Bachelor's thesis

Degree program: Information Technology

Specialization: Internet Technology

2014

Theodros Sisay Nigatu

MARITIME TRANSIT SERVICES ENTERPRISE NETWORKING ARCHITECTURE

TURKU UNIVERSITY OF APPLIED SCIE

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology| Internet Technology

2014 | 34pages

Instructor: Patric Granholm

Theodros Sisay Nigatu

MARITIME TRANSIT SERVICE ENTERPRISE NETWORK ARCHITECTURE

The Maritime Transit Service Enterprise is a government-owned but semi-autonomous organization that was established in 1979 by the government of Ethiopia. The head office is located in Addis Ababa .The purpose of the organization is to facilitate import and export goods by giving the services of bulk and general cargo, stevedoring, customs clearing, consolidation services, trucking operations, bagging services, container handling that includes storing, stuffing, and un-stuffing activities thereby fostering the development of the country.

The current network infrastructure used by Maritime Transit Service Enterprise was installed in 2004. The infrastructure is based on Windows Server 2003, which is controlled by Active Directory for data consistency and security. The Organization implements different technologies such as account package software (ACCPAC), email exchange software, fleet management software, and six different types of software packages which were designed and installed by Biz Soft of Ethiopia. The network uses an unmanageable switch that does not support Layer 2 functions such as Virtual Local Area Network, port security, spanning tree protocol and redundancy. The hardware was purchased over a long period of time and as a result, it has a physical memory limit. In general, the hardware device has not the processing power needed to handle the incurred traffic.

Maritime Transit Service Enterprise understood this fact and displayed motivation and readiness to deploy Cisco's modular Enterprise Composite Network, which are two Cisco Catalyst 4500 Series switches at the core/distribution layer and Cisco Catalyst 2960 switches at access layer. Some of the access switches are uplinked to the core/distribution switches with fiber optic and the rest with copper wire. For the branch office they are using Cisco SRW200 switches.

The purpose of this thesis is to enhance the network of Maritime Transit Service Enterprise to Enterprise Composite Network for the goal of maintaining a stable, responsive, reliable and secure Infrastructure that can help the company to automate the day - to - day activities of each functional unit for internal and external duties. The author designs a physical and logical layout, System design, installation and configurations of network devices.

By implementing Cisco's modular Enterprise Composite Network, Maritime Transit Service Enterprise can achieve modification, robustness, and scalability. As a result, the network infrastructure will be consistent, secure, and reliable and will have high performance. In addition to that, upgrading the technology will transform the work environment, boosting the workforce's productivity, profitability and morale.

KEYWORDS:

MTSE, ICT, maritime, network architecture

FOREWORD

I give thanks to all mighty God for giving me the strength, knowledge and understanding to complete this thesis. My gratitude goes to Nahom Getachew and ZeleAlem Bekele for helping me by giving the necessary information through the thesis. My appreciation goes to Patric Granholm who also happens to be my supervisor for shedding more light to this study. Finally, I appreciate the supports of my lecturers especially Väänänen Ossi and Slotte Vesa for their guidance and support that see me through concluding this study.

CONTENTS

FIGURES

LIST OF ABBREVIATIONS

MTSE	Maritime Transit Services Enterprise
LAN	Local Area Network
MAN	Metropolitan Area Networks
WAN	Wide Area Network
LLD	Low Level Design
DMZ	Demilitarized zone
VLAN	Virtual local Area network
STP	Spanning Tree Protocol
HSRP	Host Stand by Routing Protocols
LWAPP	Light-Weight Access Point Protocol
MAC	Media Access Control
QOS	Quality of Service
PE	Power over Ethernet
SSH	Secure Shell
DHCP	Dynamic Host Configuration Protocol
CAM	Content Addressable Memory

1 INTRODUCTION

Maritime Transit Services Enterprise (MTSE) is an organization setup and run by the government of Ethiopia to handle the nation's maritime and transit needs. The organization operates out of its head office located in the capital of the country and has other five branches spread around the country. MTSE also has two offices in Djibouti, the only port that the country uses for its maritime needs. The organization has about 750 employees. The organization operates from one of the sky rise buildings located in the capital.

Figure 1. MTSE Head Office (MTSE, 2013)

The main purpose of the company is to facilitate the maritime service needed by commercial and government organizations to import or export goods from Ethiopia to any county or vice versa. This includes checking bills of loading with actual goods, registration of goods on behalf of the Customs Authority. (MTSE, 1979)

1.1 Objective and purpose

Ethiopia has one of the fastest growing economies in the continent. This acceleration has put pressure on the services provided by Maritime Transit Services Enterprise. Hence, the organization needs to capitalize on the currently available technology to enhance its competitive edge and increase the quality of service provided to its customers.

The objective of the project is to redesign the overall network architecture of Maritime and Transit Services Enterprise existing legacy network. The scope of this project is to design a robust, secure, scalable and flexible network system.

The project will deliver:

- design for the network architecture
- security scheme
- site preparation guide
- hardware and software specifications needed for implementation
- recommendation for future expansion.

.

1.2 Approach and Methodology

The following structural approach and methodology are applied in the life cycle of the Project. This will create a smooth and transparent communication between the author of this thesis and MTSE during the deployment of the solution.

The project planning phase has the following steps.

