DOWNLOAD PDF PROTOCOL SEQUENCES AT EACH LAYER

Chapter 1 : Open System Interconnection Protocols - DocWiki

The Open System Interconnection (OSI) model defines a networking framework to implement protocols in seven layers. Use this handy guide to compare the different layers of the OSI model and understand how they interact with each other.

Data link layer 1. This layer includes applications or processes that use transport layer protocols to deliver the data to destination computers. At each layer there are certain protocol options to carry out the task designated to that particular layer. So, application layer also has various protocols that applications use to communicate with the second layer, the transport layer. Some of the popular application layer protocols are: Transport Layer This layer provides backbone to data flow between two hosts. This layer receives data from the application layer above it. There are many protocols that work at this layer but the two most commonly used protocols at transport layer are TCP and UDP. TCP is used where a reliable connection is required while UDP is used in case of unreliable connections. TCP divides the data coming from the application layer into proper sized chunks and then passes these chunks onto the network. So, the protocol used for this type of connection must provide the mechanism to achieve this desired characteristic. For example, while downloading a file, it is not desired to loose any information bytes as it may lead to corruption of downloaded content. UDP provides a comparatively simpler but unreliable service by sending packets from one host to another. UDP does not take any extra measures to ensure that the data sent is received by the target host or not. For example while streaming a video, loss of few bytes of information due to some reason is acceptable as this does not harm the user experience much. Network Layer This layer is also known as Internet layer. The main purpose of this layer is to organize or handle the movement of data on network. By movement of data, we generally mean routing of data over the network. The main protocol used at this layer is IP. Data Link Layer This layer is also known as network interface layer. This layer normally consists of device drivers in the OS and the network interface card attached to the system. Both the device drivers and the network interface card take care of the communication details with the media being used to transfer the data over the network. In most of the cases, this media is in the form of cables. Client requests for a service while the server processes the request for client. Now, since we have discussed the underlying layers which help that data flow from host to target over a network. Lets take a very simple example to make the concept more clear. Consider the data flow when you open a website. As seen in the above figure, the information flows downward through each layer on the host machine. At the first layer, since http protocol is being used, so an HTTP request is formed and sent to the transport layer. Here the protocol TCP assigns some more information like sequence number, source port number, destination port number etc to the data coming from upper layer so that the communication remains reliable i. At the next lower layer, IP adds its own information over the data coming from transport layer. This information would help in packet travelling over the network. Here again the communication done at the data link layer can be reliable or unreliable. This information travels on the physical media like Ethernet and reaches the target machine. Now, at the target machine which in our case is the machine at which the website is hosted the same series of interactions happen, but in reverse order. The packet is first received at the data link layer. At this layer the information that was stuffed by the data link layer protocol of the host machine is read and rest of the data is passed to the upper layer. Similarly at the Network layer, the information set by the Network layer protocol of host machine is read and rest of the information is passed on the next upper layer. Same happens at the transport layer and finally the HTTP request sent by the host application your browser is received by the target application Website server. One would wonder what happens when information particular to each layer is read by the corresponding protocols at target machine or why is it required? Well, lets understand this by an example of TCP protocol present at transport layer. At the host machine this protocol adds information like sequence number to each packet sent by this layer. Now, if the host TCP does not receive the acknowledgement within some specified time, it re sends the same packet. So this way TCP makes sure that no packet gets lost. So we see that protocol at every layer reads the information set by its counterpart to achieve the functionality of the layer it represents. A combination of IP and port on both client

and server is known as four tuple. This four tuple uniquely identifies a connection. In this section we will discuss how port numbers are chosen. You already know that some of the very common services like FTP, telnet etc run on well known port numbers. While FTP server runs on port 21, Telent server runs on port These standard port numbers are generally chosen from 1 to Client port numbers are known as ephemeral ports. By ephemeral we mean short lived. This is because a client may connect to server, do its work and then disconnect. Also, since clients need to know the port numbers of the servers to connect to them, so most standard servers run on standard port numbers. The ports reserved for clients generally range from to Port number higher than are reserved for those servers which are not standard or well known.

