Computer networks case study assignment

| | ROAMWARE “ CASE STUDY” Presented By:- Name: – ROLL NO. PRASAD B. DHAVADE. 10 SUMIT V. TIRLOTKAR. 56 Case study submitted in Second year for the degree of BACHELOR OF SCIENCE Branch: INFORMATION TECHNOLOGY Of University of Mumbai [pic] UNIVERSITY DEPARTMENT OF INFORMATION TECHNOLOGY UNIVERSITY OF MUMBAI VIDYANAGARI, SANTACRUZ (E), MUMBAI-400 098. ROAMWARE “ CASE STUDY” Bonafide Record of work done by

Name: – ROLL NO. PRASAD B. DHAVADE. 10 SUMIT V. TIRLOTKAR. 56 Case study submitted in Second year for the degree of BACHELOR OF SCIENCE Branch: INFORMATION TECHNOLOGY Of University of Mumbai August 2009 ……. Mr. NIKHIL PAWANIKAR. -Faculty Guide CONTENTS CHAPTER PAGE NO. COMPANY VISION…… 4 AWARDS…… 5-6 1. INTRODUCTION…… 1. 1 Views of Networks 7-8 1. 2 History of Computer Networks 9-10 2. NETWOK CLASSIFICATION…… 11 2. 1 Connection method 11-13 2. 2 Scale14 3. OSI REFERENCE MODEL…… 15-19 4. TYPES OF NETWORKS…… 20-25 5.

ROAMWARE’S NETWORK LAYOUT…… 26-27 6. NETWOK TOPOLOGY…… 28-31 7. BASIC HARDWARE COMPONENTS…… 31-34 8. COMPARISON WITH TCP/IP…… 35 9. FIREWALL…… 36-37 10. CONCLUSION…… 38 BIBLIOGRAPHY…… 39 Company Vision

Roamware Inc. is the leading provider of voice and data roaming solutions that enhance the roaming experience for users in more than 140 countries worldwide.

Roamware’s suite of solutions is the result of continuous and insightful innovation and has helped over 377 mobile operators manage their roaming business in tune with the varied trends in the global mobile roaming industry. With over 180 patent submissions and awards in the domain, Roamware’s thought leadership has led to the introduction of products and services that have resulted in quantum shifts in the roaming landscape. In 2007, Roamware introduced a highly acclaimed suite of digital media services that are designed to help operators leverage investments in data-centric infrastructure and applications.

This has broadened the scope, reach and value that operators can realize from their relationship with Roamware. Roamware’s product portfolio consists of over 30 solutions across the GSM and CDMA domains that are built on the Roamware Service Delivery System (SDS). The Roamware SDS facilitates seamless deployment and integration of applications and services with a mobile operator’s network operational and IT infrastructure. Roamware’s leadership in innovation and track record of success has been widely recognized in the industry.

The company has won several accolades, including being named to the global Red Herring 100 list as one of the Top 100 Private Companies in the world in 2007 and the Inc. 5000 list for 2008 that recognizes the fastest growing companies in America. Founded in 2002, Roamware is

headquartered in San Jose, California, with research and development, sales and support offices across the world. Awards Roamware’s voice and data roaming solutions are installed in over 365 mobile operators’ networks across 136 countries and generate incremental revenues for mobile operators, whilst increasing their operational efficiencies and reduce subscriber churn.

