

# TNE20002 – Network Routing Principles

Semester 1 - 2022

## Case Study Report

**ESP Team:** T008

**Lab session:** Tue 2:30 PM ATC328

**Lab tutor:** Utami Tran

### Group members:

Fatima Hanif (103173701)

Ishika Batra (103126718)

Nakshtra Yadav (103145881)

Joe Sutton Preece (102568393)

<b>Specification number</b>	2.9
<b>Class A Internal network address</b>	67.144.0.0/20
<b>Class B NAT pool public address</b>	147.9.0.0/21
<b>Class C ISP network connection address</b>	214.2.9.0/30
<b>Class B ISP Internet Web server address</b>	147.24.2.0/30
<b>Wireless Deployment Site</b>	Mackat
<b>Management VLAN Number</b>	111
<b>Percentage Growth (VLSM)</b>	35%

**Date Submitted:** 09/05/2022

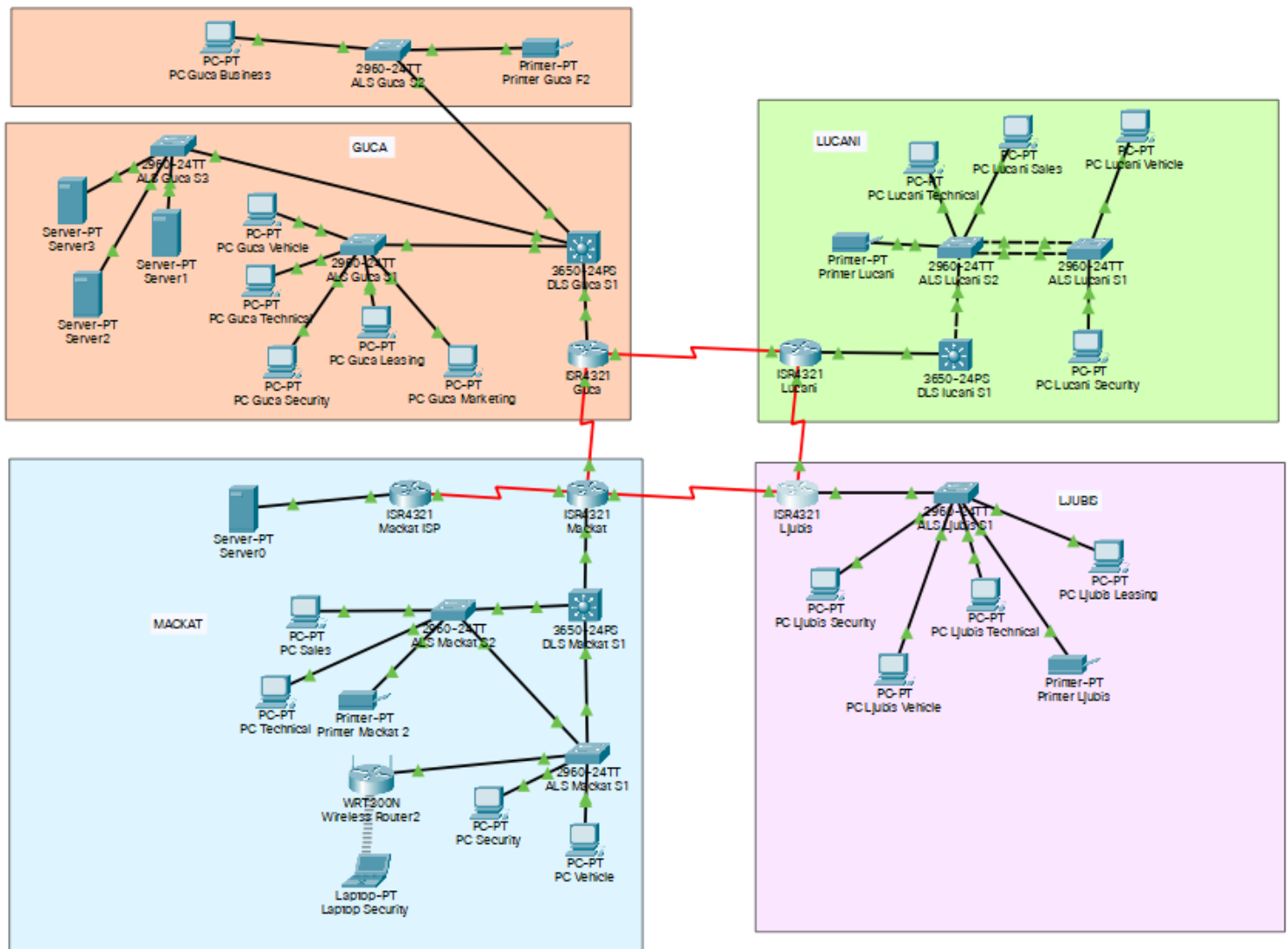
# TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
PHASE 1: CASE STUDY OVERVIEW .....	2
NETWORK TOPOLOGY .....	2
PHASE 2: IP ADDRESSING AND VLSM DESIGN .....	4
VLSM DESIGN.....	6
PHASE 3: ROUTING PROTOCOL PLANNING .....	7
PHASE 4: SWITCH AND VLAN PLANNING .....	10
PHASE 5: CONFIGURE SWITCHES,VLANs .....	12
PHASE 6: ETHERCHANNEL.....	12
PHASE 7: CONFIGURE ROUTERS AND ROUTING PROTOCOL.....	13
PHASE 8: CONFIGURING IP ADDRESSING.....	15
PHASE 9: CONFIGURING PPP AND CHAP .....	16
PHASE 10: WIRELESS LAN DEPLOYMENT SITE .....	16
PHASE 11: NAT CONFIGURATION .....	17
PHASE 12: ACCESS CONTROL AT GUCA SITE.....	19
SYSTEM TESTING AND VERIFICATION STRATEGY .....	24

## Phase I: Case study overview

Best Motors Ltd is a company that leases, buys and sells and repairs cars, trucks and buses. The Head Office is at the Guca site while the other company sites are in Ljubis, Mackat and Lucani. This written report will show and discuss how we implemented a working network that allows for cross site communication, as well as support for potential growth over the next five years.

## Network topology



**Company Site Layout:**

Guca	Ljubis
<ul style="list-style-type: none"> <li>• The Leasing, Marketing and Vehicle Servicing groups are on floor 1.</li> <li>• The Business group is on floor 2</li> <li>• The Servers are on floor 1</li> <li>• Site size 1500metres x 1500metres</li> <li>• Building Floor size 100metres x 200metres</li> <li>• Technical Support group on floor 1</li> </ul>	<ul style="list-style-type: none"> <li>• Leasing, Vehicle Servicing and Technical Support groups are on the ground floor of a single level building</li> <li>• Site size 1500metres x 2000metres</li> <li>• Building Floor size 120metres x 30metres</li> </ul>
Lucani	Mackat
<ul style="list-style-type: none"> <li>• Sales, Vehicle Servicing and Technical Support groups are on the ground floor of a single level building.</li> <li>• Site size 2000metres x 2000metres</li> <li>• Building Floor size 225metres x 30metres</li> </ul>	<ul style="list-style-type: none"> <li>• Sales, Vehicle Servicing and Technical Support groups are on the ground floor of a single level building</li> <li>• Site size 1250metres x 2000metres</li> <li>• Building Floor size 125metres x 40metres</li> </ul>

## Phase 2: IP Addressing and VLSM design

The company was provided with a 'class A' internal network of 67.144.0.0/20. For our sites to effectively communicate with one another and their own internal network, we implemented a method known as variable length subnetting. This method allows each site to efficiently prioritize the network address based on the number of required hosts for each specified VLAN. Applying this technique reduced the amount of wasted host spaces, and an increase of an additional 35% of hosts was also taken into consideration when creating the VLSM design.

The figure below shows the site workgroups that are found within the company with the total number of host requirements mentioned. Each of these workgroups are divided into different VLANs built around their work operations such as Security, Technical, and Vehicle etc.

### 2.1 Company workgroups

Site VLANs	Guca	Lucani	Ljubis	Mackat
10 Security	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$
11 Technical	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$
12 Vehicle	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$	$5 \text{ h} + 35\% = 7$
13 Leasing	$125 \text{ h} + 35\% = 169$	-	$80 \text{ h} + 35\% = 108$	-
14 Marketing	$180 \text{ h} + 35\% = 243$	-	-	-
15 Business	$200 \text{ h} + 35\% = 270$	-	-	-
16 Sales	-	$140 \text{ h} + 35\% = 189$	-	$125 \text{ h} + 35\% = 169$
Total	703	210	129	190
Overall total	1232 (hosts)			

Next, we have the sum of hosts required for each Management VLAN within the company's sites. Each switch within the company's sites will constantly have VLAN 111 Management always operating, and at least one printer that will be used for business purposes. The host requirements for the printers will also contribute to the overall host requirements needed for the VLSM design.