Chapter 2 : TCP/IP Protocol Architecture Model (System Administration Guide, Volume 3)

This article lists protocols, categorized by their nearest Open Systems Interconnection (OSI) model layers. This list is not exclusive to only the OSI protocol calendrierdelascience.com of these protocols are originally based on the Internet Protocol Suite (TCP/IP) and other models and they often do not fit neatly into OSI layers.

Coordinating all these problems are so complex and not easy to manage. The Open Systems Interconnection OSI model breaks down the problems involved in moving data from one computer to another computer. All the problems which are related to the communications are answered by specific protocols operating at different layers. Physical layers describe the electrical or optical signals used for communication. Physical layer of the Open Systems Interconnection OSI model is only concerned with the physical characteristics of electrical or optical signaling techniques which includes the voltage of the electrical current used to transport the signal, the media type Twisted Pair , Coaxial Cable , Optical Fiber etc , impedance characteristics, physical shape of the connector, Synchronization etc. The Physical Layer is limited to the processes needed to place the communication signals over the media, and to receive signals coming from that media. The lower boundary of the physical layer of the Open Systems Interconnection OSI model is the physical connector attached to the transmission media. The Data Link layer resides above the Physical layer and below the Network layer. Datalink layer is responsible for providing end-to-end validity of the data being transmitted. The MAC sub-layer maintains MAC addresses physical device addresses for communicating with other devices on the network. MAC addresses are burned into the network cards and constitute the low-level address used to determine the source and destination of network traffic. The Logical Link Control sublayer is responsible for synchronizing frames, error checking, and flow control. The Network layer of the OSI model is responsible for managing logical addressing information in the packets and the delivery of those packets to the correct destination. Routers, which are special computers used to build the network, direct the data packet generated by Network Layer using information stored in a table known as routing table. The routing table is a list of available destinations that are stored in memory on the routers. The network layer is responsible for working with logical addresses. The logical addresses are used to uniquely identify a computer on the network, but at the same time identify the network that system resides on. The logical address is used by network layer protocols to deliver the packets to the correct network. IP addresses are also known as Logical addresses or Layer 3 addresses. The Transport layer handles transport functions such as reliable or unreliable delivery of the data to the destination. On the sending computer, the transport layer is responsible for breaking the data into smaller packets, so that if any packet is lost during transmission, the missing packets will be sent again. Missing packets are determined by acknowledgments ACKs from the remote device, when the remote device receives the packets. At the receiving system, the transport layer will be responsible for opening all of the packets and reconstructing the original message. Another function of the transport layer is TCP segment sequencing. Sequencing is a connection-oriented service that takes TCP segments that are received out of order and place them in the right order. The transport layer also enables the option of specifying a "service address" for the services or application on the source and the destination computer to specify what application the request came from and what application the request is going to. Many network applications can run on a computer simultaneously and there should be some mechanism to identify which application should receive the incoming data. To make this work correctly, incoming data from different applications are multiplexed at the Transport layer and sent to the bottom layers. On the other side of the communication, the data received from the bottom layers are de-multiplexed at the Transport layer and delivered to the correct application. This is achieved by using " Port Numbers ". Port numbers identify the originating network application on the source computer and destination network application on the receiving computer. The session layer is responsible for establishing, managing, and terminating connections between applications at each end of the communication. In the connection establishment phase, the service and the rules who transmits and when, how much data can be sent at a time etc. The participating devices must agree on the rules. Once the rules are established, the data transfer phase begins. Connection termination occurs when the session is complete, and

communication ends gracefully. In practice, Session Layer is often combined with the Transport Layer. When the presentation layer receives data from the application layer, to be sent over the network, it makes sure that the data is in the proper format. If it is not, the presentation layer converts the data to the proper format. On the other side of communication, when the presentation layer receives network data from the session layer, it makes sure that the data is in the proper format and once again converts it if it is not. For example, if we select to compress the data from a network application that we are using, the Application Layer will pass that request to the Presentation Layer, but it will be the Presentation Layer that does the compression. Real traffic data will be often generated from the Application Layer. Click "Next" to Continue.

