Draft (barebones version of the report logic)

Yellow highlight means we need to fix something there!!!

//set up a content list with all the headings:+ set relevant tables in their areas and fix table data where needed and if stated

**Discussion of Network Design Issues**

**1.IP VLSM Design (4 marks)**

Efficient use of IP address allocation to the necessary groups via VLSM

Here we decided to first create subnets for each group in each areas (like Guca-printer, Ljubis-sales,etc), order them according to size needed for each (max to min size) using staff number after considering percentage growth of 30%.

Here you can see that we had kept 1 space extra in each subnet's "needed space" compared to the calculated value that comes when considering percentage growth. That's because we kept space for gateway address which will be needed for inter-vlan communication to occur between the different vlan groups that will be created

We did it in this manner to ensure that all the groups in each area are accounted for and have thier own subnet. Thus it makes it easier to enforce security policies, breaking up broadcast domains, reduce network traffic,etc

For printers, we created different subnets in each network too as it didnt seem logical to merge them with other group's subnets. Furthermore we kept space for 2 for both

For Server Farms, the number had been left to us, so we had decided to keep space for 6 servers and 1 gateway for now for as we assumed the company to have big, powerful servers with large storage and processing capabilities and thus decided to keep one server dedicated for each group (ie for leasing, marketing, business, sales, vehicle support and printer) except for security and tech support. In the vlsm you can see that that in the end it got 14 host address spacing thus can be used to allocate more servers if need be. (didnt keep for security as we assumed security will be for building protection purposes and didnt think they needed to have any server dedicated for them and didnt keep for tech support as they would mainly be maintianing other servers and entwork itself and thus again didnt need any dedicated server)

currently, as you can see in the table, we have used only 24% of the available network and still have 8190 IPs available in the network even while considering staff expansion. Furthermore, we have also considered all the hosts on each group in each area and have allocated the subnets both efficiently and ensuring that the restrcitions they had given are met. Thus we can gurantee that they meet company specifications and in some cases, even exceed it.

(for instance we have added links between the routers to ensure there is redundancy between the routers)

/////paste the table A here

(as we presumed security will only be needed for on site security and thus didnt require seperate server whilest )

**2.Routing Protocols (4 marks)**

In here we have used the routing protocol of OSPF with MD5 authentication, bandwidth allocation of 256, passive interface setup for connected networks (ie server connection to internal routers, subinterfaces on each internal routers), default route to ISP on gateway router and its advertisement to other internal routers, static route from ISP to back to internal network and SSH setup on Guca router itself. All of these had been done not only to fulfill the requirements stated but also to maintain best practise.

For instance, we have used MD5 authentication as it provides more security that plain text authentication (as it calculates Hash from OSPF packet and password) and thus prevents "sniffer attack" on network (like protocol analysers like wireshark capturing packets and seeing passsword for plain text authentication) and thus ensure that only authenticated neighbouring routers can communicate with each other. So no unauthenticated gateway router can communicate with the Main office router (Guca)

we have used bandwidth allocation of 256 on all internal serial links ensuring that all the links have the same priority for traffic

//need better reasoning for this if possible

we have also used passive interface for the connected networks to ensure that unneeded updates are not sent to the lans and thus bandwidth and CPU resources are not wasted. Furthermore, it also prevents a security risk as routing tables informaton can be used to reveal network topology.

//maybe say the last part a bit better?

we have kept the default router only on the gateway router to ensure that it knows to send out all traffic destined for the internet (ie traffic sent to any ip that doesnt fall in the range allocated to any group's subnet) and made it broadcast it to every other internal router. That way not only do we not have to configure it on each router individually, but also if a router on the way goes down, the routers will automatically configure a new route to the internet dynamically (utilising the redundant links they have with one another)

we have kept static route from ISP back to network to ensure that traffic can pass from internet into the network (if no ACLS are there to prevent it)

//say this in a better way or use a better reasoning!