Roamware’s solutions are built on the Roamware Service Delivery System (SDS), a carrier-grade platform based on open standards that enable seamless integration of multiple applications. 2008 [pic] |[pic] | | | | | | | | Inc. 000 | | | 2008 Fastest growing companies in America | | | | | | |[pic] | | | | | Deloitte | | 2008 Technology Fast 50 winner for the Silicon Valley region | | | | | | | | | 2007 | |[pic] | | | |[pic] | | | | | Deloitte | | 2007 Technology Fast 50 winner for the Silicon Valley region | | | | | | | | |[pic] | | | | | Red Herring | | Top 100 Global Award winner | | | | | | | | | | | | |[pic] | | | | Red Herring | | 100 most promising private North American technology companies. | | | | | | | 2006 | |[pic] | | | |[pic] | | | | | Deloitte | | 2006 Technology Fast 500 Award n the technology, media, telecom and life sciences companies in North America | | | | | | | |[pic] | | | | | Frost & Sullivan | | 2006 Technology Innovation Award for providing roaming solutions in over 100 countries | | | | | | | | | |[pic] | | | | | Deloitte | | 2006 Technology Fast 50 Award in the Internet, Media & Entertainment, and Communication category | | | | | | |[pic] | | | | | GSMA Awards | | Nominated for the ‘ Best Roaming Product or Service’ | | | | | 1. Introduction The network allows computers to communicate with each other and share resources and information. The Advanced Research Projects Agency (ARPA)

designed “ Advanced Research Projects Agency Network” (ARPANET) for the United States Department of Defense. It was the first computer network in the world in late 1960s and early 1970s. 1. 1 Views of Networks Users and network administrators often have different views of their networks.

Often, users who share printers and some servers form a workgroup, which usually means they are in the same geographic location and are on the same LAN. A community of interest has less of a connotation of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies. Network administrators see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e. g. , routers, bridges and application layer gateways that interconnect the physical media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more physical media.

For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology. Both users and administrators will be aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e. g. employees). Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e. g. business partners, customers).

Informally, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering standpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reach ability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS). Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications.

Especially when money or sensitive information is exchanged, the communications are apt to be secured by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users, using secure Virtual Private Network (VPN) technology. 1. 2 History of Computer Networks Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. Many of the social behavior seen in today’s Internet was demonstrably present in nineteenth-century telegraph networks, and arguably in even earlier networks using visual signals.

In September 1940 George Stibitz used a teletype machine to send instructions for a problem set from his Model K at Dartmouth College in New Hampshire to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypes to

computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J. C. R. Licklider was hired and developed a working group he called the “ Intergalactic Network”, a precursor to the ARPANet. In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at MIT, a research group supported by General Electric and Bell Labs used a computer (DEC’s PDP-8) to route and manage telephone connections. Throughout the 1960s Leonard Kleinrock, Paul Baran and Donald Davies ndependently conceptualized and developed network systems which used datagram or packets that could be used in a packet switched network between computer systems. 1965 Thomas Merrill and Lawrence G. Roberts created the first wide area network (WAN). The first widely used PSTN switch that used true computer control was the Western Electric 1ESS switch, introduced in 1965. In 1969 the University of California at Los Angeles, SRI (in Stanford), University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANet network using 50 kbit/s circuits. Commercial services using X. 25 were deployed in 1972, and later used as an underlying infrastructure for expanding TCP/IP networks.

Computer networks and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries. This expansion is mirrored by growth in the numbers and types of users of networks from the researcher to the home user. Today, computer networks are the core of modern communication. For example, all modern aspects of the Public Switched Telephone Network (PSTN) are computer-controlled, and telephony

increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased significantly in the past decade and this boom in communications would not have been possible without the progressively advancing computer network. . Network Classification The following list presents categories used for classifying networks. 2. 1 Connection Method Computer networks can also be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as Optical fiber, Ethernet, Wireless LAN, HomePNA, Power line communication or G. hn. Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges and/or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium. ITU-T G. n technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network. Wired Technologies Twisted-Pair Wire – This is the most widely used medium for telecommunication. Twisted-pair wires are ordinary telephone wires which consist of two insulated copper wires twisted into pairs and are used for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed range from 2 million bits per second to 100 million bits per second. Coaxial Cable – These cables are widely used for cable television systems, office buildings, and other worksites for local area networks.

The cables consist of copper or aluminum wire wrapped with insulating layer typically of a flexible material with a high dielectric constant, all of which are

surrounded by a conductive layer. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second. Fiber Optics – These cables consist of one or more thin filaments of glass fiber wrapped in a protective layer. It transmits light which can travel over long distance and higher bandwidths. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed could go up to as high as trillions of bits per second.

