DOWNLOAD PDF BASIC PROTOCOLS IN NETWORKING

Chapter 1 : Communication protocol - Wikipedia

A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some.

Justin Ellingwood Introduction A basic understanding of networking is important for anyone managing a server. Not only is it essential for getting your services online and running smoothly, it also gives you the insight to diagnose problems. This document will provide a basic overview of some common networking concepts. We will discuss basic terminology, common protocols, and the responsibilities and characteristics of the different layers of networking. This guide is operating system agnostic, but should be very helpful when implementing features and services that utilize networking on your server. Networking Glossary Before we begin discussing networking with any depth, we must define some common terms that you will see throughout this guide, and in other guides and documentation regarding networking. These terms will be expanded upon in the appropriate sections that follow: In networking, a connection refers to pieces of related information that are transfered through a network. This generally infers that a connection is built before the data transfer by following the procedures laid out in a protocol and then is deconstructed at the at the end of the data transfer. A packet is, generally speaking, the most basic unit that is transfered over a network. When communicating over a network, packets are the envelopes that carry your data in pieces from one end point to the other. Packets have a header portion that contains information about the packet including the source and destination, timestamps, network hops, etc. The main portion of a packet contains the actual data being transfered. It is sometimes called the body or the payload. A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually. A network interface may be associated with a physical device, or it may be a representation of a virtual interface. The "loopback" device, which is a virtual interface to the local machine, is an example of this. LAN stands for "local area network". It refers to a network or a portion of a network that is not publicly accessible to the greater internet. A home or office network is an example of a LAN. WAN stands for "wide area network". It means a network that is much more extensive than a LAN. While WAN is the relevant term to use to describe large, dispersed networks in general, it is usually meant to mean the internet, as a whole. If an interface is said to be connected to the WAN, it is generally assumed that it is reachable through the internet. A protocol is a set of rules and standards that basically define a language that devices can use to communicate. There are a great number of protocols in use extensively in networking, and they are often implemented in different layers. A port is an address on a single machine that can be tied to a specific piece of software. It is not a physical interface or location, but it allows your server to be able to communicate using more than one application. A firewall is a program that decides whether traffic coming into a server or going out should be allowed. A firewall usually works by creating rules for which type of traffic is acceptable on which ports. Generally, firewalls block ports that are not used by a specific application on a server. NAT stands for network address translation. It is a way to translate requests that are incoming into a routing server to the relevant devices or servers that it knows about in the LAN. This is usually implemented in physical LANs as a way to route requests through one IP address to the necessary backend servers. VPN stands for virtual private network. It is a means of connecting separate LANs through the internet, while maintaining privacy. This is used as a means of connecting remote systems as if they were on a local network, often for security reasons. There are many other terms that you may come across, and this list cannot afford to be exhaustive. We will explain other terms as we need them. At this point, you should understand some basic, high-level concepts that will enable us to better discuss the topics to come. Network Layers While networking is often discussed in terms of topology in a horizontal way, between hosts, its implementation is layered in a vertical fashion throughout a computer or network. What this means is that there are multiple technologies and protocols that are built on top of each other in order for communication to function more easily. Each successive, higher layer abstracts the raw data a little bit more, and makes it simpler to use for applications and users. It also allows you to leverage lower layers in new ways without having to invest the time and energy to develop the protocols and applications that handle those types of traffic. The language that we use to talk about each of the layering scheme varies significantly depending on which model you use. Regardless of the model used to discuss the layers, the path of data is the same. As data is sent out of one machine, it begins at the top of the stack and filters downwards. At the lowest level, actual transmission to another machine takes place. At this point, the data travels back up through the layers of the other computer. Each layer has the ability to add its own "wrapper" around the data that it receives from the adjacent layer, which will help the layers that come after decide what to do with the data when it is passed off. This model defines seven separate layers. The layers in this model are: The application layer is the layer that the users and user-applications most often interact with. Network communication is discussed in terms of availability of resources, partners to communicate with, and data synchronization. The presentation layer is responsible for mapping resources and creating context. It is used to translate lower level networking data into data that applications expect to see. The session layer is a connection handler. It creates, maintains, and destroys connections between nodes in a persistent way. The transport layer is responsible for handing the layers above it a reliable connection. In this context, reliable refers to the ability to verify that a piece of data was received intact at the other end of the connection. This layer can resend information that has been dropped or corrupted and can acknowledge the receipt of data to remote computers. The network layer is used to route data between different nodes on the network. It uses addresses to be able to tell which computer to send information to. This layer can also break apart larger messages into smaller chunks to be reassembled on the opposite end. This layer is implemented as a method of establishing and maintaining reliable links between different nodes or devices on a network using existing physical connections. The physical layer is responsible for handling the actual physical devices that are used to make a connection. This layer involves the bare software that manages physical connections as well as the hardware itself like Ethernet. As you can see, there are many different layers that can be discussed based on their proximity to bare hardware and the functionality that they provide. It defines the four separate layers, some of which overlap with the OSI model: In this model, the application layer is responsible for creating and transmitting user data between applications. The applications can be on remote systems, and should appear to operate as if locally to the end user. The communication is said to take place between peers. The transport layer is responsible for communication between processes. This level of networking utilizes ports to address different services. It can build up unreliable or reliable connections depending on the type of protocol used. The internet layer is used to transport data from node to node in a network. This layer is aware of the endpoints of the connections, but does not worry about the actual connection needed to get from one place to another. IP addresses are defined in this layer as a way of reaching remote systems in an addressable manner. The link layer implements the actual topology of the local network that allows the internet layer to present an addressable interface. It establishes connections between neighboring nodes to send data. This made it easier to implement and allowed it to become the dominant way that networking layers are categorized. Interfaces Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device. Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have. In addition, it will define a virtual network interface called the "loopback" or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the "lo" interface in many tools. Many times, administrators configure one interface to service traffic to the internet and another interface for a LAN or private network. In DigitalOcean, in datacenters with private networking enabled, your VPS will have two networking interfaces in addition to the local interface. The "eth0" interface will be configured to handle traffic from the internet, while the "eth1" interface will operate to communicate with the private network. Protocols Networking works by piggybacking a number of different protocols on top of each other. In this way, one piece of data can be transmitted using multiple protocols encapsulated within one another. We will talk about some of the more common protocols that you may come across and attempt to explain the difference, as well as give context as to what part of the process they are involved with. We will start with protocols implemented on the lower networking layers and work our way up to protocols with higher abstraction. Media Access Control Media access control is a communications protocol that is used to distinguish specific devices. Each device is supposed to get a unique MAC address during the manufacturing process that differentiates it from every other device on the internet. Addressing hardware by the MAC address allows you to reference a device by a unique value even when the software on top may change the name for that specific device during operation. Media access control is one of the only protocols from the link layer that you are likely to interact with on a regular basis.