We have also set up SSH on Guca as per requirement so that Technical support group can remotely and securely access it to modify any configuration or toubleshoot if need be, whilst ensuring that transfer of information remains secure via encryption

**3.Switches: VLANs, STP, EtherChannel (4 marks)**

We have set up the following vlans (....) to ensure all groups in each area have been accounted for. We have used different vlans as we decided to keep them in different subnets so as to keep the broadcast domain small and reduce unnecesary network traffic occuring on a large area of the network.

//say the ending part in a better way/ use a better reasoning for keep the groups in different vlans rather than in same vlans

Furthermore, we are using Vlan 33 for management instead of Vlan 1 as Vlan 1 is a default vlan which is a well-know configuration abused by attackers

//need more points for why we shouldnt use vlan 1 for management vlan, like maybe say "everyone knows it so......."

Also, we are turnign off unused ports so that attackers cant just plug in malicious devices into an unused port and get unauthorized access to the network itself

Moreover we turned on switchport security in Ljubis which set up the default shutdown violation mode (causes interface to become error disabled when violation occurs and sends an SNMP trap notification), max mac address allowed to be 1, etc which can be seen in the screenshot below:

//take screenshot of the port security that has been set on the interface in Ljubis

Also, we have set up SSH on the Guca switches as per requirement so that Technical support group can remotely and securely access it to modify any configuration or toubleshoot if need be, whilst ensuring that transfer of information remains secure via encryption

We have used STP in MAckat to ensure that not only does layer 2 loops not form, but also to ensure that access switches may never become root switches. This has been done by configuring distribution switch as root bridge (ie rot primary) for all vlans. This is because the distribution switches would handle local routing, filtering, traffic balancing, Qos priority, etc and thus are better suited to be root switches in a network achitecture.

We have also set etherchannels on switches in the Lucani site to ensure that increased bandwidth and redundancy can be provided to it as now multiple logical links are considered as a single logical link to trasfer data between them.

**4.Wireless LANs and Site Layout for the specified site (6 marks)**

Here we had been tasked to provide wireless Lan for the Lucani site as per specification so that site security group can access the network through it. The configuration has been done in the prototype which you can see in the screenshot and the table below

(provide a screenshot of the wireless network config ip, mask and gateway and SSID from the wireless router config part)

While considering deployment in reality we had been stumped at first due to lack of clarity in instruction and had been confused over whether to deploy through the entire site area (like how eduroam has been set up in our university) or whether we should only apply inside the building. In the end we calculated for both and realised that if we wanted to cover the entire site we would need at least 635 Access points (APs) while considering 15% overlap for seemless transition from 1 AP to another.

(calculation reference was done in: https://www.engineeringtoolbox.com/circles-within-rectangle-d\_1905.html )

Now this exceeded the number of hosts required by even Guca Business group (which had the largest number of hosts) by almost 2-3 times.

Thus, we decided to do only for the building area instead. So we opened the website in the link and inputted in the values for rectangle with dimensions of lucani 225metres x 30metres and the router radius of 45m (this is for WTR300N wireless router which we are using in the prototype and we are using the radius of its range inside the building)

//need the reference link for the website that showed that radius of the wireless is 45m indoors

Unfortunately, since the building had too short width the website kept giving us the wrong outputs as it would consider the total area only and not notice the fact that its width was far shorter than the range for the router.

So, instead we calculated it manually. We took the length of the building and devided it by diameter of our router's range which gave us 2.5 APs. So considering the fact that we needed 15% overlap, we decided to just keep 3 instead for full coverage and smoothless transition. You can see that in the diagram below which we had done in desmos graph paper

//do we need to give the datas we used to make the diagram in desmos to prove that we have indeed kept 15% overlap in area?

furthermore, we have alos tested that ping works which you can see in the following screenshot

//attach a screenshot of it being able to ping any other pcs

**5.DHCP (3 marks)**

According to instructions given we have provided DHCP for the Ljubis site only for the prototype. Here we have configured dhcp pools for each groups in the DHCP server pool as you can see in the table below. We had done this so that we dont have to statically configure ip address and gateways on each pcs and instead can do so automatically. Thus both chances of error in IP configuration and the load on the network administrator (and also the tech support group) reduces.