- After a common understanding has been reached, a contract will be signed and the project will be implemented.
- All the procured devices will be ordered and transported from the manufacturers and distributors.
- While the devices are being procured, a Low Level Design (LLD) will be prepared and delivered. This document will outline step-by-step, the configuration of each procured device and service. This will be the guide during implementation.

The thesis will detail the requirements necessary for the successful implementation of this project. Additionally, it will show the procedures and methods that will be used to stage the procured solutions.

2 THEORY AND LITERATURE REVIEW

2.1 Introduction to networking

Network is an infrastructure that facilitates interaction between devices like computers, printers, and other mobile devices used in an organization or system to share resources and information as needed. This system may utilize wire or wireless technique to achieve these functionalities. Characteristically, the devices share the processing power of a single server and additionally, may share internet access or be an exclusive integral in the system. (Balchunas, CCNP Switching Study Guide, 2012)

Basically, networks fall into three broad categories:

- Local Area Networks (LAN),
- Metropolitan Area Network (MAN)
- Wide Area Networks (WAN).

A Local Area Networks (LAN): is a network confined to a single floor or building servicing the devices found in the specified area. These systems mostly serve to share devices, information and internet access in an organization. Wired or wireless mechanisms are implemented to achieve this goal. (Teare, 2008)

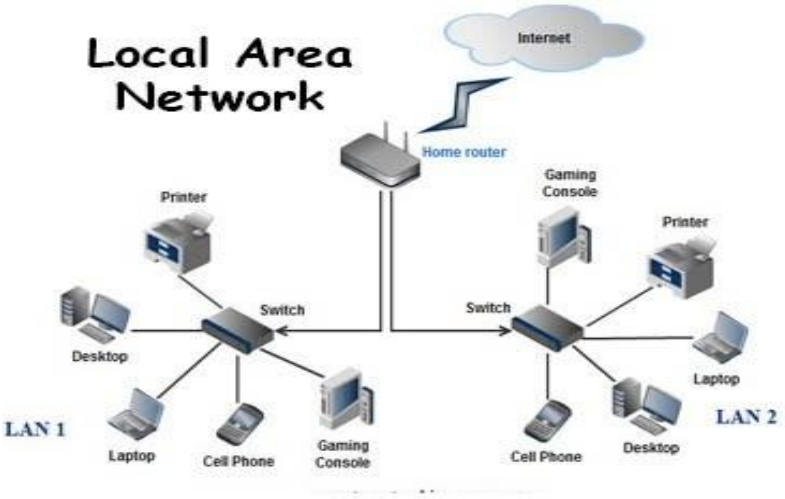

Figure 2. Typical Local Area Network (Cisco, 2009)

Metropolitan Area Networks (MAN): as implied by the name, metropolitan networks that fall in to this category are larger in scale and encompass a larger area. The network may cover interaction between two to three buildings of an organization to branches located across town. VPN and other dedicated physical and logical networking schemes are implemented. Layer three devices with selected IP schemes are mostly used to share servers, processing power and centralized storage facilities like branches with their HQs. (Teare, 2008)

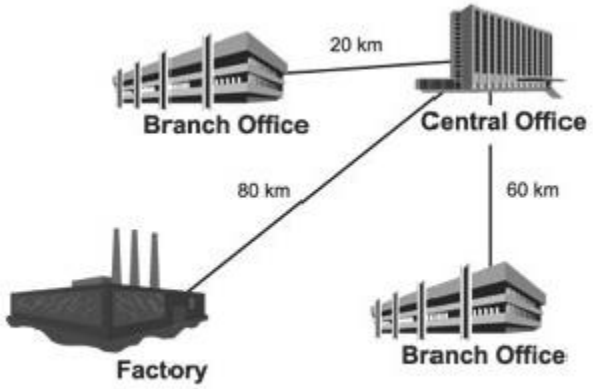

Figure 3. Typical Metropolitan Area Networks (Cisco, 2009)

Wide Area Networks (WAN): networks that fall in the wide area network category encompass a larger geographical area. These systems are mostly used for information sharing, providing services, sharing processing power and storage spaces, etc. These networks integrate and utilize diverse public and private infrastructures across metropolitan, regional, national and international boundaries. The internet can be considered a good example for WAN. (Teare, 2008)

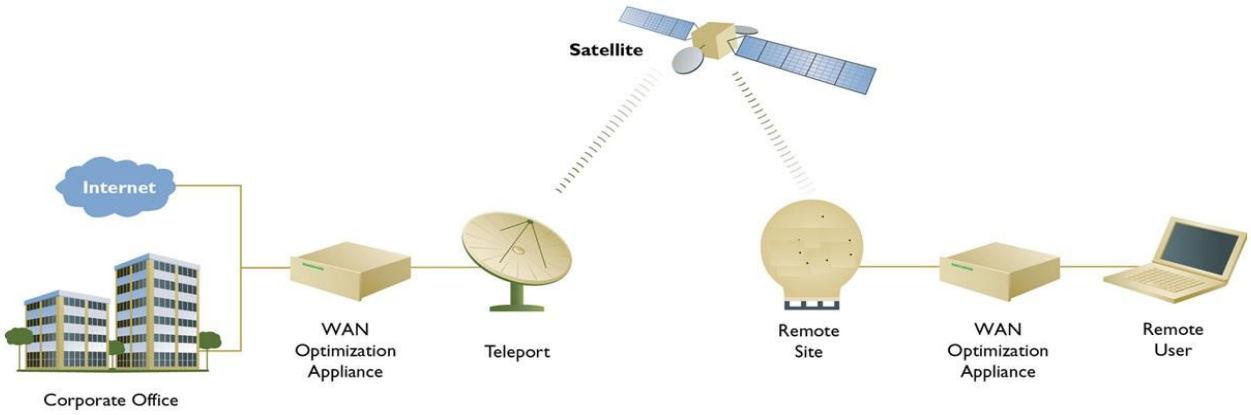

Figure 4. Typical Wide Area Network (Cisco, 2009)

