test equipment and adapters, which may be rapidly connected to a large number of corresponding connectors in quick succession for testing purposes. The use of the special plugs avoids inadvertent damage to the equipment under test, even when a narrower plug is inserted into a nominally incompatible wider jack. A modular plug crimping tool with exchangeable crimping dies Termination of cables with modular connectors is similar across the various number of positions and contacts in the plug. The crimping tool contains a die that is often exchangeable and is closely matched to the shape and pin count of the modular plug. A crimping die-set looks similar to an 8P8C jack, except for the eight teeth lining the top portion of the die. When the tool is operated, the die compresses around the 8P8C plug. As the die compresses, these teeth force the plug contacts into the conductors of the cable being terminated. The crimper may also permanently deform part of the plastic plug body in such a way that it grips the outer sheath of the cable for secure fastening and strain relief. These actions permanently attach the plug to the cable. The contact assignments (pinout) of modular connectors vary by application. Telephone network connections are standardized by registered jack designations, and Ethernet over twisted pair is specified by the ANSI/TIA-568 standard. For other applications, standardization may be lacking; for example, multiple conventions exist for the use of 8P8C connectors in RS-232 applications. For this reason, D-sub-to-modular adapters are typically shipped with the D-sub contacts (pins or sockets) terminated but not inserted into the connector body so that the D-sub-to-modular contact pairing can be assigned as needed. 4P4C modular connector on a handset cord. Wired telephone that uses 4P4C connectors for the coiled handset cord The four-position four-conductor (4P4C) connector is the standard modular connector used on both ends of telephone handset cords and is therefore often called a handset connector.[10] This handset connector is not a registered jack, because it was not intended to connect directly to telephone lines. However, it is often referred to as RJ9, RJ10, or RJ22. Handsets and often headsets for use with telephones commonly use a 4P4C connector. The two center pins are commonly used for the receiver, and the outer pins connect the transmitter so that a reversal of conductors between the ends of a cord does not affect the signal routing. This may differ for other equipment, including hands-free headsets. The Macintosh 128K, Macintosh 512K and Macintosh Plus from Apple as well as the Amiga 1000 from Commodore use 4P4C connectors to connect the keyboard to the main computer housing. The connector provides power to the keyboard on the outer two contacts and receives data signals on the inner pair. The cable between the computer and the keyboard is a coiled cord with an appearance very similar to a telephone handset cable.[11] The connector on the Amiga 1000 uses crossover wiring, similar to a telephone handset. The connector wiring on the Apple computers, however, requires a polarized straight-through pinout. Using a telephone handset cable instead of the supplied cable could short out the +5 volt DC supply and damage the Apple computer or the keyboard.[12] Modular connectors are often used for data links, such as serial line connections, because of their compact dimensions. For example, some DirecTV set-top boxes include a 4P4C data port with an adapter cord to connect to a computer serial port to control the set-top box.[13] 6P4C crimp-on–style connector Modular plugs are described by the maximum number of physical contact positions and the actual number of contacts installed in these positions. The 6P2C, 6P4C, and 6P6C modular connectors are probably best known for their use as RJ11, RJ14, and RJ25 non-powered registered jacks, respectively (and 6P4C and 6P6C for powered RJ11 and RJ14, power being delivered on the outer pairs). These interfaces use the same six-position modular connector body but have different numbers of pins installed. RJ11 is a jack, a physical interface, by definition used for terminating a single telephone line. RJ14 is similar, but for two lines, and RJ25 is for three lines. RJ61 is a similar registered jack for four lines, but uses 8P8C connectors. Cables sold as RJ11 (the name of a single-jack, not a cable) often actually use 6P4C connectors (six positions, four contacts). Two of its six possible contact positions connect tip and ring of a single telephone line, and the other two contact positions may be unused, carry a second line, or provide low-voltage power for night light or other features on the telephone set. In some installations, an extra contact was also required for the ground connection for selective ringers. The pins of the 6P6C connector are numbered 1 to 6, counting left to right when holding the connector tab side down with the opening for the cable facing the viewer. Position Pair T/R ± RJ11 RJ14 RJ25 Twisted pair colors 25-pair colors[A] Old colors[B] German colors[C] Australian colors Dutch colors[D] Diagram 1 3 T + Does not appear Does not appear T3 white/green white/green white pink orange Does not appear 6P6C connector showing the location of pin 1 2 2 T + Does not appear T2 T2 white/orange white/orange black green red orange 3 1 R − R1 R1 R1 blue blue/white red white blue red 4 1 T + T1 T1 T1 white/blue white/blue green brown white blue 5 2 R − Does not appear R2 R2 orange orange/white yellow yellow black white 6 3 R − Does not appear Does not appear R3 green green/white blue gray green Does not appear ^ Established in the 1950s for polyethylene-insulated conductor (PIC) cable.Horn, F. W. (October 1958). "'Even-Count' Cable" (PDF). Bell Laboratories Record. 