

Low Level Network Design for Logistics Company

Final Year Project

Session 2016-2020

A project submitted in partial fulfillment of the degree of

BS in Computer Science



Department of Computer Science

Faculty of Computer Science & Information Technology

The Superior College, Lahore

FALL 2020

Type (Nature of project)	[☒] Development [☐] Research [☐] R&D			
Area of specialization	Computer Networks			
FYP ID	FYP19-GROUP-022			
Project Group Members				
Sr.#	Reg. #	Student Name	Email ID	*Signature
(i)	BCSM-F16-082	Hassan Hameed	Mr.hassanhameed@gmail.com	
(ii)	BCSM-F16-099	Abdullah Salik	Abdullabuttar@gmail.com	
(iii)	BCSM-F16-117	Bisma Mirza	Itxxbis7123@gmail.com	

*The candidates confirm that the work submitted is their own and appropriate credit has been given where reference has been made to work of others

Plagiarism Free Certificate

This is to certify that, I _____ S/D of Muhammad Siddique, group leader of FYP under registration no _____ at Software Engineering Department, The Superior College, Lahore. I declare that my FYP report is checked by my supervisor.

Date: _____ Name of Group Leader: _____ Signature: _____

Name of Supervisor: Miss Maryam

Co-Supervisor: Mr. XYZ

Designation: Lecturer

Designation: Associate Professor

Signature: _____

Signature: _____

HOD: Dr. Arfan Jaffar

Signature: _____

Faculty of CS & IT, The Superior College Lahore, Pakistan

Project Report

Low Level Network Design For Logistics Company

Change Record

Author(s)	Version	Date	Notes	Supervisor's Signature
	1.0		<Original Draft>	
			<Changes Based on Feedback from Supervisor>	
			<Changes Based on Feedback From Faculty>	
			<Added Project Plan>	
			<Changes Based on Feedback from Supervisor>	

APPROVAL

PROJECT SUPERVISOR

Comments: _____

Name: _____

Date: _____

Signature: _____

PROJECT MANAGER

Comments: _____

Date: _____

Signature: _____

HEAD OF THE DEPARTMENT

Comments: _____

Date: _____

Signature: _____

Dedication

*All our efforts and struggles of educational life are dedicated to our dear parents; it would never have been possible without their priceless support and prayers. We also dedicate this work to our honorable and respected teachers, especially to our supervisor **Ms. Maryam** who taught and supported us in achieving the ultimate result.*

Thanks to all teachers specially who taught us and showed us the right path.

Thank so much.

Acknowledgements

Alhamdulillah! We thanks to Allah Almighty for giving us the ability to perform the essential tasks and achieve the desired results.

We are really thankful to our teachers and huge thanks to our supervisor for her generous transfer of knowledge and uncountable support. It was a really good experience, a very memorable one, for what we are today is the hard work of our teachers and their extensive support and well wishes for us.

We are not able to achieve this goal without you MAM. Thank you, **Ms. Maryam.**

Executive Summary

Virk Logistics Company (VLC) took the decision to upgrade its network infrastructure to follow the latest trends. Right now in the current scenario their network has their own mailing server and file server. Their mailing server is managed by their separate administration team. Moreover they have basic Internet access coming directly from their head office, and also have some management software running. They have usually complains from users who are facing recurring downtime and higher latency when accessing internet due to old setup. They also faced some ransomware attacks from past few months which became an alarming risk to their data. Now company wants to get rid of these hectic situations by upgrading their entire network infrastructure and they also want to enhance their productivity and reliability along with secure environment.

In the proposed solution they will get major changes to VLC network system. The current networking equipment using in the network was end of life and end of support as well.

The proposed network infrastructure requires multiple changes that overcome these ambiguities and earlier technologies. The upcoming results have greater bandwidth, efficiency and reliability, more security and easy management & network maintenance equipment.

The latest provided hardware will use compatible and up-to-date technologies that will facilitate maintenance and troubleshooting as well as to rectify and troubleshoot the slow access times that are currently being reported.

In addition to updating the hardware, the proposed solution will also do some amendments in the device configuration. After implementation these changes will be able to deliver more reliability and security for every node of the VLC network.

Along with the updated hardware, the updated network configurations will benefit the company to explore new possibilities in using the network to increase overall productivity and at last to better serve the needs of their clients.

Table of Contents

Plagiarism Free Certificate	ii
Dedication	v
Acknowledgements.....	vi
Executive Summary.....	vii
List of Tables	xv
Chapter 1.....	16
INTRODUCTION	16
Introduction	14
1.1 Existing System / Competitive Analysis.....	14
1.2 Problem Statement	15
1.3 Proposed Solution	15
1.4 Scope of the Project	16
1.4.1 WAN Module:.....	16
1.4.2 Service Module:	16
1.4.3 Server Farm Module:	17
1.4.4 Internet/DMZ Module:	17
1.4.5 Branch Connectivity Module:.....	17
1.5 System Architectural Design	17
1.6 Implementation Tools and Techniques.....	18
1.7 Project Plan	18
1.8 Work Breakdown Structure	19
1.8.1 Preparation	19
1.8.2 Planning	19
1.8.3 Design	19
1.8.4 Implementation	19
1.9 Roles & Responsibility Matrix:	19
1.10 Gantt Chart	24
Chapter 2.....	25
NETWORK REQUIREMENTS	25
2.1 Introduction.....	26
2.2 Functional Requirements:	26
2.3 Non-Functional Requirements:	27
2.4 Adopted methodologies.....	28
2.4.1 Prepare Phase:	28
2.4.2 Plan:	28
2.4.3 Design Phase	28

2.4.4	Implementation Phase	29
2.4.5	Operate Phase	29
2.4.6	Optimize Phase	29
2.5	Scope	31
2.6	OSI model	31
2.7	Benefits of OSI Model	31
2.8	OSI Layers and VLC Project Scope	32
2.8.1	Application Layer	32
2.8.2	Presentation Layer:	32
2.8.3	Session Layer:	33
2.8.4	Transport Layer Protocol:	33
2.8.5	Network layer:	33
2.8.6	Data Link Layer:	34
2.8.7	Physical Layer:	34
2.9	Scope of the Project	34
2.9.1	Project Scope of Virk Logistics:	35
2.10	Virk Logistics Company Security Integrity:	35
2.10.1	Existing Case:	35
2.10.2	Proposed Case:	35
2.11	Virk Logistics Failover and Redundant uplink	36
2.11.1	Existing Case:	36
2.11.2	Proposed Case:	37
2.12	SD-WAN	37
2.13	Routing	37
2.13.1	Existing Case:	37
2.13.2	Proposed Case:	37
2.14	Switching:	38
2.15	Users	38
2.16	Wireless Access:	38
2.17	Cameras:	38
2.18	Data Center:	38
2.19	Applications:	38
Chapter 3		40
PROJECT SURVEY REPORT & ANALYSIS		40
3.1	Executive Summary:	41
3.2	Participants:	41
3.3	Methodology:	41
3.4	Results:	41

3.5	Physical Design	41
3.6	Hardware Technical Specifications	42
	Hardware Description	42
	Firewall.....	43
	Firewall Name: FG-60E-BDL	43
3.7	Firewall connectivity in VLC Environment:	44
3.8	Core Switches	45
3.8.1	Core switch 1 3750G-24T:.....	45
3.8.2	Port:.....	45
3.8.3	V-LAN	46
3.8.4	Mode:.....	46
3.9	Core Switch 1 Connectivity:	46
3.10	Core Switch 2 Connectivity:.....	47
3.11	Access Switches	48
3.11.1	Model:.....	48
3.11.2	Benefits:	48
3.12	Access Switch 1:.....	49
3.13	Access Switch 2:.....	49
3.14	Access Switch 3:.....	51
3.15	Access Switch 4:.....	52
	Chapter 4.....	53
	NETWORK SECURITY	53
	PLAN.....	53
4.1	Plan	54
4.2	Tools	54
4.3	Network Connectivity:.....	55
	Switch 1.....	55
	Switch 2.....	56
	Switch 3.....	56
	Switch 4.....	56
	Core 1.....	56
	Core 2.....	56
4.4	Network Security Integration Plan	57
4.4.1	Firewall.....	57
4.4.2	Network Security Plan (Policy Map).....	58
4.5	Applied Services protocols	59
	DNS:.....	59
	IMAP:.....	59

POP3:.....	59
LDAP:.....	59
FTP:.....	59
TFTP:.....	60
HTTPS:	60
TCP:	60
UDP:	60
4.6 Firewall Address	60
4.7 Overview:	61
4.8 Forti-Gate in VLC's Environment.....	61
4.8.1 Traffic Policy Applied on FortiGate	62
4.8.2 Flow of traffic client V-LAN to Internet or Server V-LANs.....	62
4.8.3 Load Balancing	63
4.8.4 Forti-Gate as a Load Balancer (SD WAN)	63
4.8.5 Flow of Traffic from User to Server/Internet behind FortiGate SSD-WAN.....	64
4.8.6 Intrusion Detection/Prevention System	65
4.8.7 FortiGate inbuilt Intrusion Detection and Prevention System	65
4.8.8 Signature updates	66
Chapter 5.....	67
Experimental Structure	67
Definition	68
5.1 Existing System.....	68
5.1.1 Connectivity Overview of existing infrastructure	69
5.1.2 Problem Statement.....	69
5.1.3 Hardware.....	68
5.1.4 Core1.....	68
5.1.5 Core2.....	74
5.1.6 Access Switch1 (HR_MKT_VM)	78
5.1.7 Switch 2(EX_MGR_FIN_IT)	76
5.1.8 Access Switch 3 (Camera_WIFI)	77
5.1.9 VLC Gateway	81
5.1.10 HO_GW_1	88
5.1.11 HO_GW_2	91
5.1.12 VLC-EDGE-FW.....	93
5.1.13 Protocols following in existing environment	94

5.1.14	OSPF	96
5.1.15	DHCP	100
5.1.16	Spanning tree protocol	101
5.1.17	DHCP IP allocation.....	101
5.1.18	Ip Routes	106
5.1.19	Malware Protection	109
5.1.20	PING	110
5.2	Proposed Solution	117
5.3	Updated Infrastructure	118
5.3.1	Connectivity Overview of Proposed Infrastructure.....	119
5.3.2	Hardware	119
Firewall.....		120
5.3.3	Firewall connectivity in VLC Environment	121
5.4	Core Switches	122
5.4.1	Core switch 1 3750G-24T:.....	122
5.4.2	Port:.....	122
5.4.3	V-LAN	122
5.4.4	Mode:.....	123
5.5	Core Switch 1 Connectivity:	123
5.6	Core Switch 2 Connectivity:	111
5.7	Access Switches.....	121
5.7.1	Model: Cisco Catalyst 2960G-24TC-L Switch.....	121
5.7.2	Benefits:	121
5.8	Access Switch HR_MKT	121
5.9	Access Switch MGR_VM_EX.....	125
5.10	Access Switch FINANCE_IT	128
5.11	Access Switch Camera_WIFI	127
Chapter 6.....		129
Results and Conclusion		129
IPSEC VPN.....		139
CORE TO HEAD OFFICE PING.....		140
HEAD OFFICE TO CORE PING.....		141
MALWARE DETECTION.....		141
POLICIES		143
REFERENCES.....		152

List of Figures

Figure 1 Existing System Topolgy View	14
Figure 2 Proposed Solution Topology View	18
Figure 3 VLC Work Breakdown	24
Figure 4 Physical Diagram of Lahore Branch	42
Figure 5 Existing topology of VIRK LOGISTCS	68
Figure VII: HR_PC_1	102
Figure VIII: MKT-PC-1	102
Figure IX: VM-PC-1	102
Figure X: WIFI_CAM	103
Figure XI: EXECUTIVE-PC-1	103
Figure XII: FINANCE-30.....	104
Figure XIII: IT-PC-1.....	104
Figure XIV: EX-MGR-FIN-IT	105
Figure XV: CAMERA-WIFI	105
Figure XVI: HR-MKT-VM	106
Figure XVII: Core1	106
Figure XVIII:Backup_Core1.....	107
Figure XIX: VLC_Gateway.....	107
Figure XX: HO_GW_1	108
Figure XXI: HO_GW_2	109
Figure XXII: VLC-EDGE-FW.....	109
Figure XXIII: HR-PC-1 PING	110
Figure XXIV: CORE1_PING	110
Figure XXV:HR-PC-1 PING.....	111
Figure XXVI: MKT-PC-1 PING	111
Figure XXVII: VM-PC-1 PING.....	112
Figure XXVIII:EXECUTIVE-PC-1 PING	112
Figure XXIX: FINANCE_PC_1 PING.....	113
Figure XXX: IT-PC-1 PING.....	113
Figure XXXI: HR-PC-1 PING	114
Figure XXXII: MKT-PC-1 PING	114
Figure XXXIII:VM-PC-1 PING.....	115
Figure XXXIV: EXECUTIVE-PC-1 PING	115
Figure XXXV: FIREFOX-30 PING	116
Figure XXXVI: IT-PC-1 PING	116
Figure XXXVII: FILESERVER PING	117
Figure XXXVIII: New Solution for VLC.....	118
Figure XXXIX: Old ICMP	127
Figure XL: New ICMP	128
Figure XLI: HR_MKT_SW	130
Figure XLII: VM-OFFICER-SW.....	131
Figure XLIII: CAMERA	132

Figure XLIV: FINANCE-IT-SW	133
Figure XLV: HR-PC-1	133
Figure XLVI: Marketing-PC-1	134
Figure XLVII: EXEC-PC-1	135
Figure XLVIII: MGR-PC-2	135
Figure XLIX: VM-PC-1	135
Figure L: Camera_WIFI_PC-1	136
Figure LI:FIN-PC-1	136
Figure LII: IT-PC-2	137
Figure LIII: CORE1	138
Figure LIV: SKP_EDGE_FIREWALL	138
Figure LV: HO_EDGE_FIREWALL	138
Figure LVII: HO_EDGE_FIREWALL	139
Figure LVIII: SKP_EDGE_FIREWALL	140
Figure LVIII: Core1	140
Figure LIXIV: FileServer	141
Figure LXV: HR_PC_1	142
Figure LXVI: SKP_EDGE_FIREWALL	142
Figure LXIIIVII: SKP_EDGE_FIREWALL	143
Figure LXIIIVIII: HO_EDGE_FIREWALL	144
Figure LXIVIX: Any PC from SKP Branch	145
Figure LXVX: Any PC from SKP Branch	145
Figure LXVIXI: Firewall logs	146

List of Tables

Table 1 Roles & Responsibility Matrix	23
Table 2 proposed Hardware	43
Table 3 Firewall Connectivity in VLC Environment	44
Table 4 Core Switch 1 Connectivity	47
Table 5 Core Switch 2 Connectivity	48
Table 6 Access Switch 1	49
Table 7 Access Switch 2	50
Table 8 : Access Switch 3	51
Table 9 Access Switch 4	52
Table 10 Network Plan	57
Table 11 Firewall Policy table	58
Table 12 Firewall Filter Table	61
Table 13 Hardware of Existing System	68
Table 14 Configuration of Core1	69
Table 15: Configuration of Core2.....	75
Table 16: Configuration of Access Switch1(HR_MKT_VM).....	78
Table 17: Configuration of Switch2(EX_MGR_FIN_IT).....	76
Table 18: Access Switch3(Camera_WIFI).....	77
Table 19:Configuration of VLC Gateway	80
Table 20: Configuration HO_GW_1	89
Table 21: Configuration of HO_GW_2	91
Table 22: Firewall Connectivity in HO	93
Table 23: List of hardware in new infrastructure	120
Table 24: Firewall Connectivity in VLC Environment	121
Table 25:Core Switch 1 Connectivity	124
Table 26: Core Switch 2 Connectivity	111
Table 27: Access Switch 1 Configuration	122
Table 28: Access Switch 2 configuration.....	126
Table 29: Access Switch 3 Configuration	129
Table 30:Access Switch 4 configuration	127

Chapter 1

INTRODUCTION

Introduction

This project would be on an IT infrastructure of an organization (Logistics Company). It's a real time project that will be mirrored on simulator to understand the working of an enterprise network. All the information of organization would be collected from their IT experts. The objective is to provide them more reliable and secured network. The scope of this project is to multiple branches present on remote location by using Hub and Spoke architecture. Moreover, the technique of 3 tier architecture will be used to make it more scalable for future purpose.

1.1 Existing System / Competitive Analysis

Currently, VLC network can be considered as having a centralized model. The following figure provides a high level overview of VLC's existing network topology:

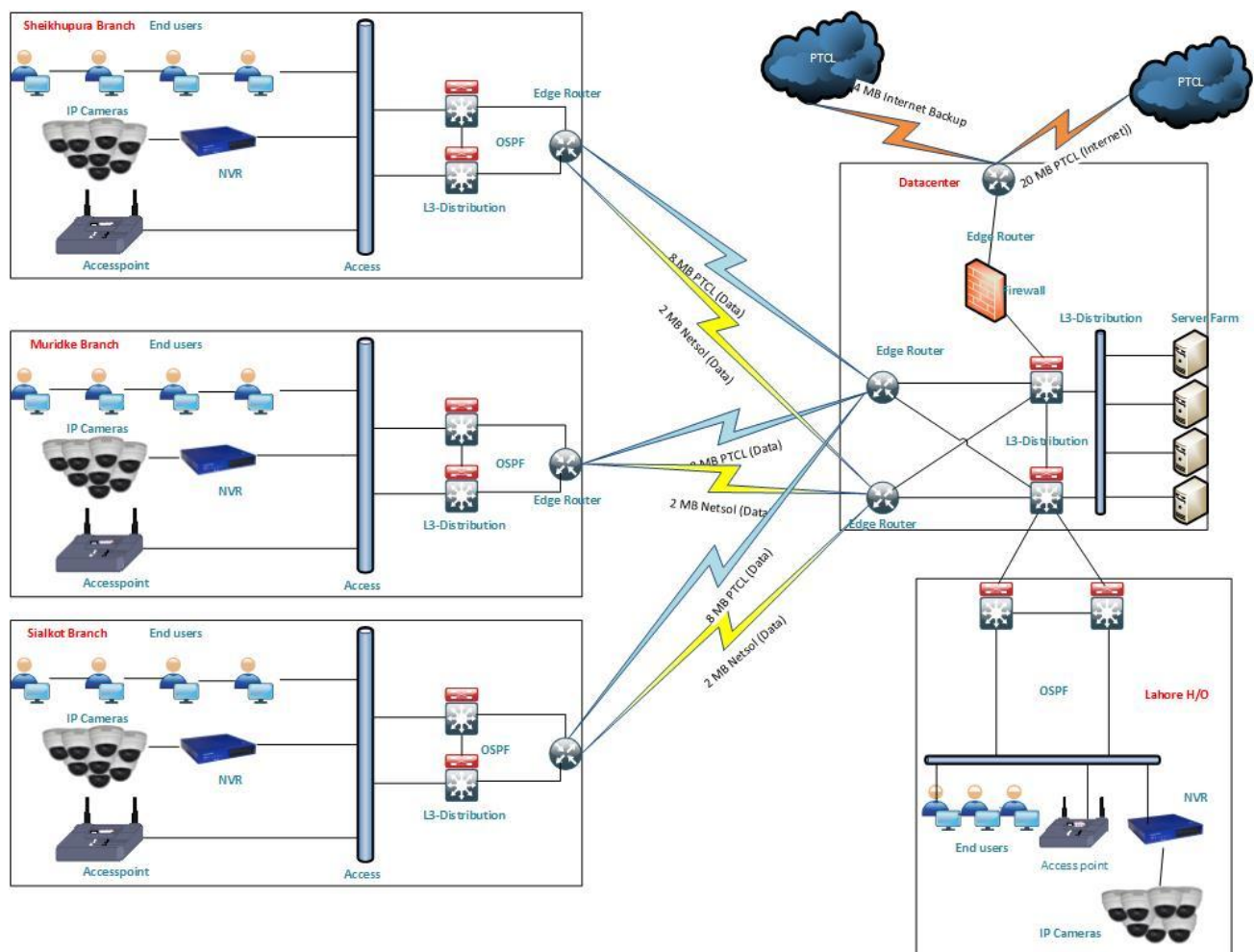


Figure 1 Existing System Topology View

1.2 Problem Statement

As the technology is increasing day by day it's getting worse to follow some traditional methods of maintaining and securing network. Often, we use devices without having the detailed knowledge and not getting as much they are designed for, which may lead to more investments and increasing risk of attacks and exploitation. Taking it to another note it's compulsory to make it legit by utilizing available viable resources to meet the goal of maximum throughput with minimum bandwidth by state of the art resource allocation techniques. Following are the major issues running in most of the organizations.

- Complex configurations
- Complex policy management
- Less scalable
- Expensive solutions
- Lack of Qos
- Old traditional security methods
- Unavailability of complete UTM Solutions
- Lag in availability
- Manually changing in connections during network failure

1.3 Proposed Solution

By considering the above-mentioned problems, the goal is to achieve the availability, Data Integrity and confidentiality is by using following techniques

- Concise configurations by modifying protocols
- Policy Management by using ACLS and Firewall policies
- More scalable network by using 3 tier architecture of Access, Distribution and Core methodologies
- Make sure the QOS and TOS by priority que management system.
- More advanced security solutions by using next generation firewalls
- Proposing reliable and dedicated devices to the specified purpose like scenario-based solutions.

- Utilizing minimum devices, performing maximum job which they have actually designed for.
- Ensure 24/7 availability by means of creating failover
- Equal load balancing for utilizing every available resource

1.4 Scope of the Project

A typical Enterprise network has many functional modules and layers. VLC's network can be viewed as composed of following functional modules:

- WAN Module
- Core Switching Module
- Server Farm Module
- Internet
- Branch Connectivity

1.4.1 WAN Module:

The WAN module is where the customer's remote offices and branches connect to access services published in VLC's Datacenter.

A pair of Cisco routers at VLC's Datacenter represents WAN layer Module, they interconnect the data center with Virk Logistics network core by using lease line from PTCL and Netsol connection as a backup. The connection is used for accessing data directly from VLC's Data Center through extended LAN connection.

1.4.2 Service Module:

Service Module of the Data Center is consist of core switching, security and application content awareness components. Existing Data Center does not have all the components of the Service modules. It only has core switching module.

Core switching module within data center represents Core Switching layer where Access Network, WAN Access Layer and Internet/DMZ Access layers aggregate.

In existing VLC's Datacenter a pair of Cisco switches provides the Core Switching facilities. All Access switches, Servers Financial and non-Financial are connected to Core switches. Internet/DMZ module and WAN modules are also connected to it.

1.4.3 Server Farm Module:

Server Farm module is comprised of Access Switches which connect Servers to Service Module. The servers are physically connected to Core Switch.

1.4.4 Internet/DMZ Module:

Internet/DMZ module is the demarcation line between Public and Private Network, it contains Firewalls for protecting DC network from outside, make possible certain services availability on the Public by utilizing DMZ security layer using separate firewall which monitors the traffic pattern for any security breaches.

VLC DC has Internet link from ISP which is terminated on one of the Cisco routers. The Internet module also has a Cisco Firewall

1.4.5 Branch Connectivity Module:

Branch Connectivity module describes network from the Branch itself. Each VLC branch has two uplinks to the WAN aggregation routers from any of the available combination of following media

- PTCL
- Netsol

1.5 System Architectural Design

To incorporate new services into the existing Data Center the network topology will be changed according to the following overall diagram.

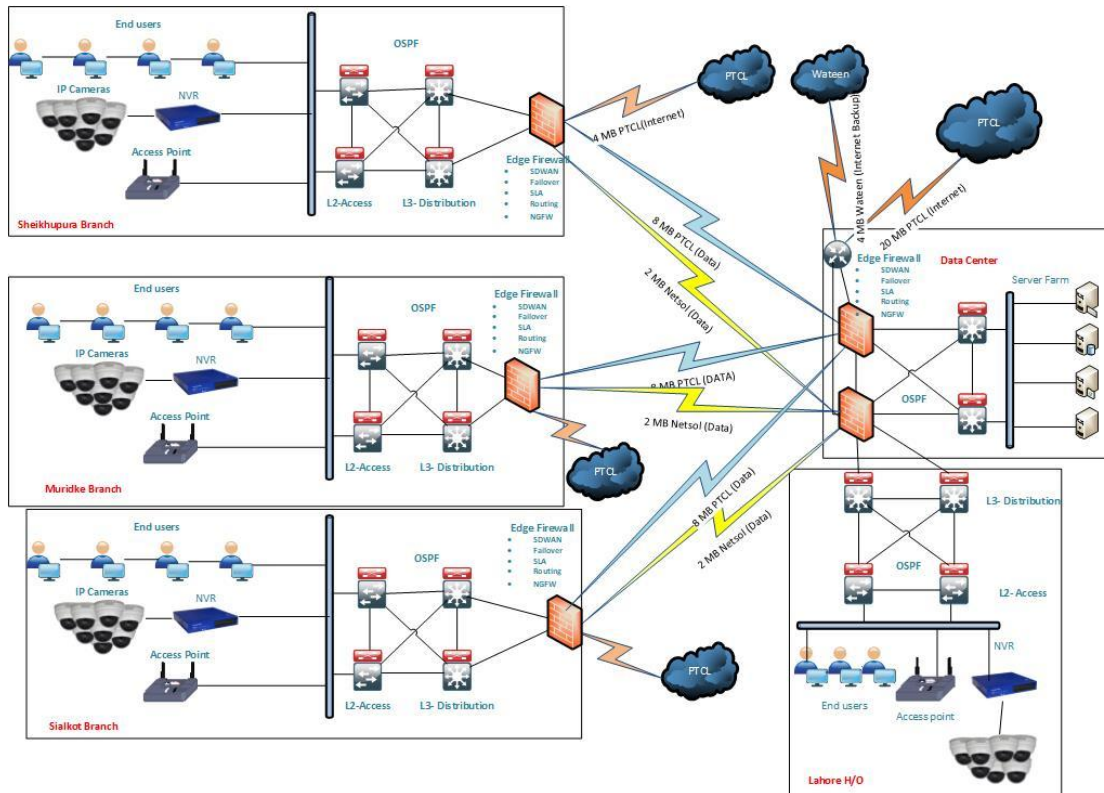


Figure 2 Proposed Solution Topology View

1.6 Implementation Tools and Techniques

Site Survey and Data Collection: Microsoft Excel, Microsoft Word.

Questionnaires: Microsoft Office, Google Forms.

Topology Design: Microsoft Visio.

Implementation/Prototyping Tool: Cisco Packet Tracer, GNS 3, Original IOS with VMware.

Testing of modules: Wireshark, GNS 3, VMware.

1.7 Project Plan

As it's a real time project so all the work breakdown is on the approval of company.

1.8 Work Breakdown Structure

1.8.1 Preparation

- 1.8.1.1 Questionnaire
- 1.8.1.2 Site Survey
- 1.8.1.3 Establish Organization & Business requirements
- 1.8.1.4 Charter Signed

1.8.2 Planning

- 1.8.2.1 Characterizing existing network
- 1.8.2.2 Identifying Network & User requirements
- 1.8.2.3 Analysis of installed network areas
- 1.8.2.4 User's identification about network service requirements.

1.8.3 Design

- 1.8.3.1 Network Analysis
- 1.8.3.2 Testing of each module
- 1.8.3.3 Creating VLC network Physical Design
- 1.8.3.4 Creating VLC network Logic Design
- 1.8.3.5 Security analysis
- 1.8.3.6 Proposed Solution

1.8.4 Implementation

- 1.8.4.1 Pre-implementation (during off hours).
- 1.8.4.2 Post-implementation (during normal hours).
- 1.8.4.3 Testing.

1.8.5 Statistical Analysis

- 1.8.5.1 Compare before and after results.
- 1.8.5.2 Training.

1.9 Roles & Responsibility Matrix:

The purpose of roles & responsibility matrix is to identify who will do what.
Faculty of CS & IT, The Superior College Lahore, Pakistan

WBS #	WBS Deliverable	Activity #	Activity to Complete the Deliverable	Duration (# of Days)	Responsible Team Member(s) & Role(s)
1.8.1.1	Questionnaire	1	Questionnaire design and response time	5	Bisma ,Hassan Abdullah
1.8.1.2	Site Survey	2	Visit to the site for complete details	10	Bisma ,Hassan Abdullah
1.8.1.3	Establish Organization and business requirements	3	Understand business requirements	5	Bisma ,Hassan Abdullah
1.8.1.4	Charter signed	4	Meeting with the IT Board & Executives	5	Bisma ,Hassan Abdullah
1.8.2.1	Characterizing existing network	5	Segregation of network in depth	10	Bisma ,Hassan Abdullah
1.8.2.2	Identifying network and user requirements	6	Questionnaire analysis and meeting with end users	5	Bisma ,Hassan Abdullah
1.8.2.3	Analysis of installed network areas	7	Network installed areas will be analyze	10	Bisma ,Hassan Abdullah
1.8.2.4	Identification of user who will require network services	8	Breakdown on the basis of users	5	Bisma ,Hassan Abdullah
1.8.3.1	Network Analysis	9	Previous network study	10	Bisma, Hassan Abdullah
1.8.3.2	Testing of each module	10	Testing on sites	5	Bisma ,Hassan Abdullah

1.8.3.3	Creating VLC network Physical Design	11	Design proposal of physical design	15	Bisma ,Hassan Abdullah
1.8.3.4	Creating VLC network logical Design	12	Design proposal of Logical design	15	Bisma ,Hassan Abdullah
1.8.3.5	Security Analysis	13	Measuring security throughput	15	Bisma ,Hassan Abdullah
1.8.3.6	Proposed solution	14	Design solution and propose to the VLC/ approval required	10	Bisma ,Hassan Abdullah
1.8.4.1	Pre implementation (During off hours)	15	Initial Implementation on off days	10	Bisma ,Hassan Abdullah
1.8.4.2	Post Implementation (During normal hours)	16	Implementation during working days	10	Bisma ,Hassan Abdullah
1.8.4.3	Testing	17	Testing each module	5	Bisma ,Hassan Abdullah
1.8.5.1	Compare before and after results	18	Statistical analysis and report	7	Bisma ,Hassan Abdullah
1.8.5.1	Training	19	Training to the new devices	2	Bisma ,Hassan Abdullah

Table 1 Roles & Responsibility Matrix

1.10 Gantt Chart

VLC Network Breakdown



Figure 3 VLC Work Breakdown

Chapter 2

NETWORK REQUIREMENTS

2.1 Introduction

It was needed to get previous data about hosts and previous devices working on the infrastructure to create the topology for better understanding. Datasheet is created to record the data. Furthermore, It will help the network designer to understand what actually equipments were being used and what will need in future for better network support for its growth. The basis of the new network design is in view of the Network Up gradation & Security methodologies rollout and emphasizes on following requirements.

2.2 Functional Requirements:

- Core Switch Configuration for unauthorized access
- Core Switch Configuration for Telnet/SSH (Remote) Access
- Core Switches Stack Configuration
- Configuration for automatically backups for switches configurations
- V-LAN Creation for each subnet
- Routing Configuration for each network (i.e. routing for site to site communication)
- NTP Configurations
- TFTP Configurations
- Broadcast Storm Control
- Spamming Control
- DDOS Attack Control
- Creation and Implementation of ACL (Access Control Lists) for each V-LAN/subnet
- Implementation of ACL (Access control Lists) as per company's Requirement
- AAA Model Configuration
- Access Controller
- Identification and Authentication
- System and communication protection
- System and information integrity
- Application Control
- Intrusion prevention system

- Threat Protection System
- Antivirus
- URL Filtering
- Web Filtration
- Sandboxing
- SSL Inspection
- IPsec VPN Tunnel
- Traffic shaping and bandwidth management
- Disaster Recovery & Incident Response
- Management Control and Procedures
 - Risk Assessment
 - End point security
 - Audit planning and accountability
 - Traffic Logging and Monitoring

2.3 Non-Functional Requirements:

- **Functionality**

The design should meet the functionality requirements of ERP and Internet applications.

- **Scalability**

Scalability is an important aspect of any design and consequently is given adequate focus in Virk Logistics network design.

- **High Availability**

Data Center Network should be designed in such a manner that access to critical Finance and Vehicle Tracking applications should be maintained in case of devices failures or even in case of main data center failure.

- **Data Center Security**

Data Center application resources should be protected and secured by deploying a layered security infrastructure.

- **Infrastructure Security**

All devices should be deployed following infrastructure security best practices.

- **Performance**

The new design should meet the performance requirements and provide QOS by managing bandwidth utilization and throughput.

- **Reliability**

The enterprise security solution should be reliable by traffic & event logging, backups and defensive by using up to date security standards and licenses.

2.4 Adopted methodologies

2.4.1 Prepare Phase:

In this phase we collected the information regarding to the current network of Virk Logistics Company. Multiple meetings and site visits were conducted to understand the actual case and after this phase we stepped towards the next phase

2.4.2 Plan:

In this first phase, We will achieve network goals by identifying the network requirements utilizing the gathered data to install the network and which network requires what network services. Precisely we need to know where to install which network and which network was working before. This will help to manage the project responsibilities, tasks, resource management and its critical milestone to implement on the changes of network. Network requirements is the output of this phase.

2.4.3 Design Phase

After working on plan phase, here comes the design phase in which implementing the initial requirements according to plan phase. A complete contingent of network design is produced that will relay on all technical requirements, in-cooperate specifications and working business scenarios to provide security, performance, reliability and availability.

2.4.4 Implementation Phase

The most important phase is implementation, After completing and approving the plan and design phase, Implementation phase begins. A goal without disrupting the previous network, implement the integrating devices according to design phase.

2.4.5 Operate Phase

Operation is the final test of the design's appropriateness. The Operate phase involves maintaining network health through day-to-day operations. In daily lifecycle's operations, detecting faults and making correction and performance monitoring gives the initial data of network.

2.4.6 Optimize Phase

Optimize phase is station on enterprise network management, The aim of it is to find out and solves issues before actual problem in network arises and to prevent it from any affect. It may need to re-design the network if there are a lot of changes needed or errors occurred, if it is specified to support technical and organizational requirements.

Following are the basic methodologies to ensure all complete ingress and egress security profiles with an upgraded network:

- 1. Network Architecture:** An initial concern to understand the network is to follow its architectural style. Here we are using is the Hub & Spoke Architecture where hub holds the Data Center of an organization and the remaining spokes connects via SD-WAN connection. The architecture of each branch is similar except head office. Architecture of VLC is discussed at above cases.
- 2. Communication setup:** Router and switches plays a major role for communication at enterprise networks. A router connects devices within a network by sending data packets between them. This data can be sent between devices, or from devices to the internet. The router does this by assigning a local IP address to each of the devices on the network.

A switch is a multiport network bridge that uses media access control addresses to forward data at the data link layer of the OSI model. Such switches are commonly known as layer-3 switches or multilayer switches.

3. **Firewall:** To prevent from any cyber attack the defensive line is firewall which is recommended by FCC (Federal Communication Commission). We will use Fort i-Gate NGFW (A market leading brand) to deploy all the security measures from single glass of pane. Firewall came up with Complete UTM Bundle and 1-3 years of free license.
4. **Documentation:** Documentation is a key component of network security rules and policies to be implemented which includes all the cyber security best practices. Traffic monitoring, reports and syslog also included for weekly security audits perform by organizations IT administrator.
5. **BYOD Plan:** Bring your own device is now in trends and according to Tech Pro Research 2016 BYOD. Technology developed rapidly and abrupt increase in wearable's i.e wireless hand frees, smart watches and other equipments with wireless capability, it is need of policy to include such devices.
6. **Educating Employee:** With the enhancement in technologies the cybercrimes are more activist than before so that it is necessary to take precautionary measures to prevent any lose and must a sign of each employee with stating that he is well known to terms and conditions if he/she doesn't follow security measures then employee is held accountable of any lose.
7. **Password Updatons:** According to Verizon-2016 Data-Breach-Investigations Report, it is stated that 63% of data breaches because of weak passwords, stolen or lost. Company will ensure all the employees should enforce the best practices to change the passwords every 60 to 90 days.
8. **Regular backup:** Backing up word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files is recommended to deal with any Data Loss. Data would sync and regularly backup on cloud storage.

9. Endpoint Security: Server/Client Anti malware licensed security tools will be used to extend the internet security policies.

10. Multifactor Authentication: East Regional Director and Azure Infrastructure Services at Microsoft Matt Littleton Cyber security said using numerous types of identification settings on email products and most major networks are simplest to do and gives more kind of protection. He also suggests that using cell numbers of employees' as a second form, because it is not possible that theft has both password or pin.

2.5 Scope

To better understand the scope of a network architecture first we have to understand the OSI model. Following are the basic features of an OSI model and after that we have discussed our project in reference to an OSI Model:

2.6 OSI model

OSI model is a considered as a backbone on networking so for newbie this is the first thing to be learnt to proceed further in this field. It is divided into seven layers, Layer 1 from bottom considers as the lower layer and then going upward to layer 7 considers as highest layer. Somehow it co-relates with each other. Basically, it is a concept of splitting a communication between these 7 layers. It is quite helpful for troubleshooting for network problems.

2.7 Benefits of OSI Model

The main purpose of OSI model is to make communication between two devices whether operated from different platforms; it is all about how protocols works. For communication first four layers are used from top to bottom and rest three use for networking.

