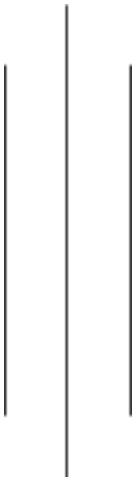
TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS

A Project Report on
Network Design of **Yarsa- Group of Companies**

For the partial completion of the course on **Computer Networks**



Submitted By:
Name: Roshani Poudel
Roll No: 077BCT071
Group: CD

Submitted To:
Department of Electronics and
Computer Engineering

Project Overview- Yarsa

This network project is a thoughtful realization of the network of a group of companies, Yarsa. A group of companies working in 3 areas of technology, as Yarsa Tech, a Made in Nepal electronics brand; Yarsa Games, a game studio developing popular games and Yarsa Labs, working on continuous innovation was the motivation behind choosing this particular company. The network design was an interesting project to work on, visualizing what the company's network topology might look like, as it grows to thousands in terms of the capacity of the devices.

The three companies, Yarsa Games, Yarsa Tech and Yarsa Labs are shown in the network, imagined to be each in a floor of a building. A control room for admin is connected to the Border router for overall control, and assigned a separate area, Area 4. It handles the hosting and resolving of the main website, *yarsa.com* in a single server. The Isp router has a Root DNS server and a web server on it's network. Each company has it's own DNS and Web server. DHCP servers are shown only as example in a few subnets, and have to be added in all of the subnets in practical use-case, to practice simplicity of IP assignment. Area 0 is the backbone of the entire network through which the inter area communication occurs as well as the connection with the ISP happens through this area. The ISP is connected via a border router and the other areas are connected via their corresponding area border routers. The taken IP address is 10.0.0.0/ 21 supporting (at max) a total of 2046 hosts.

Area Configuration:

Area 1: Yarsa Games
Coded in orange color, the area for Yarsa Games includes subnets for Creation room and Control Room. Creation room has 3 VLANs, for Managers, Senior Developers and Junior Developers. Each switch is connected to Development, Animation and Testing PCs. Control room is an area for group monitoring and control activities on the system and also includes DNS server and Web server to host the *games.yarsa.com* website.

Area 2: Yarsa Labs
Coded in green color, the area for Yarsa Labs includes subnets for Research, Development and Operations. Research subnet has a web server that hosts the *labs.yarsa.com* address, and PCs for independent or group research in the lab. Development subnet is strictly for researching for innovation and working on research projects. AP has been added for ease. DHCP server also assigns IP for connected devices. Another subnet, for Operations handles the overall operations happening behind the scenes, and also hosts DNS server that resolves the DNS query.

