Case study report

TNE20002

Group 7

Parth Tyagi
Drishti Kapoor
Yashvi Chaudhary
Ting Pong Wan

Table of Contents

Team Case Study

ESP team: TNE20002_A01_T007
Lab Class: Tuesday 14:30 ACT 328
Class Tutor: Subrata Tran

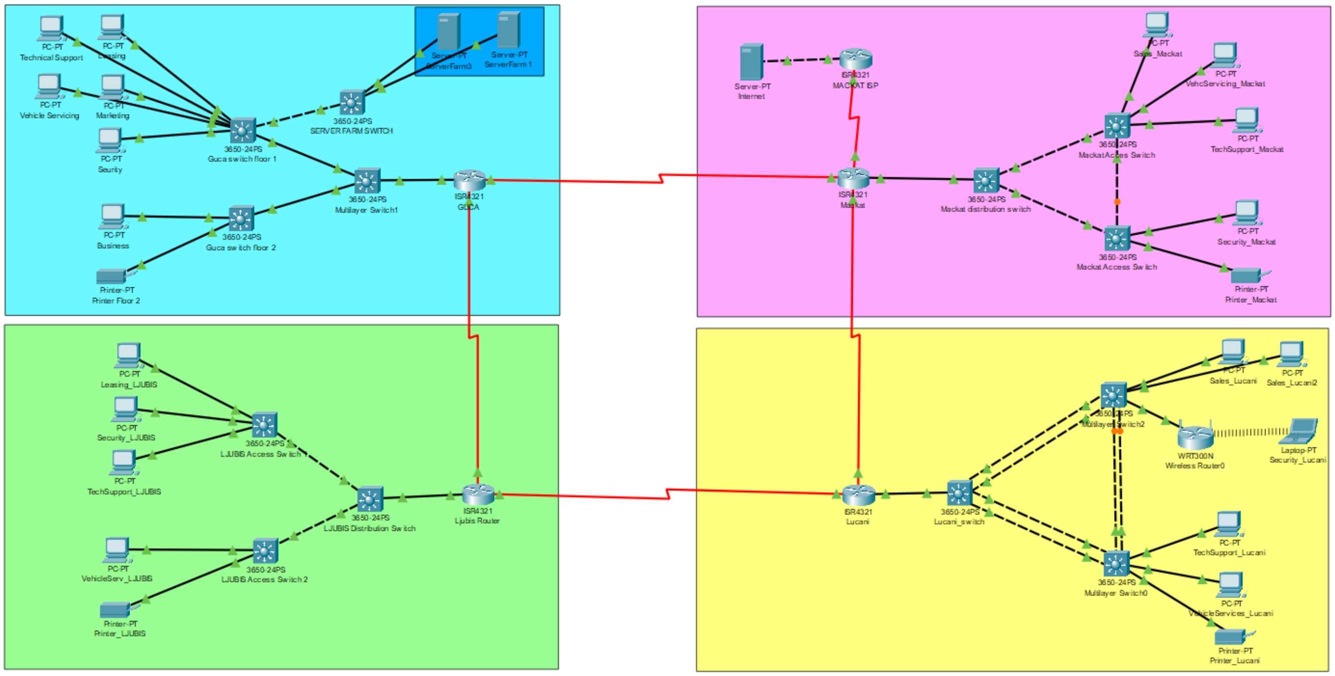
Team Members
103143089 Parth Tyagi
103168671 Drishti Kapoor
103174005 Yashvi Chaudhary
103509034 Ting Pong Wan

Specification Information

Specification Number	2.8
Class A Internal network address	67.128.0.0/17
Class B NAT pool public address	147.8.0.0/20
Class C ISP network connection address	213.2.8.0/30
Class B ISP Internet Web server address	147.23.2.0/30
Wireless Deployment Site	Lucani
Management VLAN Number	99
Percentage Growth (VLSM)	30

Network Topology

In our case study, we have created a prototype of what the network topology of a large company like BestMotors Ltd would look like. In real-life scenario, there would be a greater number of access switches because according to our requirements we need to accommodate much large number of hosts. So, we would need more access switches than provided in our implementation where we used just 2 switches to represent the scenario because this is a prototype. Similarly, we would have a greater number of servers in the server farm and more printers at each site.



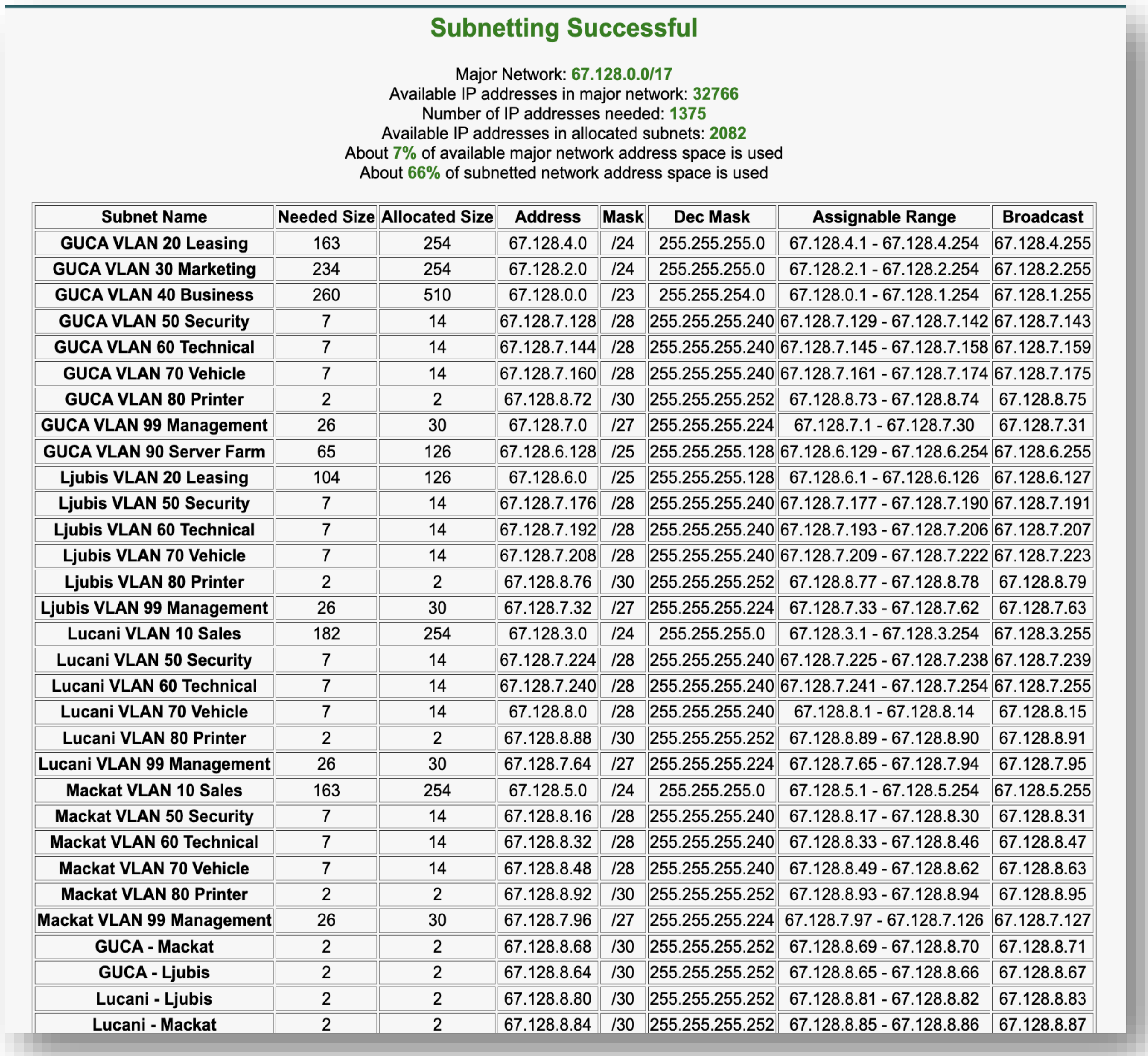
IP VLSM Design

In the case study, we were required to subnet a given network to meet the needs of the company Best Motors Ltd which leases, buys and sells and repairs cars, trucks and buses. The company currently has four sites - Guca, Ljubis, Lucani and Mackat. The head office is located at the Guca site.

