DOWNLOAD PDF DIFFERENCE BETWEEN OSI TCP IP REFERENCE MODEL

Chapter 1 : Difference between TCP/IP and OSI Model â€“ Difference Between

OSI(Open System Interconnection) TCP/IP(Transmission Control Protocol / Internet Protocol) 1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.

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.

DOWNLOAD PDF DIFFERENCE BETWEEN OSI TCP IP REFERENCE MODEL

Chapter 2 : Difference between TCP/IP Model and OSI Model Instrumentation Tools

The Internet Protocol layer is comparable to layer 3 in the OSI model. The host-to-host layer is equivalent to OSI layer 4. These are the TCP and UDP (user datagram protocol) functions.

Review Questions Chapter Description The equipment that you select for your broadband wireless wide-area network WAN plays a major role in the reliability, scalability, and profitability of your network. This sample chapter helps you evaluate and select your wireless network equipment. When you understand a little about the service layers and the protocols that these architectures use, you will be in a good position to understand the similarities and the differences between different brands of wireless equipment. The seven-layer ISO OSI reference model was first proposed around to allow connectivity or interworking between different computer systems. Prior to the OSI reference model, computer systems made by one manufacturer could not easily communicate with computer systems made by other manufacturers. The intent of the OSI reference model was to allow computer systems to successfully communicate with each other even though different vendors manufactured them. This new networking effort was based on two primary protocols: IP performed network layer functions that were equivalent to the network layer Layer 3 in the OSI model. When application layer Layer 7 protocols Telnet, FTP, SMTP, and so on and physical Layer 1 and data link layer Layer 2 protocols were added, the result was an architecture that effectively contained five layers. The major similarities and differences are as follows: Both models have a lower layer that connects the upper layers to the actual physical network. In the OSI reference model, the lower layer Layer 1 is called the physical layer. The wireless features and functionality modulation type, data rate, and so on take place at the physical layer. Access to and sharing of the wireless medium takes place at the data link layer. Routing takes place at the network layer. Peer Protocols Peer protocols run across the Internet but provide communication only between same-layer processes. One example of this same-layer communication process is a Hypertext Transfer Protocol HTTP web browser running on the application layer of one network. The HTTP browser retrieves information from its peer web server running on the application layer of another network. Although the HTTP communication is application-layer-to-application layer peer-to-peer , both networks communicate downward through their lower network layers. Services Information is passed from the top application layer of one network down through the lower layers. Each layer provides a set of services for the layer just above it and utilizes the services provided by the layer just below it. The set of services between two layers is referred to as the interface between the two layers. For example, Layer 6 provides services for Layer 7; Layer 5 provides services for Layer 6; and so on. In this way, Layer 7 the application layer can communicate all the way down to Layer 1 the physical layer. The following list illustrates how services and protocols operate. When your web browser uses HTTP over a wireless network, the information flow is as follows: The HTTP information request originates at the application layer on the originating network. The HTTP request travels downward from the application layer using the services provided by all the intermediate layers to the physical layer on the originating network. The physical layer uses the appropriate wireless protocol for example, the appropriate direct sequence spread spectrum modulation or DSSS to communicate the request over the air wirelessly to the physical layer on the other network. The physical layer on the other network uses the DSSS protocol to receive the request from the originating network. The physical layer then passes the information up through its interface to the data link layer. Using higher and higher layer services, the request passes upward until it eventually reaches the application layer. There, the HTTP protocol processes the request and replies with a response. Using services of lower and lower layers, the response travels downward to the physical layer. Using the Layer 1 DSSS protocol, the response is transmitted over the air back to the physical layer of the originating network. Using services, the originating network passes the response upward to the application layer where the HTTP protocol receives the response to its original request. Basic Packet Structure and Frame Types Packet switching store-and-forward techniques underlie the operation of layered architectures. Packet switching uses