Chapter 2 : What is a Network Protocol

We will discuss basic terminology, common protocols, and the responsibilities and characteristics of the different layers of networking. This guide is operating system agnostic, but should be very helpful when implementing features and services that utilize networking on your server.

This installment of Networking is designed to be a gentle introduction into the world of routing issues and concepts, arguably the most interesting and important part of networking, explaining the problems routing protocols address so you can understand why they do what they do. Before we get into the details, a clarification. When you hear people refer to "non-routable addresses," they are talking about RFC IP addresses, i. Despite the misleading label, they certainly are routable. You can and should have some They can even be co-mingled with your real routers. You should drop these packets at your border, as was pointed out in this Border Security article last year. This is a point of confusion for a lot of people. On to the topic at hand. Routing, in essence, is the act of finding a path from one place to another on which a packet can travel. To find this path, we need algorithms. They will generally be distributed among many routers, allowing them to jointly share information. Routing is said to contain three elements: Routing protocols, the things that allow information to be gathered and distributed Routing algorithms, to determine paths Routing databases to store information that the algorithm has discovered. The routing database sometimes corresponds directly to routing table entries, sometimes not. Our installment on layers actually introduces a bit of routing by talking about the paths an IP packet takes through operating systems and routers. What may not have been clear, though, is how the routing table lookup step works. Most routers will simply find the shortest prefix in the routing table when it looks for a path for your packet. We also need to understand some really basic problems with routing. Just like in Layer 2, routers need to be redundant. Redundancy always introduces the possibility of a loop, and every routing protocol has to deal with this. The idea of a network topology is pretty absurd in the context most people picture it. VLANs define turned the world up side down in that regard. But in routing, topology is actually important, if you zoom out a bit. If your network core has a bunch of stubs connected, many of the stub routers will know nothing about each other. But pay attention here: You get packets closer to the destination. This is also known as a routing domain. A routing domain is a set of routers that are all under the same administrative control; presumably all running the same routing protocols. When routing packets, we have a few paradigms to choose from. The telco world sets up a circuit for your telephone call as soon as you dial. The IP world does not, and it can handle much more traffic. The tradeoff is that you can get congestion, and sometimes fail to reach certain websites, whereas your telephone call will never drop because of congestion. The IP world can almost do this, through a mechanism called loose source routing. This is how it started: So we use dynamic routing protocols to figure out the paths for us. Take note that each direction can take a different path! Routing protocols are broken up into a few different categories, in two senses. These are routing protocols that deal with intra-domain routing. Second, routing protocols are said to be of two categories in another sense: The vector-distance approach is: Link-state is very computationally intensive, but it provides an entire view of the network to all routers. Most people prefer link-state protocols because they converge faster, which means that all of the routers have the same information. Come back next week for our first routing protocol: In a Nutshell Routers send packets toward their destination, normally by shipping it toward a router that knows a bit more about the destination topology. Routing is two one-way problems; it is very common for your packets to take asymmetric routes.