The speed of fiber optics is hundreds of times faster than coaxial cables and thousands of times faster than twisted-pair wire. Wireless Technologies Terrestrial Microwave – Terrestrial microwaves use Earth-based transmitter and receiver. The equipment looks similar to satellite dishes. Terrestrial microwaves use low-gigahertz range, which limits all communications to line-of-sight. Path between relay stations spaced approx. 30 miles apart. Microwave antennas are usually placed on top of buildings, towers, hills, and mountain peaks. Communications Satellites – The satellites use microwave radio as their telecommunications medium which are not deflected by the Earth’s atmosphere. The satellites are stationed in space, typically 22, 000 miles above the equator.

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 are divided to different geographic area. Each area has low-power transmitter or radio relay antenna device to relay calls from one area to the next area. Wireless LANs – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANS use spread

spectrum technology to enable communication between multiple devices in a limited area. Example of open-standard wireless radio-wave technology is IEEE 802. 11b. Bluetooth – A short range wireless technology.

Operate at approx. 1Mbps with range from 10 to 100 meters. Bluetooth is an open wireless protocol for data exchange over short distances. The Wireless Web – The wireless web refers to the use of the World Wide Web through equipments like cellular phones, pagers, PDAs, and other portable communications devices. The wireless web service offers anytime/anywhere connection. 2. 2 Scale Networks are often classified as Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Personal Area Network (PAN), Virtual Private Network (VPN), Campus Area Network (CAN), Storage Area Network (SAN), etc. depending on their scale, scope and purpose.

Usage, trust levels and access rights often differ between these types of network – for example, LANs tend to be designed for internal use by an organization’s internal systems and employees in individual physical locations (such as a building), while WANs may connect physically separate parts of an organization to each other and may include connections to third parties. Functional relationship (network architecture) Computer networks may be classified according to the functional relationships which exist among the elements of the network, e. g. , Active Networking, Client-server and Peer-to-peer (workgroup) architecture. 3. OSI Reference Model Description of OSI layers OSI Model | | | Data unit | Layer | Function | | Host layers | Data | 7. Application | Network process to application | | | | 6. Presentation | Data representation and encryption | | | | 5. Session |

Interhost communication | | | | Segment | 4. Transport | End-to-end connections and reliability | | | Media layers | Packet | 3. Network | Path determination and logical addressing | | | | Frame | 2. Data Link | Physical addressing | | | | Bit | 1. Physical | Media, signal and binary transmission | | | Layer 1: Physical Layer:- The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium.

This includes the layout of pins, voltages, cable specifications, Hubs, repeaters, network adapters, Host Bus Adapters (HBAs used in Storage Area Networks) and more. To understand the function of the Physical Layer in contrast to the functions of the Data Link Layer, think of the Physical Layer as concerned primarily with the interaction of a single device with a medium, where the Data Link Layer is concerned more with the interactions of multiple devices (i. e. , at least two) with a shared medium. The Physical Layer will tell one device how to transmit to the medium, and another device how to receive from it (in most cases it does not tell the device how to connect to the medium). Standards such as RS-232 do use physical wires to control access to the medium.

The major functions and services performed by the Physical Layer are: • Establishment and termination of a connection to a communications medium. • Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control. • Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals

operating over the physical cabling (such as copper and optical fiber) or over a radio link. Parallel SCSI buses operate in this layer, although it must be remembered that the logical SCSI protocol is a Transport Layer protocol that runs over this bus.

Various Physical Layer Ethernet standards are also in this layer; Ethernet incorporates both this layer and the Data Link Layer. The same applies to other local-area networks, such as Token ring, FDDI, ITU-T G. hn and IEEE 802. 11, as well as personal area networks such as Bluetooth and IEEE 802. 15. 4. Layer 2: Data Link Layer:- The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system.