an underlying data structure, called a packet. A packet is like a hamburger on a bun. Although the exact packet structure varies from layer to layer and protocol to protocol, most packets contain a data payload section. The data payload is the hamburger in the middle of the bun. Other fields encapsulate surround the data payload and make up the bun. The bun typically provides the following: Source and destination address information Packet numbering information Error detection and correction information Figure shows this general packet structure. Figure General Packet Structure Packets prepared by Layer 2 the data link layer are called frames. Not all frames contain payload data. Wireless APs and wireless stations exchange three types of frames, each with the following functions: Data frames carry user payload data the hamburger between different wireless network nodes. Management frames carry association and authentication requests and responses in addition to beacon information. Application Layer Functions and Protocols The application layer is where the end user programs run. Wireless equipment that you evaluate will likely have network management software that operates at the application layer level. The transport layer encapsulates data from the application layer and the session layer, if used and passes it down to the network layer. Wireless equipment that you evaluate does not usually have features that operate at the transport layer level. The network layer encapsulates data the hamburger from the transport layer between IP source, IP destination, and IP routing information. Packet routing typically goes from intermediate network to intermediate network before the packets finally arrive at their destination network. The data link layer normally performs a wide variety of functions, including segmenting the bit stream into frames, error handling, flow control, and access control. The LLC Sublayer might provide different service options, depending on the network software. The MAC sublayer interfaces to the physical wireless layer and provides the following functions: If an acknowledgment is not received, the MAC sublayer retransmits the frame. Each wireless station listens before transmitting. If a station hears that the frequency is busy, it backs off waits a random amount of time and tries again. When the frequency is clear, the station proceeds to transmit. Finally, in networks that have heavy traffic and many end users, a point coordination function PCF can be used. The PCF polls each wireless station and then tells each end user when it can transmit. NOTE You might have heard of wireless networks with a hidden node problem. This problem can occur in a network that uses DCF. In most wireless networks, certain wireless stations cannot hear all the other wireless stations. Under heavy traffic loads, several stations might try to transmit at the same time. When stations transmit at the same time, collisions occur and network throughput drops drastically. The solution to hidden-node problems is to use wireless equipment that can support PCF. The most frequently used encryption method is wired equivalent privacy WEP. Physical Layer Functions and Protocols The physical layer transports encapsulated data from the data link layer and transmits it wirelessly to the distant network. There are several physical layer wireless standards. There are also many proprietary physical layer wireless protocols. In addition to your wireless feature evaluation, you will evaluate physical layer wired-interface features such as Ethernet and serial port features.

DOWNLOAD PDF DIFFERENCE BETWEEN OSI TCP IP REFERENCE MODEL

Chapter 3 : Internet protocol suite - Wikipedia

Main Difference. The OSI and TCP/IP stands for Open Systems Interconnection and Transmission Control Protocol/Internet Protocol respectively. The principal between OSI and TCP/IP is that OSI mannequin is a reference mannequin whereas TCP/IP is an implementation of OSI mannequin.

In , Robert E. Kahn joined the DARPA Information Processing Technology Office , where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. By the summer of , Kahn and Cerf had worked out a fundamental reformulation, in which the differences between local network protocols were hidden by using a common internetwork protocol , and, instead of the network being responsible for reliability, as in the ARPANET, this function was delegated to the hosts. The protocol was implemented as the Transmission Control Program, first published in A monolithic design would be inflexible and lead to scalability issues. The design of the network included the recognition that it should provide only the functions of efficiently transmitting and routing traffic between end nodes and that all other intelligence should be located at the edge of the network, in the end nodes. This design is known as the end-to-end principle. A computer called a router is provided with an interface to each network. It forwards network packets back and forth between them. Four versions were developed: The last protocol is still in use today. The conference was founded by Dan Lynch, an early Internet activist. Key architectural principles[edit] Two Internet hosts connected via two routers and the corresponding layers used at each hop. The application on each host executes read and write operations as if the processes were directly connected to each other by some kind of data pipe. Every other detail of the communication is hidden from each process. The underlying mechanisms that transmit data between the host computers are located in the lower protocol layers. Encapsulation of application data descending through the layers described in RFC The end-to-end principle has evolved over time. Its original expression put the maintenance of state and overall intelligence at the edges, and assumed the Internet that connected the edges retained no state and concentrated on speed and simplicity. Real-world needs for firewalls, network address translators, web content caches and the like have forced changes in this principle. That is, it must be careful to send well-formed datagrams, but must accept any datagram that it can interpret e. Encapsulation is usually aligned with the division of the protocol suite into layers of general functionality. In general, an application the highest level of the model uses a set of protocols to send its data down the layers, being further encapsulated at each level. It loosely defines a four-layer model, with the layers having names, not numbers, as follows: Application layer The application layer is the scope within which applications create user data and communicate this data to other applications on another or the same host. The applications, or processes, make use of the services provided by the underlying, lower layers, especially the Transport Layer which provides reliable or unreliable pipes to other processes. The communications partners are characterized by the application architecture, such as the client-server model and peer-to-peer networking. Processes are addressed via ports which essentially represent services. Transport layer The transport layer performs host-to-host communications on either the same or different hosts and on either the local network or remote networks separated by routers. UDP is the basic transport layer protocol, providing an unreliable datagram service. The Transmission Control Protocol provides flow-control, connection establishment, and reliable transmission of data. Internet layer The internet layer exchanges datagrams across network boundaries. It provides a uniform networking interface that hides the actual topology layout of the underlying network connections. It is therefore also referred to as the layer that establishes internetworking. Indeed, it defines and establishes the Internet. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination. Link layer The link layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer includes the protocols used to describe the local network topology and