### 2.2 Management and Printer hosts requirements

VLANs	Guca	Lucani	Ljubis	Mackat
111 Management	20	15	15	15
200 Printer	2	2	2	2
Total	22	17	17	17
Overall total	73 (hosts)			

The server farms will also contribute to the final number of host requirements needed for an accurate VLSM design. These are applied to help with server functionality within the Guca site. The final number of hosts for the server farms can be found below.

### 2.3 Server Farm VLAN on Guca

VLANs	Guca	Lucani	Ljubis	Mackat
300 Server Farm	20	-	-	-
Total	20	-	-	-
Overall total	20 (hosts)			

Lastly, we need to consider the serial links used by each router connecting to the other router. These serial links will enable communications between the company's sites at their respective physical locations. A loopback0 has also been implemented purely for diagnostics and troubleshooting.

### 2.4 Loopback and Serial links between routers

Loopback 0	Serial link 1	Serial link 2	Serial link 3	Serial link 4	Total
5	2	2	2	2	13 (hosts)

The number of available hosts given to us by the **class A internal network** is 4094, however; after calculating the required number of hosts for each of the company's sites, we are only after:

$$1232 + 73 + 20 + 13 = 1,338 \text{ (hosts required)}$$

Without the use of a variable length subnetting method, the company would have used 12x the address space or 15046 extra hosts. The amount of misspent and unused IP addresses that could have gone to waste would have exceeded the total space available. However, after correctly figuring out our host requirements, we separated the networks into various subnets below according to their specified hosts.

## VLSM Design

**Table A: VLSM Design**

The remaining free address range after VLSM subnetting is from 67.144.8.7 - 67.144.15.255.

This leaves 49.8% of the major network free for later use.

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
Guca business	270	510	67.144.0.0	/23	255.255.254.0	67.144.0.1 - 67.144.1.254	67.144.1.255
Guca marketing	243	254	67.144.2.0	/24	255.255.255.0	67.144.2.1 - 67.144.2.254	67.144.2.255
Lucani sales	189	254	67.144.3.0	/24	255.255.255.0	67.144.3.1 - 67.144.3.254	67.144.3.255
Guca leasing	169	254	67.144.4.0	/24	255.255.255.0	67.144.4.1 - 67.144.4.254	67.144.4.255
Mackat sales	169	254	67.144.5.0	/24	255.255.255.0	67.144.5.1 - 67.144.5.254	67.144.5.255
Ljubis leasing	108	126	67.144.6.0	/25	255.255.255.128	67.144.6.1 - 67.144.6.126	67.144.6.127
Guca management	20	30	67.144.6.128	/27	255.255.255.224	67.144.6.129 - 67.144.6.158	67.144.6.159
Guca server farm	20	30	67.144.6.160	/27	255.255.255.224	67.144.6.161 - 67.144.6.190	67.144.6.191
Ljubis management	15	30	67.144.6.192	/27	255.255.255.224	67.144.6.193 - 67.144.6.222	67.144.6.223
Lucani management	15	30	67.144.6.224	/27	255.255.255.224	67.144.6.225 - 67.144.6.254	67.144.6.255
Mackat management	15	30	67.144.7.0	/27	255.255.255.224	67.144.7.1 - 67.144.7.30	67.144.7.31
Guca security	7	14	67.144.7.32	/28	255.255.255.240	67.144.7.33 - 67.144.7.46	67.144.7.47
Guca technical	7	14	67.144.7.48	/28	255.255.255.240	67.144.7.49 - 67.144.7.62	67.144.7.63
Guca vehicle	7	14	67.144.7.64	/28	255.255.255.240	67.144.7.65 - 67.144.7.78	67.144.7.79
Ljubis security	7	14	67.144.7.80	/28	255.255.255.240	67.144.7.81 - 67.144.7.94	67.144.7.95
Ljubis technical	7	14	67.144.7.96	/28	255.255.255.240	67.144.7.97 - 67.144.7.110	67.144.7.111
Ljubis vehicle	7	14	67.144.7.112	/28	255.255.255.240	67.144.7.113 - 67.144.7.126	67.144.7.127
Lucani security	7	14	67.144.7.128	/28	255.255.255.240	67.144.7.129 - 67.144.7.142	67.144.7.143
Lucani technical	7	14	67.144.7.144	/28	255.255.255.240	67.144.7.145 - 67.144.7.158	67.144.7.159
Lucani vehicle	7	14	67.144.7.160	/28	255.255.255.240	67.144.7.161 - 67.144.7.174	67.144.7.175
Mackat security	7	14	67.144.7.176	/28	255.255.255.240	67.144.7.177 - 67.144.7.190	67.144.7.191
Mackat technical	7	14	67.144.7.192	/28	255.255.255.240	67.144.7.193 - 67.144.7.206	67.144.7.207
Mackat vehicle	7	14	67.144.7.208	/28	255.255.255.240	67.144.7.209 - 67.144.7.222	67.144.7.223
Loopback 0	5	6	67.144.7.224	/29	255.255.255.248	67.144.7.225 - 67.144.7.230	67.144.7.231
Guca printer	2	2	67.144.7.232	/30	255.255.255.252	67.144.7.233 - 67.144.7.234	67.144.7.235
Ljubis printer	2	2	67.144.7.236	/30	255.255.255.252	67.144.7.237 - 67.144.7.238	67.144.7.239
Lucani printer	2	2	67.144.7.240	/30	255.255.255.252	67.144.7.241 - 67.144.7.242	67.144.7.243
Mackat printer	2	2	67.144.7.244	/30	255.255.255.252	67.144.7.245 - 67.144.7.246	67.144.7.247
Serial 0	2	2	67.144.7.248	/30	255.255.255.252	67.144.7.249 - 67.144.7.250	67.144.7.251
Serial 1	2	2	67.144.7.252	/30	255.255.255.252	67.144.7.253 - 67.144.7.254	67.144.7.255
Serial 2	2	2	67.144.8.0	/30	255.255.255.252	67.144.8.1 - 67.144.8.2	67.144.8.3
Serial 3	2	2	67.144.8.4	/30	255.255.255.252	67.144.8.5 - 67.144.8.6	67.144.8.7

## Phase 3: Routing protocol planning

In our topology, we have assigned the OSPF dynamic routing protocol for use on the routers that connect the sites. This gateway protocol will be used to automate the routing decisions and configurations across the network. It will also establish a low usage of network resources during normal business operations with other OSPF configured routers in the network to establish a neighbor-type class connection for all internal links.

Due to the VLSM design, providing the networks for the OSPF statements over a serial link was made easier as the subnet ranges were chosen from the remaining available hosts.

Whatever was left was given to the serial links for cost-effective configuration as each link only required 2 available spaces.

### 3.1 OSPF established neighbors

#### Mackat

```
MackatR1#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
67.144.8.6	0	FULL/ -	00:00:33	67.144.8.6	Serial0/2/0
67.144.7.253	0	FULL/ -	00:00:34	67.144.7.250	Serial0/1/0

```
MackatR1#
```

#### Lucani

```
LucaniR1# sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
67.144.7.253	0	FULL/ -	00:00:39	67.144.7.253	Serial0/1/1

```
LucaniR1#
```

#### Ljubis

```
LjubisR1#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
67.144.7.225	0	FULL/ -	00:00:31	67.144.8.5	Serial0/2/0

```
LjubisR1#
```

#### Guca

```
GucaR1#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
67.144.7.225	0	FULL/ -	00:00:34	67.144.7.249	Serial0/1/0
67.144.8.1	0	FULL/ -	00:00:32	67.144.7.254	Serial0/1/1

```
GucaR1#
```



### 3.2 Link Bandwidth for all serial links between all routers:

Link bandwidth for all serial links between routers was set to 256 Kbit according to the company's requirements.

### 3.3 Passive interfaces on Mackat router

```
router ospf 4
 log-adjacency-changes
 passive-interface Loopback0
 passive-interface GigabitEthernet0/0/1.10
 passive-interface GigabitEthernet0/0/1.11
 passive-interface GigabitEthernet0/0/1.12
 passive-interface GigabitEthernet0/0/1.16
 passive-interface GigabitEthernet0/0/1.111
 passive-interface GigabitEthernet0/0/1.200
```

### 3.4 OSPF MD5 Authentication

```
GucaR1#sh ip ospf interface s0/1/0
Serial0/1/0 is up, line protocol is up
 Internet address is 67.144.7.250/30, Area 0
  Process ID 3, Router ID 67.144.7.253, Network Type POINT-TO-POINT, Cost:
 390
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 10/10, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 67.144.7.225
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
```

For security, MD5 authentication was configured on the link between Guca and Mackat. OSPF MD5 Authentication ensures that an unauthorized IP resource cannot inject OSPF routing messages into the network without detection, thus ensuring the integrity of the routing tables in the OSPF routing network.