Chapter 3 : An Introduction to Networking Terminology, Interfaces, and Protocols | DigitalOcean

Protocols and standards are what make networks work together. Protocols make it possible for the various components of a network to communicate with each other. Standards also make it possible for network components manufactured by different companies to work together. A protocol is a set of rules.

March 27, By steve Basic Networking Course for Beginners Computer networks consist of many different components, technologies and protocols working together. Getting Started In order for two computers to talk to each other they need: To be Connected cable or Wireless this is known as the connection media. To have a common language. To have An Address. Connecting Computers Together Early computer networks used cable to connect computers together in a wired network. Most modern networks use wireless wi-Fi as the main connection media and networks tend to be a mixture of wired and wireless. The diagram below shows a wired Ethernet network. To work each device must be connected to a Ethernet hub or switch. However logically they are all connected together and share the same media which we see later. For a Wireless network the devices must connect to a wire access point as shown in the diagram below. However,again logically they share and compete for access to the same media. Wireless access usually have an Ethernet hub built in which allows them to connect to the wired Ethernet network. Ethernet Addressing In order to communicate with each other each computer needs to have a unique address. This address is called the MAC media access control address and is built into the network card. The address is also often called the physical address and the Ethernet address. It is shown as 6 hexadecimal numbers separated by colons e. Notice windows using a dash â€" as a delimiter. On modern network cards it is possible for MAC addresses to be manually assigned, but it is not normal to do so. In addition 64 bit MAC addresses are now used. Links and Networks Ethernet is a data link protocol. It is possible for computers to talk to each other using just Ethernet, and with no networking protocol, but it is not practical You can liken a link to a street. Streets have houses and houses have numbers. An Ethernet link the street has computers houses which in turn have numbers Ethernet, Mac Address or Physical Address. However you can have many streets and the streets are connected. Routers divide out Ethernet links into networks. The Networking protocol also has addresses IP address , and these addresses are not fixed but assigned by a network administrator or automatically using a service called DHCP Dynamic host Configuration protocol. Ethernet Broadcasts, Broadcast Domains and Collisions To send a message to all computers on an Ethernet network a broadcast address Mac Address of all ones is used. See Understanding binary numbers The broadcast domain is the effective range of the broadcast, which can be limited by inserting level 3 IP level network devices e. A broadcast will be re-transmitted by hubs, switches, bridges level 2 and repeaters level 1. Levels are the levels in the 7 layer OSI data model. Network devices Bridges and switches working at level 2 data link layer can create separate collision domains. Even though bridges and switches divide a network into separate collision domains, the computers are still part of the same broadcast domain. This is shown in the diagram below. However a broadcast will be seen by devices on both sides of the switch. Bridges vs Switches Bridges and switches do very similar functions and today you can only buy switches. Bridges were used to join network segments i. Hubs vs Switches Hubs operate at the physical level, and were once the primary mechanism for connecting computers together. Hubs do not create a separate collision domain they just repeat packets. They have been replaced by switches. If you look on Amazon for a hub it will be a switch. The term frame is used for data units at the data link level and the the term packet for data units and the networking level. Hence we have Ethernet frames and IP packets. The data frame contains data and frame management information. The concept used to describe data frames is that of a letter and envelope. The letter is the data which is placed inside an envelope that contains the addressing information. This concept of data being inserted into an envelope is used repeatedly in data communications, and it is an important one to grasp. The envelope containing the data letter can simply be inserted into another envelope and so on. Although the Ethernet protocol alone is sufficient to get data between two nodes on an Ethernet network, it is not used on its own. Ethernet represents what is known as a data link protocol, and for networking we need a networking protocol which in our case is IP internet protocol. It is however the IP protocol which contains the important IP addresses, which are used for connecting computers together across the Internet, and in local networks. The diagram below illustrates how data is placed inside protocol envelopes headers. At the receiving end it is unpacked in the reverse order. The IP address is the most important address as far as we are concerned, as it is a logical address, meaning it is assigned by us, and can be changed. Current networks use IPv4 Addresses. The IP IPv4 address is a 32 bit address and is written in dotted decimal notation and appears like this: So it is of this form: When troubleshooting network problems you will need to be able to identify network addresses, and if a device has one, and whether that address is valid. If a client cannot get an IP address then some clients will auto assign an IP address. Different versions of windows use different default IP addresses In either case it is unlikely to work correctly because clients with a In our street analogy they think they are on different streets. Finding Your IP Address To find the IP address on a windows computer using ipconfig, open a command line dos prompt and type the command ipconfig at the prompt. The following is displayed Note: You may have more than one network address if you have multiple network cards installed. The IP address here is You will also see the default gateway address This is the IP address of the Router, the term gateway is an old Unix expression that is still used. The IP address will be used to get the data packet to the final network segment. In order to deliver the packet to the final destination the MAC address of the destination computer must be known. A protocol know as ARP address resolution protocol is used, which uses an Ethernet broadcast to query the nodes on the network. The query is basically: Send me your MAC address. All nodes see the query but only the node with the destination IP address replies. IP Networks Computers and other devices can be grouped together into networks. In the real world this is the same as houses are grouped together into streets. To separate devices into networks a router is required. Network numbers are part of the IP address. So when you look at an IP address what you see is a number with two components. A network component and a node component It is the job of the Subnet mask to split the IP address into the network component and the Node component device address. For my network my computer has an IP address of To find the network address you do a logical AND of the two numbers. This gives a network number of

