CASE STUDY TNE2002/TNE70003 SEM 1 2022

ESP Team : T001
Lab Class : Saturday 5:30pm ONLINE
Class Tutor : Peter Granville

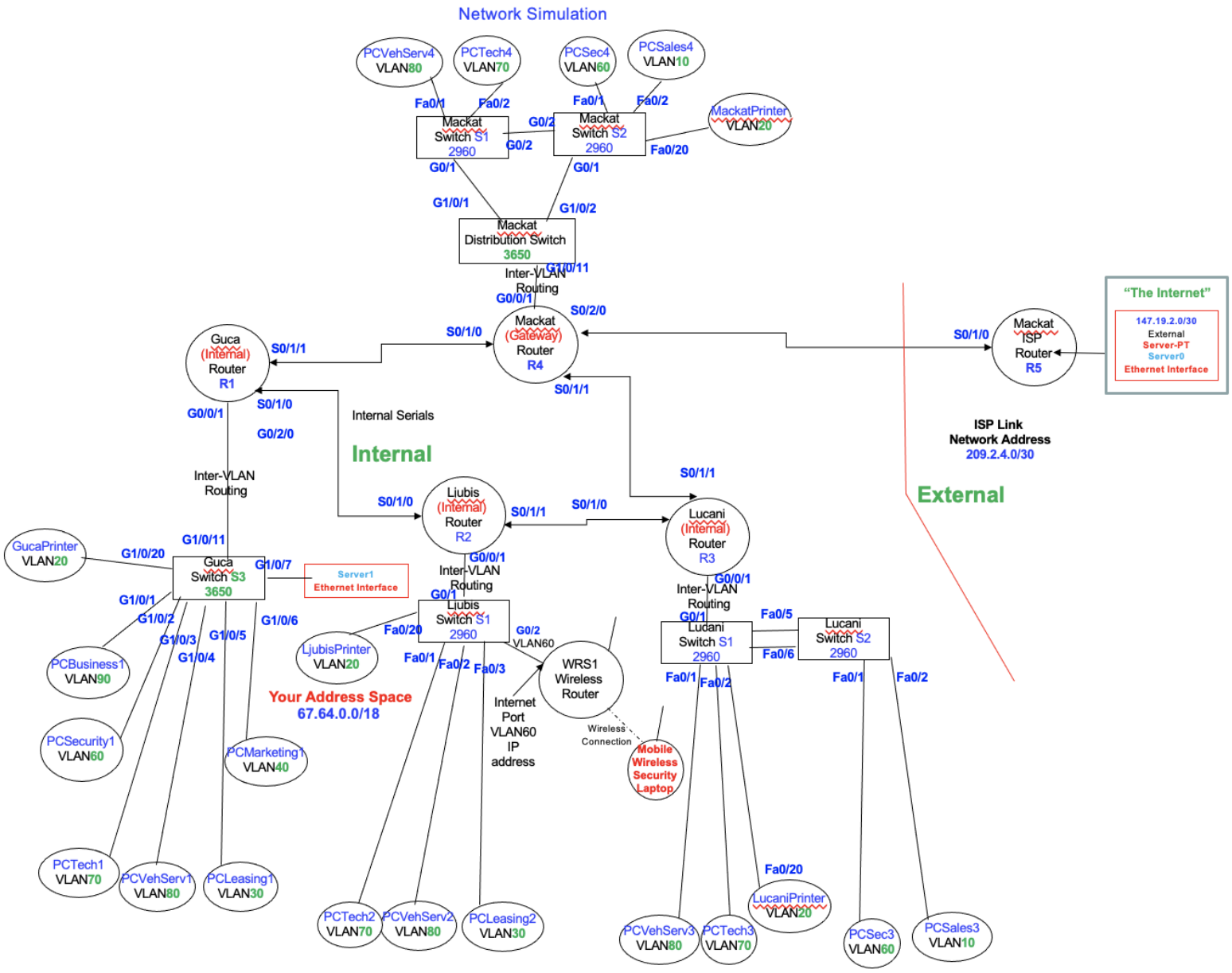
Members :

103146075	Faiz Syed Ibrahim
103218893	Matthew Mulvaney
103506446	Aldro Axeldes Marvellano
103524325	Michelle Angelica Lautan
103510544	Xin Su
102922546	Atif Javed

Case Study Specifications:

Specification Number:	2.4
Class A Internal :	67.64.0.0/18
Class B NAT Pool :	147.4.0.0/23
Class C ISP Connection :	209.2.4.0/30
Class B ISP Web Server :	147.19.2.0/30
Wireless Deployment Site :	Ljubis
Management VLAN Number :	55
Percentage Growth VLSM :	40