Note we have set static ip for printer and not dynamic one as its a company resource that will be used by all and thus will need to have a static ip, not a dynamic one.

//paste the table D (DHCP ljubis)

//fix the table-----> we set static ip for printer, not dynamic!

//so remove it from the table

Although we configured the IPs of the rest statically, by doing it though DHCP in Ljubis, we have shown a template for what set of configurations are necessary to set up DHCP for the rest if need be and thus have both followed requirements and also maintained oppurtunity for reusability and scalability

//need to improve this part. specially last line

**6.NAT (4 marks)**

Since the Ip address given to us were in public range, we had been a bit confused at the start regarding whether nat was really required or not. But since the instructions seeked it, we configured that as well.

This had taken a long period of time as we had to find the command for static ip NAT, configure them for all the servers in the server farm

////not sure about this part:

(note here we did for all the hosts in the server allocated size instead of needed host range so that if server number increases, we still will have enough nat to acomodate for it)/////,

and finally configure the remaining for remaining groups.

Since we had a lot of public ips left we had to decide how to allocate them for the dynamic one, like wehther to devide it equally amoung the rest or to give them only that which is needed. In the end we had decided to only give as must each group have in thier

///note sure about this part as not know which size we had used. need to see the ip allocation in nat config for that: "allocated size"///

. Thats because:

a) we wanted to keep some space in Nat in case the company decided to add new groups later in the future and not need to reset all the previous nat config to accomodate for it

b)we were already using needed size (which we had decided using number of hosts including expansion wherever needed and gateway address consideration). Thus there were already more than enough public ips allocated for each group. So no need to have any more.

//maybe write this point a bit better, specially the last line?

//also did we use needed size or allocated sie?

c) we are also overloading it which allows many internal hosts to share the same public address and thus further ensuring that more than enough public ips are available for each group's use

**7.Security and Access Control Policies (4 marks)**

Here we have maintained security by the following:

a) setting up MD5 authentication in OSPF link between Guca and Mackat to prevent "sniffer attacks" (details stated in the router paragraph before)

b)Configuring passive interface for subinterface (ie connnected networks on those subinterfaces) to prevent leaking of the route information table (details stated in the router paragraph before)

c)not using Vlan 1 as management vlan as it is a default vlan in all switches and known by all (details stated in switch paragraph before)

d)shutting down unallocated switchports to prevent unauthorised access to network (details stated in the switch paragraph before)

e)setting up the basic switchport security for the Ljubis access switches to ensure that only one device is attached to the port and ensure that if its not maintained, the port will shutdown and prevent access (details stated in the switch paragraph before)

f) configuring distribution switches as root bridge instead of access switches in Mackat as it is better suited to become root compared to access switches (details stated in the switch paragraph before)

g) using SSH to access both switches and router in Guca to ensure secure transfer of information (details stated in both router paragraoh and switch paragraphs)

h) setting up PPP and Chap authentication on link between gateway router and ISP router to validate the identity of the two routers before enabling communication to occurs between them

i) using ACLs to ensure that the public ips in Nats are only used by groups dedicated for it to ensure no abuse of Public ip address occurs

j)using ACls to ensure that Pcs in Marketing Vlans are denied access to Leasing Vlans (as per requirement)

k)using ACls to ensure that Pcs in Vehicle servicing Vlans are denied access to all other Vlans (as per requirement)

l)using ACls to ensure that All Pcs in all other vlans are denied access to Tech support Vlans (as per requirement)

m)using ACls so that only relevant groups can access the servers Lan and no other. Here we are letting tech support access it for maintainence purpose, and for all groups except security group access it in order to store and retrieve data (ie not letting security group access it as they dont need the use of any of the servers)

n)using ACls to ensure that all other vlans have access to internet unless denied by any previous ACls stated before. This is so that the Pcs in the vlans and communicate with one another for thier daily purposes

o)using ACls to ensure that all other vlans have access to other vlans unless denied by any previous ACls stated before. This is so that the Pcs in the vlans and communicate with resources on the internet for thier daily purposes

p)Not use "permit any any" in acls and instead specifically mention all vlan cases for the ACLS as we wanted to keep things secure and assumed that the company did not wish to allow outsiders to gain access to their network in any way