Chapter 4 : List of Common Network Port Numbers - Utilize Windows

Networking and Ethernet Basics Protocols. After a physical connection has been established, network protocols define the standards that allow computers to communicate.

An FTP server can easily be set up with little networking knowledge and provides the ability to easily relocate files from one system to another. It is typically used as a secure alternative to Telnet which does not support secure connections. Telnet TCP 23 Telnet is the primary method used to manage network devices at the command level. Unlike SSH which provides a secure connection, Telnet does not, it simply provides a basic unsecured connection. Many lower level network devices support Telnet and not SSH as it required some additional processing. Caution should be used when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear. These different TLD managers then contain information for the second level domains that are typically used by individual users for example, cisco. A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system. A DHCP server can be set up by an administrator or engineer with a poll of addresses that are available for assignment. When a client device is turned on it can request an IP address from the local DHCP server, if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the poll for assignment. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server. NTP is used to synchronize the devices on the Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate. NBT has long been the central protocol used to interconnect Microsoft Windows machines. SNMP has a number of different abilities including the ability to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific actions are occurring. Typically, these are configured to be used when an alerting condition is happening. In this situation, the device will send a trap to network management stating that an event has occurred and that the device should be looked at further for a source to the event. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet. Summary While it may seem obvious that there are large number of ports that are missing from this list, the purpose here was to just cover the most commonly seen and used protocols. The complete list of assigned ports and their assigned services can be seen at http: Hopefully the contents of this article will help in determining the correct port number to use when implementing these services. Page 1 of 1.

Chapter 5 : Networking Basics: TCP, UDP, TCP/IP and OSI Model | Pluralsight

Basic Networking Course for Beginners Computer networks consist of many different components, technologies and protocols working together. In this tutorial/course we look at the fundamentals of how computers communicate on a TCP/IP network.

