# ****Software House Network Design Documentation****

### ****1. Overview****

* **Purpose:** Outline the goals and objectives of the network.
* **Scope:** Describe the scale and boundaries of the network design, such as the number of devices, users, and primary services.

### ****2. Network Topology****

* **Diagram:** Include a visual representation of the network topology (export from Packet Tracer).
* **Description:**
  + Core Layer: Details on switches/routers used.
  + Distribution Layer: Information on subnetting and interconnections.
  + Access Layer: Details of user devices and their connections.

### ****3. Device Inventory****

Provide a list of all devices in the network, including:

* Device types (routers, switches, servers, workstations).
* Manufacturer and model (e.g., Cisco Catalyst 2960).
* Roles and configurations (e.g., DHCP Server, Core Router).

| **Device Name** | **Type** | **IP Address** | **Role** |
| --- | --- | --- | --- |
| Router1 | Router | 192.168.1.1 | Core Routing |
| Switch1 | Switch | 192.168.1.2 | VLAN Segmentation |
| Server1 | Server | 192.168.1.100 | DHCP, DNS |

### ****4. IP Addressing Scheme****

* **Subnets:** Detailed table of subnets used, including CIDR notations, IP ranges, and assignments.
* **VLANs:** VLAN configuration for traffic segmentation.

| **Subnet** | **CIDR** | **Purpose** | **Devices** |
| --- | --- | --- | --- |
| 192.168.1.0/24 | /24 | Management | Servers, Switches |
| 192.168.2.0/24 | /24 | User Devices | PCs, Laptops |

### ****5. Security Measures****

* Firewall configurations.
* Access control lists (ACLs) implementation.
* Encryption protocols (e.g., SSL/TLS, IPsec).

### ****6. Network Services****

* DHCP: Range, lease times, and configurations.
* DNS: Internal and external resolution.
* NAT: Configuration for external internet access.

### ****7. Device Configurations****

Include sample configurations for critical devices, such as:

* Router: Interface configurations, routing protocols (OSPF, EIGRP).
* Switch: VLAN and trunking configuration.
* Server: DHCP and DNS setup.

### ****8. Troubleshooting and Monitoring****

* Tools: SNMP, NetFlow, or Syslog configurations.
* Alerts: Thresholds and escalation process.
* Logs: Storage and analysis processes.

### ****9. Appendices****

* **Glossary:** Explanation of technical terms.
* **Exported Configurations:** Full text dumps or screenshots of device configurations from Packet Tracer.

### ****10. Executive Summary****

* **Project Overview:** Summarize the purpose, goals, and expected outcomes of the network design.
* **Stakeholders:** List key stakeholders, such as the software house management, IT team, and external vendors.
* **Timeline:** Include project milestones, from planning to implementation and testing.

### ****11. Network Requirements****

* **Business Requirements:**
  + Scalability needs (e.g., ability to handle growth in users/devices).
  + Redundancy for high availability.
  + Security compliance with industry standards.
* **Technical Requirements:**
  + Bandwidth and performance requirements.
  + Device and protocol standards (e.g., IPv6 compatibility).

### ****12. Network Architecture****

#### ****Physical Topology****

* Diagram: Illustrate the physical layout of the network.
* Details: Include cable types (Ethernet, Fiber Optic) and device placements.

#### ****Logical Topology****

* Explain IP address allocation.
* Highlight routing protocols (e.g., OSPF, EIGRP).
* VLAN segmentation details.

#### ****Redundancy and Failover****

* Redundant links, devices, and configurations.
* Load balancing mechanisms.

### ****13. Security Framework****

#### ****Perimeter Security****

* Firewalls: Types and rules.
* Intrusion Detection and Prevention Systems (IDPS).

#### ****Internal Security****

* Role-based access control (RBAC).
* VLAN security and inter-VLAN filtering.
* Port security measures.

#### ****Data Encryption****

* End-to-end encryption for sensitive data.
* VPN configurations for remote workers.

#### ****Security Policies****

* Network access policies.
* Incident response procedures.

### ****14. Quality of Service (QoS)****

* **Traffic Prioritization:** Policies for prioritizing traffic (e.g., VoIP, video conferencing).
* **Bandwidth Allocation:** Details on reserved bandwidth for critical applications.
* **Monitoring Tools:** Tools used to monitor and enforce QoS policies.

### ****15. Cloud Integration****

* **Services Hosted in the Cloud:** Include services like email, storage, or application hosting.
* **Hybrid Network Configuration:** Detail how on-premise and cloud environments interact.
* **Security Measures:** Specific protocols for securing data in transit to/from the cloud.

### ****16. Scalability and Future Expansion****

* Provisions for adding more devices or users.
* Plans for integrating new technologies (e.g., IoT, SD-WAN).
* Upgrade paths for hardware and software.

### ****17. Backup and Disaster Recovery****

* **Backup Strategy:** Frequency and location of backups.
* **Recovery Time Objectives (RTO):** Time to restore operations after failure.
* **Recovery Point Objectives (RPO):** Maximum acceptable data loss.

### ****18. Project Implementation****

#### ****Deployment Phases****

* **Phase 1:** Core infrastructure setup.
* **Phase 2:** Access layer installation.
* **Phase 3:** Testing and validation.
* **Phase 4:** Go-live and monitoring.

#### ****Testing Plan****

* Connectivity testing.
* Security vulnerability testing.
* Performance benchmarks.

### ****19. Training and Documentation****

* **End-User Training:** Training sessions or manuals for staff.
* **IT Team Training:** Advanced guides for managing and troubleshooting the network.
* **Documentation:** Include updated network diagrams, configurations, and logs.

### ****20. Budget and Cost Analysis****

* **Equipment Costs:** Detailed list of hardware/software with costs.
* **Maintenance Costs:** Ongoing support and updates.
* **Cost-Benefit Analysis:** Justify the expenditure with projected returns or savings.