37 (5): 208–217. Retrieved October 13, 2022. ^ While the old solid color code was well established for pair 1 and usually pair 2, there are several conflicting conventions for pair 3 (and sometimes even pair 2). The colors shown above were taken from a vendor of silver satin flat 8-conductor phone cable that claims to be standard. 6-pair solid (old) bellwire cables previously used by the Bell System use white for pair 3 tip but some vendors' cable may substitute orange for white. At least one other vendor of flat 8-conductor cable uses the sequence blue, orange, black, red, green, yellow, brown and white/slate.[citation needed] ^ This color scheme originates in the (withdrawn) national standard DIN 47100. The scheme shown here is the correct color code for interfacing with the RJ connector standards. ^ "(nl) Support document for the 'PTT norm 88'" (PDF). Watel (in Dutch). p. 8. Archived (PDF) from the original on 2016-10-08. However, with German domestic telephone equipment, and that in some neighboring countries, 6P4C plugs and sockets are typically only used to connect the telephone cord to the phone base unit, whereas the mechanically different TAE connector is used at the other end to connect to a service provider interface. Older base units may accommodate the additional connectors of TAE (E, W, a2, b2) and may feature non-RJ standard sockets that can be connected directly to TAE plugs. Further, flat DIN 47100 cables typically place the wires in ascending order. When used directly with 6P4C plugs, the color coding may be undetermined. In the powered version of the RJ11 interface, pins 2 and 5 (black and yellow) may carry low-voltage AC or DC power. While the telephone line on pins 3 and 4 (red and green) supplies enough power for most telephone terminals, old telephone terminals with incandescent lights, such as the Western Electric Princess and Trimline telephones, need more power than the phone line can supply. Typically, the power on pins 2 and 5 is supplied by an AC adapter plugged into a nearby power outlet which potentially even supplies power to all of the jacks in the house. Structured cabling networks adhering to ANSI/TIA-568, ISO/IEC 11801 (or ISO/IEC 15018 for home networks) are widely used for both computer networking and analog telephony. These standards specify the T568A or T568B wiring arrangements compatible with Ethernet. The 8P8C jack used by structured cabling physically accepts the 6-position connector that fits RJ11, RJ14 and RJ25. Only lines 1 and 2 have electrical compatibility, with T568A wiring, and only line 1 with T568B wiring, because Ethernet-compatible pin assignments split the third pair of RJ25 across two separate cable pairs, rendering that pair unusable by an analog phone. (With T568B wiring, a telephone may connect to line 3 as line 2.) Both the third and fourth pairs of RJ61 are similarly split. The incompatible T568A and T568B layouts were necessary to preserve the electrical properties of the third and fourth pairs for Ethernet, which operates at much higher frequencies than analog telephony. Because of these incompatibilities, and because RJ25 and RJ61 were never very common, the T568A and T568B conventions have largely displaced RJ25 and RJ61 for telephones with more than two lines. An 8P8C modular plug not yet crimped onto a cable An 8P8C female modular connector with a key cut (the connector used in the obsolete RJ45S specification) The 8 position 8 contact (8P8C) connector is a modular connector commonly used to terminate twisted pair and multi-conductor flat cable. These connectors are commonly used for Ethernet over twisted pair, registered jacks and other telephone applications, RS-232 serial communication using the ANSI/TIA-568 (formerly TIA/EIA-568) and Yost standards, and other applications involving unshielded twisted pair, shielded twisted pair, and multi-conductor flat cable. An 8P8C modular connection consists of a male plug and a female jack, each with eight equally spaced contacts. On the plug, the contacts are flat metal bars positioned parallel to the connector body. Inside the jack, the contacts are metal spring wires angled away from the insertion interface. When the plug is mated with the jack, the contacts meet and create an electrical connection. The spring force of the jack contacts ensures a good interface. Left: Generic 8P8C (or 8PMJ, 8-position modular jack) male connector. Right: 8P8C male connector with key, which mates with RJ41S, RJ45S, and RJ48S Although commonly referred to as RJ45 in the context of Ethernet and structured cabling, RJ45 originally referred to a specific wiring configuration of an 8P8C female connector.