the interfaces needed to effect transmission of Internet layer datagrams to next-neighbor hosts. The layers of the protocol suite near the top are logically closer to the user application, while those near the bottom are logically closer to the physical transmission of the data. Viewing layers as providing or consuming a service is a method of abstraction to isolate upper layer protocols from the details of transmitting bits over, for example, Ethernet and collision detection , while the lower layers avoid having to know the details of each and every application and its protocol. Even when the layers are examined, the assorted architectural documentsâ€”there is no single architectural model such as ISO , the Open Systems Interconnection OSI model â€”have fewer and less rigidly defined layers than the OSI model, and thus provide an easier fit for real-world protocols. One frequently referenced document, RFC , does not contain a stack of layers. It only refers to the existence of the internetworking layer and generally to upper layers; this document was intended as a snapshot of the architecture: This abstraction also allows upper layers to provide services that the lower layers do not provide. This means that all transport layer implementations must choose whether or how to provide reliability. UDP provides data integrity via a checksum but does not guarantee delivery; TCP provides both data integrity and delivery guarantee by retransmitting until the receiver acknowledges the reception of the packet. This model lacks the formalism of the OSI model and associated documents, but the IETF does not use a formal model and does not consider this a limitation, as illustrated in the comment by David D. Clark , "We reject: For multi-access links with their own addressing systems e. Ethernet an address mapping protocol is needed. Such protocols can be considered to be below IP but above the existing link system. Again, there was no intention, on the part of the designers of these protocols, to comply with OSI architecture. The link is treated as a black box. The IETF explicitly does not intend to discuss transmission systems, which is a less academic [26] [citation needed] but practical alternative to the OSI model. Link layer[edit] The link layer has the networking scope of the local network connection to which a host is attached. The link layer is used to move packets between the Internet layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card , as well as on firmware or specialized chipsets. These perform data link functions such as adding a packet header to prepare it for transmission, then actually transmit the frame over a physical medium. All other aspects below that level, however, are implicitly assumed to exist in the link layer, but are not explicitly defined. This is also the layer where packets may be selected to be sent over a virtual private network or other networking tunnel. In this scenario, the link layer data may be considered application data which traverses another instantiation of the IP stack for transmission or reception over another IP connection. Such a connection, or virtual link, may be established with a transport protocol or even an application scope protocol that serves as a tunnel in the link layer of the protocol stack. Internet layer[edit] The internet layer has the responsibility of sending packets across potentially multiple networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. The Internet Protocol performs two basic functions: Host addressing and identification: This is accomplished with a hierarchical IP addressing system. This is the basic task of sending packets of data datagrams from source to destination by forwarding them to the next network router closer to the final destination. The internet layer is not only agnostic of data structures at the transport layer, but it also does not distinguish between operation of the various transport layer protocols. IP carries data for a variety of different upper layer protocols. These protocols are each identified by a unique protocol number: The internet layer provides an unreliable datagram transmission facility between hosts located on potentially different IP networks by forwarding the transport layer datagrams to an appropriate next-hop router for further relaying to its destination. With this functionality, the internet layer makes possible internetworking, the interworking of different IP networks, and it essentially establishes the Internet. It uses a bit IP address and is therefore capable of identifying approximately four billion hosts. This limitation was eliminated in by the standardization of Internet Protocol version 6 IPv6 which uses bit addresses. IPv6 production implementations emerged in approximately Transport layer[edit] The transport layer establishes basic data channels that applications use for task-specific

