Introduction

This report provides an overview of the network setup, detailing the configurations and protocols used for each device in the network. The configuration includes routers, switches, and ISP connections, focusing on security, scalability, and performance optimization.

---

1. Devices and Roles

Head Office Router (HORouter)

- **Role:** Primary gateway for internal and external communication, VPN establishment, and VLAN routing.
- **Key Features:**
    - **VPN Setup:** Configured with IPSec and IKE (Internet Key Exchange) for secure communication with remote sites.
    - **NAT (Network Address Translation):** Enables internal devices to access the internet using a public NAT pool.
    - **Dynamic Routing:** OSPF (Open Shortest Path First) ensures dynamic and efficient route management within the network.
    - **VLAN Trunking:** Manages inter-VLAN traffic across subnets for various departments (e.g., Accounting, IT).
    - **SSH Management:** Secure remote access for administrators.

Internet Service Provider (ISP1)

- **Role:** Serves as the intermediate network provider between HORouter and remote sites.
- **Key Features:**
    - **Static Routing:** Routes are predefined for efficient data flow between the Head Office and remote locations.
    - **OSPF:** Facilitates communication with adjacent networks for seamless data exchange.
    - **Loopback Interface:** Used for routing and redundancy testing.

Internet Service Provider (ISP2)

- **Role:** Connects the Head Office and Branch Office, providing NAT and routing services.
- **Key Features:**

- **NAT:** Translates private internal addresses to public addresses, ensuring secure external communication.
- **Access Control Lists (ACLs):** Filters traffic for security, allowing only established connections and specific web traffic.
- **Routing:** Static routes to defined network subnets.

Head Office Switch (HOSwitch)

- **Role:** Handles VLAN segmentation and switchport configuration for internal network devices.
- **Key Features:**
  - **VLAN Configuration:** Segments traffic into VLANs (e.g., VLAN10 for Accounting, VLAN20 for IT).
  - **Access Management:** Secure login for administrators using local accounts.
  - **Trunk Ports:** Connects multiple VLANs to the HORouter for inter-VLAN routing.

---

2. Key Protocols and Technologies

2.1 Routing Protocols

- **OSPF (Open Shortest Path First):**
  - Dynamic routing protocol for efficient route updates.
  - Ensures redundancy and optimal path selection within the network.
- **Static Routing:**
  - Used by ISP2 and ISP1 to define specific routes between Head Office and Branch Office subnets.

2.2 Security Protocols

- **IPSec VPN:**
  - Secure encrypted tunnels for remote site communication.
  - Provides confidentiality, integrity, and authentication for data transfer.
- **IKE (Internet Key Exchange):**
  - Negotiates secure communication parameters for IPSec.
- **SSH (Secure Shell):**

    - Enables encrypted management access to network devices, replacing insecure protocols like Telnet.
- **Access Control Lists (ACLs):**
    - Restricts unauthorized traffic based on predefined rules.

2.3 Network Address Translation (NAT)

- **Dynamic NAT with Overloading:**
    - Allows multiple internal devices to share a single public IP address for internet access.
- **Static NAT:**
    - Maps a specific private IP to a public IP, ensuring accessibility for specific services.

2.4 VLANs

- Segments the internal network for efficient traffic management and security.
- Supports inter-VLAN communication through routing on the HORouter.

---

3. Summary of Connections

Device	Connection	Purpose
HORouter	To ISP1 (Serial0/1/0)	Primary internet and VPN gateway.
	To HOSwitch (GigabitEthernet0/0/0)	Manages inter-VLAN routing and NAT.
ISP1	To HORouter (198.80.1.0/30)	Handles internet traffic routing and connectivity.
	To ISP2 (Serial0/1/1)	Connects Head Office to Branch Office.
ISP2	To HORouter (198.80.2.0/30)	Manages NAT and access control for remote communication.
HOSwitch	VLANs 10, 20, 30	Provides network segmentation for departments.

---

4. Recommendations

1. **Security Enhancements:**

- Use stronger password hashing algorithms (e.g., SHA-256) to replace MD5.
- Implement an ACL on ISP1 and ISP2 to further restrict access to critical services.
- Disable unused ports on switches to prevent unauthorized access.

2. **Monitoring and Logging:**
   - Enable logging on all devices to track configuration changes and security breaches.
   - Use SNMPv3 for secure network monitoring.
3. **High Availability:**
   - Consider implementing HSRP or VRRP on routers for failover capabilities.
   - Add redundancy for ISP connections to ensure continuous availability.
4. **Performance Optimization:**
   - Enable QoS on interfaces handling critical traffic.
   - Regularly review NAT and routing configurations to ensure efficiency.

Conclusion

This network configuration ensures secure and scalable communication between the Head Office, Branch Office, and the internet. It leverages industry-standard protocols like OSPF, IPSec, and NAT to maintain high performance and robust security. The recommended enhancements will further strengthen the network's resilience and operational integrity.