Local area network architecture, which included broadcast-capable multiaccess media, was developed independently of the ISO work, in IEEE Project 802. IEEE work assumed sublayering and management functions not required for WAN use. In modern practice, only error detection, not flow control using sliding window, is present in modern data link protocols such as Point-to-Point Protocol (PPP), and, on local area networks, the IEEE 802. 2 LLC layer is not used for most protocols on Ethernet, and, on other local area networks, its flow control and acknowledgment mechanisms are rarely used. Sliding window flow control and acknowledgment is used at the Transport Layer by protocols such as TCP, but is still used in niches where X. 25 offers performance advantages. The ITU-T G. n standard, which provides high-speed local area networking over existing wires (power lines, phone lines

and coaxial cables), includes a complete Data Link Layer which provides both error correction and flow control by means of a selective repeat Sliding Window Protocol. Both WAN and LAN services arrange bits, from the Physical Layer, into logical sequences called frames. Not all Physical Layer bits necessarily go into frames, as some of these bits are purely intended for Physical Layer functions. For example, every fifth bit of the FDDI bit stream is not used by the Layer. Layer 3: Network Layer:- The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer.

The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer—sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme – values are chosen by the network engineer. The addressing scheme is hierarchical. The best-known example of a Layer 3 protocol is the Internet Protocol (IP). It manages the connectionless transfer of data one hop at a time, from end system to ingress router, router to router, and from egress router to destination end system. It is not responsible for reliable delivery to a next hop, but only for the detection of errored packets so they may be discarded.

When the medium of the next hop cannot accept a packet in its current length, IP is responsible for fragmenting the packet into sufficiently small packets that the medium can accept. A number of layer management protocols, a function defined in the Management Annex, ISO 7498/4, belong to the Network Layer. These include routing protocols, multicast group

management, Network Layer information and error, and Network Layer address assignment. It is the function of the payload that makes these belong to the Network Layer, not the protocol that carries them. Layer 4: Transport Layer:- The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.

The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the Transport Layer can keep track of the segments and retransmit those that fail. Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the Transport Layer, typical examples of Layer 4 are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Of the actual OSI protocols, there are five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the least error recovery) to class 4 (TP4, designed for less reliable networks, similar to the Internet).

Class 0 contains no error recovery, and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the Session Layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries, both of which TCP is incapable. Detailed characteristics of TP0-4 classes are shown in the following table:[4] Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification

of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail.

Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, tunneling protocols operate at the Transport Layer, such as carrying non-IP protocols such as IBM’s SNA or Novell’s IPX over an IP network, or end-to-end encryption with IPsec. While Generic Routing Encapsulation (GRE) might seem to be a Network Layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. L2TP carries PPP frames inside transport packet. Layer 5: Session Layer:-

The Session Layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls. Layer 6: Presentation Layer:-

The Presentation Layer establishes a context between Application Layer entities, in which the higher-layer entities can use different syntax and

semantics, as long as the Presentation Service understands both and the mapping between them. The presentation service data units are then encapsulated into Session Protocol Data Units, and moved down the stack. This layer provides independence from differences in data representation (e. g. , encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer. The original presentation structure used the Basic Encoding Rules of Abstract Syntax Notation One (ASN.), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML. Layer 7: Application Layer:- The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed

by the application layer. Some examples of application layer implementations include Telnet, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). 4. Types of Networks

Below is a list of the most common types of computer networks in order of scale. Personal Area Network:- A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that are used in a PAN are printers, fax machines, telephones, PDAs and scanners. The reach of a PAN is typically about 20-30 feet (approximately 6-9 meters), but this is expected to increase with technology improvements. Local Area Network:- A local area network (LAN) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport.

Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G. hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines) For example, a library may have a wired or wireless LAN for users to interconnect local devices (e. g. , printers and servers) and to connect to the internet. On a wired LAN, PCs in the library are typically connected by category 5 (Cat5) cable, running the IEEE 802. 3 protocol through a system of interconnected devices and eventually connect to the Internet. The cables to the servers are typically on Cat 5e enhanced cable, which will support IEEE 802. 3 at 1 Gbit/s.