2.2 Case Study of the existing network

2.2.1. Architecture of the network

A 15-story building accommodates the MTSE Head office, an apartment complex, a high class restaurant, a multi-purpose hall and an assembly hall. The existing network infrastructure, used by the MTSE head office was setup in 2004.It uses legacy devices which do not have the processing power needed to handle the traffic incurred currently.

The domain-based system has a hierarchical architecture with layer two switches providing a starlike network architecture for the LAN and a single gateway router servicing MTSE's internet and data exchange demand. The web-based software used within the organization, accessed by staff located at the central and branch offices, resides in a server located inside the headquarters. Additionally, the Ethiopian Customs and Revenue Authority consumes the data stored in this server, which multiplies the traffic load on the existing legacy system. The organization's website is also hosted on the Ethiopian Telecommunication server.

Generally, the following services contribute to the overall traffic serviced by the existing network:

- Traffic for the web-based application used by the staff located in the head office, at branch offices, offsite and Ethiopian Customs and Revenue Authority

- Traffic in sharing printers, scanners, etc. for the staff located in the head office
- Traffic in accessing the email exchange server software installed in a server located in the head quarter, used by staff in the head office and branches
- Additional traffic by the authentication system, which is centralized, when staff try to access the MTSE's web based application.

This network structure and architecture has not been upgraded since 2004.

2.2.2. Drawbacks of the existing network

Even though hubs are great pieces equipment, neither the software capability nor the processing power is adequate to service the overwhelming traffic. The LAN does not have a clearly defined collision domain divider. These results in unnecessary traffic in the network in addition to the fact that different hubs bought from several vendors to serve the network so that they are difficult to maintain and trouble shoot. For these specific reasons, the whole system crashes at least once each working day.

The star network architecture of the LAN also makes it vulnerable to failure, resulting in failure in one part of the network hindering communication between other parts of the network. For example, a loose power cable in one of the networking devices results in a shutdown of the entire system. An absence of redundant links also contributes to the congestion and the resulting failure in the system. The system also uses the same backbone network to service its web-based application consumers, email exchange server and access to the internet.

At least MTSE have a plan to increase the number of servers and assign tasks for each server depending on their task. For example, they need a web server for web-based programming, an email exchange server only for the email purpose and an authentication server for authentication username and password in addition to that there are different antivirus software in the system for virus protection, However, many different antivirus software are difficult to manage shoot so that MTSE have to change in one antivirus software.

There is security breach both from outside and inside users. Access to data on servers is not regulated. Sometimes this breach is carried out in a real time environment, either from servers inside the head office or branch offices. Currently unauthorized hosts or persons are allowed access to sensitive information.

3 PROJECT BENEFITS

The proposed network system uses state-of-the-art technology and design schemes. The devices used have a high rate of convergence and the capability to handle a high level of traffic without a noticeable decrease in throughput. These will increase the speed and efficiency of the staff. The staff located in the branches of the organization will be able to access the applications and other information on the servers located in the HQ with a reliable and fast connection, hence helping them give a more dependable and efficient service.

Data exchange will be consistent, secure, and reliable to ensure workforce productivity, profitability, and customer satisfaction. Additionally, upgrading the technology will transform the work environment, boosting the workforce's productivity and morale.

In order to achieve the above-mentioned benefits and insure longevity, the network needs to be capable of flexible scalability and security.

Modification: One of the challenges in the existing system is that modification to any part of the system affects the service performance of the system entirely. In the new proposed system, through modularity of the network, modification in parts of the system can be done without affecting the service performance of other sections. (Fitzgerald, 2009)

Redundancy: All of the devices that reside in the core, distribution, server-farm part and in other parts of the network have been doubled to minimize service disruption due to device failure. (Fitzgerald, 2009)

Security : Due to the sensitivity of the information handled by the organization, security has been requested on the principal points of the network for the sensitive data and services that require security from the outside and inside intruder. This will be dealt with by implementing a security strategy in multiple layers of the network and installing hardware device in the right place. (Fitzgerald, 2009)

Scalability: The enterprise can add additional branches in to the network far more easily with a minimum amount or no configuration changes on the other parts of the network. (Fitzgerald, 2009)

Robustness: The devices that have been requested in almost all parts of the network will be able to self-heal during the device or system failures. The request for a backup system can be an example of this, in the event of a disaster. (Fitzgerald, 2009)

4 NETWORK ANALYSIS

4.1 Network design

The solution implements a high-end routing & switching solution of Cisco Systems Inc. The design follows Cisco's modular Enterprise Composite Network design with two Cisco Catalyst 4500 Series switches at the core/distribution layer and different types of access layer switches. Still, there is a possibility some of the access switches are uplinked to the core/distribution switches with fiber. The details of the proposed solution are described in the sub-sections below.