[14][15][16] The original telephone-system-standard RJ45 plug has a key that excludes insertion in an un-keyed 8P8C socket.[17] The original RJ45S[a] was intended for high-speed modems and is obsolete. The RJ45S jack mates with a keyed 8P2C modular plug,[18][19] and has pins 4 and 5 (the middle positions) wired for the ring and tip conductors of a single telephone line and pins 7 and 8 shorting a programming resistor. This is a different mechanical interface and wiring scheme than ANSI/TIA-568 T568A and T568B schemes with the 8P8C connector in Ethernet and telephone applications. Generic 8P8C modular connectors are similar to those used for the RJ45S variant, although the RJ45S plug is keyed and not compatible with non-keyed 8P8C modular jacks. Telephone installers who wired RJ45S modem jacks or RJ61X telephone jacks were familiar with the pin assignments of the standard. However, the standard unkeyed modular connectors became ubiquitous for computer networking and informally inherited the name RJ45. The shape and dimensions of an 8P8C modular connector are specified for US telephone applications by the Administrative Council for Terminal Attachment (ACTA) in national standard ANSI/TIA-1096-A and international standard ISO-8877. This standard does not use the short term 8P8C and covers more than just 8P8C modular connectors, but the 8P8C modular connector type is the eight-position connector type described therein, with eight contacts installed. For data communication applications (LAN, structured cabling), International Standard IEC 60603 specifies in parts 7-1, 7-2, 7-4, 7-5, and 7-7 not only the same physical dimensions but also high-frequency performance requirements for shielded and unshielded versions of this connector for carrying frequencies up to 100, 250 and 600 MHz. T568A wiring, defined in TIA-568 T568B wiring, defined in TIA-568 8P8C connectors are frequently terminated using the T568A or T568B assignments that are defined in ANSI/TIA-568. The drawings to the right show that the copper connections and pairing are the same, the only difference is that the orange and green pairs (colors) are swapped. A cable wired as T568A at one end and wired as T568B at the other end (Tx and Rx pairs reversed) is an Ethernet crossover cable. Before the widespread acceptance of auto MDI-X capabilities, a crossover cable was needed to interconnect similar network equipment (such as Ethernet hubs to Ethernet hubs). Crossover cables are sometimes still used to connect two computers together without a switch or hub, however, most network interface cards (NIC) in use today implement auto MDI-X to automatically configure themselves based on the type of cable plugged into them. A cable wired the same at both ends is called a patch or straight-through cable, because no pin/pair assignments are swapped. If a patch or straight cable is used to connect two computers with auto MDI-X capable NICs, one NIC will configure itself to swap the functions of its Tx and Rx wire pairs. Pin T568A pair T568A color T568B pair T568B color 10BASE-T/100BASE-TX signal[20] 1000BASE-T/10GBASE-T signal Wire Diagram 1 3 white/green stripe 2 white/orange stripe TD+ DA+ tip Pin numbering on plug face. Connected pins on plug and jack have the same number. 2 3 green solid 2 orange solid TD− DA− ring 3 2 white/orange stripe 3 white/green stripe RD+ DB+ tip 4 1 blue solid 1 blue solid not used DC+ ring 5 1 white/blue stripe 1 white/blue stripe not used DC− tip 6 2 orange solid 3 green solid RD− DB− ring 7 4 white/brown stripe 4 white/brown stripe not used DD+ tip 8 4 brown solid 4 brown solid not used DD− ring Two types of 8P8C plugs and crimping tools for installing the plug onto a cable are commonly available: Western Electric/Stewart Stamping (WE/SS) and Tyco/AMP. While the two types are similar, the tooling and plug types cannot be interchanged.[b] WE/SS compatible plugs are available from a large number of manufacturers, whereas Tyco/AMP plugs are produced exclusively by Tyco Electronics.[citation needed] Both types of modular plugs can be mated with a standard 8P8C modular jack. Both types of 8P8C plugs are available in shielded and unshielded varieties for different attenuation tolerances as needed. Shielded plugs are more expensive and require shielded cable, but have a lower attenuation, and may reduce electromagnetic interference. Although a narrower 4-pin and 6-pin plug fits into the wider 8-pin jack and makes a connection with the available contacts on the plug, because the body of the smaller connector may stress the remaining contacts,[c] the smaller connector can potentially damage the springs of the larger jack. 8P8C connectors are commonly used in computer networking applications, where interconnecting cables are terminated at each end with an 8P8C