VLSM - Variable length subnet mask allows all subnet masks to have variable sizes. The VLSM will split across sites according to the total number of hosts needed for the different work groups located in each site for making up different VLANs. With VLSM we can decrease the number of host addresses which would otherwise have been wasted.

The hierarchy structure will look like: Major network > Site > Work groups.

We have been given class A internal network and the number of hosts in that is 1,048,574. However, the total number of hosts we require in our case study is 1375 (adding all our hosts). Using VLSM, we subnet the major network into different groups as per the host requirement and hence the rest range of the IP addresses do not go waste.



Subnetting Successful

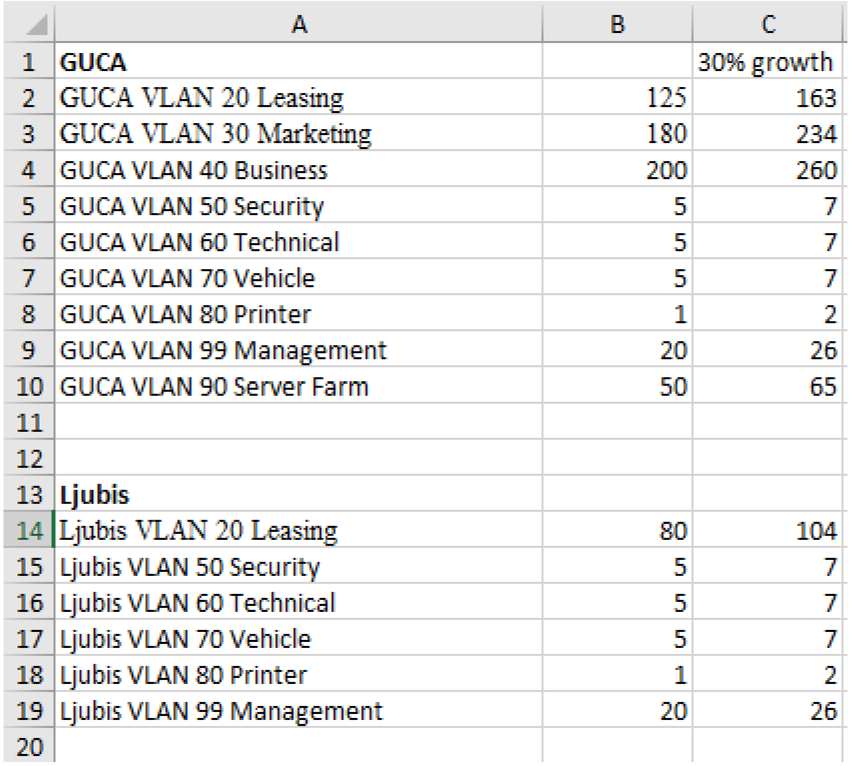
Major Network: 67.128.0.0/17
Available IP addresses in major network: 32766
Number of IP addresses needed: 1375
Available IP addresses in allocated subnets: 2082
About 7% of available major network address space is used
About 66% of subnetted network address space is used

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
GUCA VLAN 20 Leasing	163	254	67.128.4.0	/24	255.255.255.0	67.128.4.1 - 67.128.4.254	67.128.4.255
GUCA VLAN 30 Marketing	234	254	67.128.2.0	/24	255.255.255.0	67.128.2.1 - 67.128.2.254	67.128.2.255
GUCA VLAN 40 Business	260	510	67.128.0.0	/23	255.255.254.0	67.128.0.1 - 67.128.1.254	67.128.1.255
GUCA VLAN 50 Security	7	14	67.128.7.128	/28	255.255.255.240	67.128.7.129 - 67.128.7.142	67.128.7.143
GUCA VLAN 60 Technical	7	14	67.128.7.144	/28	255.255.255.240	67.128.7.145 - 67.128.7.158	67.128.7.159
GUCA VLAN 70 Vehicle	7	14	67.128.7.160	/28	255.255.255.240	67.128.7.161 - 67.128.7.174	67.128.7.175
GUCA VLAN 80 Printer	2	2	67.128.8.72	/30	255.255.255.252	67.128.8.73 - 67.128.8.74	67.128.8.75
GUCA VLAN 99 Management	26	30	67.128.7.0	/27	255.255.255.224	67.128.7.1 - 67.128.7.30	67.128.7.31
GUCA VLAN 90 Server Farm	65	126	67.128.6.128	/25	255.255.255.128	67.128.6.129 - 67.128.6.254	67.128.6.255
Ljubis VLAN 20 Leasing	104	126	67.128.6.0	/25	255.255.255.128	67.128.6.1 - 67.128.6.126	67.128.6.127
Ljubis VLAN 50 Security	7	14	67.128.7.176	/28	255.255.255.240	67.128.7.177 - 67.128.7.190	67.128.7.191
Ljubis VLAN 60 Technical	7	14	67.128.7.192	/28	255.255.255.240	67.128.7.193 - 67.128.7.206	67.128.7.207
Ljubis VLAN 70 Vehicle	7	14	67.128.7.208	/28	255.255.255.240	67.128.7.209 - 67.128.7.222	67.128.7.223
Ljubis VLAN 80 Printer	2	2	67.128.8.76	/30	255.255.255.252	67.128.8.77 - 67.128.8.78	67.128.8.79
Ljubis VLAN 99 Management	26	30	67.128.7.32	/27	255.255.255.224	67.128.7.33 - 67.128.7.62	67.128.7.63
Lucani VLAN 10 Sales	182	254	67.128.3.0	/24	255.255.255.0	67.128.3.1 - 67.128.3.254	67.128.3.255
Lucani VLAN 50 Security	7	14	67.128.7.224	/28	255.255.255.240	67.128.7.225 - 67.128.7.238	67.128.7.239
Lucani VLAN 60 Technical	7	14	67.128.7.240	/28	255.255.255.240	67.128.7.241 - 67.128.7.254	67.128.7.255
Lucani VLAN 70 Vehicle	7	14	67.128.8.0	/28	255.255.255.240	67.128.8.1 - 67.128.8.14	67.128.8.15
Lucani VLAN 80 Printer	2	2	67.128.8.88	/30	255.255.255.252	67.128.8.89 - 67.128.8.90	67.128.8.91
Lucani VLAN 99 Management	26	30	67.128.7.64	/27	255.255.255.224	67.128.7.65 - 67.128.7.94	67.128.7.95
Mackat VLAN 10 Sales	163	254	67.128.5.0	/24	255.255.255.0	67.128.5.1 - 67.128.5.254	67.128.5.255
Mackat VLAN 50 Security	7	14	67.128.8.16	/28	255.255.255.240	67.128.8.17 - 67.128.8.30	67.128.8.31
Mackat VLAN 60 Technical	7	14	67.128.8.32	/28	255.255.255.240	67.128.8.33 - 67.128.8.46	67.128.8.47
Mackat VLAN 70 Vehicle	7	14	67.128.8.48	/28	255.255.255.240	67.128.8.49 - 67.128.8.62	67.128.8.63
Mackat VLAN 80 Printer	2	2	67.128.8.92	/30	255.255.255.252	67.128.8.93 - 67.128.8.94	67.128.8.95
Mackat VLAN 99 Management	26	30	67.128.7.96	/27	255.255.255.224	67.128.7.97 - 67.128.7.126	67.128.7.127
GUCA - Mackat	2	2	67.128.8.68	/30	255.255.255.252	67.128.8.69 - 67.128.8.70	67.128.8.71
GUCA - Ljubis	2	2	67.128.8.64	/30	255.255.255.252	67.128.8.65 - 67.128.8.66	67.128.8.67
Lucani - Ljubis	2	2	67.128.8.80	/30	255.255.255.252	67.128.8.81 - 67.128.8.82	67.128.8.83
Lucani - Mackat	2	2	67.128.8.84	/30	255.255.255.252	67.128.8.85 - 67.128.8.86	67.128.8.87

