4 what is contained in the trailer of a data-link frame

As shown in the previous representation of the frame, the header and trailer are added to the already formed PDU, which is the package that contains data from the application layer to the network layer. Thus, providing an adequate demonstration of the role of the header and trailer of the frame is highly fundamental. Header function The header consists of control information whose function is to guide the entire frame to its correct destination. The header is added according to the media used, as well as the logical topology. The header, in turn, encompasses a number of fields, each dedicated to a work. However, the fields differ from one frame format to another, a typical frame header includes the following : Start of Frame field: this field identifies the beginning of the frame. When the frame travels through the media, it can be influenced by noise and therefore distorted, because the frame bits would be fused with bits caused by noise. For this reason, the frame is distinguished by bits added at first. (you'll learn more about this field in the Ethernet frame lesson). Source and destination address field: This field contains the physical address or MAC address of the transmission machine, as well as the receiving machine; are used to identify nodes in the media. Priority area/ Quality of service: indicates a certain type of communication service for its treatment. Field type: This field is responsible for indicating the top layer service contained in the frame. Logical Connection field: This fiel is responsible for establishing a logical connection between devices (nodes). Physical Link Control field: This field is used to establish media links. Flow control field: This field serves to prevent a station from overwhelming another station with data initiating and stopping traffic through the media. Congestion control field: indicates congestion in the media. These fields mentioned are not specific to a frame, but can be found in different frame formats, not necessarily in that order, or in the same fields. Tow data link layer function also adds a trailer at the end of each frame. The trailer is responsible for ensuring that the frames are received intact or without damage. A typical frame includes two fields as a trailer. Frame Sequence Field: This field is used to determine if errors occurred during frame transmission. In other words, when a frame leaves the sender, a specific arrangement of the numbers is added, and when the target is reached, the frames are checked, a calculation is made to see if the resulting numbers match those included in the header. If the numbers are the same, the frame is intact, but if the numbers are means that the frame is damaged and, as a result, will be discarded. The process creating numbers or a logical summary of the content of the frame in numbers at the source and the act of calculating the frame verification file at the destination is called Cyclic Redundancy Check or CRC, and the result is known as the CRC value. (you will learn more about how to calculate CRC in upcoming lessons). Stop Field: This field provides the frame with numbers that indicate where the end of the frame is, rather than the start field. No, post_ad no, no, no. Data Link Layer: Support and connection to top layer services The data link layer provides a means to exchange data through common local media. The data link layer performs two basic services: It allows the upper layers to access the support using techniques such as framing controls of how data is placed in the media and received from the media using techniques such as media access control and troubleshooting As with each of the OSI layers, there are specific terms of this layer: Frame - The Data Link layer PDU Node - The Layer 2 notation for network devices connected to a common medium Media/medium (physical)* - The physical means for the transfer of information between two nodes Network (physics)** - Two or more nodes connected to a common medium The data link layer is responsible for the exchange of frames between nodes through the media of a physical network. * It is important to understand the meaning of middle and middle words in the context of this chapter. Here, these words refer to the material that actually carries the signals representing the transmitted data. The media is the physical cable of copper, fiber optics or atmosphere through which the signals travel. In this chapter the media does not refer to the programming of content such as audio, animation, television and video as used when referring to digital and multimedia content. ** A physical network is different from a logical network. Logical networks are defined in the network layer by layouting the hierarchical address schema. Physical networks represent the interconnection of devices in a common medium. Sometimes a physical network is also known as a network segment. Upper layer access to the media As discussed, a network model allows each layer to work with minimal concern for the roles of the other layers. The data link layer relieves the upper layers of responsibility for putting data on the network and receiving data from the network. This layer provides services to support the communication processes of each medium on which the data should be transmitted. In any given exchange of network layer packages, there may be numerous layers of data link and transitions of At each jump along the way, a proxy device - usually a router - accepts frames from a medium, unscaths the frame, and then forwards the package into a new frame appropriate to the medium of this physical network segment. Physical. a data conversation between two distant hosts, such as a PC in Paris with an Internet server in Japan. While the two hosts may be communicating with their peer-to-peer network layer protocols (IP, for example), numerous data link layer protocols are likely to be used to transport IP packages over various types of LANs and WANs. This package exchange between two hosts requires a variety of protocols that must exist in the Data Link layer. Each transition