**8.System Testing and Verification Strategy (6 marks)**

//give screenshot of at least one instance of each testing

We have testing the following configurations in the prototype:

a) full OSPF configuration (MD5, bandwidth, Passive interface, default route to isp on gateway router and its advertisement to internal routers) + non OSPF config(static route on isp back to internal network + proper ip config + subinterface setup, ssh on Guca router, DHCP set up on Ljubis router, PPP and Chap set up on ISP and gateway link

1)sh run ------(on any Guca or Mackat router)---> Then look at individual interface where MD5 had been set

//see if any other way to test this

2)sh run------(on any internal router)---> See bandwidth set for the serial link

3) sh run ------(on any internal router)---> See router ospf

//see if any other way to test this

4)sh run -------(on the gateway router)-----> see just after the router ospf chunk + "default info originate" keyword in ospf chunk

+sh ip route --------(on gateway router)----> see static route or log starting with "S"

+sh ip route--------(on any internal router)----> see the gateway of last resort set to what

5)sh ip route --------(on ISP router)----> see static route or log starting with "S"

6)sh run ------(on any internal router)---> check the subinterfaces

+sh ip int b ------(on any internal router)---> see the subinterfaces

+ping .......... (any ip for any pcs/ switch on 1) to own vlan, 2) to different vlan on same router, to different vlan on different router, to internet server )

7)sh run ------(on Guca router)---> see the ending login part and "ssh" keyword

8)sh run ------(on Ljubis router)---> see the dhcp pool part

+on any pc in ljubis -----> ipconfig/ release and ipconfig/renew and see whether it takes a new ip from the list allocated to it's group

9) sh run ------(on mackat router and mackat isp)---> see the interface to isp link/ mackat router link and see encpasulation ppp and ppp authentication chap

b)on switches (interface vlans, normal vlans + access ports, used ports on + un-allocated ports admin shutdown, Ljubis access switches with port security, Mackat distribution switches as root bridge, Guca switches set with SSH access, proper Ip configuration on all switches with access and trunking at proper places, ensruing vlan names exist on distribution switches, etherchannel set up)

1)sh ip int b----(on any switches)----> see vlan 33

2)sh vlan b-----(on any access switches)---> see vlanss and thier ports

3) sh ip int b----(on any switches)----> see status and protocol

4) sh run----(on access switches in ljubis)----> see interface

5)sh run ---(on distribution switch in mackat)----> see spaning tree vlan .... part for both set for all vlans on it and also priority set value

6)sh run ---(on any switch in guca)----> see login part and ssh keyword

7)sh ip int b ---(any switch)----> up and up + vlan 33 ip

+ping ......(any ip for any pcs/ switch on 1) to own vlan, 2) to different vlan on same router, to different vlan on different router, to internet server ) (done before in router part)

+sh int trunk------(on any switch)----> see encapsulation, allowed and active vlans

+sh run----(on any switch)---> see interface

8)sh vlan b --(any distribution switches)---> see all vlanss exist there which were being allocated to in the access switches below

+sh int trunk------(on any switch)----> see encapsulation, allowed and active vlans

9) sh etherchannel-summary ---(on Lucani access and distribution switches)-------> see (su) in port channel and (p) beside the ports and port ids

c) wireless router set up

see the configuration set for it in packet tracer

+ping ......(any pcs)-------( from the laptop on wireless)----->

(any ip for any pcs/ switch on 1) to own vlan, 2) to different vlan on same router, to different vlan on different router, to internet server )

d)Nat configuration on gateway router

sh run-----(on the mackat router)-----> see the Nat part

+sh ip nat translations

e)ACL configuration on each routers where respective vlan groups exist

sh run---(on router where it has been set up)-----> ACL

+sh access-list --(on router where it has been set up)-----> and check counter

+ping ......(relevant pc ip) and see success or fail according to acl

+sh access-list --(on router where it has been set up)-----> and check counter again to reflect change