**IPv6 Network Security Project Report**

**Project overview:**

This project involves the design, implementation, and security hardening of an enterprise-grade IPv6 network using Cisco Packet Tracer. The objective is to simulate a realistic multi-department organization with full IPv6 addressing, routing, and access control.

The network includes three departments (Sales, HR, and Support) connected through two routers using OSPFv3 as the dynamic routing protocol. Each department operates in a separate IPv6 subnet, and inter-department access is regulated using IPv6 ACLs.

To enhance network security and manageability, the project includes:

* SSH-based remote access (restricted to the Support department)
* IPv6 Access Control Lists (ACLs) for traffic filtering
* Port security on switches to mitigate MAC spoofing

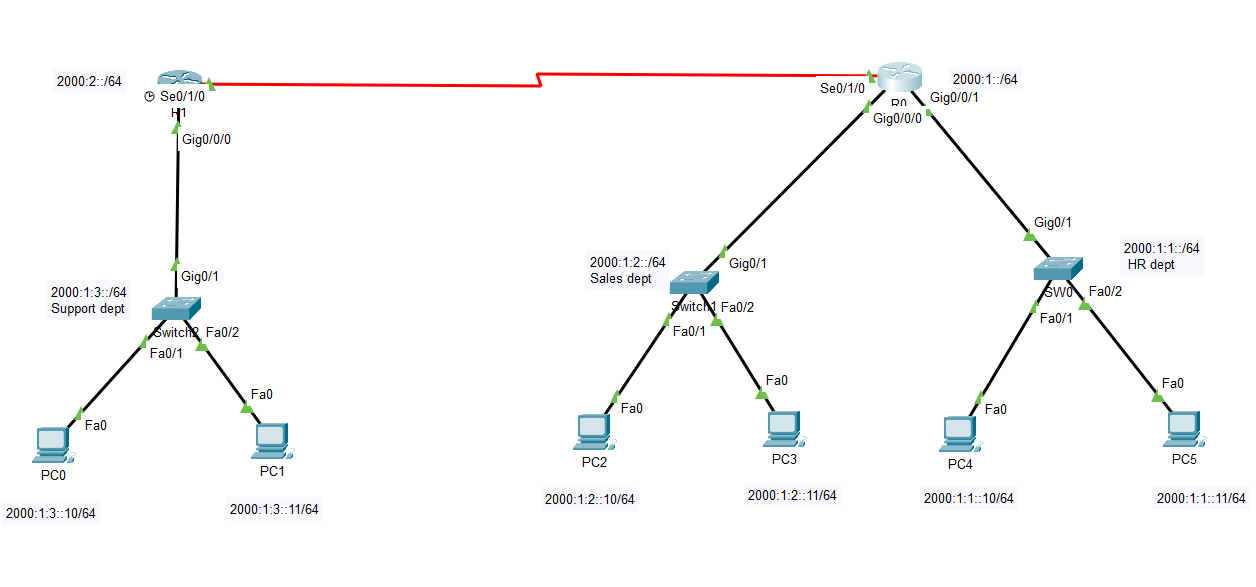
The design is modular and scalable, adhering to modern IPv6 enterprise practices. This setup reflects how real-world enterprise networks are built with security, scalability, and manageability in mind.

**Network Topology Description:**

The network is divided into three departments, each connected to Layer 2 switches, and all departments are linked via two core routers.

Components:

* 2 Routers (Router0 and Router1)
* 3 Switches (Switch0, Switch1, Switch2)
* 6 End Devices (PCs)



**IPv6 Addressing Plan:**

Addressing table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IPv6 Address** | **Subnet** | **Purpose** |
| Router0 | G0/0/0 | 2000:1:2::1 | 2000:1:2::/64 | HR Dept Gateway |
| Router0 | G0/0/1 | 2000:1:1::1 | 2000:1:1::/64 | Sales Dept Gateway |
| Router0 | S0/1/0 | 2000:1::1 | 2000:1::/64 | Link to Router1 |
| Router1 | S0/1/0 | 2000:2::1 | 2000:2::/64 | Link to Router0 |
| Router1 | G0/0/0 | 2000:1:3::1 | 2000:1:3::/64 | Support Dept Gateway |
| PC0 (Support) | NIC | 2000:1:3::10 | 2000:1:3::/64 | Support PC |
| PC1 (Support) | NIC | 2000:1:3::11 | 2000:1:3::/64 | Support PC |
| PC2 (Sales) | NIC | 2000:1:2::10 | 2000:1:2::/64 | Sales PC |
| PC3 (Sales) | NIC | 2000:1:2::11 | 2000:1:2::/64 | Sales PC |
| PC4 (HR) | NIC | 2000:1:1::10 | 2000:1:1::/64 | HR PC |
| PC5 (HR) | NIC | 2000:1:1::11 | 2000:1:1::/64 | HR PC |

**Configuration Summary:**

**1. IPv6 Addressing:**

* All interfaces manually assigned IPv6 addresses.
* Default gateways configured on PCs.

**Commands on R0:**

enable

configure terminal

ipv6 unicast-routing

interface GigabitEthernet0/0/0

ipv6 address 2000:1:2::1/64

no shutdown

interface GigabitEthernet0/0/1

ipv6 address 2000:1:1::1/64

no shutdown

interface Serial0/1/0

ipv6 address 2000:1::1/64

no shutdown

**Commands on R1:**

enable

configure terminal

ipv6 unicast-routing

interface GigabitEthernet0/0/0

ipv6 address 2000:1:3::1/64

no shutdown

interface Serial0/1/0

ipv6 address 2000:2::1/64

no shutdown

**2. Routing (OSPFv3):**

* OSPFv3 enabled on both routers using ipv6 ospf 1.
* Interfaces added to OSPF process with correct area assignments.
* Router IDs manually set for consistency.

**Commands on R0:**

ipv6 router ospf 1

router-id 1.1.1.1

exit

interface GigabitEthernet0/0/0

ipv6 ospf 1 area 0

interface GigabitEthernet0/0/1

ipv6 ospf 1 area 0

interface Serial0/1/0

ipv6 ospf 1 area 0

**Commands on R1:**

ipv6 router ospf 1

router-id 2.2.2.2

exit

interface GigabitEthernet0/0/0

ipv6 ospf 1 area 0

interface Serial0/1/0

ipv6 ospf 1 area 0

**3. Security:**

* SSH configured on both routers, restricted via ACLs to Support subnet (2000:1:3::/64).
* IPv6 ACLs applied to limit inter-department access (e.g., block Admin from reaching Sales).
* Port security configured on access switches to allow only known MAC addresses.

**SSH Configuration (Both Routers)**

hostname R0 ! or R1 depending on router

ip domain-name example.com

crypto key generate rsa

1024

username support privilege 15 secret support123

line vty 0 4

login local

transport input ssh

**Restrict SSH to Support Subnet ACL (Both Routers)**

ipv6 access-list SSH\_ONLY

permit ipv6 2000:1:3::1/64 any

deny ipv6 any any

line vty 0 4

ipv6 access-class SSH\_ONLY in

**IPv6 ACL Between Sales and HR department on R0**

ipv6 access-list BLOCK-HR-SALES

deny ipv6 2000:1:2::/64 2000:1:1::/64

deny ipv6 2000:1:1::/64 2000:1:2::/64

permit ipv6 any any

interface g0/0/1

ipv6 traffic-filter BLOCK-HR-SALES in

interface g0/0/2

ipv6 traffic-filter BLOCK-HR-SALES in

**Port Security on Switches**

interface FastEthernet0/1

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security mac-address sticky

switchport port-security violation restrict