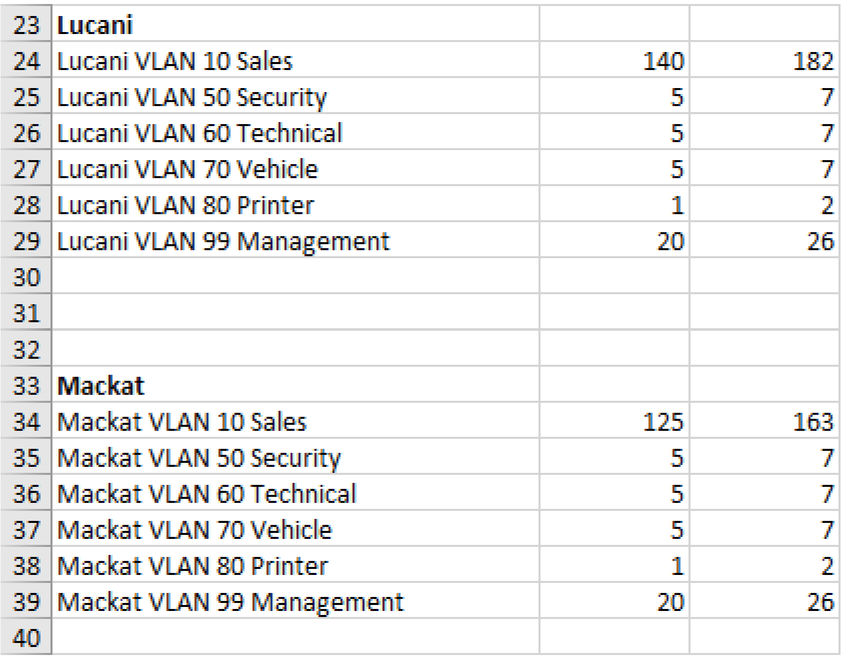
A 30% extra space was given to every subnet to match the expected growth for the company. Thus, the needed size is the sum of the original hosts required for that workgroup and the 30% expected growth.For example: in Guca VLAN20 Leasing, require number of hosts were 125+ 30% of 125 = 163
Thus, the IP Address range that is reserved for future use is : 67.128.4.164 - 67.128.4.254 .

Similarly, we have IP Addresses ranges reserved for future use in every subnet for each site.

The following tables show the required number of hosts after considering the 30% growth :-



	A	B	C
1	**GUCA**		30% growth
2	GUCA VLAN 20 Leasing	125	163
3	GUCA VLAN 30 Marketing	180	234
4	GUCA VLAN 40 Business	200	260
5	GUCA VLAN 50 Security	5	7
6	GUCA VLAN 60 Technical	5	7
7	GUCA VLAN 70 Vehicle	5	7
8	GUCA VLAN 80 Printer	1	2
9	GUCA VLAN 99 Management	20	26
10	GUCA VLAN 90 Server Farm	50	65
11			
12			
13	**Ljubis**		
14	Ljubis VLAN 20 Leasing	80	104
15	Ljubis VLAN 50 Security	5	7
16	Ljubis VLAN 60 Technical	5	7
17	Ljubis VLAN 70 Vehicle	5	7
18	Ljubis VLAN 80 Printer	1	2
19	Ljubis VLAN 99 Management	20	26
20			



23	**Lucani**		
24	Lucani VLAN 10 Sales	140	182
25	Lucani VLAN 50 Security	5	7
26	Lucani VLAN 60 Technical	5	7
27	Lucani VLAN 70 Vehicle	5	7
28	Lucani VLAN 80 Printer	1	2
29	Lucani VLAN 99 Management	20	26
30			
31			
32			
33	**Mackat**		
34	Mackat VLAN 10 Sales	125	163
35	Mackat VLAN 50 Security	5	7
36	Mackat VLAN 60 Technical	5	7
37	Mackat VLAN 70 Vehicle	5	7
38	Mackat VLAN 80 Printer	1	2
39	Mackat VLAN 99 Management	20	26
40			

We have assumed management VLAN will need 26 hosts in every site. For printer VLAN, we allow 2 hosts as per requirement. The server farm will have its own space in the VLSM design. 2 hosts per serial link between different sites have been allocated. For more information, please refer to [Table A: VLSM Design]

Routing Protocols

Routing protocols are a set of protocols that define how different routers, in order to distribute information to determine the best path to transfer packets from source to destination node (known as routing) by exchanging and updating their routing tables. There are different types of routing protocols like RIP, EIGRP, OSPF.

Open Shortest Path First *(OSPF)* is a link-state routing protocol which is selected as the routing protocol in our case study. OSPF offers faster convergence and scales to much larger network implementations.
Bandwidth of all internal router serial links were set to 256 KB as per the requirement. Passive interfaces were configured to disable sending updates (Hello packets) out of those interfaces, although OSPF continues to announce or advertise the interface's connected network.
By configuring passive interfaces, we reduce the number of devices that interact which in turn reduces the load on the CPU.

OSPF MD5 authentication uses MD5 algorithm to generate a hash value for every OSPF packet's content and password. This hash value is sent in the packet. The receiver on the other end who knows the same password, calculates its own hash value. If the hash value matches, it means that there is no change in the contents of the packet and the message has been unchanged. This method provides more security. All OSPF MD5 authentication is implemented between the link of *Guca* and *Mackat* to enhance data integrity. No unauthorized IP can successfully send hoax OSPF routing messages into the network.

A default route is the route to which the router forwards the incoming packet when no other route is available to forward that packet after looking at the routing table. A default static route to *Mackat ISP* has been configured. Therefore, for every packet that arrives at the router but does not have a matching entry in the routing table, it will be forwarded to the Mackat ISP instead of being dropped. Then, this default route was also advertised to the internal routers. Router settings are documented in [Table C: Router Details]

Switches: VLANs, STP, EtherChannel

VLANs

VLAN stands for **Virtual Local Area Network**. This enables devices from one or more networks to combine into a single logical network. Implementing VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases.
In our scenario, VLANs are created based on work groups present at each site to enhance access control. The same work group shares the same VLAN number regardless of the site it resides in for easier management. For example, the VLAN number of the Security workgroup is 50 in every single site of the company. [Table B: Switch Details]

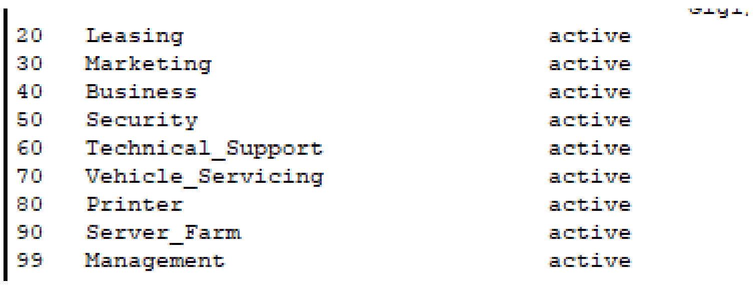
VLAN 99 is configured as the *management VLAN* on all the sites instead of using the default management VLAN 1 as it is a good practice to have management VLAN separate from the native one. The VLAN number will be matching the router sub-interface number for easy management.