4.2 The Physical layout

The physical layout has a star topology with the selected switches and is presented in later sections. The Cisco 4500 switches will perform central routing and control, while the Cisco Catalyst 2960 switches will provide end user connectivity.

The physical design has the following features:

- In the server room, each server will be directly aggregated to each core switch.
- It is recommended to add dedicated switches to aggregate those servers and connect with the core switches. This will create a demilitarized zone of the network (DMZ).
- There are two routers for the same purpose. In case one router it fails, then the backup router is used as an option to go the Customs Office. Different VLANs provide access to the Internet and connect to the branch office.
- Cisco 2960 and Cisco 4500 switches are required to connect computers, printers, and other devices on different floors of the building,
- The building is equipped with fiber lines. Category 6e cabling and wall plates are used in the office.
- Only authorized persons are allowed to enter a server room using a keycard system.

4.3 Logical layout

The logical layout to be implemented is a hierarchical star. The selected devices will centralize and structure the logical data interaction of the entire system

.

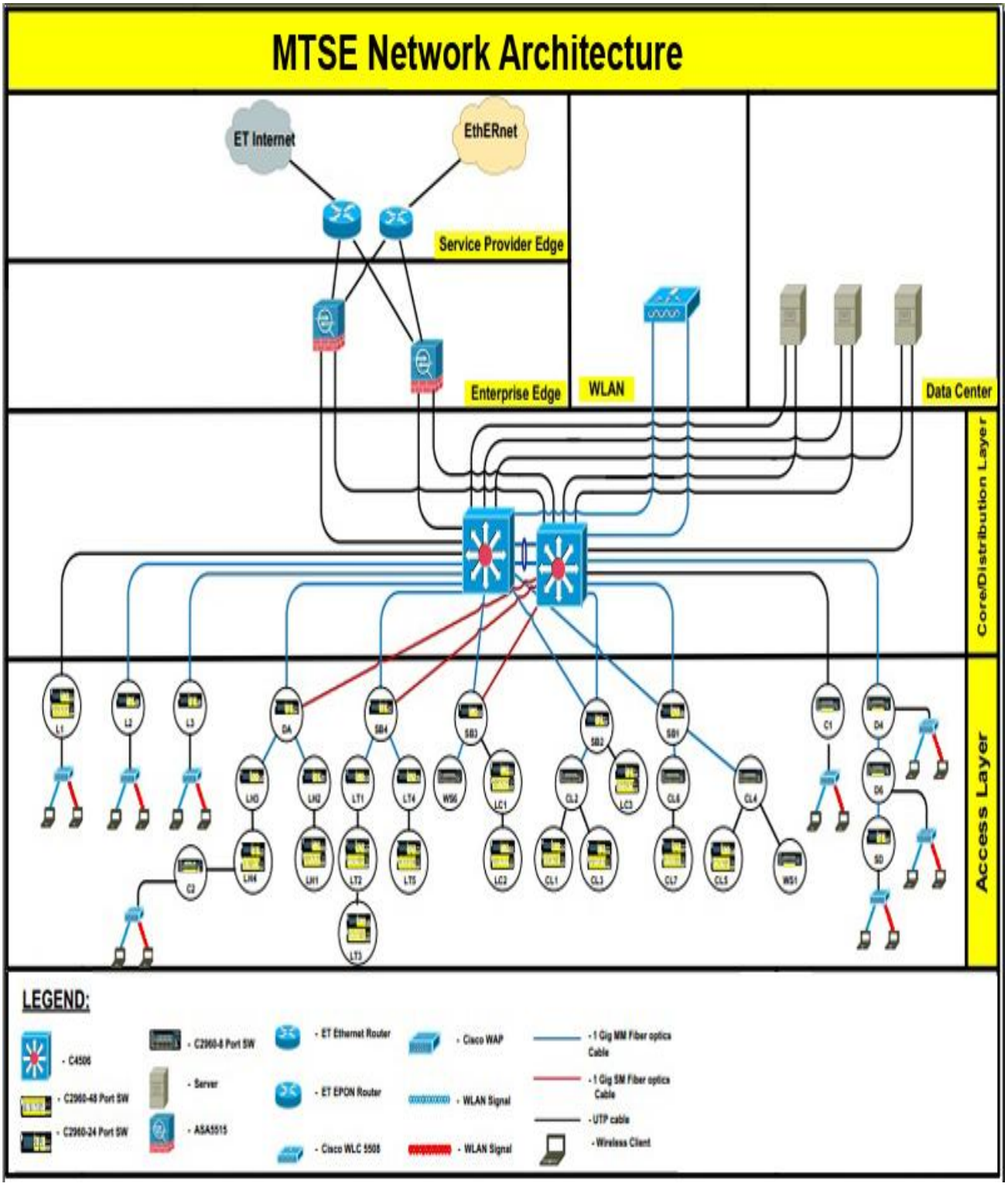

Figure 5. MTSE Network Architecture

4.4 Software analysis

4.4.1 Distribution Layer

The distribution layer connects the core layer, the server farm, and the DMZ to the access layer. In this layer, packets are routed between subnets and VLAN. Hence, the following functionalities are proposed for MTSE's network:

- Providing static routing to access the internet and another one to access the customs server
- Working as spanning tree protocol (STP) for Root Bridge in a local load balancing method between them. When accessing VLANs from different buildings, half of the traffic will be switched through one core switch and the other half will be handled by the second core switch.
- Providing gateway redundancy for access switch VLANs. It will be implemented to have the load balanced between the core switches and the STP .
- Providing dynamic host configuration protocol (DHCP) services for entire data center client end-points and for the end-users.
- Working as STP (PVSTP, MST) Root Bridge in a local load balancing method between them. Half of the access VLANs from different buildings will be switched through one core switch and the other half will be handled by the second core switch.
- Providing HSRP gateway redundancy for access switch VLANs. It will be implemented to achieve load balance between the core switches and the STP (PVSTP, MST) topology. The SVIs will be in active state on the core switch same as the primary root bridge configuration which will ensure perfect logical load balancing between these core switches for traffic coming from the access layer.
- Providing routing services, like OSPF, EIGRP, RIP,STATIC to the Server Farm and uplink Cisco ASA firewalls

4.4.2 Access Layer

The access layer is the layer that connects the client node to the distribution layer. This layer is the second line of defense in the network through different configuration. The following proposed functionalities are going to be configured in this layer:

VLAN (Virtual LAN) is a logical group of computers despite their location or geographical distribution. For example, the marketing department has 26 computers and one printer. Out of these computers, 15 are on the second floor and the rest are on the seventh floor including their printers. By creating a VLAN, despite their location they are in different broadcast domains from the rest of the network.

The MTSE has the following VLANs in their infrastructure:

- Import and export cargo forwarding
- Bulk and general cargo stevedoring
- customs clearing
- Air cargo agency and consolidation services
- Marketing department
- Information department
- Accounting department
- Human resources
- Container handling that includes storing, stuffing, and un-stuffing activities
- Trucking operations and bagging services
- Management VLAN

By implementing the above VLAN at least MTSE have 10 broadcast domains in addition to a collision domain in each segment. As a result, one switch will be configured as a server and the rest as clients so that they can distribute all VLAN information from server to clients.

Redundancy:- for reliability purposes, there is always an immediate backup to a fault by installing additional network devices or cables. Installing an additional device creates a broadcast storm; however, by configuring a spanning tree protocol, the broadcast storm is avoided.

In Figure 5, all the network devices are connected to DMZ both through a primary path and an alternative path. When the primary path is disrupted, automatically the alternate path starts to transmit data

.

Port Security: Either dynamically learned or statically assigned the MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. Depending on the configuration, they can shut down the port by protecting the network from intruders or unidentified computers.

The following port security procedures are applied in the MTSE network:

- All demilitarized zone of servers that are connected with the distribution layer are configured with statically secure MAC- addresses. When the source MAC address of the incoming traffic is different from the statically configured MAC address then the port automatically shuts down and reports to the network administrator. (Balchunas, 2012)
- All the computers that are connected with the access layer ports are configured dynamically. By implementing sticky MAC addresses procedures the port learns the MAC-address for the first time dynamically and stores in Content addressable memory (CAM) that maps the MAC addresses to the ports. When it is violated it implements the policy of restriction and reports to the network administrator by sending a Simple Network Management Protocol (SNMP) trap. (Balchunas, 2012)
- After a secure MAC address is configured or learned on one secure port, the sequence of events that occurs when port security detects that secure MAC- address on a different port in the same VLAN is known as a MAC move violation. (Balchunas, CCNP Switching Study Guide, 2012)

BY implementing port security the MTSE not only avoids the attackers from sending a whole bunch of mock-up (fake) source MAC addresses but also protect employees from plugging in to their own hub and switch in to the system.

Secure Shell (SSH2) is a network management protocol between two network devices for the purpose of secure data communication via a virtual secure channel with the help of special installed software. By configuring secure shell in the switches, a network administrator can control all devices from his office or branch office, for example, one of the security policy of MTSE is that all unused switches ports are shutdown. However, the marketing department decides to move some computer from the second floor to the seventh floor and it plug to switch port while the network administrator is in the branch office. Without going to the actual switch by virtual login, the network administrator command-line logs in and this command execution solves the problem..

Power over Ethernet: For deployment of IP telephony, wireless and video surveillance, there will be no need for additional power supplies or outlets for IP phones, IP cameras, or

wireless access points. They speed up deployment and installation and take advantage of advanced communications technologies quickly. (Cisco, 2011)

Quality of Service: Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required Quality of Service (QoS) by managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network becomes the secret to a successful end-to-end business solution (Cisco, 2011)

4.5 Hardware analysis

Below the devices to be used for the implementation of the proposed system are discussed briefly. Selecting the equipment is based on the following criteria.

Reliability: Whether devices are consistently performing according to their specifications in the network. In addition to that, the history of the device or the experience from the past technical capability affect the selection of the devices .

Availability: Unfortunately we do not have lot of availability in the country. However, in the near future the rapid growth and development of the country is forcing bigger companies to use current network technology.

Troubleshooting and maintenance: MTSE expect that a network administrator is capable of managing the network. In case it is beyond his/her capacity, then they can require support from the vendor.

Warranty: The vendor has an obligation for two years' warranty. In case the hardware fails, the vendor is going to replace the device.