Chapter 3 : Windows Network Architecture and the OSI Model - Windows drivers | Microsoft Docs

OSI Seven Layers Model Explained with Examples Learn how Seven Layers OSI model works in computer network including functions and protocols involved in each layer of OSI Model (Application, Presentation, Session, Transportation, Network, Data link and physical layer).

Each component of this protocol suite is discussed briefly in this article. The wide variety of media-access protocols supported in the OSI protocol suite allows other protocol suites to exist easily alongside OSI on the same network media. Supported media-access protocols include IEEE In addition, the OSI suite implements two types of network services: ISO - This standard defines the internal organization of the network layer IONL , which divides the network layer into three distinct sublayers to support different subnetwork types. ISO - This standard defines network layer addressing and describes the connection-oriented and connectionless services provided by the OSI network layer. CLNS does not perform connection setup or termination because paths are determined independently for each packet that is transmitted through a network. In addition, CLNS provides best-effort delivery, which means that no guarantee exists that data will not be lost, corrupted, misordered, or duplicated. CLNS relies on transport layer protocols to perform error detection and correction. CONP is an OSI network layer protocol that carries upper-layer data and error indications over connection-oriented links. CONP is based on the X. It is a network layer service that acts as the interface between the transport layer and CONP, and it is described in the ISO standard. CMNS performs functions related to the explicit establishment of paths between communicating transport layer entities. These functions include connection setup, maintenance, and termination. This contrasts with CLNS. Network Layer Addressing OSI network layer addressing is implemented by using two types of hierarchical addresses: A network service access point NSAP is a conceptual point on the boundary between the network and the transport layers. The IDP field is divided into two parts: The DSP is subdivided into four parts by the authority responsible for its administration. The Address Administration fields allow for the further administration of addressing by adding a second authority identifier and by delegating address administration to subauthorities. The Area field identifies the specific area within a domain and is used for routing purposes. The Station field identifies a specific station within an area and also is used for routing purposes. The Selector field provides the specific n-selector within a station and, much like the other fields, is used for routing purposes. The reserved n-selector 00 identifies the address as a network entity title NET. If this is the case, the NSAP address for each transport entity usually differs only in the last byte called the n-selector. NETs are useful for addressing intermediate systems ISs , such as routers, that do not interface with the transport layer. Connectionless transport service is supported only by Transport Protocol Class 4. TP0 requires connection-oriented network service. Transport Protocol Class 1 TP1 performs segmentation and reassembly, and offers basic error recovery. TP1 requires connection-oriented network service. Transport Protocol Class 2 TP2 performs segmentation and reassembly, as well as multiplexing and demultiplexing of data streams over a single virtual circuit. TP2 requires connection-oriented network service. Transport Protocol Class 3 TP3 offers basic error recovery and performs segmentation and reassembly, in addition to multiplexing and demultiplexing of data streams over a single virtual circuit. TP3 also sequences PDUs and retransmits them or reinitiates the connection if an excessive number are unacknowledged. TP3 requires connection-oriented network service. Transport Protocol Class 4 TP4 offers basic error recovery, performs segmentation and reassembly, and supplies multiplexing and demultiplexing of data streams over a single virtual circuit. TP4 sequences PDUs and retransmits them or reinitiates the connection if an excessive number are unacknowledged. TP4 provides reliable transport service and functions with either connection-oriented or connectionless network service. The session protocol allows session-service users SS-users to communicate with the session service. An SS-user is an entity that requests the services of the session layer. Session service provides four basic services to SS-users. First, it establishes and terminates connections between SS-users and synchronizes the data exchange between them. Second, it performs various negotiations for the use of session layer tokens, which the SS-user must possess to begin communicating. Third, it inserts synchronization points in transmitted data

