Project Brief: Hospital Management System Network Design and Implementation

Syed Arshaq Hussain Kirmani | 22i-0834 | CS-D

Objective

The objective of this project is to design and implement a robust and scalable network infrastructure for a hospital management system, ensuring seamless connectivity and secure communication across departments. The network architecture will support critical hospital operations by enabling efficient data sharing, reliable inter-device communication, and secure internet access. The system will integrate advanced technologies like DHCP for automated IP address allocation, NAT for secure external connectivity, and a dynamic routing protocol for optimized data flow. By providing a structured layout across three floors and leveraging devices such as routers, switches, PCs, wireless access points, smartphones, printers, and telephones, the network will meet the hospital's requirements for efficient departmental interaction and patient care management.

Technologies Used

This project is built in Cisco Packet Tracer. It contains 4 routers, 3 for each floor of the hospital and another that is responsible for configuring NAT with the help of a server. A total of two servers were used in the project, one for NAT and the other for DHCP. The network ensures seamless communication between devices.

Challenges & Learnings

NAT was a little challenging to implement but the rest of the project was easy. Through this project I learned how to configure multiple devices and how to build a real-life robust network topology. It was a fun project to work on.

Implementation Details

Floor and Department Layout

1st Floor: Network - 192.168.10.0

- Reception
- Emergency Department
- Pharmacy

2**nd Floor**: Network – 192.168.14.0

- Surgery Department
- Radiology
- Patient Records

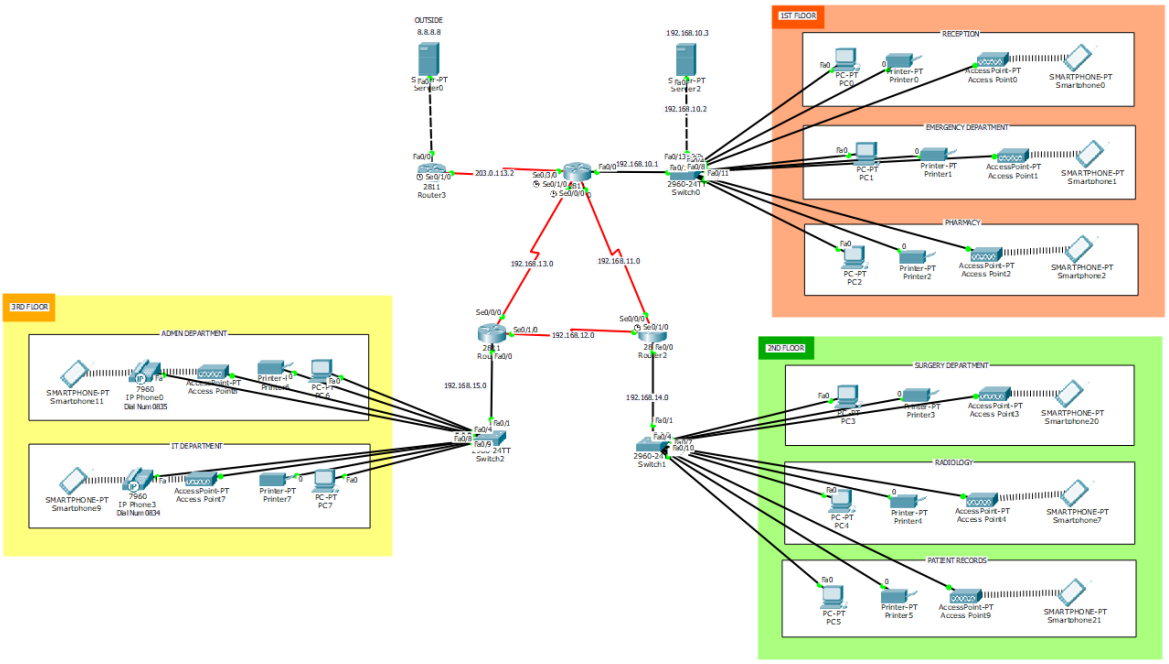
3rd Floor: Network – 192.168.15.0

- Admin Department
- IT Department

Network Design Requirements

1. Routers
2. Switches
3. PCs
4. Wireless Access Points
5. Smartphones
6. Printers
7. Telephones
8. Routing Protocol
9. DHCP Configuration
10. NAT
11. Inter-Device Communication