- Plethora number of choices for customers to use any kind of manufacturer hardware because all kind of hardware's and software's work together.
- It is convenient because it does work on multiple platforms.
- It is easy for users to understand functional and networking terms.
- Every layer has its own functionalities which ensure the networks to work without any fault or error.
- It also plays role in securing the data by encryption and decryption. Message or data

move from one place to another in securable mode.

2.8 OSI Layers and VLC Project Scope

This project is mainly focused on the implementation of firewall to achieve the higher security ratings and also on the QoS of Bandwidth and traffic shaping to deliver the valuable result on a security and better speed.

2.8.1 Application Layer:

The application layer is the top of the OSI model. It is the layer through which users interact. It provides services to the user.

When we implement Forti Gate firewall in an existing environment it will provide the following facilities and security on an application layer.

Our deployed firewall will be able to detect the threats by inspecting through particular running protocols like

- FTP: Stands for File Transfer Protocol. It is used to send or receive files in multiple computers through network.
- DNS: Stands for Domain Name System, preferable use for converting alphabets words to numbering ip addresses.
- HTTP: Hyper Text Transfer Protocol. Which is used for transferring information like document, file, image, video between computers over internet.
- HTTPS: The purpose of HTTPS is to ensure the protection, integrity, and privacy of the data exchanged between a server and a client.

This process also allows for the use of deep packet inspection and the sharing of functionality with Intrusion Prevention Systems (IPS).

2.8.2 Presentation Layer:

The presentation layer ensures that the communications passing through are in the appropriate form for the recipient. For ensuring VLC network security at presentation layer the services of SSL inspection will be enabled on flow-based mode of firewall.

SSL: stands for Secure Socket Layer is used to create an encrypted channel between the client

and the server. Transmission of such data as credit card details, account login information, any other sensitive information has to be encrypted to prevent eavesdropping.

For all SSL encrypted content in VLC network we will use full SSL inspection or deep inspection. When full SSL inspection is used, the Forti-Gate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The Forti-Gate then re-encrypts the content, creates a new SSL session between the Forti-Gate.

2.8.3 Session Layer:

The session layer establishes, controls, and ends sessions occurring between communicative applications. For VLC network suggested firewall is able to create more than required sessions to fulfil the speed necessities. Suggested firewall is able to create 1.3 Million concurrent sessions of tcp and the speed of new sessions 30,000/sec which is enough for a company's running applications.

2.8.4 Transport Layer Protocol:

The transport layer is represented by two protocols TCP and UDP. The IP protocol in the network layer delivers a datagram from a source host to the destination host. By delivering security in VLC network TLS is a most important feature to ensure the tag of security for improvement in security, FortiOS 6.0.6 uses the ssl-min-proto-version option to control the minimum SSL protocol version used in communication between Fort I Gate and third-party SSL and TLS services.

2.8.5 Network layer:

- Internet Protocol (IP) is the primary part of the Network Layer of the OSI Model that is responsible for routing traffic across network boundaries. It is the protocol that is responsible for addressing. For VLC network firewall is also utilized to get full functionalities of layer 3
- Failover: SD-WAN, advanced routing, and WAN optimization capabilities, delivering a security-driven networking WAN edge transformation in a unified offering. Due to redundant link of Data and Internet at Virk logistics company proper failover will be

created by applying the Fort i-Gate SD-Wan feature which will enhance the productivity of a company and provide the noticeable speed and in case of any downlink it will reroute the traffic to the other active uplink so the risk of dis-connectivity is reduced to zero.

- Port Forwarding: It is basically a application of network address translation (NAT) that helps to communicate through router or firewall using one address and combination of ports number.

2.8.6 Data Link Layer:

The data link layer is used for the encoding, decoding and logical organization of data bits. Data packets are framed and addressed by this layer, which has two sublayers. The data link layer's first sublayer is the media access control (MAC) layer. It is used for source and destination addresses.

2.8.7 Physical Layer:

The physical layer of the network focuses on hardware elements, such as cables, repeaters, and network interface cards. By far the most common protocol used at the physical layer is Ethernet.

By considering volume of a VLC network Fort i-Gate 60E provides redundant interfaces to easily deal with complete connectivity.

Following are the interfaces of proposed firewall.

1. USB Port
2. Console Port
3. 1 x G E RJ 45 DMZ Port
4. 2 x G E RJ 45 WAN Ports
5. 7 x G E RJ 45 Internal Ports

2.9 Scope of the Project

This section is actually giving the information about the project's extension also the summary of the network and departments which were facing some issues. This scope section specifies that

is the new network for the project or just did the modification in the network. It also tells about the network line segments such as the the network is based on LAN, or its connectivity in regarding buildings or campuses.

2.9.1 Project Scope of Virk Logistics:

The scope of the Virk Logistics project is to update the existing LAN environment mainly focused on perimeter that connects to the head office in Lahore. The new edge firewall will be able to provide the following measures:

2.10 Virk Logistics Company Security Integrity:

2.10.1 Existing Case:

In the Existing network VLC used no security mechanism on their perimeter. The company just relied on their router security modes like AAA and ACL which does not meet the security measures parallel to the advanced technology. The obsoleted mechanism leads the company to the major risks and vulnerable for latest attack vectors. Router lack the inspection of applications and encrypted data.

- **AAA:** It is stand for Authentication, Authorization and Accounting, is a technique to track user activities by controlling their access to network resources and ip-based networks. It is commonly implemented as a dedicated server.
- **ACL:** An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination.

2.10.2 Proposed Case:

But to meet the latest trends of network security we have selected the best market leading firewall which comprises on the following features and security profiles to ensure the Integrity of data, port and packet security

1. **Firewall VPN:** Organizations select Forti-Gate scalable and high-performance Crypto VPNs to protect users from man-in-the-middle attacks and ultimately data from breaches that can occur while high-speed data is in motion. Fortinet VPN technology provides secure communications across the Internet between multiple networks and

endpoints, through both IPsec and Secure Socket Layer (SSL) technologies, leveraging FortiASIC hardware acceleration to provide high-performance communications and data privacy.

- 2. App Control and IPS:** Based on Forti-Gate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the Forti-Gate unit.
- 3. Anti Virus:** From an antivirus profile we can configure the Forti-Gate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. Firewall supports SSL/SSH content scanning and inspection.
- 4. URL Filtering:** URL filtering limits access by comparing web traffic against a database to prevent employees from accessing unproductive, harmful sites such as phishing pages.
- 5. Sandboxing:** Sandboxing is a technique in which you create an isolated test environment, a “sandbox,” in which to execute or “detonate” a suspicious file or URL that is attached to an email or any other incoming file or packet.
- 6. SSL Inspection:** By enabling this feature, it allows the Fort i-Gate firewall to filter on traffic that is using the SSL encrypted protocol. The encrypted protocols that can be inspected are: HTTPS. SMTPS.

By utilizing complete Unified Threat Management bundle firewall will be able to ensure the security integrity for VLC environment.

2.11 Virk Logistics Failover and Redundant uplink

2.11.1 Existing Case:

If the primary Data connection fails, the router automatically attempts to bring up a new link on another channel this feature is called failover. In the existing environment of VLC Two uplinks for DATA is dedicated for traffic flow towards the H/O from branch offices. But one link is always down due to manual failover methodology handled by the edge router. The team simply insert the cable of backup data link in router if one link gets down and the remaining link state

goes down so company has to pay the rent for downlink as well and was not able to utilize both link at the same time and also has to do a manual changing of uplink connections.

2.11.2 Proposed Case:

But by utilizing FortiGate SD-WAN feature in VLC network environment we will be able to ensure the High Availability of network ensuring Speed and reliability as well. This feature eliminate the high latency in the network and provide the uninterruptable communication from branch to head office providing the feel of seamless communication and also utilize both the uplinks. SD-WAN feature is further discussed.

2.12 SD-WAN

An SD-WAN solution connects users to any application wherever it resides from data center to the cloud. SD-WAN intelligently determines which path best meets the ideal performance needs for a specific application. It then routes the traffic through to the ideal WAN path.

2.13 Routing

Routing module contains existence of some routing rules.

2.13.1 Existing Case:

In an existing environment the complete routing is done on layer 3 switches where there is no concept of High Availability clusters and if one link is down traffic does not reroute to the backup router the team manually changes the port if one link or device is down. OSPF is only suitable for the large environment where thousands of communicating devices are. It uses algorithm named as a link state routing (LSR). Major problem to run the OSPF are listed below

- It requires high memory and processing requirements than RIP.
- It utilizes a high bandwidth at the initial link-state packet flooding.

2.13.2 Proposed Case:

On proposed solution the Layer 3 switches remain the same but some their configuration will be modified to achieve the better speed and performance rate. Proper High Availability cluster will be created in which if one link or device is down the traffic will automatically reroute to another link or device after maintenance the equal distribution and load balancing

Faculty of CS & IT, The Superior College Lahore, Pakistan

automatically transfer the traffic on available link. Rip protocol will be used instead of OSPF because of the following features:

- Demands lower processing and memory requirements
- Only sends updates when routing info changes and don't do flooding

2.14 Switching:

The switching scope is limited to the layer two switches of VLC environment which are actively working and has no need to some major changes

2.15 Users

There are up to 50 users at each site. 10 users in the Monitoring, 20 User for HR and marketing, 5 Managers and executives, 5 In IT Support and 10 in Finance.

2.16 Wireless Access:

Every building has a wide area lobby where wireless access to the network is needed. Company uses 2 Access points to cover its are. Each access point covered up to 400Sqft and are not controller based.

2.17 Cameras:

There are up to 15 cameras used at each site some of them are bullet camera and others are Dome but all the cameras are IP based connected with NVR and accessed from Head office.

2.18 Data Center:

Data center is located in Head Office containing File Server, Application Server and Mail Server.

2.19 Applications:

Following are the most frequent applications used by Virk Logistics:

- Microsoft Office 2013
- ERP
- Microsoft Server 2008
- Oracle

- Tracking Applications

The necessary equipment and suitable topology require for the network design of the branch. Such as secure wireless access, internet sharing, IP address management, features and services. All kind of material bills must added along with authorized products from Microsoft, Cisco, Hikvision, Fortinet, and 3M.

Chapter 3

PROJECT SURVEY REPORT & ANALYSIS

3.1 Executive Summary:

After gathering requirements (Functional, Non-Functional) from VLC, team scheduled the survey to understand nature of robustness of breaches in the network for analysis and further strategic up gradation plan. After permission letter from university team visited VLC for data gathering and conducted survey from employees of their multiple sites through Google forms online link. In this document we will further elaborate final report after analysis of current problem.

3.2 Participants:

- 6 Executives from all sites.
- 12 Managers from all sites
- 33 employees of different scale from all sites.

3.3 Methodology:

The Survey was conducted by keeping Quantitative approach using forms.google.com.

3.4 Results:

According to the survey report, It comes to know that about 60% users experienced a security breach which effect the user information in past 5 years. Mostly users prefer wireless connection and they often change security settings. There are about 33.3% guests who can easily have access to the network while sharing files. Their networks are most affected with Trojans, hackers attack and viruses, they have a formal documented security file but unfortunately half of them had not understood properly.

3.5 Physical Design

Two Core switches are the heart of the network at each site connecting different functional modules. Switches has uplink to the firewall which further route the traffic to internet and data (Extended LAN links). All the physical diagrams on every site is similar so following is the generic diagram of VLC Networking infrastructure.

Following is the Physical Diagram for Lahore Branch

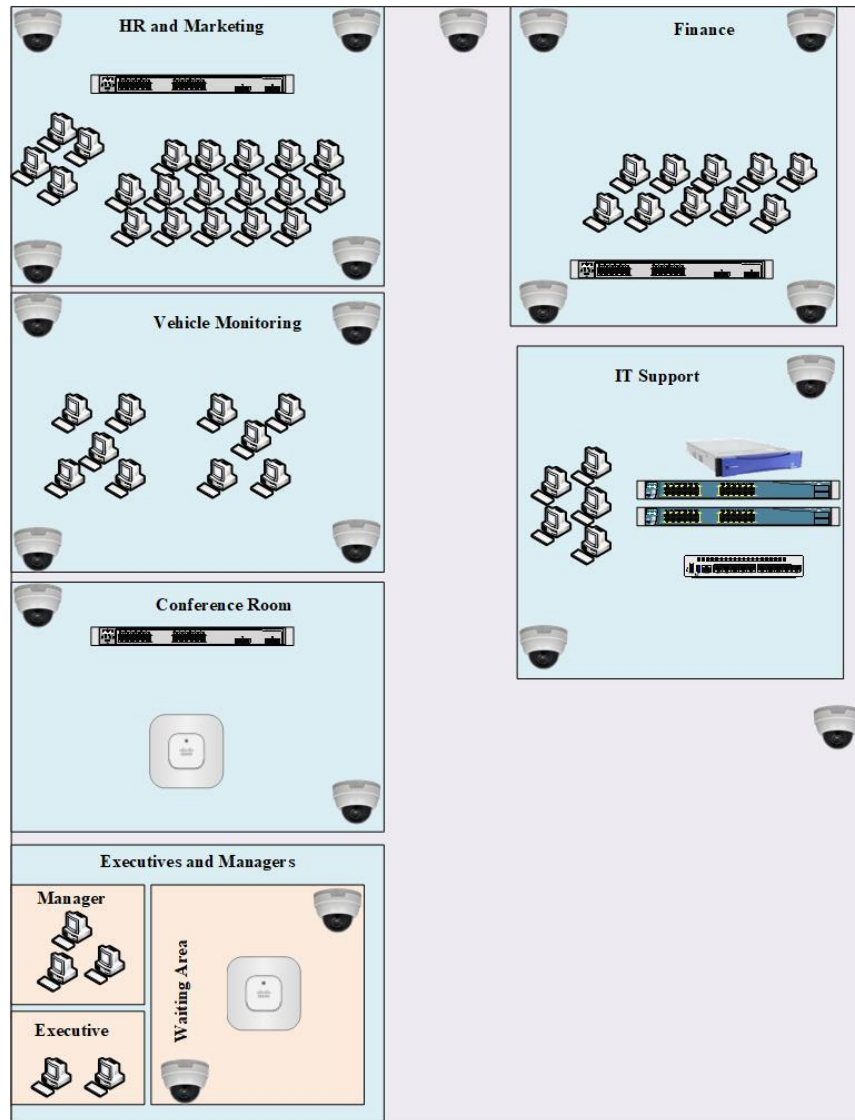


Figure 4 Physical Diagram of Lahore Branch

3.6 Hardware Technical Specifications

Hardware Description

For the sake of completeness general hardware description of the equipment procured as part of the VLC center resiliency project will be provided in this section.

S. No.	Product	Description	Qty
	Switch(L-2)		
1	WS-C2960G-24TC-L	Cisco Catalyst 2960G Switch 20 x 10/100/100 Gigabit Ethernet Ports (Non-PoE) - 4 x Dual Purpose Port - LAN Base Image	12
2	WS-C2960X-24PS-L	Cisco Catalyst Switch 2960X switch 24 x 10/100/1000 Gigabit PoE Ethernet Ports - 4 x SFP Uplinks - LAN Base Image	4
	Switch(L-3)		
3	WS-C3750G-24TS-S	Cisco Catalyst 3750G Switch includes 24 x 10/100/1000 Ports - 4 x SFP Ports - Standard Image	8
	Firewall		
4	FG-60E-BDL	FG-60E-BDL Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection.	3
5	FG-200E-BDL	Fort i-Gate-200E-BDL Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection	1

Table 2 proposed Hardware

Firewall

Firewall Name: FG-60E-BDL

This firewall actually delivers the information all over the network in a secured way, it is considered as a backbone of any securable communication, and its operating system is only made for this security and privacy for advanced security threats and attacks. It represents in networking appliances industry as a family of firewall at enterprise platforms. Forti-Gate is actually base on Forti-ASIC, It produces low latency and gives high throughput just because of its purpose-built integrated architecture in security effective industry. The Forti-Gate 60-E series contains networking functionality and consolidated security for targeted distributed enterprises.

Interfaces

- i. Console-Port
- ii. 1 x GE-RJ45 DMZ Ports
- iii. 2 x GE-RJ 45 WAN Ports
- iv. 7 x GE-RJ 45 Internal Ports

Powered by FortiASIC- SoC3

- Combines a RISC-based CPU with Fortinet's proprietary FortiASIC™ content and network processors for unmatched performance
- It helps small networks to design appliance and enable performance breakthrough.
- For maximum throughput, it supports firewall-acceleration for all kind of packet sizes.
- For protection and vital performance ot delivers accelerated TUM content.
- Increases VPN working for quality speed and remote access.

3.7 Firewall connectivity in VLC Environment:

Following is the port connectivity of firewall how all the ingress devices terminate on firewall and from which links the firewall reroutes the traffic toward a defined destination.

Port	Description	IP
Wan 1	Connected with PTCL (Internet)	192.168.10.10/24
Wan 2	Reserve	-
1	Connected with Core Switch 1	10.10.10.2/24
2	Connected with Core Switch 2	10.10.11.2/24
3	Connected with PTCL (Data)	172.11.5.2/16
4	Connected with Netsol (Data)	172.20.20.2/16
5	Reserve	
6	Reserve	
7	Reserve	
8	Reserve	

Table 3 Firewall Connectivity in VLC Environment

- Wan 1 port is directly connected with PTCL internet uplink assigned an IP of class C which is 192.168.10.10
- Wan 2 port is reserved for future use if the branch site also get the redundant internet link.
- 1 port is directly connected with core switch 1 having face into the ingress interface of a network containing an IP address of /24 which is 10.10.10.2.

- 2 port is directly connected with core switch 2 having face into the ingress interface of a network containing an ip address of /24 which is 10.10.11.2.
- 3 port is connected with the lease line provided by PTCL which extended the lan of a branch site to the H/O by using ip address of 172.11.5.2 of /16.
- 4 port is connected with the lease line provided by Netsol which extended the lan of a branch site to the H/O by using ip address of 172.20.20.2 of /16.
- Remaining Ports are reserved for future use.

3.8 Core Switches

3.8.1 Core switch 1 3750G-24T:

Cisco Catalyst-3750 Series switch 3750G-24T is an initiative line of product that makes LAN operating efficiency by joining industry-leading ease of use and for stackable switches the highest resiliency available. The Cisco Catalyst-3750 Series deployed of converged applications and brings to changing business needs by providing support for converged network patterns, configuration flexibility, and automation of intelligent network-services configurations for mid-sized organizations and enterprise branch offices

- 24 Ethernet 10/100/1000 ports
- Innovative stacking technology
- high-speed stacking bus, 32-Gbps
- 1 RU stackable, multilayer switch
- IP Base software feature set (IPB)
- Enterprise-class intelligent services delivered to the network edge

3.8.2 Port:

Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently being used as the backbone in many enterprise networks

3.8.3 V-LAN:

A V-LAN is a broadcast domain created by switches. Normally, it is a router or layer 3 switches creating that broadcast domain. With V-LAN's, a switch can create the broadcast domain.

3.8.4 Mode:

- **Trunk:** A trunk port is a port which is used just to carry the V-LANs traffic which will be accessible for the any switch, a process known as trunking. Trunk ports mark frames with unique identifying tags – either 802.1Q tags or Inter-Switch Link (ISL) tags – as they move between switches.
- **Access:** forces the port to be an access port while and any device plugged into this port will only be able to communicate with other devices that are in the same V-LAN.

3.9 Core Switch 1 Connectivity:

Core switch 1 resides in an IT department working as a back bone to the entire lan network. All the access switches are terminating on core switches. There are two core switches to deal with redundant traffic. Both the switches are working in Active/Passive mode. If one switch get down another switch will take responsibility of the entire communication. Following are the connectivity tables of both core switches.

WS-C3750G-24TS-S

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with LAN_1 (Firewall)	10.10.10.1/24	L3
GigabitEthernet1/2	Connected with Switch_1	V-LAN 20,30	Trunk
GigabitEthernet1/3	Connected with Switch_2	V-LAN 40,50,60,90	Trunk
GigabitEthernet1/4	Connected with Switch_3	V-LAN 70,80	Trunk
GigabitEthernet1/5	Connected with Switch_4	V-LAN 90	Access
GigabitEthernet1/6	Connected with NVR	V-LAN 90	Access
GigabitEthernet1/7	Reserve		
GigabitEthernet1/8	Reserve		
GigabitEthernet1/9	Reserve		
GigabitEthernet1/10	Reserve		
GigabitEthernet1/11	Reserve		
GigabitEthernet1/12	Reserve		
GigabitEthernet1/13	Reserve		
GigabitEthernet1/14	Reserve		
GigabitEthernet1/15	Reserve		
GigabitEthernet1/16	Reserve		
GigabitEthernet1/17	Reserve		
GigabitEthernet1/18	Reserve		
GigabitEthernet1/19	Reserve		
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 4 Core Switch 1 Connectivity

3.10 Core Switch 2 Connectivity:

WS-C3750G-24TS-S

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with LAN_1 (Firewall)	10.10.11.1/24	L3
GigabitEthernet1/2	Connected with Switch_1	V-LAN 20,30	Trunk
GigabitEthernet1/3	Connected with Switch_2	V-LAN 40,50,60,90	Trunk
GigabitEthernet1/4	Connected with Switch_3	V-LAN 70,80	Trunk
GigabitEthernet1/5	Connected with Switch_4	V-LAN 90	Access
GigabitEthernet1/6	Connected with NVR	V-LAN 90	Access
GigabitEthernet1/7	Reserve		
GigabitEthernet1/8	Reserve		
GigabitEthernet1/9	Reserve		
GigabitEthernet1/10	Reserve		
GigabitEthernet1/11	Reserve		
GigabitEthernet1/12	Reserve		
GigabitEthernet1/13	Reserve		
GigabitEthernet1/14	Reserve		
GigabitEthernet1/15	Reserve		
GigabitEthernet1/16	Reserve		
GigabitEthernet1/17	Reserve		
GigabitEthernet1/18	Reserve		
GigabitEthernet1/19	Reserve		
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 5 Core Switch 2 Connectivity

3.11 Access Switches

3.11.1 Model:

Cisco Catalyst-2960G-24TC-L Switch

Cisco Catalyst 2960G-24TC-L Switch is a Catalyst 2960-X Series with fixed configurations switch. It supports upto 10/100/1000 enhanced local area network (LAN) services with Ethernet connectivity small or middle size networks or branches.

3.11.2 Benefits:

Main benefit of this switch is, we can extend the existing network by wired connectivity to get more employees. If anyone have a bit networking experience.

3.12 Access Switch 1:

Access switch 1 manage the traffic of HR and marketing department. The allowed V-LANs are V-LAN 20 and V-LAN 30 which holds the traffic of each group of users.

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with HR PC 1	V-LAN 20	Access
GigabitEthernet1/4	Connected with HR PC 2	V-LAN 20	Access
GigabitEthernet1/5	Connected with HR PC 3	V-LAN 20	Access
GigabitEthernet1/6	Connected with HR PC 4	V-LAN 20	Access
GigabitEthernet1/7	Connected with MKT PC 1	V-LAN 30	Access
GigabitEthernet1/8	Connected with MKT PC 2	V-LAN 30	Access
GigabitEthernet1/9	Connected with MKT PC 3	V-LAN 30	Access
GigabitEthernet1/10	Connected with MKT PC 4	V-LAN 30	Access
GigabitEthernet1/11	Connected with MKT PC 5	V-LAN 30	Access
GigabitEthernet1/12	Connected with MKT PC 6	V-LAN 30	Access
GigabitEthernet1/13	Connected with MKT PC 7	V-LAN 30	Access
GigabitEthernet1/14	Connected with MKT PC 8	V-LAN 30	Access
GigabitEthernet1/15	Connected with MKT PC 9	V-LAN 30	Access
GigabitEthernet1/16	Connected with MKT PC 10	V-LAN 30	Access
GigabitEthernet1/17	Connected with MKT PC 11	V-LAN 30	Access
GigabitEthernet1/18	Connected with MKT PC 12	V-LAN 30	Access
GigabitEthernet1/19	Connected with MKT PC 13	V-LAN 30	Access
GigabitEthernet1/20	Connected with MKT PC 14	V-LAN 30	Access
GigabitEthernet1/21	Connected with MKT PC 15	V-LAN 30	Access
GigabitEthernet1/22	Connected with MKT PC 16	V-LAN 30	Access
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 6 Access Switch 1

3.13 Access Switch 2:

Access switch 2 manage the traffic of following department:

- Vehicle Monitoring
- Conference Room
- Managers and Executives

The allowed V-LANs are V-LAN 40,50,60 and V-LAN 90 which holds the traffic of each group of users.

2960G-24TC-L

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with Manager PC 1	V-LAN 40	Access
GigabitEthernet1/4	Connected with Manager PC 2	V-LAN 40	Access
GigabitEthernet1/5	Connected with Manager PC 3	V-LAN 40	Access
GigabitEthernet1/6	Connected with Executives PC 1	V-LAN 50	Access
GigabitEthernet1/7	Connected with Executives PC 1	V-LAN 50	Access
GigabitEthernet1/8	Connected with Vehicle Monitoring PC 1	V-LAN 60	Access
GigabitEthernet1/9	Connected with Vehicle Monitoring PC 2	V-LAN 60	Access
GigabitEthernet1/10	Connected with Vehicle Monitoring PC 3	V-LAN 60	Access
GigabitEthernet1/11	Connected with Vehicle Monitoring PC 4	V-LAN 60	Access
GigabitEthernet1/12	Connected with Vehicle Monitoring PC 5	V-LAN 60	Access
GigabitEthernet1/13	Connected with Vehicle Monitoring PC 6	V-LAN 60	Access
GigabitEthernet1/14	Connected with Vehicle Monitoring PC 7	V-LAN 60	Access
GigabitEthernet1/15	Connected with Vehicle Monitoring PC 8	V-LAN 60	Access
GigabitEthernet1/16	Connected with Vehicle Monitoring PC 9	V-LAN 60	Access
GigabitEthernet1/17	Connected with Vehicle Monitoring PC 10	V-LAN 60	Access
GigabitEthernet1/18	Connected with Access point 1	V-LAN 90	Access
GigabitEthernet1/19	Connected with Access point 2	V-LAN 90	Access
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 7 Access Switch 2

3.14 Access Switch 3:

Access switch 3 manage the traffic of following department:

- Finance
- IT Support

The allowed V-LANs are V-LAN 70 and V-LAN 80 which holds the traffic of each group of users.

2960G-24TC-L

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with Finance PC 1	V-LAN 70	Access
GigabitEthernet1/4	Connected with Finance PC 2	V-LAN 70	Access
GigabitEthernet1/5	Connected with Finance PC 3	V-LAN 70	Access
GigabitEthernet1/6	Connected with Finance PC 4	V-LAN 70	Access
GigabitEthernet1/7	Connected with Finance PC 5	V-LAN 70	Access
GigabitEthernet1/8	Connected with Finance PC 6	V-LAN 70	Access
GigabitEthernet1/9	Connected with Finance PC 7	V-LAN 70	Access
GigabitEthernet1/10	Connected with Finance PC 8	V-LAN 70	Access
GigabitEthernet1/11	Connected with Finance PC 9	V-LAN 70	Access
GigabitEthernet1/12	Connected with Finance PC 10	V-LAN 70	Access
GigabitEthernet1/13	Connected with IT Support PC 1	V-LAN 80	Access
GigabitEthernet1/14	Connected with IT Support PC 2	V-LAN 80	Access
GigabitEthernet1/15	Connected with IT Support PC 3	V-LAN 80	Access
GigabitEthernet1/16	Connected with IT Support PC 4	V-LAN 80	Access
GigabitEthernet1/17	Connected with IT Support PC 5	V-LAN 80	Access
GigabitEthernet1/18	Reserve		
GigabitEthernet1/19	Reserve		
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 8 : Access Switch 3

3.15 Access Switch 4:

Access switch 4 manage the traffic of Cameras:

The allowed V-LAN is V-LAN 90 which holds the traffic all the cameras running in a VLC environment. Here Poe Switch will be used which holds the capabilities of Power over Ethernet providing the power to all cameras.

WS-C2960X-24PS-L

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with HM_C1	V-LAN 90	Access
GigabitEthernet1/4	Connected with HM_C2	V-LAN 90	Access
GigabitEthernet1/5	Connected with HM_C3	V-LAN 90	Access
GigabitEthernet1/6	Connected with HM_C4	V-LAN 90	Access
GigabitEthernet1/7	Connected with VM_C1	V-LAN 90	Access
GigabitEthernet1/8	Connected with VM_C2	V-LAN 90	Access
GigabitEthernet1/9	Connected with VM_C3	V-LAN 90	Access
GigabitEthernet1/10	Connected with VM_C4	V-LAN 90	Access
GigabitEthernet1/11	Connected with CR_C1	V-LAN 90	Access
GigabitEthernet1/12	Connected with CR_C2	V-LAN 90	Access
GigabitEthernet1/13	Connected with WA_C1	V-LAN 90	Access
GigabitEthernet1/14	Connected with WA_C2	V-LAN 90	Access
GigabitEthernet1/15	Connected with F_C1	V-LAN 90	Access
GigabitEthernet1/16	Connected with F_C2	V-LAN 90	Access
GigabitEthernet1/17	Connected with F_C3	V-LAN 90	Access
GigabitEthernet1/18	Connected with F_C4	V-LAN 90	Access
GigabitEthernet1/19	Connected with IT_C1	V-LAN 90	Access
GigabitEthernet1/20	Connected with IT_C2	V-LAN 90	Access
GigabitEthernet1/21	Connected with L_C1	V-LAN 90	Access
GigabitEthernet1/22	Connected with GT_C1	V-LAN 90	Access
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 9 Access Switch 4

Chapter 4

NETWORK SECURITY

PLAN

4.1 Plan

This project will be implemented on tools to create a virtual environment for the simulation of a real time project and after the implementation it will presented to the VLC's IT manager for the proceeding.

4.2 Tools

- **GNS3:** It is a abbreviation of Graphical Network Simulator-3. A network based software emulator. It helps to virtualized the project for better understanding . It uses Dynamics emulation software to simulate Cisco IOS.

Project use: Implementation of GNS3 in our project is to run multiple IOS and VMS to emulate their real time working. GNS3 will be loaded with multiple IOS like CISCO IOUs of layer 3 and layer two. GNS3 will be connected with GNS3 VM server running on a VMware tool. GNS3 host directly communicate with the VM server by using port 3080 with ip 192.168.136.128/24.

- **VMware:** VMware Workstation is a virtual machine software that is used for x86 and x86-64 computers to run multiple operating systems over a single physical host computer. Each virtual machine can run a single instance of any operating system (Microsoft, Linux, etc.) simultaneously.

Project use: We will use VMware in our project implementation to run the GNS3 Virtual server without using another extra hardware. VMware will provide the ease to run and manage VMs. VMware will run parallel to the GNS3 host.

- **IOS & Images:** In computing, a system image is a serialized copy of the entire state of a computer system stored in some non-volatile form such as a file. Cisco Internetwork Operating System is a family of network operating systems used on many Cisco Systems routers and current Cisco network switches. core function of Cisco IOS is to enable data communications between network nodes.

Project Use: We will use following images to run a complete network scenario:

Cisco IOSv 15.6

Cisco IOU L3

Cisco IOU L2 15.1g

Cisco IOU L2 15.2d

FortiGate 6.0.0

Firefox 31.1.1~2

- **Forti-Gate-VM:**

FortiGate VM is a full-featured Forti-Gate packaged as a virtual appliance. Forti-Gate-VM virtual appliance is ideal for monitoring and enforcing virtual traffic on leading virtualization, cloud, and SDN platforms including VMware vSphere, Hyper-V, Xen, KVM, and AWS.

Project use:

FortiGate VM will be Installed in gns3 to get the functionalities of a real time firewall. Firewall will be configured through console for enabling browser access. After it firewall will be accessed and managed by Firefox browser which is also installed in GNS3.

- **PuTTY**

PuTTY is a like a command line interface. (Tetz) It is an open source terminal for serial console and network applications.

Project use:

We will use Putty to access the console of all the network devices. puTTY is also installed in GNS3.

4.3 Network Connectivity:

For establishing the environment, we will do the following connectivity to simulate the real time project.

Switch 1

We will connect the users of HR and Marketing department switch downlink having V-LAN id 20,30 with respective ip addresses as 20.0.0.10/24 and 30.0.0.10/24 along with uplink to core 1 and core2.

Switch 2

We will connect the users of Vehicle monitoring, conference room, managers & executives department downlink having V-LAN id 40,50,60,90 with respective ip addresses as 40.0.0.10/24 , 50.0.0.10/24 , 60.0.0.10/24 and 90.0.0.10/24 along with uplink at core 1 and core 2.

Switch 3

We will connect the users of Finance and It support departments downlink having V-LAN id 70,80 with respective ip addresses as 70.0.0.10/24 and 80.0.0.10/24 along with uplink at core 1 and core2.

Switch 4

Camera department is downlink having V-LAN id 90 with respective ip address as 90.0.0.10/24 along with uplink at core 1.

Core 1

IT Department is downlink having ip address as 10.10.10.1/24 of uplink firewall and switches having different V-LANS, 20 and 30 V-LAN id are configured on switch1, 40,50,60 and 90 V-LAN id's are configured on switch2, V-LAN 70,80 are configured at switch 3,V-LAN id 90 is configured on switch 4.Main features is that all these V-LANs are uplink at core2.

Core 2

IT Department is downlink having ip address as 10.10.10.1/24 of uplink firewall and switches having different V-LANS, 20 and 30 V-LAN id are configured on switch1, 40,50,60 and 90 V-LAN id's are configured on switch2, V-LAN 70,80 are configured at switch 3,V-LAN id 90 is configured on switch 4.Main features is that all these V-LANs are uplink at core1.

Switch/Firewall	Department	Connected	Interface	Assigned IP	V-LAN ID
Switch_1	HR and Marketing	Core 1	Gig2/0/1	20.0.0.10/24	20
		Core 2	Gig2/0/2	30.0.0.10/24	30
Switch_2	Vehicle Monitoring, Conference Room, Managers & Executives	Core 1	Gig2/0/1	40.0.0.10/24 50.0.0.10/24 60.0.0.10/24 90.0.0.10/24	40
		Core 2	Gig2/0/2		50
Switch_3	Finance	Core 1	Gig2/0/1	70.0.0.10/24	70
		Core 2	Gig2/0/2	80.0.0.10/24	80
Switch_4	Camera	Core 1	Fa1/1	90.0.0.10/24	90
		Core 2	Fa1/2		
Core_1	IT Department	Firewall	Gig2/0/1	10.10.10.1/24	-
		Switch_1	Gig2/0/2	-	20,30
		Switch_2	Gig2/0/3	-	40,50,60,90
		Switch_3	Gig2/0/4	-	70,80
		Switch_4	Gig2/0/5	-	90
		NVR	Gig2/0/6	-	90
		Core_2	Gig2/0/10	-	20,30,40,50,60,70,80,90
Core_2	IT Department	Firewall	Gig2/0/1	10.10.11.1/24	-
		Switch_1	Gig2/0/2	-	20,30
		Switch_2	Gig2/0/3	-	40,50,60,90
		Switch_3	Gig2/0/4	-	70,80
		Switch_4	Gig2/0/5	-	90
		NVR	Gig2/0/6	-	90
		Core_1	Gig2/0/10	-	20,30,40,50,60,70,80,90
Firewall	IT Department	PTCL (Internet)	Wan 1	192.168.10.10/24	-
		Reserve	Wan 2	-	-
		Core_1	1	10.10.10.2/24	-
		Core_2	2	10.10.11.2/24	-
		PTCL (Data)	3	172.11.5.2/16	-
		Netsol (Data)	4	172.20.20.2/16	-

Table 10 Network Plan

4.4 Network Security Integration Plan

4.4.1 Firewall

Firewall is downlink with IT department having PTCL (internet) uplink with 192.168.10.10/24 ip address, also core 1 and core 2 assigned 10.10.10.2/24 and 10.10.11.2/24 ip addresses respectively. PTCL(DATA) and NETSOL(data) having ip addresses as 172.11.5.2/16 and 172.20.20.2/16.

4.4.2 Network Security Plan (Policy Map)

A network security policy is a formal document that outlines the principles, procedures and guidelines to enforce, manage, monitor and maintain security on a computer network. It is designed to ensure that the computer network is protected from any act or process that can breach its security. In this following table we have set policies, services and actions against sources.

Table Description:

There are about 9 policies(Executives, Managers, HR, Marketing, Finance, Vehicle, IT Support, AP, Camera), all are having almost same incoming interface and outgoing interface like LAN_1/,LAN_2 and WAN1/PTCL(Data)/NETSOL(Data) respectively, All are set accept action and their services are ALL ALLOW only Finance, VM and camera have some different services also their schedules are set to 9-5 and only cameras are working 24/7.