### 3.5 Default route to Mackat ISP

```
217.2.9.0/24 is variably subnetted, 3 subnets, 2 masks
C    214.2.9.0/30 is directly connected, Serial0/1/1
C    214.2.9.1/32 is directly connected, Serial0/1/1
L    214.2.9.2/32 is directly connected, Serial0/1/1
S*   0.0.0.0/0 is directly connected, Serial0/1/1

MackatR1#
```

### 3.6 ISP advertised to internal network

```

MackatISP#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, E - EGP
       i - IS-IS, 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

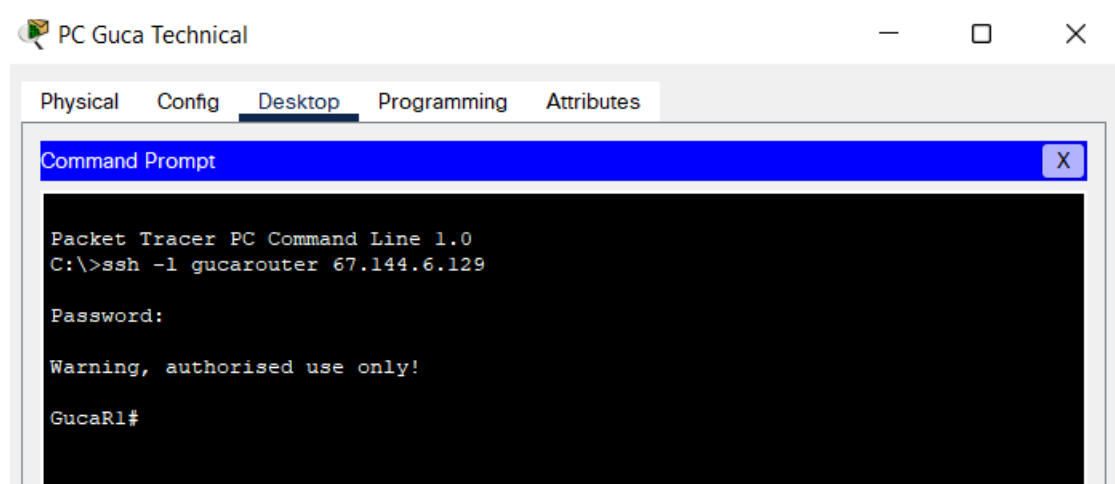
Gateway of last resort is not set

    67.0.0.0/20 is subnetted, 1 subnets
S       67.144.0.0/20 is directly connected, Serial0/1/1
    147.9.0.0/21 is subnetted, 1 subnets
S       147.9.0.0/21 is directly connected, Serial0/1/1
    147.24.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       147.24.2.0/30 is directly connected, GigabitEthernet0/0/0
L       147.24.2.1/32 is directly connected, GigabitEthernet0/0/0
    214.2.9.0/24 is variably subnetted, 3 subnets, 2 masks
C       214.2.9.0/30 is directly connected, Serial0/1/1
L       214.2.9.1/32 is directly connected, Serial0/1/1
C       214.2.9.2/32 is directly connected, Serial0/1/1

```

### 3.7 Router accessible via SSH for maintenance by PCs in Technical Support Group for maintenance

To allow for easier ongoing maintenance, the Guca router was made accessible by SSH to the technical support group on site.



## Phase 4: Switch and VLAN planning

To separate management traffic from general traffic, a dedicated management VLAN was established using VLAN number 111 on all sites. All networking devices were configured to be in this VLAN.

For added security at all sites, all unused ports are administratively shut down on all sites.

In the Ljubis site, there is a configuration for port security on each connected outward facing port on the access layer switches in the Ljubis site. This helps in avoiding any unauthorized connections and drops the packet if mac addresses are unknown. It is done to ensure that traffic control is enabled in the network so that the network won't be able to receive any suspicious traffic from the external network. To allow ease of communication between devices, we have configured mac address sticky command, which allows switches to learn addresses dynamically and add them to their address able.

### 4.1 Port Security on Ljubis Switch

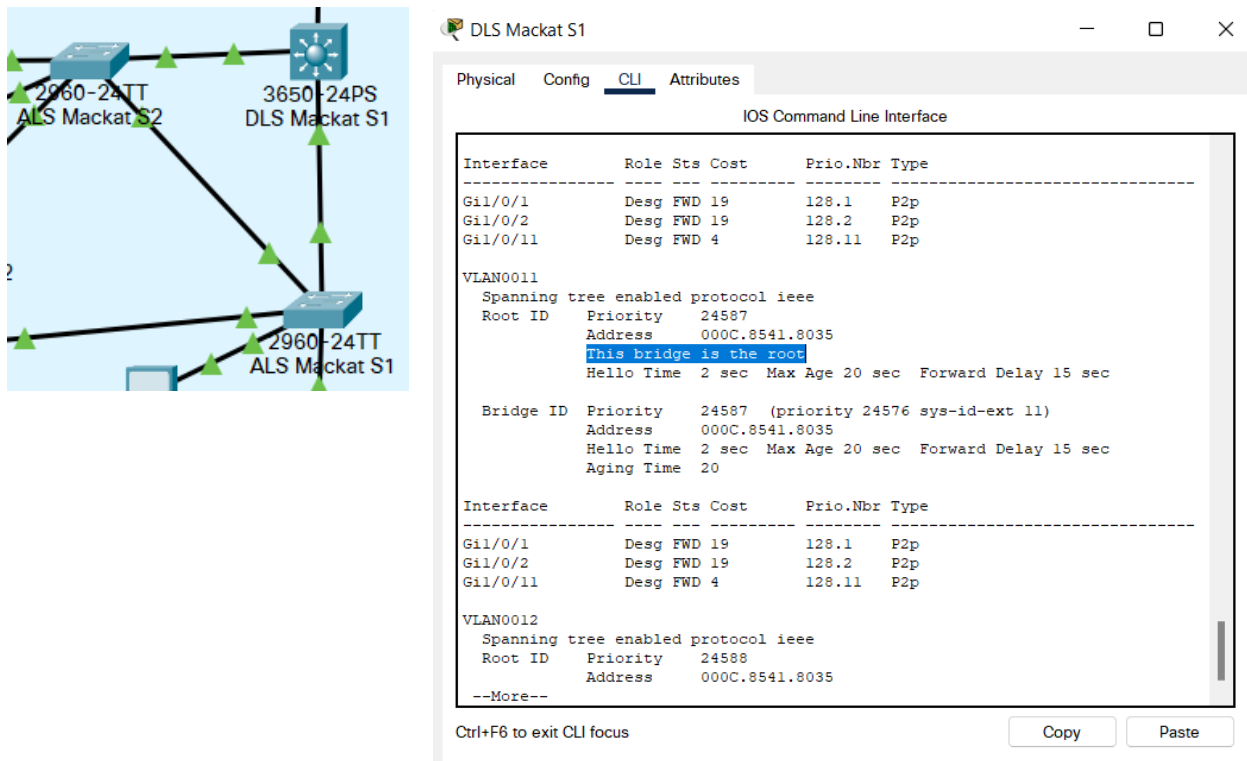
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/3	1	1	0	Protect
Fa0/4	1	1	0	Protect
Fa0/5	1	0	0	Protect
Fa0/6	1	1	0	Protect
Fa0/7	1	1	0	Protect

### 4.2 Switch VLANs (Guca S1)

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Guca_Security	active	Fa0/5
11	Guca_Technical	active	Fa0/4
12	Guca_Vehicle	active	Fa0/3
13	Guca_Leasing	active	Fa0/6
14	Guca_Marketing	active	Fa0/7
111	Guca_Management	active	
200	Guca_Printer	active	
300	ServerFarm	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

### 4.3 Implemented path redundancy on Mackat and created Distribution switch (DLSMackatS1) as route bridge

This is done to ensure that the number of ways for packet to reach its destination is optimized. If in any case there is a network failure, this way the packet can still reach its destination. It also helps avoid layer 2 looping which leads to mac address instability and causes broadcast storm which collapses the network.