Throughout this article you will find useful information concerning the protocol suite of the century: Fasten your seat belts and have a good ride! It consists of four instead of seven layers. Despite their architectural differences, both models have interchangeable transport and network layers and their operation is based upon packet-switched technology. The diagram below indicates the differences between the two models: The Application layer deals with representation, encoding and dialog control issues. Its responsibilities include application data segmentation, transmission reliability, flow and error control. Their purpose is to route packets to their destination independent of the path taken. The network access layer deals with all the physical issues concerning data termination on network media. Host-to-Host Layer Protocols Two protocols: We will look at the details of both these protocols as well as their interaction with the upper layer. TCP protocol data units are called segments. The sending and receiving TCP entities exchange data in the form of segments, which consist of a fixed byte header followed by a variable size data field. TCP is responsible for breaking down a stream of bytes into segments and reconnecting them at the other end, retransmitting whatever might be lost and also organizing the segments in the correct order. The segment size is restricted by the maximum transfer unit MTU of the underlying link layer technology MTU is generally bytes which is the maximum payload size of the Ethernet. The image below shows the TCP segment format. The most important fields are explained further on. Source Port and Destination Port fields together identify the two local end points of the particular connection. Ports are used to communicate with the upper layer and distinguish different application sessions on the host. The Sequence Number and Acknowledgment Number fields specify bytes in the byte stream. The sequence number is used for segment differentiation and is useful for reordering or retransmitting lost segments. The Acknowledgment number is set to the next segment expected. The Window field indicates how many bytes can be transmitted before an acknowledgment is received. The Checksum field is used to provide extra reliability and security to the TCP segment. The actual user data are included after the end of the header. The image below shows a request-response message sequence carried over TCP. Notice the fields discussed above: The reason for that is because certain data types do not require reliable delivery and extra overhead. Real-time traffic for example, needs to be transported in an efficient way without error correction and retransmission mechanisms. UDP is considered to be a connectionless protocol. It leaves reliability to be handled by the application layer. All it cares about is fast transmission. The UDP segment format is presented in the diagram below: Notice the small header size. Which One Should You Use? Choosing the right transport protocol to use depends on the type of data to be transferred. For information that needs reliability, sequence transmission and data integrity -- TCP is the transport protocol to use. For data that require real-time transmission with low overhead and less processing -- UDP is the right choice. The following table summarizes the key-characteristics of each one of these protocols. Keep them in mind when choosing the transport protocol for your data. See how they stack up with this assessment from Smarterer. Get our content first. If this message remains, it may be due to cookies being disabled or to an ad blocker. Stelios is currently working as a VoIP Engineer in a Telecom company, where he uses his knowledge in practice. His enthusiasm, ambition and knowledge motivate him to offer his best.

Chapter 6 : TCP/IP Ports and Protocols | TCP/IP Ports and Protocols | Pearson IT Certification

The protocols described below each enable this critical function of routers and computer networking. How Routing Protocols Work Every network routing protocol performs three basic functions.

Basic Internet Knowledge and Protocols Basic Internet Knowledge and Protocols Introduction The Internet is generally defined as a global network connecting millions of computers More than countries are linked into exchanges of data, news, and opinions. A protocol is a standard procedure used to connect two data communication devices. The Internet is a massive network of networks. Packet switching is a digital networking communication method used for transmitting data. Each site has a unique URL. Concepts History of Internet: In this, Ray has included symbol as address. A system must contain the IP address and it should be unique. The Internet protocol consists of two protocols: The Internet Protocol determines basic applications, for example, electronic mail, terminal imitating, and record exchange. Internet protocol architecture consists of four layers, they are: Data link layer Transport layer Application layer Data link layer: The data link layer is used for the encoding, decoding and logical organization of data bits. Data packets are framed and addressed by this layer. The main aim of this layer is to deliver packets from source to destination across multiple links networks. If two computers system are connected to the same link then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller. The main aim of the transport layer is to be delivered the entire message from source to destination. It decides if data transmission should be on the parallel path or single path. It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services. A web server is a computer that provides web services to the client. A page hosted on the internet is known as web page. It can be viewed by a browser. A browser can help locate a website on the internet. Email is an electronic mail. It is used to send and receive the messages. It consists of two components like message header and message body. The message header contains added addresses and the body contains any information and sends any attached contents. The Internet makes your work easy by communication technologies. It is hard to find an Internet user, who has not used it to download music and movies. Apart from it, there are lots of other things that can be downloaded using the internet as well. Search for relevant information: If you are not sure about something, then one of the easiest ways to know more about it is by searching it on the internet. Online booking has made things really easy. The process is very easy, convenient and super-fast. The use of internet is not limited merely to booking tickets. With help of net, you can do a full-fledged online shopping. On popular e-stores like Ebay, Amazon etc. One of the best things about internet is that is has made communication very easy and convenient. We can make friends through social networks like Facebook, twitter etc. Social networks have got really big since last decade. Facebook and Twitter are the new online sites who like to share all the latest happening of their life on these social networks and keep their profile duly updated. Banking was never so easy and convenient before! Right from opening an account to operating it, E-Banking has really useful for everyone. We can also do online transactions from the other accounts sitting at the home. Data sharing was never so easy and quick before!

