**Technical Report**

**Project Title:** Small Enterprise Network Design & Implementation  
**Engineer:** Habibur Rahman  
**Date Completed:** May 2025

**1. Overview**

This technical report outlines the architecture and configuration of a secure, scalable, and resilient small enterprise network. The solution includes the deployment of Edge Routers (HO-RT01 & HO-RT02), Layer 3 Core Switches (Core\_SW01 & Core\_SW02), and Layer 2 Access Switches (Access\_SW01, Access\_SW02, Access\_SW03). The network has been meticulously designed to support VLAN segmentation, inter-VLAN routing, DHCP services, secure remote access, and high availability through HSRP and OSPF routing.

**Network Diagram**

**A computer network diagram with many connected objects

AI-generated content may be incorrect.**

**2. Network Infrastructure Overview**

**Edge Routers: HO-RT01 & HO-RT02**

**Administrative Security**

* **SSH Remote Access (Version 2)** enabled with domain alphatech.local for RSA key support.
* **User-Based Authentication**:
  + Local user admin (privilege level 15) secured with MD5-encrypted password.
* **VTY Line Configuration**:
  + SSH-only access.
  + ACL 10 permits access only from VLAN 10 (Admin) and VLAN 99 (Management).
  + Session timeout set to 5 minutes (exec-timeout 5 0).

**Interface & IP Assignment**

* **Gi0/0 (WAN)**:
  + HO-RT01: 90.209.58.18/30 (NAT outside)
  + HO-RT02: 92.109.07.12/30 (NAT outside)
* **Gi0/1 (LAN)**:
  + HO-RT01: 10.10.0.2/24
  + HO-RT02: 10.10.0.3/24
  + **NAT inside**, **HSRP Group 1**: Virtual IP 10.10.0.1, Priority 110/100 with preempt.
* **Gi0/2**: Internal backhaul between HO-RT01 and HO-RT02 (10.20.0.1/30)

**High Availability (HSRP)**

* **HSRP Group 1 on Gi0/1**: Provides virtual gateway for LAN clients.
* **Preempt Enabled**: HO-RT01 regains control when restored.

**Routing Protocols**

* **OSPF Process ID 1**:
  + Router ID: 1.1.1.1 (HO-RT01)
  + Router ID: 2.2.2.2 (HO-RT02)
  + Area 0 Backbone includes: Internal VLANs, infrastructure supernet (10.10.0.0/16), and WAN.
  + log-adjacency-changes enabled.

**NAT Configuration**

* **Dynamic NAT Overload**:
  + Translates all internal traffic via ACL 1 to public IPs on Gi0/0.

**Access Control Lists (ACLs)**

* **ACL 10**: Restricts SSH access to VLANs 10 and 99.
* **ACL 1**: Permits internal addresses for NAT translation.

**3. Layer 3 Core Switches: Core\_SW01 & Core\_SW02**

**VLAN Design**

|  |  |
| --- | --- |

**Trunking & Inter-VLAN Routing**

* All uplinks use 802.1Q trunking.
* **Switched Virtual Interfaces (SVIs)** configured for all VLANs with unique IPs.

**Security Controls**

* **SSH Remote Access** with ACL restriction.
* **MD5-encrypted enable secret** for privileged EXEC access.

**Port Security**

* Sticky MAC learning.
* Max 2 MAC addresses per port.
* Violation mode: Restrict.
* Default state: Admin shutdown.

**Routing & Redundancy**

* **OSPF Process ID 1**, Area 0:
  + Logs neighbor changes for stability monitoring.
  + Routes redistributed between VLANs and Edge Router.
* **Static Default Route**: Defined for Internet-bound traffic.
* **Multiple Static Routes** to 10.10.0.0/16 for path diversity.

**High Availability (HSRP)**

* HSRP enabled on SVIs for all key VLANs.
* Virtual IPs act as gateways.
* Priority: 110 with preempt for mastership recovery.

**Network Services**

* **DHCP Relay (IP Helper)** to centralised DHCP server (VLAN 60).
* **NTP**: Server 10.10.60.4 ensures synchronised logging and authentication.
* **SNMP**: Communities defined for read/write access.

**Logging**

* All events forwarded to logging server (10.10.60.4) at debug level.

**4. Layer 2 Access Switches: Access\_SW01**

**Administrative Hardening**

* **service password-encryption** enabled.
* **AAA** with local authentication.
* **ACL SSH-IT\_ADMIN-ONLY**:
  + Allows access only from 10.10.99.0/24 and 10.10.10.0/24 subnets.

**DHCP Snooping**

* Enabled for VLANs: 10, 20, 30, 40, 60, 99.
* Trusted Ports: Fa0/1–2 (uplinks), Fa0/23 (DHCP server), Gi0/1 (stack).

**STP Enhancements**

* **Mode**: PVST+
* **PortFast & BPDU Guard**: Enabled by default on all access ports.
* **System ID Extension**: Ensures bridge ID uniqueness.

**Port Security**

* Max 2 MAC addresses per port.
* Sticky MACs.
* Violation mode: Restrict.
* Ports Fa0/3–Fa0/21: Default shutdown.

**Interface Configuration Summary (Access\_SW01)**

| **Interface** | **Description** | **Mode** | **VLAN** | **Features** |
| --- | --- | --- | --- | --- |
| Fa0/1 | Uplink to Core\_SW01 | Trunk | All | DHCP Snooping Trust, PortFast Trunk |
| Fa0/2 | Uplink to Core\_SW02 | Trunk | All | DHCP Snooping Trust, PortFast Trunk |
| Fa0/3–21 | User Access | Access | 10 | Port Security, BPDU Guard, Admin Down |
| Fa0/22,24 | Regular Access | Access | 60 | STP PortFast |
| Fa0/23 | DHCP Server Port | Access | 60 | DHCP Snooping Trust |
| Gi0/1 | Stack to Access\_SW02/03 | Trunk | All | DHCP Snooping Trust, PortFast Trunk |
| Gi0/2 | Reserved (Shutdown) | — | — | — |

**IP Addressing and VLAN Allocation Table**A screenshot of a computer screen

AI-generated content may be incorrect.

**5. Conclusion**

This enterprise network is purpose-built to provide secure, high-performance, and resilient connectivity across departments. By leveraging best practices in VLAN design, Layer 3 routing, and administrative security, the solution achieves a strong balance of manageability and operational integrity. High availability mechanisms, such as HSRP and redundant routing, combined with granular access control and auditing, ensure continuity and protection in dynamic business environments.

Future enhancements may include IPSec VPN tunnels for inter-site connectivity, centralised identity-based access control using RADIUS/TACACS+, and wireless networks.