The image shows a network diagram on the left and a CLI screenshot for DLS Mackat S1 on the right. The diagram illustrates a network topology with three switches: 2960-24TT ALS Mackat S2, 3650-24PS DLS Mackat S1, and 2960-24TT ALS Mackat S1. The CLI screenshot displays the configuration for DLS Mackat S1, showing the CLI interface with tabs for Physical, Config, CLI, and Attributes. The CLI output shows the configuration for VLAN0011 and VLAN0012, including spanning tree settings and interface configurations.

```

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gil/0/1        Desg FWD 19      128.1    P2p
Gil/0/2        Desg FWD 19      128.2    P2p
Gil/0/11       Desg FWD 4      128.11   P2p

VLAN0011
Spanning tree enabled protocol ieee
Root ID        Priority      24587
Address        000C.8541.8035
                This bridge is the root
Hello Time     2 sec      Max Age 20 sec  Forward Delay 15 sec

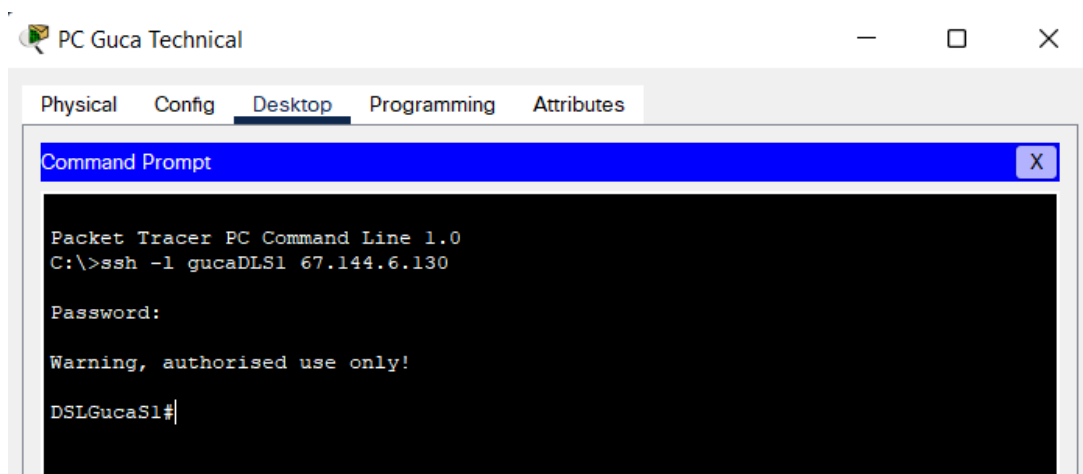
Bridge ID      Priority      24587 (priority 24576 sys-id-ext 11)
Address        000C.8541.8035
Hello Time     2 sec      Max Age 20 sec  Forward Delay 15 sec
Aging Time     20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gil/0/1        Desg FWD 19      128.1    P2p
Gil/0/2        Desg FWD 19      128.2    P2p
Gil/0/11       Desg FWD 4      128.11   P2p

VLAN0012
Spanning tree enabled protocol ieee
Root ID        Priority      24588
Address        000C.8541.8035
--More--
  
```

### 4.4 Switches accessible via SSH for maintenance by PCs in Technical Support Group for maintenance

To allow for easier ongoing maintenance, the Guca switches were made accessible by SSH to the technical support group on site.



The image shows a screenshot of a PC window titled "PC Guca Technical". The window contains a "Command Prompt" window with the following text:

```

Packet Tracer PC Command Line 1.0
C:\>ssh -l gucaDLS1 67.144.6.130

Password:

Warning, authorised use only!

DSLGucaS1#
  
```

## Phase 5: Configure switches, VLANs

In this network, we have used 2 different switches, WS-C3650-24PS and WS-C2960-24TT.

The reason why we choose to use the WS-C3650-24PS to connect the routers to the internal switches is because WS-3650-24PS has more ports and has much more powerful ports than WS-C2960-24TT (GigabitEthernet ports).

Furthermore, the reason why we had chosen to use the WS-C2960-24TT was so that they can be utilized as a distribution switch to PCs of each VLAN is because they're cheaper than using a WS-C3650-24PS as a distribution switch, while still having close to, if not; the same amount of ports as WS-C3650-24PS. However, they may not have as powerful in comparison to WS-C3650-24PS (FastEthernet ports).

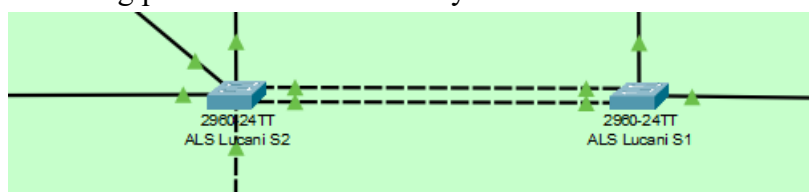
Below is a table filled with all the switch information of the network:

**Table B: Switch Details**

Name	Model	# of Ports	Location	IP on mgmt. VLAN	Default Gateway
DSLGucaS1	3650	24 + 4	Guca	67.144.6.130	67.144.6.129
ALSGucaS1	2960	24 + 2	Guca	67.144.6.131	67.144.6.129
ALSGucaS2	2960	24 + 2	Guca	67.144.6.133	67.144.6.129
ALSGucaS3	2960	24 + 2	Guca	67.144.6.132	67.144.6.129
DLSLucaniS1	3650	24 + 4	Lucani	67.144.6.226	67.144.6.225
ALSLucaniS1	2960	24 + 2	Lucani	67.144.6.228	67.144.6.225
ALSLucaniS2	2960	24 + 2	Lucani	67.144.6.227	67.144.6.225
ALSLjubisS1	2960	24 + 2	Ljubis	67.144.6.194	67.144.6.193
DSLmackatS1	3650	24 + 4	Mackat	67.144.7.2	67.144.7.1
ALSMackatS1	2960	24 + 2	Mackat	67.144.7.3	67.144.7.1
ALSMackatS2	2960	24 + 2	Mackat	67.144.7.4	67.144.7.1

## Phase 6: EtherChannel

The plan includes EtherChannel between networking devices to improve redundancy and boost bandwidth. This was configured on the Lucani site for the prototype using LACP across 2 ports. This is because if a physical link goes down, the other Ether Channel link will be used for sending and receiving packets. It is a better way to utilize bandwidth on redundant links



for layer 2 technology such as MAC address. We have used LACP as this helps to protect the network against switching loops occurred in switches when not configured properly.

Below are the CLI status for the Ether Channel from the **ALS Lucani S2** and **ALS Lucani S1**.

### 6.1.1 Ether Channel S2:

```

ALSLucaniS2#sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----
1      Pol(SU)          LACP       Fa0/3(P) Fa0/4(P)

```

### 6.1.2 Ether Channel S1

```

ALSLucaniS1#sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----
1      Pol(SU)          LACP       Fa0/3(P) Fa0/4(P)

```

## Phase 7: Configure Routers and Routing protocol

For the servers in the Mackat site, an ISP Class B address given in the email specifications was configured on to the server. This web server will be represented as the “Internet” in the network. In addition to that, a static route has been configured on the Mackat ISP router to connect it back to the internal network. This is to ensure that there is an existing connection between the internal router and the external router connecting to the Internet:

**Table C: Router Details**

**Site: Mackat**

**Router name: MackatR1**

Sub Interface	Description	VLAN #	Network Address	Interface IP Address	CIDR
<b>G0/0/1.111</b>	Connection to Mackat Management	111	67.144.7.0	67.144.7.1	/27
<b>G0/0/1.200</b>	Connection to Mackat Printer	200	67.144.7.244	67.144.7.245	/30
<b>G0/0/1.16</b>	Connection to Mackat Sales	16	67.144.5.0	67.144.5.1	/24
<b>G0/0/1.10</b>	Connection to Mackat Security	10	67.144.7.176	67.144.7.177	/28
<b>G0/0/1.11</b>	Connection to Mackat Technical	11	67.144.7.192	67.144.7.193	/28
<b>G0/0/1.12</b>	Connection to Mackat Vehicle	12	67.144.7.208	67.144.7.209	/28