that allow the session to be recovered in the event of errors or interruptions. Finally, it enables SS-users to interrupt a session and resume it later at a specific point. A connectionless version of the session protocol is specified in the ISO standard. The presentation protocol enables presentation-service users PS-users to communicate with the presentation service. A PS-user is an entity that requests the services of the presentation layer. Such requests are made at presentation-service access points PSAPs. Presentation service negotiates transfer syntax and translates data to and from the transfer syntax for PS-users, which represent data using different syntaxes. The presentation service is used by two PS-users to agree upon the transfer syntax that will be used. When a transfer syntax is agreed upon, presentation-service entities must translate the data from the PS-user to the correct transfer syntax. A connectionless version of the presentation protocol is specified in the ISO standard. An application entity is the part of an application process that is relevant to the operation of the OSI protocol suite. An application entity is composed of the user element and the application service element ASE. The user element is the part of an application entity that uses ASEs to satisfy the communication needs of the application process. The ASE is the part of an application entity that provides services to user elements and, therefore, to application processes. Both of these might be present in a single application entity. In many cases, multiple CASEs are used by a single application entity. Association control service element ACSE - Creates associations between two application entities in preparation for application-to-application communication Remote operations service element ROSE - Implements a request-reply mechanism that permits various remote operations across an application association established by the ACSE Reliable transfer service element RTSE - Allows ASEs to reliably transfer messages while preserving the transparency of complex lower-layer facilities Commitment, concurrence, and recovery service elements CCRSE - Coordinates dialogues among multiple application entities. Specific-Application Service Elements Specific-application service elements SASEs are ASEs that provide services used only by a specific application process, such as file transfer, database access, and order entry, among others. OSI Protocols Application Processes An application process is the element of an application that provides the interface between the application itself and the OSI application layer. Some of the standard OSI application processes include the following: Common management-information protocol CMIP - Performs network-management functions, allowing the exchange of management information between ESs and management stations. Directory services DS - Serves as a distributed directory that is used for node identification and addressing in OSI internetworks. File transfer, access, and management FTAM - Provides file-transfer service and distributed file-access facilities. Message handling system MHS - Provides a transport mechanism for electronic messaging applications and other applications by using store-and-forward services. Virtual terminal protocol VTP - Provides terminal emulation that allows a computer system to appear to a remote ES as if it were a directly attached terminal. Q - Describe the OSI connectionless network protocol. Q - Describe the OSI connection-oriented network protocol. Q - How are requests to services at the session layer made within OSI protocols? Q - Name some of the media types that the OSI protocol suite supports. A - IEEE Q - Why was the OSI protocol suite created? A - The OSI specifications were conceived and implemented by two international standards organizations: Q - Describe the session layer protocols within the OSI protocol suite. A - The session layer implementation of the OSI protocol suite consists of a session protocol and a session service. The session protocol enables session-service users SS-users to communicate with the session service. Q - Describe the presentation layer protocols of the OSI protocol suite. A - The presentation layer implementation of the OSI protocol suite consists of a presentation protocol and a presentation service. Q - What are the two types of ASEs? A - ASEs fall into one of the two following classifications:

Chapter 4 : TCP/IP Protocol Fundamentals Explained with a Diagram

Layer 2, the Data Link Layer: This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The protocols are used by the Data Link Layer include: ARP, CSLIP, HDLC, IEEE, PPP, X, SLIP, ATM, SDLS and PLIP.