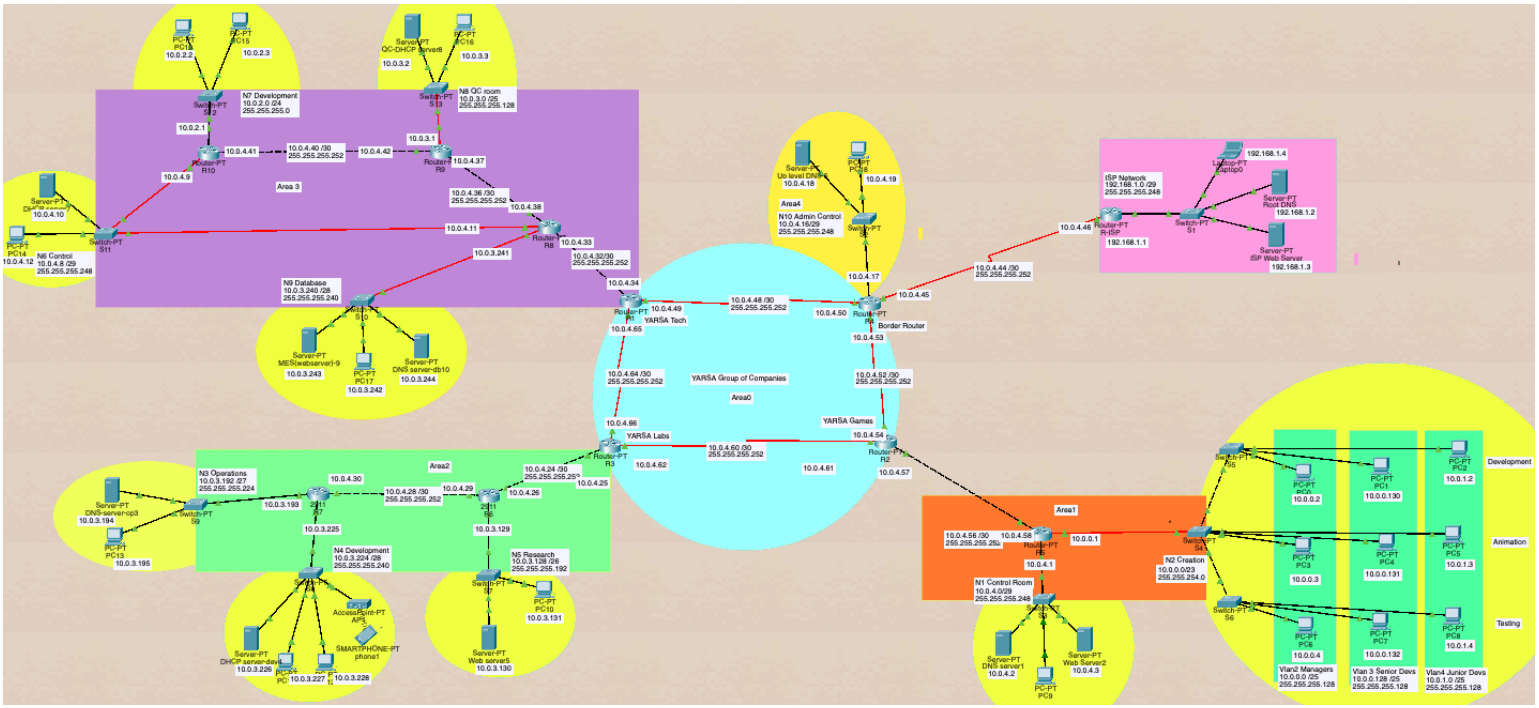
Area 3: Yarsa Tech
Coded in Purple color, Yarsa Tech is an electronics manufacturer and has four different subnets. The first one is for database storage, that also hosts the DNS and web servers for this company. Development subnet is for development of technological tools, QC room subnet for testing the quality standards, and a Control subnet for handling control operations.

There is a 3 level hierarchy of DNS server,i.e. DNS server (Local), Up level DNS and Root server. The configuration is done such that the addresses **yarsa.com, labs.yarsa.com, games.yarsa.com, tech.yarsa.com and roshni.com** can be accessed from any device on the whole network.

Yellow color in the Network topology refers to a subnet each. Pink color for ISP network and Cyan color for area 0 (backbone area).