in a router could require a different data link layer protocol for transportation in a new medium. Note that each link between devices uses a different medium. Between the PC and the router can be an Ethernet link. Routers are connected via a satellite link, and the laptop is connected via a wireless link to the latest router. In this example, as an IP package travels from the PC to the laptop, it will encapsulate in the Ethernet frame, decapsulated, processed, and then encapsulated in a new data link framework to cross the satellite link. For the final link, the package will use a wireless data link frame from the router to the laptop. The data link layer effectively isolates communication processes in the upper layers of media transitions that can occur from end to end. It receives a package and is directed to a top layer protocol, in this case IPv4 or IPv6, which does not need to be aware of what means the communication will use. Without the data link layer, a network layer protocol, such as IP, would have to make provisions to connect to all kinds of media that might exist along a delivery path. On the other hand, ip should adapt every time a new network or medium technology was developed. This process would hinder protocol and innovation and the development of network media. This is a key reason to use a layered approach to networking. The data link layer service range must include all currently used media types and methods to access it. Due to the number of communication services provided by the data link layer, it is difficult to generalize their role and provide examples of a generic set of services. For this reason, please note that any given protocol may or may not support all of these data link layer services. ISO 7498: Internetworking Basics : MTU : Data Link Layer - Controling across Local Media Layer 2 protocols specify the encapsulation of a package in a frame and techniques for obtaining the encapsulated package in and out of each medium. The technique used to obtain the media input and output framework is called a multimedia access control method. Because the data is transferred through different media, different methods of controlling access to the media may be required during the course of a single communication. Each network environment that packages encounter while traveling from a local host to a remote host may have different features. For example, a network environment may consist of many hosts facing access to network support ad hocly. Another environment may consist of a direct connection between only two devices on which data flows sequentially as bits in an orderly manner. The media access control methods described by data link layer protocols define the processes by which network devices can access network media and transmit frames in various network environments. A node that is a final device uses an adapter to make the network connection. For example, to connect to a LAN, the device would use the appropriate network interface card (NIC) to connect to the LAN media. The adapter manages the framing and multimedia access control. On intermediate devices such as a router, where the type of media could change for each connected network, different physical interfaces are used on the router to encapsulate the package in the appropriate frame, and a suitable multimedia access control method is used to access each link. The figure router has an Ethernet interface to connect to the LAN and a serial interface to connect to the WAN. As the router processes the frames, it will use the data link layer services to receive the frame of a medium, unseal it in layer 3 PDU, recapsulate the PDU in a new frame and place the frame in the middle of the next network link. Data Link Layer: Creating a Frame The description of a frame is a key element of each data link layer protocol. Data link layer protocols require control information to allow protocols to work. Control information can say: Which nodes are in communication with each other When communication between individual nodes begins and when it ends What errors occurred while communicating nodes Which nodes will communicate below The data link layer prepares a package for transport through local media encapsulating it with a header and trailer to create a frame. Unlike the other POUs discussed in this course, the data link layer frame includes: Data - The network layer header package - Contains control information, such as addressing, and is located at the beginning of the PDU trailer - Contains control information added at the end of PDU format data for transmission When data travels on the media , becomes a stream of or 1s and 0s. If a node receives long bit streams, how do you determine where a frame starts and stops or what bits the address represents? Framing breaks the flow into decipherable groupings, with control information inserted in the header and and values in different fields. This format gives physical signals a structure that can be received by nodes and decoded in packages to the destination. Typical field types include: Start and Stop Indicator Fields - The initial and final boundaries of the Denomination or Address Field type field - The type of PDU contained in the Quality framework - control fields A data field -The payload of the frame (network layer package) Fields at the end of the frame form the trailer. These fields are used for troubleshooting and mark the end of the frame. Not all protocols include all of these fields. The standards of a specific data link protocol define the actual frame format. Examples of frame formats will be discussed at the end of this chapter. Data Link Layer : Connecting the top layer services to the media The data link layer exists as a layer of connection between the layer software processes above it and the physical layer below it. As such, it prepares the network layer packages for transmission through some kind of support, be it copper, fiber, or atmosphere. In many cases, the Data Link layer is embodied as a physical entity, such as an Ethernet Network Interface Card (NIC), which is inserted into a computer's system bus