2025 Home Lab - System Administration

Executive Summary:

This is my outline and plan to design a powerful networking environment inside my home. The lab will simulate a small-to-mid-sized business infrastructure by integrating printers, thin clients, physical and cloud servers, virtualization, storage solutions, and layered security. The goal is to create a scalable and realistic IT ecosystem that supports learning, experimentation, and professional development in systems administration, cybersecurity, and DevOps.

---

1. Objectives

- **Build an enterprise-like environment to host apps, services, and simulated users**
- **Practice server management, virtualization, and remote access**
- **Integrate cloud and local services for hybrid workflows**
- **Run secure network segmentation with firewall policies**
- **Enable deployment of real tools used in production (Active Directory, file shares, backups, etc.)**

---

2. Hardware Plan

- **Rack Frame: 12U–25U server rack, cable management and airflow-ready**
- **Servers: Dell R630 or self-built Ryzen/ECC setup**
- **Firewall Router: pfSense box or Ubiquiti EdgeRouter**
- **Switches: Managed 24-port Gigabit PoE switch (for VLANs, APs, cameras)**
- **NAS/Storage: TrueNAS or Synology box for backups and shared drives**

- **UPS & PDU: Battery backup with surge protection and remote control**
- **Clients: Thin clients for terminal access, multiple test workstations**
- **Printers: Networked printers for print server configuration**

---

3. Software Stack

- **OSes: Windows Server 2022, Ubuntu Server, optional Kali for security practice**
- **Virtualization: Proxmox or Hyper-V for VM hosting**
- **Directory Services: Active Directory domain controller + Group Policy**
- **Web Services: Apache/Nginx, Node.js app backend**
- **Cloud Integration: Azure, AWS, or Google Cloud for hybrid use**
- **Monitoring & Logs: Netdata, Uptime Kuma, or ELK stack**
- **Backups: Automated nightly rsync or BorgBackup jobs**
- **Scripting/Automation: PowerShell, Bash, Ansible (optional)**

---

4. Network Architecture

- **VLANs for separating user devices, servers, management, IoT**
- **DNS/DHCP via pfSense or Pi-hole**
- **Public access control via port forwarding or reverse proxy**
- **OpenVPN or WireGuard for secure remote access**

- **Firewall ruleset for layered security testing**

---

5. Use Cases

- **Host and manage custom-built full-stack apps**
- **Deploy a print server and test device provisioning**
- **Simulate help desk workflows and ticketed escalation**
- **Practice remote monitoring, patching, and scripting**
- **Test group policies, permission delegation, and backup recovery**

---

6. Skills & Outcomes

- **Networking fundamentals and subnetting**
- **Windows/Linux server deployment and maintenance**
- **Service hosting, DNS, DHCP, and domain management**
- **Security hardening and traffic analysis**
- **Realistic simulation of business-grade IT infrastructure**

---

7. Future Expansions

- **Add cloud-based backup and container orchestration**

- **Implement multi-factor authentication and SSO**
- **Build a full DevOps pipeline for CI/CD and Git-based deployment**
- **Set up honeypot or SIEM system for cybersecurity practice**

---

8. Conclusion

This home lab design for 2025 sets the foundation for deep technical growth in enterprise networking, cybersecurity, and system administration. It is built with flexibility in mind — to test, break, rebuild, and ultimately master technologies that power real-world IT environments.