**Slide 1: Introduction**

"Good day everyone, We are Group 2 presenter, and today We’ll be presenting the network topology for our project. In this setup, We have implemented a **Star Topology** with protocols and services that ensure smooth network operations, security, and efficient communication. Let's dive into the key components of this network."

**Slide 2: Star Topology Overview**

"First, We have used a **Star Topology** as the core of this network. This topology is ideal because all devices, including our routers, servers, and PCs, connect directly to a central switch.

The **Star Topology** offers several advantages:

1. **Ease of troubleshooting**: Since each device is connected independently, if one connection fails, only that device is affected, not the entire network.
2. **Scalability**: We can easily add more devices without disrupting the existing network.
3. **Performance**: Each connection has its dedicated bandwidth, minimizing data collisions and improving performance.

In this topology, the central switch handles traffic flow between VLANs and to the various servers connected to it."

**Slide 3: OSPF Protocol**

"For the routing protocol, We have used **OSPF (Open Shortest Path First)**.

OSPF is a dynamic routing protocol, and its advantages are particularly beneficial for our network:

1. It finds the best path for data to travel across different subnets, improving network efficiency.
2. OSPF adapts quickly to changes in the network, such as link failures, ensuring that data flow continues with minimal downtime.
3. It scales well in large networks, making it a suitable choice for enterprise-level setups like ours.

This protocol ensures seamless inter-VLAN communication, which We’ll discuss in more detail shortly."

**Slide 4: Network Security with SSH, ACL, and NAT**

"Next, let’s talk about security. Ensuring that our network remains secure is one of our top priorities. For this, We’ve configured three main security features: **SSH, ACLs (Access Control Lists), and NAT**.

1. **SSH (Secure Shell):**
   * We've implemented SSH on the routers to secure remote access. SSH encrypts the communication between the network administrator and the devices, ensuring that sensitive data, such as login credentials, are not exposed.
   * This was configured on **line con 0** and **line vty** to restrict and secure access to the router’s command-line interface.
2. **ACL (Access Control Lists):**
   * **ACLs** are used to filter traffic and enhance security by defining which devices can communicate with specific parts of the network. For instance, only authorized administrators are allowed to remotely access the router via SSH, while limiting access to certain internal network resources.
   * We applied the **ACLs** to:
     + Deny unauthorized external access to our internal network.
     + Permit SSH connections only from specified IP addresses.
     + Ensure that only required traffic is allowed through, further enhancing the network’s security.
3. **NAT (Network Address Translation):**
   * **NAT** provides an additional layer of security by masking the internal IP addresses of our devices from the external network. This prevents external entities from knowing the exact IP addresses of devices within the network, protecting them from potential attacks.
   * It also allows multiple devices on our internal network to share a single public IP address, which is useful for conserving IP addresses.

Together, **SSH**, **ACL**, and **NAT** provide a robust defense against unauthorized access, ensure secure communication across our network, and protect internal resources from external threats."

**Slide 5: Inter-VLAN Routing**

"To allow devices in different VLANs to communicate, We have configured **Inter-VLAN Routing**. This ensures that data can travel between devices in different VLANs—such as the DNS server, web server, and PCs—while maintaining segregation for security and management.

For example:

* VLAN 10 is assigned to the **DNS server**,
* VLAN 20 is assigned to the **Web server**,
* VLAN 30 is for the PCs on the network.

Through inter-VLAN routing configured on the **Admin Router**, we ensure that devices from these VLANs can communicate securely without affecting the overall network performance."

**Slide 6: Server Services: DNS, Web, DHCP, and NAT**

"Let’s now talk about the server services that are part of our network:

1. **DNS Server**:
   * The **DNS Server** translates domain names into IP addresses. In our case, We have configured it with IP **8.8.8.8**, which is Google’s DNS, providing fast and reliable domain name resolution for our internal network.
2. **Web Server**:
   * The **Web Server**, assigned IP **9.9.9.9**, hosts web applications and services that can be accessed by internal and external clients. This ensures smooth access to internal company resources and websites.
3. **DHCP Server**:
   * The **DHCP Server** automates the assignment of IP addresses to devices within the network, ensuring that devices are dynamically assigned appropriate addresses without manual configuration.
4. **NAT Server**:
   * We’ve also set up the **NAT Server**, which, as mentioned earlier, hides the internal network structure from external users while allowing secure communication through a single public IP.

These services ensure that our network operates smoothly and efficiently, with minimal manual intervention required for basic functions like IP addressing, domain name resolution, and web access."

**Slide 7: Conclusion**

"In conclusion, the **Star Topology** combined with **OSPF**, **NAT with** **SSH and ACL’s**, along with our server services like DNS, Web, and DHCP, create a robust, scalable, and secure network environment.

This setup allows efficient communication between devices, ensures security for sensitive data, and is scalable for future expansion.

Thank you for your attention. We are happy to answer any questions you may have."