DOWNLOAD PDF DATA NETWORKS, IP AND THE INTERNET

Chapter 1 : What is the Operation of TCP and IP in data communication networks? | Winstudent

IP (Internet protocol) is the central pillar of the Internet and was designed primarily for internetworking as being a simple protocol almost any network could carry. The business world appears to increasingly revolve around data communications and the Internet and all modern data networks are based around either the Internet or at least around.

Some sort of network access protocol, such as the Ethernet logic, is used to connect a computer to a subnetwork. This protocol enables the host to send data across the subnetwork to another host or, if the target host is on another subnetwork, to a router that will forward the data. IP is implemented in all of the end systems and the routers. It acts as a relay to move a block of data from one host, through one or more routers, to another host. TCP is implemented only in the end systems; it keeps track of the blocks of data to assure that all are delivered reliably to the appropriate application. For successful communication, every entity in the overall system must have a unique address. Actually, two levels of addressing are needed. Each host on a subnetwork must have a unique global internet address; this allows the data to be delivered to the proper host. Each process with a host must have an address that is unique within the host; this allows the host-to-host protocol TCP to deliver data to the proper process. These latter addresses are known as ports. Let us trace a simple operation. Suppose that a process, associated with port 3 at host A, wishes to send a message to another process, associated with port 2 at host B. Note that IP need not be told the identity of the destination port. All it needs to know is that the data are intended for host B. Next, IP hands the message down to the network access layer e. To control this operation, control information as well as user data must be transmitted, as suggested in Figure 2. Let us say that the sending process generates a block of data and passes this to TCP. TCP may break this block into smaller pieces to make it more manageable. The control information is to be used by the peer TCP protocol entity at host B. Examples of items in this header include. When the TCP entity at B receives the segment, it must know to whom the data are to be delivered. TCP numbers the segments that it sends to a particular destination port sequentially, so that if they arrive out of order, the TCP entity at B can reorder them. The sending TCP includes a code that is a function of the contents of the remainder of the segment. The receiving TCP performs the same calculation and compares the result with the incoming code. A discrepancy results if there has been some error in transmission. These segments must be transmitted across one or more subnetworks and relayed through one or more intermediate routers. This operation, too, requires the use of control information. Thus IP appends a header of control information to each segment to form an IP datagram. An example of an item stored in the IP header is the destination host address in this example, B. Finally, each IP datagram is presented to the network access layer for transmission across the first subnetwork in its journey to the destination. The network access layer appends its own header, creating a packet, or frame. The packet is transmitted across the subnetwork to router J. The packet header contains the information that the subnetwork needs to transfer the data across the subnetwork. Examples of items that may be contained in this header include: The subnetwork must know to which attached device the packet is to be delivered. The network access protocol might request the use of certain subnetwork facilities, such as priority. At router J, the packet header is stripped off and the IP header examined. On the basis of the destination address information in the IP header, the IP module in the router directs the datagram out across subnetwork 2 to B. To do this, the datagram is again augmented with a network access header. When the data are received at B, the reverse process occurs. TCP provides a reliable connection for the transfer of data between applications. A connection is simply a temporary logical association between two entities in different systems. A logical connection refers to a given pair of port values. For the duration of the connection each entity keeps track of TCP segments coming and going to the other entity, in order to regulate the flow of segments and to recover from lost or damaged segments. The Sequence Number, Acknowledgment Number, and Window fields provide flow control and error control. The checksum is a bit frame check sequence used to detect errors in the TCP segment. Chapter 20 provides more details. UDP enables a procedure to send messages to other procedures with a minimum of protocol mechanism. Because it is connectionless, UDP has very little to do. Essentially, it adds a port addressing capability to IP. This is best seen by examining the UDP header, shown in Figure 2.

UDP also includes a checksum to verify that no error occurs in the data; the use of the checksum is optional. The header includes bit source and destination addresses. The Header Checksum field is used to detect errors in the header to avoid misdelivery. The Protocol field indicates which higher-layer protocol is using IP. Chapter 18 provides more detail. This specification was turned into a standard in known as IPv6. But the driving force behind the development of the new protocol was the need for more addresses. The current IP uses a bit address to specify a source or destination. With the explosive growth of the Internet and of private networks attached to the Internet, this address length became insufficient to accommodate all systems needing addresses.

Chapter 2 : How do computers connect to each other over the Internet?