data exchange. The layer establishes host-to-host connectivity, meaning it provides end-to-end message transfer services that are independent of the structure of user data and the logistics of exchanging information for any particular specific purpose and independent of the underlying network. The protocols in this layer may provide error control , segmentation , flow control , congestion control , and application addressing port numbers. End-to-end message transmission or connecting applications at the transport layer can be categorized as either connection-oriented , implemented in TCP, or connectionless , implemented in UDP. For the purpose of providing process-specific transmission channels for applications, the layer establishes the concept of the network port. This is a numbered logical construct allocated specifically for each of the communication channels an application needs. For many types of services, these port numbers have been standardized so that client computers may address specific services of a server computer without the involvement of service announcements or directory services. Because IP provides only a best effort delivery , some transport layer protocols offer reliability. For example, the TCP is a connection-oriented protocol that addresses numerous reliability issues in providing a reliable byte stream: It is message-stream-orientedâ€”not byte-stream-oriented like TCPâ€”and provides multiple streams multiplexed over a single connection. It also provides multi-homing support, in which a connection end can be represented by multiple IP addresses representing multiple physical interfaces , such that if one fails, the connection is not interrupted. It was developed initially for telephony applications to transport SS7 over IP , but can also be used for other applications. The User Datagram Protocol is a connectionless datagram protocol. Like IP, it is a best effort, "unreliable" protocol. Reliability is addressed through error detection using a weak checksum algorithm. Real-time Transport Protocol RTP is a datagram protocol that is designed for real-time data such as streaming audio and video. By convention certain well known ports are associated with specific applications. Application layer[edit] The application layer includes the protocols used by most applications for providing user services or exchanging application data over the network connections established by the lower level protocols. This may include some basic network support services such as protocols for routing and host configuration. Such functions are the realm of libraries and application programming interfaces. Application layer protocols generally treat the transport layer and lower protocols as black boxes which provide a stable network connection across which to communicate, although the applications are usually aware of key qualities of the transport layer connection such as the end point IP addresses and port numbers. Application layer protocols are often associated with particular client-server applications, and common services have well-known port numbers reserved by the Internet Assigned Numbers Authority IANA.

DOWNLOAD PDF DIFFERENCE BETWEEN OSI TCP IP REFERENCE MODEL

Chapter 4 : Difference between OSI and TCP IP Model | Difference Between

TCP/IP is a standard protocol used for every network including the Internet, whereas, OSI is not a protocol but a reference model used for understanding and designing the system architecture. TCP/IP is a four layered model, whereas, OSI has seven layers.

OSI, on the other hand, is a communication gateway between the network and the end users. This protocol can borrow its roots from the Department of Defense, which developed it to allow different devices to be connected to the internet. Just what differences are there among the two? First off is the model of implementation on which each is developed. OSI, on the other hand, was developed as a reference model that could be employed online. The model around which OSI was developed upon is a theoretical model and not the internet. There are four levels or layers upon which TCP is developed. The OSI gateway, on the other hand, is developed upon a seven-layer model. The OSI model is, in most cases, referred to as a reference tool, being the older of the two models. OSI is also known for its strict protocol and boundaries. It allows for a loosening of the rules, provided the general guidelines are met. OSI, on the other side, seems to take a different approach to the presentation, having different session and presentation layers altogether. It is also imperative to note the design followed when protocols were being designed. In OSI, the model development came first and then the protocol development came in second. OSI, on the other hand, seems to do quite well, supporting both connectionless and connection-oriented communication within the network layer. Last but not least is the protocol dependency of the two. OSI follows a vertical approach. OSI uses different session and presentation layers. OSI developed model then protocol. In the network layer, OSI supports both connectionless and connection-oriented communication.

DOWNLOAD PDF DIFFERENCE BETWEEN OSI TCP IP REFERENCE MODEL

Chapter 5 : OSI & TCP/IP models

OSI vs TCP IP Model. TCP/IP is a communication protocol that allows for connections of hosts to the internet. OSI, on the other hand, is a communication gateway between the network and the end users.