Network Topology Diagram



IP VLSM Design (Table A at the end)

The company has allocated the 67.64.0.0/18 network for the internal network. IPv4 address space is limited, hence we have used VLSM or Variable Length Subnet Mask which is a design strategy where all subnet masks can have varying sizes. This enables the allocated IP Address space to be efficiently utilised with the size of each subnet of the network determined by the number of devices anticipated to need i.p. addresses on that subnet of the network. The VLSM was designed in a way that the anticipated 40% percentage growth of the various company work groups was taken into consideration. By implementing VLSM, about 13 percent of the available major network address space is used, with the rest available for future use. Moreover, about 70 percent of the subnetted network address space is used.

We assumed the network size of the Management, Server Farm and Printer VLAN while following the requirements of each of them. The Server Farm in the Head Office of Guca was allocated 17 addresses (maximum of 30). Hence, using networking, each location will be able to have approximately 4 independent servers which would be sufficient and would also allow for locations to have more than 4 servers if required. The Management and Printer VLAN are assigned a maximum of 30 and 14 network addresses respectively for each location.

The Serial Links are direct point to point links. They are not VLANs and do not need to cater for future growth. If a new site was added in the future, then new subnetted network addresses would need to be added for the new point to point links from the unused address space from the major network 67.64.0.0/18

Routing Protocols (Table C at the end)

Each site has several VLANs. So, within each site we used a router-on-a-stick topology with sub-interfaces on the router for each of the VLANs on the switches at that site. As you can see in the Topology Diagram, we have configured each internal router to be connected to two other internal routers. This provides path redundancy. The Mackat gateway router has added importance as all connections to the internet go through it.

The OSPF (Open Shortest Path First) routing protocol is used by a variety of vendors making it a popular choice with the flexibility to use products from multiple different vendors (ideal if a router were to fail and a replacement needed to be quickly installed and the preferred brand is unavailable).

There are only four internal routers in this simulation, so we have chosen to use single-area OSPF as the OSPF packets won't overwhelm the available resources on the routers. The bandwidth on site-to-site serial links has been limited to 256. Traffic between sites can be expensive and it's important to limit the speed to a level that can be reliably handled by the site-to-site links and network devices such as routers.

Encrypting site to site traffic to make it harder for an attacker to intercept this traffic is advisable. To demonstrate this feature, we have used MD5 authentication for the link between the Guca and Mackat sites. In the production network we would use this for all site-to-site links.

Passive-interfaces can be configured for ports on the router that are known to not be connected to another router participating in the OSPF routing. As there are a lot of subnets, we have set the passive-interface to be on by default for all router ports and then turned it off for the site-to-site serial links. This is much faster to configure and would mean less reconfiguration is needed if an additional VLAN were to be added.

The Gateway router has a default route configured to the ISP router and advertises this route to the other internal routers. This is to demonstrate this feature. In a production network multiple gateway routers connected to different ISPs would be ideal for redundancy.

With multiple sites it is likely not cost efficient to have IT people onsite 24x7 at every site to handle issues. With SSH access to the Guca router, most issues can be remotely troubleshooted by the Technical Support group. This is enabled just at the Guca site to demonstrate this feature, but in the production network we would recommend configuring SSH access to all the routers. SSH provides a secure connection and thus we would recommend using this rather telnet which is not secure.

Switches: VLANs, STP, EtherChannel (Table B at the end)

VLANs

We have created 10 different VLANs according to the requirements for the network. Rather than using VLAN 1 as the default management VLAN at each site, we have configured a Management VLAN (VLAN 55) that will include all the switches.

A separate VLAN has been assigned to the Printers (VLAN 20) in each site, so they are accessible by all groups. The Server VLAN (VLAN 100) configured in Guca Location can hold a maximum of 30 addresses, enough for all the sites to have more than 4 individually. Not all VLANs have been configured on all switches. Only VLANs required in the location have been configured with the same VLAN numbers for easier reference.

VLANs were assigned to switch ports with the goal of making testing easier. Actual physical implementation needs were not considered, and ports were assigned to VLANs based on their port numbers to keep things simple and allow for easy network testing.

EtherChannel

We have demonstrated path redundancy with our internal router configuration and with the Mackat switches having multiple paths to the distribution switch.

Ether Channel provides another important form of redundancy, called link redundancy. This way if an ethernet cable were to fail or a port, hopefully the other cable would still be fine, and that link would remain active.

We have demonstrated this feature with the Lucani access switches. We have two switches connected to each other via EtherChannel. Each switch has multiple host PCs attached.