All the unused ports are shutdown. This ensures security in case some attacker tries to plug a device into the unused port to access the network. This good practice prevents the network from being vulnerable to the outsiders.

The access switch ports on the *Ljubis* site have been configured with port security - *violation mode protect* and *mac address sticky*. When a violation occurs in protect mode, switchport will drop the traffic from unknown MAC addresses but continue to send traffic from the known ones. Sticky mode ensures that the MAC addresses are learnt dynamically from the connected devices and are put into the running configuration like static addresses. This way only packets whose MAC address match would be forwarded; other packets would be restricted. Router sub-interface settings are documented in [Table C: Router Details]

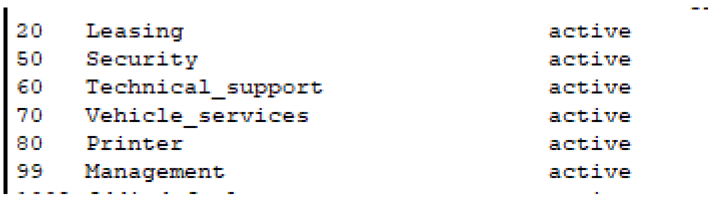
Each of the sites are provided with the VLANs required:

Guca VLANs



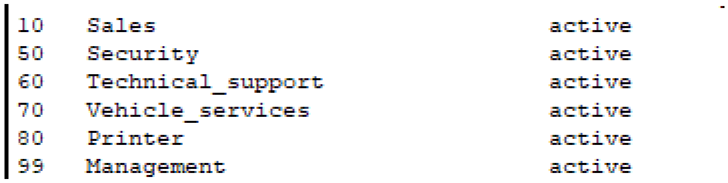
```
20   Leasing                          active
30   Marketing                        active
40   Business                         active
50   Security                         active
60   Technical_Support                active
70   Vehicle_Servicing                active
80   Printer                          active
90   Server_Farm                      active
99   Management                       active
```

Ljubis VLANs



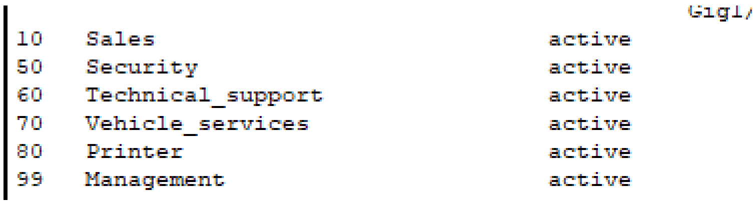
```
20   Leasing                          active
50   Security                         active
60   Technical_support                active
70   Vehicle_services                 active
80   Printer                          active
99   Management                       active
```

Lucani VLANs



```
10   Sales                            active
50   Security                         active
60   Technical_support                active
70   Vehicle_services                 active
80   Printer                          active
99   Management                       active
```

Mackat VLANs



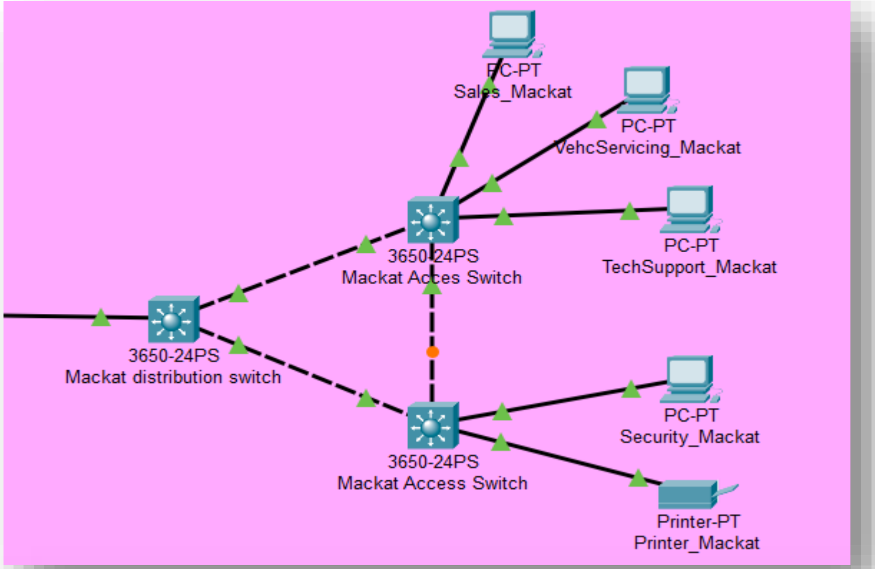
```
                                                Gig1/
10   Sales                            active
50   Security                         active
60   Technical_support                active
70   Vehicle_services                 active
80   Printer                          active
99   Management                       active
```

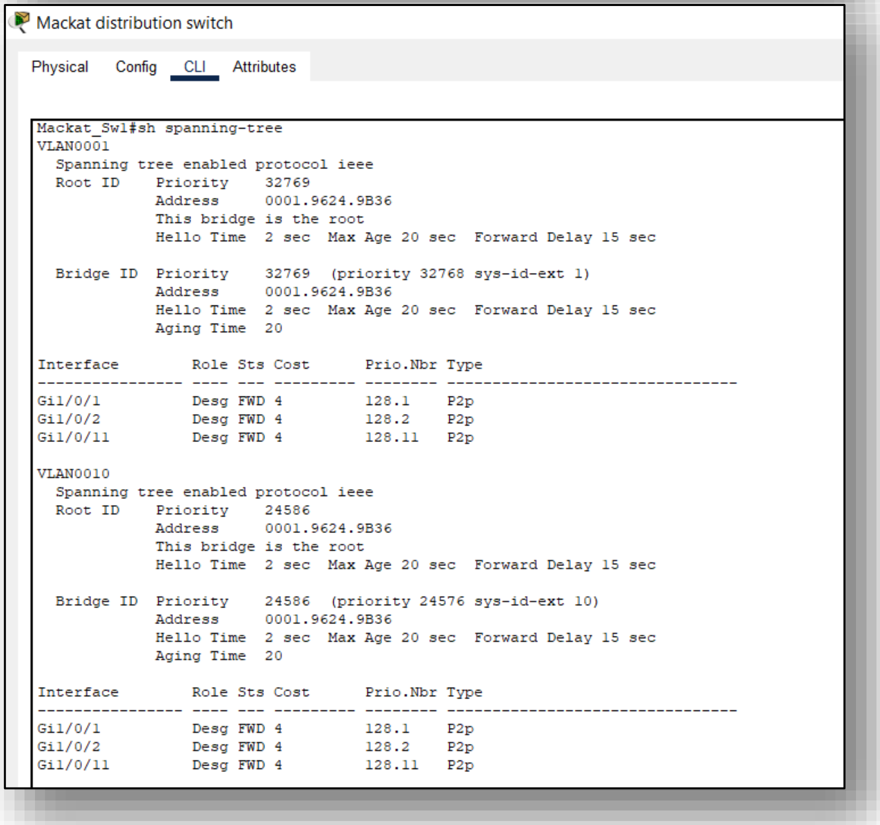
Details of switches are in [Table B: Switch Details]

STP

Having redundant paths in a switched ethernet network can cause layer 2 loops which causes broadcast, multicast, and unknown unicast frames to loop endlessly. When this occurs, switches keep on updating their MAC address tables which leads to MAC address table instability. It also causes broadcast storms which can disable the network in seconds. *Spanning Tree Protocol* (STP) is a loop prevention protocol that helps us maintain redundancy along with loop-free layer 2 topology. It has been implemented in the *Mackat* site as per the requirement. There are three switches in Mackat. The switch that is directly connected to the router is configured as a root bridge in the distribution layer (distribution switch). The other two switches act as switches in the access layer (access switches).