An IP Packet is a packet of data which carries a data load and an IP header. Any piece of data (TCP packets, in the case of a TCP/IP network) is broken into bits and placed into these packets and transmitted over the network.

Terrestrial microwaves are in the low gigahertz range, which limits all communications to line-of-sight. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals. Cellular and PCS systems use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. Free-space optical communication uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices. Exotic technologies[edit] There have been various attempts at transporting data over exotic media: It was implemented in real life in Node networking Apart from any physical transmission media there may be, networks comprise additional basic system building blocks, such as network interface controllers NICs , repeaters , hubs , bridges , switches , routers , modems , and firewalls. Any particular piece of equipment will frequently contain multiple building blocks and perform multiple functions. Network interfaces[edit] An ATM network interface in the form of an accessory card. A lot of network interfaces are built-in. A network interface controller NIC is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information. For example, the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce. Repeaters and hubs[edit] A repeater is an electronic device that receives a network signal , cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart. A repeater with multiple ports is known as an Ethernet hub. Repeaters work on the physical layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance and may affect proper function. As a result, many network architectures limit the number of repeaters that can be used in a row, e. Hubs and repeaters in LANs have been mostly obsoleted by modern switches. Bridges[edit] A network bridge connects and filters traffic between two network segments at the data link layer layer 2 of the OSI model to form a single network. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks. Bridges come in three basic types: Directly connect LANs Remote bridges: Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers. Switches[edit] A network switch is a device that forwards and filters OSI layer 2 datagrams frames between ports based on the destination MAC address in each frame. It can be thought of as a multi-port bridge. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches. Routers[edit] A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram Internet protocol information from layer 3. The routing information is often processed in conjunction with the routing table or forwarding table. A router uses its routing table to determine where to forward packets. A destination in a routing table can include a "null" interface, also known as the "black hole" interface because data can go into it, however, no further processing is done for said data, i. Modems[edit] Modems MOdulator-DEModulator are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by

the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology. Firewalls[edit] A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks. Network structure[edit] Network topology is the layout or organizational hierarchy of interconnected nodes of a computer network. Different network topologies can affect throughput, but reliability is often more critical. With many technologies, such as bus networks, a single failure can cause the network to fail entirely. In general the more interconnections there are, the more robust the network is; but the more expensive it is to install. Common network topologies Common layouts are: This is still a common topology on the data link layer , although modern physical layer variants use point-to-point links instead. This is the typical layout found in a Wireless LAN , where each wireless client connects to the central Wireless access point. A fully connected network: Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI , the network topology is a ring actually two counter-rotating rings , but the physical topology is often a star, because all neighboring connections can be routed via a central physical location. Overlay network[edit] A sample overlay network An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay network are connected by virtual or logical links. Each link corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may and often does differ from that of the underlying one. For example, many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet. The most striking example of an overlay network is the Internet itself. The Internet itself was initially built as an overlay on the telephone network. Address resolution and routing are the means that allow mapping of a fully connected IP overlay network to its underlying network. Another example of an overlay network is a distributed hash table , which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table actually a map indexed by keys. Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ , DiffServ , and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. The overlay network has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes that a message traverses before it reaches its destination. For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery a kind of multicast. Academic research includes end system multicast, [20] resilient routing and quality of service studies, among others. Message flows A-B in the presence of a router R , red flows are effective communication paths, black paths are across the actual network links. A communication protocol is a set of rules for exchanging information over a network. In a protocol stack also see the OSI model , each protocol leverages the services of the protocol layer below it, until the lowest layer controls the hardware which sends information across the media. The use of protocol layering is today ubiquitous across the field of computer networking. Communication protocols have various characteristics. They may be connection-oriented or connectionless , they may use circuit mode or packet switching , and they may use hierarchical addressing or flat addressing. There are many communication protocols, a few of which are described below. The complete IEEE protocol suite provides a diverse set of networking capabilities. The protocols have a flat addressing scheme. They operate mostly at levels 1 and 2 of the OSI model. It is standardized by IEEE It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by data-gram transmission at the Internet protocol IP level. At its core, the protocol suite defines the addressing, identification, and routing specifications for Internet Protocol Version 4 IPv4 and for IPv6, the next generation of the protocol with a much enlarged addressing capability. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM Pulse-Code Modulation format. It uses asynchronous time-division multiplexing and encodes

data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. While the role of ATM is diminishing in favor of next-generation networks , it still plays a role in the last mile , which is the connection between an Internet service provider and the home user.