OSI protocols are a family of standards for information exchange. In the ISO model was introduced, which consisted of seven different layers. This model has been criticized because of its technicality and limited features. Each layer of the ISO model has its own protocols and functions. In some networks, protocols are still popular using only the data link and network layers of the OSI model. Techopedia explains OSI Protocols The OSI protocol stack works on a hierarchical form, from the hardware physical layer to the software application layer. There are a total of seven layers. Data and information are received by each layer from an upper layer. After the required processing, this layer then passes the information on to the next lower layer. A header is added to the forwarded message for the convenience of the next layer. Each header consists of information such as source and destination addresses, protocol used, sequence number and other flow-control related data. Layer 1, the Physical Layer: This layer deals with the hardware of networks such as cabling. Layer 2, the Data Link Layer: This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The protocols are used by the Data Link Layer include: Layer 3, the Network Layer: This is the most important layer of the OSI model, which performs real time processing and transfers data from nodes to nodes. Routers and switches are the devices used for this layer. The network layer assists the following protocols: Layer 4, the Transport Layer: The transport layer works on two determined communication modes: Connection oriented and connectionless. This layer transmits data from source to destination node. It uses the most important protocols of OSI protocol family, which are: Layer 5, the Session Layer: The session layer creates a session between the source and the destination nodes and terminates sessions on completion of the communication process. The protocols used are: Layer 6, the Presentation Layer: The functions of encryption and decryption are defined on this layer. It converts data formats into a format readable by the application layer. The following are the presentation layer protocols: Layer 7, the Application Layer: This layer works at the user end to interact with user applications. QoS quality of service , file transfer and email are the major popular services of the application layer. This layer uses following protocols:

Chapter 5 : Seven Layers of OSI Model and functions of seven layers of OSI model

At the host machine this protocol adds information like sequence number to each packet sent by this layer. At the target machine, when packet reaches at this layer, the TCP at this layer makes note of the sequence number of the packet and sends an acknowledgement (which is received seq number + 1).

Only use this option if the end of the options list does not coincide with the end of the header. The Class 1 option is used to align an option with a word boundary. Other than that this option does not contain any useful information. Its main purpose is for aligning and formatting. The Class 2 option indicates the maximum segment size that it will receive. It can only be included in the initial request and in segments where the SYN item bit is set. If this option is not used, there is no size limit. The IP header appears as follows: Each field contains information about the IP packet that it carries. The descriptions in the following sections should be helpful. Version Number The version number indicates the version of IP that is in use for this packet. IP version 4 Ipv4 is currently in widespread use. Header Length The header length indicates the overall length of the header. The receiving machine then knows when to stop reading the header and start reading data. Type of Service Mostly unused, the Type of Service field indicates the importance of the packet in a numerical value. Higher numbers result in prioritized handling. Total Length Total length shows the total length of the packet in bytes. The total packet length cannot exceed 65, bytes or it will be deemed corrupt by the receiver. Identification If there is more than one packet an invariable inevitability , the identification field has an identifier that identifies its place in line, as it were. Fragmented packets retain their original ID number. Flags The first flag, if set, is ignored. If the MF More Fragments bit is turned on 1 , there are packet fragments to come, the last of which is set to off 0. Offset If the Flag field returns a 1 on , the Offset field contains the location of the missing piece s indicated by a numerical offset based on the total length of the packet. If a packet is discarded or lost in transit, an indicator is sent back to the sending computer that the loss occurred. The sending machine then has the option of resending that packet. Protocol The protocol field holds a numerical value indicating the handling protocol in use for this packet. Checksum The checksum value acts as a validation checksum for the header. Source Address The source address field indicates the address of the sending machine. Destination Address The destination address field indicates the address of the destination machine. Options and Padding The Options field is optional. If used, it contains codes that indicate the use of security, strict or loose source routing, routing records, and timestamping. If no options are used, the field is called padded and contains a 1. Padding is used to force a byte value that is rounded.

Chapter 6 : Introducing the TCP/IP Protocol Suite - System Administration Guide: IP Services

One or more protocols is associated with each layer. The layers represent data transfer operations that are common to all types of data transfers among cooperating networks. The OSI model lists the protocol layers from the top (layer 7) to the bottom (layer 1).