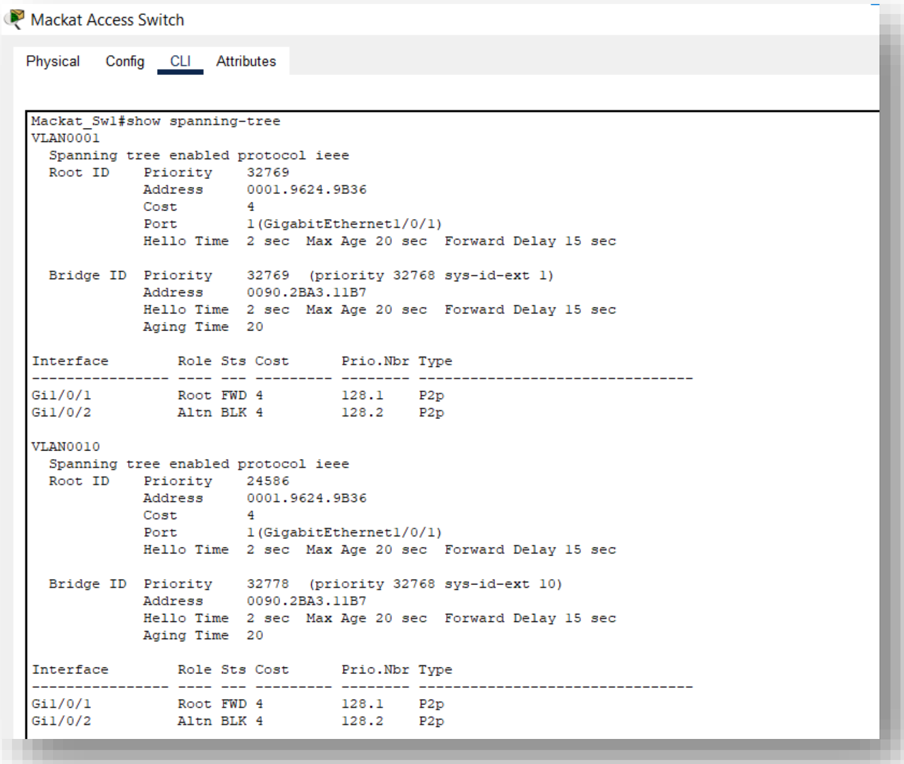
This is a part of the Mackat site where the STP has been applied. The Mackat distribution switch is the root bridge for all the VLANS. We can verify it by viewing the show spanning-tree command in CLI. It says *"This bridge is the root"*





```
Mackat_Sw1#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9624.9B36
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0001.9624.9B36
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/11         Desg FWD 4         128.11   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0001.9624.9B36
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24586  (priority 24576 sys-id-ext 10)
             Address     0001.9624.9B36
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Desg FWD 4         128.2    P2p
Gi1/0/11         Desg FWD 4         128.11   P2p
```

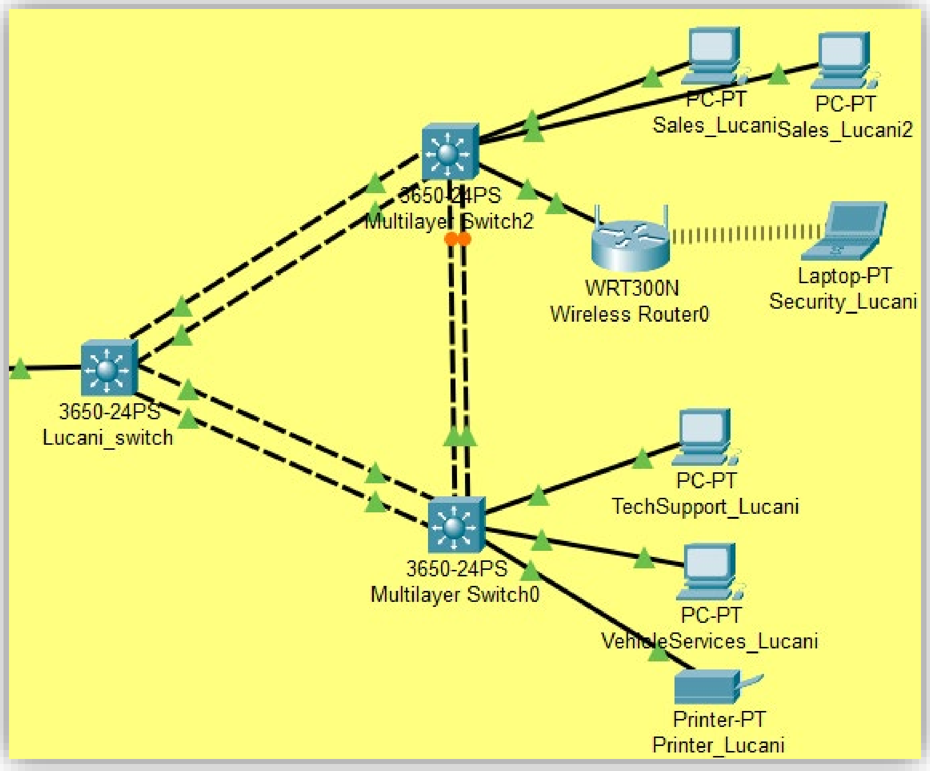
The access switch that is below in the image *(Mackat_Sw1)* has one of its ports in the blocking state. Refer to the screenshot below which is what is displayed when we view the spanning-tree in the CLI of that switch.
In this way, even if one of the links fail, network traffic will still reach the destination.

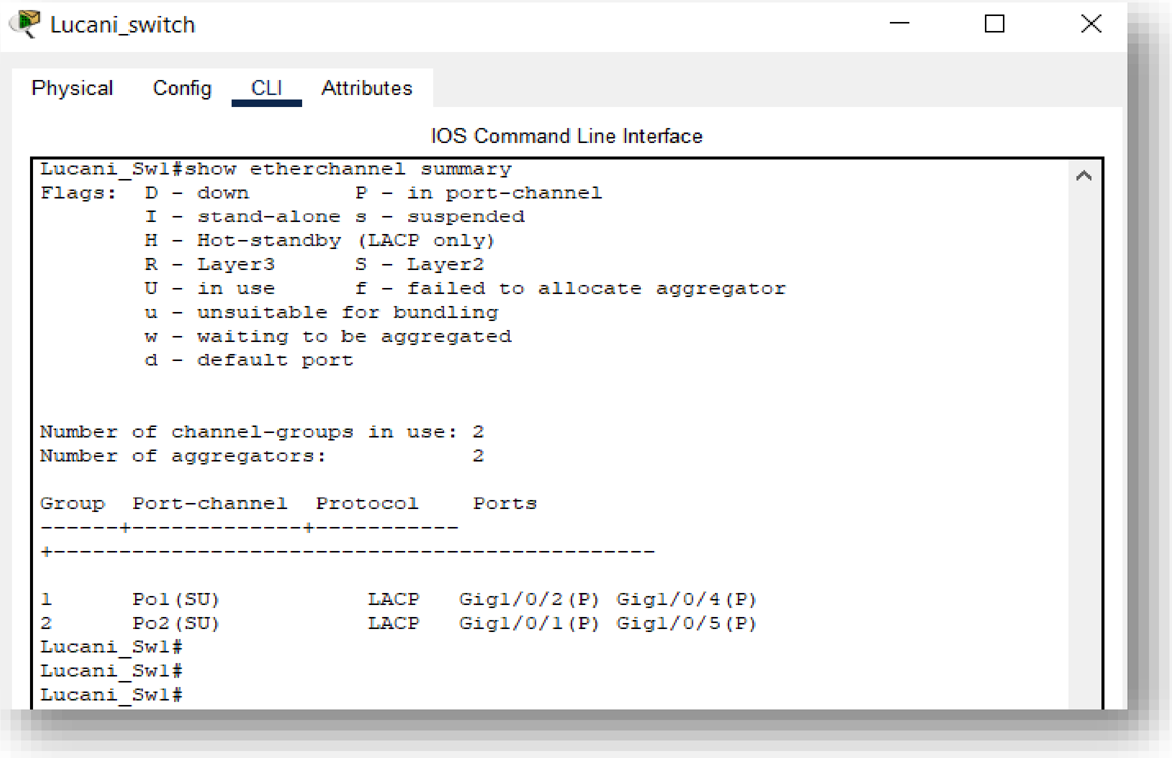


```
Mackat_Sw1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9624.9B36
             Cost        4
             Port        1(GigabitEthernet1/0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0090.2BA3.11B7
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Root FWD 4         128.1    P2p
Gi1/0/2          Altn BLK 4         128.2    P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    24586
             Address     0001.9624.9B36
             Cost        4
             Port        1(GigabitEthernet1/0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0090.2BA3.11B7
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/1          Root FWD 4         128.1    P2p
Gi1/0/2          Altn BLK 4         128.2    P2p
```