modular plug wired according to TIA/EIA standards. Most wired Ethernet communications are carried over Category 5e or Category 6 cable terminated with 8P8C modular plugs. The connector is also used in other telecommunications connections, including ISDN and T1. Where building network and telephone wiring is pre-installed, the center (blue) pair is often used to carry telephony signals. While this allows an RJ11 plug to connect, it may damage the modular jack; an approved converter prevents damage. In landline telephony, an 8P8C jack is used at the point a line enters the building to allow the line to be broken to insert automatic dialing equipment, including intrusion alarm panels. The EIA/TIA-561 standard describes the use of 8P8C connectors for RS-232 serial interfaces.[23] This application is common as a console interface for network equipment, such as switches, routers, and headless computers. 8P8C modular connectors are also commonly used as a microphone connector for PMR, LMR, and amateur radio transceivers. Frequently the pinout is different, usually mirrored (i.e. what would be pins 1 to 8 in the ANSI/TIA-568 standard might be pins 8 to 1 in the radio and its manual). In analog mobile telephony, the 8P8C connector was used to connect an AMPS cellular handset to its (separate) base unit; this usage is now obsolete. The physical connector is standardized as the IEC 60603-7 8P8C modular connector with different categories of performance. The physical dimensions of the male and female connectors are specified in ANSI/TIA-1096-A and ISO-8877 standards and normally wired to the T568A and T568B pinouts specified in the ANSI/TIA-568 standard to be compatible with both telephone and Ethernet. A similar standard jack once used for modem and data connections, the RJ45S, used a keyed variety of the 8P8C body with an extra tab that prevents it from mating with other connectors; the visual difference compared to the more common 8P8C is subtle, but it is a different connector. The original RJ45S[18][24] keyed 8P2C modular connector, obsolete today, had pins 5 and 4 wired for tip and ring of a single telephone line and pins 7 and 8 shorting a programming resistor. Electronics catalogs commonly advertise 8P8C modular connectors as RJ45. An installer can wire the jack to any pin-out or use it as part of a generic structured cabling system such as ISO/IEC 15018 or ISO/IEC 11801 using 8P8C patch panels for both phone and data. A router-to-router crossover cable uses two 8-position connectors and a unshielded twisted pair (UTP) cable with differently wired connectors at each end. The pin arrangement for a 10P10C socket A 10P10C plug The 10P10C connector is commonly referred to as an RJ50 connector,[25] although this was never a standard registered jack. The 10P10C has 10 contact positions and 10 contacts. The most common uses of the 10P10C connector are in proprietary data transfer systems.[26] ANSI/TIA-968-A: Telephone terminal equipment: Technical requirements for connection of terminal equipment to the telephone network at the Wayback Machine (archived 2018-09-28) ANSI/TIA-1096-A: Telecommunications telephone terminal equipment connector requirements for connection of terminal equipment to the telephone network IEC 60603-7-1: Connectors for electronic equipment: Part 7-1: Detail specification for 8-way, shielded free and fixed connectors with common mating features, with assessed quality IEC 60603-7-2: Connectors for electronic equipment: Part 7-2: Detail specification for 8-way, unshielded, free and fixed connectors, for data transmissions with frequencies up to 100 MHz IEC 60603-7-4: Connectors for electronic equipment: Part 7-4: Detail specification for 8-way, unshielded, free and fixed connectors, for data transmissions with frequencies up to 250 MHz IEC 60603-7-5: Connectors for electronic equipment: Part 7-5: Detail specification for 8-way, shielded, free and fixed connectors, for data transmissions with frequencies up to 250 MHz IEC 60603-7-7: Connectors for electronic equipment: Part 7-7: Detail specification for 8-way, shielded, free and fixed connectors, for data transmissions with frequencies up to 600 MHz ISO/IEC 8877, EN 28877: Information Technology—Telecommunications and Information Exchange between Systems—Interface Connector and Contact Assignments for ISDN Basic Access Interface Located at Reference Points S and T US government documents define registered jack applications of modular connectors for telecommunications.[d] See Registered jack § History and authority BS 6312 – British equivalent to RJ25 EtherCON – ruggedized 8P8C Ethernet connector XJACK - retractable 8P8C Ethernet connector GG45 TERA ^ The often omitted S suffix indicates this is a wiring configuration supporting a single telephone line. ^ WE/SS and Tyco/AMP 8P8C plugs have different spacings for the cable strain relief.