Chapter 7 : Learn Networking Basics

If you are completely new to networking then the basic course will introduce you to the basic networking protocols used in small home/office networks and on the Internet. Setting Up and building a Home Network will introduce some basic networking component and show you how to build a home network and connect it to the Internet.

Communicating systems[edit] The information exchanged between devices through a network or other media is governed by rules and conventions that can be set out in communication protocol specifications. The nature of a communication, the actual data exchanged and any state -dependent behaviors, is defined by these specifications. In digital computing systems, the rules can be expressed by algorithms and data structures. Protocols are to communication what algorithms or programming languages are to computations. This communication is governed by well-understood protocols, which can be embedded in the process code itself. Transmission is not necessarily reliable, and individual systems may use different hardware or operating systems. This framework implements the networking functionality of the operating system. At the time the Internet was developed, abstraction layering had proven to be a successful design approach for both compiler and operating system design and, given the similarities between programming languages and communication protocols, the originally monolithic networking programs were decomposed into cooperating protocols. Instead they use a set of cooperating protocols, sometimes called a protocol suite. The protocols can be arranged based on functionality in groups, for instance there is a group of transport protocols. The functionalities are mapped onto the layers, each layer solving a distinct class of problems relating to, for instance: The selection of the next protocol is accomplished by extending the message with a protocol selector for each layer. The data received has to be evaluated in the context of the progress of the conversation, a protocol therefore must include rules describing the context. These kind of rules are said to express the syntax of the communication. Other rules determine whether the data is meaningful for the context in which the exchange takes place. These kind of rules are said to express the semantics of the communication. Messages are sent and received on communicating systems to establish communication. Protocols should therefore specify rules governing the transmission. In general, much of the following should be addressed: The bitstrings are divided in fields and each field carries information relevant to the protocol. Conceptually the bitstring is divided into two parts called the header and the payload. The actual message is carried in the payload. The header area contains the fields with relevance to the operation of the protocol. Bitstrings longer than the maximum transmission unit MTU are divided in pieces of appropriate size. The addresses are carried in the header area of the bitstrings, allowing the receivers to determine whether the bitstrings are of interest and should be processed or should be ignored. A connection between a sender and a receiver can be identified using an address pair sender address, receiver address. Usually some address values have special meanings. An all-1s address could be taken to mean an addressing of all stations on the network, so sending to this address would result in a broadcast on the local network. The rules describing the meanings of the address value are collectively called an addressing scheme. This is referred to as address mapping. On the Internet, the networks are connected using routers. The interconnection of networks through routers is called internetworking. Detection of transmission errors Error detection is necessary on networks where data corruption is possible. In a common approach, CRCs of the data area are added to the end of packets, making it possible for the receiver to detect differences caused by corruption. The receiver rejects the packets on CRC differences and arranges somehow for retransmission. Acknowledgements are sent from receivers back to their respective senders. To cope with this, under some protocols, a sender may expect an acknowledgement of correct reception from the receiver within a certain amount of time. Thus, on timeouts , the sender may need to retransmit the information. Exceeding the retry limit is considered an error. This is known as media access control. Arrangements have to be made to accommodate the case of collision or contention where two parties respectively simultaneously transmit or wish to transmit. As a result, pieces may arrive out of sequence. Retransmissions can result in duplicate pieces. By marking the pieces with sequence information at the sender, the receiver can determine what was lost or duplicated, ask for necessary retransmissions and reassemble the original message. Flow control can be implemented by messaging from receiver to sender. Design of complex protocols often involves decomposition into simpler, cooperating protocols. Such a set of cooperating protocols is sometimes called a protocol family or a protocol suite, [10] within a conceptual framework. Communicating systems operate concurrently. An important aspect of concurrent programming is the synchronization of software for receiving and transmitting messages of communication in proper sequencing. Concurrent programming has traditionally been a