# Praveen Manokaran

|  |  |
| --- | --- |
| Network Engineer | [praveen.manokaran@outlook.com](mailto:praveen.manokaran@outlook.com) |
| Thanjavur, India | +91-8270511837 |

## Profile Summary

* Aspiring Network Engineer with hands-on training in CCNA, CCNP, and foundational knowledge in MCSA from recognized training institutes.
* Well-versed in networking concepts including routing protocols (OSPF, EIGRP, Static Routing), switching, VLANs, and Switchport Security.
* Familiar with network security basics, including firewall configurations and tools like Nmap and Wireshark.
* Gained practical skills through simulations in Cisco Packet Tracer and project-based learning.
* Completed technical projects including network vulnerability scanning and web application development.
* Strong analytical thinking, troubleshooting ability, and eagerness to grow in a professional network infrastructure environment.
* Passionate about continuously upgrading skills and pursuing certifications in the near future.

## Skills Stack

|  |  |
| --- | --- |
| **Category** | **Skills** |
| **Networking & Protocols** | OSPF, EIGRP, Static Routing, VLANs, Inter-VLAN Routing, STP, ACLs, NAT, DHCP |
| **Network Tools** | Cisco Packet Tracer, Wireshark, Nmap |
| **Operating Systems** | Windows Server (MCSA basics), Linux (basic commands) |
| **Security Basics** | Firewall fundamentals, Basic Ethical Hacking knowledge |
| **Cloud & Virtualization** | Microsoft Azure (intro level) |
| **Web & Scripting** | HTML, CSS, JavaScript(basic), Python (basic) |
| **Soft Skills** | Problem-solving, Communication, Teamwork, Adaptability |

## Academic Details

|  |  |  |  |
| --- | --- | --- | --- |
| Class | Institution | Percentage | Year of Passing |
| B.E (Computer Science) | Karpagam Institute of Technology, Coimbatore | 7.43 (CGPA) | 2023 |
| Twelfth (HSC) | Kurinji Matric Hr. Sec. School, Namakkal | 59 | 2019 |
| Tenth (SSLC) | Kurinji Matric Hr. Sec. School, Thanjavur | 88 | 2017 |

## Projects in Portfolio

### Enterprise Network Design [(GitHub Link)](https://github.com/praveen-manokaran/Enterprise-Network-Simulation.git)

**Objective:**

Design and implement a scalable and secure enterprise network infrastructure using VLANs, inter-VLAN routing, and Layer 3 switching.

**Key Configurations & Steps:**

* Created VLANs for HR, Sales, and IT departments.
* Assigned ports to appropriate VLANs.
* Configured trunk ports between access switches and the core Layer 3 switch.
* Enabled inter-VLAN routing on the Layer 3 switch.
* Verified end-to-end connectivity across departments.
* Designed a structured and scalable topology with access and distribution layers.

**Outcome:**

Achieved full inter-VLAN communication and stable core network layout for enterprise scalability.

### Firewall and Network Security Setup (DMZ-Based Network) [(GitHub Link)](https://github.com/praveen-manokaran/Firewall-and-Network-Security-Setup-DMZ-Based-Network-.git)

**Objective:**

Secure enterprise network using a DMZ and firewall policies with extended ACLs, providing controlled access to web and DNS servers.

**Key Configurations & Steps:**

* Built a DMZ zone using a dedicated switch and firewall router.
* Connected HR, Sales, and IT VLANs through access switches to a core switch.
* Placed Web (192.168.40.10) and DNS (192.168.40.20) servers in the DMZ.
* Configured ACLs to:
* Allow IT to access DNS and Web server.
* Allow HR & Sales to access only the Web server.
* Restrict DNS server access from HR and Sales.
* Prevent servers from initiating connections to internal VLANs.
* Verified with successful ping tests from all clients and servers.

**Outcome:**

Successfully implemented firewall ACL-based security with DMZ server access restrictions, simulating real-world enterprise protection layers.

### Site-to-Site VPN Configuration using ISAKMP and IPsec [(GitHub Link)](https://github.com/praveen-manokaran/Site-to-Site-VPN-Configuration-using-ISAKMP-and-IPsec.git)

**Objective:**To design and implement a secure site-to-site IPsec VPN between two branch offices using Cisco routers in Packet Tracer, ensuring encrypted communication between LANs over a simulated public network, while applying authentication, traffic policies, and encryption standards relevant to real-world enterprise VPN deployments.

**Key Configurations & Steps:**

* **Secure Branch Connectivity:** Simulated a site-to-site IPsec VPN between Router A and Router B. Connected 192.168.10.0/24 and 192.168.20.0/24 securely over a WAN link.
* **Traffic Encryption & Tunneling:** Configured ISAKMP policy and IPsec transform set. Encrypted traffic between the two LANs through the public interface (WAN IPs).
* **Policy-Based VPN Logic:** Applied an extended ACL to define "interesting traffic." This ACL triggered the VPN only for specific LAN-to-LAN communication.
* **Pre-Shared Key Authentication:** Used *crypto isakmp key* with peer IPs for authentication. Ensured both routers trusted each other using a shared secret.
* **Tunnel Verification and Testing:** Used ping tests between PCs from both LANs to confirm tunnel operation. Checked VPN status with *show crypto isakmp sa* and *ipsec sa*.

**Outcome:**

Successfully established an IPsec site-to-site VPN tunnel between two simulated branch networks using Cisco routers in Packet Tracer. The project demonstrated encrypted communication, proper ISAKMP Phase 1 and Phase 2 configuration, and verified tunnel activity through simulated traffic.