**Site: Guca****Router name: GucaR1**

Sub Interface	Description	VLAN #	Network Address	Interface IP Address	CIDR
G0/0/1.15	Connection to Guca Business	15	67.144.0.0	67.144.0.1	/23
G0/0/1.13	Connection to Guca Leasing	13	67.144.4.0	67.144.4.1	/24
G0/0/1.111	Connection to Guca Management	111	67.144.6.128	67.144.6.129	/27
G0/0/1.14	Connection to Guca Marketing	14	67.144.2.0	67.144.2.1	/24
G0/0/1.200	Connection to Guca Printer	200	67.144.7.232	67.144.7.233	/30
G0/0/1.10	Connection to Guca Security	10	67.144.7.32	67.144.7.33	/28
G0/0/1.300	Connection to Guca Server Farm	300	67.144.6.160	67.144.6.161	/27
G0/0/1.11	Connection to Guca Technical	11	67.144.7.48	67.144.7.49	/28
G0/0/1.12	Connection to Guca Vehicle	12	67.144.7.64	67.144.7.65	/28

**Site: Ljubis****Router name: LjubisR1**

Sub Interface	Description	VLAN	Network Address	Interface IP Address	CIDR
G0/0/1.13	Connection to Ljubis Leasing	13	67.144.6.0	67.144.6.1	/25
G0/0/1.111	Connection to Ljubis Management	111	67.144.6.192	67.144.6.193	/27
G0/0/1.200	Connection to Ljubis Printer	200	67.144.7.236	67.144.7.237	/30
G0/0/1.10	Connection to Ljubis Security	10	67.144.7.80	67.144.7.81	/28
G0/0/1.11	Connection to Ljubis Technical	11	67.144.7.96	67.144.7.97	/28
G0/0/1.12	Connection to Ljubis Vehicle	12	67.144.7.112	67.144.7.113	/28

**Site: Lucani****Router name: LucaniR1**

Sub Interface	Description	VLAN	Network Address	Interface IP Address	CIDR
G0/0/1.111	Connection to Lucani Management	111	67.144.6.224	67.144.6.225	/27
G0/0/1.200	Connection to Lucani Printer	200	67.144.7.240	67.144.7.241	/30
G0/0/1.16	Connection to Lucani Sales	16	67.144.3.0	67.144.3.1	/24
G0/0/1.10	Connection to Lucani Security	10	67.144.7.128	67.144.7.129	/28
G0/0/1.11	Connection to Lucani Technical	11	67.144.7.144	67.144.7.145	/28
G0/0/1.12	Connection to Lucani Vehicle	12	67.144.7.160	67.144.7.161	/28

## Phase 8: Configuring IP Addressing

In the Ljubis site, DHCP has been configured, which is a network management protocol which automatically configures IP networks for devices, allowing them to use any communication protocol in the network. This helps in reducing operation task with the network administrator as well as optimizing IP address plans and allowing user mobility to be easily managed throughout the network.

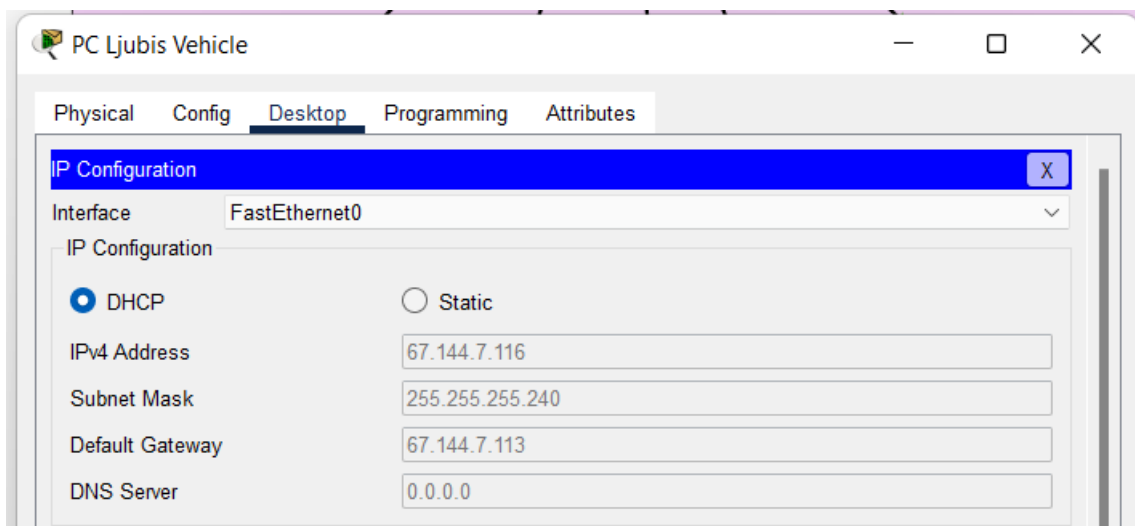
The table below shows the DHCP pool used to distribute the network address amongst all the VLANs located at the Ljubis site as well as the excluded address range for all VLANs which will be used for management of devices.

**Table D: Ljubis DHCP Server Pool IP Host Addresses:**

VLAN Name	Excluded address range	IP Address Pool Range	Subnet Mask/ CIDR	Default Gateway
10	67.144.6.1 - 67.144.6.3	67.144.7.84 - 67.144.7.94	/28	67.144.7.81
11	67.144.7.237 - 67.144.7.239	67.144.7.100 - 67.144.7.110	/28	67.144.7.97
12	67.144.7.81 - 67.144.7.83	67.144.7.116 - 67.144.7.126	/28	67.144.7.113
13	67.144.7.97 - 67.144.7.99	67.144.6.4 - 67.144.6.126	/25	67.144.6.1

The PC in Vehicle uses a DHCP IP for its configuration taken from VLAN 12 with a default gateway of 67.144.7.113. This default gateway assigned by the DHCP will then be referenced as a sub interface for VLAN 12 on the router for its specific site (Ljubis). This DHCP example can be seen below:

### 8.1 DHCP Configurations on PC Ljubis Vehicle





**Table E: Statically assigned IP Host Addresses – Servers, Printers etc:**

Name	VLAN	IP Address	CIDR	Default Gateway IP Address	Service provided
Server1	300	67.144.6.162	/27	67.144.6.161	Server farm hosting different types of servers such as a file server, email server, active directory server etc
Server2	300	67.144.6.163	/27	67.144.6.161	
Server3	300	67.144.6.164	/27	67.144.6.161	
Printer Lucani	200	67.144.7.242	/30	67.144.7.241	Printer for Lucani site
Printer Ljubis	200	67.144.7.238	/30	67.144.7.237	Printer for Ljubis site
Printer Mackat	200	67.144.7.246	/30	67.144.7.245	Printer for Mackat site
Printer Guca F2	200	67.144.7.234	/30	67.144.7.233	Printer for Guca site floor 2

## Phase 9: Configuring PPP and CHAP

PPP (Point-to-point protocol) is a layer 2 communication protocol commonly used between 2 routers without any hosts. Point-to-point Protocol will be used for connection authentication, transmission, encryption, and compression for data packets that would be sent between Mackat gateway and the ISP router. This is to make sure that no other external source can intercept the transmitting data packages within the internal network and resulting in the package and not being received by the 2<sup>nd</sup> router.

CHAP authentication scheme is specified for authenticating remote users connecting to networks or systems using PPP. CHAP's three-way handshake protocol provides strong protection against password guessing and eavesdropping attacks.

## Phase 10: Wireless LAN Deployment Site

The specifications for the company's network had specifically mentioned a wireless LAN deployment that would be running within the Mackat site. For the wireless LAN operation, we used a combination of wireless LAN wireless router set to an area coverage of 40m'. This ensures that the size of the Mackat site; stated at 125m x 40m, will be reasonably coated with a wireless local area network but not the whole site which is stated at 1250 x 2000m. The wireless routers used within the Mackat site are the AP-PT and the AP(Accesspoint)-PT-AC. The WRT 300N was selected to be used within the local area network as it holds the ability to function with dual band tech operating with 1-2.4GHz.