[21][22] Using a WE/SS 8P8C crimp die set on a Tyco/AMP 8P8C plug crushes the top of the connector and damages the crimp die set, and vice versa. ^ The body of a 6P6C or 4P4C plug typically projects out by more than one millimeter further than the contacts and presses the outermost contacts of the larger connector further than if a full-size connector were inserted. ^ 4P4C and 10P10C connectors are not defined in these standards. ^ a b Krumreich C.L., Mosing L.W., The Evolution of a Telephone, Bell Laboratories Record 44(1) p.14 (January 1966) ^ Walden S.W., Telephone Sets Go Mod (Modular, That Is), Bell Laboratories Record, Vol. 52(8) p. 238 (Sept. 1974) ^ AT&T, Registration Interface—Selection and General Information, Bell System Practices, Section 463-400-100 Issue 1, May 1976 ^ FCC 47 CFR Part 68 Connection of Terminal Equipment to the Telephone Network, Section 68.502 superseded by T1.TR5-1999 ^ "Six Conductor/Six Position Line Cord Module" (PDF). Bel-Stewart Connector. Bel. Retrieved 3 August 2021. ^ "RJ-45 Plug for Proposed CAT 6 Specifications" (PDF). Molex #449150001, Modular Plug, Category 6, Long Body, Unshielded, 8/8. Molex, LLC. Retrieved 3 August 2021. ^ "Six Conductor/Six Position Line Cord Module" (PDF). Bel-Stewart Connector. Bel. Retrieved 3 August 2021. ^ "RJ-45 Plug for Proposed CAT 6 Specifications" (PDF). Molex #449150001, Modular Plug, Category 6, Long Body, Unshielded, 8/8. Molex, LLC. Retrieved 3 August 2021. ^ "Universal Modular Plug". ^ BICSI (October 7, 2002). "Background Information". Telecommunications Cabling Installation (2nd ed.). McGraw-Hill Professional. p. 88. ISBN 0-07-140979-3. 4-position and 4-contact connectors are used primarily for telephone handset cords. ^ "Apple Macintosh Plus", My Old Computers, archived from the original on 2009-02-27, retrieved 2010-10-16. ^ "Mac Plus Keyboard Cable", Syrinx, UK: Megadon, ...the cable is the same as the telephone cable that connects handsets to the phone, unfortunately [...] this type of cable and pretty much any type of pre manufactured cable [...] is wired wrong for the Mac Plus. Under no circumstances should you use this cable as you will damage your keyboard and/or your Mac! ^ "Direc TV Channel Control" (wiki). GB-PVR. Archived from the original on 2008-10-19. Each end of a handset cord is wired opposite the other... ^ Trulove 2005, pp. 23, 132: Designing LAN Wiring Systems: The 8-pin modular jack is sometimes referred to as an "RJ-45", because the connector/jack components are the same. However, RJ-45 actually applies to a special purpose jack configuration that is not used in LAN or standard telephone wiring. […] Work Area Outlets: Modular jacks are often referred to as "RJ-45" jacks. This is not really the correct moniker, although it is in very common use. ^ Oliviero, Andrew; Woodward, Bill (July 20, 2009). "Connectors". Cabling: The Complete Guide to Copper and Fiber-Optic Networking (4th ed.). Sybex. p. 294. ISBN 978-0-470-47707-6. The RJ (registered jack) prefix is one of the most widely (and incorrectly) used prefixes in the computer industry; nearly everyone, including people working for cabling companies, is guilty of referring to an eight-position modular jack (sometimes called an 8P8C) as an RJ-45. ^ Semenov, Andrey B.; Strizhakov, Stanislav K.; Suncheley, Igor R. (October 3, 2002). "Electrical Cable Connectors". Structured cable systems. Springer. p. 129. ISBN 3-540-43000-8. The traditional 8-contact connector, which is called Western Plug, 8PMJ (8-position modular jack), 8P8C (8 position 8 conductor), or somewhat incorrectly RJ-45, is used widely in SCS practice. ^ Trulove 2005, p. 219: User Cords and Connectors: This 8-pin modular plug is probably the most subject to name abuse, because it resembles the specialized RJ-45 connector. However, the RJ-45 wiring pattern (which includes an interface programming resistor) is so radically different from that of T568A and B that it really should not be called by that name at all. ^ a b Modular jack wiring, Ontario, California: HVS, archived from the original on 2010-02-08 ^ Modular wiring reference, Siemon ^ IEEE 802.3 14.5.1 MDI connectors ^ "Stewart Connector 937-SP-3088 – Eight conductor/eight position line cord module" (PDF). Glen Rock, Pennsylvania: Bel Stewart Connector. 2006-02-01. Archived from the original (PDF) on 2018-04-18. Retrieved 2018-04-18. ^ "Tyco/AMP 5-554739-2 – Modular plug assembly, 8 position, flat oval cable" (PDF). Harrisburg, Pennsylvania: Tyco Electronics. 2008-03-31. Archived from the original (PDF) on 2011-07-24. Retrieved 2009-09-10. ^ "RJ45", Layer 1, Zytrax. ^ "Modular Wiring Reference". Siemon. Retrieved 2010-10-14. ^ "RJ50 - Everything you need to know !". instrumentic.info. 2023-01-15. Retrieved 2024-08-20. ^ 10 pin RJ50 (10P10C) male (connector diagram and applications), Pinouts guide, archived from the original on 2013-05-18, retrieved 2010-10-17 Trulove, James (December 19, 2005), LAN wiring (3rd ed.), McGraw-Hill Professional, ISBN 0-07-145975-8. Wikimedia Commons has media related to Modular connectors. How to Make a Network Cable, a how-to article from wikiHow Premium Modular Plugs at the Wayback Machine (archived 2013-02-15) Catalog page showing the difference between solid and stranded contacts Retrieved from "