Managed switches give more control on LAN and offer advanced features to control the traffic. However, an unmanaged switch allows Ethernet devices to communicate with one another. Even if it is expensive, among different switches selecting a Cisco device is the best option.

4.5.1 Distribution Switches

The proposed solution for the distribution layer of the network is to aggregate all access switch and wireless controller into two redundant Cisco 4500 series switches. The Cisco 4500 series switch provides high performance and security through Layer 2 to Layer 4. (Cisco, 2011)

Figure 6. Cisco 4500 series switches (Cisco, 2011)

The access switches are uplinked to the core/distribution switches with fiber lines and the rest with copper (CAT 6e) wiring. In case the need arises to upgrade the system, this switch have the capability of providing five line cards and one supervisor engine is populated with SUP-7LE Supervisor Engine and one SFP line card.

According to Cisco, innovation in the Supervisor Engine 7L-E includes: (Cisco, 2011)

- In case of the bandwidth upgrade in future, it can support up to 520Gbps system performance with 48Gbps per slot to every line-card slot
- Pluggable Plus [SFP+] optics or four Gigabit Ethernet uplinks (SFP optics)
- 225 Mbps IPV4 throughput
- 110 Mbps IPV6 throughput
- 48G Bandwidth /slot
- Up to 10 years of investment protection through backward and forward

Figure 7. Cisco 4500 E (Cisco, 2011)

“The Cisco Catalyst 4500-E Series extends to the network edge with intelligent network services. These include a sophisticated Quality of Service (QoS), predictable performance, advanced security, comprehensive management, and integrated resiliency. Scalability of these intelligent network services is made possible with a dedicated and specialized resource known as Ternary Content-Addressable Memory (TCAM).” (Cisco, 2011)

4.5.2 Access Switches

Access switches provide end-user connectivity for computers/laptops, printers wireless access points. In case network disruption or inside intruder for mitigating man-in-the-middle attacks such as MAC, IP, and ARP spoofing, then the switch's superior Layer 2 threat defense capabilities are the best choice. For all of these reasons, Cisco Catalyst 2960 switches are proposed to be used for this layer. (Cisco,2011)

Figure 8. Cisco Catalyst 2960 switch (Cisco, 2011)

“The Cisco Catalyst 2960 Series Switches are the leading Layer 2 edge switches. These switches provide improved ease of use, highly secure business operations, improved sustainability, and a borderless network experience. The 2960 Series are fixed-configuration access switches designed for enterprise, midmarket, and branch office networks to provide lower total cost of ownership. The hardware structure of the Cisco 2960 switch enables various borderless network services such as mobility, security, sustainability. In addition to that, they are minimizing the power consumption of the device. Cisco Catalyst 2960 Series Switches include the following features.” (Cisco, 2011)

Figure 9. Cisco Catalyst 2960G-24TC-L (Cisco, 2011)

According to Cisco, Catalyst 2960 Series Switches include the following features (Cisco, 2011)

Threat defense (Port Security, DHCP Snooping, Dynamic ARP inspection (DAI), IP source guard)

- Cisco Trust Sec
- Other advanced security features
- Cisco Energy Wise technology
- Efficient switch operation
- Intelligent power management.

According to Cisco, the Catalyst 2960G-24TC-L fixed configuration is proposed with the following configuration (Cisco, 2011)

a. WS-C2960G-24TC-L: Catalyst 2960 24 10/100/1000 4 T/SFP LAN Base Image

b. CAB-ACE: AC Power Cord (Europe) C13 CEE 7 1.5M

c. GLC-SX-MMD=: 1000BASE-SX SFP transceiver as module MMF 850nm DOM

d. GLC-LH-SMD=: 1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm

4.5.3 Access Switches for branch offices

Currently, the branch offices have 20 to 50 workstations with plans to increase the number to 75. Additionally, network printers are also shared. Cisco SRW200 series Small Business switches are proposed for end user connection in all branch offices. These switches provide end-user connectivity for desktops, laptops, servers, and network printers.

“The Cisco SRW 200 Series Switches are a series of affordable intelligent switches that combine powerful network performance and reliability. They also have essential network management features needed for a solid business network. Currently, these switches combine powerful network performance and reliability with the essential network management. These Fast Ethernet or Gigabit Ethernet switches provide basic management, security, Quality of Service (QoS) and Cisco Discovery Protocol. Additional features include: an easy-to-use web user interface, Cisco Discovery Protocol and Cisco Smart Ports. These switches are ideal for deploying and configuring a rock-solid business network in minutes.” (Cisco, 2013)

Figure 10. Cisco SRW200 Series Switches. (Cisco, 2013)

Power-saving features include:

- Automatic power down on Gigabit ports when a link is not active
- Embedded intelligence to adjust power based on length of cables on Gigabit Ethernet models
- which reduces power consumption, increases reliability, and provides quieter operation.

5 WIRELESS ARCHITECTURE

The Cisco Unified Wireless Network architecture unifies the configuration and control of the wireless LAN on the central controller. This enables the wireless LAN to function as an intelligent information network and support advanced services. This architecture simplifies operational management by compacting large numbers of managed endpoints and autonomous access points into a centralized and unified controlled system. (Enterprise Mobility 4.1 Design Guide)

In the MTSE's Unified Wireless Network architecture, access points are "lightweight", meaning that they cannot act independently of a controller. The access point configurations and firmware are managed by the wireless LAN controller. Therefore, no individual configuration of each access point is required. The access points handle only real-time MAC functionality. This leaves all the non-real-time MAC functionality to be processed by the wireless LAN controller (Enterprise Mobility 4.1 Design Guide) .