### Checking the possibility of deploying a LAN

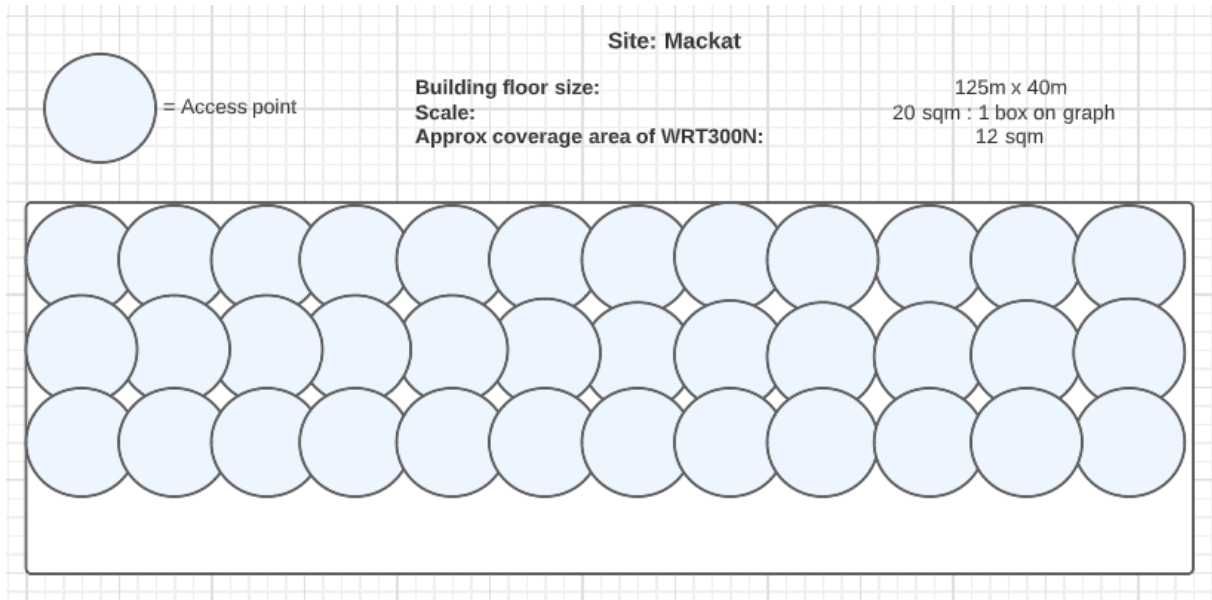
Area of site:  $1250\text{m} \times 2000\text{m} = 2500,000 \text{ m}^2$

Area of building:  $125 \times 40\text{m} = 5000\text{m}^2$

Assuming 1600 sqft (149sqm) per access point coverage, **No of Access points required: 34**

**Table F: Wireless Access Points Details**

Name	Model	SSID	Channel	Coverage area
Wireless Router2	WRT300N	11223344	1	149sqm



## Phase II: NAT Configuration

NAT (Network Address Translation) is a method of remapping and protecting a site's internal network IP address over a large area. This is performed by altering the network address information of a packet's IP address. The reason we implemented a NAT configuration on the gateway router at Mackat is so that the private IP network is allowed to be able to connect to the Internet (public network) which would be server0. The configured NAT also works in combination with an ACL that permits or denies hosts from the internal network to communicate with the internet. The provided NAT pool address is 147.9.0.0/21.

For this to be achieved, we took the number of remaining hosts provided by the NAT pool after assigning the addresses and divided them per VLAN according to their hosts requirements. After appointing a network address to each specific NAT pool corresponding to the sites VLAN, an ACL dedicated to this pool was developed to permit communication with each VLAN.

### 11.1 Static NAT Allocations:

Description	Source	Target
Server1	67.144.6.162	147.9.0.1
Server2	67.144.6.163	147.9.0.2
Server3	67.144.6.164	147.9.0.3

## 11.2 Dynamic NAT Pools:

Name	Source Network Address	Source Netmask	Target Range Start	Target Range End
mPOOLVLAN16	67.144.5.0	0.0.0.255	147.9.0.4	147.9.0.172
mPOOLVLAN10	67.144.7.176	0.0.0.15	147.9.0.173	147.9.0.179
mPOOLVLAN11	67.144.7.192	0.0.0.15	147.9.0.180	147.9.0.186
mPOOLVLAN12	67.144.7.208	0.0.0.15	147.9.0.187	147.9.0.193
mPOOLVLAN111	67.144.7.0	0.0.0.31	147.9.4.41	147.9.4.55
gPOOLVLAN15	67.144.0.0	0.0.1.255	147.9.0.194	147.9.1.208
gPOOLVLAN13	67.144.4.0	0.0.0.255	147.9.1.209	147.9.2.122
gPOOLVLAN111	67.144.6.128	0.0.0.31	147.9.4.56	147.9.4.75
gPOOLVLAN14	67.144.2.0	0.0.0.255	147.9.2.123	147.9.3.110
gPOOLVLAN10	67.144.7.32	0.0.0.15	147.9.3.111	147.9.3.117
gPOOLVLAN11	67.144.7.48	0.0.0.15	147.9.3.118	147.9.3.124
gPOOLVLAN12	67.144.7.64	0.0.0.15	147.9.3.125	147.9.3.131
luPOOLVLAN111	67.144.6.224	0.0.0.31	147.9.4.91	147.9.4.105
luPOOLVLAN16	67.144.3.0	0.0.0.255	147.9.4.5	147.9.4.19
luPOOLVLAN10	67.144.7.128	0.0.0.15	147.9.4.20	147.9.4.26
luPOOLVLAN11	67.144.7.144	0.0.0.15	147.9.4.27	147.9.4.33
luPOOLVLAN12	67.144.7.160	0.0.0.15	147.9.4.34	147.9.4.40
ljPOOLVLAN13	67.144.6.0	0.0.0.127	147.9.3.132	147.9.3.239
ljPOOLVLAN111	67.144.6.192	0.0.0.31	147.9.4.76	147.9.4.90
ljPOOLVLAN10	67.144.7.80	0.0.0.15	147.9.3.240	147.9.3.246
ljPOOLVLAN11	67.144.7.96	0.0.0.15	147.9.3.247	147.9.3.253
ljPOOLVLAN12	67.144.7.112	0.0.0.15	147.9.3.254	147.9.4.4

## 11.3 NAT ACL Binding Pool

We are assigning a particular range from the NAT pool to all VLANs by using this command:

```
ip nat pool mPOOLVLAN16 147.9.0.4 147.9.0.172 netmask 255.255.248.0
```

Next, we assigned access-control list to all the network addresses in the VLAN by using the command:

```
Ip access-list extended mACLVLAN16
Permit ip 67.144.5.0 0.0.0.255 any
```

And at the end, we are binding the ACL to the NAT Pool which is overloaded by using the command below. (NAT Overloading, also known as Port Address Translation (PAT) is designed to map multiple private IP addresses to a single public IP address (many-to-one) by using different ports)

```
Ip nat inside source list mACLVLAN16 pool mPOOLVLAN16 overload
```

## 11.4 NAT Statistics

```
MackatR1#sh ip nat statistics
Total translations: 3 (3 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/1/1
Inside Interfaces: Serial0/1/0 , Serial0/2/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list gACLVLAN10 pool gPOOLVLAN10 refCount 0
pool gPOOLVLAN10: netmask 255.255.248.0
start 147.9.3.111 end 147.9.3.117
type generic, total addresses 7 , allocated 0 (0%), misses 0
-- Inside Source
access-list gACLVLAN11 pool gPOOLVLAN11 refCount 0
pool gPOOLVLAN11: netmask 255.255.248.0
start 147.9.3.118 end 147.9.3.124
type generic, total addresses 7 , allocated 0 (0%), misses 0
-- Inside Source
access-list gACLVLAN111 pool gPOOLVLAN111 refCount 0
pool gPOOLVLAN111: netmask 255.255.248.0
start 147.9.4.56 end 147.9.4.75
type generic, total addresses 20 , allocated 0 (0%), misses 0
-- Inside Source
access-list gACLVLAN12 pool gPOOLVLAN12 refCount 0
pool gPOOLVLAN12: netmask 255.255.248.0
start 147.9.3.125 end 147.9.3.131
type generic, total addresses 7 , allocated 0 (0%), misses 0
-- Inside Source
access-list gACLVLAN13 pool gPOOLVLAN13 refCount 0
pool gPOOLVLAN13: netmask 255.255.248.0
```

## 11.5 NAT translations

```
MackatR1# sh ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 147.9.0.1 67.144.6.162 --- ---
--- 147.9.0.2 67.144.6.163 --- ---
--- 147.9.0.3 67.144.6.164 --- ---
```

## Phase 12: Access Control at Guca site

We have also implemented the use of Access Control Lists at the Guca Site. Access control is used as a system authentication so that traffic within the network is controlled. The reason why we have implemented access control lists at the Guca site is because Guca is the largest site in our network and major amounts of business data is being constantly sent to Guca. With implementing an Access Control List at Guca, the network checks what data packets enter the site, and if the data packets might be from an external source, and it can either denies or permits the request depending on the permissions outlined in the table given below.

The same rules can be implemented on other sites as well according to company's requirements.