Network Topology



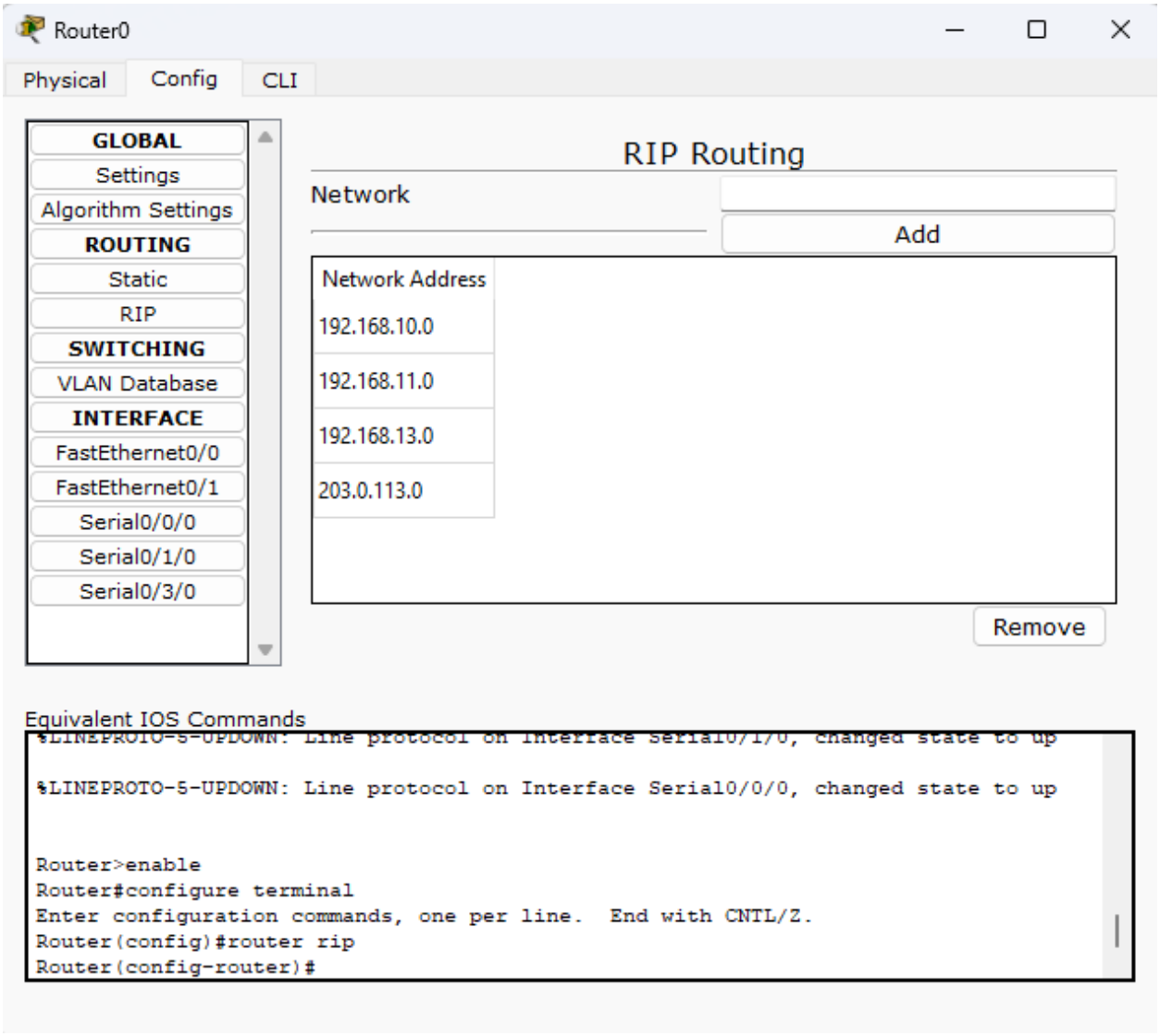
Scenarios

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smartphone11	Smartphone0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	Smartphone20	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2	Smartphone9	ICMP		0.000	N	2	(edit)	(delete)