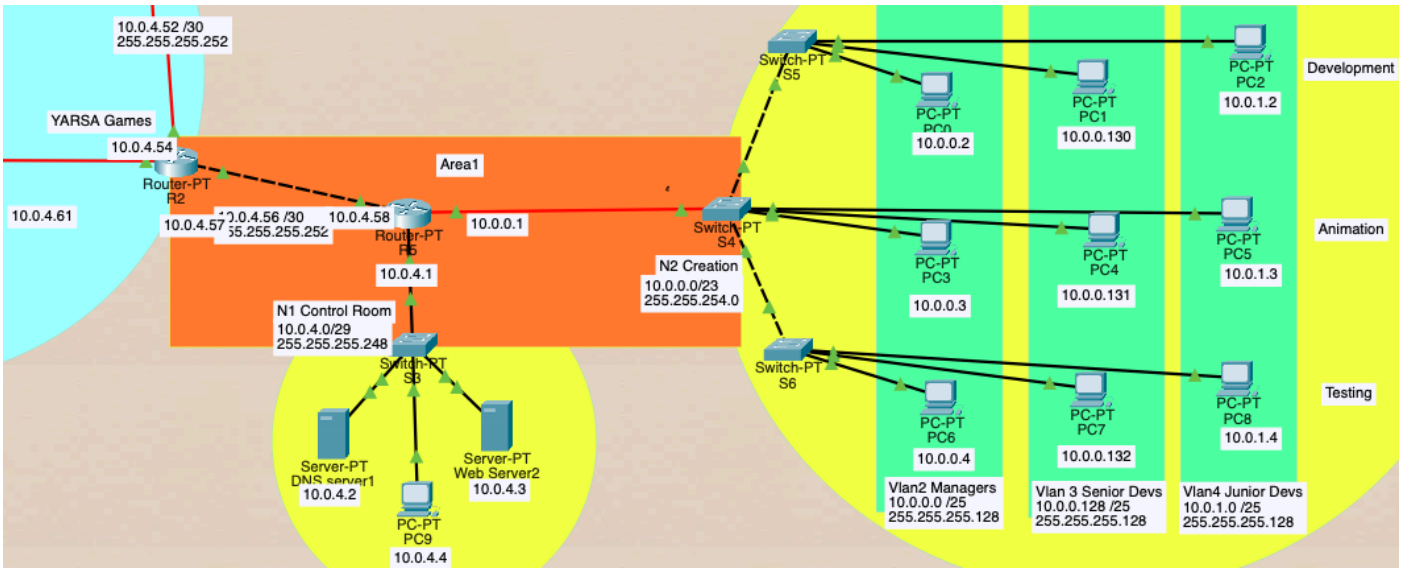
Network Implementation

Realisation of the Network of the group of companies, Yarsa:

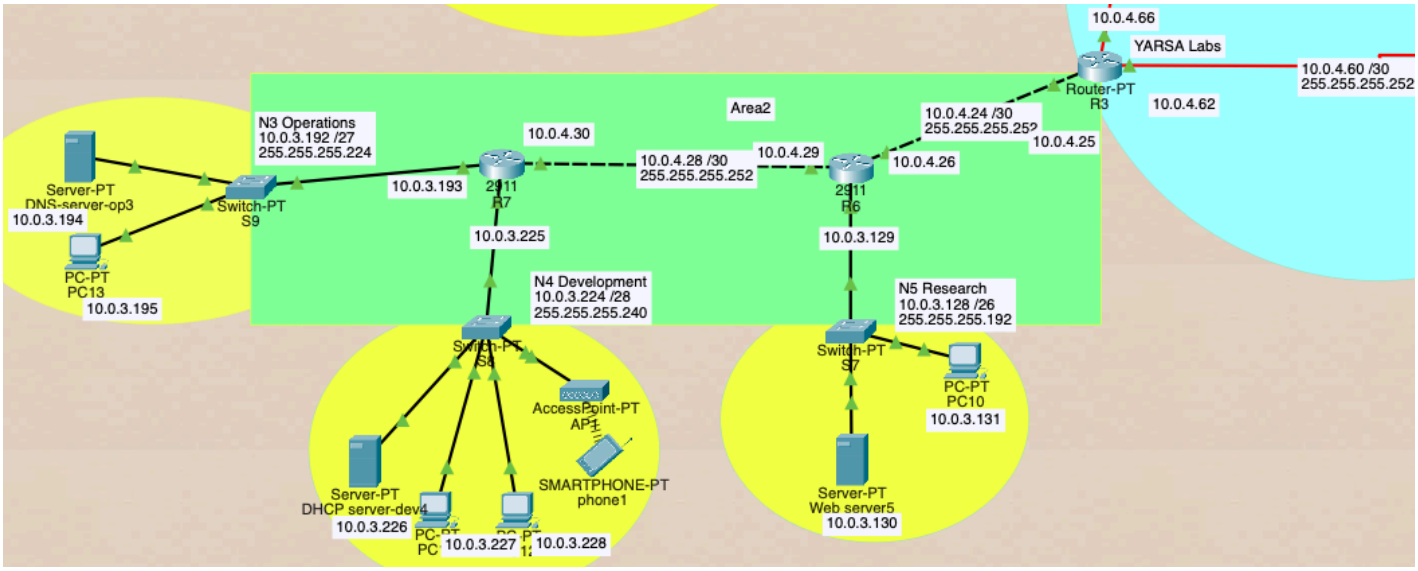


Area 0, Area 4 and ISP:

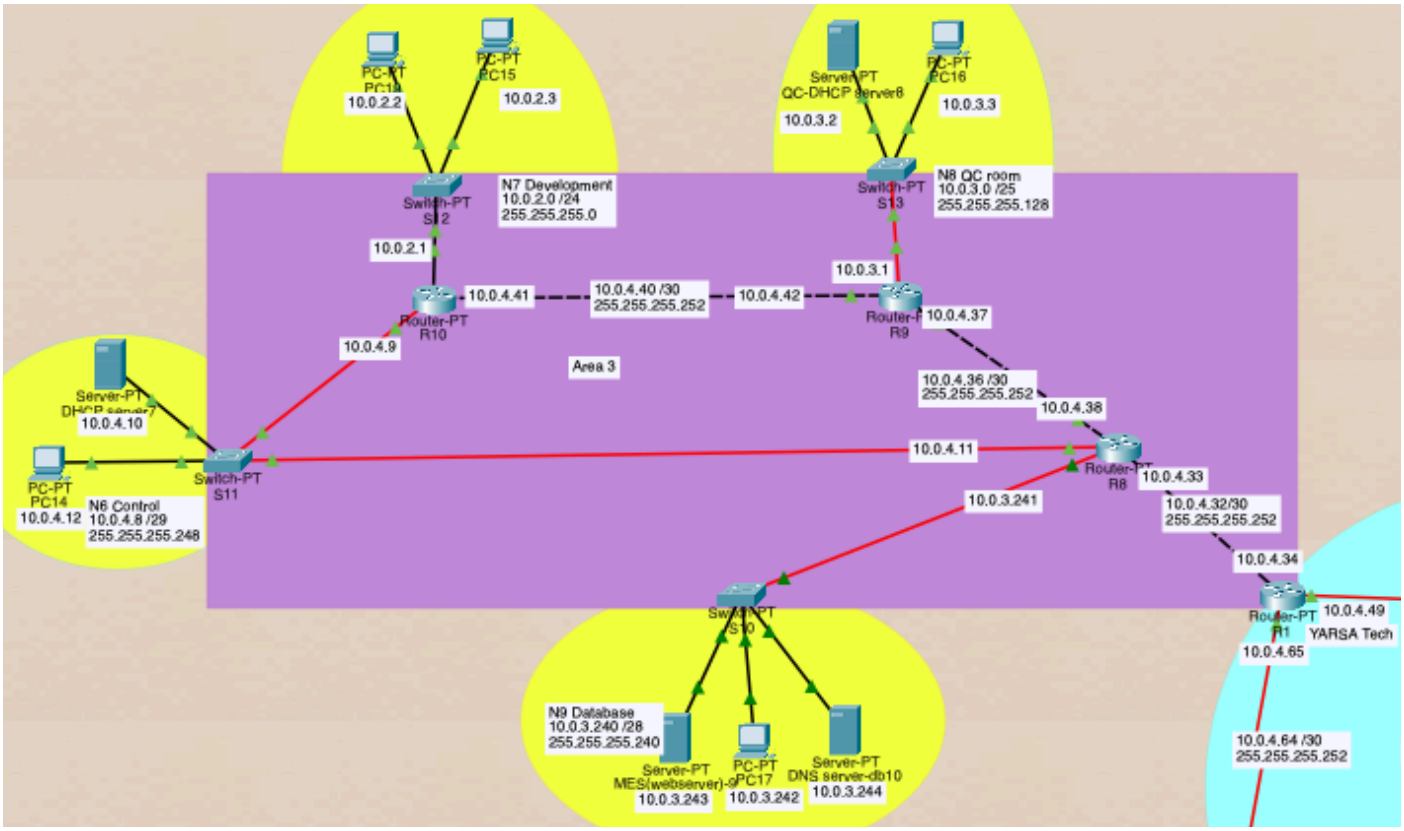
Area 1(Yarsa Games):



Area 2 (Yarsa Labs):



Area 3 (Yarsa Tech):



Ip address: 10.0.0.0 /21

Subnet Division with VLSM:

Subnet	Hosts Required	Subnet Mask	Subnet mask bit	Total IPs	Network Address	Broadcast Address	Usable IP Range	Wildcard Mask
N2	350	255.255.254.0	/23	512	10.0.0.0	10.0.1.255	10.0.0.1 - 10.0.1.254	0.0.1.255
N7	240	255.255.255.0	/24	256	10.0.2.0	10.0.2.255	10.0.2.1 - 10.0.2.254	0.0.0.255
N8	120	255.255.255.128	/25	128	10.0.3.0	10.0.3.127	10.0.3.1 - 10.0.3.126	0.0.0.127
N5	60	255.255.255.192	/26	64	10.0.3.128	10.0.3.191	10.0.3.129 - 10.0.3.190	0.0.0.63
N3	28	255.255.255.224	/27	32	10.0.3.192	10.0.3.223	10.0.3.193 - 10.0.3.222	0.0.0.31
N4	13	255.255.255.240	/28	16	10.0.3.224	10.0.3.239	10.0.3.225 - 10.0.3.238	0.0.0.15
N9	10	255.255.255.240	/28	16	10.0.3.240	10.0.3.255	10.0.3.241 - 10.0.3.254	0.0.0.15
N1	6	255.255.255.248	/29	8	10.0.4.0	10.0.4.7	10.0.4.1 - 10.0.4.6	0.0.0.7
N6	6	255.255.255.248	/29	8	10.0.4.8	10.0.4.15	10.0.4.9 - 10.0.4.14	0.0.0.7
N10	5	255.255.255.248	/29	8	10.0.4.16	10.0.4.23	10.0.4.17 - 10.0.4.22	0.0.0.7
Net-ISP	5	255.255.255.248	/29	8	192.168.1.0	192.168.1.7	192.168.1.1 - 192.168.1.6	0.0.0.7

Point to point connections:

2 hosts Connection	CIDR Prefix	Subnet Mask	Total IPs	Network Address	Broadcast Address	Usable IP Range	Wildcard Mask
R3 - R6	10.0.4.24/30	255.255.255.252	4	10.0.4.24	10.0.4.27	10.0.4.25 - 10.0.4.26	0.0.0.3
R6 - R7	10.0.4.28/30	255.255.255.252	4	10.0.4.28	10.0.4.31	10.0.4.29 - 10.0.4.30	0.0.0.3
R1 - R8	10.0.4.32/30	255.255.255.252	4	10.0.4.32	10.0.4.35	10.0.4.33 - 10.0.4.34	0.0.0.3
R8 - R9	10.0.4.36/30	255.255.255.252	4	10.0.4.36	10.0.4.39	10.0.4.37 - 10.0.4.38	0.0.0.3
R9 - R10	10.0.4.40/30	255.255.255.252	4	10.0.4.40	10.0.4.43	10.0.4.41 - 10.0.4.42	0.0.0.3
R4 - RISP	10.0.4.44/30	255.255.255.252	4	10.0.4.44	10.0.4.47	10.0.4.45 - 10.0.4.46	0.0.0.3
R1 - R4	10.0.4.48/30	255.255.255.252	4	10.0.4.48	10.0.4.51	10.0.4.49 - 10.0.4.50	0.0.0.3
R2 - R4	10.0.4.52/30	255.255.255.252	4	10.0.4.52	10.0.4.55	10.0.4.53 - 10.0.4.54	0.0.0.3
R2 - R5	10.0.4.56/30	255.255.255.252	4	10.0.4.56	10.0.4.59	10.0.4.57 - 10.0.4.58	0.0.0.3
R3 - R2	10.0.4.60/30	255.255.255.252	4	10.0.4.60	10.0.4.63	10.0.4.61 - 10.0.4.62	0.0.0.3
R1 - R3	10.0.4.64/30	255.255.255.252	4	10.0.4.64	10.0.4.67	10.0.4.65 - 10.0.4.66	0.0.0.3

Server IP Configurations:

Server Name	Network Name	Network Address	Server IP	Description
DNS Server1 (Yarsa Games)	N1	10.0.4.0/29	10.0.4.2	Located in the control network of Yarsa Games, managing DNS services for domain resolution.
Web Server2 (Yarsa Games)	N1	10.0.4.0/29	10.0.4.3	Located in the Control network of Yarsa Games, hosting its web services.
DNS Server3 (Yarsa Labs)	N3	10.0.3.192/27	10.0.3.194	Located in the Operations network of Yarsa Labs, managing DNS services for domain resolution.
DHCP Server4 (Yarsa Labs)	N4	10.0.3.224/28	10.0.3.226	Located in the Development network of Yarsa Labs, issuing IP addresses to devices in the network.
Web Server5 (Yarsa Labs)	N5	10.0.3.128/26	10.0.3.130	Located in the Research network of Yarsa Labs, hosting its web services.
DNS+ Web Server (up level in Admin Area)	N10	10.0.4.16/29	10.0.4.18	Located in the Admin Control network, managing DNS services in 2nd level of DNS.
DHCP Server7 (Yarsa Tech)	N6	10.0.4.8/29	10.0.4.10	Located in the Control network of Yarsa Tech, issuing IP addresses to devices.
DHCP Server8 (Yarsa Tech)	N8	10.0.3.0/25	10.0.3.2	Located in the Quality control network of Yarsa Tech, issuing IP addresses to devices.
MES(web) Server9 (Yarsa Tech)	N9	10.0.3.240/28	10.0.3.243	Located in the Database network, hosting MES services.
DNS Server 10 (Yarsa Tech)	N9	10.0.3.240/28	10.0.3.244	Located in the Database network, handling DNS services.
Root DNS (ISP network)	ISP network	192.168.1.0/29	192.168.1.2	To resolve all queries at the ISP
ISP web server	Isp network	192.168.1.0/29	192.168.1.3	To host multiple requests at the ISP