topic in operating systems theory texts. Mealy and Moore machines are in use as design tools in digital electronics systems encountered in the form of hardware used in telecommunication or electronic devices in general. In analogy, a transfer mechanism of a protocol is comparable to a central processing unit CPU. The framework introduces rules that allow the programmer to design cooperating protocols independently of one another. Protocols are to computer communication what programming languages are to computation. In modern protocol design, protocols are layered to form a protocol stack. Layering is a design principle which divides the protocol design task into smaller steps, each of which accomplishes a specific part, interacting with the other parts of the protocol only in a small number of well-defined ways. Layering allows the parts of a protocol to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple. Layering also permits familiar protocols to be adapted to unusual circumstances. For example, the mail protocol can be adapted to send messages to aircraft by changing the V. The communication protocols in use in the Internet are designed to function in diverse and complex settings. This model was expanded to four layers by additional protocols. However, the Internet protocol development has not focussed on the principle of layering as mandatory recipe for communication, rather it evolved as a convenient description of modularity and protocol cooperation. A different model is the OSI seven layer model , which was developed internationally as a rigorous reference model for general communication, with much stricter rules of protocol interaction and a rigorous layering concept of functionality. Typically, application software is built upon a robust data transport layer. Underlying this transport layer is a datagram delivery and routing mechanism that is typically connectionless in the Internet. Packet relaying across networks happens over another layer that involves only network link technologies, which are often specific to certain physical layer technologies, such as Ethernet. Layering provides opportunities to exchange technologies when needed, for example, protocols are often stacked in a tunneling arrangement to accommodate connection of dissimilar networks. Protocol layering[edit] Figure 3. Message flows using a protocol suite. Black loops show the actual messaging loops, red loops are the effective communication between layers enabled by the lower layers. Protocol layering now forms the basis of protocol design. The Internet protocol suite consists of the following layers: Computations deal with algorithms and data and communication involves protocols and messages, so the analog of a data flow diagram is some kind of message flow diagram. The systems both make use of the same protocol suite. The vertical flows and protocols are in system and the horizontal message flows and protocols are between systems. The message flows are governed by rules, and data formats specified by protocols. The blue lines therefore mark the boundaries of the horizontal protocol layers. The horizontal protocols are layered protocols and all belong to the protocol suite. Layered protocols allow the protocol designer to concentrate on one layer at a time, without worrying about how other layers perform. This can be achieved using a technique called Encapsulation. The pieces contain a header area and a data area. The result is that at the lowest level the piece looks like this: This rule therefore ensures that the protocol layering principle holds and effectively virtualizes all but the lowest transmission lines, so for this reason some message flows are coloured red in figure 3. To ensure both sides use the same protocol, the pieces also carry data identifying the protocol in their header. The design of the protocol layering and the network or Internet architecture are interrelated, so one cannot be designed without the other. The Internet offers universal interconnection, which means that any pair of computers connected to the Internet is allowed to communicate. Each computer is identified by an address on the Internet. All the interconnected physical networks appear to the user as a single large network. This interconnection scheme is called an internetwork or internet. The netid identifies a network and the hostid identifies a host. The term host is misleading in that an individual computer can have multiple network interfaces each having its own Internet address. An Internet Address identifies a connection to the network, not an individual computer. The mapping is called address resolution. This way physical addresses are only used by the protocols of the network interface layer. Message flows in the presence of a router Physical networks are interconnected by routers. Routers forward packets between interconnected networks making it possible for hosts to reach hosts on other physical networks. The message flows between two communicating systems A and B in the presence of a router R are illustrated in figure 4. Datagrams are passed from router to router until a router is reached that can deliver the datagram on a physically attached network called direct delivery. The table consists of pairs of networkids and the paths to be taken to reach known networks.

Chapter 8 : Data Communication & Computer Network

This is a list of articles that list different types or classifications of communication protocols used in computer networks.