GUCA - Access Control List	
<b>Server Farm 1 Server Farm 2 ACL</b>	ip access-list extended ACLVLAN15 remark Deny HTTP access to server1 and permit server2 access from Business VLAN15 deny tcp 67.144.0.0 0.0.1.255 host 67.144.6.162 eq www permit tcp 67.144.0.0 0.0.1.255 host 67.144.6.163 eq www deny ip 67.144.0.0 0.0.1.255 host 67.144.6.163 permit ip any any
<b>Server Farm 3</b>	ip access-list extended ACLVLAN10 remark Permit HTTP access to server3 and deny tcp access server1 and no access to server2 from Security VLAN10 deny tcp 67.144.7.32 0.0.0.15 host 67.144.6.162 eq www deny ip 67.144.7.32 0.0.0.15 host 67.144.6.163 permit tcp 67.144.7.32 0.0.0.15 host 67.144.6.164 eq www permit ip any any
<b>PC host on Marketing VLAN denied access to Leasing VLAN</b>	ip access-list extended ACLVLAN14 remark Marketing denied access to leasing permit icmp 67.144.2.0 0.0.0.255 67.144.4.0 0.0.0.255 echo-reply deny icmp 67.144.2.0 0.0.0.255 67.144.4.0 0.0.0.255 permit ip any any
<b>PCs in Vehicle VLAN denied access to all other VLANs</b>	ip access-list extended ACLVLAN12 remark Vehicle Services Denied access to Other vlans permit icmp 67.144.7.64 0.0.0.15 67.144.0.0 0.0.1.255 echo-reply permit icmp 67.144.7.64 0.0.0.15 67.144.4.0 0.0.0.255 echo-reply permit icmp 67.144.7.64 0.0.0.15 67.144.2.0 0.0.0.255 echo-reply permit icmp 67.144.7.64 0.0.0.15 67.144.6.128 0.0.0.31 echo-reply permit icmp 67.144.7.64 0.0.0.15 67.144.7.232 0.0.0.3 echo-reply permit icmp 67.144.7.64 0.0.0.15 67.144.7.32 0.0.0.15 echo-reply permit icmp 67.144.7.64 0.0.0.15 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.7.64 0.0.0.15 67.144.0.0 0.0.1.255 deny icmp 67.144.7.64 0.0.0.15 67.144.4.0 0.0.0.255 deny icmp 67.144.7.64 0.0.0.15 67.144.2.0 0.0.0.255 deny icmp 67.144.7.64 0.0.0.15 67.144.6.128 0.0.0.31 deny icmp 67.144.7.64 0.0.0.15 67.144.7.232 0.0.0.3 deny icmp 67.144.7.64 0.0.0.15 67.144.7.32 0.0.0.15 deny icmp 67.144.7.64 0.0.0.15 67.144.7.48 0.0.0.15 permit ip any any

<b>All other VLANs denied access to Technical Support VLAN</b>	<pre> ip access-list extended ACLVLAN11 remark All other Vlans denied access to Tech Support permit icmp 67.144.0.0 0.0.1.255 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.0.0 0.0.1.255 67.144.7.48 0.0.0.15 permit icmp 67.144.4.0 0.0.0.255 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.4.0 0.0.0.255 67.144.7.48 0.0.0.15 permit icmp 67.144.6.128 0.0.0.15 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.6.128 0.0.0.15 67.144.7.48 0.0.0.15 permit icmp 67.144.2.0 0.0.0.255 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.2.0 0.0.0.255 67.144.7.48 0.0.0.15 permit icmp 67.144.7.232 0.0.0.3 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.7.232 0.0.0.3 67.144.7.48 0.0.0.15 permit icmp 67.144.7.32 0.0.0.15 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.7.32 0.0.0.15 67.144.7.48 0.0.0.15 permit icmp 67.144.7.64 0.0.0.15 67.144.7.48 0.0.0.15 echo-reply deny icmp 67.144.7.64 0.0.0.15 67.144.7.48 0.0.0.15 permit ip any any </pre>
--	--

The ACL rules active in Guca are operating in two-way: from a source to a destination host. This is mainly due to the initiated traffic from any of the set VLANS being denied a service by an ACL configuration. With these rules in place, the source host or the destination will be gridlocked depending on the location of the distribution side. The IP traffic will flow across a connected interface if a 'Permit IP any any' statement has been placed in an access-list; granted that it hasn't been given any previous rules during its configuration. Examples of these commands can be seen in the table above.

We have also tested our ACL configurations and provided results in the table G below.

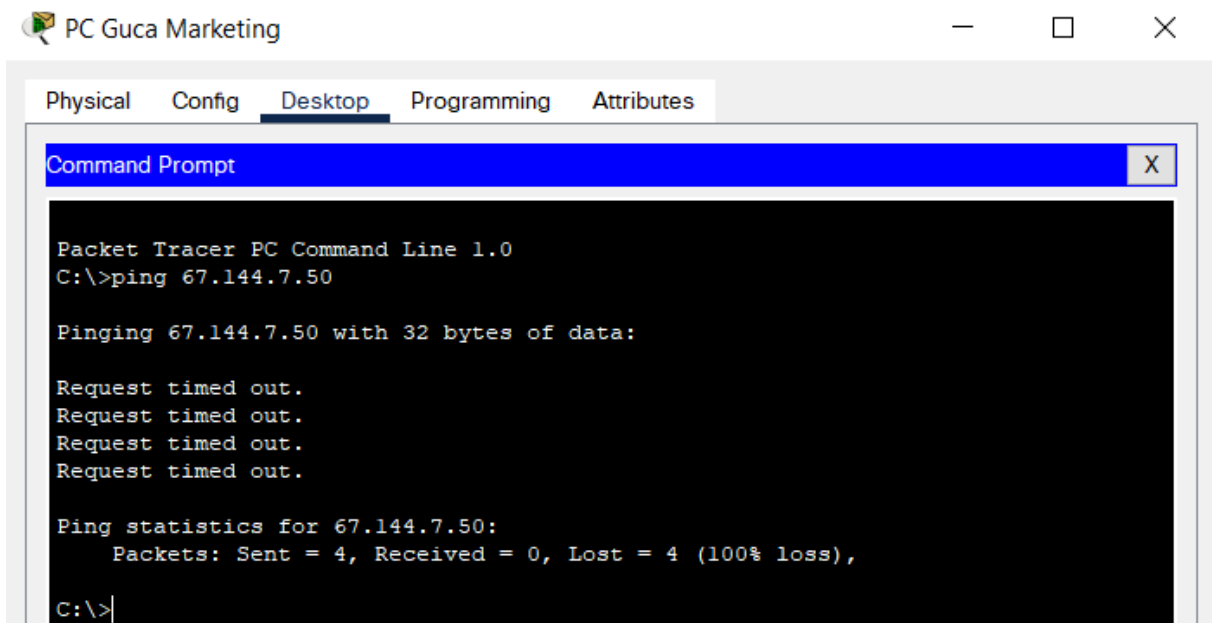
**Table G: Record of ACL Testing Guca**

Source Host	Destination Host/Server	Protocol	Expected Results	Correct
PC Guca Business	Server1	HTTP	Denied	Yes
PC Guca Business	Server2	HTTP	Permitted	Yes
PC Guca Business	Server 2	IP	Denied	Yes
PC Guca Security	Server 1	HTTP	Denied	Yes
PC Guca Security	Server2	IP	Denied	Yes
PC Guca Security	Server3	HTTP	Permitted	Yes
PC Guca Marketing	PC Guca Leasing	ICMP	Denied	Yes
PC Guca Vehicle	PC Guca Business	ICMP	Denied	Yes
PC Guca Vehicle	PC Guca Leasing	ICMP	Denied	Yes
PC Guca Vehicle	PC Guca Management	ICMP	Denied	Yes

<b>PC Guca Vehicle</b>	PC Guca Marketing	ICMP	Denied	Yes
<b>PC Guca Vehicle</b>	PC Guca Security	ICMP	Denied	Yes
<b>PC Guca Vehicle</b>	PC Guca Technical	ICMP	Denied	Yes
<b>PC Guca Vehicle</b>	Server1	ICMP	Denied	Yes
<b>PC Guca Business</b>	PC Guca Technical	ICMP	Denied	Yes
<b>PC Guca Leasing</b>	PC Guca Technical	ICMP	Denied	Yes
<b>PC Guca Management</b>	PC Guca Technical	ICMP	Denied	Yes
<b>PC Guca Marketing</b>	PC Guca Technical	ICMP	Denied	Yes
<b>PC Guca Security</b>	PC Guca Technical	ICMP	Denied	Yes
<b>PC Guca Vehicle</b>	PC Guca Technical	ICMP	Denied	Yes
<b>Server1</b>	PC Guca Technical	ICMP	Denied	Yes

