XYZ Insurance (Pvt) Ltd.

Networking debrief

12/9/2018

IDM

K.P.I. Shenesh Perera

Contents

[Introduction 2](#_Toc532294522)

[Networking Principles 3](#_Toc532294523)

[Types of different networks/network topologies 4](#_Toc532294524)

[Virtual Local Area Network (VLAN) 4](#_Toc532294525)

[Networking Devices 5](#_Toc532294526)

[1. Repeater 5](#_Toc532294527)

[2. Hub 5](#_Toc532294528)

[3. Bridge 5](#_Toc532294529)

[4. Switch 6](#_Toc532294530)

[5. Routers 6](#_Toc532294531)

[6. Gateway 6](#_Toc532294532)

[7. Bridging router 6](#_Toc532294533)

[Network Operating Systems 6](#_Toc532294534)

[Servers 7](#_Toc532294535)

[1. Application server 7](#_Toc532294536)

[2. Catalog server 7](#_Toc532294537)

[3. Communications server 7](#_Toc532294538)

[4. Computing server 7](#_Toc532294539)

[5. Database server 7](#_Toc532294540)

[Network system and server proposal 7](#_Toc532294541)

# Introduction

The report will contain comprehensive analysis, information and descriptions to explain, clarify and solidify information with related to the networking concepts, protocols, topologies, devices, systems, software involved and any of the below mentioned factors that will pertain to maintain and organize a network in XYZ Insurance Company.

Complicated jargon and incomprehensible phenomena will be avoided so as to give any reader be it experienced or not in the field of networking a solid understanding.

# Networking Principles

The most known and common network principles known to networking are the OSI model and the TCP/IP model. Below in the table a full comparison of the protocols, networking concepts and solutions have been described.

|  |  |
| --- | --- |
| Open Systems Interconnection Model | Transmission Control Protocol/Internet Protocol Model |
| * It is a theoretical model primarily used for computer systems. * Consists of 7 main layers. * Developed by International Standard Organization. * Usage is pretty low. * Follows a vertical approach * The transport layer in the OSI model guarantees the successful delivery of packets. * The OSI model has separate presentation and session layers. * Transport and network layers are compulsorily connection oriented. * OSI is mostly a guidance tool for learners in the networking field. * The OSI model is vague in terms of including protocols into the model as at times 1 protocol functions in multiple layers. * Protocols are easily changed in the OSI model as technology advances. * The OSI model defines interfaces, services and protocols used clearly and are also protocol independent. * The physical layer that performs media, signal and binary transmission uses 802.11, DSL, SDH, V.34, RJ45 and RS-232 protocols. * The data link layer that performs physical addressing uses Ethernet, 802.11, MAC/LLC, HDP, Fiber Channel, Frame relay, HDLC, PPP, Q.921 and Token ring protocols. * The network layer that performs path determination and logical addressing uses IP, ARP, IPsec, ICMP, IGMP and OSPF protocols. * The transport layer that performs end to end connections and reliability uses TCP, UDP, SCTP, SSL and TLS protocols. * The session layer that performs inter-host communication uses TCP, SIP, RTP and RPC-named pipes. * The presentation layer that performs data representation and encryption uses HTML, DOC, JPEG, MP3, AVI and sockets. * The application layer that performs network process to application procedures uses DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet and FTP protocols. | * It is a client to server based model for transmission of data over the internet. * Consists of 4 main layers. * Developed by Department of defense. * Usage and implementation is frequent. * Follows a horizontal approach * The TCP/IP model there is no guarantee that packets will be delivered successfully but it is more reliable than OSI. * TCP/IP model does not have such separate layers. * Transport layer and network layers are both connection & connection less oriented. * The TCP/IP model could be called the implementation of the OSI model. * The TCP/IP model does not have such a problem. * Replacing or introducing a new protocol is not easy. * TCP/IP is protocol dependent and there is no clear differentiation between interfaces and protocols. * Have a combined layer for data link and physical called network access layer that uses Ethernet, token ring, ATM or frame relay protocols. * Network layer is called internet layer, and performs the function uses ARP, IP, IGMP and ICMP protocols. * Transport layer uses TCP and UDP protocols. * Application, presentation and session layer are combined and are called the application layer, and uses HTTP, SMTP, Telnet, FTP, DNS, RIP, SNMP etc. protocols. |