It was designed to be a reference model for describing the functions of a communication system. The OSI model provides a framework for creating and implementing networking standards and devices and describes how network applications on different computers can communicate through the network media. It has seven layers, with each layer describing a different function of data traveling through a network. Here is the graphical representation of these layers: The layers are usually numbered from the last one, meaning that the Physical layer is considered to be the first layer. It is useful to remember these layers, since there will certainly be a couple of questions on the CCNA exam regarding them. So, what is the purpose of these layers? They are most commonly used by vendors. They enable them to implement some functionality into a networking device, which then enables easier interoperability with devices from other vendors. Here is a brief description of each of the layers of the OSI model. Physical â€" defines how to move bits from one device to another. It details how cables, connectors and network interface cards are supposed to work and how to send and receive bits. Data Link â€" encapsulates a packet in a frame. A frame contains a header and a trailer that enable devices to communicate. A header, most commonly, contains a source and a destination MAC address. A trailer contains the Frame Check Sequence field, which is used to detect transmission errors. The data link layer has two sublayers: Logical Link Control â€" used for flow control and error detection. Media Access Control â€" used for hardware addressing and for controlling the access method. Network â€" defines device addressing, routing, and path determination. Device logical addressing is used to identify a host on a network e. Transport â€" segments great chunks of data received from the upper layer protocols. Establishes and terminates connections between two computers. Used for flow control and data recovery. Session â€" defines how to establish and terminate a session between the two systems. Presentation â€" defines data formats. Compression and encryption are defined at this layer. Application â€" this layer is the closest to the user. It enables network applications to communicate with other network applications. The following table shows which protocols reside on which layer of the OSI model: Like the OSI model, it describes general guidelines for designing and implementing computer protocols. It consists of four layers: Network Access, Internet, Transport, and Application: OSI model prescribes the steps needed to transfer data over a network and it is very specific in it, defining which protocol is used at each layer and how.

Chapter 6 : TCP/IP Model Vs. OSI Model

The TCP/IP model and OSI model are both conceptual models used for description of all network communications, while TCP/IP itself is also an important protocol used in all Internet operations. Generally, when we talk about layer 2, layer 3 or layer 7 in which a network device works, we are referring to the OSI model.

This model divides the entire networking functions into layers, where each layer performs a specific function. This model gives a brief idea about the process of data formatting, transmission, and finally the reception. Each of these functions take place in the layers, as described by the model. Let us have a look at the four layers: It is also known as Network Access layer and Network Interface layer. It explains how the data is transmitted from the host, through the network. The physical connectors like the coaxial cables, twisted pair wires, the optical fiber, interface cards, etc. Internet Layer This layer is also known as the Network Layer. The main function of this layer is to route the data to its destination. The data that is received by the link layer is made into data packets IP datagrams. The data packets contain the source and the destination IP address or logical address. These packets are sent on any network and are delivered independently. This indicates that the data is not received in the same order as it was sent. Transport Layer This layer is responsible for providing datagram services to the Application layer. This layer allows the host and the destination devices to communicate with each other for exchanging messages, irrespective of the underlying network type. Error control, congestion control, flow control, etc. TCP gives a reliable, end-to-end, connection-oriented data transfer, while UDP provides unreliable, connectionless data transfer between two computers. Application Layer It provides the user interface for communication. This is the layer where email, web browsers or FTP run. It is a theoretical model which explains the working of the networks. Physical Layer As the name suggests, this is the layer where the physical connection between two computers takes place. Data Link Layer The main function of this layer is to convert the data packets received from the upper layer into frames, and route the same to the physical layer. Error detection and correction is done at this layer, thus making it a reliable layer in the model. It establishes a logical link between the nodes and transmit frames sequentially. Network Layer The main function of this layer is to translate the network address into physical MAC address. The data has to be routed to its intended destination on the network. This layer is also responsible to determine the efficient route for transmitting the data to its destination. While doing so, it has to manage problems like network congestion, switching problems, etc. Transport Layer This layer provides end-to-end delivery of data between two nodes. It divides data into different packets before transmitting it. On receipt of these packets, the data is reassembled and forwarded to the next layer. If the data is lost in transmission or has errors, then this layer recovers the lost data and transmits the same. Session Layer This layer is responsible to establish and terminate connections between two communicating machines. This connection is known as a session, hence the name. It establishes full-duplex, half-duplex and simplex connection for communication. The sessions are also used to keep a track of the connections to the web server. Presentation Layer The data conversion takes place at this layer. The data that it receives from the application layer is converted into a suitable format that is recognized by the computer. For example, the conversion of a file from. Application Layer This layer provides a user interface by interacting with the running application. E-mail, FTP, web browsers, etc. It is absolutely vital to learn the above differences, if anyone wants to be an expert in the field of communication.