and makes the connection between running software processes on your computer and physical media. However, IAS is not just a physical entity. The software associated with the NIC allows the NIC to perform its intermediate functions of preparing the data for the transmission and encoding of the data as signals to be sent in the associated media. Data Link Sublayers To support a wide variety of network functions, the Data Link layer is often divided into two sublayers: a top sublayer and a lower sublayer. The top sublayer defines software processes that provide services to network layer protocols. The lower sublayer defines the media access processes performed by your hardware. Separating the data link layer into sublayers allows a frame type defined by the upper layer to access different media types defined by the lower layer. Such is the case in many LAN technologies, including Ethernet. The two common LAN sublayers are: Logical Link Control Logical Link Control (LLC) places information in the frame that identifies which network layer protocol is being used for the framework. This information allows various layer 3 protocols, such as ip and IPX, to use the same network interface and media. Media Access Control Media Access Control (MAC) provides a data link layer by addressing and delimiting the data according to the media's physical signaling requirements and the type of data link layer protocol in Data Link Layer - Standards Unlike protocols in the upper layers of the TCP/IP suite, data link layer protocols are generally not defined by request for comment (RFCs). Although the Internet Engineering Task (IETF) maintains the protocols and functional services for the TCP/IP protocol suite in the upper layers, the IETF does not define the functions and operation of the network access layer of this model. The TCP/IP network access layer is the equivalent of the OSI data link and the physical layers. These two layers will be discussed in separate chapters for further examination. The functional protocols and services of the Data Link layer are described by engineering organizations (such as iEEE, ANSI and ITU) and communications companies. Engineering organizations establish public and open standards and protocols. Communications companies can establish and use owner protocols to take advantage of new advances in technology or market opportunities. The services and specifications of the data link layer are defined by multiple standards based on a variety of technologies and media to which the protocols apply. Some of these standards integrate the services layer 2 and layer 1. Engineering organizations that define open standards and protocols applied to the data link layer include: International Organization for Standardization (ISO) Institute of Electrical and Electronics Engineers (IEEE) American National Standards Institute (ANSI) International Telecommunication Union (ITU) Unlike upper layer protocols, which are mainly implemented in software such as the host operating system or specific applications, data link layer processes occur in both software and hardware. The protocols in this layer are implemented within the electronics of the network adapters with which the device connects to the physical network. For example, a device that implements the data link layer on a computer would be the network interface card (NIC). For a laptop, a wireless PCMCIA adapter is commonly used. Each of these adapters is hardware that meets the standards and protocols of layer 2. multimedia access control techniques by placing data in the media that regulate the placement of data frames in the media is known as multimedia access control. Among the different implementations of data link layer protocols, there are different methods of controlling access to the media. These multimedia access control techniques define whether and how the media's nodes share. Media access control is the equivalent of traffic rules governing the entry of motor vehicles to a road. The absence of any media access control would be the equivalent of vehicles ignoring the rest of the traffic and entering the without taking into account the rest of the vehicles. However, not all roads and entrances are the same. Traffic can enter the road by merging, waiting for its turn in a stop sign, or by obeying the signal lights. A driver follows a different set of rules for each type of entry. Similarly, there are different ways to regulate frameworks in the media. The protocols in the Data Link layer define the rules for accessing different media. Some multimedia access control methods use highly controlled processes to ensure that frames are securely placed in the media. These methods are defined by sophisticated protocols, which require mechanisms that enter over the network. The media access control method used depends on: Media sharing - If and how nodes share media topology - How the connection between nodes appears in the Media Access Control data link layer for shared media Some network topologies share a common medium with multiple nodes. At any time, there may be a number of devices trying to send and receive data using network support. There are rules governing how these devices share the media. There are two basic methods of media access control for shared media: Controlled - Each node has its own time to use the containment-based medium - All nodes compete for the use of the controlled means of access for shared media When using the controlled access method, network devices take turns, in sequence, to access the media. This method is also known as scheduled or deterministic access. If a device does not need to access the media, the opportunity to use the media moves to the next online device. When a device places a frame on the media, no other device can do so until the frame has reached the destination and has been processed by the destination. While controlled access is well ordered and provides predictable performance, deterministic methods can be inefficient because a device must wait its turn before it can use the media. Contention-based access for shared media is also known as