A wireless LAN may exist using a different IEEE protocol, 802. 11b, 802. 11g or possibly 802. 11n. The staff computers (bright green in the figure) can get to the color printer, checkout records, and the academic network and the Internet. All user computers can get to the Internet and the card catalog. Each workgroup can get to its local printer. Note that the printers are not accessible from outside their workgroup. [pic] Typical library network, in a branching tree topology and controlled access to resources All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors).

Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called “ layer 3 switches” because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks’ customer access routers. The defining characteristics of LANs, in contrast to WANs (wide area networks), include their higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines. Current Ethernet or other IEEE 802. 3 LAN technologies operate at speeds up to 10 Gbit/s. This is the data transfer rate.

IEEE has projects investigating the standardization of 40 and 100 Gbit/s. Campus Area Network:- A campus area network (CAN) is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area. It can be considered one form of a metropolitan area network, specific to an academic setting. In the case of a university campus-

based campus area network, the network is likely to link a variety of campus buildings including; academic departments, the university library and student residence halls. A campus area network is larger than a local area network but smaller than a wide area network (WAN) (in some cases).

The main aim of a campus area network is to facilitate students accessing internet and university resources. This is a network that connects two or more LANs but that is limited to a specific and contiguous geographical area such as a college campus, industrial complex, office building, or a military base. A CAN may be considered a type of MAN (metropolitan area network), but is generally limited to a smaller area than a typical MAN. This term is most often used to discuss the implementation of networks for a contiguous area. This should not be confused with a Controller Area Network. A LAN connects network devices over a relatively short distance.

A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. Metropolitan Area Network:- A metropolitan area network (MAN) is a network that connects two or more local area networks or campus area networks together but does not extend beyond the boundaries of the immediate town/city. Routers, switches and hubs are connected to create a metropolitan area network. Wide Area Network:- A wide area network (WAN) is a computer network that covers a broad area (i. e. any network whose communications links cross metropolitan, regional, or national boundaries [1]).

Less formally, a WAN is a network that uses routers and public communications links Contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs), which are usually limited to a room, building, campus or specific metropolitan area (e. g. , a city) respectively. The largest and most well-known example of a WAN is the Internet. A WAN is a data communications network that covers a relatively broad geographic area (i. e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. Global Area Network:- A global area networks (GAN) (see also IEEE 802. 0) specification is in development by several groups, and there is no common definition. In general, however, a GAN is a model for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is " handing off" the user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial WIRELESS local area networks (WLAN). [4] Virtual Private Network:- A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e. g. , the Internet) instead of by physical wires.

The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have

explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. A VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

A VPN allows computer users to appear to be editing from an IP address location other than the one which connects the actual computer to the Internet. Internetwork:- An Internetwork is the connection of two or more distinct computer networks or network segments via a common routing technology. The result is called an internetwork (often shortened to internet). Two or more networks or network segments connected using devices that operate at layer 3 (the ‘ network’ layer) of the OSI Basic Reference Model, such as a router. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork. In modern practice, interconnected networks use the Internet Protocol.

There are at least three variants of internetworks, depending on who administers and who participates in them: • Intranet • Extranet • Internet Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet is not considered to be a part of the intranet or extranet, although it may serve as a portal for access to portions of an extranet. Intranet:- An intranet is a set of networks, using the Internet Protocol and IP-based tools

such as web browsers and file transfer applications that are under the control of a single administrative entity.

That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information. Extranet:- An extranet is a network or internetwork that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities (e. g. , a company’s customers may be given access to some part of its intranet creating in this way an extranet, while at the same time the customers may not be considered ‘ trusted’ from a security standpoint).

Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network. Internet:- The Internet consists of a worldwide interconnection of governmental, academic, public, and private networks based upon the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the U. S. Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW). The ‘ Internet’ is most commonly spelled with a capital ‘ I’ as a proper noun, for historical reasons and to distinguish it from other generic internetworks.