Project Description

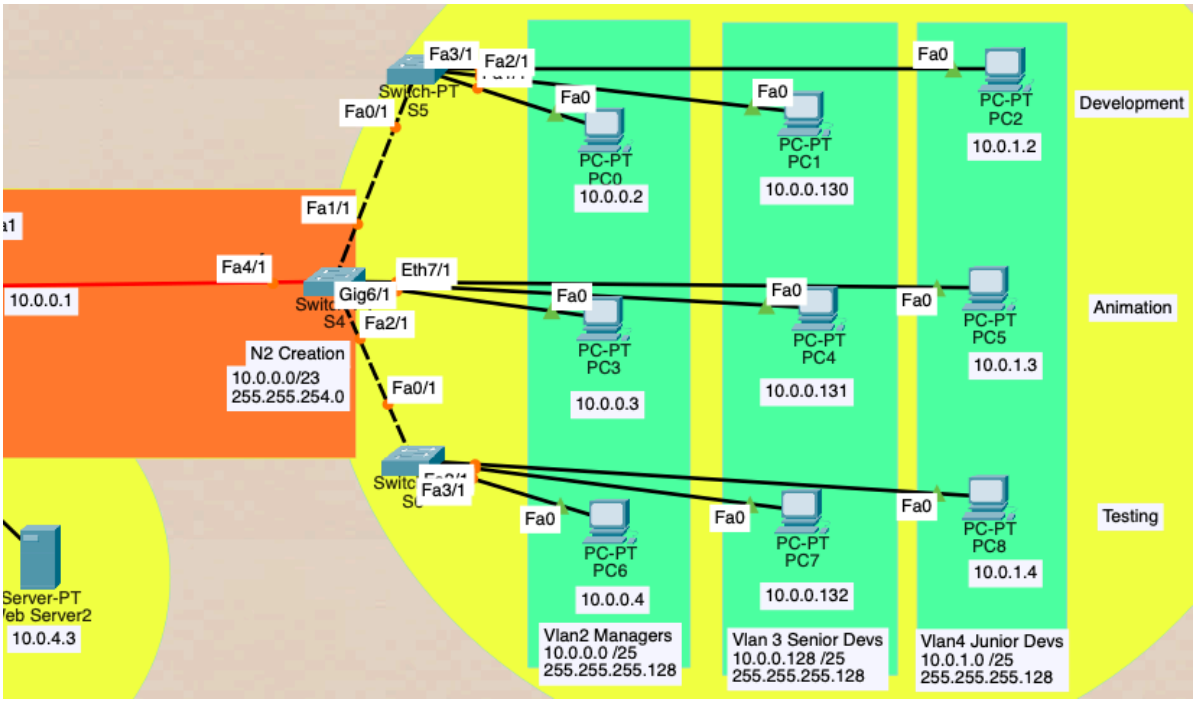
As per the requirement, the routers were renamed, password protected and telnet was enabled. For the labeling, DNS servers are suffixed by DNS, the web servers are labeled by web and the networks themselves are named along with their IP and subnet mask.

All the pings from each device to the another was successful and the shortest route was configured to follow. Default addresses were routed from all routers towards the ISP router and the CIDR prefix was used to route requests from ISP to our network.

A change from the proposal was made to isp router, only 2 ips were available earlier. Now, 6 total devices can be added. This was a shortcoming of the evaluation during the proposal submission.