Today computer networks are everywhere. You will find them in homes, offices, factories, hospitals leisure centres etc. But how are they created? What technologies do they use? In this tutorial you will learn the basic networking technologies, terms and concepts used in all types of networks both wired and wireless, home and office. Home and Office Networks The network you have at home uses the same networking technologies, protocols and services that are used in large corporate networks and on the Internet. The only real difference between an home network and a large corporate network is the size. A home network will have between 1 and 20 devices and a corporate network will have many thousands. Setting Up and building a Home Network will introduce some basic networking component and show you how to build a home network and connect it to the Internet. Networking Types and Structures Networks can be wired or wireless with most networks being a mixture of both. Wired vs Wireless Networks Early pre networks were predominately wired. Today however most networks will use a mixture of wired and wireless network. Wired networks use Ethernet as the data link protocol. Wired networks are faster than Wireless. Data rates were periodically increased from the original 10 megabits per second, to 1gigabits per second. Most home networks use Mbps. More secure than Wireless Need to Use cable which can be unsightly, difficult to run and expensive. Note a new technology that uses mains cable overcomes many of these disadvantages. Wireless Networks â€" Advantages and Disadvantages Wireless networks use Wi-fi as the data link protocol. However other wireless options are being developed for the IOT Internet of things. Advantages Generally easier to set up. Can be used both on home and public networks No cables required. Can be used with mobile phones and tablets. Wireless Networks Disadvantages Generally Slower than wired networks. Not as secure depending on set up. Networking Topologies and Layout There are many different ways network nodes can be connected together. There are many different ways network nodes can be connected together. Common connection technologies like Wi-Fi, Bluetooth etc are designed to work using a particular network topology. When designing networks and choosing connection protocols having an understanding of these topologies is important.

Chapter 9 : Network Protocol - Types of Network Protocols

1 Basic Networking Concepts 1. Introduction 2. Protocols 3. Protocol Layers 4. Network Interconnection/Internet.

Linear Bus, Star, Tree Network Diagramming Software Edraw Network Diagrammer is a new, rapid and powerful network design software for network drawings possessing diversified examples and templates. Network Diagram Software for Windows Mac Version Linux Version Network Protocol Overview The OSI model, and any other network communication model, provides only a conceptual framework for communication between computers, but the model itself does not provide specific methods of communication. Actual communication is defined by various communication protocols. In the context of data communication, a protocol is a formal set of rules, conventions and data structure that governs how computers and other network devices exchange information over a network. In other words, a protocol is a standard procedure and format that two data communication devices must understand, accept and use to be able to talk to each other. In modern protocol design, protocols are "layered" according to the OSI 7 layer model or a similar layered model. Layering is a design principle which divides the protocol design into a number of smaller parts, each part accomplishing a particular sub-task and interacting with the other parts of the protocol only in a small number of well-defined ways. Layering allows the parts of a protocol to be designed and tested without a combinatorial explosion of cases, keeping each design relatively simple. Layering also permits familiar protocols to be adapted to unusual circumstances. Detailed rules and procedures of a protocol or protocol group are often defined by a lengthy document. A wide variety of communication protocols exists. These protocols were defined by many different standard organizations throughout the world and by technology vendors over years of technology evolution and development. The IP, the Internet Protocol, is responsible for exchanging information between routers so that the routers can select the proper path for network traffic, while TCP is responsible for ensuring the data packets are transmitted across the network reliably and error free. The LAN protocols suite is for the physical and data link layers of communications over various LAN media such as Ethernet wires and wireless radio waves. The WAN protocol suite is for the lowest three layers and defines communication over various wide-area media, such as fiber optic and copper cables. Network communication has slowly evolved. Because of this, the protocols which define the network communication are highly inter-related. Many protocols rely on others for operation. For example, many routing protocols use other network protocols to exchange information between routers. In addition to standards for individual protocols in transmission, there are now also interface standards for different layers to talk to the ones above or below usually operating system specific. The protocols for data communication cover all areas as defined in the OSI model. However, the OSI model is only loosely defined. A protocol may perform the functions of one or more of the OSI layers, which introduces complexity to understanding protocols relevant to the OSI 7 layer model. In real-world protocols, there is some argument as to where the distinctions between layers are drawn; there is no one black and white answer. To develop a complete technology that is useful for the industry, very often a group of protocols is required in the same layer or across many different layers. Different protocols often describe different aspects of a single communication; taken together, these form a protocol suite. Protocols can be implemented either in hardware or software or a mixture of both. Typically, the lower layers are implemented in hardware, with the higher layers being implemented in software. Protocols could be grouped into suites or families, or stacks by their technical functions, or origin of the protocol introduction, or both. A protocol may belong to one or multiple protocol suites, depending on how you categorize it. ISO has its own suite of protocols for internetworking communications, which is mainly deployed in European countries.