non-deterministic methods based on containment allow any device to try to access the media whenever it has data to send. To avoid complete chaos in the media, these methods use a multiple access process (CSMA) of Carrier Sense to first detect whether the media carry a signal. If a carrier signal is detected on the media from another node, another device is transmitted. When the device trying to transmit sees that the media is busy, it will wait and try again after a short period of time. If no carrier signal is detected, the device transmits your data. Ethernet and wireless networks use multimedia access control based on containment. The CSMA process may fail and two devices may be transmitted to the Time. This is called data collision. If this happens, the data sent by both devices will be corrupted and should be resented. Methods of controlling access to media based on containment do not have the overload of controlled access methods. A monitoring mechanism that can be accessed in the media is not necessary. However, containment-based systems do not scale well under heavy media use. As use and number of nodes nodes the likelihood of successful access to the media without a collision decreases. In addition, the recovery mechanisms needed to correct errors due to these collisions further decrease performance. The CSMA is usually implemented in conjunction with a method of resolving media containment. The two commonly used methods are: CSMA/Collision Detection in CSMA/Collision Detection (CSMA/CD), the device monitors support for the presence of a data signal. If a data signal is absent, indicating that the media is free, the device transmits the data. If signals are detected showing that another device was transmitting at the same time, all devices stop sending and trying again later. Traditional forms of Ethernet use this method. CSMA/Collision Avoidance In CSMA/Collision Avoidance (CSMA/CA), the device examines the media for the presence of a data signal. If the media is free, the device sends a notification through the media of its intention to use it. Your device then sends the data. This method is used by 802.11 wireless network technologies. Media access control for unshared media control protocols for unshared media requires little or no control before placing frames on the media. These protocols have simpler rules and procedures for controlling media access. This is the case of point-to-point topologies. In point-to-point topologies, the media interconnects only two nodes. In this provision, nodes should not share the media with other hosts or determine whether a frame is intended for this node. Therefore, data link layer protocols have little to do with controlling unshared media access. Full duplex and half duplex In point-to-point connections, the Data Link layer should take into account whether the communication is half duplex or full duplex. See figure to see differences in both methods. Mid-duplex communication means that devices can transmit and receive in the media, but cannot do so simultaneously. Ethernet has established arbitration rules for resolving disputes arising from instances when more than one station attempts to transmit at the same time. In fully duplex communication, both devices can transmit and receive in the media at the same time. The Data Link layer assumes that the media is available for transmission of both nodes at any time. Therefore, there is no media arbitration necessary in the data link layer. Details of a specific media access control technique can only be examined by studying a specific media access control technique Specific. Within this course, we will study traditional ethernet, which uses CSMA/CD. Other techniques will be covered in later courses. Logical topology vs. Physical topology The topology of a network is the layout or relationship of network devices and the interconnections between them. Network topologies can be seen physically and logically. Physical physical topology the nodes and physical connections between them. The representation of how support is used to interconnect devices is physical topology. These will be covered in later chapters of this course. A logical topology is the way a network transfers frames from one node to another. This provision consists of virtual connections between the nodes of a network independent of its physical disposition. These logical signal paths are defined by data link layer protocols. The data link layer sees a network's logical topology when controlling data access to the media. It is the logical topology that influences the type of network framing and multimedia access control used. The physical or wired topology of a network probably won't be the same as logical topology. The logical topology of a network is closely related to the mechanism used to manage network access. Access methods provide procedures for managing network access so that all stations have access. When multiple entities share the same support, some mechanism must be in place to control access. Access methods apply to networks to regulate this media access. Access methods will be discussed in more detail later. The logical and physical topologies commonly used in networks are: Multi-access ring point-to-point The logical implementations of these topologies and their methods of controlling access to the associated media are considered in the following sections. Point-to-point topology A point-to-point topology connects two nodes directly together, as shown in the figure. In data networks with point-to-point topologies, the media access control protocol can be very simple. All media stills can only travel to or from both nodes. The frames are placed in the media by the node at one end and removed from the media by the node at the other end of the point-to-point circuit. In point-to-point networks, if the data can only flow in one direction at a time, it is functioning as a half-duplex link. If the data can flow correctly through the link from each node simultaneously, it is a complete duplex link. Data link layer protocols could provide more sophisticated multimedia access