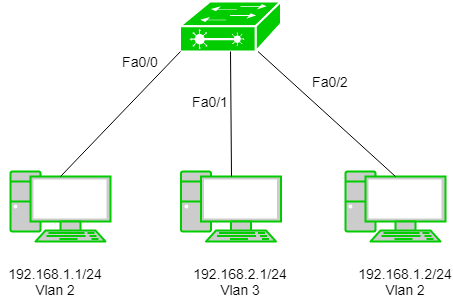
# Types of different networks/network topologies

There are a plenty of types of networks such as LAN, WAN, WLAN, VLAN, MAN, PAN, VPN, EPN etc. but for the sake of this report I will compare the most commonly met types of networks LAN, WAN and MAN with each other, then a network topology known as VLAN and another called VPN.

|  |  |  |
| --- | --- | --- |
| Local Area Network | Wide Area Network | Metropolitan Area Network |
| * A network that connects a group of computers in a small geographical area. * Privately owned. * Easy to design. * Easy to maintain. * High speed. * Short propagation delay. * Fault tolerance is high. * Budget required is low. * Software security is sufficient for most part. Hardware security is optional. * Bandwidth required is quite low but depends on the size of the LAN and network traffic. | * It spans large locality and connects countries together. * Public or privately owned * Difficult to design. * Difficult to maintain. * Significantly low speed. * Long propagation delay. * Fault tolerance is quite low. * Budget required is high. * Hardware security is compulsory. * Very high bandwidth is compulsory. | * It covers relatively large region such as cities, towns. * Public or privately owned, * Difficult depends on the complexity * Difficult to maintain. * Moderate speed. * Short propagation delay. * Fault tolerance is moderately high. * Budget required is high. * Hardware security is compulsory. * High bandwidth is compulsory. |

Figure 1.0, geeksforgeeks.com, saurabhsharma56

## Virtual Local Area Network (VLAN)



A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

Higher-end switches allow the functionality and implementation of VLANs. The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features.

A VLAN allows several networks to work virtually as one LAN. One of the most beneficial elements of a VLAN is that it removes latency in the network, which saves network resources and increases network efficiency.

In addition, VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Traffic patterns can also easily be controlled by using VLANs.

|  |  |
| --- | --- |
| Pros | Cons |
| * Allows network administrators to apply additional security to network communication * Makes expansion and relocation of a network or a network device easier * Provides flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations * Decreases the latency and traffic load on the network and the network devices, offering increased performance | * Higher risk of virus issues because one infected system may spread a virus through the whole network * Equipment limitations exist in very large networks because additional routers might be needed to control the workload * Effective at controlling latency than a WAN, but less efficient than a LAN |

VLANs are typically used in a company to isolate departments so that the network traffic within one network does not mingle with the other, this way that department can be treated as an entirely different network. Therefore you can enhance or decrease the security in that VLAN.

# Networking Devices

Devices that facilitate and provide services in a network are known as network devices, often in the industry they are referred to with respect to their functionality per the OSI model.

1. Repeater

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak so as to extend the length to which the signal can be transmitted over the same network. An important point is that repeaters do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

1. Hub

A hub is a multiport repeater. A hub connects wires coming from different branches, ex: the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies.

1. Bridge

A bridge operates at the data link layer. A bridge is a repeater, with higher functionality of filtering content by reading the MAC addresses of both source and destination. It is also used for interconnecting 2 LANs working on the same protocol. It has a single input and single output port, thus making it also a 2 port device.

1. Switch

A switch is a multiport bridge with a buffer memory and is designed so efficiency and performance is boosted. A switch is a data link layer device. Switches can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward healthy and accurate packets selectively to correct ports only.

1. Routers

A router is a device like a switch that routes data packets based on their IP addresses. A router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.