Policy Name	Incoming Interface	Outgoing Interface	Source	Destination	Schedule	Services	Action
EXEC_Priv	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	Exec	all	Not set	ALL allow	Accept
Managers_Priv	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	Mgrs	all	9-5	ALL allow	Accept
HR	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	HR	all	9-5	ALL allow	Accept
Marketing	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	Mktng	all	9-5	ALL allow	Accept
Finance	Lan_1/ Lan_2	PTCL(Data) / Netsol(Data)	Finance	all	9-5	DNS, IMAP, POP3, LDAP, FTP, TFTP,	Accept
Vehicle Monitoring	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	VM	all	9-5	HTTPS, DNS, IMAP, POP3, LDAP	Accept
IT Support	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	IT	all	9-5	ALL allow	Accept
Conference Room/AP	Lan_1/ Lan_2	WAN1/ PTCL(Data)/ Netsol(Data)	CR_AP	all	9-5	ALL allow	Accept
Camera	Lan_1/ Lan_2	PTCL(Data)/ Netsol(Data)	Cams	all	24x7	TCP,UDP,LDAP_UDP	Accept

Table 11 Firewall Policy table

4.5 Applied Services protocols

DNS:

DNS often uses the UDP (User Datagram Protocol) to performs request. It is consists of single request of User Datagram Protocol from User Datagram Protocol following client to the server.

Port: 53

IMAP:

Internet Message Access Protocol (IMAP) manages the email messages from mail server because it is email protocol. Although, It allows users to see the messages and manipulate because they are locally stored in a computer device.

Port: 993

POP3:

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline.

Port: 110

LDAP:

Lightweight Directory Access Protocol (LDAP) is a client/server protocol used to access and manage directory information. It reads and edits directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

Port: 389

FTP:

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

Port: 20

TFTP:

Trivial File Transfer Protocol(TFTP) use user data protocol(UDP) for delivering data to diskless workstations, routers and x-terminals as it is high level protocol for transferring.

Port: 69

HTTPS:

The purpose of HTTPS is to ensure the protection, integrity, and privacy of the data exchanged between a server and a client.

Port: 443

TCP:

Transmission Control Protocol (TCP) is a protocol which let us know whether the connection is established or not.

Port: 0-1023

UDP:

UDP (User Datagram Protocol) can also used for communication but it does not confirm whether the receiver side get the data or not. It uses low latency connection over internet.

Port: 0-65535

4.6 Firewall Address

In this table we applied filter for some policies through firewall. All filters would be active whether it is antivirus, web filter, DNS Filter, App control, IPS or SSL inspection. They all are having different subnets address which are given in table.

Source Definition	Address/Subnet	Anti-virus	Web Filter	DNS Filter	App Control	IPS	SSL Inspection
Exec	50.0.0.0/24	Active	Active	Active	Active	Active	Active
Mgrs	40.0.0.0/24	Active	Active	Active	Active	Active	Active
HR	20.0.0.0/24	Active	Active	Active	Active	Active	Active
Mktng	30.0.0.0/24	Active	Active	Active	Active	Active	Active
Finance	70.0.0.0/24	Active	Active	Active	Active	Active	Active
VM	60.0.0.0/24	Active	Active	Active	Active	Active	Active
IT	80.0.0.0/24	Active	Active	Active	Active	Active	Active
CR_AP	90.0.0.0/24	Active	Active	Active	Active	Active	Active
Cams	90.0.0.0/24	Active	Active	Active	Active	Active	Active

Table 12 Firewall Filter Table

4.7 Overview:

Firewalls basically plays vital role in protection of any network because it helps to protect networks from inside from any outside unauthorized access in network. If there is need of availability outside the network then it manages the separate network for outsider, it is possibly only through DMZ(Demilitarized zone). The firewall allows limited access to the DMZ. The users are configured on high security zone and servers are configured in multiple DMZ security zones. All the traffic from users V-LAN going to Server V-LAN will go through firewall as well servers of different V-LAN are also on different security zone and have to go through the firewall to access other security zone server. Firewall is configured in one arm-mode with core switch.

Note: In order to pass traffic through the firewall, the profiles must be known. The information will be documented during the implementation phase.

4.8 Forti-Gate in VLC's Environment

Firewall is configured as Active mode. Management Interface will be used for this purpose. Firewall connected to Core Switch 1 & Core Switch 2 will be configured as active firewall.

FortiGate admin context used following logical routing:

- Core switch route traffic from user V-LANs to server subnet(Located at H/O), there are static routes available on core switch which point user traffic to firewall SVI interface named as ingress interface on high security zone.

- Firewall applies the security policy based on protection applied on it and reroute traffic using another interface of corresponding address either its Internet or Data link towards H/O.
- The egress traffic return to core switch from firewall after coming from Internet or H/O DC.
- For all V-LAN the firewall is configured as default gateway. Default Gateway for all V-LAN subnets are configured on Fort i-Gate as SVI interfaces.
- For all egress connections firewall work as a failover and load balancer as well if any interface is down.

4.8.1 Traffic Policy Applied on FortiGate

Traffic policy which is applied on Forti-Gate helps to determine which traffic to pass through firewall from another networks. By default it does not allow any traffic to pass through firewall until or unless it is permitted by an Access control list(ACL), and by applying ACL to interfaces. It can specify which IP addresses and traffic types can pass through the interfaces to access other network.

Based on VLC requirement security policy ACLs will be used on Fort i-Gate to implement firewall rules. The policy will allow only the needed connections and services to pass through to the datacenter (Located at H/O), with the rule-set as specific and strict as possible.

4.8.2 Flow of traffic client V-LAN to Internet or Server V-LANs

- Traffic initiate from user for server in server V-LAN behind the Fort i-Gate, the packet first reach to core switch which is Default Gateway of user PC.
- Core Switch will look into its routing table if the destination subnet is known then it routes the packet to firewall.
- All incoming traffic coming to firewall is of same security zone, firewall look into destination subnet and then identifies the outgoing interface and then look into access list apply on it.
- If security policy permits the traffic then it allow the connection otherwise drop the packet.

- Once firewalls allow the packet it will send to corresponding subnet egress interface to core switch of H/O.
- Once core switch received packet from firewall it forwards packet to server farm switch where server is directly connected.

Note: For rest of the Server subnet SVI will configured once list of all server, V-LAN and their subnet will be provided. Firewall Security policy will be applied once we completed list of all applications and their port requirements sheet.

4.8.3 Load Balancing

A process of deciding which link of client request will be accepted. Like, if the request of a client is consist of a HTTP (Hypertext Transport Protocol) for web page or FTP (File Transfer Protocol) to download any file so the load balancer will select the defined path for the client.

The main Features of load balancing are listed as under:

1. Reduce the places in the work flow where a single point of failure can bring the process to a halt.
2. Expand the capacity of the resources to handle the required workload.
3. Have it configured so that the process of balancing the workload is automatic?

Often, it can be just as important for an organizations member to be able to access the Internet as it is for the native of the Internet to access the Web facing resources.

4.8.4 Forti-Gate as a Load Balancer (SD WAN)

It manages wide area network through software defined approach. It also helps to use internet traffic by using private wide area network services to remain available for critical and real time applications. This will help the network to improve its traffic flow and balanced the load on the network.

Following are the advantages of SD-WAN:

- It reduces the costs with 3G/4G/LTE and many others through transport independence.
- IT improves performance applications with availability and agility.

- IT also optimized user efficiency and experience through public cloud application and SaaS.

SD-WAN has 3 terms:

- **SD-WAN interface**

It has interfaces for traffic and atleast one interface is connected to SD-WAN for connection of upto 255 more members for configuration and allow traffic for communication is called SD-WAN.

- **Performance-SLA**

IT is also called health check, It is usually used to check link failures and link quality of member interface. If SD-WAN members unable to detect server can reroute or remove routes for traffic. To select preferred members interface for forwarding traffic SD-WAN can be used.

- **SD-WAN rule**

It is also called service, Some traffic can send dynamically to the best link or through some specific routes with the help of SD-WAN.

Following are the modes:

- **Manual:** Assign interfaces a priority manually.
- **Auto:** Assign interfaces a priority based on quality.
- **SLA:** Assign interfaces a priority based on selected SLA settings.
- **Priority:** Assign interfaces a priority based on the link-cost-factor quality of the interface.
- **Load-balance:** Distribute traffic among all available links based on the load balance algorithm.

4.8.5 Flow of Traffic from User to Server/Internet behind FortiGate SSD-WAN

- Traffic initiate from user for server (which is actually VIP IP address of Server) in server V-LAN behind the Fort i-Gate, the packet first reach to core switch which is Default Gateway of user PC.

- Core Switch will look into its routing table, if the destination subnet is known then it routes the packet to firewall.
- All incoming traffic coming to firewall is of same security zone, firewall will look into destination server subnet identify the outgoing interface and then look into access list and apply on it.
- If security policy permits the traffic then it allow the connection otherwise drops all the packet.
- Once firewalls allow the packet it will send to corresponding destination subnet egress interface.
- Once core switch received packet it forward packet to Fort i-Gate load balancer .
- Load balancer looks into SD-WAN table, perform load balancing algorithm, and send packet to the elected link.
- If packet initiate from server, it first go to load balancer which is servers default gateway. Load balancers have firewall as its default gateway so LB forwards the packet to Firewall.
- Firewall have reverse route for users subnet point to core switch using inside interface.

4.8.6 Intrusion Detection/Prevention System

This section addresses the need for an Intrusion Detection and Prevention solution within the VLC network that should improve visibility of security threats and intrusions in respective domains. The scope of this section will cover the Low-Level details for the design and deployment of an Intrusion prevention infrastructure.

4.8.7 FortiGate inbuilt Intrusion Detection and Prevention System

The Fort i-Gate IDS/IPS's will monitor specified traffic by placing its monitoring interface in the applicable V-LAN's that are identified by the VLC's security policy.

The switching platform will "supply" the Firewall with the traffic that need to be monitor. This is done by same egress and ingress interface that identifies which traffic should be inspected.

Objectives

Faculty of CS & IT, The Superior College Lahore, Pakistan

- Traffic capturing on the Firewall and the switches.
- Definition of the signature policies for the Fort i-Gate IDS/IPS.
- Management of the IDS/IPS.
- Monitoring of alarms generated by the IDS/IPS.
- Fine tuning of the signatures on the IDS/IPS.

Constraints

- Ensure that all traffic is not captured twice in different locations.
- Defining the policies based on the known environment.
- Enabling relevant signatures while at the same time reducing false positives.
- Ease of administration, management and upgrades.
- Scalability for the future addition of IDS/IPS signatures.

4.8.8 Signature updates

Signatures can be updated automatically on the IDS/IPS however some manual intervention is always recommended as the new signature might not be enabled or not required in VLC's environment. Notifications of new available signatures and a link to the update can be received from FortiLabs via an automated email by using the registration URL.

Chapter 5

Experimental Structure

Definition

This project would be on an IT infrastructure of an organization (Logistics Company). It's a real time project that will be mirrored on simulator to understand the working of an enterprise network. All the information of organization would be collected from their IT experts. The objective is to provide them more reliable and secured network. The scope of this project is to multiple branches present on remote location by using Hub and Spoke architecture. Moreover, the technique of 3 tier architecture will be used to make it more scalable for future purpose.

5.1 Existing System

Following is the figure showing how the existing system was running and topology design view of Sheikhpura branch connecting with Lahore Head Office.

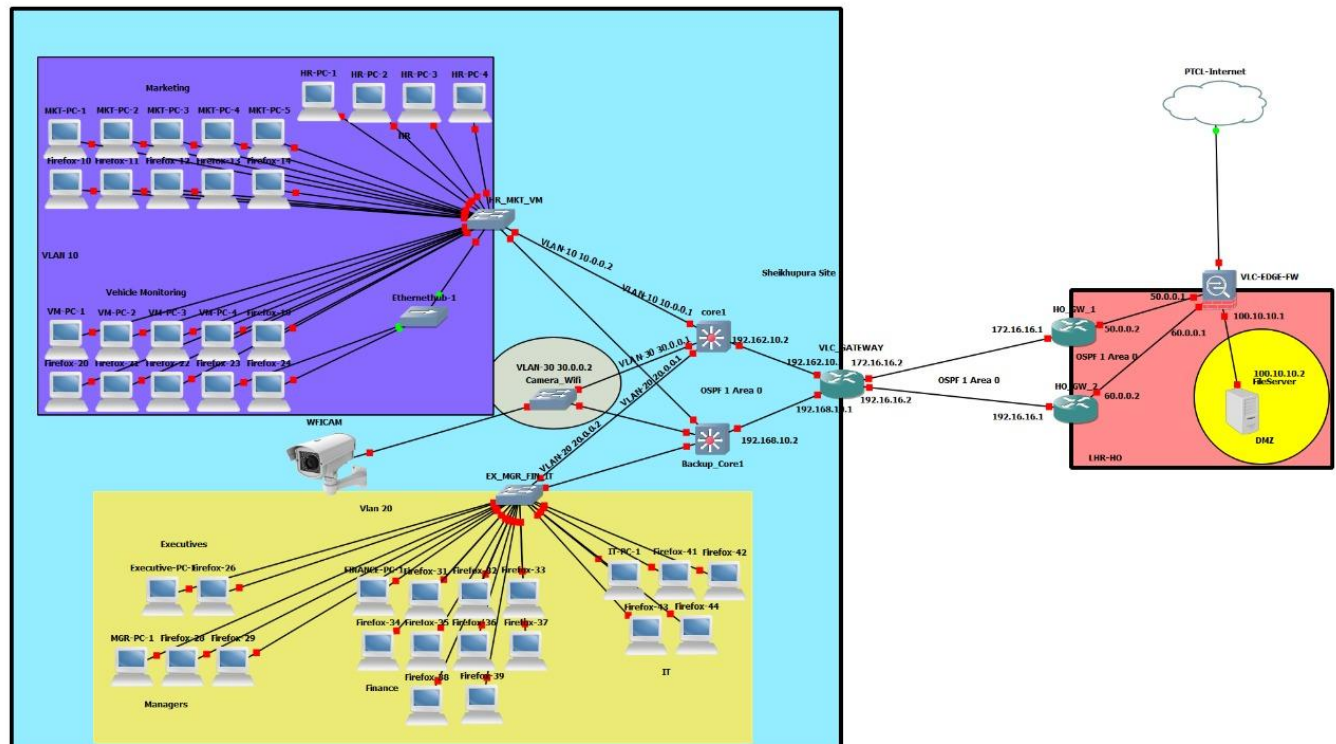


Figure 5 Existing topology of VIRK LOGISTICS

5.1.1 Connectivity Overview of existing infrastructure

According to the survey in an existing system they have around 45 users divided into 6 departments and the list of each department is given below.

- HR
- Marketing
- Vehicle Monitoring
- Executives
- Managers
- Finance
- IT

They divided all departments in 2 segments and assigned 1 access switch on each segment so a single access switch holding 3 departments on the same V-LAN. They also have two Access points and number of cameras on one dedicated Poe switch.

All of the 3 access switches terminating on a Layer 3 core switch. All of the V-LANs are propagated from a core switch and each of access switch contain its own DHCP pool according to their respective V-LAN.

They also have a backup core switch which is the replica of main Core switch here name as Core1 .The backup switch will be activated in case of failure of main core switch manually.

The core switches communicate with gateway via their uplink by using OSPF protocol. Now the gateway is responsible to route the traffic via dedicated lease lines from two service providers PTCL and Netsol extending their LAN towards Head Office. The redundant links are operated automatically by OSPF protocol. All of the traffic route towards the ASA firewall located at the edge of H/O either they want to communicate with Internet or their File servers residing in the DMZ of H/O.

5.1.2 Problem Statement

Technology enhanced rapidly with the passage of time but we are stuck to old traditions and do not follow new concepts and technologies while developing any network. VIRK LOGISTICS did the same mistake by hiring old tradition IT experts which lead them to face many problems such as security, scalability, complex configuration, manually doing failover. Following this figure, we can see that they have connected multiple departments with one switch (HR_MKT_VM) which causes extra load on particular switch.

5.1.3 Hardware

List of hardware's in existing system.

S. No.	Product	Description	Qty
	Switch(L-2)		
1	WS-C2960G-24TC-L	Cisco Catalyst 2960G Switch 20 x 10/100/100 Gigabit Ethernet Ports (Non-PoE) - 4 x Dual Purpose Port - LAN Base Image	2
2	WS-C2960G-24PS-L	Cisco Catalyst 2960S-24PS Layer 2 - Gigabit Ethernet Switch - 24 x 10/100/1000 PoE Ports - 370W - 4 x SFP - LAN Base – Managed	1
	Switch(L-3)		
3	WS-C3750G-24TS-S	Cisco Catalyst 3750G Switch includes 24 x 10/100/1000 Ports - 4 x SFP Ports - Standard Image	
	HUB		
4	SG110D 110 Series	SG110D 110 Series 8-Port Unmanaged Network Switch is used	1
	Cable		
5	Cat 5 cable	Cat 5 Unshielded cable is <u>laid</u> all over the infrastructure	overall

Table 13 Hardware of Existing System

5.1.4 Core1

Core 1 switch resides in an IT department working as a back bone to the entire LAN network. All the access switches are terminating on core switches. There are two core switches to deal with redundant traffic. (WS-C3750G-24T-S Datasheet)Both the switches are working in Active/Passive mode manually. If one switch get down another switch will be started to take responsibility of the entire communication manually. Following are the connectivity tables of both core switches.

WS-C3750G-24TS-S

Port	Description	V-LAN	Mode
Ethernet0/0	Connected with VLC_GATEWAY	192.162.10.2	Static
Ethernet0/1	Connected with HR_MKT_VM	V-LAN 10	Trunk
Ethernet0/2	Connected with EX_MGR_FIN_IT	V-LAN 20	Trunk
Ethernet0/3	Connected with Camera Wifi	V-LAN 30	Trunk
Ethernet1/0	Reserve		
Ethernet1/1	Reserve		
Ethernet1/2	Reserve		
Ethernet1/3	Reserve		
Ethernet 2/0	Reserve		
Ethernet 2/1	Reserve		
Ethernet 2/3	Reserve		
Ethernet 3/0	Reserve		
Ethernet 3/1	Reserve		
Ethernet 3/2	Reserve		
Ethernet 3/3	Reserve		

Table 14 Configuration of Core1

Configuration

```

!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname CORE_1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
!
ip cef
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
V-LAN internal allocation policy ascending
!
!
interface Loopback0
ip address 1.0.0.1 255.255.255.0
!
interface Ethernet0/0
no switchport

```

```

!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2

```

```

.....
ip address 192.162.10.2 255.255.255.0
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk

duplex auto
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
duplex auto
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto

interface V-LAN20
ip address 20.0.0.1 255.255.255.0
!
interface V-LAN30
ip address 30.0.0.1 255.255.255.0
!
router ospf 1
network 1.0.0.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.255 area 0
network 20.0.0.0 0.0.0.255 area 0
network 30.0.0.0 0.0.0.255 area 0
network 192.162.10.0 0.0.0.255 area 0
!
!
no ip http server
!
!
control-plane
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
!
End

```

```

.....
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN10
ip address 10.0.0.1 255.255.255.0
!
interface V-LAN11
no ip address
shutdown
!

```

5.1.5 Core2

This switch was replica of core1 switch and handled manually.

WS-C3750G-24TS-S

Port	Description	V-LAN	Mode
Ethernet0/0	Connected with VLC_GATEWAY	192.168.10.2	Static
Ethernet0/1	Connected with HR_MKT_VM	V-LAN 10	Trunk
Ethernet0/2	Connected with EX_MGR_FIN_IT	V-LAN 20	Trunk
Ethernet0/3	Connected with <u>Camera Wifi</u>	V-LAN 30	Trunk
Ethernet1/0	Reserve		
Ethernet1/1	Reserve		
Ethernet1/2	Reserve		
Ethernet1/3	Reserve		
Ethernet 2/0	Reserve		
Ethernet 2/1	Reserve		
Ethernet 2/3	Reserve		
Ethernet 3/0	Reserve		
Ethernet 3/1	Reserve		
Ethernet 3/2	Reserve		
Ethernet 3/3	Reserve		

Table 15: Configuration of Core2

Configuration

```

!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Backup_Core1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!

```

```

!
interface Ethernet0/2
switchport trunk encapsulation dot1q
duplex auto
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3

```

```

!
!
!
V-LAN internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
no switchport
ip address 192.168.10.2 255.255.255.0
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto

shutdown
!
interface V-LAN10
ip address 10.0.0.1 255.255.255.0
!
interface V-LAN11
no ip address
!
interface V-LAN20
ip address 20.0.0.1 255.255.255.0
!
interface V-LAN30
ip address 30.0.0.1 255.255.255.0
!
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
network 20.0.0.0 0.0.0.255 area 0
network 30.0.0.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
!
!
no ip http server
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0

```

```

duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface V-LAN1
no ip address

```

```

privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

5.1.6 Access Switch1 (HR_MKT_VM)

Access switch 1 manage the traffic of HR, Vehicle Monitoring and Marketing department. The 9allowed V-LANs 10 which holds the traffic of all connected departments.

Port	Description	V-LAN	Mode
Ethernet0/0	Connected with Core 1	ALL	Trunk
Ethernet0/1	Connected with HR PC 1	V-LAN 10	Access
Ethernet0/2	Connected with HR PC 2	V-LAN 10	Access
Ethernet0/3	Connected with HR PC 3	V-LAN 10	Access
Ethernet1/0	Connected with HR PC 4	V-LAN 10	Access
Ethernet1/1	Connected with MKT PC 1	V-LAN 10	Access
Ethernet1/2	Connected with MKT PC 2	V-LAN 10	Access
Ethernet1/3	Connected with MKT PC 3	V-LAN 10	Access
Ethernet 2/0	Connected with MKT PC 4	V-LAN 10	Access
Ethernet 2/1	Connected with MKT PC 5	V-LAN 10	Access
Ethernet 2/3	Connected with MKT PC 6	V-LAN 10	Access
Ethernet 3/0	Connected with MKT PC 7	V-LAN 10	Access
Ethernet 3/1	Connected with MKT PC 8	V-LAN 10	Access
Ethernet 3/2	Connected with VM PC 9	V-LAN 10	Access
Ethernet 3/3	Connected with VM PC 10	V-LAN 10	Access
Ethernet 4/0	Connected with VM PC 11	V-LAN 10	Access
Ethernet4/1	Connected with VM PC 12	V-LAN 10	Access
Ethernet 4/2	Connected with VM PC 13	V-LAN 10	Access
Ethernet 4/3	Connected with VM PC 14	V-LAN 10	Access
Ethernet5/0	Connected with VM PC 15	V-LAN 10	Access
Ethernet5/1	Connected with VM PC 16	V-LAN 10	Access
Ethernet5/2	Connected with HUB(VM) PC 23	V-LAN 10	Access
	Connected with HUB(VM) PC 24	V-LAN 10	Access
Ethernet5/3	Connected with core2	ALL	Trunk

Table 16: Configuration of Access Switch1(HR_MKT_VM)

Configuration

```
HR_MKT_VM#sh run
Building configuration...
```

```
Current configuration : 2843 bytes
```

```
!
! Last configuration change at 18:35:59 UTC Tue
Jun 30 2020
```

```
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname HR_MKT_VM
!
boot-start-marker
boot-end-marker
!
!
```

```
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
```

```
!
no aaa new-model
!
!
```

```
no ip icmp rate-limit unreachable
!
```

```
ip dhcp excluded-address 10.0.0.1
ip dhcp excluded-address 10.0.0.2
ip dhcp excluded-address 10.0.0.3
ip dhcp excluded-address 10.0.0.4
ip dhcp excluded-address 10.0.0.5
ip dhcp excluded-address 10.0.0.1 10.0.0.10
!
```

```
ip dhcp pool HR_MKT_VM_DHCP
network 10.0.0.0 255.255.255.0
default-router 10.0.0.1
dns-server 8.8.8.8
```

```
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
```

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
V-LAN internal allocation policy ascending
```

```
!
ip tcp synwait-time 5
!
```

```
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

```
interface Ethernet0/1
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet0/2
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet0/3
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet1/0
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet1/1
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet1/2
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet1/3
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet2/0
switchport access V-LAN 10
switchport mode access
!
```

```
interface Ethernet2/1
switchport access V-LAN 10
!
```

```
interface Ethernet2/2
```

```

switchport access V-LAN 10
!
interface Ethernet2/3
switchport access V-LAN 10
!
interface Ethernet3/0
switchport access V-LAN 10
!
interface Ethernet3/1
switchport access V-LAN 10
!
interface Ethernet3/2
switchport access V-LAN 10
!
interface Ethernet3/3
switchport access V-LAN 10
!
interface Ethernet4/0
switchport access V-LAN 10
!
interface Ethernet4/1
switchport access V-LAN 10
!
interface Ethernet4/2
switchport access V-LAN 10
!
interface Ethernet4/3
switchport access V-LAN 10
!
interface Ethernet5/0
switchport access V-LAN 10
!
interface Ethernet5/1
switchport access V-LAN 10
!
interface Ethernet5/2
switchport access V-LAN 10
!
interface Ethernet5/3
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN10
ip address 10.0.0.2 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!

```

5.1.7 Switch 2(EX_MGR_FIN_IT)

Access switch 2 manage the traffic of following department:

- IT
- Finance
- Managers and
- Executives

The allowed V-LANs 20 which holds the traffic of each group of users. (WS-C2960+24TC-L Datasheet)

2960G-24TC-L

Port	Description	V-LAN	Mode
Ethernet0/0	Connected with Core 1	NA	Trunk
Ethernet0/1	Connected with EX PC 25	V-LAN 20	Access
Ethernet0/2	Connected with EX PC 26	V-LAN 20	Access
Ethernet0/3	Connected with MGR PC 27	V-LAN 20	Access
Ethernet1/0	Connected with MGR PC 28	V-LAN 20	Access
Ethernet1/1	Connected with FIN PC 29	V-LAN 20	Access
Ethernet1/2	Connected with FIN PC 30	V-LAN 20	Access
Ethernet1/3	Connected with FIN PC 31	V-LAN 20	Access
Ethernet 2/0	Connected with FIN PC 32	V-LAN 20	Access
Ethernet 2/1	Connected with FIN PC 33	V-LAN 20	Access
Ethernet 2/2	Connected with FIN PC 34	V-LAN 20	Access
Ethernet 2/3	Connected with FIN PC 35	V-LAN 20	Access
Ethernet 3/0	Connected with FIN PC 36	V-LAN 20	Access
Ethernet 3/1	Connected with FIN PC 37	V-LAN 20	Access
Ethernet 3/2	Connected with FIN PC 38	V-LAN 20	Access
Ethernet 3/3	Connected with FIN PC 39	V-LAN 20	Access
Ethernet 4/0	Connected with IT PC 40	V-LAN 20	Access
Ethernet4/1	Connected with IT PC 41	V-LAN 20	Access
Ethernet 4/2	Connected with IT PC 42	V-LAN 20	Access
Ethernet 4/3	Connected with IT PC 43	V-LAN 20	Access
Ethernet5/0	Connected with IT PC 44	V-LAN 20	Access
Ethernet5/1	Empty		
Ethernet5/2	Empty		
Ethernet5/3	Connected to Backup_Core1	V-LAN 20	Trunk

Table 17: Configuration of Switch2(EX_MGR_FIN_IT)

Configuration

```
EX_MGR_FIN_IT#sh run
Building configuration...
```

```
Current configuration : 2705 bytes
!
! Last configuration change at 21:42:38 UTC Tue
Jun 30 2020
!
```

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname EX_MGR_FIN_IT
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 20.0.0.1 20.0.0.10
!
```

```
ip dhcp pool EX_MGR_FN_IT
network 20.0.0.0 255.0.0.0
default-router 20.0.0.1 255.255.255.0
dns-server 8.8.8.8
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
V-LAN internal allocation policy ascending
!
```

```
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access V-LAN 20
switchport mode access
!
interface Ethernet0/2
switchport access V-LAN 20
switchport mode access
!
interface Ethernet0/3
switchport access V-LAN 20
switchport mode access
!
interface Ethernet1/0
!
interface Ethernet1/1
switchport access V-LAN 20
switchport mode access
!
interface Ethernet1/2
switchport access V-LAN 20
switchport mode access
!
interface Ethernet1/3
switchport access V-LAN 20
switchport mode access
!
interface Ethernet2/0
!
interface Ethernet2/1
switchport access V-LAN 20
switchport mode access
!
interface Ethernet2/2
switchport access V-LAN 20
switchport mode access
!
interface Ethernet2/3
switchport access V-LAN 20
switchport mode access
!
```

```
interface Ethernet3/0
!
interface Ethernet3/1
switchport access V-LAN 20
switchport mode access
!
interface Ethernet3/2
switchport access V-LAN 20
switchport mode access
!
interface Ethernet3/3
switchport access V-LAN 20
switchport mode access
!
interface Ethernet4/0
!
interface Ethernet4/1
switchport access V-LAN 20
switchport mode access
!
interface Ethernet4/2
switchport access V-LAN 20
switchport mode access
!
interface Ethernet4/3
switchport access V-LAN 20
switchport mode access
!
interface Ethernet5/0
!
interface Ethernet5/1
switchport access V-LAN 20
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

```

switchport mode access
!
interface Ethernet5/2
switchport access V-LAN 20
switchport mode access
!
interface Ethernet5/3
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN20
ip address 20.0.0.2 255.255.255.0
!
ip forward-protocol nd

```

5.1.8 Access Switch 3 (Camera_WIFI)

Access switch 3 manages the traffic of Cameras:

The allowed V-LAN 30 which holds the traffic all the cameras running in a VLC environment. Here Poe Switch will be used which holds the capabilities of Power over Ethernet providing the power to all cameras. (WS-C2960X-24PS-L Datasheet)

WS-C2960X-24PS-L

Port	Description	V-LAN	Mode
Ethernet0/0	Connected with Core 1	NA	Trunk
Ethernet0/1	Connected with HM_C1	V-LAN 30	Access
Ethernet0/2	Connected with HM_C2	V-LAN 30	Access
Ethernet0/3	Connected with HM_C3	V-LAN 30	Access
Ethernet1/0	Connected with HM_C4	V-LAN 30	Access
Ethernet1/1	Connected with VM_C1	V-LAN 30	Access
Ethernet1/2	Connected with VM_C2	V-LAN 30	Access
Ethernet1/3	Connected with VM_C3	V-LAN 30	Access
Ethernet 2/0	Connected with VM_C4	V-LAN 30	Access
Ethernet 2/1	Connected with CR_C1	V-LAN 30	Access
Ethernet 2/3	Connected with CR_C2	V-LAN 30	Access
Ethernet 3/0	Connected with WA_C1	V-LAN 30	Access
Ethernet 3/1	Connected with WA_C2	V-LAN 30	Access
Ethernet 3/2	Connected with F_C1	V-LAN 30	Access
Ethernet 3/3	Connected with F_C2	V-LAN 30	Access
Ethernet 4/0	Connected with F_C3	V-LAN 30	Access
Ethernet4/1	Connected with F_C4	V-LAN 30	Access
Ethernet 4/2	Connected with IT_C1	V-LAN 30	Access
Ethernet 4/3	Connected with IT_C2	V-LAN 30	Access
Ethernet5/0	Connected with L_C1	V-LAN 30	Access
Ethernet5/1	Connected with GT_C1	V-LAN 30	Access
Ethernet5/2	Connected with wifi_1	V-LAN 30	Access
Ethernet5/3	Connected with wifi_2	V-LAN 30	Access

Table 18: Access Switch3(Camera_WIFI)

Configuration

```

Camera_Wifi#sh run
Building configuration...

Current configuration : 2751 bytes
!
! Last configuration change at 21:38:38 UTC Tue
Jun 30 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Camera_Wifi
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 30.0.0.1 30.0.0.10
!
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport trunk allowed V-LAN 30
switchport trunk encapsulation dot1q
!
interface Ethernet0/1
switchport access V-LAN 30
switchport mode access
!
interface Ethernet0/2
switchport access V-LAN 30
switchport mode access
!
interface Ethernet0/3
switchport access V-LAN 30
switchport mode access
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
switchport access V-LAN 30
switchport mode access
!

```

```

ip dhcp pool Cam_Wifi
network 30.0.0.0 255.255.255.0
default-router 30.0.0.1
dns-server 8.8.8.8
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
V-LAN internal allocation policy ascending

```

```

interface Ethernet2/1
switchport access V-LAN 30
switchport mode access
!
interface Ethernet2/2
switchport access V-LAN 30
switchport mode access
!
interface Ethernet2/3
switchport access V-LAN 30
switchport mode access
!
interface Ethernet3/0
switchport access V-LAN 30
switchport mode access
!

```

```

interface Ethernet5/1
switchport access V-LAN 30
switchport mode access
!
interface Ethernet5/2
switchport access V-LAN 30
switchport mode access
!
interface Ethernet5/3
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN30
ip address 30.0.0.2 255.255.255.0

```

5.1.9 VLC Gateway

It's a gateway between sheikhupura branch and head office Lahore for communication.

Port	Description	IP Address	Mode
GigabitEthernet0/0	Connected with HO_GW_1	172.16.16.2/24	L3
GigabitEthernet0/1	Connected with core1	192.162.10.1/24	L3
GigabitEthernet0/2	Connected with Backup_Core1	192.168.10.1/24	L3
GigabitEthernet0/3	Connected with HO_GW_2	192.16.16.2/24	L3

Table 19: Configuration of VLC Gateway

Configuration

```

!
! Last configuration change at 20:44:08 UTC Tue
Jun 30 2020
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VLC_GATEWAY
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
ethernet lmi ce
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
redundancy
!
!
interface GigabitEthernet0/0
ip address 172.16.16.2 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1
ip address 192.162.10.1 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/2
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/3
ip address 192.16.16.2 255.255.255.0
duplex auto
speed auto
media-type rj45
!
router ospf 1
network 172.16.16.0 0.0.0.255 area 0
network 192.16.16.0 0.0.0.255 area 0
network 192.162.10.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
banner exec _____
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not
supported by Cisco's *
* Technical Advisory Center. Any use or
disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any
third party for any *
* purposes is expressly prohibited except as
otherwise authorized by *
* Cisco in writing.
*
*****
*****
banner _____ incoming

```

```
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not
supported by Cisco's *
* Technical Advisory Center. Any use or
disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any
third party for any *
* purposes is expressly prohibited except as
otherwise authorized by *
* Cisco in writing.
*
*****
*****
```

```
banner login _____
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not
supported by Cisco's *
* Technical Advisory Center. Any use or
disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any
third party for any *
* purposes is expressly prohibited except as
otherwise authorized by *
* Cisco in writing.
*
*****
*****
```

```
!
line con 0
line aux 0
line vty 0 4
login
transport input none
!
no scheduler allocate
!
end
```

5.1.10 HO_GW_1

This is first gateway in Head office. All Traffic passes from here.

Port	Description	IP Address	Mode
GigabitEthernet0/0	Connected with VLC-Gateway	172.16.16.1/24	L3
GigabitEthernet0/1	Connected with VLC-EDGE-FW	50.0.0.2/24	L3
GigabitEthernet0/2			
GigabitEthernet0/3			

Table 20: Configuration HO_GW_1

Configuration

```

!
! Last configuration change at 20:44:49 UTC Tue
Jun 30 2020
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HO_GW_1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
interface lmi ce
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
redundancy
shutdown
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
!
router ospf 1
 redistribute connected subnets
 redistribute static subnets
 network 50.0.0.0 0.0.0.255 area 0
 network 172.16.16.0 0.0.0.255 area 0
 default-metric 1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner exec _____
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not

```

```

!
!
interface GigabitEthernet0/0
ip address 50.0.0.2 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1
ip address 172.16.16.1 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/2
no ip address

* IOSv is strictly limited to use for evaluation,
demonstration and IOS.
* education. IOSv is provided as-is and is not
supported by Cisco's
* Technical Advisory Center. Any use or
disclosure, in whole or in part,
* of the IOSv Software or Documentation to any
third party for any
* purposes is expressly prohibited except as
otherwise authorized by
* Cisco in writing.
*
*****
*****

banner login
*****
*****

* IOSv is strictly limited to use for evaluation,
demonstration and IOS.
* education. IOSv is provided as-is and is not
supported by Cisco's
* Technical Advisory Center. Any use or
disclosure, in whole or in part,
* of the IOSv Software or Documentation to any
third party for any
* purposes is expressly prohibited except as
otherwise authorized by
* Cisco in writing.
*
*****
*****

```

```

supported by Cisco's
* Technical Advisory Center. Any use or
disclosure, in whole or in part,
* of the IOSv Software or Documentation to any
third party for any
* purposes is expressly prohibited except as
otherwise authorized by
* Cisco in writing.
*
*****
*****

banner incoming
*****
*****

```

```

!
line con 0
line aux 0
line vty 0 4
login
transport input none
!
no scheduler allocate
!
End

```

5.1.11 HO_GW_2

Port	Description	IP Address	Mode
GigabitEthernet0/0	Connected with VLC-Gateway	192.16.16.1/24	L3
GigabitEthernet0/1	Connected with VLC-EDGE-FW	60.0.0.2/24	L3
GigabitEthernet0/2			
GigabitEthernet0/3			

Table 21: Configuration of HO_GW_2

Configuration

```

!
! Last configuration change at 20:44:49 UTC Tue
Jun 30 2020
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HO_GW_1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ethernet lmi ce
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
Redundancy
!
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
!
router ospf 1
redistribute connected subnets
redistribute static subnets
network 50.0.0.0 0.0.0.255 area 0
network 172.16.16.0 0.0.0.255 area 0
default-metric 1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
banner exec _____
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS...

```

```

!
interface GigabitEthernet0/0
ip address 50.0.0.2 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1
ip address 172.16.16.1 255.255.255.0
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/2
no ip address
shutdown

```