control processes for logical point-to-point topologies, but this would only add unnecessary protocol. Logical point-to-point networks End-to-end nodes that communicate on a point-to-point network can be physically connected through a series of intermediate devices. However, the use of physical devices on the network does not affect logical topology. As shown in the figure, the source and destination node may be indirectly with each other through a certain geographical distance. In some cases, the logical connection between nodes forms what is called a virtual circuit. A virtual circuit is a logical connection created within a network between two network devices. The two nodes at each end of the virtual circuit frames with each other. This happens even if frames are directed through proxy devices. Virtual circuits are important logical communication constructions used by some layer 2 technologies. The multimedia access method used by the Data Link protocol is determined by point-to-point logical topology, not physical topology. This means that the point-to-point logical connection between two nodes may not necessarily be between two physical nodes at each end of a single physical link. Multi-access topology A multi-access logical topology allows multiple nodes to communicate using the same shared media. Data from a single node can be placed on the media at the same time. Each node sees all the frames on the media, but only the node that the frame is addressed to processes the contents of the frame. Having many nodes share access to the media requires a data Link media access control method to regulate data transmission and thus reduce collisions between different signals. The multimedia access control methods used by the logical topologies of various accesses are usually CSMA/CD or CSMA/CA. However, token step methods can also be used. There are several media access control techniques available for this type of logical topology. The data link layer protocol specifies the media access control method that will provide the appropriate balance between frame control, frame protection, and network overload. Ring topology In a logical ring topology, each node in turn receives a frame. If the frame is not addressed to the node, the node passes the frame to the next node. This allows a ring to use a controlled media access control technique called a token step. Nodes in a logical ring topology remove the frame from the ring, examine the address and send it if it is not addressed for this node. In a ring, all nodes around the ring - between the source and the target node examine the frame. There are multiple media access control techniques that could be used with a logical ring, depending on the level of control required. For example, only one frame at a time is usually carried by the media. If no data is transmitted, a signal (known as a token) can be placed on the media and a node can only place a data frame on the media when it has the token. Note that the data link layer sees a logical ring topology. Real physical wiring topology could be another topology. Multimedia Access Data Link Layer Protocols and Framing Data Link Layer Protocols – The framework reminds you that although there are many different data link layer protocols describing the data link layer frames, each type of has three basic parts: all data link layer protocols encapsulate layer 3 PDU within the frame data field. However, the structure of the frame and the fields contained in the header and trailer vary according to the protocol. Protocol. The data link layer protocol describes the characteristics required for package transport across different media. These characteristics of the protocol are integrated into the encapsulation of the framework. When the frame reaches its destination and the Data Link protocol removes the media framework, the framing information is read and discarded. There is no frame structure that meets the needs of all data transport in all types of media. As shown in the figure, depending on the environment, the amount of control information required in the framework varies depending on the media's multimedia access control requirements and logical topology. Framing - Header function The frame header contains the control information specified by the data link layer protocol for specific logical topology and the media used. Frame control information is unique for each type of protocol. It is used by the Layer 2 protocol to provide features required by the communication environment. Typical frame header fields include: Start Frame Field - Indicates the start of the Source and Destination Address Fields - Indicates source and destination nodes frame in the Priority / Media Service Quality field - Indicates a particular type of communication service for field type processing - Indicates the top layer service contained in the Logical Connection Control Field - Used to establish a logical connection between the Physical Link Control Field nodes - Used to set the media link flow control field - Used to start and stop traffic over the media congestion control field - Indicates congestion in the media The above field names are non-specific fields listed as examples. Different data link layer protocols can use different fields from those mentioned. Because the purposes and functions of data link layer protocols are related to specific topologies and media, each protocol must be examined to gain a detailed understanding of its framework structure. As protocols are discussed in this course, more information about the structure of the framework will be explained. Addressing: Where the Data Link Layer goes provides addresses that are used to transport the frame through shared local media. The device addresses of this layer are known as physical addresses. The data link layer address is contained within the frame header and specifies the target node of the frame on the local network. The frame header can also contain the source address of the frame. Unlike the logical addresses of layer 3 that are hierarchical, physical addresses do not indicate in which device is located. If