EtherChannel

EtherChannel is a link aggregation technology that groups together multiple physical ethernet links into one single logical link. It helps to provide more bandwidth, increase redundancy and provide fault tolerance between devices. It is implemented using *Link Aggregation Control Protocol (LACP)* in site *Lucani*. It is implemented between the 2 switches in the access layer as well as between switches in the access layer to the switch in the distribution layer by bundling together the 2 physical links into one logical link between each pair. If one of the links goes down, the other link will be used.





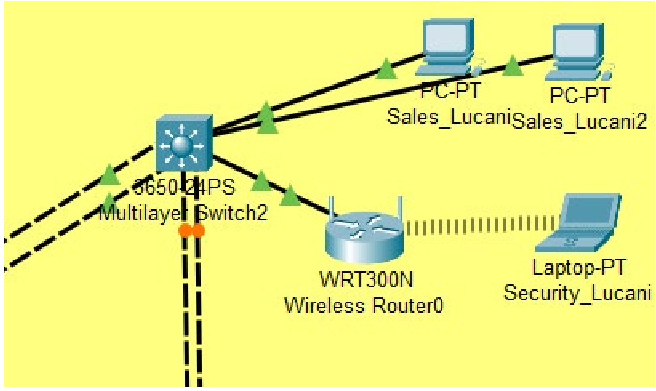
```
Lucani_Sw1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+----------------------------------------------

1      Po1(SU)           LACP   Gig1/0/2(P) Gig1/0/4(P)
2      Po2(SU)           LACP   Gig1/0/1(P) Gig1/0/5(P)
Lucani_Sw1#
Lucani_Sw1#
Lucani_Sw1#
```

On viewing the *etherchannel summary*, we observe that ports Gig1/0/2 and Gig1/0/4 have been bundled together in group 1 with *LACP* protocol and Gig1/0/1 and Gig1/0/5 in group2

Wireless LANs and Site layout for the specified site

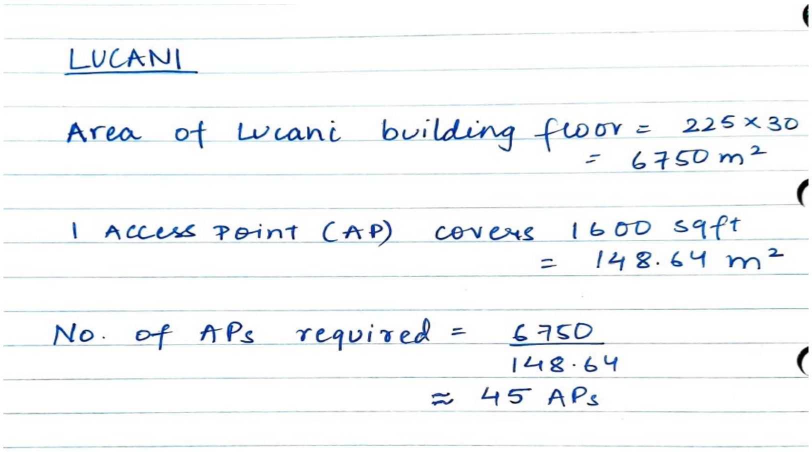
Wireless LANs

In the scenario, Lucani was selected as the wireless deployment site. We have configured a wireless access point with the details documented in [Table F: Wireless Access Point Details]. The said access point resides in the Lucani Security VLAN configured with a static IP address for simple IP address management. In the prototype, we have put a Security group laptop to test and demonstrate the wireless connection between the access point and the Security group.



Site layout for the specified site

Let's assume our ideal wireless coverage is 75%. With the chosen wireless access point model – WRT300N, it will need around 44 - 45 access point to cover the building floor in Lucani. Image below is our calculation for the number of access-points that would be required in the real-scenario to provide access to the security group. [Table F: Wireless Access Point details]

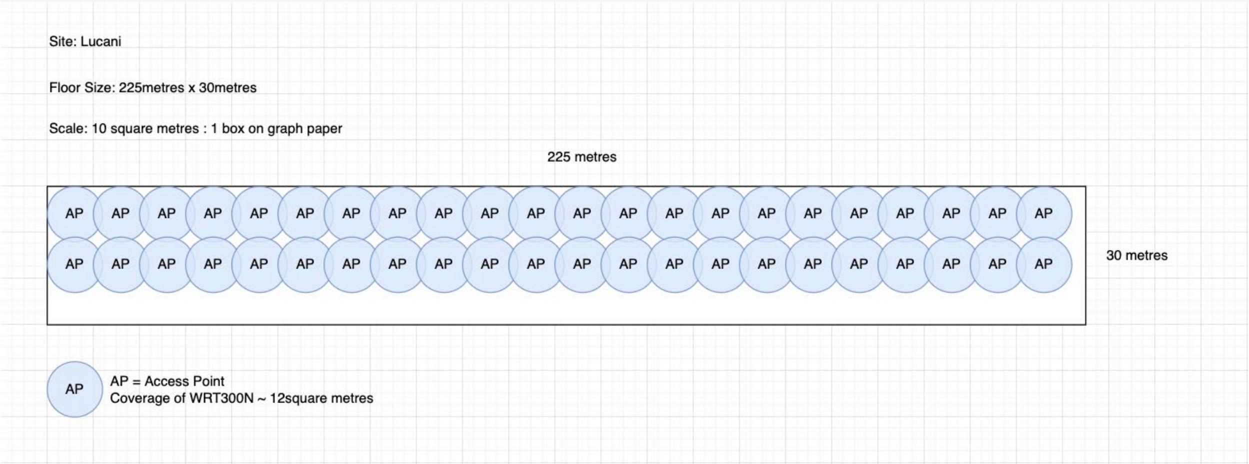


LUCANI

Area of Lucani building floor = 225 × 30
= 6750 m^2

1 Access Point (AP) covers 1600 sqft
= 148.64 m^2

No. of APs required = $\frac{6750}{148.64}$
≈ 45 APs


Site: Lucani
Floor Size: 225metres x 30metres
Scale: 10 square metres : 1 box on graph paper
225 metres
AP
30 metres
AP
AP = Access Point
Coverage of WRT300N ~ 12square metres

DHCP

Dynamic Host Configuration Protocol v4 (DHCPv4) assigns IPv4 addresses and other network configuration information dynamically. The DHCPv4 server dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address and this allows us to use any communication protocol. DHCP has been implemented on the *Ljubis* site where the *Ljubis* router has been configured to act as the DHCP server and dynamically provide IP address information to PC workstations/Laptops. The DHCP pools for all the VLANs and their respective default gateway router addresses have been created on the router. It helps the network administrator with IP addresses configuration without requiring him to manually configure IPs for all end user devices. Please refer to [Table D: Ljubis DHCP Server Pool IP Host Addresses] for more details.