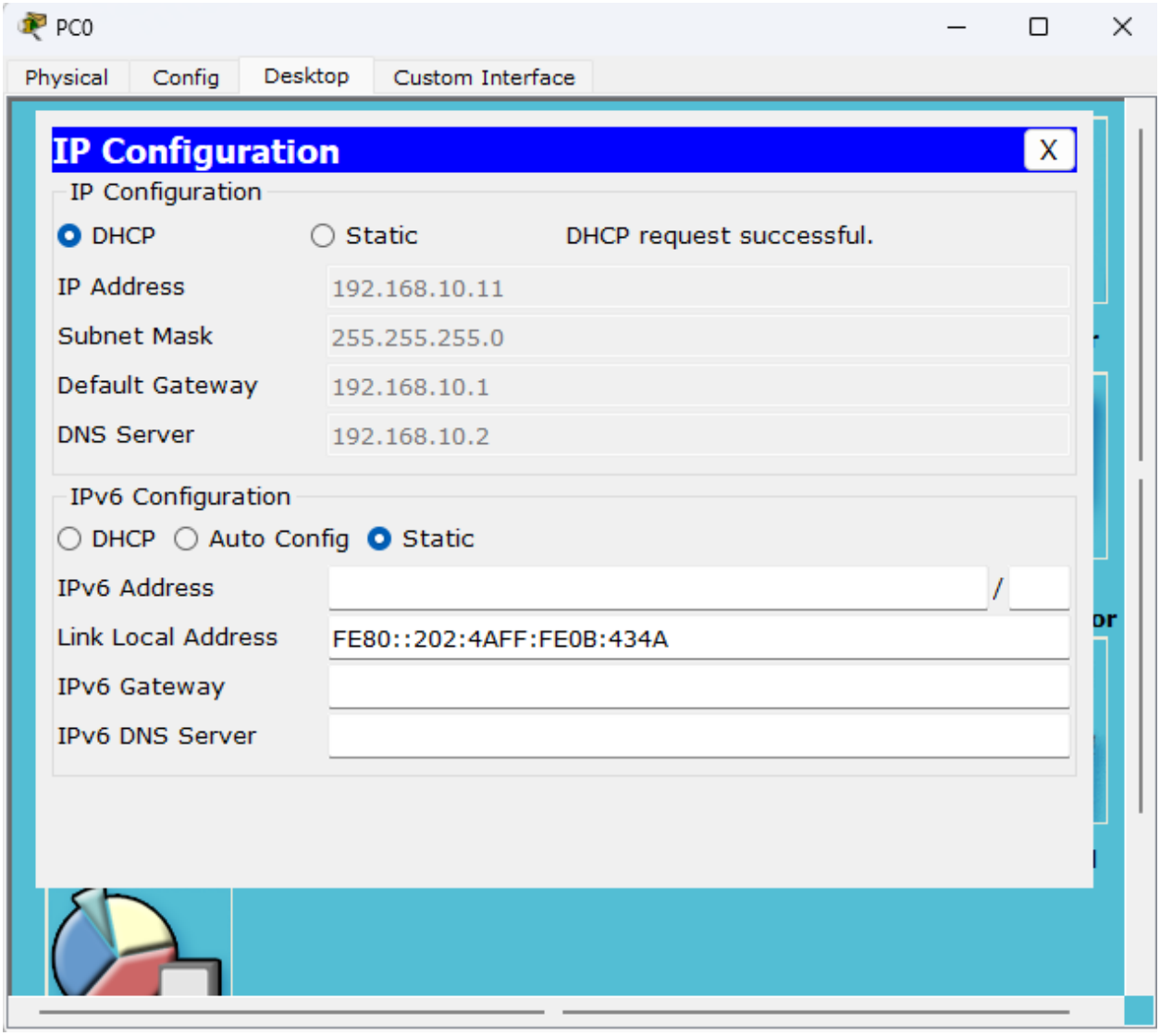
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC6	Printer1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC6	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Server0	Smartphone2	ICMP		0.000	N	2	(edit)	(delete)