EtherChannel can also improve performance. Ether Channel will still only send a single packet over a single link, however with multiple PCs in use, EtherChannel can help ensure that upstream links are saturated less of the time.

LACP is an IEEE standard so if a switch were to fail it could be replaced with a different switch from a different vendor.

In the production network we would use this feature at all sites for switch-to-switch connections. Typically, if hosts were using Fast Ethernet, you'd then use EtherChannel with Gigabit Ethernet for the upstream link to the Distribution Switch. Ether Channel could also be considered for connecting critical servers to access switches. However, it typically wouldn't be used for ordinary host PCs as the disruption caused by one user losing their connection typically wouldn't justify the added cost of providing redundant links.

STP

In the Mackat network we have configured STP. For demonstration purposes we have a Distribution switch connected to the router and two access switches connected to each other and to the Distribution switch.

Spanning Tree Protocol is used to logically break switching loops. Whilst Layer 3 uses IPv4 Time to Live and IPv6 hop count to stop packets from looping endlessly, Layer 2 doesn't have a way to stop frames from looping forever, so redundant logical paths need to be blocked. Thus, STP is enabled by default and should never be disabled. Even if there isn't a loop in a network it's very easy to create one by mistake and a Layer 2 loop can take down a whole network if it's not protected against.

We have configured Per VLAN Spanning Tree which is the default on the 2960 switches. Rapid Per VLAN Spanning Tree has faster convergence, but it uses more resources.

The Distribution switch is the root bridge so the links directly connected to it will never be blocked. The direct link between the two access switches is there in case one of the links to the Distribution switch fails.

The Distribution switch being the root bridge will ensure that traffic flows quickly to this switch which is where most of the traffic that can't stay within the access switch is going to go to or via anyway. We have used a more powerful and faster model for the Distribution switch compared with the access switches as more

traffic will need to flow through it. In a production network it would be advisable to consider multiple distribution switches with each access switch connected to two distribution switches for more redundancy.

Wireless LANs and Site Layout for the Specified Site (Table F at the end)

To calculate the wireless access points, the first step is to calculate the site and building area. As per the given instructions, the site size is 1500m x 2000m and the building floor size is 120m x 30m.

Since we need wireless coverage for a large area, a basic service set (BSS) isn't sufficient. Moreover, we want SSID to remain the same for all APs. Hence the security group team member can access the network while moving around the site without changing any wireless setting. For this purpose, we use a common distribution system (CDS). The CDS allows multiple access points for the extended service sets (ESS) to appear as a single BSS. For maximum utilization of AP range, we use non-overlapping channels 1, 6, 11 and 16. The Wireless access point we use has a range of 450m^2. To calculate the number of AP required we divide the area by the range of the wireless router.

Calculation of Wireless access point:

Site size: 1500m x 2000m = 3,000,000m^2

Building size: 120m x 30m = 3600m^2

Range of the wireless router = 450 m^2

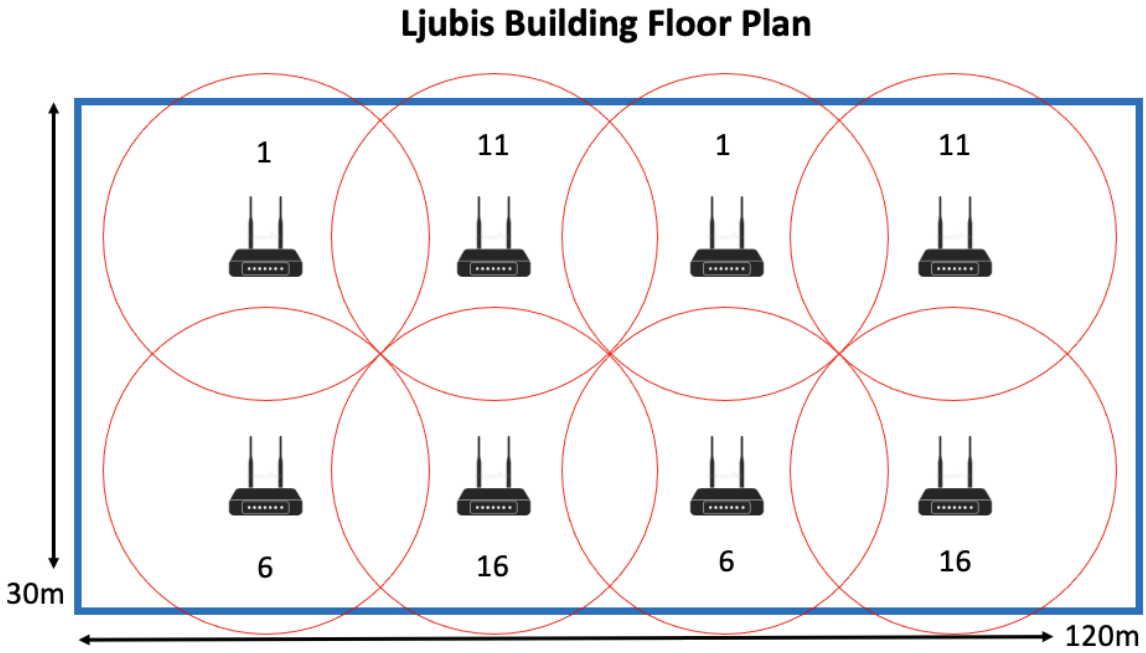
Total AP require = Building area / AP range