VLAN Assignment

For VLAN configuration, subnetting has been done inside the given subnet. The Net-ID for network2, 10.0.0.0 /23 was further divided and after OSPF, each VLAN is treated as a separate network. InterVLAN routing is also configured. The aim of this configuration is to allow separate employees in different sectors(development, animation or testing) to meet up with the same level of people, i.e, seniors, juniors and managers, so that they can work and execute together.



The default gateway for the VLANs are: VLAN2- 10.0.0.1, VLAN3- 10.0.0.1289, and VLAN4- 10.0.1.1.

OSPF was done in between routers to exchange their information with the neighboring routers. Different areas were created to segregate the network traffic.

Connectivity Tests:

The Ping Test was done to ensure that all devices on the network are properly configured, and all routes are properly setup. All PCs successfully pinged any other PC in the network, that showed the network connectivity without any issues and failure.

The default routes were also tested, by testing for a random address on the Internet. Routing tables were carefully observed to ensure OSPF configuration. In order to debug, traceroute command and simulation modes were used.

DNS Verification:

Web server access test were carried out to confirm connectivity and access of Web Servers from different devices inside the network. All PCs were able to browse the web servers "tech.yarsa.com", “labs.yarsa.com” and “games.yarsa.com” hosted in the level 3 DNS, without any issues, confirming that the web servers are accessible and functioning as expected. In up level (level 2) DNS, "yarsa.com" was hosted without any issues and in root level, “roshni.com” was hosted.

In DNS server of Yarsa Tech, any Address record request for tech.yarsa.com would be resolved to its own Web server. Else, any other com Name Server (NS) record would be passed to up_level, that holds the address of up_level DNS. Similar configs were done for yarsa games and yarsa labs.

No.	Name	Type	Detail
0	com	NS	up_level
1	tech.yarsa.com	A Record	10.0.3.243
2	up_level	A Record	10.0.4.18

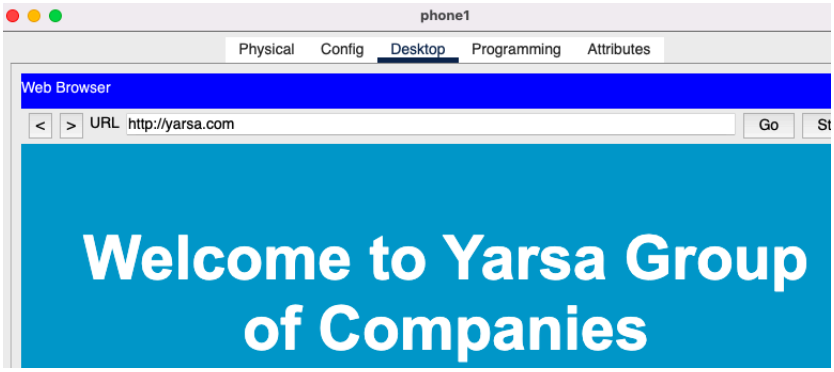
In up level DNS, the A record request for yarsa.com would be passed to the web server hosted in this network itself. Any other request coming for *.yarsa.com would be resolved to their own DNS server, eg: if a request for games.yarsa.com is received, the dns request is passed out to the DNS of games.yarsa.com network. Any other request (indicated by .) is passed on the root for resolving.

No.	Name	Type	Detail
0	.	NS	root
1	games.yarsa.com	NS	games_dns
2	games_dns	A Record	10.0.4.2
3	labs.yarsa.com	NS	labs_dns
4	labs_dns	A Record	10.0.3.194
5	root	A Record	192.168.1.2
6	tech.yarsa.com	NS	tech_dns
7	tech_dns	A Record	10.0.3.244
8	yarsa.com	A Record	10.0.4.18

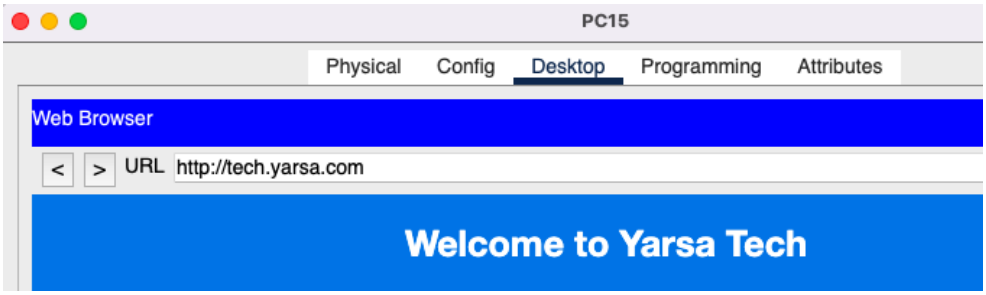
In root DNS, roshni.com is resolved to root web server. Any request for yarsa.com is passed to the up_level_DNS server.