Routing

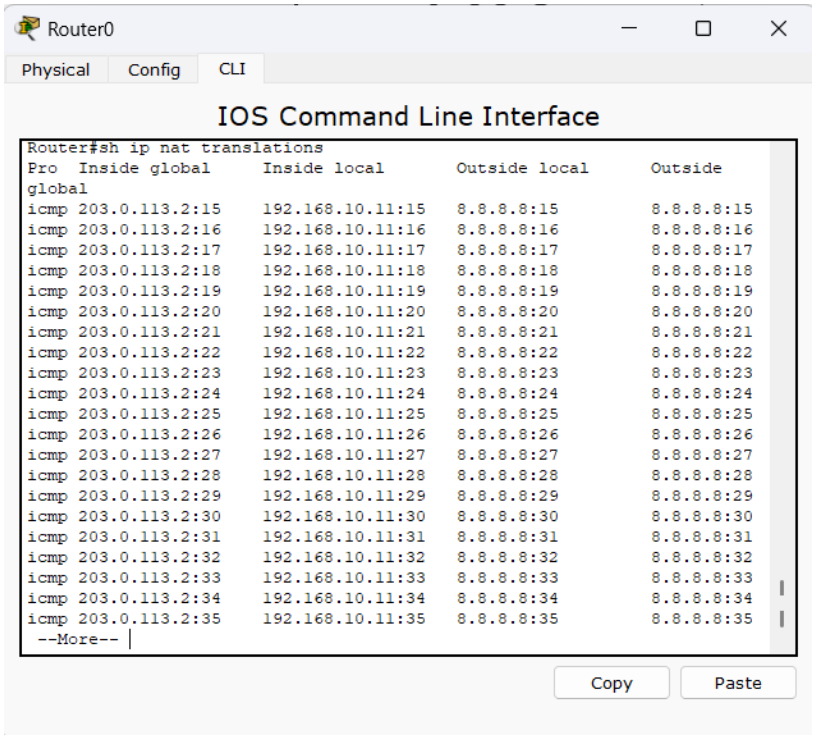
RIP routing used on each router

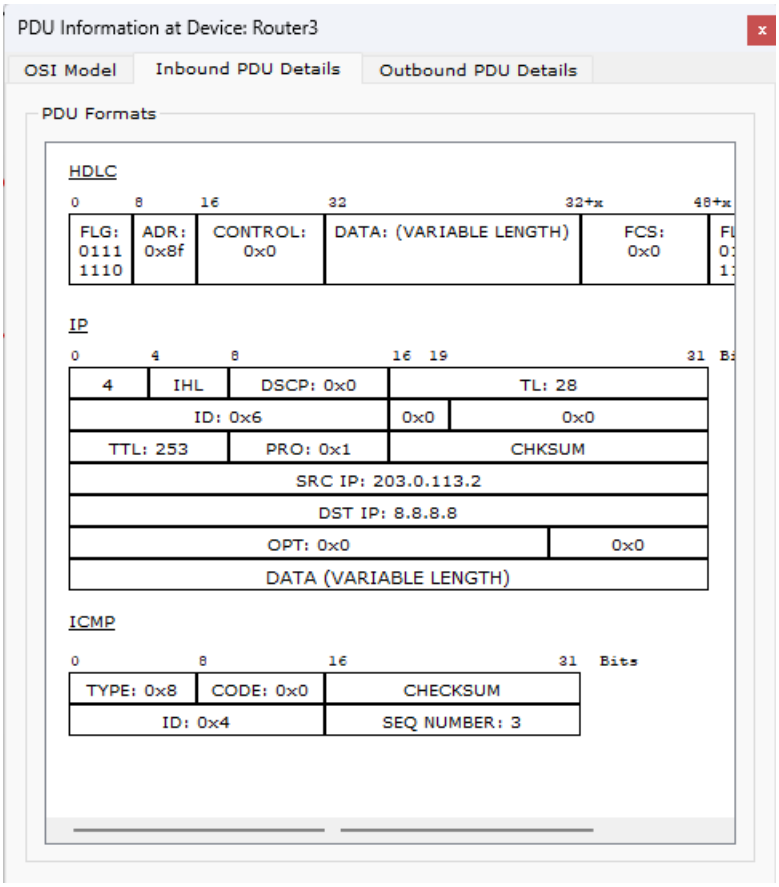


DHCP


PC0
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
DHCP request successful.
IP Address
192.168.10.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1
DNS Server
192.168.10.2
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:4AFF:FE0B:434A
IPv6 Gateway
IPv6 DNS Server

NAT Translations





Conclusion

The hospital management system network was successfully designed to meet the hospital's operational and communication needs. The system ensures seamless connectivity across three floors, enabling departments such as reception, emergency, pharmacy, surgery, radiology, and IT to function efficiently. Features like DHCP simplify IP address management, NAT enhances secure internet access, and a dynamic routing protocol ensures optimal data flow. Devices including routers, switches, PCs, wireless access points, printers, and telephones were integrated to support the hospital's diverse technological requirements.

In future, it is recommended to enhance the network, implement advanced security measures, integrate IoT devices for better patient care, and use monitoring tools for optimal performance. Prioritize scalability for future growth and establish a robust backup and disaster recovery plan to ensure data integrity and continuity.