Access points interact with the controller through a Light-Weight Access Point Protocol (LWAPP).

LWAPP defines the following:

- Control messaging protocol and format (control traffic)
- Data encapsulation (data traffic)

Wireless LAN client data packets are encapsulated in LWAPP between the access point and the wireless LAN controller. Wireless LAN controller forward data frames to and from wireless LAN clients after encapsulating or de-encapsulating the frames. When a packet is sent by a wireless LAN client, the access point receives it, encapsulates it with an LWAPP header, and forwards it to the controller. At the controller, the LWAPP header is removed and the frame switched from the controller onto a Virtual LAN (VLAN) in the switching infrastructure. (Enterprise Mobility 4.1 Design Guide)

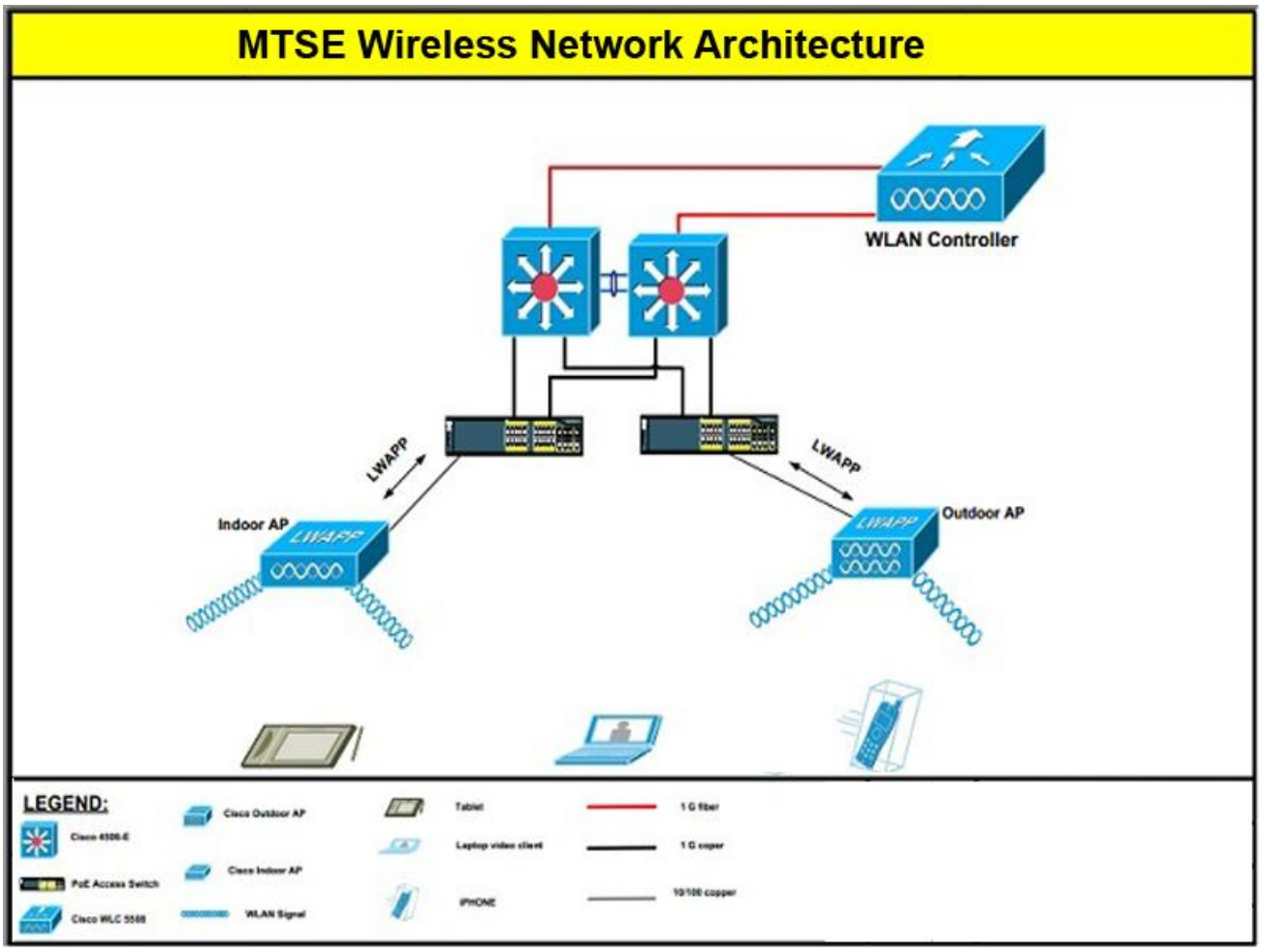

Figure 11. MTSE Wireless Network Architecture

When a client on the wired network sends a packet to a wireless LAN client, the packet first goes into the wireless LAN controller where an LWAPP header is added to it and then forwarded to the specific access point. The LWAPP header is removed from the frame by the access point, encrypted if necessary, and then bridged onto the RF medium.