```

*****
*****

```

```

* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not
supported by Cisco's *
* Technical Advisory Center. Any use or
disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any
third party for any *
* purposes is expressly prohibited except as
otherwise authorized by *
* Cisco in writing.
*
*****
*****

```

```

banner login _____
*****
*****
* IOSv is strictly limited to use for evaluation,
demonstration and IOS *
* education. IOSv is provided as-is and is not
supported by Cisco's *
* Technical Advisory Center. Any use or
disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any
third party for any *
* purposes is expressly prohibited except as
otherwise authorized by *
* Cisco in writing.
*

```

```

* education. IOSv is provided as-is and is not
supported by Cisco's *
* Technical Advisory Center. Any use or
disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any
third party for any *
* purposes is expressly prohibited except as
otherwise authorized by *
* Cisco in writing.
*
*****
*****

```

```

banner _____ incoming

```

```

*****
*****
!
line con 0
line aux 0
line vty 0 4
login
transport input none
!
no scheduler allocate
!
end

```

5.1.12 VLC-EDGE-FW

Following is the port connectivity of firewall how all the ingress devices terminate on firewall and from which links the firewall reroutes the traffic toward a defined destination.

Port	Description	IP
GigabitEthernet0/0		
GigabitEthernet0/1	Connected with HO_GW_1	50.0.0.1/24
GigabitEthernet0/2	Connected with HO_GW_2	60.0.0.1/24
GigabitEthernet0/3	Connected with <u>FileServer</u>	100.10.10.2/24
GigabitEthernet0/4	Reserve	NULL
GigabitEthernet0/5	Reserve	NULL
GigabitEthernet0/6	Reserve	NULL

Table 22: Firewall Connectivity in HO

- GigabitEthernet0/0 is reserved
- GigabitEthernet0/1 is directly connected with HO_GW_1 assigned an ip of class C which is 50.0.0.1.
- GigabitEthernet0/2 is directly connected with HO_GW_2 assigned an ip of class C which is 60.0.0.1.
- GigabitEthernet0/3 is directly connected with Fileserver assigned an ip of class C which is 100.10.10.2.

- Remaining Ports are reserved for future use.

Configuration

```

: Saved

:
: Serial Number: 9AUH4059M91
: Hardware: ASA, 2048 MB RAM, CPU
Pentium II 1795 MHz
: Written by enable_15 at 21:11:31.049 UTC Tue
Jun 30 2020
!
ASA Version 9.12(2)4
!
hostname ciscoasa
enable password
$sha512$5000$E4hOkCURcfyBQQAhJA1Ctw==$
vAPSJONuRBK/SOkX8+clsA== pbkdf2
names
no mac-address auto

!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.29 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside1
 security-level 100
 ip address 50.0.0.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 nameif inside
 security-level 100
 ip address 60.0.0.1 255.255.255.0
 ospf message-digest-key 1 md5 cisco
 ospf authentication message-digest
!
interface GigabitEthernet0/3
 nameif DMZ
 security-level 50

interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network LAN
 subnet 0.0.0.0 0.0.0.0
pager lines 23
mtu outside 1500
mtu inside1 1500
mtu inside 1500
mtu DMZ 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
!
object network LAN
 nat (any,outside) dynamic interface
router ospf 1
 network 50.0.0.0 255.255.255.0 area 0

```

```
ip address 100.10.10.1 255.0.0.0
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
```

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igmp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging
infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crf configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain
_SmartCallHome_ServerCA
certificate ca 0509
308205b7 3082039f a0030201 02020205
09300d06 092a8648 86f70d01 01050500
3045310b 30090603 55040613 02424d31
19301706 0355040a 13105175 6f566164
6973204c 696d6974 6564311b 30190603
55040313 1251756f 56616469 7320526f
6f742043 41203230 1e170d30 36313132
34313832 3730305a 170d3331 31313234
31383233 33335a30 45310b30 09060355
04061302 424d3119 30170603 55040a13
1051756f 56616469 73204c69 6d697465
```

```
network 50.0.0.0 255.0.0.0 area 0
network 60.0.0.0 255.255.255.0 area 0
network 60.0.0.0 255.0.0.0 area 0
log-adj-changes
redistribute connected
redistribute static
default-information originate
!
```

```
172a3a74 8333307d 615411cb edabe0e6
d2a27ef5 6b6f18b7 0a0b2dfd e93eef0a
c6b310e9 dcc24617 f85dfda4 daff9e49
5a9ce633 e62496f7 3fba5b2b 1c7a35c2
d667feab 66508b6d 28602bef d760c3c7
93bc8d36 91f37ff8 db1113c4 9c7776c1
aeb7026a 817aa945 83e205e6 b956c194
378f4871 6322ec17 6507958a 4bdf8fc6
5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9
f80473f2 e9fe5c98 8cf573af 6bb47ecd
d45c022b 4c39e1b2 95952d42 87d7d5b3
9043b76c 13f1dedd f6c4f889 3fd175f5
92c391d5 8a88d090 ecdc6dde 89c26571
968b0d03 fd9cbf5b 16ac92db eafe797c
adebaff7 16cbdbcd 252be51f fb9a9fe2
51cc3a53 0c48e60e bdc9b476 0652e611
13857263 0304e004 362b2019 02e874a7
1fb6c956 66f07525 dc67c10e 616088b3
3ed1a8fc a3da1db0 d1b12354 df44766d
ed41d8c1 b222b653 1cdf351d dca1772a
31e42df5 e5e5dbc8 e0ffe580 d70b63a0
ff33a10f ba2c1515 ea97b3d2 a2b5bef2
8c961e1a 8f1d6ca4 6137b986 7333d797
969e237d 82a44c81 e2a1d1ba 675f9507
a32711ee 16107bbc 454a4cb2 04d2abef
d5fd0c51 ce506a08 31f991da 0c8f645c
03c33a8b 203f6e8d 673d3ad6 fe7d5b88
c95efbcc 61dc8b33 77d34432 35096204
921610d8 9e2747fb 3b21e3f8 eb1d5b02
03010001 a381b030 81ad300f 0603551d
130101ff 04053003 0101ff30 0b060355
1d0f0404 03020106 301d0603 551d0e04
1604141a 8462bc48 4c332504 d4eed0f6
03c41946 d1946b30 6e060355 1d230467
30658014 1a8462bc 484c3325 04d4eed0
f603c419 46d1946b a149a447 3045310b
30090603 55040613 02424d31 19301706
0355040a 13105175 6f566164 6973204c
696d6974 6564311b 30190603 55040313
1251756f 56616469 7320526f 6f742043
```

```

64311b30 19060355 04031312 51756f56
61646973 20526f6f 74204341 20323082
0222300d 06092a86 4886f70d 01010105
00038202 0f003082 020a0282 0201009a
18ca4b94 0d002daf 03298af0 0f81c8ae
4c19851d 089fab29 4485f32f 81ad321e
9046bfa3 86261a1e fe7e1c18 3a5c9c60

```

```

7c5fe726 b3f73290 9850d437 7155f692
2178f795 79faf82d 26876656 3077a637
78335210 58ae3f61 8ef26ab1 ef187e4a
5963ca8d a256d5a7 2fbc561f cf39c1e2
fb0aa815 2c7d4d7a 63c66c97 443cd26f
c34a170a f890d257 a21951a5 2d9741da
074fa950 da908d94 46e13ef0 94fd1000
38f53be8 40e1b46e 561a20cc 6f588ded
2e458fd6 e9933fe7 b12cdf3a d6228cdc
84bb226f d0f8e4c6 39e90488 3cc3baeb
557a6d80 9924f56c 01fbf897 b0945beb
fdd26ff1 77680d35 6423acb8 55a103d1
4d4219dc f8755956 a3f9a849 79f8af0e
b911a07c b76aed34 d0b62662 381a870c
f8e8fd2e d3907f07 912a1dd6 7e5c8583
99b03808 3fe95ef9 3507e4c9 626e577f
a75095f7 bac89be6 8ea201c5 d666bf79
61f33c1c e1b9825c 5da0c3e9 d848bd19
a2111419 6eb2861b 683e4837 1a88b75d
965e9cc7 ef276208 e291195c d2f121dd
ba174282 97718153 31a99ff6 7d62bf72
e1a3931d cc8a265a 0938d0ce d70d8016
b478a53a 874c8d8a a5d54697 f22c10b9
bc5422c0 01506943 9ef4b2ef 6df8ecda
f1e3b1ef df918f54 2a0b25c1 2619c452
100565d5 8210eac2 31cd2e
quit
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
match default-inspection-traffic

```

```

41203282 02050930 0d06092a 864886f7
0d010105 05000382 0201003e 0a164d9f
065ba8ae 715d2f05 2f67e613 4583c436
f6f3c026 0c0db547 645df8b4 72c946a5
03182755 89787d76 ea963480 1720dce7
83f88dfc 07b8da5f 4d2e67b2 84fdd944
fc775081 e67cb4c9 0d0b7253 f8760707
4147960c fbe08226 93558cfe 221f6065

```

```

class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect nethios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error
policy-map type inspect dns
migrated_dns_map_2
parameters
message-length maximum client auto
message-length maximum 512
no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/service/DDCEService
destination address email
callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment

```

```

!
!
policy-map type inspect dns
  migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
  policy-map global_policy
    subscribe-to-alert-group inventory periodic
    monthly
    subscribe-to-alert-group configuration periodic
    monthly
    subscribe-to-alert-group telemetry periodic
    daily
  profile License

  destination address http
  https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination transport-method http
  Cryptochecksum:58e05ae70cb3ee6aeaa98534f
  adc0e52
: end

```

5.1.13 Protocols following in existing environment

Telnet

- By the use of Login credentials telnet allows users to log on to different hosts within the network.
- For the connection's protocol telnet use TCP.
- The service of telnet available on the host machine port 23.
- Telnet is a character based communication tool which is not be able to run GUI based tools. And it is also not used for the cursor transmission and other GUI terms.
- This is an inefficient protocol.
- While reaching to the other end every single keystroke required for the several context switches.
- Due to slow typing speeds telnet is expensive.

Core 1 Telnet

```
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
!
```

Core 2 Telnet

```
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
```

Access Switch 1(HR_MKT_VM) Telnet

```
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
```

Switch 2 (EX_MGR_FIN_IT.) Telnet

```
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
```

```
!
```

Access Switch 3 (Camera_Wifi.) Telnet

```
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
```

VLC Gateway Telnet

```
!
line con 0
line aux 0
line vty 0 4
login
transport input none
!
no scheduler allocate
!
```

HO_GW_1

```
!
line con 0
line aux 0
line vty 0 4
login
transport input none
!
no scheduler allocate
!
```

HO_GW_2

```
!
line con 0
line aux 0
line vty 0 4
login
transport input none
!
no scheduler allocate
```

!

SSH/Telnet

```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh version 2
console timeout 0
```

VLC-EDGE-FW

```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh version 2
console timeout 0
```

5.1.14 OSPF

- OSPF stands for Open Shortest Path First which is actually a routing protocol in Internet Protocol network. It operates within a single autonomous system and use a link state routing algorithm and also falls into the group of interior gateway protocol. (fouad)
- It is a very concerted processor which sustains multiple copies of routing information.
- It is also used to increase the amount of memory needed.
- OSPF actually logically divide using the areas.
- It is somehow difficult to learn rather than other protocols.
- If the whole network is in the use of OSPF, it controls the network and also inform the other connected routers if the linked was changes or bounce.

Core1 OSPF Protocol

CORE_1#show ip ospf 1 database

OSPF Router with ID (1.0.0.1) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#
Checksum Link count			
1.0.0.1	1.0.0.1	185	0x80000004
0x001AA7 5			
50.0.0.2	50.0.0.2	127	0x80000002
0x006152 2			
172.16.16.2	172.16.16.2		68
0x80000004 0x00BD79 4			
192.16.16.1	192.16.16.1		66
0x80000002 0x003F1D 2			
192.168.1.29	192.168.1.29		136
0x80000002 0x009021 1			
192.168.10.2	192.168.10.2		185
0x80000004 0x005190 4			

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#
Checksum			
50.0.0.1	192.168.1.29		136
0x80000001 0x004281			
172.16.16.2	172.16.16.2		128
0x80000001 0x006831			
192.16.16.2	172.16.16.2		68
0x80000001 0x0007D0			
192.162.10.2 1.0.0.1	185		0x80000001
0x00CE29			
192.168.10.2	192.168.10.2		187
0x80000001 0x001FEB			

Type-5 AS External Link States

Core2 Protocol

Backup_Core1#show ip ospf 1 database

OSPF Router with ID (192.168.10.2) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#
Checksum Link count			
1.0.0.1	1.0.0.1	1037	0x80000004
0x001AA7 5			
50.0.0.2	50.0.0.2	977	0x80000002
0x006152 2			
172.16.16.2	172.16.16.2		918
0x80000004 0x00BD79 4			
192.16.16.1	192.16.16.1		916
0x80000002 0x003F1D 2			
192.168.1.29	192.168.1.29		986
0x80000002 0x009021 1			
192.168.10.2	192.168.10.2		1035
0x80000004 0x005190 4			

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#
Checksum			
50.0.0.1	192.168.1.29		986
0x80000001 0x004281			
172.16.16.2	172.16.16.2		978
0x80000001 0x006831			
192.16.16.2	172.16.16.2		918
0x80000001 0x0007D0			
192.162.10.2 1.0.0.1			1037
0x80000001 0x00CE29			
192.168.10.2	192.168.10.2		1035
0x80000001 0x001FEB			

Type-5 AS External Link States

```

Link ID      ADV Router    Age      Seq#
Checksum Tag
0.0.0.0      192.168.1.29  984      0x80000001
0x0079B1 1
100.0.0.0      192.168.1.29  984
0x80000001 0x000DA7 0
192.168.1.0      192.168.1.29  984
0x80000001 0x006945 0

```

```

192.168.1.0      192.168.1.29  1834
0x80000001 0x006945 0

```

VLC_GATEWAY

Backup_Core1#show ip ospf 1 database

OSPF Router with ID (192.168.10.2)
(Process ID 1)

Router Link States (Area 0)

```

Link ID      ADV Router    Age      Seq#
Checksum Link count
1.0.0.1      1.0.0.1      1037     0x80000004
0x001AA7 5
50.0.0.2      50.0.0.2      977      0x80000002
0x006152 2
172.16.16.2      172.16.16.2      918
0x80000004 0x00BD79 4
192.16.16.1      192.16.16.1      916
0x80000002 0x003F1D 2
192.168.1.29      192.168.1.29      986
0x80000002 0x009021 1
192.168.10.2      192.168.10.2      1035
0x80000004 0x005190 4

```

Net Link States (Area 0)

```

Link ID      ADV Router    Age      Seq#
Checksum
50.0.0.1      192.168.1.29  986
0x80000001 0x004281
172.16.16.2      172.16.16.2      978
0x80000001 0x006831
192.16.16.2      172.16.16.2      918
0x80000001 0x0007D0
192.162.10.2      1.0.0.1      1037
0x80000001 0x00CE29
192.168.10.2      192.168.10.2      1035
0x80000001 0x001FEB

```

```

Link ID      ADV Router    Age      Seq#
Checksum Tag
0.0.0.0      192.168.1.29  1834
0x80000001 0x0079B1 1
100.0.0.0      192.168.1.29  1834
0x80000001 0x000DA7 0
192.168.1.0      192.168.1.29  1834
0x80000001 0x006945 0

```

HO_GW_1

HO_GW_1#sh ip ospf 1 database

OSPF Router with ID (50.0.0.2) (Process ID 1)

Router Link States (Area 0)

```

Link ID      ADV Router    Age      Seq#
Checksum Link count
1.0.0.1      1.0.0.1      1036     0x80000004
0x001AA7 5
50.0.0.2      50.0.0.2      981      0x80000002
0x006152 2
172.16.16.2      172.16.16.2      925
0x80000004 0x00BD79 4
192.16.16.1      192.16.16.1      923
0x80000002 0x003F1D 2
192.168.1.29      192.168.1.29      989
0x80000002 0x009021 1
192.168.10.2      192.168.10.2      1036
0x80000004 0x005190 4

```

Net Link States (Area 0)

```

Link ID      ADV Router    Age      Seq#
Checksum
50.0.0.1      192.168.1.29  989
0x80000001 0x004281
172.16.16.2      172.16.16.2      982
0x80000001 0x006831
192.16.16.2      172.16.16.2      925
0x80000001 0x0007D0
192.162.10.2      1.0.0.1      1036
0x80000001 0x00CE29

```

```

Type-5 AS External Link States
Link ID      ADV Router    Age      Seq#
Checksum Tag
0.0.0.0      192.168.1.29      1834
0x80000001 0x0079B1 1

0.0.0.0      192.168.1.29      1837
0x80000001 0x0079B1 1
100.0.0.0    192.168.1.29      1837
0x80000001 0x000DA7 0
192.168.1.0  192.168.1.29      1837
0x80000001 0x006945 0

HO_GW_2

HO_GW_2#sh ip ospf 1 database

        OSPF Router with ID (192.16.16.1)
        (Process ID 1)

        Router Link States (Area 0)

Link ID      ADV Router    Age      Seq#
Checksum Link count
1.0.0.1      1.0.0.1      1067     0x80000004
0x001AA7 5
50.0.0.2     50.0.0.2     1013     0x80000002
0x006152 2
172.16.16.2  172.16.16.2  957
0x80000004 0x00BD79 4
192.16.16.1  192.16.16.1  953
0x80000002 0x003F1D 2
192.168.1.29 192.168.1.29 1021
0x80000002 0x009021 1
192.168.10.2 192.168.10.2 1067
0x80000004 0x005190 4

        Net Link States (Area 0)

Link ID      ADV Router    Age      Seq#
Checksum
50.0.0.1     192.168.1.29 1021
0x80000001 0x004281
172.16.16.2  172.16.16.2  1012
0x80000001 0x006831

```

```

192.16.16.2      172.16.16.2      957
0x80000001 0x0007D0
192.162.10.2     1.0.0.1      1067
0x80000001 0x00CE29
192.168.10.2     192.168.10.2  1067
0x80000001 0x001FEB

```

Type-5 AS External Link States

VLC-EDGE-FW

```

!
object network LAN
 nat (any outside) dynamic interface
router ospf 1
 network 50.0.0.0 255.255.255.0 area 0
 network 50.0.0.0 255.0.0.0 area 0
 network 60.0.0.0 255.255.255.0 area 0
 network 60.0.0.0 255.0.0.0 area 0
 log-adj-changes
 redistribute connected
 redistribute static
 default-information originate
!

```

5.1.15DHCP

DHCP stands for dynamic host configuration protocol which actually assigns ip address to devices when we are connected to internet. It will become a single point of failure when we have one DHCP server because it does not able to request. It will deliver wrong information in DHCP clients if it contains. (Rouse)

```

Access Switch1 (HR_MKT_VM)
!
ip dhcp excluded-address 10.0.0.1
ip dhcp excluded-address 10.0.0.2
ip dhcp excluded-address 10.0.0.3
ip dhcp excluded-address 10.0.0.4
ip dhcp excluded-address 10.0.0.5
ip dhcp excluded-address 10.0.0.1 10.0.0.10
!
ip dhcp pool HR_MKT_VM_DHCP
 network 10.0.0.0 255.255.255.0
 default-router 10.0.0.1
 dns-server 8.8.8.8
!

Switch 2 (EX_MGR_FIN_IT)
!
ip dhcp excluded-address 20.0.0.1 20.0.0.10
!
ip dhcp pool EX_MGR_FN_IT
 network 20.0.0.0 255.0.0.0
 default-router 20.0.0.1 255.255.255.0
 dns-server 8.8.8.8
!
no ip domain-lookup
ip sct
no ipv6 sct
!

Access Switch 3 (Camera_Wifi)
!
ip dhcp excluded-address 30.0.0.1 30.0.0.10
!
ip dhcp pool Cam_Wifi
 network 30.0.0.0 255.255.255.0
 default-router 30.0.0.1
 dns-server 8.8.8.8
!

```

```

!
!
no ip domain-lookup
ip cef
no ipv6 cef
!

```

5.1.16 Spanning tree protocol

- Spanning tree protocol developed before switches. It is a Layer 2 protocol which is used to avert the looping cause in network and also repair the network failures or changings due to the redundant loops. (Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches, 2019)
- Spanning Tree protocol actually an old protocol which is sometimes not efficient for the implementation of network disruption.
- STP actually maintain a single path and traffic flows from one node to another which is actually sometimes restrict or blocks some traffic or paths.
- It is acceptable in the past but in the various virtualized technology it is not reliable that can handle virtualized infrastructure.

5.1.17 DHCP IP allocation

DHCP

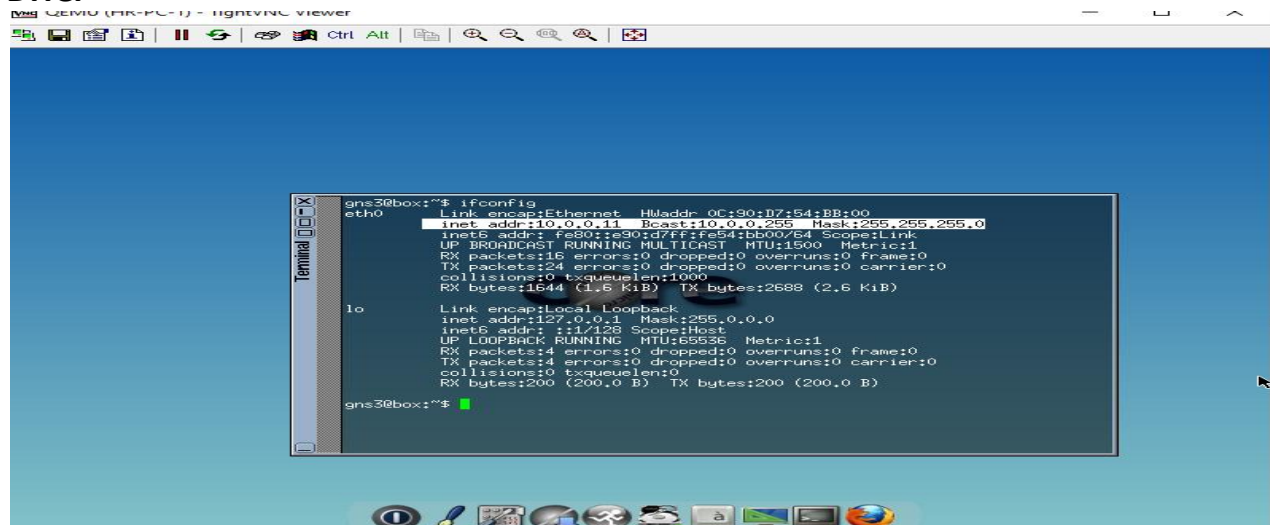
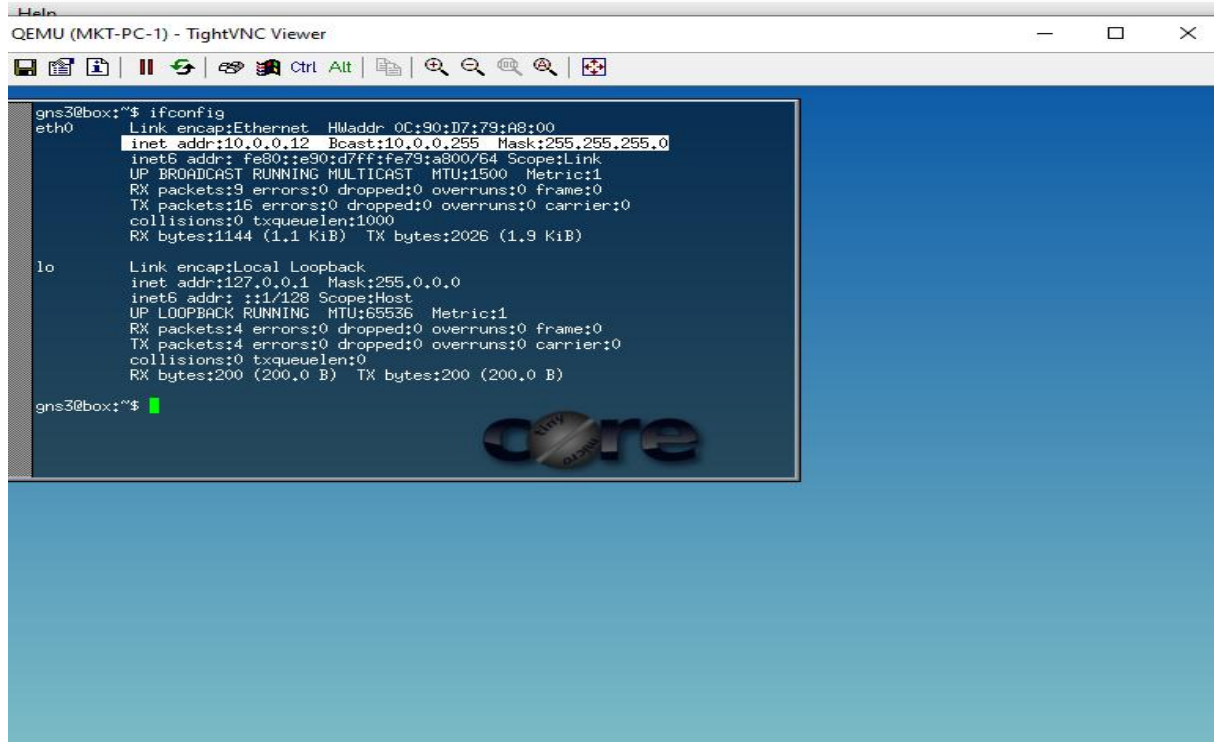


Figure VI: HR_PC_1

Description: The HR PC is obtaining dhcp allocated address successfully which is 10.0.0.11 on VLAN 10



```

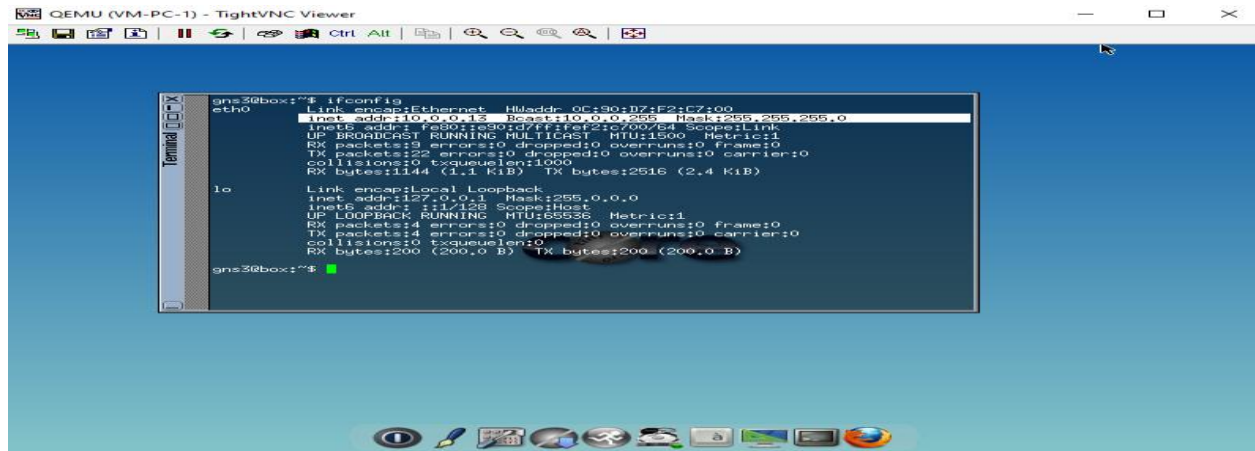
gns3@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:90:D7:79:A8:00
          inet addr:10.0.0.11  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::e90:d7ff:fe79:a800/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1144 (1.1 KiB)  TX bytes:2026 (1.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:200 (200.0 B)  TX bytes:200 (200.0 B)

gns3@box:~$
  
```

Figure VII: MKT-PC-1

Description: The MKT PC is obtaining dhcp allocated address successfully which is 10.0.0.12 on VLAN 10



```

gns3@box:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 0C:90:D7:F2:67:00
          inet addr:10.0.0.12  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::e90:d7ff:fe72:c700/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1144 (1.1 KiB)  TX bytes:2516 (2.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:200 (200.0 B)  TX bytes:200 (200.0 B)

gns3@box:~$
  
```

Figure VIII: VM-PC-1

Description: The VM PC is obtaining dhcp allocated address successfully which is 10.0.0.13 on VLAN 10

```
WIFICAM>
WIFICAM> ip dhcp
DDORA IP 30.0.0.11/24 GW 30.0.0.1

WIFICAM> show
```

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
WIFICAM	30.0.0.11/24	30.0.0.1	00:50:79:66:68:00	10140	127.0.0.1:10141
	fe80::250:79ff:fe66:6800/64				

Figure IX: WIFI_CAM

Description: The Wifi & Camera PC is obtaining dhcp allocated address successfully which is 30.0.0.11 on VLAN 30

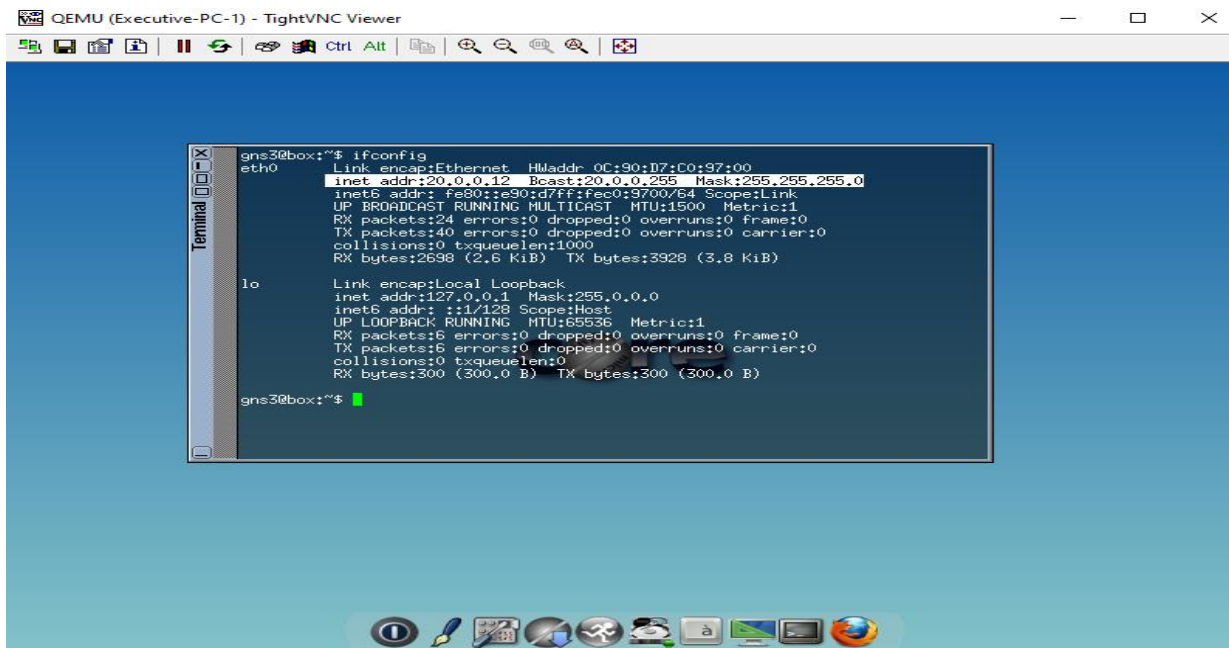


Figure X: EXECUTIVE-PC-1

Description: The Executive PC is obtaining DHCP allocated address successfully which is 20.0.0.12 on VLAN 20

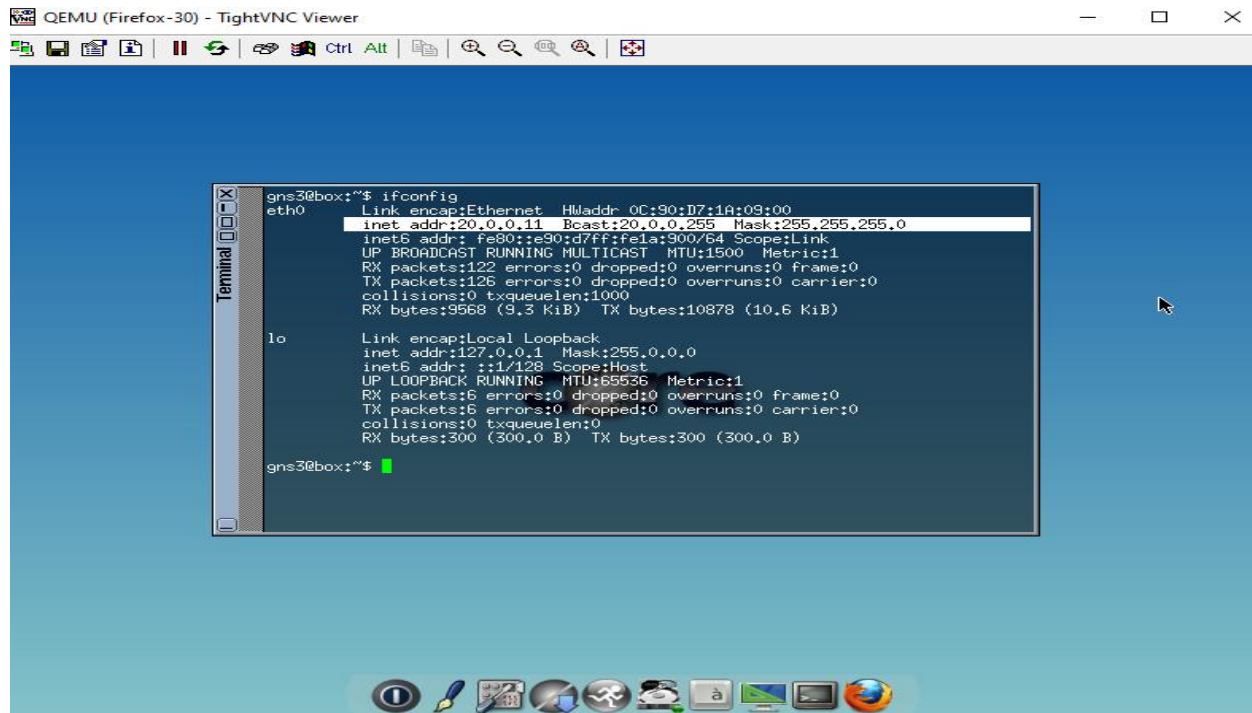


Figure XI: FINANCE-30

Description: The FINANCE PC is obtaining DHCP allocated address successfully which is 20.0.0.11 on VLAN 20

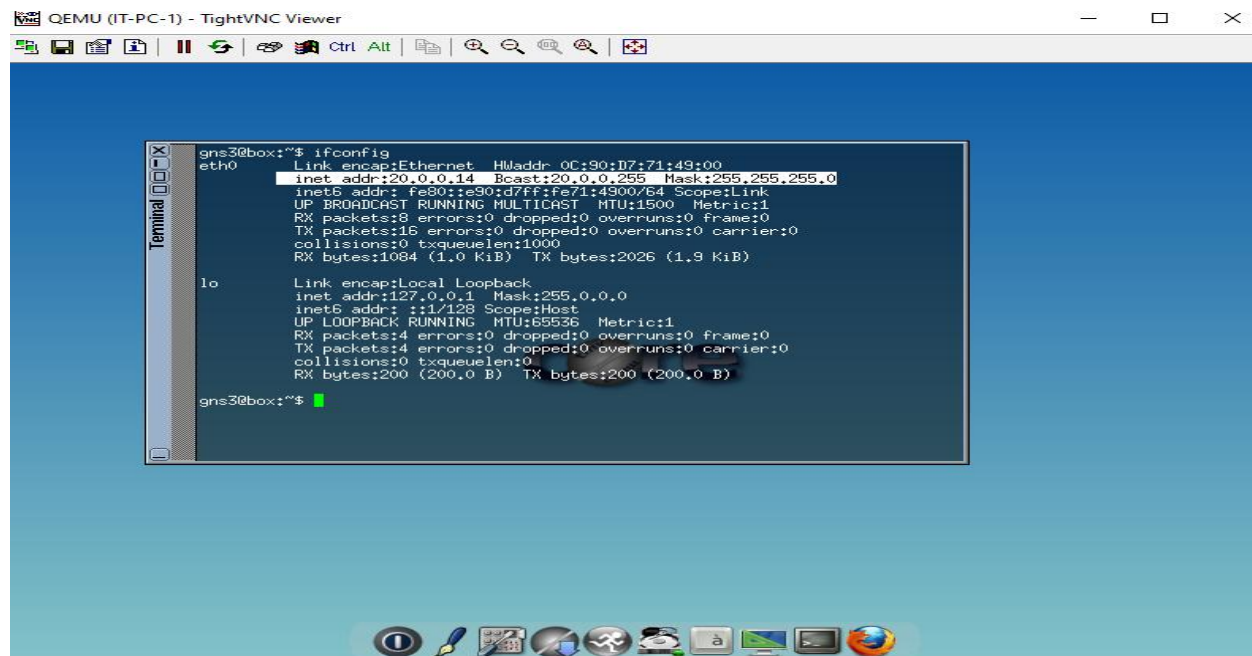
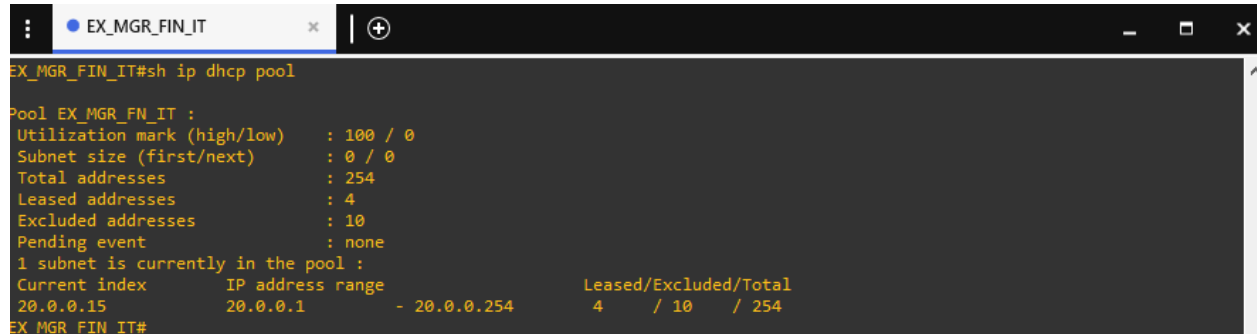


Figure XII: IT-PC-1

Description: The FINANCE PC is obtaining dhcp allocated address successfully which is 20.0.0.14 on VLAN 20

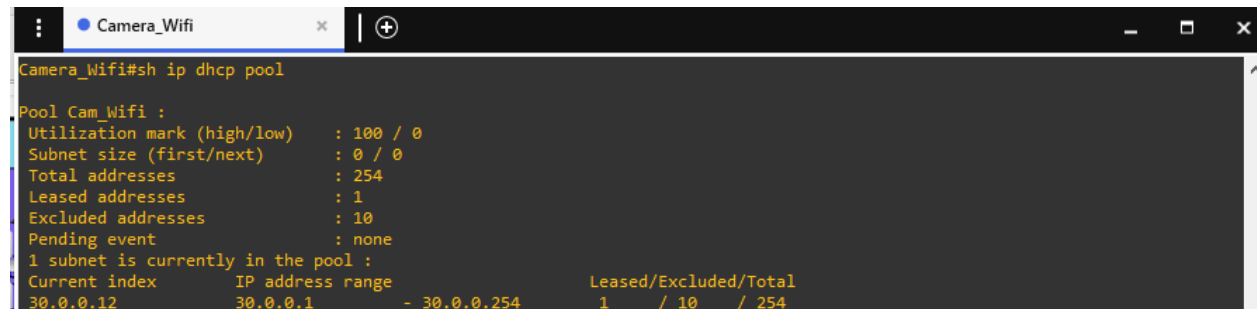


```

EX_MGR_FIN_IT#sh ip dhcp pool
Pool EX_MGR_FN_IT :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)       : 0 / 0
Total addresses                 : 254
Leased addresses                : 4
Excluded addresses             : 10
Pending event                  : none
1 subnet is currently in the pool :
Current index      IP address range      Leased/Excluded/Total
20.0.0.15         20.0.0.1       - 20.0.0.254      4    / 10    / 254
EX MGR FIN IT#
  
```

Figure XIII: EX-MGR-FIN-IT

Description: The DHCP server is successfully created on EX_MGR_FIN_IT Switch running on VLAN 20 having 20.0.0.1 as a gateway.