= 3600 m^2 /450 m^2 = 8 APs

As per the calculation we require 8 AP to cover the whole building.

The case study requirements suggest that the wireless connection needs to spread across the whole site, after calculation of the number of APs required to cover the

entire area (3,000,000m2 / 450m2 = 6666 APs), which isn't practical. Hence, we decide to cover the area only of the building for this case study.



DHCP (Table D and E at the end)

On the Ljubis site, we utilized DHCP to automatically assign IP addresses to PCs. The router will function as a DHCP server, storing a pool of IP addresses that will be used to allocate IP addresses to Ljubis PCs. If we utilize static IP configuration to assign IP addresses to many PCs this will require considerable time for the initial configuration and for ongoing maintenance and increase the chances of mistakes. To reduce these problems, we must use DHCP to automatically assign IP addresses. In this prototype, we just implement and illustrate DHCP on one site, but if the customer requires it, we may implement it on multiple sites. Furthermore, we put just one PC into each VLAN (except the printer and management VLANs) to demonstrate this feature. DHCP is also highly useful for client computers that move around a lot and need to update their IP address every time.

In the prototype, we additionally exclude specific IP addresses so that they are not used on the PC. These addresses are: 67.64.7.126,67.64.7.142,67.64.7.158 and 67.64.7.97 - 67.64.7.110. These are excluded as these are the ip address that is

already used for default gateway of each PC and Ip address of a printer that is statically configured. These ip addresses should not be included in the ip address pool of the dhcp server(Ljubis router). Each device needs a unique ip address on the local network.

NAT (Table G and H at the end)

We configured Network Address Translation(NAT) to translate our private IP addresses to routable public IP addresses to access the internet (the outside network) from the inside network (the company sites).

The Mackat Router is the gateway router, and all NAT configuration is done on that router. The serial link to the ISP router is configured to be a connection to the outside network and the serial links to company routers and router sub-interfaces to Mackat VLANs are configured to be from the inside network.

Traffic between the inside and outside network will be translated using NAT. There are more internal I.P. addresses than external I.P. addresses so we can't have a unique external I.P. address for every device. Therefore, the NAT Pool is configured to overload.

The Servers in the Server Farm may need to be accessed remotely so our demonstration server in the prototype Server 1 in Guca site is configured with a static NAT address.

NAT is configured to work with all the VLANs. The Access Control List is configured to allow all IP traffic from the Mackat VLANs and the rest of the internal network.

Security and Access Control Policies (Table I at the end)

We use ACL to provide security to our network. That way, we can control who is allowed to enter or exit the network. In our case, extended ACL is used because it provides more granular control over when to permit and deny packets based on the source and destination host/subnet according to the given rules. It also is the best choice when the ACLs are configured close to the source.

We first created a text document with the 5 stated rules. We configured the access group named TestingGuca and made our first attempt to implement the 5 rules in the case study details starting from the most specific because of the top to down sequential nature of ACL in cisco. So, we started off with denying marketing vlan access to the leasing vlan; then denying the vehicle servicing vlan access into any other vlan; then denying all other vlans access to technical support vlan; and finally permitted all other traffic.

After that, we placed the access group into all subinterfaces in the guca router, Starting from subinterface Gi0/0/1.20 up until subinterface Gi0/0/1.100 to enable the rules that we've created to work.

However when testing the rules we came up with we noted that the requirements to permit all vlans to access the internet and lastly permit access to all other vlan unless being specified from the previous rules were not met.

We noted other access control rules needed to meet the requirements. Namely that the Technical Support VLAN can access any other VLAN and can access the Guca router and switch using SSH. We also noted that PC hosts from any VLAN can access the internet. So, we refined our rules to meet these implied requirements.