There are two modes of LWAPP operations:

- LWAPP Layer 2 Transport Mode: When communication between the access point and the wireless LAN controller is in native, Layer 2 Ethernet frames, it is called Layer 2 LWAPP mode.
- LWAPP Layer 3 Transport Mode: When Control and Data messages are transported over the IP network in UDP packets, it is called Layer 3 LWAPP mode. This is the generally preferred solution, since transport architecture is inherently more flexible and scalable than Layer 2 LWAPP mode.

6 SECURITY

As stated in the previous sections, employees located at the head and branch offices and other organizations that consume data from the servers located inside the headquarters, use the system frequently. This traffic necessitates a security scheme that will ensure the integrity of the users that contribute to the traffic. Additionally, due to the sensitivity of the data handled by the system, all users accessing the network should be filtered and routed to their respective level of access.

Most of the communication between the branch offices and the head office is done through email, hence, securing the exchange server is also one of the major tasks involved.

Therefore, the Cisco ASA 5515-X series firewall is proposed. In addition to comprehensive antimalware capabilities, the Cisco ASA 5515-X optionally provides additional broad and deep network security through an array of integrated cloud and software based security services. This includes Cisco Scan Safe Cloud Web Security and the only context-aware IPS with no need for additional hardware modules. (Cisco ASA5515-K9 Firewall, 2010)

The Cisco ASA 5500 Series integrates multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec/VPN. These technologies, combined with real-time reputation technology, deliver highly effective network and application layer security, user-based access control and improved employee productivity. (Cisco ASA5515-K9 Firewall, 2010)

The firewall, as can be seen in the MTSE network architecture design (Fig. 5), will be placed interfacing Ethiopia Telecom's network, which is the Internet Service Provider, and internal LAN of MTSE.

The proposed design provides high security and scalability. That is, Cisco ASA 5515 firewall performs specific tasks.

Figure 12. Cisco ASA5515-K9 Firewall (Cisco ASA5515-K9 Firewall, 2010)

The following service will be configured in the firewall:

- Rule-based protection between zones of different security level (external, EthERnet, DMZ, Internal)
- Through access list, state-based inspection of traffic, and identification and blockage of attacks
- due to the host servers, MTSE will have a public IP, hence Network Address Translation (NAT) and Port Address Translation (PAT)
- Comprehensive Anti-Malware capabilities, including Anti-Virus, BotNet traffic filter, and Anti-Spyware
- High-performance Virtual Private Network (VPN) and always-on remote access
- ASA 5500 Strong Encryption License (3DES/AES) and it is neither per user nor per seat comes as a default configuration.

- According to Cisco, ASA 5515-K9 Firewall will have the following constituent configuration: (Cisco ASA5515-K9 Firewall, 2010)
- ASA5515-K9: ASA 5515-X with SW 6GE Data 1GE Mgmt AC 3DES/AES
- SF-ASA-8.6-K8: ASA 5500 Series Software Ver. 8.6 for ASA 5512X--5555X DES
- CAB-ACE: AC Power Cord (Europe) C13 CEE 7 1.5M
- ASA-VPN-CLNT-K9: Cisco VPN Client Software (for almost all operating systems: Windows, Solaris, Linux and MAC)
- ASA5500-ENCR-K9: ASA 5500 Strong Encryption License (3DES/AES)
- ASA-ANYCONN-CSD-K9: ASA 5500 Any Connect Client + Cisco Security Desktop Software

7 DISCUSSION AND CONCLUSION

The proposed system, upon implementation, will have an immense impact on the data exchange and communication scheme of the entire organization. Additionally, the security of the organization's network will be elevated to the current standards set by the industry.

Generally, by utilizing the proposed system, MTSE will be able to deliver flexible, scalable modest, security, a reliable effective. In addition to that, upgrading the technology will transform the work environment, boosting the workforce's productivity and morale of the staff.

8 REFERENCES

2008, J. H. (2008). *Windows Server 2008.*

Balchunas, A. (2012). *CCNP Switching Study Guide.*

Balchunas, A. (2012). *CCNP Switching Study Guide.*

Cisco ASA5515-K9 Firewall. (2010, January 15). Retrieved from www.cisco.com: http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-701253.html

Cisco. (2013, 1 1). *Cisco 200 Series Switches*. Retrieved from www.cisco.com: http://www.cisco.com/c/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369.html

Cisco. (2011, 1 1). *Cisco 2960*. Retrieved from www.cisco.com: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.pdf

Cisco. (2011, February 7). *Cisco corporation4500*. Retrieved from www.cisco.com: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/release/note/OL_24465.pdf

Cisco. (2009). *Cisco.com*. Retrieved from http://www.cisco.com/c/en/us/products/index.html

Enterprise Mobility 4.1 Design Guide. (n.d.). Retrieved December 2008, from www.cisco.com: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.pdf

Fitzgerald, J. &. (2009). *Business Data Communications and Networking (10th ed.).*

MTSE. (2013, September 12). Retrieved March 18, 2014, from http://www.skyscrapercity.com/showthread.php?t=1384524

MTSE. (1979, September 20). *MTSE*. Retrieved from http://www.ethiopianshippinglines.com.et/Agents.htm

Teare, D. (2008). *Self-Study Guide Designing for Cisco Internetwork Solutions.* Indianapolis.