and other sensitive data. HSTS (HTTP Strict Transport Security) - web security policy mechanism used to protect against protocol downgrade attacks and cookie hijacking. HTML (Hypertext Markup Language) - is the standard markup language for creating Web pages. HTTP (Hypertext Transfer Protocol) - HTTP is the foundation of the World Wide Web, and is used to load webpages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message. HTTP uses port 80. HTTPS (Hypertext Transfer Protocol Secure) - a secure version of HTTP that uses encryption to protect data in transit. HTTPS uses port 443. IaaS (Infrastructure as a Service) - a cloud computing model in which infrastructure resources, such as servers and storage, are provided by a third-party provider. IAM (Identity and Access Management) - a cybersecurity practice that enables IT administrators to restrict access to organizational resources so that only the people who need access have access. ICMP (Internet Control Message Protocol) - a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. IDS (Intrusion Detection System) - a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat. IPS (Intrusion Prevention System) - a network security technology that goes beyond the capabilities of an IDS (Intrusion Detection System) by actively preventing identified threats from being carried out. An IPS monitors network traffic, just like an IDS, but it can also take action to prevent attacks. IEEE (Institute of Electrical and Electronics Engineers) - The IEEE describes itself as the world's largest technical professional society -- promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members. IKE (Internet Key Exchange) - a standard protocol used to set up a secure and authenticated communication channel between two parties via a virtual private network (VPN). IMAP (Internet Message Access Protocol) - an Internet standard protocol used by email clients to retrieve email messages from a mail server over a TCP/IP connection. IMAP uses port 143. IoT (Internet Of Things Devices) - physical devices that are connected to the internet and that can exchange data with each other. IP (Internet Protocol) - a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. IPv4 (Internet Protocol version 4) - an IPv4 address is a 32-bit address that is usually represented in dotted decimal notation, with a decimal value representing each of the four octets (bytes) that make up the address. IPv6 (Internet Protocol version 6) - a network protocol that serves as the successor to IPv4. The purpose of IPv6 is to provide a larger address space for the internet as the number of connected devices continues to grow. One of the main differences between IPv6 and IPv4 is the size of the address space. IPv4 uses 32-bit addresses, allowing for approximately 4.3 billion unique addresses. In contrast, IPv6 uses 128-bit addresses, which allows for an almost unlimited number of unique addresses. ISA (Interconnection Security Agreement) - a document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. ISO (International Organization for Standardization) - an international standard-setting organization. ISP (Internet Service Provider) - a company that provides Internet access to customers. JSON (JavaScript Object Notation) - a lightweight data interchange format. LDAP (Lightweight Directory Access Protocol) - is a software protocol for enabling anyone to locate data about organizations, individuals and other resources such as files and devices in a network -- whether on the public internet or a corporate intranet. LDAP is a "lightweight" version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is considered lightweight because it uses a smaller amount of code than other protocols. MAC (Media Access Control) - a unique identifier assigned to a network interface controller (NIC). MAC (Mandatory Access Control) - limiting access to resources based on the sensitivity of information. MCSP (Managed Cloud Service Provider) - provides managed cloud services to customers. Managed cloud services are a type of cloud computing service in which a third-party provider manages and delivers cloud computing resources and services to customers over the internet. MFA (Multi-Factor Authentication) - a security feature that requires multiple forms of authentication to access a resource. MITB (Man In The Browser) - an MITB attack injects malicious software (malware) into a victim's web browser. The malware typically exploits vulnerabilities in the browser or its plugins to intercept and manipulate data exchanged between the browser and the websites the user visits. MITM (Man-in-the-Middle) - a type of cyber attack in which an attacker intercepts communications between two parties in order to either steal or change the data in transit. MSSP (Managed Security Service Provider) - provides managed security services to customers, typically on a subscription basis. MTBF (Mean Time Between Failures) - average amount of time between system failure which shows how reliable a system is. MTTD (Mean Time To Detect) - average time it takes for an organization to detect a security incident or