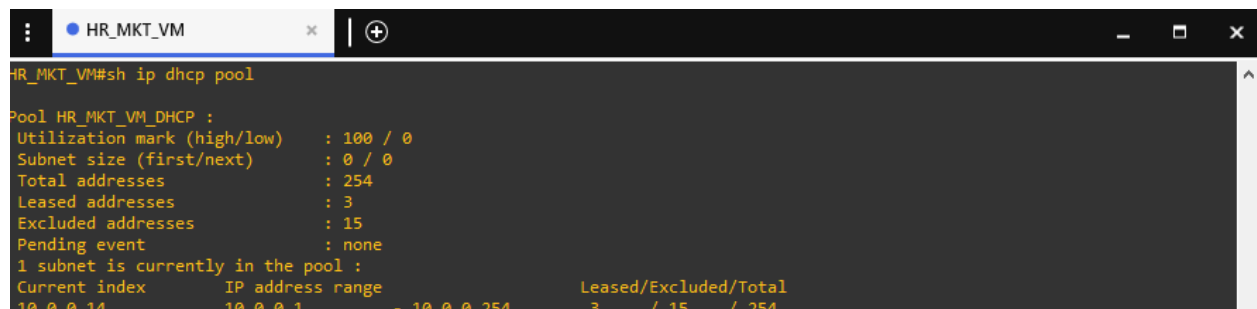


```

Camera_Wifi#sh ip dhcp pool
Pool Cam_Wifi :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)       : 0 / 0
Total addresses                 : 254
Leased addresses                : 1
Excluded addresses             : 10
Pending event                  : none
1 subnet is currently in the pool :
Current index      IP address range      Leased/Excluded/Total
30.0.0.12         30.0.0.1       - 30.0.0.254      1    / 10    / 254
  
```

Figure XIV: CAMERA-WIFI

Description: The DHCP server is successfully created on Camera_wifi Switch running on VLAN 30 having 30.0.0.1 as a gateway.



```

HR_MKT_VM#sh ip dhcp pool
Pool HR_MKT_VM_DHCP :
Utilization mark (high/low)    : 100 / 0
Subnet size (first/next)       : 0 / 0
Total addresses                 : 254
Leased addresses                : 3
Excluded addresses             : 15
Pending event                  : none
1 subnet is currently in the pool :
Current index      IP address range      Leased/Excluded/Total
10.0.0.14         10.0.0.1       - 10.0.0.254      3    / 15    / 254
  
```

Figure XV: HR-MKT-VM

Description: The DHCP server is successfully created on HR_MKT_VM Switch running on VLAN 10 having 10.0.0.1 as a gateway.

5.1.18 Ip Routes

```

CORE1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, Su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       Ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.162.10.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.162.10.1, 00:00:00, Ethernet0/0
L 1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 1.0.0.0/24 is directly connected, Loopback0
L 1.0.0.1/32 is directly connected, Loopback0
L 10.0.0.0/24 is directly connected, Vlan10
C 10.0.0.1/32 is directly connected, Vlan10
C 20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 20.0.0.0/24 is directly connected, Vlan20
C 20.0.0.1/32 is directly connected, Vlan20
C 30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 30.0.0.0/24 is directly connected, Vlan30
C 30.0.0.1/32 is directly connected, Vlan30
C 50.0.0.0/24 is subnetted, 1 subnets
O 50.0.0.0 [110/12] via 192.162.10.1, 00:00:00, Ethernet0/0
C 60.0.0.0/24 is subnetted, 1 subnets
O 60.0.0.0 [110/12] via 192.162.10.1, 00:00:00, Ethernet0/0
O E2 100.0.0.0/8 [110/20] via 192.162.10.1, 00:00:00, Ethernet0/0
C 172.16.0.0/24 is subnetted, 1 subnets
O 172.16.16.0 [110/11] via 192.162.10.1, 00:00:00, Ethernet0/0
O 192.16.16.0/24 [110/11] via 192.162.10.1, 00:00:00, Ethernet0/0
C 192.162.10.0/24 is variably subnetted, 2 subnets, 2 masks
L 192.162.10.0/24 is directly connected, Ethernet0/0
L 192.162.10.2/32 is directly connected, Ethernet0/0
O E2 192.168.1.0/24 [110/20] via 192.162.10.1, 00:00:00, Ethernet0/0
O 192.168.10.0/24 [110/11] via 192.162.10.1, 00:00:00, Ethernet0/0

CORE1#
CORE1#
CORE1#
CORE1#
CORE1#

```

Figure XVI: Core1

Description: After running static and dynamic protocol (OSPF) we obtained the above routes in our core switch1.

```

Backup_Core1#ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, LI - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
        + - replicated route, % - next hop override

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.168.10.1, 00:08:16, Ethernet0/0
O    1.0.0.0/32 is subnetted, 1 subnets
O    1.0.0.1 [110/12] via 192.168.10.1, 00:09:22, Ethernet0/0
O    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.24 is directly connected, Vlan10
L    10.0.0.1/32 is directly connected, Vlan10
O    20.0.0.0/24 is directly connected, Vlan20
L    20.0.0.1/32 is directly connected, Vlan20
C    30.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    30.0.0.24 is directly connected, Vlan30
L    30.0.0.2/32 is directly connected, Vlan30
O    50.0.0.0/24 is subnetted, 1 subnets
O    50.0.0.0 [110/12] via 192.168.10.1, 00:08:16, Ethernet0/0
O    60.0.0.0/24 is subnetted, 1 subnets
O    60.0.0.0 [110/12] via 192.168.10.1, 00:08:16, Ethernet0/0
O E2 100.0.0.0/8 [110/20] via 192.168.10.1, 00:08:16, Ethernet0/0
O    172.16.0.0/24 is subnetted, 1 subnets
O    172.16.16.0 [110/11] via 192.168.10.1, 00:09:22, Ethernet0/0
O    192.16.16.0/24 [110/11] via 192.168.10.1, 00:09:22, Ethernet0/0
O    192.162.10.0/24 [110/11] via 192.168.10.1, 00:09:22, Ethernet0/0
O E2 192.168.1.0/24 [110/20] via 192.168.10.1, 00:08:16, Ethernet0/0
--More--
Jul 2 13:05:12.676: RIP-4-DUP/000: Duplicate address 10.0.0.1 on Vlan10, sourced by aabb.cc80.0300
C    192.168.10.0/24 is directly connected, Ethernet0/0
L    192.168.10.2/32 is directly connected, Ethernet0/0
Backup_Core1#
Backup_Core1#
Backup_Core1#
Backup_Core1#

```

Figure XVII:Backup_Core1

Description: After running static and dynamic protocol (OSPF) we obtained the above routes in our backup_core1.

```

VLC_GATEWAY#ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, LI - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
        + - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is 172.16.16.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 172.16.16.1, 00:08:16, GigabitEthernet0/0
O    1.0.0.0/32 is subnetted, 1 subnets
O    1.0.0.1 [110/2] via 192.162.10.2, 00:09:25, GigabitEthernet0/1
O    10.0.0.0/24 is subnetted, 1 subnets
O    10.0.0.0 [110/2] via 192.168.10.2, 00:09:15, GigabitEthernet0/2
O    20.0.0.0/24 is subnetted, 1 subnets
O    20.0.0.0 [110/2] via 192.168.10.2, 00:09:15, GigabitEthernet0/2
O    30.0.0.0/24 is subnetted, 1 subnets
O    30.0.0.0 [110/2] via 192.168.10.2, 00:09:25, GigabitEthernet0/1
O    50.0.0.0/24 is subnetted, 1 subnets
O    50.0.0.0 [110/2] via 192.168.10.2, 00:09:15, GigabitEthernet0/2
O    60.0.0.0/24 is subnetted, 1 subnets
O    60.0.0.0 [110/2] via 192.162.10.2, 00:09:25, GigabitEthernet0/1
O    50.0.0.0/24 is subnetted, 1 subnets
O    50.0.0.0 [110/2] via 172.16.16.1, 00:08:16, GigabitEthernet0/0
O E2 100.0.0.0/8 [110/20] via 172.16.16.1, 00:06:14, GigabitEthernet0/3
O    172.16.0.0/24 is variably subnetted, 2 subnets, 2 masks
L    172.16.16.0/24 is directly connected, GigabitEthernet0/0
L    172.16.16.2/32 is directly connected, GigabitEthernet0/0
O    192.16.16.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.162.10.0/24 is directly connected, GigabitEthernet0/1
L    192.162.10.1/32 is directly connected, GigabitEthernet0/1
O E2 192.168.1.0/24 [110/20] via 172.16.16.1, 00:08:16, GigabitEthernet0/0
O    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/2
L    192.168.10.1/32 is directly connected, GigabitEthernet0/2

```

Figure XVIII: VLC_Gateway

Description: After running static and dynamic protocol (OSPF) we obtained the above routes in our VLC_GATEWAY.

```
HO_GW_1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        Ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is 50.0.0.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 50.0.0.1, 00:09:40, GigabitEthernet0/0
      1.0.0.0/32 is subnetted, 1 subnets
      O 1.0.0.1 [110/3] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
      O 10.0.0.0/24 is subnetted, 1 subnets
      O 10.0.0.0 [110/3] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
      O 20.0.0.0/24 is subnetted, 1 subnets
      O 20.0.0.0 [110/3] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
      O 30.0.0.0/24 is subnetted, 1 subnets
      O 30.0.0.0 [110/3] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
      O 50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
      C 50.0.0.0/24 is directly connected, GigabitEthernet0/0
      L 50.0.0.2/32 is directly connected, GigabitEthernet0/0
      O 60.0.0.0/24 is subnetted, 1 subnets
      O 60.0.0.0 [110/3] via 172.16.16.2, 00:06:41, GigabitEthernet0/1
      O E2 100.0.0.0/8 [110/20] via 50.0.0.1, 00:09:40, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
      C 172.16.16.0/24 is directly connected, GigabitEthernet0/1
      L 172.16.16.1/32 is directly connected, GigabitEthernet0/1
      O 192.16.16.0/24 [110/2] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
      O 192.162.10.0/24 [110/2] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
      O E2 192.168.1.0/24 [110/20] via 50.0.0.1, 00:09:40, GigabitEthernet0/0
      O 192.168.10.0/24 [110/2] via 172.16.16.2, 00:00:55, GigabitEthernet0/1
HO_GW_1#
HO_GW_1#
HO_GW_1#
HO_GW_1#
HO_GW_1#
HO_GW_1#
```

Figure XIX: HO_GW_1

Description: After running static and dynamic protocol (OSPF) we obtained the above routes in our HO_GW_1.

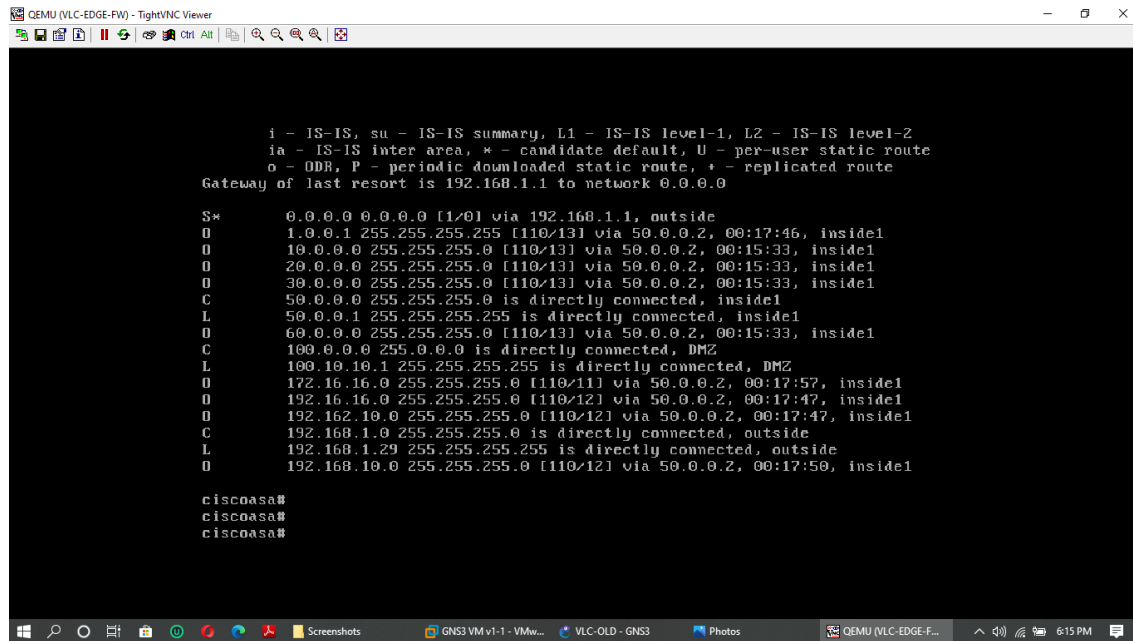
```
HO_GW_2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        Ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        a - application route
        + - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is 192.16.16.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      1.0.0.0/32 is subnetted, 1 subnets
      O 1.0.0.1 [110/3] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O 10.0.0.0/24 is subnetted, 1 subnets
      O 10.0.0.0 [110/3] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O 20.0.0.0/24 is subnetted, 1 subnets
      O 20.0.0.0 [110/3] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O 30.0.0.0/24 is subnetted, 1 subnets
      O 30.0.0.0 [110/3] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O 50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
      C 50.0.0.0/24 is directly connected, GigabitEthernet0/1
      L 50.0.0.2/32 is directly connected, GigabitEthernet0/1
      O 60.0.0.0/24 is subnetted, 1 subnets
      O 60.0.0.0 [110/3] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O E2 100.0.0.0/8 [110/20] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
      C 172.16.16.0/24 is directly connected, GigabitEthernet0/0
      L 172.16.16.1/32 is directly connected, GigabitEthernet0/0
      O 192.162.10.0/24 [110/2] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O E2 192.168.1.0/24 [110/20] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
      O 192.168.10.0/24 [110/2] via 192.16.16.2, 00:10:55, GigabitEthernet0/0
HO_GW_2#
HO_GW_2#
HO_GW_2#
HO_GW_2#
HO_GW_2#
HO_GW_2#
```

Figure XX: HO_GW_2

Description: After running static and dynamic protocol (OSPF) we obtained the above routes in our HO_GW_2.



```

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
O      1.0.0.1 255.255.255.255 [110/13] via 50.0.0.2, 00:17:46, inside1
O      10.0.0.0 255.255.255.0 [110/13] via 50.0.0.2, 00:15:33, inside1
O      20.0.0.0 255.255.255.0 [110/13] via 50.0.0.2, 00:15:33, inside1
O      30.0.0.0 255.255.255.0 [110/13] via 50.0.0.2, 00:15:33, inside1
C      50.0.0.0 255.255.255.0 is directly connected, inside1
L      50.0.0.1 255.255.255.255 is directly connected, inside1
O      60.0.0.0 255.255.255.0 [110/13] via 50.0.0.2, 00:15:33, inside1
C      100.0.0.0 255.0.0.0 is directly connected, DMZ
L      100.10.10.1 255.255.255.255 is directly connected, DMZ
O      172.16.16.0 255.255.255.0 [110/11] via 50.0.0.2, 00:17:57, inside1
O      192.16.16.0 255.255.255.0 [110/12] via 50.0.0.2, 00:17:47, inside1
O      192.162.10.0 255.255.255.0 [110/12] via 50.0.0.2, 00:17:47, inside1
C      192.168.1.0 255.255.255.0 is directly connected, outside
L      192.168.1.29 255.255.255.255 is directly connected, outside
O      192.168.10.0 255.255.255.0 [110/12] via 50.0.0.2, 00:17:50, inside1

ciscoasa#
ciscoasa#
ciscoasa#
  
```

Figure XXI: VLC-EDGE-FW

Description: After running static and dynamic protocol (OSPF) we obtained the above routes in our EDGE Firewall

5.1.19 Malware Protection

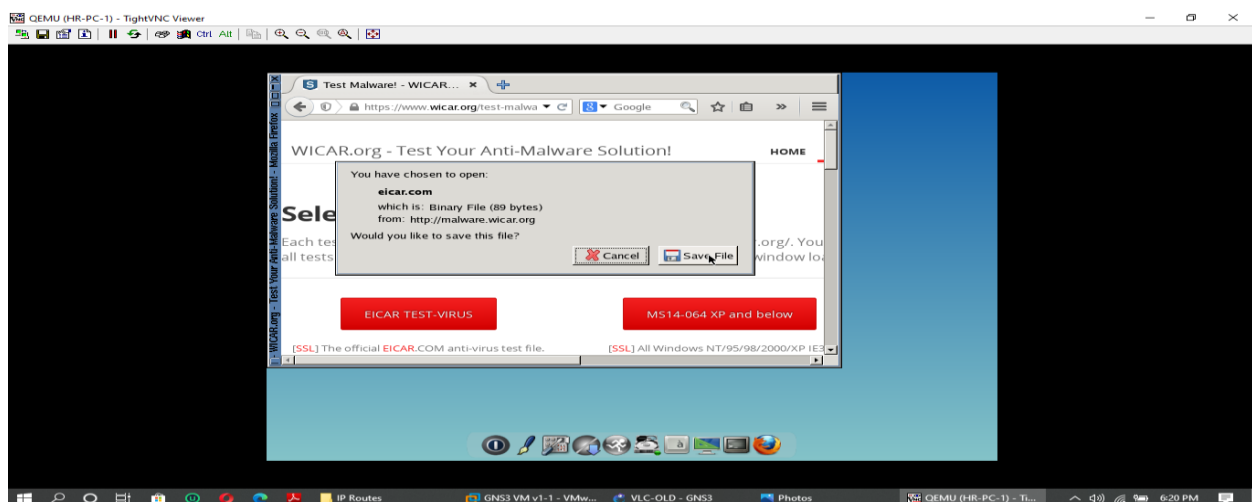


Figure XXII: HR-PC-1 PING

Description: Here we used the wicar.org website to test their security condition. So we executed a malware link inside from VLC network and unluckily the firewall didn't block the malware and allowed to access which made it vulnerable. We realized their existing network is opened to the threats and ransomware.

5.1.20 PING

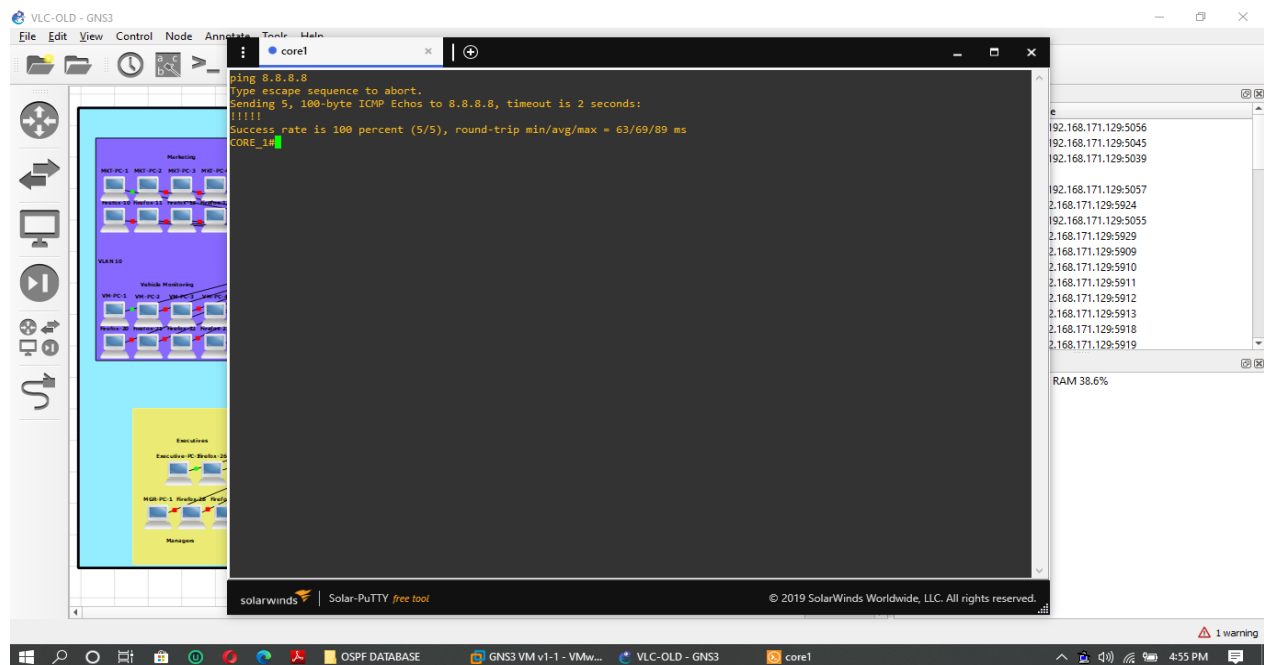


Figure XXIII: CORE1_PING

Description: Here we did ping from Core1 to google DNS server 8.8.8.8 and got an average rate of 69 milliseconds. (Peeva, 2013)

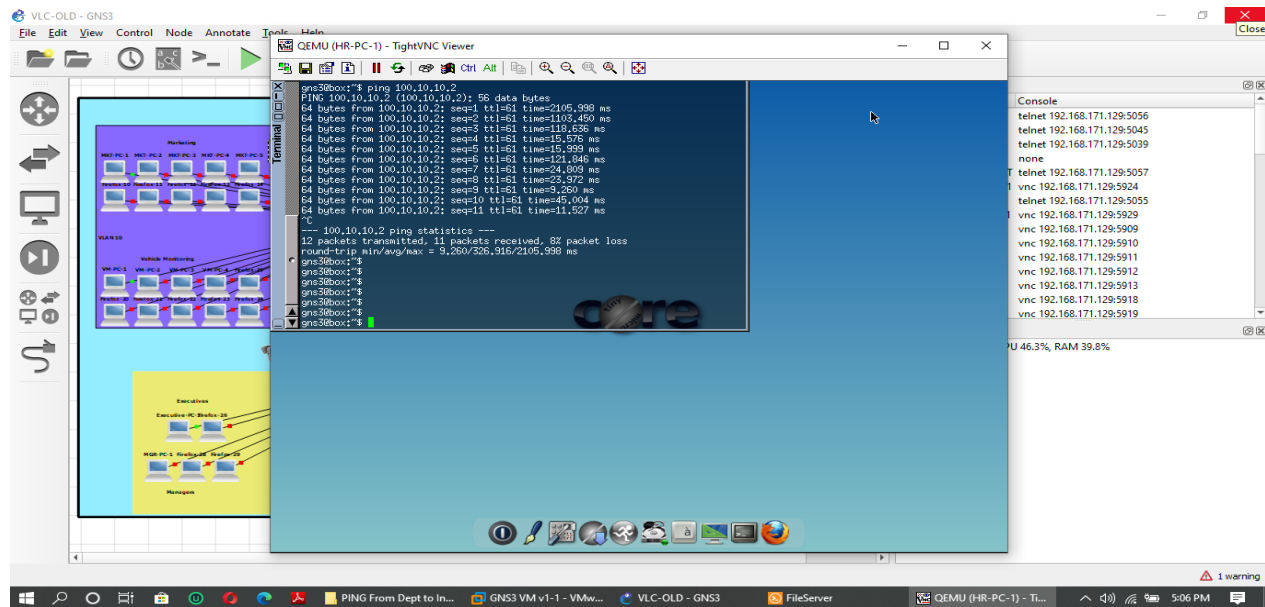


Figure XXIV:HR-PC-1 PING

Description: Here we did ping from HR_PC_1 to Head Office Fileserver 100.10.10.2 and got an average rate of 326.916 milliseconds of roundtrip time.

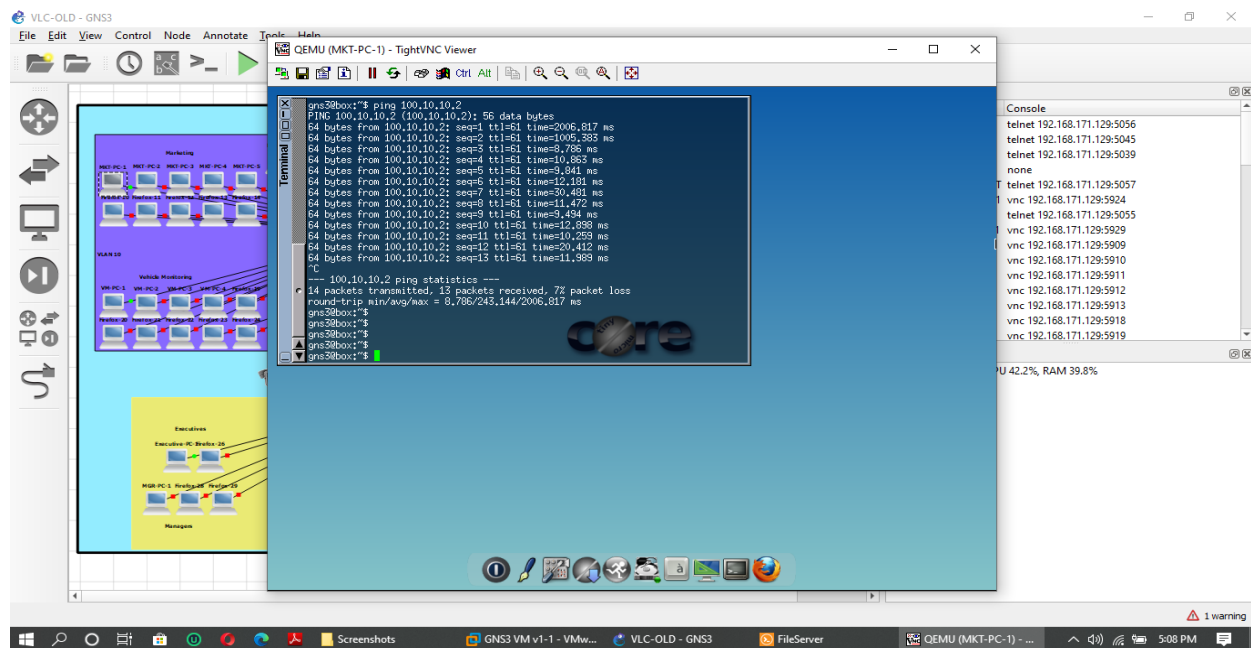


Figure XXV: MKT-PC-1 PING

Description: Here we did ping from MKT_PC_1 to Head Office Fileserver 100.10.10.2 and got an average rate of 243.144 milliseconds of roundtrip time.

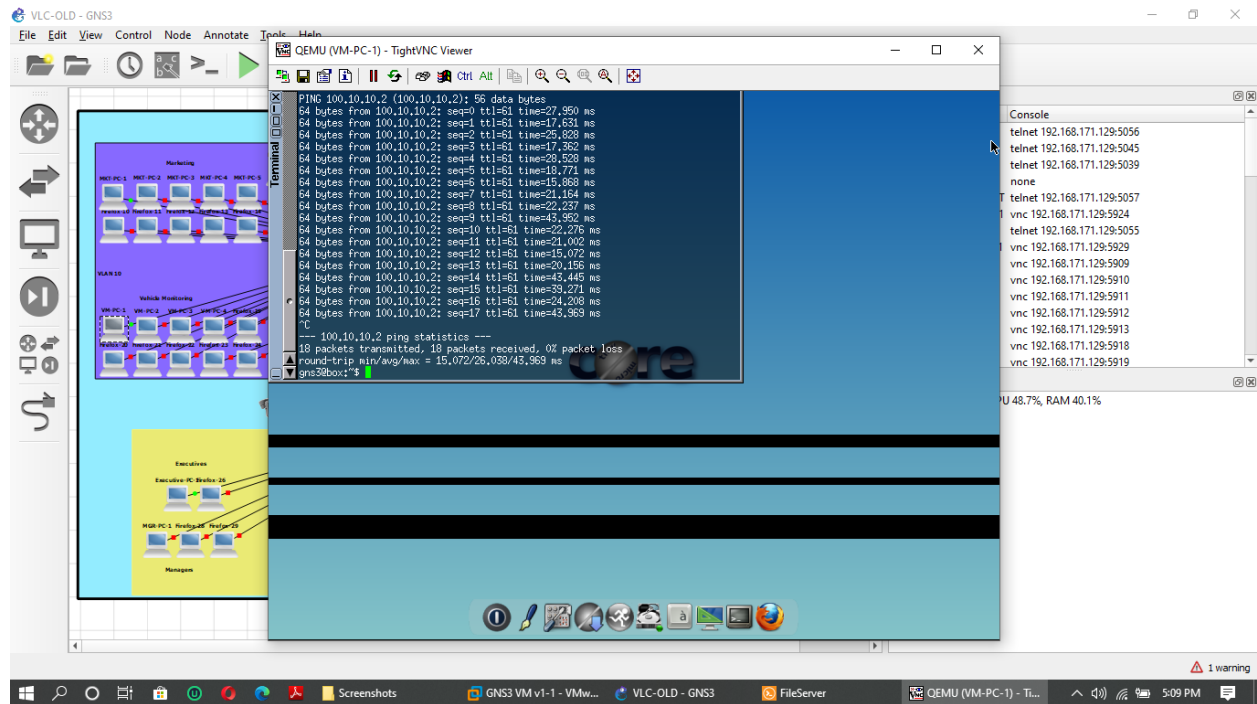


Figure XXVI: VM-PC-1 PING

Description: Here we did ping from VM_PC_1 to Head Office Fileserver 100.10.10.2 and got an average rate of 26.038 milliseconds of roundtrip time.

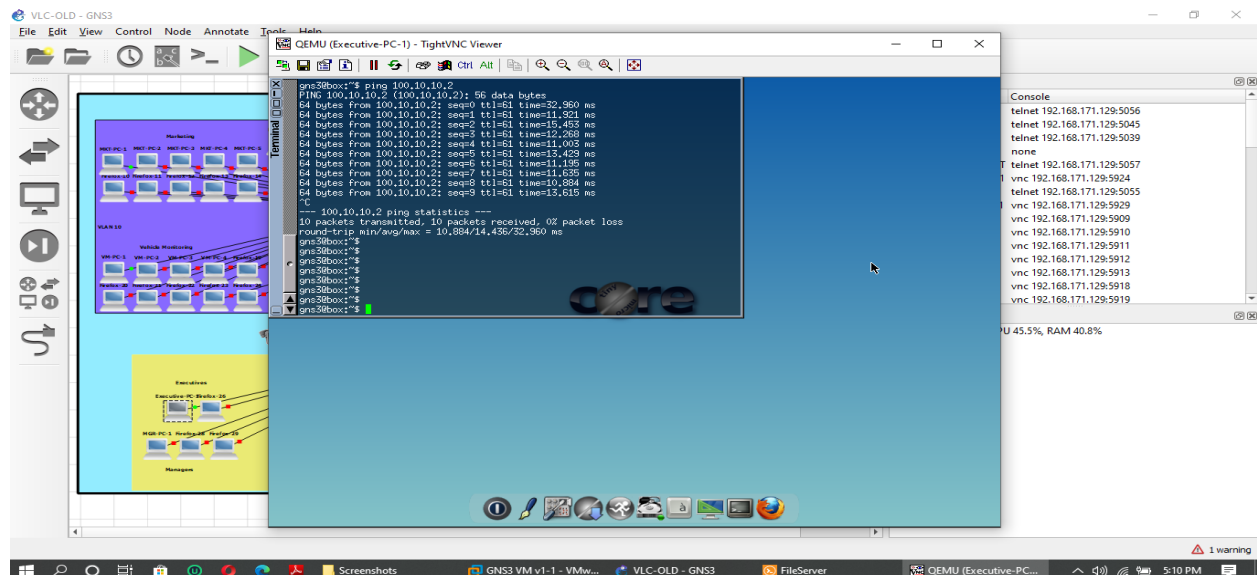


Figure XXVII:EXECUTIVE-PC-1 PING

Description: Here we did ping from Executive_PC_1 to Head Office Fileserver 100.10.10.2 and got an average rate of 14.436 milliseconds of roundtrip time.

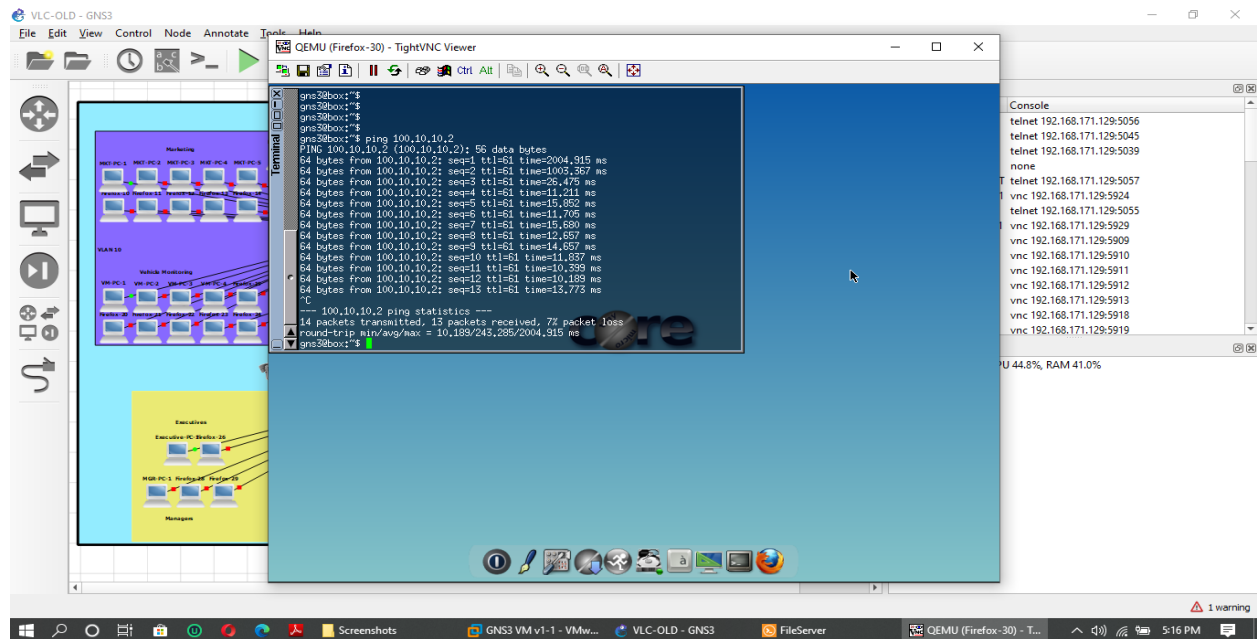


Figure XXVIII: FINANCE_PC_1 PING

Description: Here we did ping from FINANCE_PC_1 to Head Office Fileserver 100.10.10.2 and got an average rate of 243.285 milliseconds of roundtrip time.