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP Addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths. 6. Network Topology Computer networks may be classified according to the network topology upon which the network is based, such as bus network, star network, ring network, mesh network, star-bus network, tree or hierarchical topology network.

Network topology signifies the way in which devices in the network see their logical relations to one another. The use of the term “ logical” here is significant. That is, network topology is independent of the “ physical” layout of the network. Even if networked computers are physically placed in a linear arrangement, if they are connected via a hub, the network has a Star topology, rather than a bus topology. In this regard the visual and operational characteristics of a network are distinct; the logical network topology is not necessarily the same as the physical layout. Networks may be classified based on the method of data used to convey the data, these include digital and analog networks. Bus Network Topology:- [pic] Bus Network Topology

In local area networks where bus technology is used, each machine is connected to a single cable. Each computer or server is connected to the single bus cable through some kind of connector. A terminator is required at

each end of the bus cable to prevent the signal from bouncing back and forth on the bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the MAC address or IP address on the network that is the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data does match the machine address, the data is accepted.

Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable breaks, the entire network will be down, since there is only one cable. Since there is one cable, the transfer speeds between the computers on the network is faster. Star Network Topology:- [pic] Star Network Topology In local area networks where the star topology is used, each machine is connected to a central hub.

In contrast to the bus topology, the star topology allows each machine on the network to have a point to point connection to the central hub. All of the traffic which transverses the network passes through the central hub. The hub acts as a signal booster or repeater which in turn allows the signal to travel greater distances. As a result of each machine connecting directly to the hub, the star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding other machines. The primary disadvantage of the star topology is the hub is a single point of failure. If the hub were to fail the entire network would fail

as a result of the hub being connected to every machine on the network. Ring Network Topology:- pic] Ring Network Topology In local area networks where the ring topology is used, each computer is connected to the network in a closed loop or ring. Each machine or computer has a unique address that is used for identification purposes. The signal passes through each machine or computer connected to the ring in one direction. Ring topologies typically utilize a token passing scheme, used to control access to the network. By utilizing this scheme, only one machine can transmit on the network at a time. The machines or computers connected to the ring act as signal boosters or repeaters which strengthen the signals that transverse the network.

The primary disadvantage of ring topology is the failure of one machine will cause the entire network to fail. Mesh Network Topology:- The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed’s Law. [pic] Fully connected mesh topology Fully connected:- The type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

Note: The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected. Partially connected:- [pic] Partially connected mesh topology The type of network topology in

which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network. Note:

In most practical networks that are based upon the physical partially connected mesh topology, all of the data that is transmitted between nodes in the network takes the shortest path (or an approximation of the shortest path) between nodes, except in the case of a failure or break in one of the links, in which case the data takes an alternate path to the destination. This requires that the nodes of the network possess some type of logical ‘ routing’ algorithm to determine the correct path to use at any particular time. 7. Basic Hardware Components All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers.

In addition, some method of connecting these building blocks is required, usually in the form of galvanic cable (most commonly Category 5 cable). Less common are microwave links (as in IEEE 802. 12) or optical cable (“ optical fiber”). An ethernet card may also be required. Network Interface Cards:- A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. Repeaters:- A repeater is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an

bstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable which runs longer than 100 meters. Hubs:- A network hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address. Bridges:- A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports.

Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received. Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived. Bridges come in three basic types: 1.

Local bridges: Directly connect local area networks (LANs) 2. Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced by routers. 3. Wireless bridges: Can be used to join LANs or connect remote stations to LANs. Switches:- A network switch is a device that forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC

addresses in the packets. This is distinct from a hub in that it only forwards the packets to the ports involved in the communications rather than all ports connected.

Strictly speaking, a switch is not capable of routing traffic based on IP address (OSI Layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports, with the intention being that most or the entire network is connected directly to the switch, or another switch that is in turn connected to a switch. Switch is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content (e. g. , a Web URL identifier).