Chapter 3 : How Information Travels on the Internet | HowStuffWorks

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

Function[edit] Sample encapsulation of application data from UDP to a Link protocol frame The Internet Protocol is responsible for addressing hosts, encapsulating data into datagrams including fragmentation and reassembly and routing datagrams from a source host to a destination host across one or more IP networks. Each datagram has two components: The IP header includes source IP address, destination IP address, and other metadata needed to route and deliver the datagram. The payload is the data that is transported. This method of nesting the data payload in a packet with a header is called encapsulation. IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into subnetworks , involving the designation of network prefixes. IP routing is performed by all hosts, as well as routers , whose main function is to transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols , either interior gateway protocols or exterior gateway protocols , as needed for the topology of the network. A central control component of this model was the "Transmission Control Program" that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the Transmission Control Protocol and User Datagram Protocol at the transport layer and the Internet Protocol at the network layer. IP versions 0 to 3 were experimental versions, used between and It proposes the first version of the IP header, using 0 for the version field. The IP header is different from the modern IPv4 header. The dominant internetworking protocol in the Internet Layer in use today is IPv4 ; the number 4 is the protocol version number carried in every IP datagram. Version 5 was used by the Internet Stream Protocol , an experimental streaming protocol. The successor to IPv4 is IPv6. Its most prominent difference from version 4 is the size of the addresses. While IPv4 uses 32 bits for addressing, yielding c. Although adoption of IPv6 has been slow, as of June [update] , all United States government systems have demonstrated basic infrastructure support for IPv6. Under the end-to-end principle, the network infrastructure is considered inherently unreliable at any single network element or transmission medium and is dynamic in terms of availability of links and nodes. No central monitoring or performance measurement facility exists that tracks or maintains the state of the network. For the benefit of reducing network complexity , the intelligence in the network is purposely located in the end nodes. As a consequence of this design, the Internet Protocol only provides best-effort delivery and its service is characterized as unreliable. In network architectural language, it is a connectionless protocol , in contrast to connection-oriented communication. Various error conditions may occur, such as data corruption , packet loss and duplication. Because routing is dynamic, meaning every packet is treated independently, and because the network maintains no state based on the path of prior packets, different packets may be routed to the same destination via different paths, resulting in out-of-order delivery to the receiver. All error conditions in the network must be detected and compensated by the participating end nodes. The upper layer protocols of the Internet protocol suite are responsible for resolving reliability issues. For example, a host may buffer network data to ensure correct ordering before the data is delivered to an application. IPv4 provides safeguards to ensure that the IP packet header is error-free. A routing node calculates a checksum for a packet. If the checksum is bad, the routing node discards the packet. Although the Internet Control Message Protocol ICMP allows such notification, the routing node is not required to notify either end node of these errors. By contrast, in order to increase performance, and since current link layer technology is assumed to provide sufficient error detection, [8] the IPv6 header has no checksum to protect it. One of the technical constraints is the size of data packets allowed on a given link. Facilities exist to examine the maximum transmission unit MTU size of the local link and Path MTU Discovery can be used for the entire intended path to the destination. The IPv4 internetworking layer has the ability to automatically fragment the original datagram into smaller units for transmission. In this case, IP provides re-ordering of fragments delivered out of order. Consequently, many Internet protocols exhibited

vulnerabilities highlighted by network attacks and later security assessments. In , a thorough security assessment and proposed mitigation of problems was published.

Chapter 4 : Internet communication | Axis Communications

IP(Internet protocol) is the central pillar of the Internet and wasdesigned primarily for internetworking as being a simple protocolalmost any network could racedaydvl.com business world appears to increasingly revolve around datacommunications and the Internet and all modern data networks arebased around either the Internet or at least around IP.