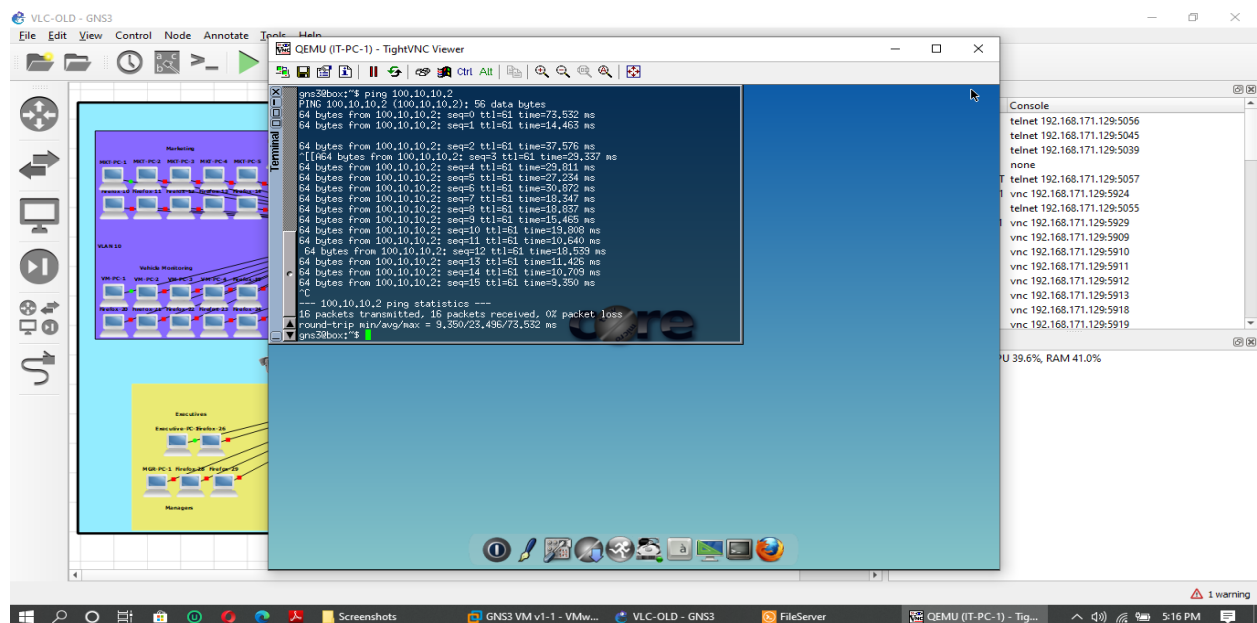


Figure XXIX: IT-PC-1 PING

Description: Here we did ping from IT_PC_1 to Head Office Fileserver 100.10.10.2 and got an average rate of 23.496 milliseconds of roundtrip time.

Department to Internet

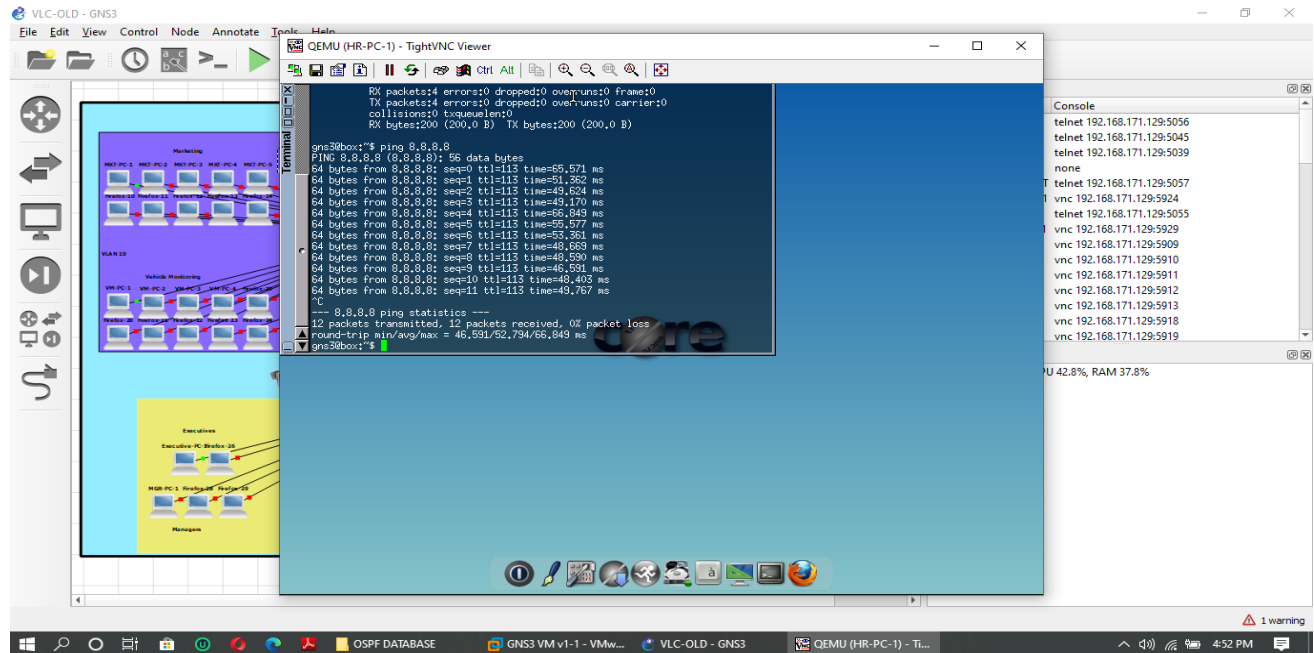


Figure XXX: HR-PC-1 PING

Description: Here we did ping from HR-PC-1 to Google DNS Server 8.8.8.8 and got an average rate of 52.794 milliseconds of roundtrip time.

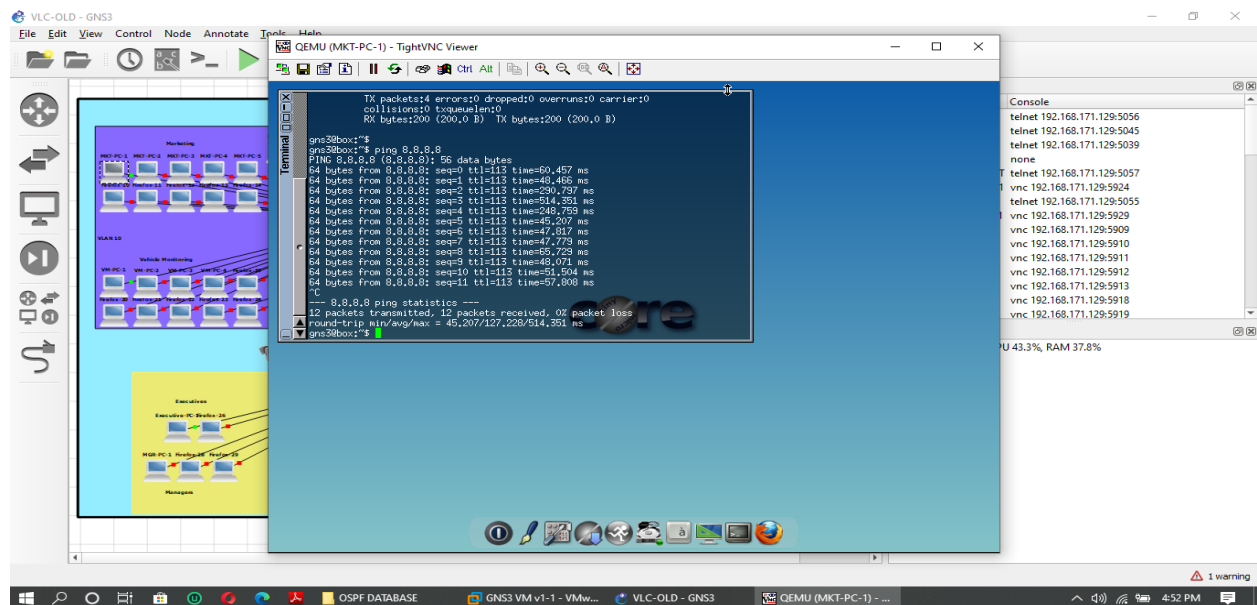


Figure XXXI: MKT-PC-1 PING

Description: Here we did ping from MKT-PC-1 to Google DNS Server 8.8.8.8 and got an average rate of 127.228 milliseconds of roundtrip time.

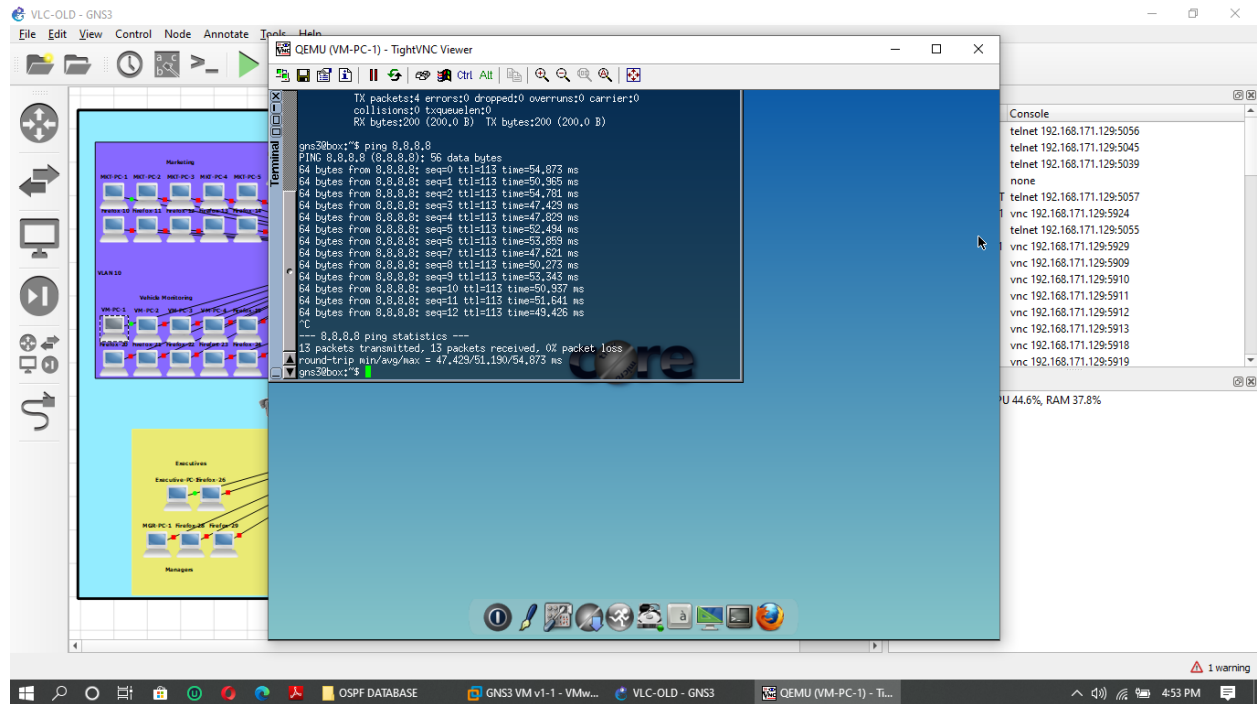


Figure XXXII: VM-PC-1 PING

Description: Here we did ping from VM-PC-1 to Google DNS Server 8.8.8.8 and got an average rate of 51.190 milliseconds of roundtrip time.

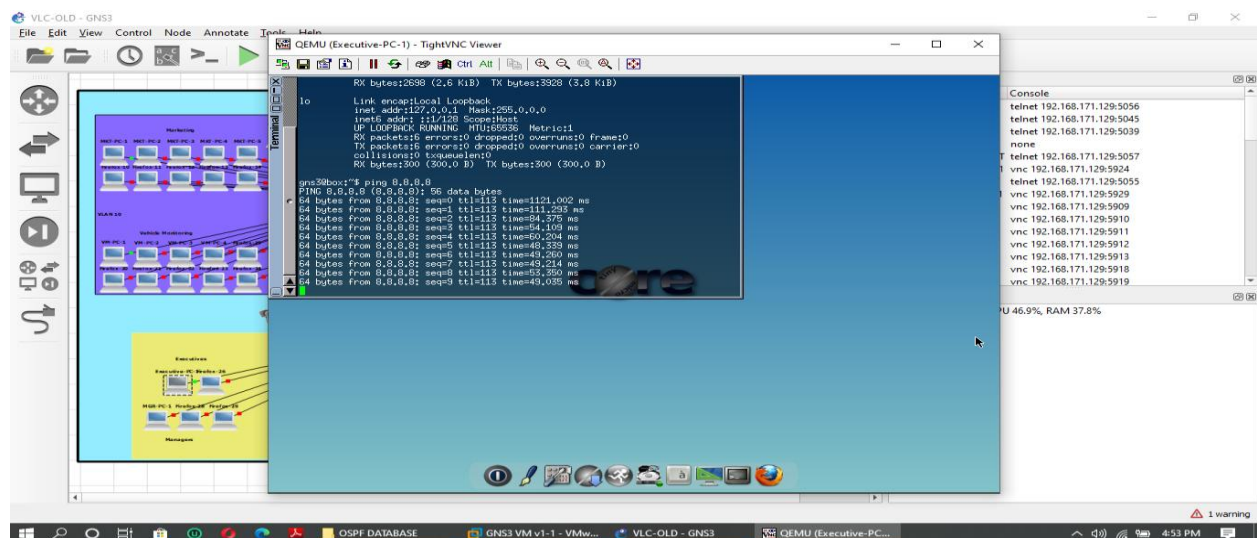


Figure XXXIII: EXECUTIVE-PC-1 PING

Description: Here we did ping from Executive-PC-1 to Google DNS Server 8.8.8 and got an average rate of 49.260 milliseconds of roundtrip time.

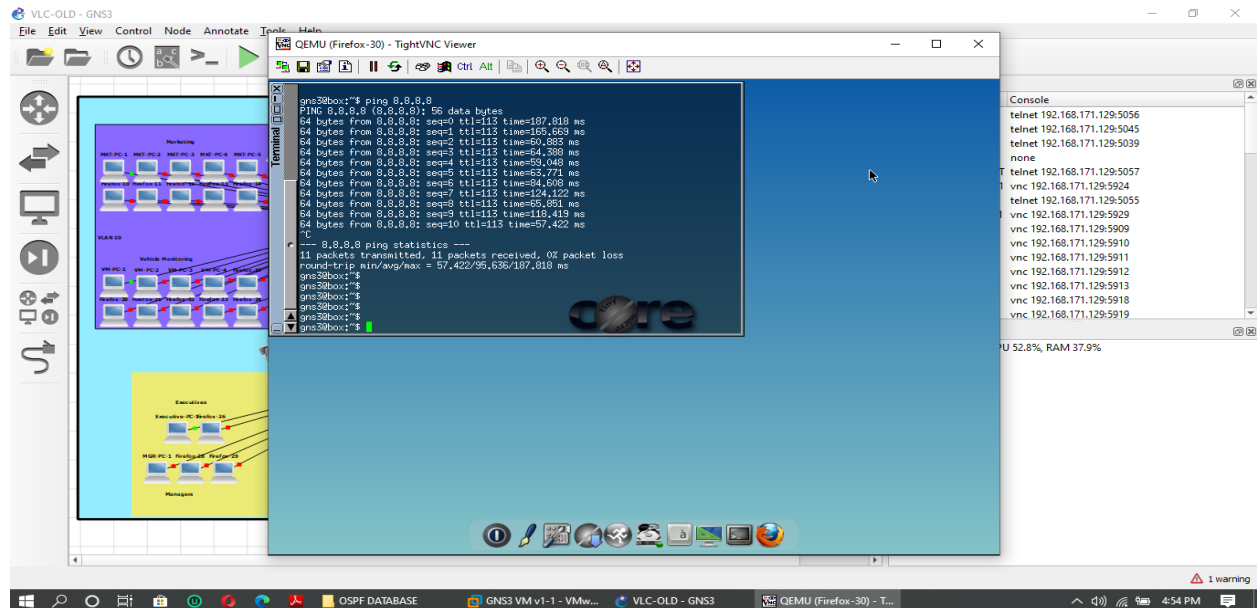


Figure XXXIV: FIREFOX-30 PING

Description: Here we did ping from Finance-PC-1 to Google DNS Server 8.8.8 and got an average rate of 95.636 milliseconds of roundtrip time.

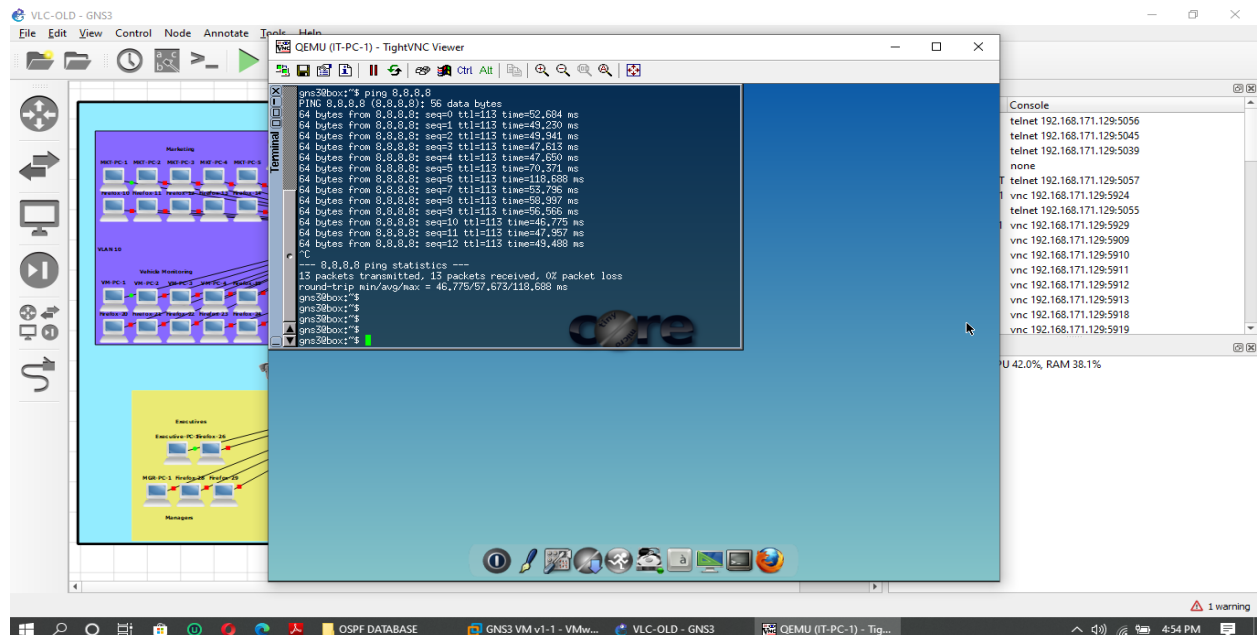


Figure XXXV: IT-PC-1 PING

Description: Here we did ping from IT-PC-1 to Google DNS Server 8.8.8.8 and got an average rate of 57.673.190 milliseconds of roundtrip time.

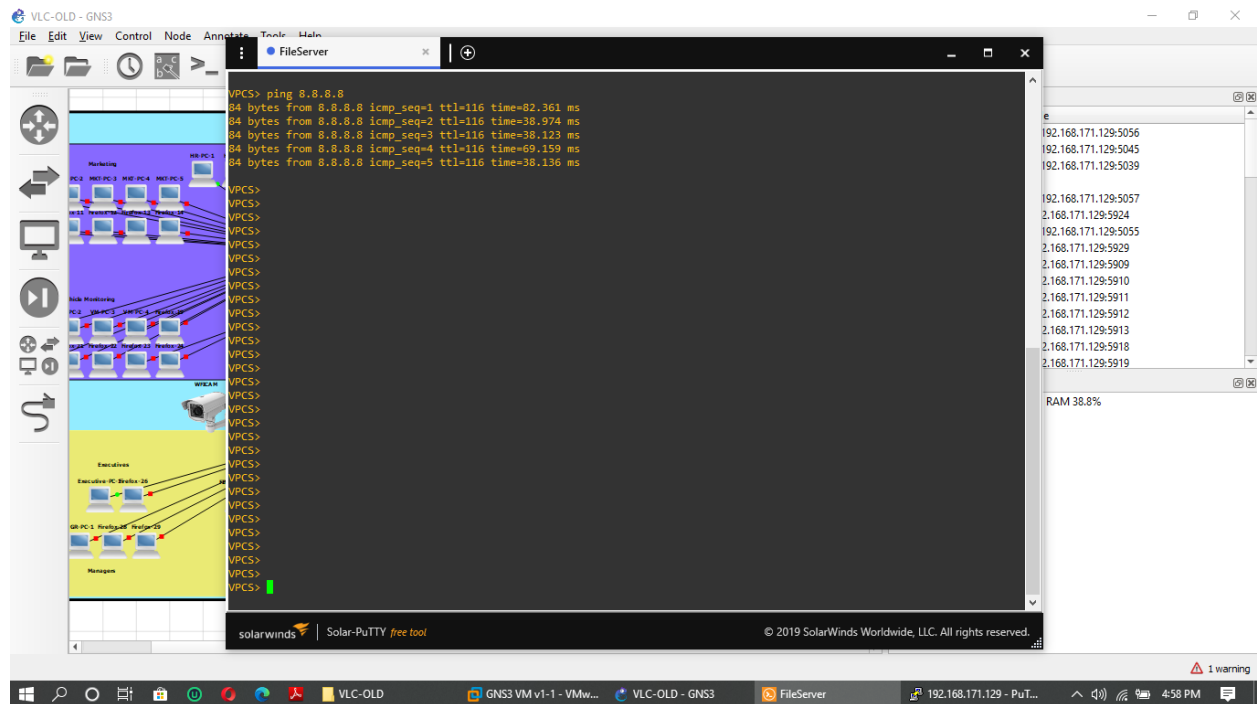


Figure XXXVI: FILESERVER PING

Description: Here we did ping from FileServer to Google DNS Server 8.8.8.8 and got an average rate of 38.974 milliseconds of roundtrip time.

5.2 Proposed Solution

By considering the above-mentioned problems, the goal is to achieve the availability, Data Integrity and confidentiality is by using following techniques

- Concise configurations by modifying protocols
- Policy Management by using ACLS and Firewall policies
- More scalable network by using 3 tier architecture of Access, Distribution and Core methodologies
- Secure VPN
- Make sure the QOS and TOS by priority que management system.
- More advanced security solutions by using next generation firewalls

5.3.1 Connectivity Overview of Proposed Infrastructure

According to our proposed plan each of the department is lied within a separate V-LAN to manage the traffic separately according to their role. HR and Marketing departments contains total 20 nodes and connected with HR_MKT_SW switch. Managers, Executives and vehicle monitoring departments containing 15 nodes are connected with VM_OFFICER_SW access switch. Camera and Access Points are terminated on a dedicated POE Switch. Finance and IT Departments containing 15 nodes are connected with Finance_IT_SW access switch.

All of the switches connected with core switch and having redundant link so if one link fails other link will hold all of the traffic with seamless communication. Core switches are running in Active/Passive mode to achieve the High Availability environment. Now finally the core having uplink with Fort i-Gate firewall which will work as a network Edge providing All Unified Threat Management features. The firewall contains one WAN link which is directly connected with ISP and having SD-WAN connection with Head Office Lahore. The SD-WAN feature allow the firewall to do load balancing and Active/Active Failover to maintain seamless traffic flow.

At head office File server is located at DMZ of H/O Firewall.

- Vehicle Monitoring
- Executives
- Managers
- Finance
- IT

5.3.2 Hardware

For the sake of completeness general hardware description of the equipment procured as part of the VLC center resiliency project will be provided in this section

S. No.	Product	Description	Qty
	Switch(L-2)		
1	WS-C2960G-24TC-L	Cisco Catalyst 2960G Switch 20 x 10/100/100 Gigabit Ethernet Ports (Non-PoE) - 4 x Dual Purpose Port - LAN Base Image	12
2	WS-C2960X-24PS-L	Cisco Catalyst Switch 2960X switch 24 x 10/100/1000 Gigabit PoE Ethernet Ports - 4 x SFP Uplinks - LAN Base Image	4
	Switch(L-3)		
3	WS-C3750G-24TS-S	Cisco Catalyst 3750G Switch includes 24 x 10/100/1000 Ports - 4 x SFP Ports - Standard Image	8
	Firewall		
4	FG-60E-BDL	FG-60E-BDL Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection.	3
5	FG-200E-BDL	Fort i-Gate-200E-BDL Hardware plus 24x7 FortiCare and FortiGuard Unified (UTM) Protection	1

Table 23: List of hardware in new infrastructure

Firewall

FG-60E-BDL

The Fortinet Enterprise Firewall Solution delivers end-to-end network security with one platform, one network security operating system and unified policy management with a single pane of glass for the industry's best protection against the most advanced security threats and targeted attacks. (FortiGate/FortiWiFi). The Forti-Gate family of network appliances represents the industry's broadest range of enterprise firewall platforms. Targeted for distributed enterprises, the Forti-Gate 60E series contains consolidated security and networking functionality, various connectivity options along with Industry's best performance in a compact form factor.

Interfaces

Console Port

2x GE RJ45 WAN Ports

1x GE RJ45 DMZ Ports

7x GE RJ45 Internal Ports

- Combines a RISC-based CPU with Fortinet's proprietary FortiASIC™ content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection

- Accelerates VPN performance for high speed, secure remote access

5.3.3 Firewall connectivity in VLC Environment

Following is the port connectivity of firewall how all the ingress devices terminate on firewall and from which links the firewall reroutes the traffic toward a defined destination.

Port	Description	IP
Wan 1	Connected with PTCL (Internet)	192.168.10.10/24
Wan 2	Reserve	-
1	Connected with Core Switch 1	10.10.10.2/24
2	Connected with Core Switch 2	10.10.11.2/24
3	Connected with PTCL (Data)	172.11.5.2/16
4	Connected with Netsol (Data)	172.20.20.2/16
5	Reserve	
6	Reserve	
7	Reserve	
8	Reserve	

Table 24: Firewall Connectivity in VLC Environment

- Wan 1 port is directly connected with PTCL internet uplink assigned an ip of class C which is 192.168.10.10
- Wan 2 port is reserved for future use if the branch site also get the redundant internet link.
- 1 port is directly connected with core switch 1 having face into the ingress interface of a network containing an ip address of /24 which is 10.10.10.2.
- 2 port is directly connected with core switch 2 having face into the ingress interface of a network containing an ip address of /24 which is 10.10.11.2.
- 3 port is connected with the lease line provided by PTCL IPSEC which extended the lan of a branch site to the H/O by using network address of 15.1.1.0/24.
- Remaining Ports are reserved for future use.

5.4 Core Switches

5.4.1 Core switch 1 3750G-24T:

Cisco Catalyst 3750 Series switch 3750G-24T is an innovative product line that improves LAN operating efficiency by combining industry-leading ease of use and the highest resiliency available for stackable switches. This new product series represents the next generation in desktop switches, and features Cisco Stack Wise technology, a 32-Gbps stack interconnect that allows customers to build a unified, highly resilient switching system - one switch at a time. For mid-sized organizations and enterprise branch offices, the Cisco Catalyst 3750 Series eases deployment of converged applications and adapts to changing business needs by providing configuration flexibility, support for converged network patterns, and automation of intelligent network-services configurations

- 24 Ethernet 10/100/1000 ports
- 32-Gbps, high-speed stacking bus
- Innovative stacking technology
- 1 RU stackable, multilayer switch
- Enterprise-class intelligent services delivered to the network edge
- IP Base software feature set (IPB)

5.4.2 Port:

Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently being used as the backbone in many enterprise networks

5.4.3 V-LAN

A V-LAN is a broadcast domain created by switches. Normally, it is a router or layer 3 switch creating that broadcast domain. With V-LAN's, a switch can create the broadcast domain.

5.4.4 Mode:

- **Trunk:** A trunk port is a port that is assigned to carry traffic for all the V-LANs that are accessible by a specific switch, a process known as trunking. (Chapter: Configuring Access and Trunk Interfaces) Trunk ports mark frames with unique identifying tags – either 802.1Q tags or Inter-Switch Link (ISL) tags – as they move between switches.
- **Access:** forces the port to be an access port while and any device plugged into this port will only be able to communicate with other devices that are in the same V-LAN.

5.5 Core Switch 1 Connectivity:

Core switch 1 resides in an IT department working as a back bone to the entire lan network. All the access switches are terminating on core switches. There are two core switches to deal with redundant traffic. Both the switches are working in Active/Passive mode. If one switch get down another switch will take responsibility of the entire communication. Following are the connectivity tables of both core switches.

WS-C3750G-24TS-S

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with LAN_1 (Firewall)	10.10.10.1/24	L3
GigabitEthernet1/2	Connected with Switch_1	V-LAN 20,30	Trunk
GigabitEthernet1/3	Connected with Switch_2	V-LAN 40,50,60,90	Trunk
GigabitEthernet1/4	Connected with Switch_3	V-LAN 70,80	Trunk
GigabitEthernet1/5	Connected with Switch_4	V-LAN 90	Access
GigabitEthernet1/6	Connected with NVR	V-LAN 90	Access
GigabitEthernet1/7	Reserve		
GigabitEthernet1/8	Reserve		
GigabitEthernet1/9	Reserve		
GigabitEthernet1/10	Reserve		
GigabitEthernet1/11	Reserve		
GigabitEthernet1/12	Reserve		
GigabitEthernet1/13	Reserve		
GigabitEthernet1/14	Reserve		
GigabitEthernet1/15	Reserve		
GigabitEthernet1/16	Reserve		
GigabitEthernet1/17	Reserve		
GigabitEthernet1/18	Reserve		
GigabitEthernet1/19	Reserve		
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 25:Core Switch 1 Connectivity

Configuration

```

VLC_CORE_1#sh run
Building configuration...

Current configuration : 5139 bytes
!
! Last configuration change at 16:03:52 UTC
Wed Jul 1 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname VLC_CORE_1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$tIJ5$SnFkP1oyfAPi1K2fN.bmkv/
!
no aaa new-model
!
!
ip cef
no ipv6 cef
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
V-LAN internal allocation policy ascending
!
!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport mode trunk
!
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
!
interface GigabitEthernet0/3
switchport trunk encapsulation dot1q
media-type rj45
negotiation auto
!
interface GigabitEthernet0/0
no switchport
ip address 10.10.10.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet1/0
switchport trunk encapsulation dot1q
media-type rj45
negotiation auto
!
interface GigabitEthernet1/1
switchport trunk encapsulation dot1q
media-type rj45
negotiation auto
!
interface GigabitEthernet1/2
switchport trunk encapsulation dot1q
media-type rj45
negotiation auto
!
interface GigabitEthernet1/3
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45
negotiation auto
!
interface GigabitEthernet2/0
switchport trunk encapsulation dot1q
switchport mode trunk
media-type rj45

```

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
shutdown
media-type rj45
negotiation auto
!
interface GigabitEthernet0/2
negotiation auto
!
interface GigabitEthernet2/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/0
media-type rj45
negotiation auto
!
interface GigabitEthernet3/1
media-type rj45
negotiation auto
!
interface GigabitEthernet3/2
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
```

```
negotiation auto
!
interface GigabitEthernet2/1
media-type rj45
negotiation auto
!
interface GigabitEthernet2/2
media-type rj45
negotiation auto
!
interface GigabitEthernet3/3
media-type rj45
negotiation auto
!
interface V-LAN20
ip address 20.0.0.10 255.255.255.0
!
interface V-LAN30
ip address 30.0.0.10 255.255.255.0
!
interface V-LAN40
ip address 40.0.0.10 255.255.255.0
!
interface V-LAN50
ip address 50.0.0.10 255.255.255.0
!
interface V-LAN60
ip address 60.0.0.10 255.255.255.0
!
interface V-LAN70
ip address 70.0.0.10 255.255.255.0
!
interface V-LAN80
ip address 80.0.0.10 255.255.255.0
!
interface V-LAN90
ip address 90.0.0.10 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.10.10.2
ip route 0.0.0.0 255.255.255.0 10.10.10.2
!
control-plane
```

```

media-type rj45          !
negotiation auto         !
!                         line con 0
interface GigabitEthernet3/3  line aux 0
media-type rj45          line vty 0 4
negotiation auto         login
!                         !
interface GigabitEthernet3/3  !
media-type rj45           End

```

5.6 Core Switch 2 Connectivity:

WS-C3750G-24TS-S

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with LAN_1 (Firewall)	10.10.11.1/24	L3
GigabitEthernet1/2	Connected with Switch_1	V-LAN 20,30	Trunk
GigabitEthernet1/3	Connected with Switch_2	V-LAN 40,50,60,90	Trunk
GigabitEthernet1/4	Connected with Switch_3	V-LAN 70,80	Trunk
GigabitEthernet1/5	Connected with Switch_4	V-LAN 90	Access
GigabitEthernet1/6	Connected with NVR	V-LAN 90	Access
GigabitEthernet1/7	Reserve		
GigabitEthernet1/8	Reserve		
GigabitEthernet1/9	Reserve		
GigabitEthernet1/10	Reserve		
GigabitEthernet1/11	Reserve		
GigabitEthernet1/12	Reserve		
GigabitEthernet1/13	Reserve		
GigabitEthernet1/14	Reserve		
GigabitEthernet1/15	Reserve		
GigabitEthernet1/16	Reserve		
GigabitEthernet1/17	Reserve		
GigabitEthernet1/18	Reserve		
GigabitEthernet1/19	Reserve		
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 26: Core Switch 2 Connectivity

Configuration

5.7 Access Switches

5.7.1 Model: Cisco Catalyst 2960G-24TC-L Switch

Cisco Catalyst 2960G-24TC-L Switch is a Catalyst 2960-X Series fixed-configuration switch. It offers 10/100/1000 Ethernet connectivity with enhanced local area network (LAN) services for midsize and branch office networks.

5.7.2 Benefits:

If you have networking experience, you can use this switch to extend an existing network, bringing wired connectivity to more employees and supporting new wireless deployments.

5.8 Access Switch HR_MKT

Access switch 1 manage the traffic of HR and marketing department. The allowed V-LANs are V-LAN 20 and V-LAN 30 which holds the traffic of each group of users.

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with HR PC 1	V-LAN 20	Access
GigabitEthernet1/4	Connected with HR PC 2	V-LAN 20	Access
GigabitEthernet1/5	Connected with HR PC 3	V-LAN 20	Access
GigabitEthernet1/6	Connected with HR PC 4	V-LAN 20	Access
GigabitEthernet1/7	Connected with MKT PC 1	V-LAN 30	Access
GigabitEthernet1/8	Connected with MKT PC 2	V-LAN 30	Access
GigabitEthernet1/9	Connected with MKT PC 3	V-LAN 30	Access
GigabitEthernet1/10	Connected with MKT PC 4	V-LAN 30	Access
GigabitEthernet1/11	Connected with MKT PC 5	V-LAN 30	Access
GigabitEthernet1/12	Connected with MKT PC 6	V-LAN 30	Access
GigabitEthernet1/13	Connected with MKT PC 7	V-LAN 30	Access
GigabitEthernet1/14	Connected with MKT PC 8	V-LAN 30	Access
GigabitEthernet1/15	Connected with MKT PC 9	V-LAN 30	Access
GigabitEthernet1/16	Connected with MKT PC 10	V-LAN 30	Access
GigabitEthernet1/17	Connected with MKT PC 11	V-LAN 30	Access
GigabitEthernet1/18	Connected with MKT PC 12	V-LAN 30	Access
GigabitEthernet1/19	Connected with MKT PC 13	V-LAN 30	Access
GigabitEthernet1/20	Connected with MKT PC 14	V-LAN 30	Access
GigabitEthernet1/21	Connected with MKT PC 15	V-LAN 30	Access
GigabitEthernet1/22	Connected with MKT PC 16	V-LAN 30	Access
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 27: Access Switch 1 Configuration

Configuration

```

HR_MKT_SW#sh run
Building configuration...