NAT

NAT (Network Address Translation) enables the translation of source and destination IP addresses and ports. It is a method which maps the IP address space into another by modifying the network address information in the IP header of packets while they are in transit across a traffic routing device. It is a method which reduces the need for IPv4 public addresses thereby hiding the private network ranges.
NAT offers security and privacy by advertising only one address for the entire network and effectively hiding the internal network. It also prevents the depletion of the legally registered IP addresses.

Three types of address translation are:

Static NAT – It is a method which maps network traffic from a static public IP address to an internal private IP address/network.

Dynamic NAT – It is a technique in which multiple public IP addresses are mapped and translated to an internal or private IP address.
Port Address Translation (PAT) / NAT Overload – It is the method in which a public IP address is mapped to multiple private IP addresses by using different ports.

In our scenario, we have configured NAT on the router which acts as a gateway router to the Internet which is the *Mackat* router. We have used the NAT pool given to us in the specifications and used it first to apply NAT overload on the Mackat router. Due to this, it translates multiple internal IP addresses to a public address, mapped with different port numbers, so it doesn't need multiple public addresses for multiple internal IPs. Static NAT has been applied to assign a static IP address to each of the servers (*Security Server and Common Server*) in the Server Farm. First, we define the pools for each VLAN and ACLs to permit the internal network traffic, then establish dynamic source translation by binding the pools to the ACLs. By specifying the inside and outside NAT interfaces is what defines how the NAT will take place on the network traffic traversing through.
On Mackat ISP, by configuring a static route pointing to the Public NAT pool the network traffic from the Internet can be traversed to the internal network defined by the NAT pool.

Security and Access Control Policies

Security

SSH

SSH (Secure Shell) helps us to provide secure remote connection to network devices such as routers and switches. It was chosen over Telnet to provide remote access to *Guca* router and all the management devices at Guca site for maintenance by the *Technical Support* group because SSH provides an encrypted channel while Telnet sends data in plain text and does not have a mechanism to ensure data confidentiality and security. SSH helps in preventing attacks such as IP spoofing, IP source routing, DNS spoofing, etc.

Credentials for SSH configured in our prototype:
Username - group7
Password - casestudy

PPP

PPP - Point-to-Point Protocol is a data link layer communication protocol between two routers. It specifies the frame format of the data to be transmitted, method of encapsulation and the authentication rules of the communicating devices. The two authentication protocols of *PPP are CHAP (*Challenge Handshake Authentication Protocol) and *PAP* (Password Authentication

Protocol).
In our case study, we have configured PPP on the link between ISP and Mackat. It is helping in providing encryption, authentication and compression.

CHAP

CHAP is the method used by PPP to verify the identity of the remote users. We have configured CHAP authentication on the link to the ISP. It uses a 3-way handshake to verify the identity of the user. This method uses cryptographic hash value for the authentication. CHAP authentication is also configured on the link between ISP and Mackat.

Access Control Policies

ACL

Access Control Lists (ACLs) act as network traffic filters that can control the incoming and outgoing traffic. ACLs defined on the router's/ any network device interface define how to forward or block a packet from that particular interface. ACLs act as a firewall which restricts/allows/blocks the packets from the source to destination.
In our Case Study, Named ACLs are implemented on the *GUCA* site to control the flow of IP traffic to the internet and within the internal network as well.

ACL rules are defined for the access to the *Server Farm* LAN in which **Security Server** can only be accessed by the Security group whereas cannot be accessed by any other VLAN in the GUCA site. On the other hand, **Common Server** can be accessed by all the VLANs.
Here is the reference to ACL table provided below: [Table G: Record of ACL Testing Guca]

ACL rules are defined so that PC hosts in the *Marketing* VLAN cannot access the *Leasing* VLAN, and the hosts *Vehicle Servicing* VLAN is denied access to the hosts in all the other VLANs. Also, rules are applied to define that hosts in other VLANs cannot access the hosts in the *Technical Support* VLAN.

In our case study, we have applied ACLs regarding IP and ICMP protocols. IP is the network layer protocol for routing and addressing packets of data in order to traverse through networks and arrive at the correct destination. ICMP is a protocol which defines how the messages are sent between devices.

System Testing and Verification Strategy

The following steps were taken to test and verify the strategies:

1. *show vlan brief, show run :* these were used to verify the configuration of switches and the VLAN configurations along with their respective ports and their status.
2. *show ether channel and show ether channel summary* : these were used to check the etherchannel configurations which was implemented using LACP
3. *show ip route, show ip ospf neighbor*: these were used to verify the OSPF configurations
4. *show ip interface brief, show ip dhcp pool* : IP addressing and DHCP configurations can be verified using these commands
5. *show ip nat translations, show ip nat statistics*: these can be used to verify the NAT configurations
6. The ACL implementations were verified by trying to ping the respective PCs belonging to those VLANS and checking if the ACL restriction/permission had worked.

Appendix: Tables A to G

Table A: VLSM Design

Site Location	Host required	Subnet Network Address	Subnet Prefix	Max Number of Hosts	VLAN Name
Guca	163	67.128.4.0	/24	254	Leasing
Guca	234	67.128.2.0	/24	254	Marketing
Guca	260	67.128.0.0	/23	510	Business
Guca	7	67.128.7.128	/28	14	Security
Guca	7	67.128.7.144	/28	14	Technical_Support
Guca	7	67.128.7.160	/28	14	Vehicle_Servicing
Guca	2	67.128.8.72	/30	2	Printer
Guca	26	67.128.7.0	/27	30	Management
Guca	65	67.128.6.128	/25	126	Server_Farm

Ljubis	104	67.128.6.0	/25	126	Leasing
Ljubis	7	67.128.7.176	/28	14	Security
Ljubis	7	67.128.7.192	/28	14	Technical
Ljubis	7	67.128.7.208	/28	14	Vehicle
Ljubis	2	67.128.8.76	/30	2	Printer
Ljubis	26	67.128.7.32	/27	30	Management
Lucani	182	67.128.3.0	/24	254	Sales
Lucani	7	67.128.7.224	/28	14	Security
Lucani	7	67.128.7.240	/28	14	Technical
Lucani	7	67.128.8.0	/28	14	Vehicle
Lucani	2	67.128.8.88	/30	2	Printer
Lucani	26	67.128.7.64	/27	30	Management
Mackat	163	67.128.5.0	/24	254	Sales
Mackat	7	67.128.8.16	/28	14	Security
Mackat	7	67.128.8.32	/28	14	Technical
Mackat	7	67.128.8.48	/28	14	Vehicle
Mackat	2	67.128.8.92	/30	2	Printer
Mackat	26	67.128.7.96	/27	30	Management
GUCA & Mackat	2	67.128.8.68	/30	2	GUCA - Mackat
GUCA & Ljubis	2	67.128.8.64	/30	2	GUCA - Ljubis
Lucani & Ljubis	2	67.128.8.80	/30	2	Lucani - Ljubis
Lucani & Mackat	2	67.128.8.84	/30	2	Lucani - Mackat

Table B: Switch Details

We have used the WS-C3650-24PS switch as they have relatively more number of ports.