The T-Score web application â€" Web form and data processing We will get slightly more precise and technical in the next section , for now let us address some elementary concepts. The number of the packets depends on the size of the data. For simplicity, let us think about the transmission of a text file. Wikipedia If we picture a file as a train, the packets would be the individual wagons. Each packet is like an envelope sent by normal mail, with the actual data, part of the original file, inside. We could summarize the journey of a file such as an e-mail message or a web page, from computer A to computer B, as follows. As we mentioned, communication paths most often constituted by physical wires between computer A and computer F Figure on the Internet are often redundant. Physically, on the hardware level, there relays are constituted by Routers. As the name implies, routers allow packets to find the best route between two computers that do not belong to the same network. Data are generally relayed through several such routers before they reach their final destination. The crucial thing to understand here, is that at any given time we re talking about milliseconds , the best route between 2 computers may change. Routers are able to determine, at the moment of sending a particular packet, the best route at this time. When sending the next packet, the best route may be different. Therefore, each packet from the same file could take a different route in order to reach the intended destination. The dialogue will end when all the packets have reached the destination. Although this packet organization might seem complex, it has a number of advantages, with respect to an hypothetical model based on sending entire unfragmented files. Bandwidth is limited, so this would be highly inefficient and would clutter the network. With packets, if something goes wrong with a packet, you just have to re-send this packet, not the whole file. The bandwidth is finite imagine you only have one rail. In order to send a small one packet file a one wagon train , you have to wait until the big file a 20 wagon train for example has passed. If you fragment the 20 wagon train into the individual packets, and send one at a time, then the one packet train has a fair chance to go through together with the packets of the 20 wagons train. As it works now, you can download your e-mail 50K while you download this big video file GB. This discussion is closely related to the concept of net neutrality. In a condition of neutrality, all packets are equal, and have the same privileges and the same speed of transmission. In a non-neutral situation, a provider might, for example, limit the bandwidth or make this bandwidth more expensive , for certain kind of packets, for example those related to peer to peer traffic file exchange between users , or maybe those related to VoIP traffic, for commercial or other purposes.

Chapter 5 : Named Data Networking (NDN) - A Future Internet Architecture

An IP network is a communication network that uses Internet Protocol (IP) to send and receive messages between one or more computers. As one of the most commonly used global networks, an IP network is implemented in Internet networks, local area networks (LAN) and enterprise networks.

This need led to the development of IP addressing and the many IP-based protocols for communicating over the Internet, which is a global system of interconnected computer networks. Before IP addressing is discussed, some of the basic elements of Internet communication such as routers, firewalls and Internet service providers are covered below. A router routes information from one network to another based on IP addresses. It forwards only data packages that are to be sent to another network. A router is most commonly used for connecting a local network to the Internet. Traditionally, routers were referred to as gateways. Firewalls A firewall is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks that are connected to the Internet. Messages entering or leaving the Internet pass through the firewall, which examines each message, and blocks those that do not meet the specified security criteria. When connecting to the Internet, terms such as upstream and downstream are used. Upstream describes the transfer rate with which data can be uploaded from the device to the Internet; for instance, when video is sent from a network camera. Downstream is the transfer speed for downloading files; for instance, when video is received by a monitoring PC. In most scenarios â€" for example, a laptop that is connected to the Internet â€" downloading information from the Internet is the most important speed to consider. In a network video application with a network camera at a remote site, the upstream speed is more relevant since data video from the network camera will be uploaded to the Internet. IP addressing Any device that wants to communicate with other devices via the Internet must have a unique and appropriate IP address. IP addresses are used to identify the sending and receiving devices. There are currently two IP versions: The main difference between the two is that the length of an IPv6 address is longer bits compared with 32 bits for an IPv4 address. IPv4 addresses are most commonly used today. IPv4 addresses IPv4 addresses are grouped into four blocks, and each block is separated by a dot. Each block represents a number between 0 and ; for example, Certain blocks of IPv4 addresses have been reserved exclusively for private use. These private IP addresses are Such addresses can only be used on private networks and are not allowed to be forwarded through a router to the Internet. All devices that want to communicate over the Internet must have its own individual, public IP address. A public IP address is an address allocated by an Internet service provider. An ISP can allocate either a dynamic IP address, which can change during a session, or a static address, which normally comes with a monthly fee. Ports A port number defines a particular service or application so that the receiving server e. Port numbers can range from 0 to For example, a web service via HTTP is typically mapped to port 80 on a network camera. Setting an IPv4 address for an Axis network video product can be done mainly in two ways: Using a dynamic IP address means that the IP address for a network device may change from day to day. With dynamic IP addresses, it is recommended that users register a domain name e. The network video product can then update a dynamic DNS server with its current IP address so that users can access the product using a domain name. The software can also be used to assign static, private IP addresses for Axis network video products. This is recommended when using video management software to access network video products. In a network video system with potentially hundreds of cameras, a software program such as AXIS Camera Management is necessary in order to effectively manage the system. This is a process called port forwarding. Port forwarding works as follows. The router is configured to forward any data coming into a predefined port number to a specific device on the private network side of the router. To a receiving client, it looks like the packets originated from the router. The reverse happens with outgoing data packets. Thanks to port forwarding in the router, network cameras with private IP addresses on a local network can be accessed over the Internet. In this illustration, the router knows to forward data request coming into port to a network camera with a private IP address of The network camera can then begin to send video.