Switches may operate at one or more OSI model layers, including physical, data link, network, or transport (i. e. , end-to-end). A device that operates simultaneously at more than one of these layers is called a multilayer switch. Overemphasizing the ill-defined term “ switch” often leads to confusion when first trying to understand networking. Many experienced network designers and operators recommend starting with the logic of devices dealing with only one protocol level, not all of which are covered by OSI. Multilayer device selection is an advanced topic that may lead to selecting particular implementations, but multilayer switching is simply not a real-world design concept. Routers:-

A router is a networking device that forwards packets between networks using information in protocol headers and forwarding tables to determine the best next router for each packet. Routers work at the Network Layer of the OSI model and the Internet Layer of TCP/IP. 8. Comparison with TCP/IP In the TCP/IP model of the Internet, protocols are deliberately not as rigidly designed into strict layers as the OSI model. RFC 3439 contains a section entitled “ Layering considered harmful. ” However, TCP/IP does recognize four broad layers of functionality which are derived from the operating scope of their contained protocols, namely the scope of the software application, the end-to-end transport connection, the internetworking range, and lastly the scope of the direct links to other nodes on the local network.

Even though the concept is different than in OSI, these layers are nevertheless often compared with the OSI layering scheme in the following way: The Internet Application Layer includes the OSI Application Layer, Presentation Layer, and most of the Session Layer. Its end-to-end Transport Layer includes the graceful close function of the OSI Session Layer as well as the OSI Transport Layer. The internetworking layer (Internet Layer) is a subset of the OSI Network Layer, while the Link Layer includes the OSI Data Link and Physical Layers, as well as parts of OSI’s Network Layer. These comparisons are based on the original seven-layer protocol model as defined in ISO 7498, rather than refinements in such things as the internal organization of the Network Layer document.

The presumably strict consumer/producer layering of OSI as it is usually described does not present contradictions in TCP/IP, as it is permissible that protocol usage does not follow the hierarchy implied in a layered model.

Such examples exist in some routing protocols (e. g. , OSPF), or in the description of tunneling protocols, which provide a Link Layer for an application, although the tunnel host protocol may well be a Transport or even an Application Layer protocol in its own right. The TCP/IP design generally favors decisions based on simplicity, efficiency and ease of implementation. 9. Firewall A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.

It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques: 1. Packet filters: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.

Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing. 2. Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation. 3. Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can

flow between the hosts without further checking. 4. Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses. Function of Firewall:-

A firewall is a dedicated appliance, or software running on a computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. It is a software or hardware that is normally placed between a protected network and a not protected network and acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in. A firewall’s basic task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a “ perimeter network” or Demilitarized zone (DMZ).

A firewall’s function within a network is similar to physical firewalls with fire doors in building construction. In the former case, it is used to prevent network intrusion to the private network. In the latter case, it is intended to contain and delay structural fire from spreading to adjacent structures. Without proper configuration, a firewall can often become worthless. Standard security practices dictate a “ default-deny” firewall ruleset, in which the only network connections which are allowed are the ones that have been explicitly allowed. Unfortunately, such a configuration requires detailed understanding of the network applications and endpoints required for the organization’s day-to-day operation.

Many businesses lack such understanding, and therefore implement a “ default-allow” ruleset, in which all traffic is allowed unless it has been specifically blocked. This configuration makes inadvertent network connections and system compromise much more likely. 10. Conclusion Bibliography Referred Books:- 1. Data Networks – BERTSEAKAS & GALLEGER. 2. Computer Networks & Internets – DOUGLAS E. COMER 3. Telecommunication Networks – SCWARTZ Referred Websites:- ? http://www. roamware. com ? http://www. yahoo. com ? http://www. wikipedia. com ? http://www. google. com NOTES 5. ROAMWARE’S NETWORK LAYOUT ————————– NODE 1 NODE 2 NODE 39 NODE 40 NODE 1 NODE 2 NODE 39 NODE 40