Name	Model	# of Ports	Location	Management VLAN IP Address	Default Gateway IP Address	Management VLAN
Guca_Sw1	3650-24PS	24	Guca	67.128.7.4/27	67.128.7.1	99
Guca_Sw2	3650-24PS	24	Guca	67.128.7.3/27	67.128.7.1	99
Guca_Sw3	3650-24PS	24	Guca	67.128.7.2/27	67.128.7.1	99
Mackat_Sw1	3650-24PS	24	Mackat	67.128.7.98/27	67.128.7.97	99
Mackat_Sw2	3650-24PS	24	Mackat	67.128.7.99/27	67.128.7.97	99
Mackat_Sw3	3650-24PS	24	Mackat	67.128.7.100/27	67.128.7.97	99
Lucani_Sw1	3650-24PS	24	Lucani	67.128.7.66/27	67.128.7.65	99
Lucani_Sw2	3650-24PS	24	Lucani	67.128.7.67/27	67.128.7.65	99
Lucani_Sw3	3650-24PS	24	Lucani	67.128.7.68/27	67.128.7.65	99
Ljubis_Sw1	3650-24PS	24	Ljubis	67.128.7.34/27	67.128.7.33	99
Ljubis_Sw2	3650-24PS	24	Ljubis	67.128.7.36/27	67.128.7.33	99
Ljubis_Sw3	3650-24PS	24	Ljubis	67.128.7.35/27	67.128.7.33	99

Table C: Router Details

Site: Guca

Router Name: Guca_R1

Interface	Description	VLAN Name	Network Address	Interface IP Address	Subnet Mask
gi0/0/1	physical interface	/	/	/	/
gi0/0/1.20	VLAN20	Leasing	67.128.4.0	67.128.4.1	/24

	Leasing				
gi0/0/1.30	VLAN30 Marketing	Marketing	67.128.2.0	67.128.2.1	/24
gi0/0/1.40	VLAN40 Business	Business	67.128.0.0	67.128.0.1	/23
gi0/0/1.50	VLAN50 Security	Security	67.128.7.128	67.128.7.129	/28
gi0/0/1.60	VLAN60 Technical_Support	Technical_Support	67.128.7.144	67.128.7.145	/28
gi0/0/1.70	VLAN70 Vehicle_Servicing	Vehicle_Servicing	67.128.7.160	67.128.7.161	/28
gi0/0/1.80	VLAN80 Printer	Printer	67.128.8.72	67.128.8.73	/30
gi0/0/1.90	VLAN90 Server_Farm	Server_Farm	67.128.6.128	67.128.6.129	/25
gi0/0/1.99	VLAN99 Management	Management	67.128.7.0	67.128.7.1	/27
Serial0/1/0	Connection to Mackat	Guca - Mackat	67.128.8.68	67.128.8.69	/30
Serial0/1/1	Connection to Ljubis	Guca - Ljubis	67.128.8.64	67.128.8.65	/30

Site: Ljubis
Router Name: Ljubis_R1

Interface	Description	VLAN Name	Network Address	Interface IP Address	Subnet Mask
gi0/0/01	physical interface	/	/	/	/
gi0/0/1.20	vlan 20 Leasing	Leasing	67.128.6.0	67.128.6.1	/25

gi0/0/1.50	vlan 50 Security	Security	67.128.7.176	67.128.7.177	/28
gi0/0/1.60	vlan 60 Technical_Support	Technical	67.128.7.192	67.128.7.193	/28
gi0/0/1.70	vlan 70 Vehicle Servicing	Vehicle	67.128.7.208	67.128.7.209	/28
gi0/0/1.80	vlan 80 Printer	Printer	67.128.8.76	67.128.8.77	/30
gi0/0/1.99	vlan 99 Management	Management	67.128.7.32	67.128.7.33	/27
Serial0/1/0	connection to Lucani	Lucani - Ljubis	67.128.8.80	67.128.8.82	/30
Serial0/1/1	connection to Guca	GUCA - Ljubis	67.128.8.64	67.128.8.66	/30

Site: Lucani
Router Name: Lucani_R1

Interface	Description	VLAN Name	Network Address	Interface IP Address	Subnet Mask
gi0/0/1	Physical interface	/	/	/	/
gi0/0/1.10	Vlan10 - Sales	Sales	67.128.3.0	67.128.3.1	/24
gi0/0/1.50	Vlan50 - Security	Security	67.128.7.224	67.128.7.225	/28
gi0/0/1.60	Vlan60 - Technical Support	Technical	67.128.7.240	67.128.7.241	/28
gi0/0/1.70	Vlan70 - Vehicle Servicing	Vehicle	67.128.8.0	67.128.8.1	/28

gi0/0/1.80	Vlan80 - Printer	Printer	67.128.8.88	67.128.8.89	/30
gi0/0/1.99	Vlan99 - Management	Management	67.128.7.64	67.128.7.65	/27
Serial0/1/0	Connection to Ljubis	Lucani - Ljubis	67.128.8.80	67.128.8.81	/30
Serial0/1/1	Connection to Mackat	Lucani - Mackat	67.128.8.84	67.128.8.85	/30

Site: Mackat

Router Name: Mackat_R1

Interface	Description	VLAN Name	Network Address	Interface IP Address	Subnet Mask
gi0/0/1	Physical interface	/	/	/	/
gi0/0/1.10	vlan 10 sales	Sales	67.128.5.0	67.128.5.1	/24
gi0/0/1.50	vlan 50 Security	Security	67.128.8.16	67.128.8.17	/28
gi0/0/1.60	vlan 60 Technical support	Technical	67.128.8.32	67.128.8.33	/28
gi0/0/1.70	vlan 70 Vehicle services	Vehicle	67.128.8.48	67.128.8.49	/28
gi0/0/1.80	vlan 80 Printer	Printer	67.128.8.92	67.128.8.93	/30
gi0/0/1.99	vlan 99 Management	Management	67.128.7.96	67.128.7.97	/27
Serial0/1/0	connection to Guca	Guca - Mackat	67.128.8.68	67.128.8.70	/30
Serial0/1/1	connection to Lucani	Lucani - Mackat	67.128.8.84	67.128.8.86	/30

Serial0/2/0	connection to ISP	Class C ISP network connection address	213.2.8.0	213.2.8.2	/30

Table D: Ljubis DHCP Server Pool IP Host Addresses

VLAN Name	IP Address Pool Range	Subnet Mask	Default Gateway
Leasing	67.128.6.1 - 67.128.6.126	/25	67.128.6.1
Security	67.128.7.177 - 67.128.7.190	/28	67.128.7.177
Technical	67.128.7.193 - 67.128.7.206	/28	67.128.7.193
Vehicle	67.128.7.209 - 67.128.7.222	/28	67.128.7.209
Printer	67.128.8.77 - 67.128.8.78	/30	67.128.8.77

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

Name	In VLAN #	IP Address	Subnet Mask	Default Gateway	Service
Security Server	90	67.128.6.130	255.255.255.128	67.128.6.129	FTP
Common Server	90	67.128.6.132	255.255.255.128	67.128.6.129	FTP
Printer_Guca	80	67.128.8.74	255.255.255.252	67.128.8.73	Printing
Printer_Mackat	80	67.128.8.94	255.255.255.252	67.128.8.93	Printing
Printer_Lucani	80	67.128.8.90	255.255.255.252	67.128.8.89	Printing

Table F: Wireless Access Point Details

Name	Model	SSID	Channel
Wireless Router	WRT300N	Security WLAN	1-2.412GHz

Table G: Record of ACL Testing Guca

Source Host	Destination Host/Server	Protocol	Expected Result	Achieved
Host on Security	Server Farm 1	IP	Permitted	Yes
Host on Leasing/Marketing/ Technical Support/ VehicleServicing/ Business/	Server Farm 1	IP	Denied	Yes
Host on Marketing	Host on Leasing	ICMP	Denied	Yes
Host on Vehicle Servicing	Host on Leasing/Marketing/ Technical Support/ Security/Business/	ICMP	Denied	Yes
Host on Leasing/Marketing/ Vehicle Servicing/ Security/Business/	Host on Technical Support	ICMP	Denied	Yes
Host on any VLAN	Internet Web Server	IP	Permitted	Yes

The END