DOWNLOAD PDF DIFFERENCE BETWEEN OSI TCP IP REFERENCE MODEL

Chapter 7 : OSI and TCP/IP Reference Models > Deploying License-Free Wireless Wide-Area Networks

People often use OSI model and TCP/IP model interchangeably but there are some major differences between both models. TCP/IP model came into existence almost a decade before the implementation of OSI model ().

The main purpose behind developing the protocol was to build a robust and automatically recovering phone line failure while on the battlefield. This model was made up of two components, namely, seven-layer model and the subset of protocols. But they do have very subtle differences too. The most apparent difference is the number of layers. This model divides the entire networking functions into layers, where each layer performs a specific function. This model gives a brief idea about the process of data formatting, transmission, and finally the reception. Each of these functions take place in the layers, as described by the model. Let us have a look at the four layers: It is also known as Network Access layer and Network Interface layer. It explains how the data is transmitted from the host, through the network. The physical connectors like the coaxial cables, twisted pair wires, the optical fiber, interface cards, etc. Internet Layer This layer is also known as the Network Layer. The main function of this layer is to route the data to its destination. The data that is received by the link layer is made into data packets IP datagrams. The data packets contain the source and the destination IP address or logical address. These packets are sent on any network and are delivered independently. This indicates that the data is not received in the same order as it was sent. Transport Layer This layer is responsible for providing datagram services to the Application layer. This layer allows the host and the destination devices to communicate with each other for exchanging messages, irrespective of the underlying network type. Error control, congestion control, flow control, etc. TCP gives a reliable, end-to-end, connection-oriented data transfer, while UDP provides unreliable, connectionless data transfer between two computers. Application Layer It provides the user interface for communication. This is the layer where email, web browsers or FTP run. It is a theoretical model which explains the working of the networks. Physical Layer As the name suggests, this is the layer where the physical connection between two computers takes place. Data Link Layer The main function of this layer is to convert the data packets received from the upper layer into frames, and route the same to the physical layer. Error detection and correction is done at this layer, thus making it a reliable layer in the model. It establishes a logical link between the nodes and transmit frames sequentially. Network Layer The main function of this layer is to translate the network address into physical MAC address. The data has to be routed to its intended destination on the network. This layer is also responsible to determine the efficient route for transmitting the data to its destination. While doing so, it has to manage problems like network congestion, switching problems, etc. Transport Layer This layer provides end-to-end delivery of data between two nodes. It divides data into different packets before transmitting it. On receipt of these packets, the data is reassembled and forwarded to the next layer. If the data is lost in transmission or has errors, then this layer recovers the lost data and transmits the same. Session Layer This layer is responsible to establish and terminate connections between two communicating machines. This connection is known as a session, hence the name. It establishes full-duplex, half-duplex and simplex connection for communication. The sessions are also used to keep a track of the connections to the web server. Presentation Layer The data conversion takes place at this layer. The data that it receives from the application layer is converted into a suitable format that is recognized by the computer. For example, the conversion of a file from. Application Layer This layer provides a user interface by interacting with the running application. E-mail, FTP, web browsers, etc. It is absolutely vital to learn the above differences, if anyone wants to be an expert in the field of communication.

Chapter 8 : osi and tcp/ip model - - The Cisco Learning Network

Difference between OSI model and TCP/IP model The Internet Protocol Suite also known as TCP/IP is the set of communications protocols used for the Internet and other similar networks. It is named from two of the most important

protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two.

Chapter 9 : BeginByBasics: Similarities & DIfference Between TCP/IP & OSI Model

The TCP/IP model does not have a session layer (Layer 5 of the OSI reference model) or a presentation layer (Layer 6 of the OSI reference model). Both models have a lower layer that connects the upper layers to the actual physical network.