your device moves to another network or subnet, it will continue to work with the same physical address layer 2. Because the frame is only used to transport data between nodes through local media, the data link layer address is only used for local delivery. Addresses in this make no sense beyond the local network. Compare this with layer 3, where package header addresses are taken from the source host to the destination host, regardless of the number of network breaks along the path. If the frame package is to move to another network segment, the intermediate device - a router - will decay the original frame, create a new frame for the package and send it to the new segment. The new framework will use the source and destination addressing as needed to transport the package through the new media. Addressing requirements The need for data link layer addressing in this layer depends on logical topology. Point-to-point topologies, with only two interconnected nodes, do not require addressing. Once in the middle, the frame only has one place it can go. Because the ring and multi-access topologies can connect many nodes in a common medium, addressing is required for these typologies. When a frame reaches each node in the topology, the node examines the target address of the header to determine if it is the target of the frame. Framing – Function of Trailer Data Link layer protocols add a trailer to the end of each frame. The trailer is used to determine if the frame arrived without error. This process is called troubleshooting. Note that this is different from bug fixes. Error detection is achieved by placing a logical or mathematical summary of the bits that make up the frame in the trailer. Frame check sequence the Frame Sequence (FCS) field is used to determine if there were errors in the transmission and reception of the frame. Troubleshooting is added to the Data Link layer because this is where data is transferred through the media. Support is a potentially unsafe environment for data. Signals in the media could be subject to interference, distortions or losses that would substantially change the bit values representing these signals. The troubleshooting mechanism provided by using the FCS field discovers most of the errors caused to the media. To ensure that the content of the frame received at the destination matches that of the frame left by the source node, a transmission node creates a logical summary of the frame content. This is known as the cyclic redundancy check value (CRC). This value is placed in the Frame Verification Sequence (FCS) field in the frame to render the contents of the frame. When the frame reaches the target node, the receiver node calculates its own logical summary, or CRC, of the frame. The receiver node compares the two CRC values. If the two values are the same, the frame is considered to have come as transmitted. If the CRC value of the FCS differs from the CRC on the receiver node, the frame is discarded. There is always the small chance that a frame with a good CRC result will be really corrupt. Bit errors can be when the CRC is calculated. Upper layer protocols would be required to detect and correct this data loss. The protocol used in the Data Link layer will determine whether an error correction will be made. FCS is used to detect the error, but not all protocols will support bug fixes. Data Link Layer Protocols - The framework on a TCP/IP network, all OSI Layer 2 protocols work with the Internet protocol in layer 3 OSI. However, the actual layer 2 protocol used depends on the logical topology of the network and the implementation of the physical layer. Given the wide range of physical means used throughout the range of networked topologies, there is a correspondingly high number of 2 layer protocols in use. Protocols to be discussed in CCNA courses include: Ethernet Point-to-Point Protocol (PPP) High-Level Data Link Control (HDLC) Frame Relay Asynchronous Transfer Mode (ATM) Each protocol performs a multimedia access control for specified Layer 2 logical topologies. This means that multiple different network devices can act as nodes operating in the data link layer when these protocols are implemented. These devices include the network adapter or network interface cards (NICs) on computers, as well as interfaces on 2 layer routers and switches. The Layer 2 protocol used for a specific network topology is determined by the technology used to implement this topology. The technology is determined, in turn, by the size of the network - in terms of the number of hosts and geographic reach - and the services that must be provided over the network. LAN Technology A Local Area Network typically uses high bandwidth technology that is capable of supporting a large number of hosts. The relatively small geographic area of a LAN (a single building or a multi-building campus) and its high user density make this technology profitable. WAN technology However, the use of high-bandwidth technology is not usually cost effective for broad area networks covering large geographic areas (cities or multiple cities, for example). The cost of long-distance physical links and the technology used to carry signals over these distances typically results in lower bandwidth capacity. The difference in bandwidth usually results in the use of different protocols for LANs and WANs. Ethernet Protocol for LANs Ethernet is a family of network technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet standards define both layer 2 protocols and Layer 1 technologies. Ethernet is the most widely used LAN technology and supports data bandwidths of 10, 100, 1000 or 10,000 Mbps. Basic format IEEE sublayers and sublayers of layers 1 and 2 of OSI remain consistent in all forms of Ethernet. However, methods for detecting and placing data on media vary with different implementations. Ethernet provides unen recognized shared media using CSMA/CD as multimedia access methods. Shared media requires the Ethernet package header to use a data link layer address to identify the source and destination nodes. As with most lan protocols, this address is known