Port forwarding is traditionally done by first configuring the router. Different routers have different ways of doing port forwarding and there are web sites such as www. To make the task of port forwarding easier, Axis offers the NAT traversal feature in many of its network video products. If a router is not manually specified, then the network video product will automatically search for NAT routers on the network and select the default router. In addition, the service will automatically select an HTTP port if none is manually entered. Axis network video products enable port forwarding to be set using NAT traversal. IPv6 addresses An IPv6 address is written in hexadecimal notation with colons subdividing the address into eight blocks of 16 bits each; for example, The major advantages of IPv6, apart from the availability of a huge number of IP addresses, include enabling a device to automatically configure its IP address using its MAC address. For communication over the Internet, the host requests and receives from the router the necessary prefix of the public address block and additional information. Port forwarding is also no longer needed. Other benefits of IPv6 include renumbering to simplify switching entire corporate networks between providers, faster routing, point-to-point encryption according to IPSec, and connectivity using the same address in changing networks Mobile IPv6. An IPv6 address is enclosed in square brackets in a URL and a specific port can be addressed in the following way: The product will then receive an IPv6 address according to the configuration in the network router. These transport protocols act as carriers for many other protocols. TCP provides a reliable, connection-based transmission channel. It handles the process of breaking large chunks of data into smaller packets and ensures that data sent from one end is received on the other. In general, TCP is used when reliable communication is preferred over transport latency. UDP is a connectionless protocol and does not guarantee the delivery of data sent, thus leaving the whole control mechanism and error-checking to the application itself. UDP provides no transmissions of lost data and, therefore, does not introduce further delays.

Chapter 6 : What is virtual private networks and IP security in data communication networks? | Winstudent

This is because data sent over the Internet (and most computer networks) are sent in manageable chunks. On the Internet, these chunks of data are known as packets. The packets would go through the Application Layer and continue to the TCP layer.

What is virtual private networks and IP security in data communication networks? Essentially, a VPN consists of a set of computers that are interconnected through a relatively insecure network and provide security using encryption and special protocols. At each company site, workstations, servers, and databases are linked by one or more local area networks LANs. The LAN is under the control of the network manager and can be configured and tuned to cost-effective performance. The Internet or some other public network may be used to interconnect sites, providing cost savings over using a private network and offloading WAN management tasks to public network providers. The same public network provides remote workers and other mobile workers access to the enterprise system from a remote site. But the manager faces a basic requirement: Using a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. In order to solve this problem, managers can choose from a variety of encryption and authentication packages and products. Proprietary solutions present many problems. First, how secure is the solution? If a proprietary encryption or authentication scheme is used, the level of security provided may be scarcely ensured in the technical literature. The second is the compatibility issue. No administrator wants to restrict the selection of workstations, servers, routers, firewalls, etc. The report points to a general consensus that the Internet requires more and better security and identifies key areas of security mechanisms. Including the need to protect the network infrastructure from unauthorized network traffic monitoring and control, and the need to use end-user authentication and encryption mechanisms to protect end-user traffic. To provide security, the IAB includes authentication and encryption as a necessary security feature in the next generation of IP that is released as IPv6. Fortunately, these security features are designed to work with both current IPv4 and future IPv6. This means that vendors can now begin to provide these capabilities, and many vendors now have some IPSec capabilities in their products. The IPSec specification now exists as a set of Internet standards. Examples of their use include the following: Companies can establish secure virtual private networks over the Internet or the public WAN. This makes the enterprise heavily dependent on the Internet and reduce its demand for private networks, cost savings and network management overhead. End users with IP security protocols can make local calls to Internet service providers ISPs and gain secure access to corporate networks. This reduces the tolls of traveling employees and telecommuters. IPSec can be used to protect communications with other organizations, ensure authentication and confidentiality, and provide key exchange mechanisms. While some network and e-business applications have built-in security protocols, they use IPSec to enhance security. IPSec ensures that all traffic specified by the network administrator is encrypted and authenticated, adding an additional layer of security to any content provided by the application layer. Organizations maintain LANs in decentralized locations. These protocols operate in network devices such as routers or firewalls that connect each LAN to the outside world. It is also possible to securely transfer a single user to a WAN. This user station must implement the IPSec protocol to provide security. Traffic within a company or workgroup does not incur security-related processing overhead. When IPSec is implemented in a firewall or router, there is no need to change the software on the user or server system. Even if IPSec is implemented in the end system, upper-level software including applications is not affected. There is no need to train users on security mechanisms, publish keying material on a per-user basis, or revoke keying material when users leave the organization. This is useful for offsite workers and for setting up secure virtual subnetworks for sensitive applications within an organization. Authentication and encryption are often required for VPNs because it is important to 1 ensure that unauthorized users do not penetrate the virtual private network and 2 ensure that eavesdroppers on the Internet can not read messages sent over the virtual private network. The key exchange feature allows manual exchange of keys and automatic schemes.