System Testing and Verification Strategy

Our approach was to systematically test the prototype as we went along and to thoroughly test it again with everything complete. Picking up mistakes closer to when they are made can help avoid consequential problems including countless hours testing for issues only to find a previous section was not done right. However,

it is worth noting that sometimes properly testing a feature depends on completing later sections so there is only limited testing that can be done at the time of configuration.

It is important to go back and check everything at the end to make sure that configuring NAT, ACLs etc. does not break other parts of the network configuration.

Firstly, we created a topology diagram (see the start of this report) to meet the company requirements. We determined which VLANs we would need and how big they would need to be and did the VLSM Design.

We then created the Packet Tracer file and put all the devices needed in it and hooked them up without configuring them.

From there we configured the switches with VLANs, management interface VLAN I.P. address, default gateway, STP at Mackat Site and EtherChannel at Lucani.

We could do basic testing that the Ether Channel was working but as no PCs were configured and no routers, we couldn't yet do much of the testing. Similarly, we could verify that the Mackat Distribution Switch was the root bridge for STP.

We configured the routers and routing protocols and a static route from the ISP Router to the internal network.

We tested for failover from the default path to the Mackat gateway router to the backup path from the non-gateway internal routers by shutting down the relevant serial port on the non-gateway router and checking for updates to the routing table.

At this point we could test pinging from a switch at one site to a switch at another site and check that the port on a switch that was connected to a router was showing as a trunk. However, the PCs were not yet configured.

We then configured DHCP and the remaining I.P. addresses and tested pinging from PCs to PCs in the same site, other sites, PCs to switches, PCs to routers, PCs to external web server, PCs to server in Guca Server Farm etc.

We configured PPP and CHAP on the link to the ISP router and confirmed that traffic to the external web server still worked.

Wireless was configured and we confirmed that the security laptop could access all devices within the site.

We configured NAT and verified that all PCs could still connect to the external server. Some trial and error were needed as the topology is more complicated than that of Scenario 5. We figured out that the sub-interfaces on the Mackat Gateway Router needed to be set to be inside networks as well as the links to the other internal routers from the Gateway router. The link to the ISP router was set to be a connection to an outside network.

Finally, we tested traffic that needed to be blocked by the required ACL list was not blocked and working, wrote up ACLs in a text file and then ran the commands, tested them to make sure all rules were working as required, removed the ACLs when there was problem identified and refined our list in the text file and kept on reapplying new attempts until we got it right.

Finally, we tested the network thoroughly to make sure that all the requirements were still met and that nothing was broken.

Table A: VLSM Design

Guca:

No. of host add. required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max No. of Hosts Possible	Assignable Range	Add. Space Future Use Y/N	VLAN Name	Site Location
280	67.64.0.0	255.255.254.0	/23	510	67.64.0.1 – 67.64.1.254	Y	Guca Business	Guca
252	67.64.2.0	255.255.255.0	/24	254	67.64.2.1 – 67.64.2.254	Y	Guca Marketing	Guca
175	67.64.4.0	255.255.255.0	/24	254	67.64.4.1 – 67.64.4.254	Y	Guca Leasing	Guca
25	67.64.6.128	255.255.255.224	/27	30	67.64.6.129 – 67.64.6.158	Y	Guca Management	Guca
7	67.64.7.48	255.255.255.240	/28	14	67.64.7.49 – 67.64.7.62	Y	Guca Printer	Guca
17	67.64.7.0	255.255.255.224	/27	30	67.64.7.1 – 67.64.7.30	Y	Guca Server Farm	Guca
7	67.64.7.64	255.255.255.240	/28	14	67.64.7.65 – 67.64.7.78	Y	Guca Security	Guca
7	67.64.7.80	255.255.255.240	/28	14	67.64.7.81 – 67.64.7.94	Y	Guca Technical Support	Guca
7	67.64.7.32	255.255.255.240	/28	14	67.64.7.33 – 67.64.7.46	Y	Guca Vehicle Servicing	Guca

Ljubis:

No.of host add. required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max No. of Hosts Possible	Assignable Range	Add. Space Future Use Y/N	VLAN Name	Site Location
112	67.64.6.0	255.255.255.128	/25	126	67.64.6.1 – 67.64.6.126	Y	Ljubis Leasing	Ljubis
25	67.64.6.160	255.255.255.224	/27	30	67.64.6.161 – 67.64.6.190	Y	Ljubis Management	Ljubis
7	67.64.7.96	255.255.255.240	/28	14	67.64.7.97 – 67.64.7.110	Y	Ljubis Printer	Ljubis
7	67.64.7.112	255.255.255.240	/28	14	67.64.7.113 – 67.64.7.126	Y	Ljubis Security	Ljubis
7	67.64.7.128	255.255.255.240	/28	14	67.64.7.129 – 67.64.7.142	Y	Ljubis Technical Support	Ljubis
7	67.64.7.144	255.255.255.240	/28	14	67.64.7.145 – 67.64.7.158	Y	Ljubis Vehicle Servicing	Ljubis