breach after it occurs. MTTR (Mean Time To Repair) - average time that it takes to fix a system. NAC (Network Access Control) - a system used to control access to a network based on the identity of the user or device. NAT (Network Address Translation) - a technique used to map private IP addresses to public IP addresses. NDA (Non Disclosure Agreement) - contract that prevents any side of the business to give away the secrets to others. NFC (Near Field Communication) - short-range wireless communication technology that enables data exchange between devices that are within close proximity to each other, typically within a few centimeters. NIDS (Network Intrusion Detection System) - a system used to detect unauthorized activity on a network. NIPS (Network Intrusion Prevention System) - type of security system that is used to detect and prevent unauthorized access, attacks, and other malicious activity on a network. NIST (National Institute of Standards and Technology) - a U.S. government agency that develops standards for technology and engineering. NTFS (New Technology File System) - a file system used in Windows operating systems. OAuth (Open Authorization) - open standard protocol that is used for authorization and authentication between applications or services. It allows users to grant access to their private resources stored on one website to another website or application, without sharing their credentials, such as passwords. OCSP (Online Certificate Status Protocol) - a protocol used to check the validity of a digital certificate. OSI (Open Systems Interconnection) - conceptual framework that is used to standardize and describe the communication functions of a telecommunication or computing system. The OSI model is divided into seven layers, each with a specific function, that define the communication process between two devices in a network. PaaS (Platform as a Service) - a cloud computing model in which a third-party provider offers a platform for developing and deploying applications. PAM (Privileged Access Management) - type of security solution that helps organizations manage and control access to privileged accounts and systems. PCI DSS (Payment Card Industry Data Security Standard) - a set of security standards for protecting credit card data. PGP (Pretty Good Privacy) - an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. PMF (Protected Management Frames) - security feature used in Wi-Fi networks to protect against certain types of attacks that can be carried out against wireless management frames. POP3 (Post Office Protocol version 3) - a protocol used to retrieve email messages from a mail server. PPP (Point-to-Point Protocol) - a protocol used to establish a direct connection between two devices. RAID (Redundant Array of Inexpensive Disks) - a technique used to increase the reliability and performance of data storage. RADIUS (Remote Authentication Dial-In User Service) - networking protocol that is used to provide centralized authentication, authorization, and accounting (AAA) management for users who connect and use network services. RADIUS is commonly used in enterprise and service provider environments, such as Wi-Fi networks, virtual private networks (VPNs), and dial-up services. RAM (Random Access Memory) - computer's short-term memory, where the data that the processor is currently using is stored. Your computer can access RAM memory much faster than data on a hard disk, SSD, or other long-term storage device, which is why RAM capacity is critical for system performance. RAT (Remote Access Trojan) - a type of malware that allows an attacker to remotely control a victim's computer. RDP (Remote Desktop Protocol) - a protocol used to remotely access and control a desktop computer. REST (Representational State Transfer) - software architectural style that describes the architecture of the web. RFID (Radio Frequency Identification) - a technology used for tracking and identifying objects using radio waves. RIPEMD (RACE Integrity Primitives Evaluation Message Digest) - a cryptographic hash function. RTO (Recovery Time Objective) - the maximum amount of time it takes to recover data after a disaster. RTOS (Real Time Operating System) - an operating system commonly found in Internet of Things Devices. RBAC (Rule Based Access Control) - high level rules that determine how, where and when employees can access spaces or resources. S/MIME (Secure/Multipurpose Internet Mail Extensions) - standard for secure email messaging that provides encryption and digital signing capabilities. SAN (Storage Area Network) - specialized, high-speed network that provides network access to storage devices. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SaaS (Software as a Service) - a cloud computing model in which a third-party provider offers software applications. SAE (Simultaneous Authentication of Equals) - key exchange protocol that provides stronger security and that replaced PSK in WPA2. SATCOM (Secure Satellite Communications) - refers to the use of satellite technology for communication purposes, including voice, data, and video transmission. SCADA (Supervisory Control and Data Acquisition) - a system used to control and monitor industrial processes. SCP (Secure Copy Protocol) - a protocol used to securely transfer files between two devices. SFTP (Secure File Transfer Protocol) - a protocol used to securely transfer files between two devices. SHA (Secure Hash Algorithm) - SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions. SID (Security Identifier) - a unique identifier used to identify a user or group in Windows operating systems. SIEM (Security Information and Event Management) - type of security solution that provides real-time analysis of security alerts and events generated by network hardware and applications. SMTP (Simple Mail Transfer Protocol) - a protocol used to send email messages between servers. SNMP (Simple Network Management Protocol) - a protocol used to manage and monitor network devices. SOAR (Security Orchestration, Automation and Response) - security technology that helps organizations automate and streamline their security operations and incident response processes. SoC (System on Chip) - integrated circuit (IC) that combines various components of a computer or electronic system into a single chip. SQL (Structured Query Language) - a programming language used for managing and manipulating data in relational databases. SSH (Secure Shell) - a protocol used for secure remote access to a device. Uses Port 22. SSL (Secure Sockets Layer) - SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern TLS encryption used today. A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP". STP (Spanning Tree Protocol) - a protocol used to prevent loops in a network topology. STIX (Structured Threat Information Exchange) - designed to support the sharing of cybersecurity threat intelligence between different organizations and cybersecurity technologies. TACACS+ (Terminal Access Controller Access Control System Plus) - protocol used for providing centralized authentication, authorization, and accounting (AAA) services for network devices such as routers, switches, and firewalls. TAXII (Trusted Automated Exchange of Indicator Information) - application protocol for exchanging Cyber Threat Intelligence over HTTPS. It works with STIX. TCP (Transmission Control Protocol) - a protocol used to establish a reliable connection between two devices. Uses three way handshake. TOTP (Time Based One Time Password) - TOTP uses a timestamp and a time-based factor to generate the password. Specifically, TOTP calculates the message authentication code based on the current time and a time interval (usually 30 seconds). TPM (Trusted Platform Module) - chip on motherboard that can be used to store critical information such as encryption keys. TPM can be used for FDE (Full Disk Encryption). UBA (User Behaviour Analysis) - checks whether user activity sticks out from their usual activity. UDP (User Datagram Protocol) - a protocol used for sending datagrams over a network. Connectionless. UEFI (Unified Extensible Firmware Interface) - modern version of BIOS. UEFI can be used for securely starting a device. URL (Uniform Resource Locator) - a unique identifier used to locate a resource on the Internet. It is also referred to as a web address. VLAN (Virtual Local Area Network) - a logical grouping of devices on a network that are grouped together based on factors such as function, department, or location, rather than physical location. VM (Virtual Machine) - a software environment that emulates a physical computer. VPN (Virtual Private Network) - a virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments. VTP (VLAN Trunking Protocol) - proprietary protocol used by Cisco switches to exchange VLAN information. With VTP, you can synchronize VLAN information (such as VLAN ID or VLAN name) with switches inside the same VTP domain. WAF (Web Application Firewall) - firewall used to protect web applications. WAP (Wireless Access Point) - network device that receives and transmits data over WLAN. WEP (Wired Equivalent Privacy) - wired equivalent privacy is meant to protect Wi-Fi transmissions by encrypting the data so outsiders who are not inside the encrypted network will not be able to read the messages or data contained within. WEP is better than no security at all, and it is still used on older devices that do not support WPA or WPA2. WIDS (Wireless Intrusion Detection System) - a system used to detect unauthorized access to a wireless network. WPA (Wi-Fi Protected Access) - a security protocol used for wireless networks. There is WPA, WPA2, WPA3. X.509 - a standard for public key certificates used for authentication in network communication. XML (Extensible Markup Language) - a markup language used for encoding documents in a format that is both human-readable and machine-readable. XSS (Cross-Site Scripting) - a type of attack in which an attacker injects malicious code into a web page viewed by other users. Usually this code is javascript code. There are 3 main versions of XSS: DOM Based, Stored and Reflected XSS. Back To Top