Each host involved in a communication transaction runs its own implementation of the protocol stack. Physical Network Layer The physical network layer specifies the characteristics of the hardware to be used for the network. For example, it specifies the physical characteristics of the communications media. It also provides error control and "framing. Internet Layer This layer, also known as the network layer, accepts and delivers packets for the network. IP is responsible for: Packet formatting - IP assembles packets into units known as IP datagrams. Datagrams are fully described in "Internet Layer". Fragmentation - If a packet is too large for transmission over the network media, IP on the sending host breaks the packet into smaller fragments. IP on the receiving host then reconstructs the fragments into the original packet. Previous releases of the Solaris operating environment implemented version 4 of the Internet Protocol, which is written IPv4. However, because of the rapid growth of the Internet, it was necessary to create a new Internet Protocol with improved capabilities, such as increased address space. This new version, known as version 6, is written IPv6. The Solaris operating environment supports both versions, which are described in this book. To avoid confusion when addressing the Internet Protocol, the following convention is used: When the term IPv4 is used in a description, the description applies only to IPv4. When the term IPv6 is used in a description, the description applies only to IPv6. ARP assists IP in directing datagrams to the appropriate receiving host by mapping Ethernet addresses 48 bits long to known IP addresses 32 bits long. This type of communication is known as "end-to-end. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discreet packets. This transmission consists of a starting point, which opens the connection, the entire transmission in byte order, and an ending point, which closes the connection. TCP attaches a header onto the transmitted data. This header contains a large number of parameters that help processes on the sending machine connect to peer processes on the receiving machine. TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a "reliable, connection-oriented" protocol. It does not provide any means of verifying that connection was ever achieved between receiving and sending hosts. Because UDP eliminates the processes of establishing and verifying connections, applications that send small amounts of data use it rather than TCP. Application Layer The application layer defines standard Internet services and network applications that anyone can use. These services work with the transport layer to send and receive data. There are many applications layer protocols, some of which you probably already use. Some of the protocols include:

Chapter 7 : Transport Layer ISO OSI TCP ports UDP datagram

We talk about these protocols as being in the application layer, but in reality, most of these protocols actually extend down through the session layer. In reality, most services or protocols can span multiple layers, but we talk about these as being application layer protocols because that is the highest layer that these protocols function at.

Application layer is present on the top of the Transport layer. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data. Internet layer pack data into data packets known as IP datagrams , which contain source and destination address logical address or IP address information that is used to forward the datagrams between hosts and across networks. The Internet layer is also responsible for routing of IP datagrams. Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire. The most popular LAN architecture among those listed above is Ethernet. An Access Method determines how a host will place data on the medium. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision , each host will wait for a small interval of time and again the data will be retransmitted. Click "Next" to continue.

Chapter 8 : List of network protocols (OSI model) - Wikipedia

The third layer of the seven layers of Open Systems Interconnection (OSI) network model is the Network layer. The Network layer of the OSI model is responsible for managing logical addressing information in the packets and the delivery of those packets to the correct destination.