Mackat:

No. of host add. required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max No. of Hosts Possible	Assignable Range	Add. Space Future Use Y/N	VLAN Name	Site Location
175	67.64.5.0	255.255.255.0	/24	254	67.64.5.1 – 67.64.5.254	Y	Mackat Sales	Mackat

25	67.64.6.224	255.255.255.224	/27	30	67.64.6.225 – 67.64.6.254	Y	Mackat Management	Mackat
7	67.64.7.224	255.255.255.240	/28	14	67.64.7.225 – 67.64.7.238	Y	Mackat Printer	Mackat
7	67.64.7.240	255.255.255.240	/28	14	67.64.7.241 – 67.64.7.254	Y	Mackat Security	Mackat
7	67.64.8.0	255.255.255.240	/28	14	67.64.8.1 – 67.64.8.14	Y	Mackat Technical Support	Mackat
7	67.64.8.16	255.255.255.240	/28	14	67.64.8.17 – 67.64.8.30	Y	Mackat Vehicle Servicing	Mackat

Lucani:

No. of host add. required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max No. of Hosts Possible	Assignable Range	Add. Space Future Use Y/N	VLAN Name	Site Location
196	67.64.3.0	255.255.255.0	/24	254	67.64.3.1 – 67.64.3.254	Y	Lucani Sales	Lucani
25	67.64.6.192	255.255.255.224	/27	30	67.64.6.193 – 67.64.6.222	Y	Lucani Management	Lucani
7	67.64.7.160	255.255.255.240	/28	14	67.64.7.161 – 67.64.7.174	Y	Lucani Printer	Lucani
7	67.64.7.176	255.255.255.240	/28	14	67.64.7.177 – 67.64.7.190	Y	Lucani Security	Lucani

7	67.64.7.192	255.255.255.240	/28	14	67.64.7.193 – 67.64.7.206	Y	Lucani Technical Support	Lucani
7	67.64.7.208	255.255.255.240	/28	14	67.64.7.209 – 67.64.7.222	Y	Lucani Vehicle Servicing	Lucani

Serial Connections:

No. of host add. required	Subnet Network Address	Subnet Mask	Subnet Prefix	Max No. of Hosts Possible	Assignable Range	Add. space Future Use Y/N	VLAN Name	Site Location
2	67.64.8.32	255.255.255.252	/30	2	67.64.8.33 – 67.64.8.34	N	Serial 1	N/A
2	67.64.8.36	255.255.255.252	/30	2	67.64.8.37 – 67.64.8.38	N	Serial 2	N/A
2	67.64.8.40	255.255.255.252	/30	2	67.64.8.41 – 67.64.8.42	N	Serial 3	N/A
2	67.64.8.44	255.255.255.252	/30	2	67.64.8.45 – 67.64.8.46	N	Serial 4	N/A

VLAN Plan

VLAN Number	*Name*
10	Sales Group
20	Printer
30	Leasing Group
40	Marketing Group

55	Management
60	Security Group
70	Technical Support Group
80	Vehicle Servicing Group
90	Business Group
100	Server Farm

Table B: Switch Details

Name	Model	No. of ports (total)	Location	Management VLAN IP address	Default Gateway IP address	Management VLAN
GucaAccessS1	3650	28	Guca	67.64.6.129 255.255.255.224	67.64.6.158 255.255.255.224	55
LjubisAccessS1	2960	26	Ljubis	67.64.6.161 255.255.255.224	67.64.6.190 255.255.255.224	55
LucaniAccessS1	2960	26	Lucani	67.64.6.193 255.255.255.224	67.64.6.222 255.255.255.224	55
LucaniAccessS2	2960	26	Lucani	67.64.6.194 255.255.255.224	67.64.6.222 255.255.255.224	55
MackatDistSw	3650	28	Mackat	67.64.6.225 255.255.255.224	67.64.6.254 255.255.255.224	55
MackatAccessS1	2960	26	Mackat	67.64.6.226 255.255.255.224	67.64.6.254 255.255.255.224	55
MackatAccessS2	2960	26	Mackat	67.64.6.227 255.255.255.224	67.64.6.254 255.255.255.224	55