Chapter 7 : Computer network - Wikipedia

Some transaction-oriented applications make use of UDP; one example is SNMP (Simple Network Management Protocol), the standard network management protocol for TCP/IP networks. Because it is connectionless, UDP has very little to do.

The T-Score web application â€" Web form and data processing Dozens of different PC brands are available and around. More importantly, many different operating systems are available and installed on the various computers. The client-server paradigm â€" Source: Still, we can find all these operating systems both on clients and on servers, although with different shares. Desktop operating systems market share in April Usage share of operating system on client computers, as estimated by analysis on wikimedia traffic â€" â€" Source: Wikipedia It is fascinating to witness the moment, around August , in which operating systems for mobile phones Android and iOS overtake Windows 7, used on desktop computers, as assessed by the user agents of devices visiting the Wikipedia website. Operating systems of devices visiting the Wikipedia website from April to April Wikimedia Server operating systems A typical server rack. According to a recent survey by W3Techs , Linux jumps from the 1. MacOS, which is not in the server business anymore, is estimated to be at less than 0. MacOS, at less than 0. With respect to the web server software itself rather than the OS used on web server computers, W3Techs provides the following data. Web server software, May W3Techs This somewhat long overview underscores the variability of operating systems used on clients and server computers. How can such deeply diverse systems communicate and smoothly exchange data on the Internet? After all, it is common knowledge that a Windows. The answer to this question is that both Macs and PCs and Linux and all other OS used on computers and the wealth of other devices connected to the Internet nowadays use a common language, a common set of rigidly defined rules, to communicate over the internet. The transport layer manages, among other things, the fragmentation of the files it receives from the application layer into packets, that are then passed to the Internet layer, and the remounting of packets received from the Internet layer see Figures and , to yield files that are passed to the application layer. The file is then passed down to the Transport layer for the fragmentation in packets. The physical layer is where the packets physically move, by using ethernet cables, satellites, fibers, wireless systems, depending on what is available between computer A and B. If the computers are in the same room, they might connect through a couple of ethernet cables with a router in between, or maybe wirelessly, if the computer are connected via wireless to the same router. The packet, thanks to the routers, will find the correct route from A to B. It is worth reminding that not all packets will take the same route, as at any given time a particular route among the various available connections on the Internet are redundant, remember? A moment later, maybe when the next packet is sent, this might change and the best route will be different. In computer B, packets will travel up from the physical layer, to the Internet layer and then to the transport layer that re-assembles the packets into the original file, the e-mail that was sent from computer A. This is of course a simplified scheme where quite a few details were intentionally omitted did we mention there must be a mail server in between A and B for instance?

Chapter 8 : Data transmission on the Internet â€“ Bioinformatics Web Development

â€¢ Secure remote access through the Internet: End users with IP security protocols can make local calls to Internet service providers (ISPs) and gain secure access to corporate networks. This reduces the tolls of traveling employees and telecommuters.

Chapter 9 : VPN services The ultimate guide to protecting your data on the internet | ZDNet

Wide-Area Network (WAN) - A wide-area network covers a large geographic area and typically consists of multiple computer networks. The Internet is a type of WAN that relies on a large global network of service providers that use routers, switches, modems, and servers to provide connectivity to workers and organizations around the globe.