SYN - Synchronize sequence numbers FIN - No more data from sender These fields are referred to as flags, because the value of one of these fields is only 1 bit and, therefore, has only two values: When a bit value is set to 1, it indicates what control information is contained in the segment. Using a four-step process, flags are exchanged to terminate a TCP connection. Step 1 A TCP client begins the three-way handshake by sending a segment with the SYN Synchronize Sequence Number control flag set, indicating an initial value in the sequence number field in the header. This initial value for the sequence number, known as the Initial Sequence Number ISN , is randomly chosen and is used to begin tracking the flow of data from the client to the server for this session. The ISN in the header of each segment is increased by one for each byte of data sent from the client to the server as the data conversation continues. As shown in the figure, output from a protocol analyzer shows the SYN control flag and the relative sequence number. The SYN control flag is set and the relative sequence number is at 0. Although the protocol analyzer in the graphic indicates the relative values for the sequence and acknowledgement numbers, the true values are 32 bit binary numbers. We can determine the actual numbers sent in the segment headers by examining the Packet Bytes pane. Here you can see the four bytes represented in hexadecimal. Step 2 The TCP server needs to acknowledge the receipt of the SYN segment from the client to establish the session from the client to the server. To do so, the server sends a segment back to the client with the ACK flag set indicating that the Acknowledgment number is significant. With this flag set in the segment, the client recognizes this as an acknowledgement that the server received the SYN from the TCP client. The value of the acknowledgment number field is equal to the client initial sequence number plus 1. This establishes a session from the client to the server. The ACK flag will remain set for the balance of the session. Recall that the conversation between the client and the server is actually two one-way sessions: In this second step of the three-way handshake, the server must initiate the response from the server to the client. To start this session, the server uses the SYN flag in the same way that the client did. It sets the SYN control flag in the header to establish a session from the server to the client. The SYN flag indicates that the initial value of the sequence number field is in the header. This value will be used to track the flow of data in this session from the server back to the client. As shown in the figure, the protocol analyzer output shows that the ACK and SYN control flags are set and the relative sequence and acknowledgement numbers are shown. There is no user data in this segment. The value in the acknowledgment number field contains one more than the initial sequence number received from the server. Once both sessions are established between client and server, all additional segments exchanged in this communication will have the ACK flag set. As shown in the figure, the protocol analyzer output shows the ACK control flag set and the relative sequence and acknowledgement numbers are shown. Security can be added to the data network by: Denying the establishment of TCP sessions Only allowing sessions to be established for specific services Only allowing traffic as a part of already established sessions This security can be implemented for all TCP sessions or only for selected sessions. Therefore, to terminate a single conversation supported by TCP, four exchanges are needed to end both sessions. In this explanation, the terms client and server are used in this description as a reference for simplicity, but the termination process can be initiated by any two hosts that complete the session: When the client has no more data to send in the stream, it sends a segment with the FIN flag set. The server sends a FIN to the client, to terminate the server to client session. When the client end of the session has no more data to transfer, it sets the FIN flag in the header of a segment. Next, the server end of the connection will send a normal segment containing data with the ACK flag set using the acknowledgment number, confirming that all the bytes of data have been received. When all segments have been acknowledged, the session is closed. The session in the other direction is closed using the same process. The receiver indicates that there is no more data to send by setting the FIN flag in the header of a segment sent to the source. A return

acknowledgement confirms that all bytes of data have been received and that session is, in turn, closed. It is also possible to terminate the connection by a three-way handshake. When the client has no more data to send, it sends a FIN to the server. If the server also has no more data to send, it can reply with both the FIN and ACK flags set, combining two steps into one. The client replies with an ACK. For the original message to be understood by the recipient, the data in these segments is reassembled into the original order. Sequence numbers are assigned in the header of each packet to achieve this goal. During session setup, an initial sequence number ISN is set. This initial sequence number represents the starting value for the bytes for this session that will be transmitted to the receiving application. As data is transmitted during the session, the sequence number is incremented by the number of bytes that have been transmitted. This tracking of data byte enables each segment to be uniquely identified and acknowledged. Missing segments can be identified. Segment sequence numbers enable reliability by indicating how to reassemble and reorder received segments, as shown in the figure. The receiving TCP process places the data from a segment into a receiving buffer. Segments are placed in the proper sequence number order and passed to the Application layer when reassembled. Any segments that arrive with noncontiguous sequence numbers are held for later processing. Then, when the segments with the missing bytes arrive, these segments are processed. The TCP services on the destination host acknowledge the data that it has received to the source application. The segment header sequence number and acknowledgement number are used together to confirm receipt of the bytes of data contained in the segments. The sequence number is the relative number of bytes that have been transmitted in this session plus 1 which is the number of the first data byte in the current segment. TCP uses the acknowledgement number in segments sent back to the source to indicate the next byte in this session that the receiver expects to receive. This is called expectational acknowledgement. The source is informed that the destination has received all bytes in this data stream up to, but not including, the byte indicated by the acknowledgement number. The sending host is expected to send a segment that uses a sequence number that is equal to the acknowledgement number. Remember, each connection is actually two one-way sessions. Sequence numbers and acknowledgement numbers are being exchanged in both directions. In the example in the figure, the host on the left is sending data to the host on the right. It sends a segment containing 10 bytes of data for this session and a sequence number equal to 1 in the header. The receiving host on the right receives the segment at Layer 4 and determines that the sequence number is 1 and that it has 10 bytes of data. The host then sends a segment back to the host on the left to acknowledge the receipt of this data. In this segment, the host sets the acknowledgement number to 11 to indicate that the next byte of data it expects to receive in this session is byte number When the sending host on the left receives this acknowledgement, it can now send the next segment containing data for this session starting with byte number Looking at this example, if the sending host had to wait for acknowledgement of the receipt of each 10 bytes, the network would have a lot of overhead. To reduce the overhead of these acknowledgements, multiple segments of data can be sent before and acknowledged with a single TCP message in the opposite direction. This acknowledgement contains an acknowledgement number based on the total number of bytes received in the session. For example, starting with a sequence number of , if 10 segments of bytes each were received, an acknowledgement number of would be returned to the source. The amount of data that a source can transmit before an acknowledgement must be received is called the window size. Window Size is a field in the TCP header that enables the management of lost data and flow control. Therefore, TCP provides methods of managing these segment losses. Among these is a mechanism to retransmit segments with unacknowledged data. A destination host service using TCP usually only acknowledges data for contiguous sequence bytes. If one or more segments are missing, only the data in the segments that complete the stream are acknowledged. For example, if segments with sequence numbers to and to were received, the acknowledgement number would be This is because there are segments with the sequence numbers to that have not been received. When TCP at the source host has not received an acknowledgement after a predetermined amount of time, it will go back to the last acknowledgement number that it received and retransmit data from that point forward. For a typical TCP implementation, a host may transmit a segment, put a copy of the segment in a retransmission queue, and start a timer. When the data acknowledgment is received, the segment is deleted from the queue. If the