Table C: Router Details

Site: Guca **Router Name: GucaR1**

Int./Sub Interface Type/No.	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
g0/0/1	Connect to Guca Switch	-	-	-	-
g0/0/1.20	Connect to Printer	Printer	67.64.7.48	67.64.7.62	/28
g0/0/1.30	Connect to Leasing	Leasing	67.64.4.0	67.64.4.254	/24
g0/0/1.40	Connect to Marketing	Marketing	67.64.2.0	67.64.2.254	/24
g0/0/1.55	Management VLAN	Management	67.64.6.128	67.64.6.158	/27
g0/0/1.60	Connect to Security	Security	67.64.7.64	67.64.7.78	/28
g0/0/1.70	Connect to Tech	Tech	67.64.7.80	67.64.7.94	/28
g0/0/1.80	Connect to Vehicle Servicing	Vehicle Servicing	67.64.7.32	67.64.7.46	/28
g0/0/1.90	Connect to Business	Business	67.64.0.0	67.64.1.254	/23
g0/0/1.100	Connect to Server Farm	Server Farm	67.64.7.0	67.64.7.30	/27
s0/1/0	Connect to Ljubis R2	Serial Link	67.64.8.32	67.64.8.33	/30
s0/1/1	Connect to Mackat R4	Serial Link	67.64.8.36	67.64.8.37	/30

Site: Ljubis Router Name: LjubisR2

Int./Sub Interface Type/No.	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
g0/0/1	Connect to Ljubis Switch	-	-	-	-
g0/0/1.20	Connect to Printer	Printer	67.64.7.96	67.64.7.110	/28
g0/0/1.30	Connect to Leasing	Leasing	67.64.6.0	67.64.6.126	/25
g0/0/1.55	Management VLAN	Management	67.64.6.160	67.64.6.190	/27
g0/0/1.60	Connect to Security	Security	67.64.7.112	67.64.7.126	/28
g0/0/1.70	Connect to Tech	Tech	67.64.7.128	67.64.7.142	/28
g0/0/1.80	Connect to Vehicle Servicing	Vehicle Servicing	67.64.7.144	67.64.7.158	/28
s0/1/0	Connect to Guca R1	Serial Link	67.64.8.32	67.64.8.34	/30
s0/1/1	Connect to Lucani R3	Serial Link	67.64.8.40	67.64.8.41	/30

Site: Lucani Router Name: LucaniR3

Int./Sub Interface Type/No.	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
g0/0/1	Connect to Lucani S1	-	-	-	-
g0/0/1.10	Connect to Sales	Sales	67.64.3.0	67.64.3.254	/24
g0/0/1.20	Connect to Printer	Printer	67.64.7.160	67.64.7.174	/28

g0/0/1.55	Management VLAN	Management	67.64.6.192	67.64.6.222	/27
g0/0/1.60	Connect to Security	Security	67.64.7.176	67.64.7.190	/28
g0/0/1.70	Connect to Tech	Tech	67.64.7.192	67.64.7.206	/28
g0/0/1.80	Connect to Vehicle Servicing	Vehicle Servicing	67.64.7.208	67.64.7.222	/28
s0/1/0	Connect to Ljubis R2	Serial Link	67.64.8.40	67.64.8.42	/30
s0/1/1	Connect to Mackat R4	Serial Link	67.64.8.44	67.64.8.45	/30

Site: Mackat **Router Name: MackatR4**

Int./Sub Interface Type/No.	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
g0/0/1	Connect to Mackat Dist Sw	-	-	-	-
g0/0/1.10	Connect to Sales	Sales	67.64.5.0	67.64.5.254	/24
g0/0/1.20	Connect to Printer	Printer	67.64.7.224	67.64.7.238	/28
g0/0/1.55	Management VLAN	Management	67.64.6.224	67.64.6.254	/27
g0/0/1.60	Connect to Security	Security	67.64.7.240	67.64.7.254	/28
g0/0/1.70	Connect to Tech	Tech	67.64.8.0	67.64.8.14	/28
g0/0/1.80	Connect to Vehicle Servicing	Vehicle Servicing	67.64.8.16	67.64.8.30	/28
s0/1/0	Connect to Guca R1	Serial Link	67.64.8.36	67.64.8.38	/30
s0/1/1	Connect to Lucani R3	Serial Link	67.64.8.44	67.64.8.46	/30

s0/2/0	Connect to Mackat ISP R5	Serial Link	209.2.4.0	209.2.4.2	/30

Site: Mackat **Router Name: MackatISPR5**

Int./Sub Interface Type/No.	Description and Purpose	Network/VLAN Name	Network Address	Interface IP address	Subnet Mask /value
g0/0/0	External Server	-	147.19.2.0	147.19.2.1	/30
s0/1/0	Connect to Mackat R4	Serial Link	209.2.4.0	209.2.4.1	/30