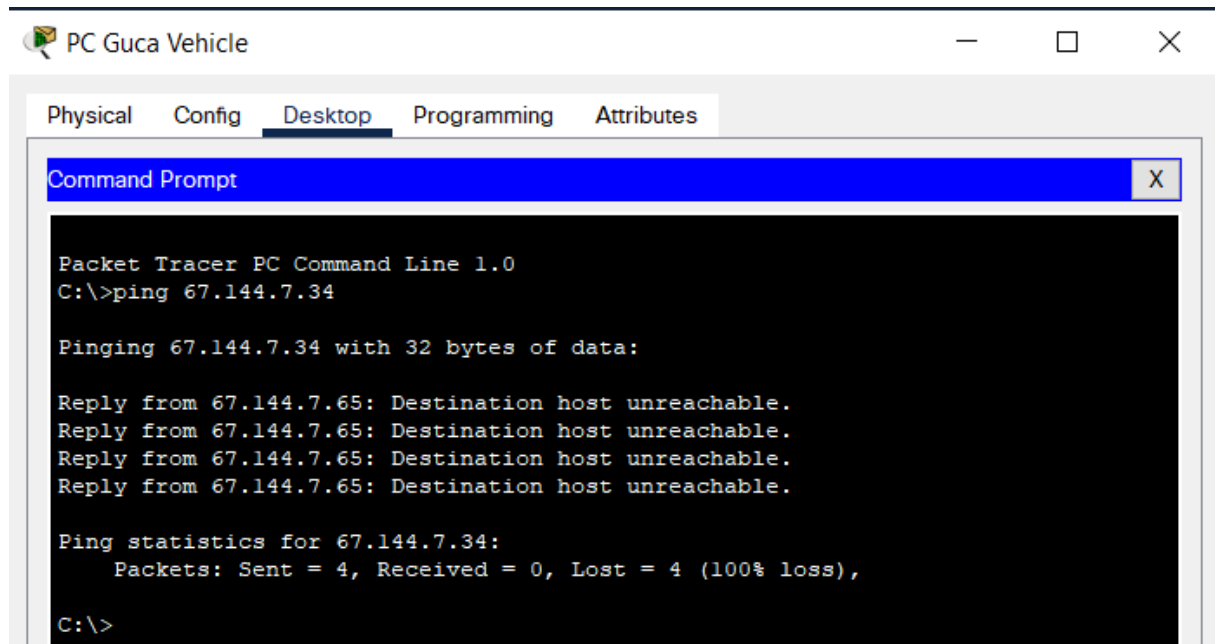
## 12.1 All VLANs denied access to Technical support

E.g.- Marketing to Technical:

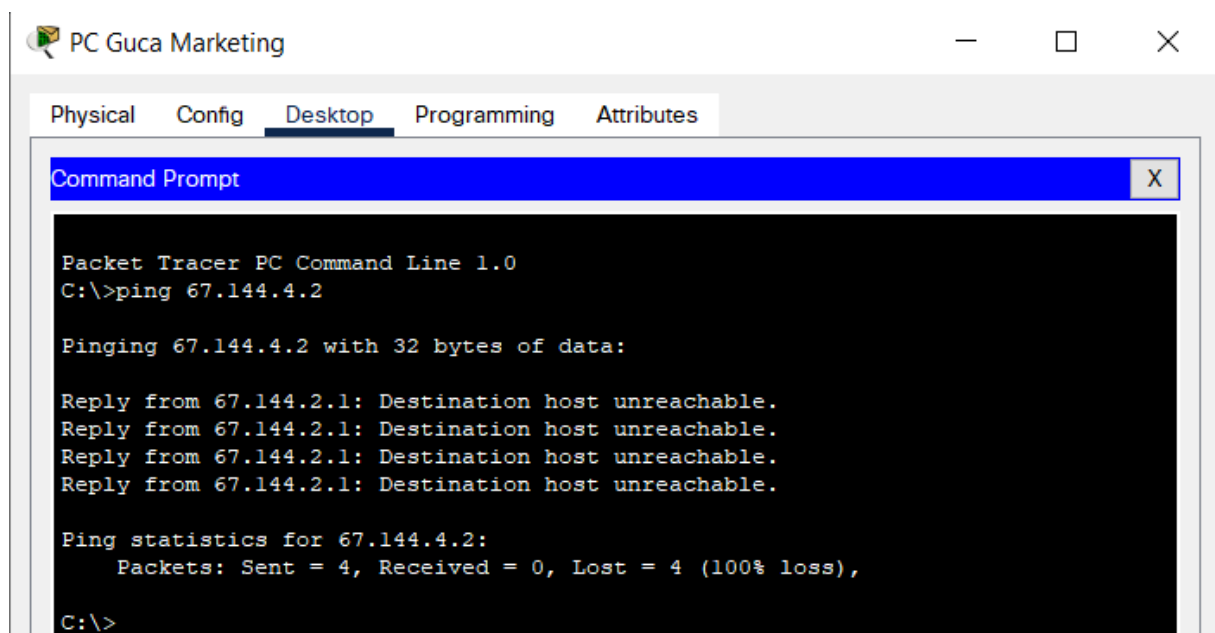


## 12.2 Vehicle VLAN denied access to all VLANs

E.g. – Vehicle to Security

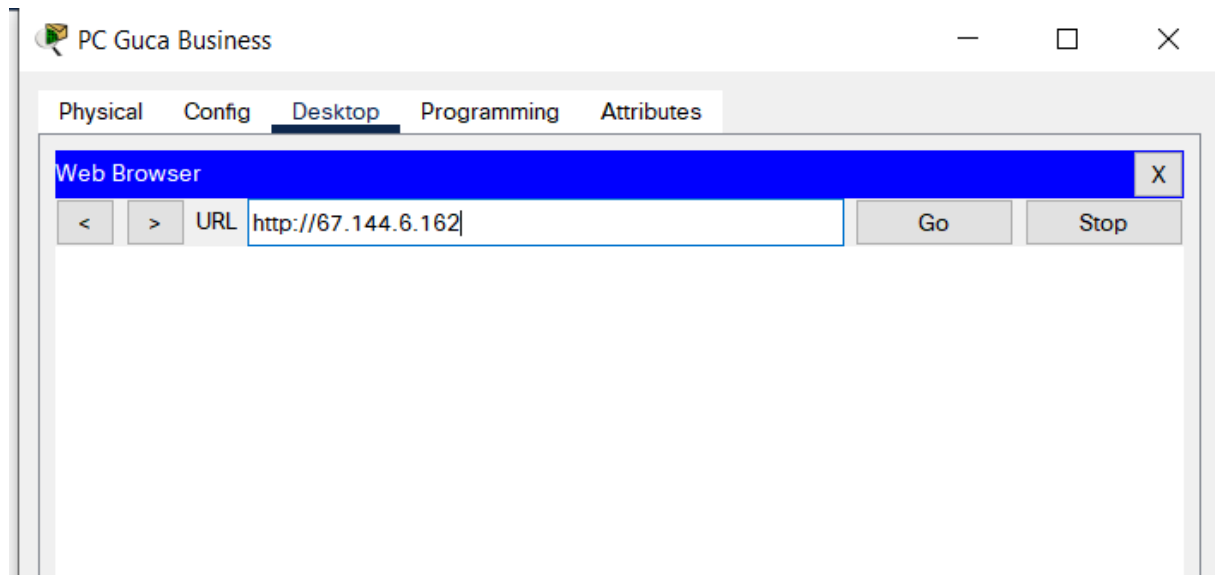


## 12.3 Marketing VLAN denied access to Leasing VLAN





## 12.4 HTTP access denied to server 1 from Business VLAN



## System testing and verification strategy

The following steps have been taken to test and verify the strategies implemented:

1. Configured switches and necessary VLANs – Verified using *sh vlan brief*, *sh run*
2. Ether channel – We have implemented LACP ether channel only at the Lucani site. We test and verify this by using *"sh ether channel"* and *"sh ether channel summary"*
3. We have implemented OSPF as the routing protocol across the whole network. The commands used to verify this are *"sh ip route"*, *"sh ip ospf neighbor"*, and *"sh run"*
4. Configuring IP Addresses for the network - When configuring IP addresses, we implemented DHCP only at the Ljubis site whereas, the rest of the sites were manually given an IP address. The commands to test these are, *"sh ip interface brief"*, *"sh run"*, and *"sh ip dhcp pool"*
5. NAT configurations – For this, we verified it using the *"sh ip nat translations"*, *"sh ip nat statistics"* and *"sh run"*
6. According to the case study, we implemented ACL only in the Guca site. Before implementing ACL, we checked the connectivity of the network. We tested that the PCs could ping each other, can browse, can ping the internet web server and all other VLANs. The records of ACL testing are shown in Table G.