Current configuration : 3567 bytes
!
! Last configuration change at 16:03:43 UTC
Wed Jul 1 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname HR_MKT_SW
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$5Ay4$rob3dec/JYnDK76skJzR3.
!
no aaa new-model
!
!
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 20.0.0.1 20.0.0.10
ip dhcp excluded-address 30.0.0.1 30.0.0.10
!
ip dhcp pool HR
network 20.0.0.0 255.255.255.0
default-router 20.0.0.10
dns-server 8.8.8.8
!
ip dhcp pool Marketing
network 30.0.0.0 255.255.255.0
default-router 30.0.0.10
dns-server 8.8.8.8
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
V-LAN internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Port-channel1
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
!
interface Ethernet0/2
description HR_PC
switchport access V-LAN 20
switchport mode access
!
interface Ethernet0/3
description HR_PC
switchport access V-LAN 20
switchport mode access
!
interface Ethernet1/0
description HR_PC
switchport access V-LAN 20
switchport mode access
!
interface Ethernet1/1
description HR_PC
switchport access V-LAN 20
switchport mode access
!
interface Ethernet1/2
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet1/3
description Marketing_PC
switchport access V-LAN 30

```

```

switchport mode access
!
interface Ethernet2/0
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet2/1
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet2/2
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet2/3
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet3/0
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet3/1
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet3/2
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet3/3
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet4/0
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet4/1
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet4/2
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet4/3
description Marketing_PC
switchport access V-LAN 30
switchport mode access
!
interface Ethernet5/0
switchport access V-LAN 30
switchport mode access
!
interface Ethernet5/1
switchport access V-LAN 30
switchport mode access
!
interface Ethernet5/2
!
interface Ethernet5/3
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN20
ip address 20.0.0.12 255.255.255.0
!
interface V-LAN30
ip address 30.0.0.11 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15

```

```

logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End

```

5.9 Access Switch MGR_VM_EX

Access switch 2 manage the traffic of following department:

- Vehicle Monitoring
- Conference Room
- Managers and Executives

The allowed V-LANs are V-LAN 40,50,60 and V-LAN 90 which holds the traffic of each group of users.

2960G-24TC-L

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with Manager PC 1	V-LAN 40	Access
GigabitEthernet1/4	Connected with Manager PC 2	V-LAN 40	Access
GigabitEthernet1/5	Connected with Manager PC 3	V-LAN 40	Access
GigabitEthernet1/6	Connected with Executives PC 1	V-LAN 50	Access
GigabitEthernet1/7	Connected with Executives PC 1	V-LAN 50	Access
GigabitEthernet1/8	Connected with Vehicle Monitoring PC 1	V-LAN 60	Access
GigabitEthernet1/9	Connected with Vehicle Monitoring PC 2	V-LAN 60	Access
GigabitEthernet1/10	Connected with Vehicle Monitoring PC 3	V-LAN 60	Access
GigabitEthernet1/11	Connected with Vehicle Monitoring PC 4	V-LAN 60	Access
GigabitEthernet1/12	Connected with Vehicle Monitoring PC 5	V-LAN 60	Access
GigabitEthernet1/13	Connected with Vehicle Monitoring PC 6	V-LAN 60	Access
GigabitEthernet1/14	Connected with Vehicle Monitoring PC 7	V-LAN 60	Access
GigabitEthernet1/15	Connected with Vehicle Monitoring PC 8	V-LAN 60	Access
GigabitEthernet1/16	Connected with Vehicle Monitoring PC 9	V-LAN 60	Access
GigabitEthernet1/17	Connected with Vehicle Monitoring PC 10	V-LAN 60	Access
GigabitEthernet1/18	Connected with Access point 1	V-LAN 90	Access
GigabitEthernet1/19	Connected with Access point 2	V-LAN 90	Access
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 28: Access Switch 2 configuration

Configuration

```

VM_OFFICER_SW#sh run
Building configuration...

Current configuration : 3322 bytes
!
! Last configuration change at 07:59:48 UTC
Thu Jun 25 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname VM_OFFICER_SW
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
ip dhcp pool Managers
network 40.0.0.0 255.255.255.0
default-router 40.0.0.10
dns-server 8.8.8.8
!
ip dhcp pool Executives
network 50.0.0.0 255.255.255.0
default-router 50.0.0.10
dns-server 8.8.8.8
!
ip dhcp pool Vehicle_Monitoring
network 60.0.0.0 255.255.255.0
default-router 60.0.0.10
dns-server 8.8.8.8
!
!
ip cef
no ipv6 cef
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
V-LAN internal allocation policy ascending
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
!
interface Ethernet0/2
description Manager_PC
switchport access V-LAN 40
switchport mode access
!
interface Ethernet0/3
description Manager_PC
switchport access V-LAN 40
switchport mode access
!
interface Ethernet1/0
description Manager_PC
switchport access V-LAN 40
switchport mode access
!
interface Ethernet1/1
description Executives_PC
switchport access V-LAN 50
switchport mode access
!
interface Ethernet1/2
description Executives_PC
switchport access V-LAN 50
switchport mode access
!
interface Ethernet1/3
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet2/0
description Vehicle_Monitoring_PC
switchport access V-LAN 60

```

```

switchport mode access
!
interface Ethernet2/1
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet2/2
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet2/3
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet3/0
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet3/1
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet3/2
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet3/3
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet4/0
description Vehicle_Monitoring_PC
switchport access V-LAN 60
switchport mode access
!
interface Ethernet4/1
description AP_1

```

```

switchport access V-LAN 90
switchport mode access
!
interface Ethernet4/2
description AP_2
switchport access V-LAN 90
switchport mode access
!
interface Ethernet4/3
!
interface Ethernet5/0
!
interface Ethernet5/1
!
interface Ethernet5/2
!
interface Ethernet5/3
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN20
no ip address
shutdown
!
interface V-LAN40
ip address 40.0.0.11 255.255.255.0
!
interface V-LAN50
ip address 50.0.0.11 255.255.255.0
!
interface V-LAN60
ip address 60.0.0.11 255.255.255.0
!
interface V-LAN90
ip address 90.0.0.11 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!

```

```
!  
control-plane  
!  
!  
line con 0  
logging synchronous  
line aux 0  
line vty 0 4  
login  
!  
End
```

5.10 Access Switch FINANCE_IT

Access switch 3 manage the traffic of following department:

- Finance
- IT Support

The allowed V-LANs are V-LAN 70 and V-LAN 80 which holds the traffic of each group of users.

2960G-24TC-L

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with Finance PC 1	V-LAN 70	Access
GigabitEthernet1/4	Connected with Finance PC 2	V-LAN 70	Access
GigabitEthernet1/5	Connected with Finance PC 3	V-LAN 70	Access
GigabitEthernet1/6	Connected with Finance PC 4	V-LAN 70	Access
GigabitEthernet1/7	Connected with Finance PC 5	V-LAN 70	Access
GigabitEthernet1/8	Connected with Finance PC 6	V-LAN 70	Access
GigabitEthernet1/9	Connected with Finance PC 7	V-LAN 70	Access
GigabitEthernet1/10	Connected with Finance PC 8	V-LAN 70	Access
GigabitEthernet1/11	Connected with Finance PC 9	V-LAN 70	Access
GigabitEthernet1/12	Connected with Finance PC 10	V-LAN 70	Access
GigabitEthernet1/13	Connected with IT Support PC 1	V-LAN 80	Access
GigabitEthernet1/14	Connected with IT Support PC 2	V-LAN 80	Access
GigabitEthernet1/15	Connected with IT Support PC 3	V-LAN 80	Access
GigabitEthernet1/16	Connected with IT Support PC 4	V-LAN 80	Access
GigabitEthernet1/17	Connected with IT Support PC 5	V-LAN 80	Access
GigabitEthernet1/18	Reserve		
GigabitEthernet1/19	Reserve		
GigabitEthernet1/20	Reserve		
GigabitEthernet1/21	Reserve		
GigabitEthernet1/22	Reserve		
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 29: Access Switch 3 Configuration

Configuration

Finance_IT_SW#sh run	!
Building configuration...	ip dhcp pool Finance
	network 70.0.0.0 255.255.255.0
Current configuration : 2714 bytes	default-router 70.0.0.10
!	dns-server 8.8.8.8
! Last configuration change at 07:34:11 UTC	!
Thu Jun 25 2020	ip dhcp pool IT
!	network 80.0.0.0 255.255.255.0
version 15.2	default-router 80.0.0.10
service timestamps debug datetime msec	dns-server 8.8.8.8
service timestamps log datetime msec	!
no service password-encryption	!
service compress-config	no ip domain-lookup
!	ip cef
hostname Finance_IT_SW	no ipv6 cef
!	!
boot-start-marker	!
boot-end-marker	!
!	spanning-tree mode rapid-pvst
!	spanning-tree extend system-id
logging discriminator EXCESS severity drops	!
6 msg-body drops EXCESSCOLL	V-LAN internal allocation policy ascending
logging buffered 50000	!
logging console discriminator EXCESS	ip tcp synwait-time 5
!	!
no aaa new-model	interface Ethernet0/0
!	switchport trunk encapsulation dot1q
no ip icmp rate-limit unreachable	!
!	interface Ethernet0/1

```

switchport trunk encapsulation dot1q
!
interface Ethernet0/2
switchport access V-LAN 70
switchport mode access
!
interface Ethernet0/3
switchport access V-LAN 70
switchport mode access
!
interface Ethernet1/0
switchport access V-LAN 70
switchport mode access
!
interface Ethernet1/1
switchport access V-LAN 70
switchport mode access
!
interface Ethernet1/2
switchport access V-LAN 70
switchport mode access
!
interface Ethernet1/3
switchport access V-LAN 70
switchport mode access
!
interface Ethernet2/0
switchport access V-LAN 70
switchport mode access
!
interface Ethernet2/1
switchport access V-LAN 70
switchport mode access
!
interface Ethernet2/2
switchport access V-LAN 70
switchport mode access
!
interface Ethernet2/3
switchport access V-LAN 70
switchport mode access
!
interface Ethernet3/0
switchport access V-LAN 80
switchport mode access
!
interface Ethernet3/1
switchport access V-LAN 80
switchport mode access
!
interface Ethernet3/2
switchport access V-LAN 80
switchport mode access
!
interface Ethernet3/3
switchport access V-LAN 80
switchport mode access
!

```

```

interface Ethernet4/0
switchport access V-LAN 80
switchport mode access
!
interface Ethernet4/1
!
interface Ethernet4/2
!
interface Ethernet4/3
!
interface Ethernet5/0
!
interface Ethernet5/1
!
interface Ethernet5/2
!
interface Ethernet5/3
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN70
ip address 70.0.0.11 255.255.255.0
!
interface V-LAN80
ip address 80.0.0.11 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End

```

5.11 Access Switch Camera_WIFI

Access switch 4 manage the traffic of Cameras:

The allowed V-LAN is V-LAN 90 which holds the traffic all the cameras running in a VLC environment. Here Poe Switch will be used which holds the capabilities of Power over Ethernet providing the power to all cameras.

WS-C2960X-24PS-L

Port	Description	V-LAN	Mode
GigabitEthernet1/1	Connected with Core 1	NA	Trunk
GigabitEthernet1/2	Connected with Core 2	NA	Trunk
GigabitEthernet1/3	Connected with HM_C1	V-LAN 90	Access
GigabitEthernet1/4	Connected with HM_C2	V-LAN 90	Access
GigabitEthernet1/5	Connected with HM_C3	V-LAN 90	Access
GigabitEthernet1/6	Connected with HM_C4	V-LAN 90	Access
GigabitEthernet1/7	Connected with VM_C1	V-LAN 90	Access
GigabitEthernet1/8	Connected with VM_C2	V-LAN 90	Access
GigabitEthernet1/9	Connected with VM_C3	V-LAN 90	Access
GigabitEthernet1/10	Connected with VM_C4	V-LAN 90	Access
GigabitEthernet1/11	Connected with CR_C1	V-LAN 90	Access
GigabitEthernet1/12	Connected with CR_C2	V-LAN 90	Access
GigabitEthernet1/13	Connected with WA_C1	V-LAN 90	Access
GigabitEthernet1/14	Connected with WA_C2	V-LAN 90	Access
GigabitEthernet1/15	Connected with F_C1	V-LAN 90	Access
GigabitEthernet1/16	Connected with F_C2	V-LAN 90	Access
GigabitEthernet1/17	Connected with F_C3	V-LAN 90	Access
GigabitEthernet1/18	Connected with F_C4	V-LAN 90	Access
GigabitEthernet1/19	Connected with IT_C1	V-LAN 90	Access
GigabitEthernet1/20	Connected with IT_C2	V-LAN 90	Access
GigabitEthernet1/21	Connected with L_C1	V-LAN 90	Access
GigabitEthernet1/22	Connected with GT_C1	V-LAN 90	Access
GigabitEthernet1/23	Reserve		
GigabitEthernet1/24	Reserve		

Table 30:Access Switch 4 configuration

Configuration

```

Camera#sh run
Building configuration...

Current configuration : 3206 bytes
!
! Last configuration change at 07:50:12 UTC Thu Jun
25 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Camera
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
!
ip dhcp pool Camera
network 90.0.0.0 255.255.255.0
default-router 90.0.0.10
dns-server 8.8.8.8
!
!

```

```

!
interface Ethernet0/1
switchport trunk encapsulation dot1q
!
interface Ethernet0/2
description HM_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet0/3
description HM_C2
switchport access V-LAN 90
switchport mode access
!
interface Ethernet1/0
description HM_C3
switchport access V-LAN 90
switchport mode access
!
interface Ethernet1/1
description HM_C4
switchport access V-LAN 90
switchport mode access
!
interface Ethernet1/2
description VM_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet1/3
description VM_C2
switchport access V-LAN 90
switchport mode access
!
interface Ethernet2/0
description VM_C3

```

```

ip dhcp pool Camera
network 90.0.0.0 255.255.255.0
default-router 90.0.0.10
dns-server 8.8.8.8
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
V-LAN internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk

```

```

description VM_C2
switchport access V-LAN 90
switchport mode access
!
interface Ethernet2/0
description VM_C3
switchport access V-LAN 90
switchport mode access
!
interface Ethernet2/1
description VM_C4
switchport access V-LAN 90
switchport mode access
!
interface Ethernet2/2
description CR_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet2/3
description CR_C2
switchport access V-LAN 90
switchport mode access

```

```

!
interface Ethernet3/0
description WA_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet3/1
description WA_C2
switchport access V-LAN 60
switchport mode access
!
interface Ethernet3/2
description F_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet3/3
description F_C2
switchport access V-LAN 90
switchport mode access
!
interface Ethernet4/0
description F_C3
switchport access V-LAN 90
switchport mode access
!
interface Ethernet4/1
description F_C4
switchport access V-LAN 90
switchport mode access
!
interface Ethernet4/2
description IT_C1

```

```

interface Ethernet5/3
!
interface V-LAN1
no ip address
shutdown
!
interface V-LAN40
ip address 90.0.0.11 255.255.255.0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end

```

```

switchport access V-LAN 90
switchport mode access
!
interface Ethernet4/3
description IT_C2
switchport access V-LAN 90
switchport mode access
!
interface Ethernet5/0
description L_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet5/1
description GT_C1
switchport access V-LAN 90
switchport mode access
!
interface Ethernet5/2
!

```

5.12 Comparison between Old Infrastructure and Proposed Solution

Comparison on the basis of Internet Control Messaging Protocol (ICMP).

- VLC OLD

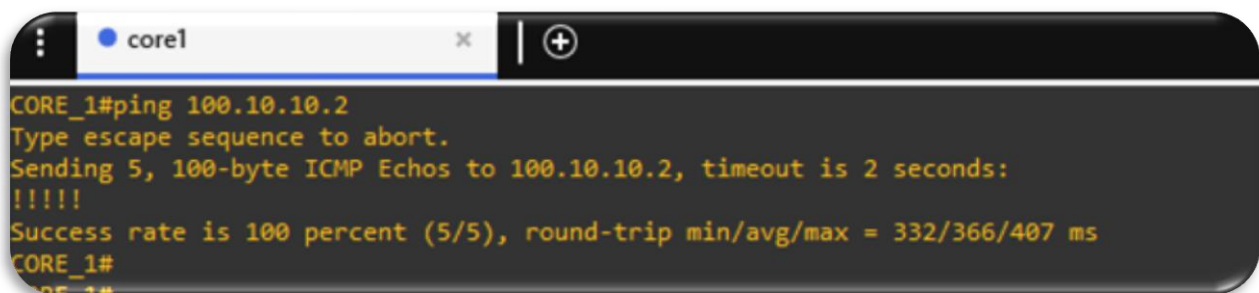


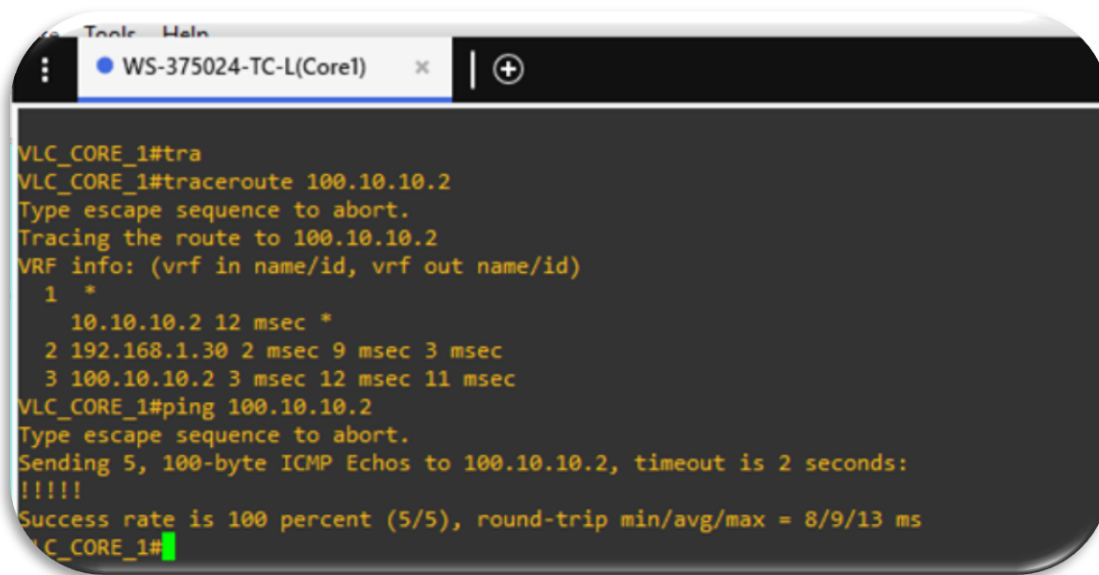
Figure XXXVIII: Old ICMP

Description: In the above picture we PING the FileServer located as 100.10.10.2 in the Head Office. So we Got following results:

Transfer Rate: Successful

Average round trip time: 336 ms

- VLC NEW

A screenshot of a terminal window with a dark background and yellow text. The window title bar shows 'Tools Help' and a tab labeled 'WS-375024-TC-L(Core1)'. The terminal content shows a user at the 'VLC_CORE_1' prompt running 'tracert 100.10.10.2'. The output shows three hops: 10.10.10.2 (12 msec), 192.168.1.30 (2 msec, 9 msec, 3 msec), and 100.10.10.2 (3 msec, 12 msec, 11 msec). Then, the user runs 'ping 100.10.10.2', and the output shows 'Sending 5, 100-byte ICMP Echos to 100.10.10.2, timeout is 2 seconds: !!!!!' and 'Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/13 ms'.