Table D: Ljubis DHCP Server Pool IP Host Addresses

VLAN Name	*IP Address Pool Range*	*Subnet Mask /value*	*Default Gateway IP Address*
Ljubis Leasing	67.64.6.1 – 67.64.6.125	255.255.255.128	67.64.6.126
LjubisTechnical Support	67.64.7.129 – 67.64.7.141	255.255.255.240	67.64.7.142
Ljubisa Vehicle Services	67.64.7.145- 67.64.7.157	255.255.255.240	67.64.7.158

Table E: Statically Assigned IP Host Addresses

Server/ Printer etc Name	VLAN No	IP Address	Subnet Mask /Value	Default Gateway IP Address	Service/s Provided
LjubisPrinter	20	67.64.7.98	255.255.255.240	67.64.7.110	printing
Guca Printer	20	67.64.7.49	255.255.255.240	67.64.7.62	printing
Guca Business PC	90	67.64.0.1	255.255.254.0	67.64.1.254	Business monitoring
Guca Marketing Pc	40	67.64.2.1	255.255.255.0	67.64.2.254	Marketing
Guca Leasing PC	30	67.64.4.1	255.255.255.0	67.64.4.254	To do leasing
Server 1	100	67.64.7.1	255.255.255.224	67.64.7.30	As a server
Guca Security PC	60	67.64.7.65	255.255.255.240	67.64.7.78	For security purposes
Guca Tech Support PC	70	67.64.7.81	255.255.255.240	67.64.7.94	Technology Support
Guca vehicle Servicing PC	80	67.64.7.33	255.255.255.240	67.64.7.46	To service broken vehicle
Lucani Vehicle Servicing PC	80	67.64.7.209	255.255.255.240	67.64.7.222	To Service broken vehicle

Lucani Technical Support PC	70	67.64.7.193	255.255.255.240	67.64.7.206	For technical support
Lucani Printer	20	67.64.7.161	255.255.255.240	67.64.7.174	For printing
Lucani Sales PC	10	67.64.3.1	255.255.255.0	67.64.3.254	To do Sales
Lucani Security PC	60	67.64.7.177	255.255.255.240	67.64.7.190	For security Purposes
Mackat Printer	20	67.64.7.225	255.255.255.240	67.64.7.238	To do printing
Mackat Security PC	60	67.64.7.241	255.255.255.240	67.64.7.254	For security purposes
Mackat Sales PC	10	67.64.5.1	255.255.255.0	67.64.5.254	To do Sales
Mackat Technical Support PC	70	67.64.8.1	255.255.255.240	67.64.8.14	For technology support
Mackat Vehicle Servicing PC	80	67.64.8.17	255.255.255.240	67.64.8.30	For fixing vehicles
External Server0	100	147.19.2.2	255.255.255.252	147.19.2.1	For external network server

Table F: Wireless Access Point Details

Name	Model	SSID	Channel
Ljubis Wireless1	WRT300N	securityaccessgroup	1
Ljubis Wireless2	WRT300N	securityaccessgroup	6
Ljubis Wireless3	WRT300N	securityaccessgroup	11
Ljubis Wireless4	WRT300N	securityaccessgroup	16
Ljubis Wireless5	WRT300N	securityaccessgroup	1
Ljubis Wireless6	WRT300N	securityaccessgroup	6
Ljubis Wireless7	WRT300N	securityaccessgroup	11
Ljubis Wireless8	WRT300N	securityaccessgroup	16

Table G: NAT Pool for each VLAN

VLAN No	Starting IP Address	Ending IP Address
10	147.4.0.1	147.4.0.10
20	147.4.0.11	147.4.0.30
55	147.4.0.31	147.4.0.41

60	147.4.0.42	147.4.0.60
70	147.4.0.61	147.4.0.80
80	147.4.0.81	147.4.0.99

Table H: Server Static NAT

Server Name	Static Inside IP address	Static Outside IP address
Server1	67.64.7.1	147.4.0.111

Table I: Record of ACL Testing Guca

Source Host	Destination Host	Protocol	Expected Result	Achieved
Marketing	Leasing	any	Deny	Yes
Vehicle Servicing	Any host in a VLAN outside Vehicle Servicing	any	Deny	Yes
Any host outside Tech Support VLAN	Technical Support	any	Deny	Yes
Technical Support	any	any	Permit	Yes
Any	Internet Web Server	http	Permit	Yes
Any	Any not blocked by rule above	any	Permit	Yes