Our project aims to design and configure a network using the Packet Tracker application. The topology consists of 8 routers, 10 switches, DHCP servers, web servers, an Access Point, and other network components, all interconnected in a configured manner.

In configuring the routers, we utilized OSPF technology to establish connections within the internal network. Each router is equipped with an HWIC-2T configuration card, connected to each other through serial ports. Throughout the project, we encountered challenges, and in addressing them, we learned valuable lessons. One major issue was the routers not recognizing each other as neighbors when introducing them to OSPF. To resolve this, we meticulously planned and structured the network, paying careful attention to connecting the ports repeatedly.

Another challenge was the failure of some devices to receive IP addresses from the DHCP server. We tackled this by carefully setting the gateways to the correct pools, which deepened our understanding of how routers operate and how packets find their paths.

The most daunting problem was experienced in the (Dark Blue) region, where, upon reopening the application, continuous packet spam occurred. It was identified as devices attempting to obtain an IP from DHCP but failing to locate the DHCP server. This was resolved by modify only one port in the switches from TRUNK to ACCESS mode.

Looking at the project in detail zone by zone:

Light Blue Zone:

DHCP server allocates IP addresses to all devices in the internal network. Additionally, a web server is present that our names in the main page, accessible to all devices in the network.

Light Green Zone:

An Access Point is set up, assigned a specific IP, and devices connected to it receive IPs from our DHCP server.

Dark Blue Zone:

Three VLAN configurations (Guest, Staff, Management) are implemented on a switch, each with dedicated subnets. Each VLAN obtains IPs from its respective DHCP server.

Orange Zone:

Dynamic routing protocol is implemented within the network. This is the external internet, and due to configurations on R1 router, requests to www.secretfiles.com from our devices within the network are redirected to R1. NAT is applied, and there is also an active DNS server responding to internet searches in the format www.secretfiles.com rather than IP addresses.