```
VLC_CORE_1#tra
VLC_CORE_1#tracert 100.10.10.2
Type escape sequence to abort.
Tracing the route to 100.10.10.2
VRF info: (vrf in name/id, vrf out name/id)
  0  10.10.10.2 12 msec *
  1  192.168.1.30 2 msec 9 msec 3 msec
  2  100.10.10.2 3 msec 12 msec 11 msec
VLC_CORE_1#ping 100.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.10.10.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/13 ms
VLC_CORE_1#
```

Figure XXXIX: New ICMP

Description: In the above picture we PING the FileServer located as 100.10.10.2 in the Head Office. So We Got following results:

Transfer Rate: Successful

Average round trip time: 9 ms

Chapter 6

Results and Conclusion

Description: Here we made two DHCP pools on HR_MKT_SW to manage traffic of VLAN 20 and 30 so the DHCP pool HR Having 20.0.0.1 as a gateway from VLAN 20 and DHCP pool Marketing have 30.0.0.1 as a gateway from VLAN 30.



Figure XLI: VM-OFFICER-SW

Description: Here we made three DHCP pools on VM_OFFICER_SW to manage traffic of VLAN 40,50 and 60 so the DHCP pool Managers having 40.0.0.1 as a gateway from VLAN 40, DHCP pool Executives have 50.0.0.1 as a gateway from VLAN 50 and DHCP pool Vehicle_Monitoring having 60.0.0.1 as a gateway from VLAN 60.

Description: Here we made one DHCP pool on Camera SW to manage traffic of VLAN 90 so the DHCP pool Camera having 90.0.0.1 as a gateway from VLAN 90.



Figure XLIII: FINANCE-IT-SW

Description: Here we made two DHCP pools on Finance_IT_SW to manage traffic of VLAN 70 and 80 so the DHCP pool Finance having 70.0.0.1 as a gateway from VLAN 70 and DHCP pool IT have 80.0.0.1 as a gateway from VLAN 80.

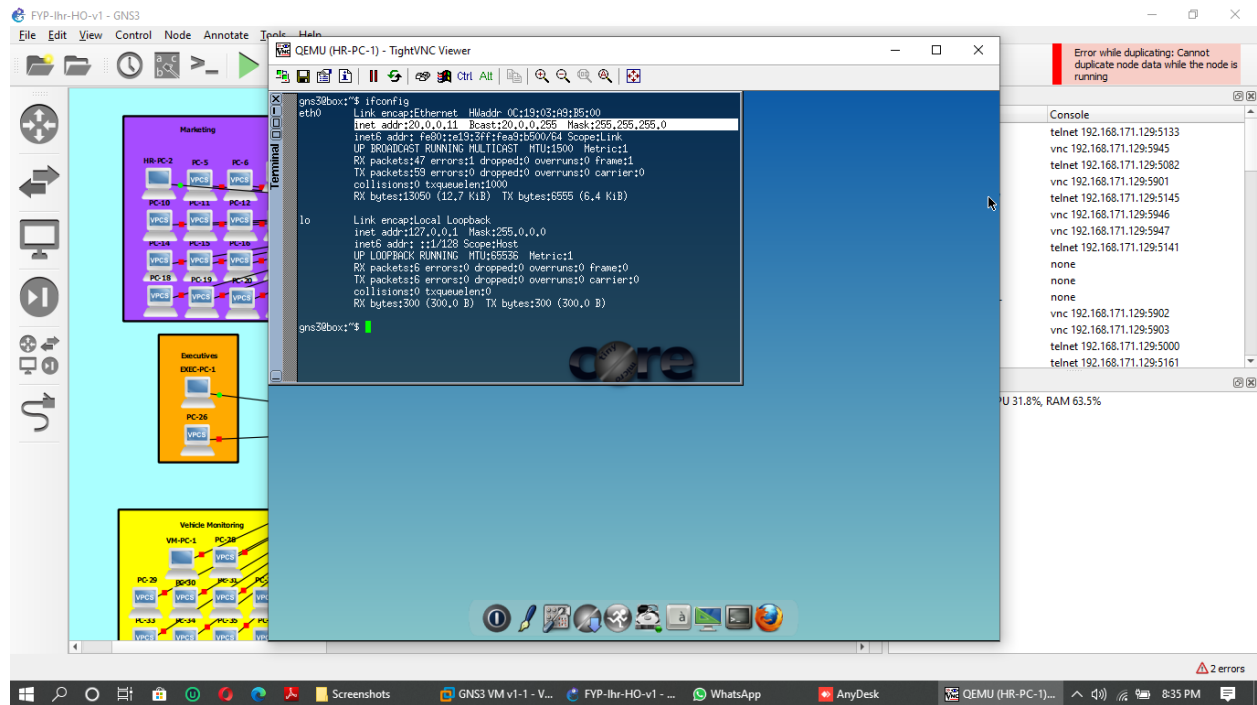


Figure XLIV: HR-PC-1

Description: The HR-PC-1 is obtaining DHCP allocated address successfully which is 20.0.0.11 on VLAN 20

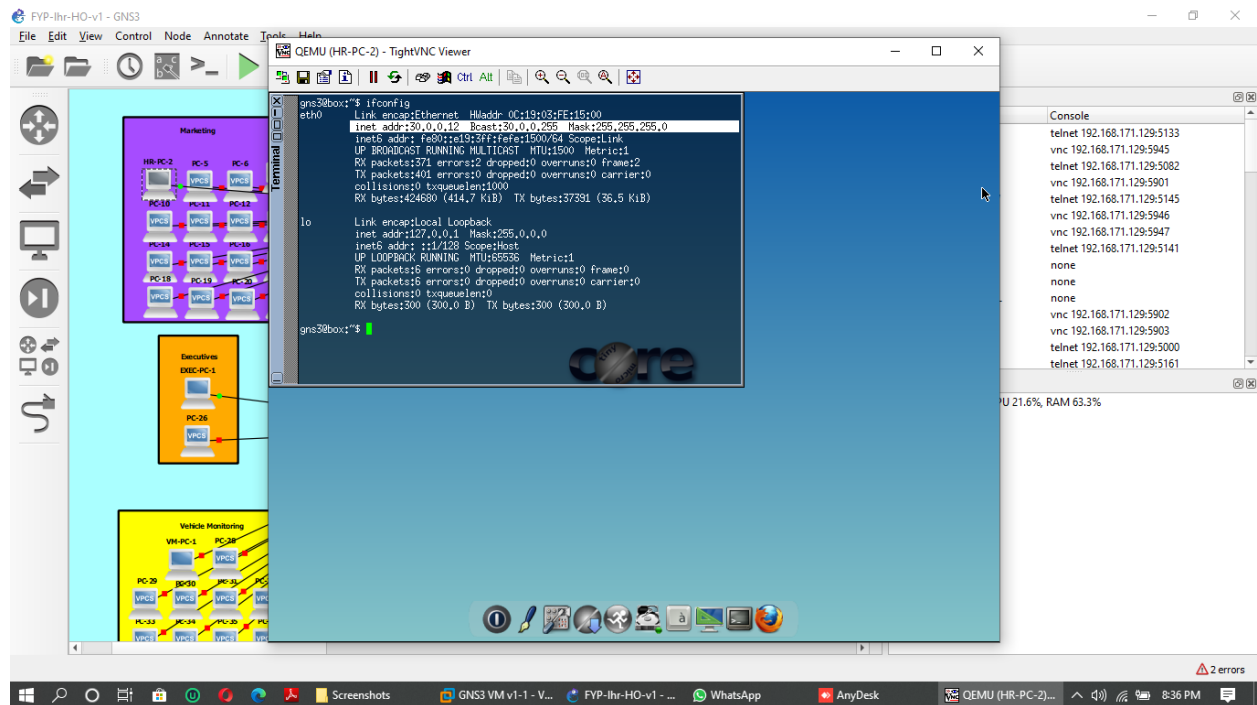


Figure XLV: Marketing-PC-1

Description: The Marketing-PC-1 is obtaining DHCP allocated address successfully which is 30.0.0.12 on VLAN 30

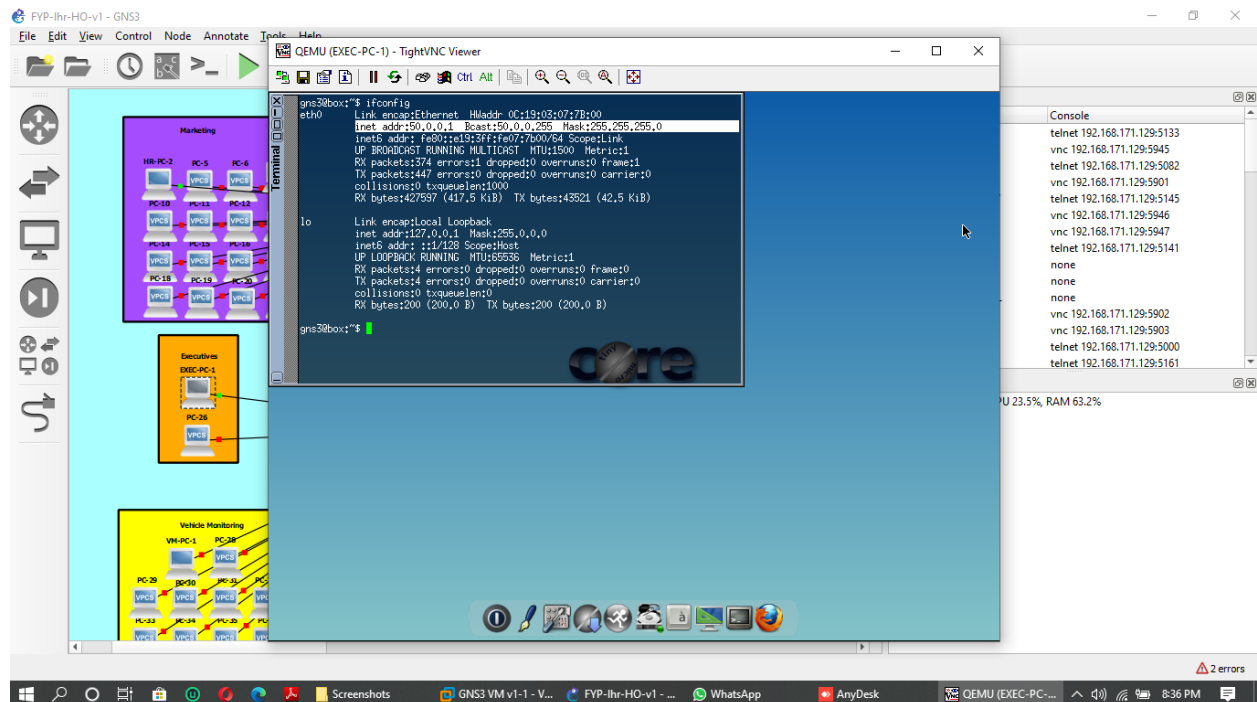


Figure XLVI: EXEC-PC-1

Description: The EXEC-PC-1 is obtaining DHCP allocated address successfully which is 50.0.0.1 on VLAN 50.

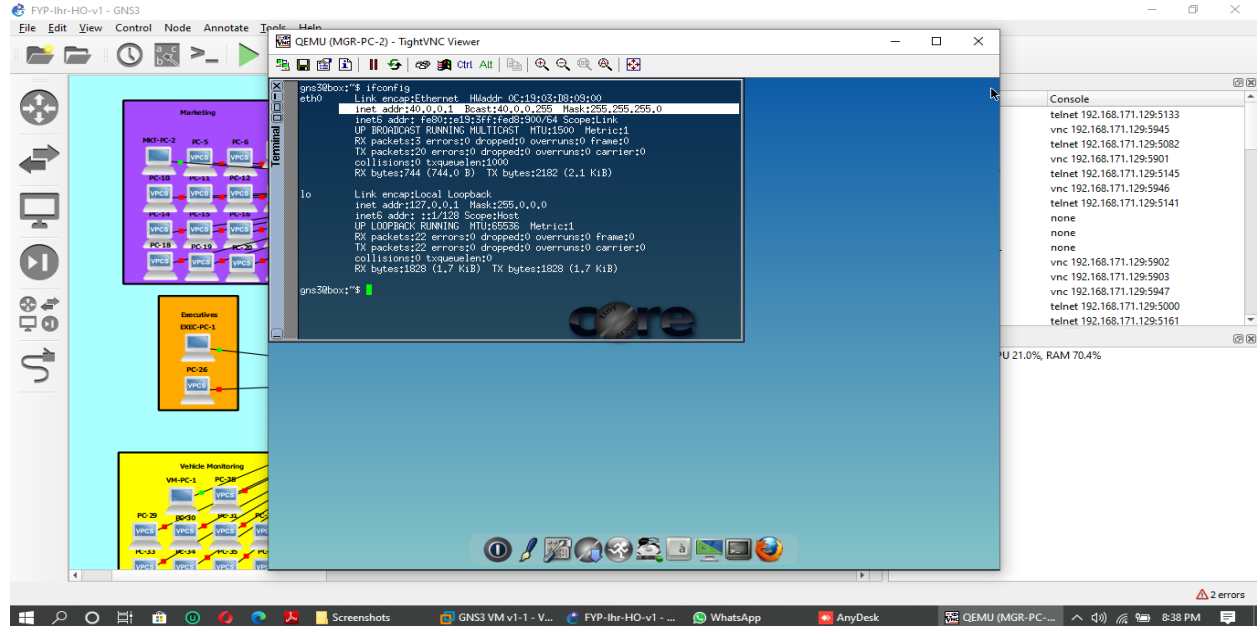


Figure XLVII: MGR-PC-2

Description: The MGR-PC-2 is obtaining DHCP allocated address successfully which is 40.0.0.1 on VLAN 40.

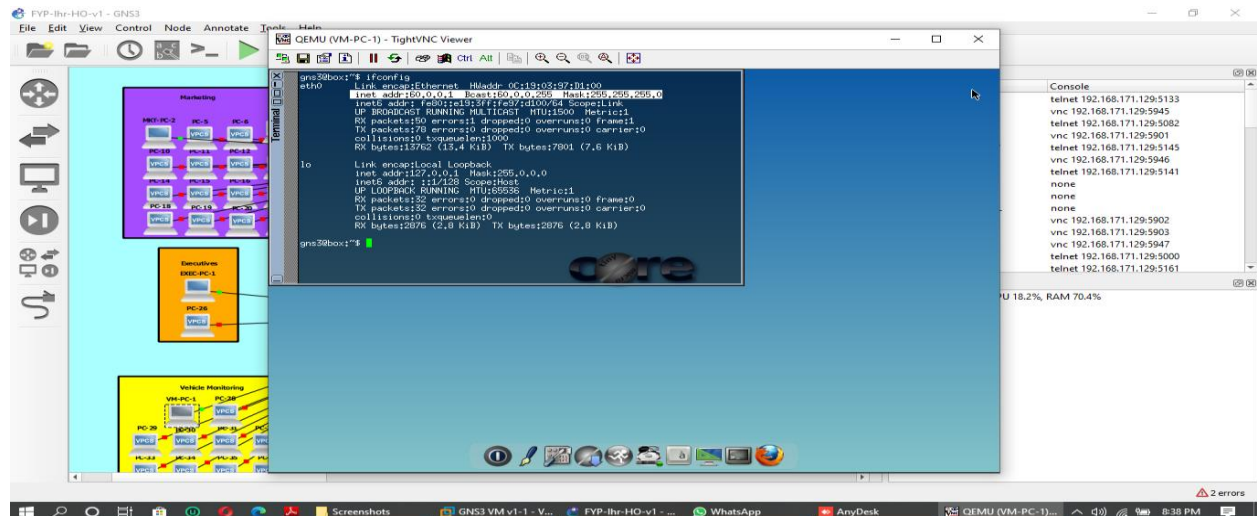


Figure XLVIII: VM-PC-1

Description: The VM-PC-1 is obtaining DHCP allocated address successfully which is 60.0.0.1 on VLAN 60.

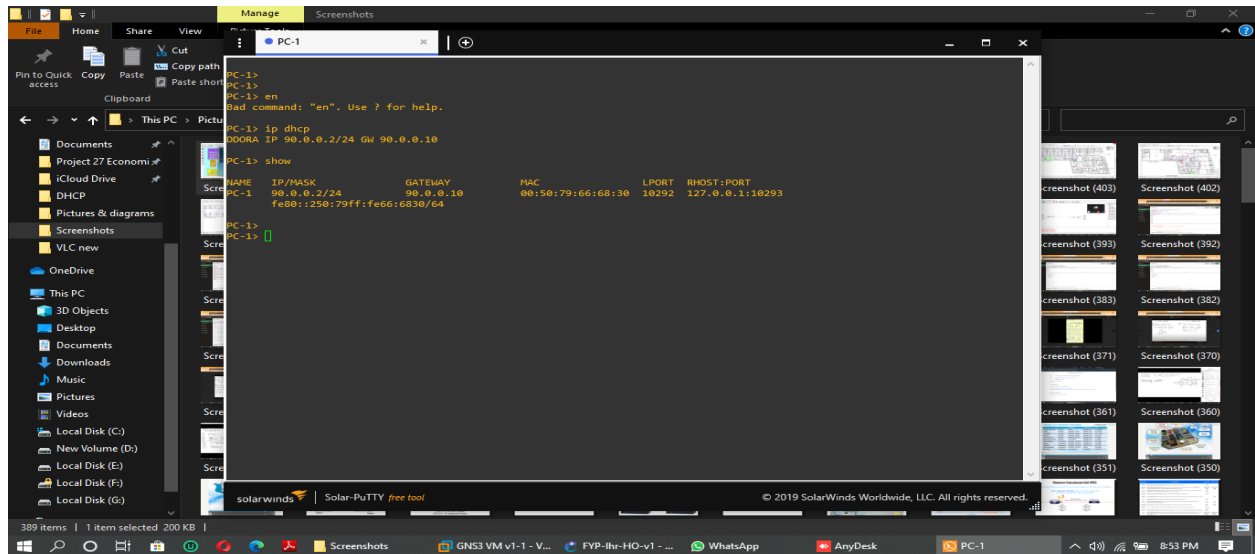


Figure XLIX: Camera_WIFI_PC-1

Description: The Camera_WIFI_PC-1 obtaining DHCP allocated address successfully which is 90.0.0.1 on VLAN 90.

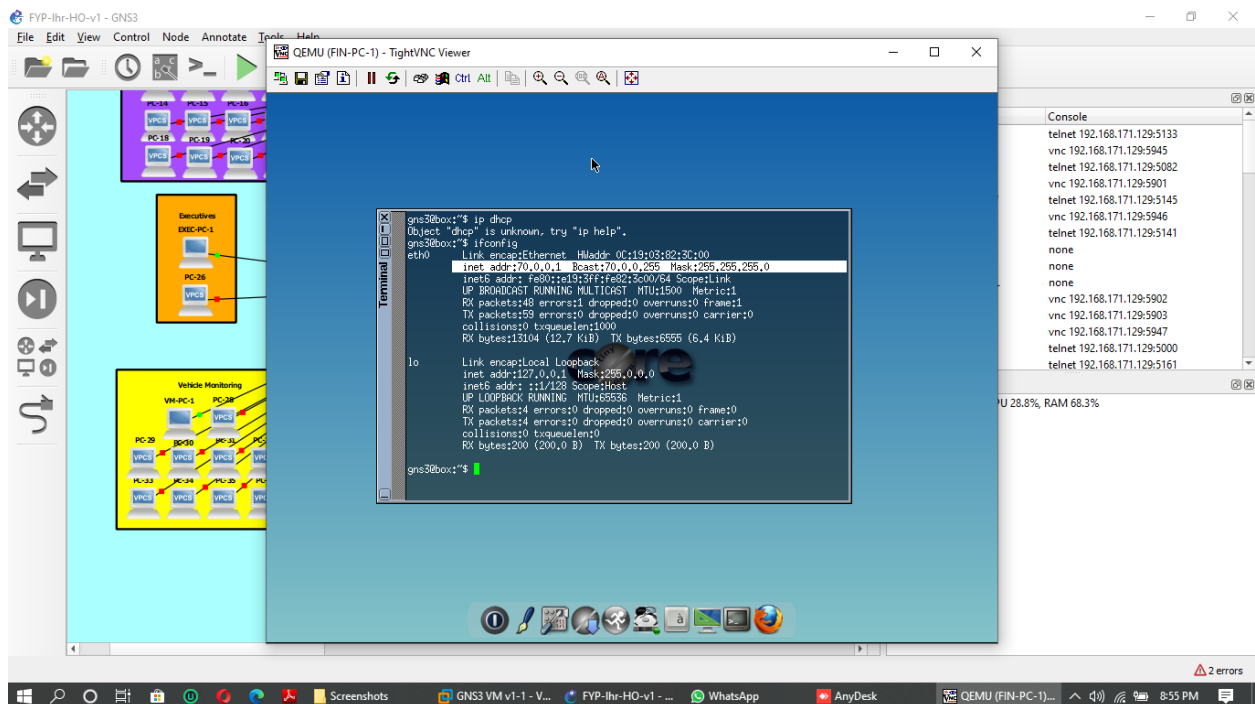


Figure L:FIN-PC-1

Description: The FIN-PC-1 obtaining DHCP allocated address successfully which is 70.0.0.1 on VLAN 70.

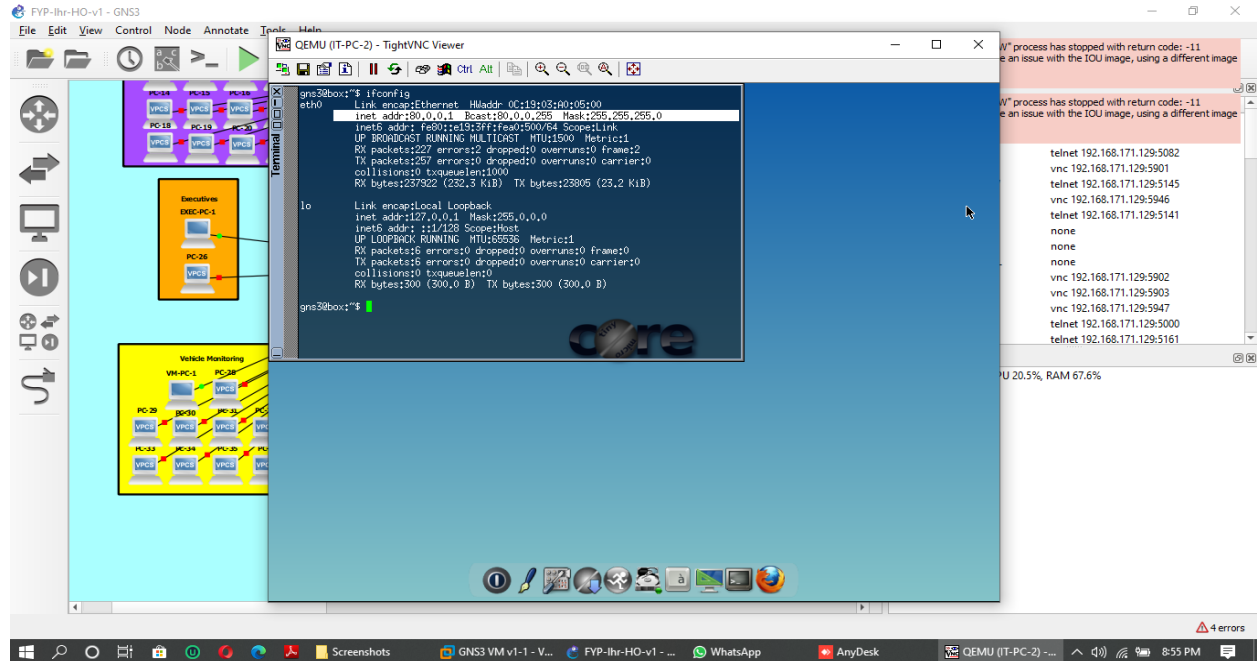


Figure 11: IT-PC-2

Description: The IT-PC-2 obtaining DHCP allocated address successfully which is 80.0.0.1 on VLAN 80.

IP ROUTES

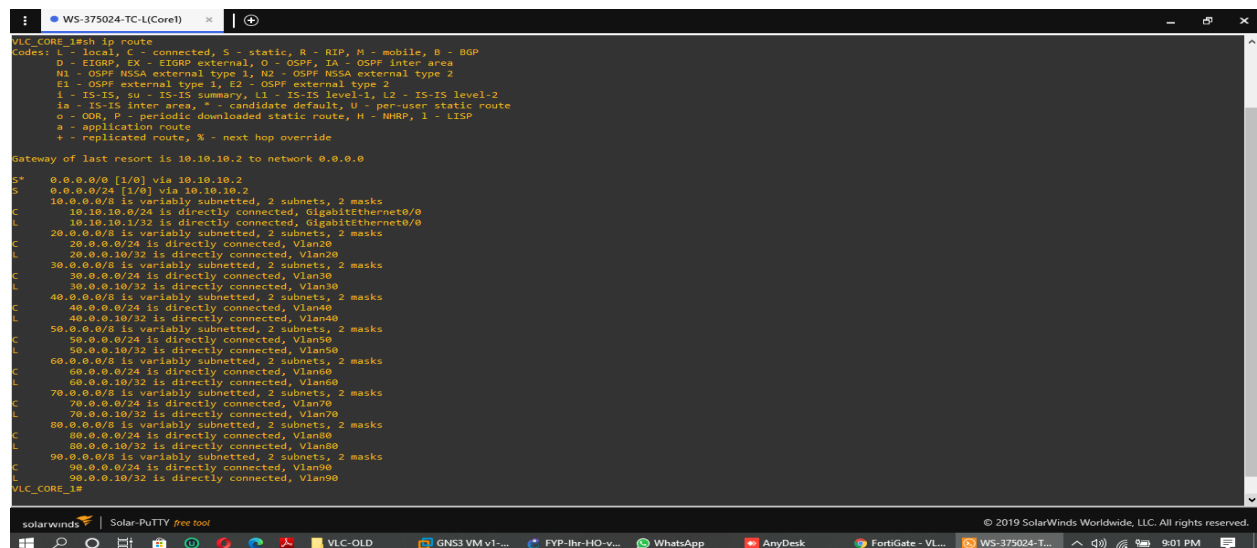


Figure LII: CORE1

Description: After done with static and directly connected routing we have obtained the above stated routes on our CORE1 Switch.

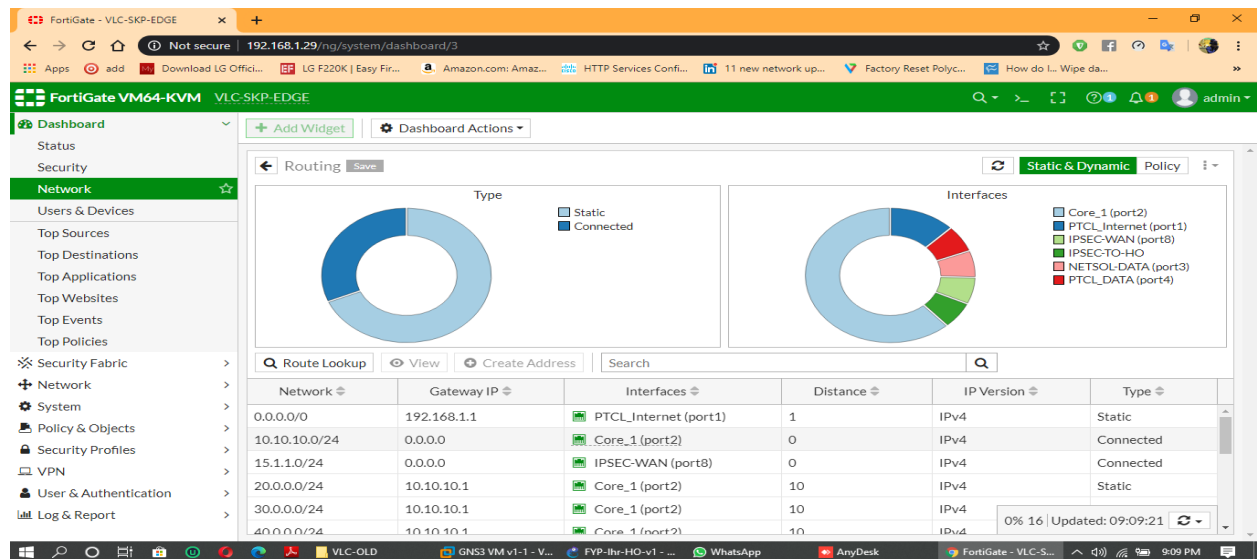


Figure LIII: SKP_EDGE_FIREWALL

Description: After done with static and directly connected routing we have obtained the above stated routes on our SKP_EDGE FIREWALL.

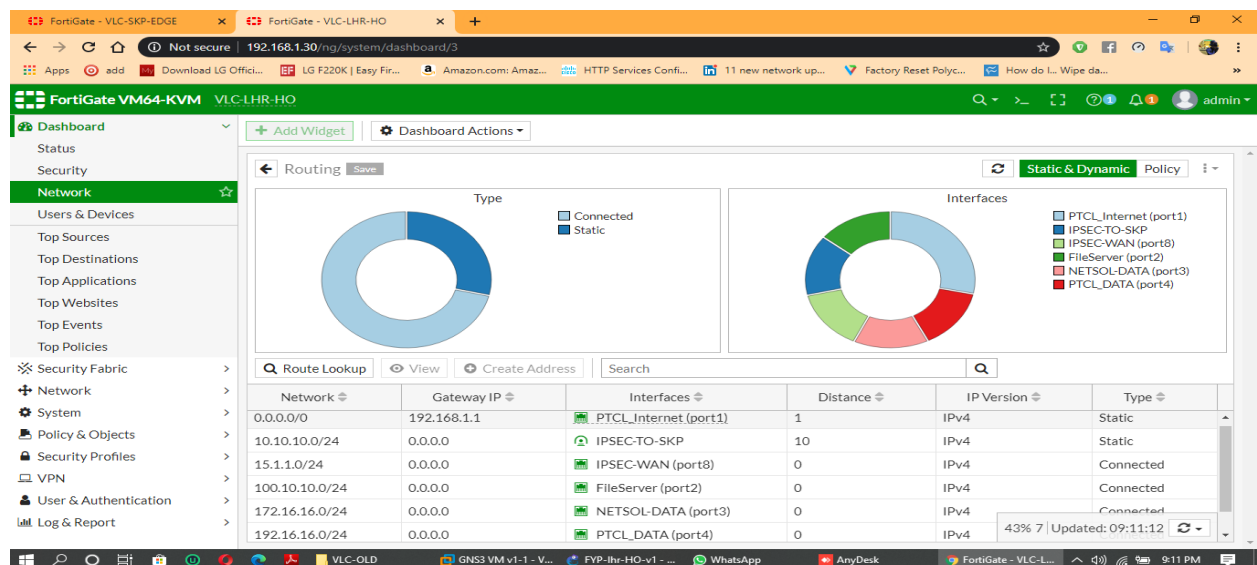


Figure LIV: HO_EDGE_FIREWALL

Description: After done with static and directly connected routing we have obtained the above stated routes on our HO_EDGE FIREWALL.

IPSEC VPN

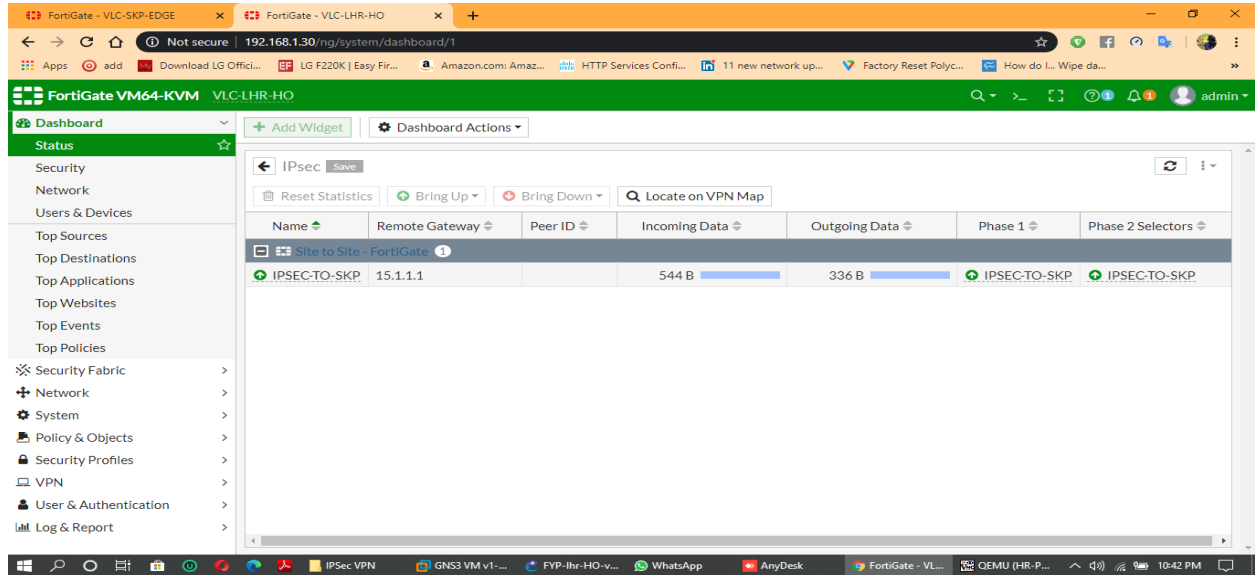


Figure LVI: HO_EDGE_FIREWALL

Description: Here we can see that the IPsec tunnel created between the Head Office Lahore and Sheikhpura branch which will allow the traffic in an encrypted form. (IPsec (Internet Protocol Security)) The tunnel is created and managed between two fortigate firewall and its also bring up successfully to transfer the data over the secure channel which will help to provide a risk free data communication between both offices. Now the MITM attack chances became zero by utilizing auto generated hashing algorithms to encrypt and decrypt the traffic.

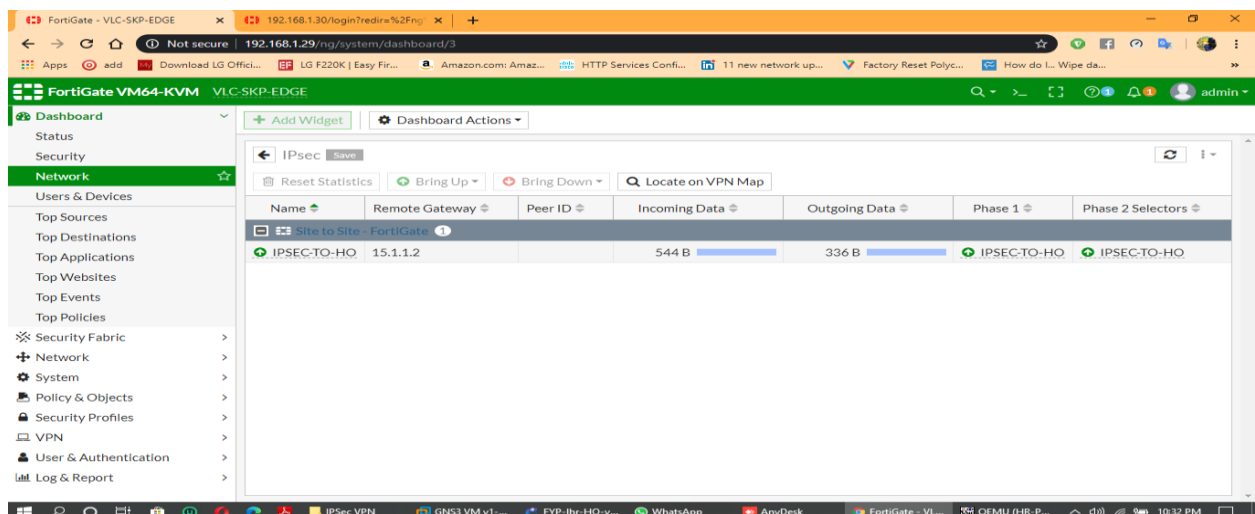


Figure LVIII: SKP_EDGE_FIREWALL

Description: Here we can also see the IPsec tunnel created between SKP branch and Head Office is configured and bring up successfully. The firewall is also showing the transfer rate of packets between both the branches. Now the user can securely reach the fileserver with encrypted data to avoid the risk of information stealing.

CORE TO HEAD OFFICE PING

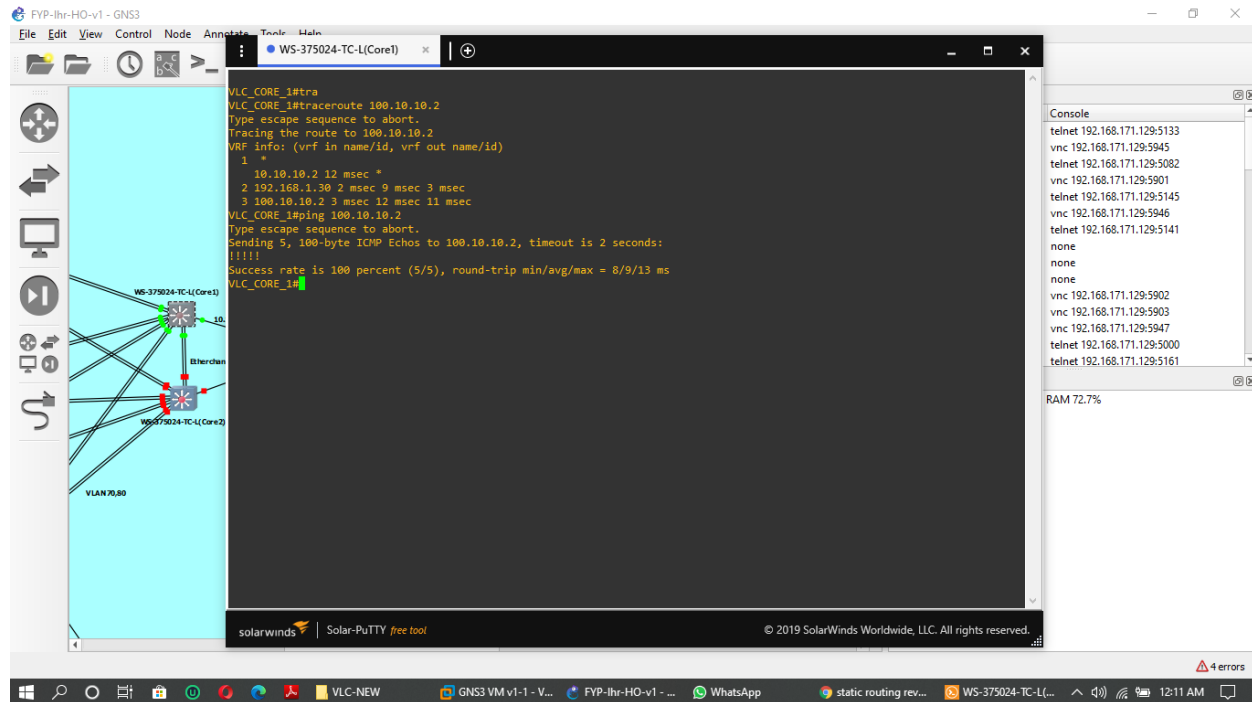


Figure LVIII: Core1

Description: The ICMP traffic is generated from the Core1 Switch located in VLC Sheikhpura and sent towards the File Server having destination IP of 100.10.10.2. The average round trip time of ICMP packet is about 9 ms which is faster than previous structure.

Figure LIXV: HR_PC_1

Description: After deploying the new structure now we can clearly see that while accessing dummy malware from www.wicar.org the firewall quickly blocked the malicious webpage to protect them from attacks.

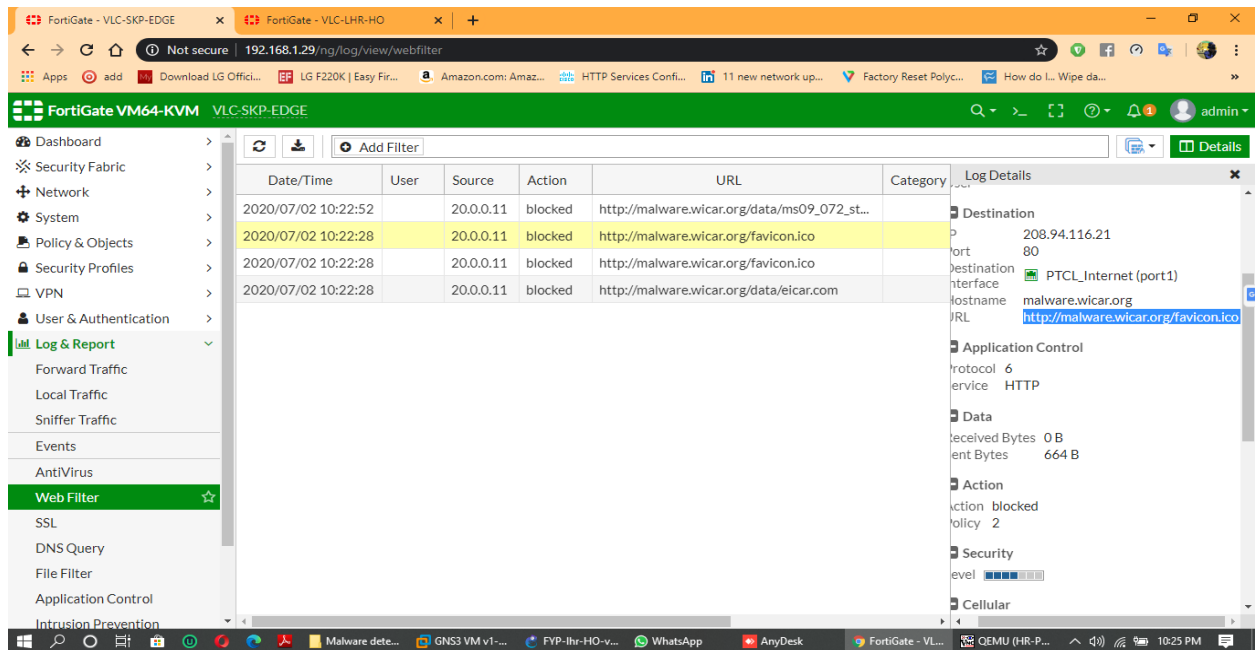


Figure LXVI: SKP_EDGE_FIREWALL

Description: Here we can see when the user (HR_MKT_PC) tried to access malicious webpage the firewall not only blocked the webpage it also generated a log which is stating the incoming ip 20.0.0.11 tried to access malware.wicar.org over HTTP and now its blocked.

POLICIES

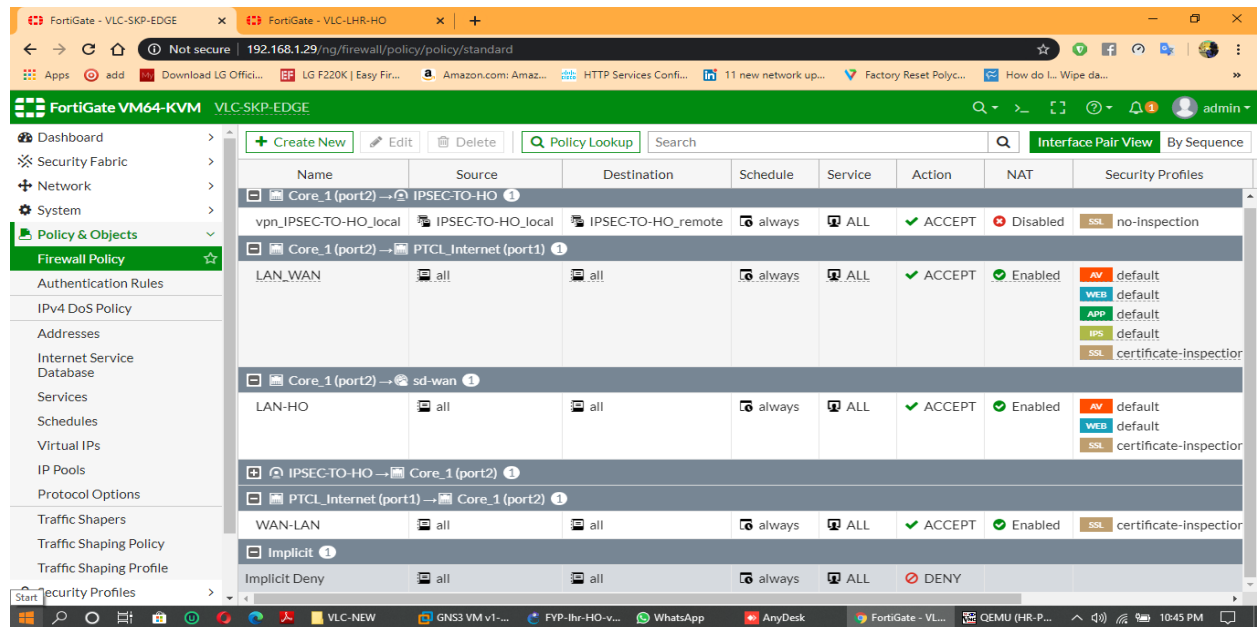


Figure LXIVII: SKP_EDGE_FIREWALL

Description: The policies are applied on SKP_EDGE_FIREWALL to make secure and safe communication possible so the policies are containing following features to make their network secure:

1. Antivirus
2. Web Filtration
3. DNS (FortiCloud)
4. Application Control
5. Intrusion Prevention System
6. Secure Socket Layer Protection

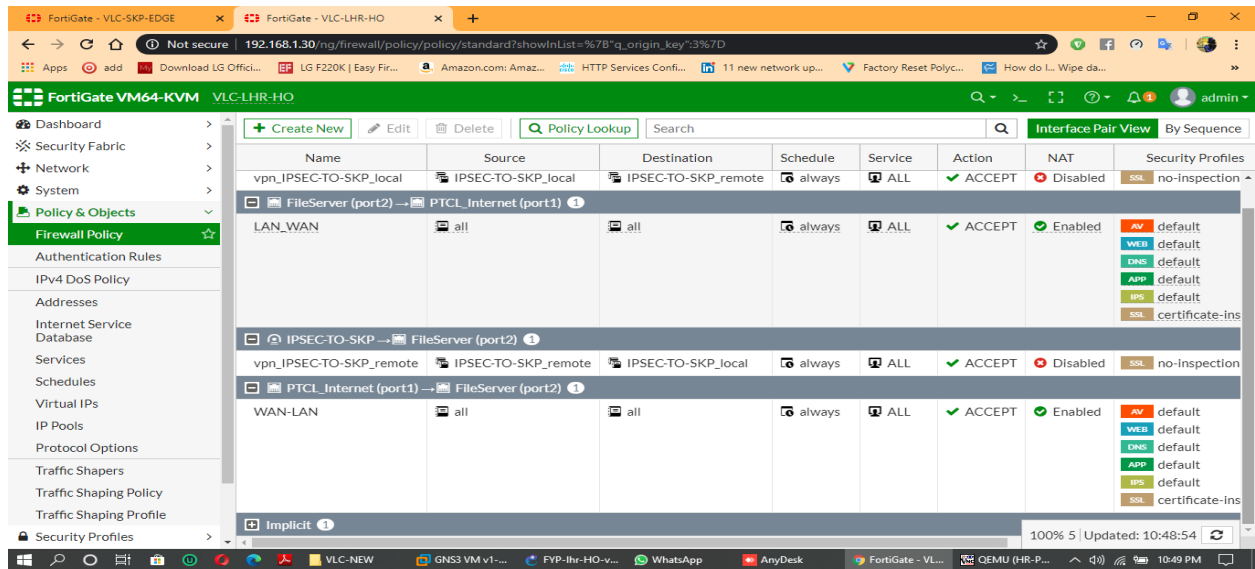


Figure LXIIVIII: HO_EDGE_FIREWALL

Description: The policies are applied on HO_EDGE_FIREWALL to make secure and safe communication possible so the policies are containing following features to make their network secure:

1. Antivirus
2. Web Filtration
3. DNS (FortiCloud)
4. Application Control
5. Intrusion Prevention System
6. Secure Socket Layer Protection

Comparison on the basis of Network Security

Case Scenario:

We used the website **www.wicar.org** which releases malware dummy signatures to test your Antivirus or secure gateways. Following are the **vulnerability test results**.

VLC OLD

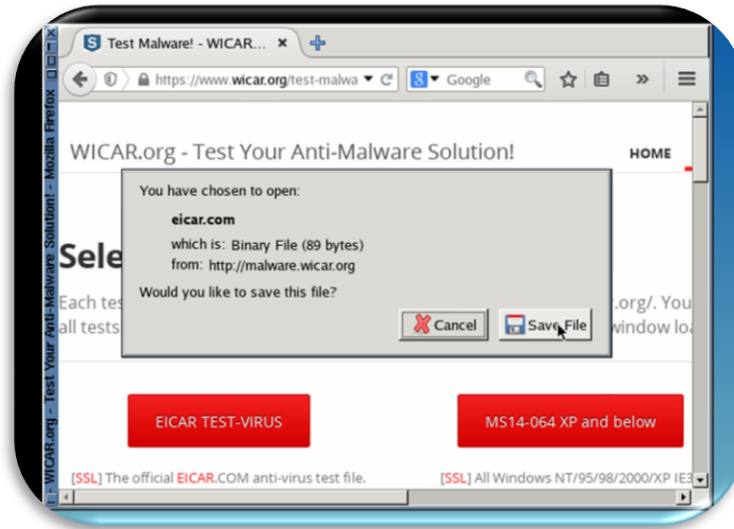


Figure LXIIIIX: Any PC from SKP Branch

Analysis & Results:

As in the old environment VLC was using Cisco ASA-5505 Firewall which is an obsoleted model even without using Firepower license. So their environment is open to the new threats. In the above test case we try to access the malicious link and then it tried to get download and machine processed the payload which caused damage to the files and running applications.

VLC NEW

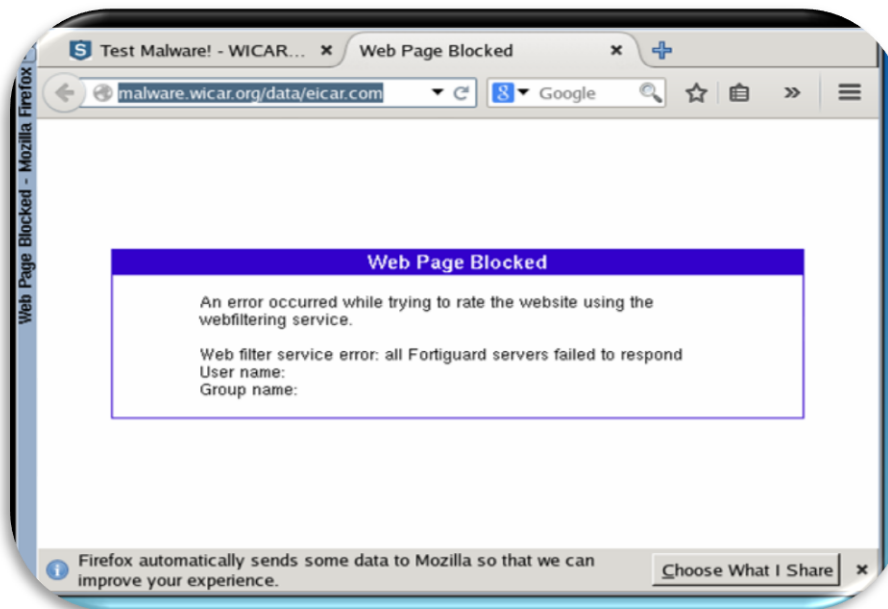


Figure LXIVX: Any PC from SKP Branch

Date/Time	User	Source	Action	URL	Category	Log Details
2020/07/02 10:22:52		20.0.0.11	blocked	http://malware.wicar.org/data/ms09_072_st...		
2020/07/02 10:22:28		20.0.0.11	blocked	http://malware.wicar.org/favicon.ico		Destination 208.94.116.21 Port 80 Destination PTCL_Internet (port1) Interface Hostname malware.wicar.org
2020/07/02 10:22:28		20.0.0.11	blocked	http://malware.wicar.org/favicon.ico		
2020/07/02 10:22:28		20.0.0.11	blocked	http://malware.wicar.org/data/eicar.com		

Figure LXVXI: Firewall logs

Analysis & Results:

In the proposed solution in the light of security we proposed the **Forti-Gate-60E-BDL** as a secure gateway. We tried to open the same link to download malicious file but the Fort i-Gate UTM solution processed the data and block the webpage due to its web filtration policy. It was predefined policy provided by FortiGuard services. So this solution made their organization secured and reliable against the latest threat vectors and trends.

Conclusion:

This project documentation is a complete proposed solution for secure and reliable network and system in a LAN environment by utilizing the latest trends and technologies. Network security always get challenges from the updated and potential threats which will always add risk to the normal workflow.

The proposed design shows that we can minimize the risk of threats and to maximize the bandwidth and its consumption in a well managed way. We also realized that the traffic flow can be more secure by encrypting the traffic and sending the confidential data over the internet protocol between the user and file server. The major reason of network security is to provide availability, integrity, and confidentiality.

So the main agenda behind secure channel of IPSec VPN is to get prevention from MITM attacks, Hackers and other malicious attacks. Company not only gets secured from outsiders it also gets secured from internal users by using intrusion prevention systems so it will cover the security from angle of 360.

Users are registered on active directory and also assigned to specified VLANs so separate vlans allow the system to add Quality of service among users regarding to their bandwidth. Now the company can manage traffic from each department separately to apply different policies for different type of users.

Redundant links and aggregation devices provide the scalability and reliability of a network by providing downtime reduced from hours to few seconds. The automated protocols switch the traffic from one channel to other to provide seamless communication. So that all of the mechanism is discussed in detail proved to work well together providing required security and low latency in a professional setting.

References

Chapter: Configuring Access and Trunk Interfaces. (n.d.). Retrieved from www.cisco.com:

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/AccessTrunk.html>

FortiGate/FortiWiFi. (n.d.). Retrieved from www.fortinet.com:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60E_Series.pdf

fouad, h. (n.d.). *HOW OSPF PROTOCOL WORKS & BASIC CONCEPTS: OSPF NEIGHBOR, TOPOLOGY & ROUTING TABLE, OSPF AREAS & ROUTER ROLES, THEORY & OVERVIEW.*

Retrieved from www.firewall.cx: <http://www.firewall.cx/networking-topics/routing/ospf-routing-protocol/1110-ospf-operation-basic-advanced-concepts-ospf-areas-roles-theory-overview.html>

IPsec (Internet Protocol Security). (n.d.). Retrieved from networklessons.com:

<https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security>

Peeva, B. (2013, april 13). *What Is a Ping Test?* Retrieved from www.websitepulse.com:

<https://www.websitepulse.com/blog/what-is-ping-test>

Rouse, M. (n.d.). *DHCP (Dynamic Host Configuration Protocol).* Retrieved from searchnetworking.techtarget.com:

<https://searchnetworking.techtarget.com/definition/DHCP>

Tetz, E. (n.d.). *Cisco Networking: Using PuTTY*. Retrieved from www.dummies.com:

<https://www.dummies.com/programming/networking/cisco/cisco-networking-using-putty/>

Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. (2019, december 11). Retrieved from www.cisco.com:

[https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-](https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-)
[protocol/5234-](https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-)

[5.html#:~:text=Spanning%20Tree%20Protocol%20\(STP\)%20is,are%20deadly%20to%20a%20network.](https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html#:~:text=Spanning%20Tree%20Protocol%20(STP)%20is,are%20deadly%20to%20a%20network.)

WS-C2960+24TC-L Datasheet. (n.d.). Retrieved from www.router-switch.com :

<https://www.router-switch.com/pdf/ws-c2960+24tc-l-datasheet.pdf>

WS-C2960X-24PS-L Datasheet. (n.d.). Retrieved from www.router-switch.com:

<https://www.router-switch.com/pdf/ws-c2960x-24ps-l-datasheet.pdf>

WS-C3750G-24T-S Datasheet. (n.d.). Retrieved from www.router-switch.com:

<https://www.router-switch.com/pdf/ws-c3750g-24t-s-datasheet.pdf>