as the MAC address of the node. An Ethernet MAC address is 48-bit and is generally represented in hexadecimal format. The Ethernet frame has many fields, as shown in the figure. In the data link layer, the frame structure is almost identical for all Ethernet speeds. However, in the physical layer, different versions of Ethernet apply bits to the media differently. Ethernet II is the Ethernet framework format used in TCP/IP networks. Ethernet is such an important part of data networking, we have dedicated a chapter to it. We also use it in examples throughout this series of courses. The Point-to-Point Protocol (PPP) is a protocol used to deliver frames between two nodes. Unlike many data link layer protocols defined by electrical engineering organizations, the PPP standard is defined by RFCs. PPP was developed as a WAN protocol and remains the protocol of choice for implementing many serial WANs. PPP can be used in various physical media, including twisted torque, fiber optic lines and satellite transmission, as well as for virtual connections. PPP uses a layered architecture. To accommodate the different types of media, PPP establishes logical connections, called sessions, between two nodes. The PPP session hides the underlying physical media from the upper PPP protocol. These sessions also provide PPP with a method to encapsulate various protocols through a point-to-point link. Each protocol encapsulated on the link establishes its own PPP session. PPP also allows both nodes to negotiate options within the PPP session. This includes authentication, compression and multilink (the use of multiple physical connections). Wireless Protocol for LANs 802.11 is an extension of IEEE 802 standards. It uses the same 802.2 LLC and 48-bit address scheme as another 802 LANs, however, there are many differences in the MAC sublayer and physical layer. In a wireless environment, the environment requires special considerations. There is no definable physical connectivity; Therefore, external factors can interfere with data transfer and it is difficult to control access. To meet these challenges, wireless standards have additional controls. Standard IEEE 802.11, commonly known as Wi-Fi, is a containment-based system using a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) media access process. CSMA/CA specifies a random backoff for all the nodes they are hoping to transmit. The most likely opportunity for average containment is right after the media becomes available. Make nodes go backwards during a random period reduces collision. 802.11 networks also use Data Link recognitions to confirm that a framework is received correctly. If the shipping station does not detect the recognition framework, either because the original data frame or recognition has not been received intact, the frame is relayed. This explicit recognition outweighs interference and other radio-related problems. Other 802.11 compatible services include authentication, association (wireless device connectivity) and privacy (encryption). The figure shows a frame 802.11. Contains these fields: Protocol version field - Frame version 802.11 type and subtype fields - Identifies one of the three functions and sub functions of the frame: control, data, and Management In the DS field - Set to 1 in the data frames intended for the distribution system (wireless structure devices) From the DS field - Set to 1 in data frames leaving the More Fragments Distribution System field - Set to 1 for frames that have another fragment reentry field - Set to 1 if the frame is a re Transmission of a previous frame power management field - Set to 1 to indicate that a node will be in power saving mode More Data field - Set to 1 to indicate to a node in power saving mode that more frames are buffer for this Wired Equivalent Privacy (WEP) field - Set to 1 if the frame contains information WEP encryption for security command field - Set to 1 in a data type frame that uses strictly ordered service class (does not need reordering) Field Duration/DD - Depending on the type of frame, represents time, in microseales, required to transmit the frame or association identity (AID) for the station that transmitted the target address framework (DA) field - MAC address of the final destination node in the network source field (SA) - MAC address of the started frame receiver Address Field (AR) - MAC address that identifies the wireless device that is the immediate recipient of the Frame Transmitter Address (TA) field - MAC address that identifies the wireless device that transmitted the frame sequence number field - Indicates the sequence number assigned to the frame; Relay frames are identified by duplicate sequence numbers Fragment Number field - Indicates the number for each fragment of a frame Frame field body - Contains the information that is transported; for data frames, usually an FCS field IP package - Contains a 32-bit cyclic redundancy check (CRC) of the framework PPP protocol: PPP provider extensions: Putting it All Together Follow Data Through an Internetwork The figure of the following page presents a data transfer between two hosts through a task on the Internet. We emphasize the function of each layer during communication. For this example, we will represent a request between a client and a server. To focus on the data transfer process, we are omitting many items that may occur in a real transaction. At every step we are only paying attention to the main elements. Many parts of headers are ignored, for example. We are assuming that all routing tables are converging and the ARP tables are complete. In addition, we are assuming that a TCP session has already been established between the client and the server. We will also assume that DNS search for the WWW server is already cached in the client. In the WAN connection between the two routers, we are assuming that PPP has already established a physical circuit and has established a PPP session. On the next page, you can go through this communication. We encourage you to carefully read each explanation and study the operation of the layers for each device. Device.