acknowledgment is not received before the timer expires, the segment is retransmitted. The animation demonstrates the retransmission of lost segments. Hosts today may also employ an optional feature called Selective Acknowledgements. If both hosts support Selective Acknowledgements, it is possible for the destination to acknowledge bytes in discontinuous segments and the host would only need to retransmit the missing data. Flow control assists the reliability of TCP transmission by adjusting the effective rate of data flow between the two services in the session. When the source is informed that the specified amount of data in the segments is received, it can continue sending more data for this session. This Window Size field in the TCP header specifies the amount of data that can be transmitted before an acknowledgement must be received. The initial window size is determined during the session startup via the three-way handshake. TCP feedback mechanism adjusts the effective rate of data transmission to the maximum flow that the network and destination device can support without loss. TCP attempts to manage the rate of transmission so that all data will be received and retransmissions will be minimized. See the figure for a simplified representation of window size and acknowledgements. In this example, the initial window size for a TCP session represented is set to bytes. When the sender has transmitted bytes, it waits for an acknowledgement of these bytes before transmitting more segments in this session.

Chapter 9 : The 7 Layers of the OSI Model - Webopedia Study Guide

ICMP (Internet Control Message Protocol) is a _____ layer core protocol that reports on the success or failure of data delivery. Network Layer IP is an unreliable, connectionless protocol.

Layer 1 - Physical Did You Know? Most of the functionality in the OSI model exists in all communications systems, although two or three OSI layers may be incorporated into one. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail , and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network , providing freedom from compatibility problems. It is sometimes called the syntax layer. Session Layer 5 This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination. Transport Layer 4 OSI Model, Layer 4, provides transparent transfer of data between end systems, or hosts , and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer. Network Layer 3 Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits , for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing , internetworking , error handling, congestion control and packet sequencing. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization , flow control and error checking. Physical Layer 1 OSI Model, Layer 1 conveys the bit stream - electrical impulse, light or radio signal â€" through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. It was published in as standard ISO Tweet This Study Guide! Webopedia study guides offer quick facts to help students prepare for computer science courses. Did you find this guide useful? Click to share it with friends and classmates on Twitter.