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.

---

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

VLAN ID	Name	Network/CIDR notation	Subnet	Gateway
10	admin	10.10.10.0/24	255.255.255.0	10.10.10.1
20	Sales	10.10.20.0/24	255.255.255.0	10.10.20.1
30	Finanace	10.10.30.0/24	255.255.255.0	10.10.30.1
40	Guest	10.10.40.0/24	255.255.255.0	10.10.40.1
60	Servers	10.10.60.0/24	255.255.255.0	10.10.60.1
99	Management	10.10.99.0/27	255.255.255.224	10.10.99.1

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

Interface	Description	Mode	VLAN	Features
Gi0/1	Stack to Access_SW02/03	Trunk	All	DHCP Snooping Trust, PortFast Trunk
Gi0/2	Reserved (Shutdown)	—	—	—

IP Addressing and VLAN Allocation Table

	ISP																	
Alphateck.local	HO-RT01: 90.209.58.18/30																	
	HO-RT02 :92.109.07.12/30																	
	Vlan 10 : Admin			Vlan 20: Sales			Vlan 30: Finance			Vlan 40: Guest			Vlan 99: Mgnt			Vlan 60 :Server		
	Network	Host	Devices	Network	Host	Devices	Network	Host	Devices	Network	Host	Devices	Network	Host	Devices	Network	Host	Devices
Network	10.10.10.	/24		10.10.20.	/24		10.10.30.	/24		10.10.40.	/24		10.10.99.	/27		10.10.60.	/24	
Satrting IP adddress	10.10.10.	1	Gateway	10.10.20.	1	Gateway	10.10.30.	1	Gateway	10.10.40.	1	Gateway	10.10.99.	1	Gateway	10.10.60.	1	Gateway
	10.10.10.	2	Core_SW01	10.10.20.	2	Core_SW01	10.10.30.	2	Core_SW01	10.10.40.	2	Core_SW01	10.10.99.	2	Core_SW01	10.10.60.	2	
	10.10.10.	3	Core_SW02	10.10.20.	3	Core_SW02	10.10.30.	3	Core_SW02	10.10.40.	3	Core_SW02	10.10.99.	3	Core_SW02	10.10.60.	3	
	10.10.10.	4		10.10.20.	4		10.10.30.	4		10.10.40.	4		10.10.99.	4	Access_sw03	10.10.60.	4	AT-SVR01
	10.10.10.	5		10.10.20.	5		10.10.30.	5		10.10.40.	5		10.10.99.	5	Access_sw01	10.10.60.	5	AT-DHCP01
	10.10.10.	6		10.10.20.	6		10.10.30.	6		10.10.40.	6		10.10.99.	6	Access_sw02	10.10.60.	6	
	10.10.10.	7		10.10.20.	7		10.10.30.	7		10.10.40.	7		10.10.99.	7		10.10.60.	7	ATFS01
	10.10.10.	8		10.10.20.	8		10.10.30.	8		10.10.40.	8		10.10.99.	8		10.10.60.	8	
	10.10.10.	9		10.10.20.	9		10.10.30.	9		10.10.40.	9		10.10.99.	9	HO-RT01	10.10.60.	9	
	10.10.10.	10		10.10.20.	10		10.10.30.	10		10.10.40.	10		10.10.99.	10	HO-RT02	10.10.60.	10	
	10.10.10.	11		10.10.20.	11		10.10.30.	11		10.10.40.	11		10.10.99.	11		10.10.60.	11	
End IP address	10.10.10.	254		10.10.20.	254		10.10.30.	254		10.10.40.	254		10.10.99.	30		10.10.60.	254	

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.