1. Gateway

A gateway is a passage to connect two networks together that may work upon different networking models. They work as the messenger agent that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than any switch or router

1. Bridging router

It is a device which combines features of both a bridge and router. It can work either at the data link layer or at network layer. Working as a router, it is capable of routing packets across networks and working as a bridge, it is capable of filtering local area network traffic.

# Network Operating Systems

A network operating system is an OS designed for the purpose of supporting and maintaining multiple workstations, database sharing, and application sharing alongside printer access sharing among multiple computers in a network. Certain standalone operating systems, such as Microsoft Windows NT and Digital’s OpenVMS, come with multipurpose capabilities and can also act as network operating systems. Some of the most well-known network operating systems include Microsoft Windows Server 2003, Microsoft Windows Server 2008, Linux and Mac OS X.

GNU/Linux branch has the best server operating systems, Ubuntu 16.04 LTS can be used as a server operating system but it’s learning curve is high, almost everything is command line based however this ensures precision and very high security. Ubuntu is a highly flexible NOS, most of the best network analysis, maintenance and troubleshooting software exist for the linux branch and Ubuntu has it all.

Mac OSX is used widely but I personally do not recommend it as a NOS as it is more suited as a development environment for a single user, it does have quality features but repairing, troubleshooting and analyzing mac OS systems is difficult. Although security is high, the availability of software that facilitates maintenance and analysis in a network are usually not released for mac systems.

As such the best choice for businesses like XYZ Insurance is the Microsoft Windows server branch, as it is easy to use, cheap and troubleshooting is quite the easy task. However security is not as efficient as the previously mentioned branches, althought this is the case it can easily be compensated through encryption and anti-virus programs.

# Servers

## Application server

These servers’ hosts web apps allowing users in the network to run and use them preventing the installation a copy on their own computers. These servers need not be part of the WWW.

## Catalog server

These servers maintain an index of information that can be found across a large distributed network. The distributed network may include computers, users, files shared on file servers and web apps. Examples of catalog servers are name servers.

## Communications server

These servers maintain an environment needed for 1 communication endpoint to find other endpoints located in the network and communicate with them. These servers may or may not include a directory of containing communication endpoints and a presence detection service, depending on the flexibility and security parameters of the network.

## Computing server

These servers share vast amounts of computing resources which include CPU and RAM over a network. Any computer program that needs more CPU power and RAM than a personal computer can afford use these types of servers.

## Database server

These servers maintain any form of database over a network. Candidates of these servers are spreadsheets, accounting software, asset management software or virtually any computer program that consumes well-organized data, especially in large volumes. Database servers are crucial in environments that require storage of information in an organized manner.

# Network system and server proposal

Per the afore mentioned information I propose that XYZ Insurance uses a Local Area Network within the entire building then with the assistance of routers create VLANs to separate each department of the company.

The company should split the insurance, investment, marketing and admin departments in a VLAN topology and give each of them a separate network address. Then proceed to centralize insurance, investment and marketing departments with the help of a router. With the help of inter-VLAN communication, the admin department should be granted access to communicate any of the traffic from the other departments.

As this is an insurance company it is ideal to pass the traffic of the network through a firewall. A firewall restricts access to and from the network using the help of rules, which can be facilitated with a router or a firewall device itself.

It is highly ideal if XYZ could ensure the usage of Triple DES encryption, and with the help of IP phones use VoIP protocols to ensure effective communication. Any system unit within the network that must stream insensitive data must have User Datagram Protocol implemented while all session based sensitive data streaming must be done through API enabled web servers that have TCP/IP enabled.

It is highly recommended that XYZ uses a database server, VSIS a company that specializes in the field of providing ICT solutions to Sri Lanka offers support for databases as well. Visit this link; <http://vsis.lk/database/> to read more about them. Contact them at +94 11 2 038 500. They are backed by Microsoft and Oracle. A direct insight on the costing and bandwidth required cannot be depicted as there is no proper information given as to what and how much data is processed within the network but an estimate of a total cost of 340, 591 LKR is charged by VSIS for a company of this scale this includes security, complete database design, server implementation and training to IT staff. A service agreement can be established to partner with VSIS to ensure further support from them.

Install this server with Windows Server 2012 and ensure that the server makes system restore points before attempting to update.