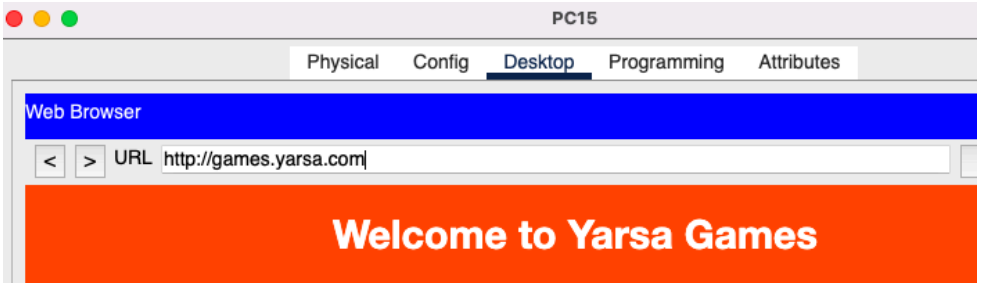
No.	Name	Type	Detail
0	roshni.com	A Record	192.168.1.3
1	up_level2	A Record	10.0.4.18
2	yarsa.com	NS	up_level2

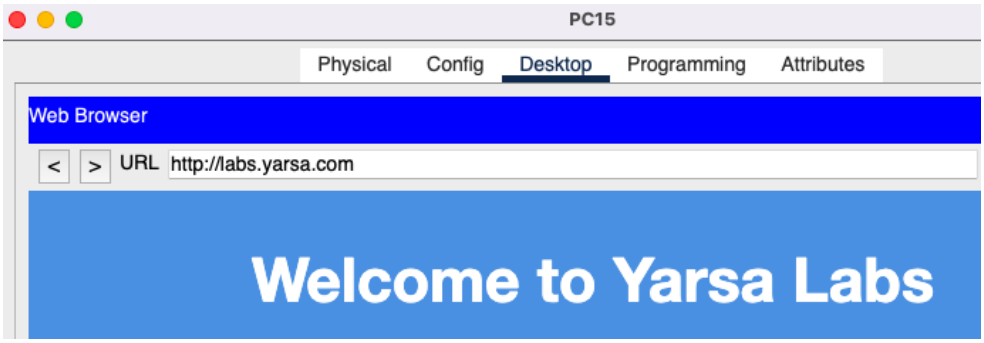
From phone(area 2):



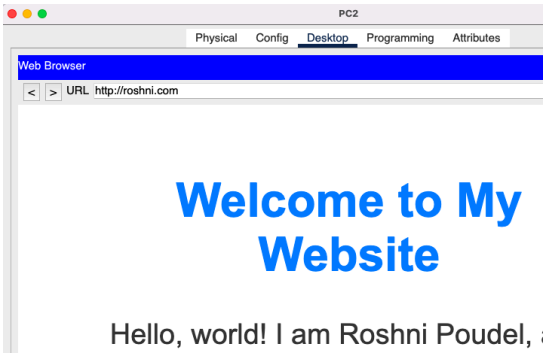
From Area3 (of yarsa tech) :







From vlan PC2 to root DNS for resolving, the request was successful.



Conclusion:

The network design for Yarsa Company was successfully implemented using Cisco Packet Tracer. The network was divided into four OSPF areas to efficiently manage different companies and admin control section. The IP addressing scheme was carried out using VLSM to ensure optimal use of IP addresses. The devices were correctly configured and interconnected, and VLANs were established to segregate network traffic effectively. Each of the internal networks were reachable from any computer and all the Internet Traffic was forwarded to the Upstream Service Provider. Similarly, the network packets were forwarded to our network from ISP without Dynamic routing using minimum possible route entries. Finally, each of the servers were made operable so that they can be accessed from any computers and in this way, our objective for this project was fulfilled.