**Enterprise Network Security & Management**

**IP Addressing Table**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Department/Network** | **Subnet** | **Device** | **IP Address** | **Notes** | | HR | 192.168.10.0/24 | PC0, PC1, PC3 | 192.168.10.2 | Hosts | | IT | 192.168.20.0/24 | PC2, PC4 | 192.168.20.2 | Hosts | | SALE | 192.168.30.0/24 | PC5, PC6 | 192.168.30.2 | Hosts | | ADMIN | 192.168.5.16/29 | ADMIN PC | 192.168.5.18 | Admin User | | WEB Server | 192.168.5.0/29 | Web Server | 192.168.5.3 | Only accessible to some networks | | NTP/TACACS Server | 192.168.5.8/29 | NTP & TACACS Server | 192.168.5.9 | Centralized Auth/Time Server | | FINANCE | 192.168.40.0/27 | PC7, PC9 | 192.168.40.2 | Hosts | | R&D | 192.168.40.32/27 | PC11, PC12 | 192.168.40.34 | Hosts | | F&B | 192.168.40.64/27 | PC8, PC10 | 192.168.40.66 | Hosts | | Router Interfaces | 192.168.1.0/30 | G0/0–G0/2 | 192.168.1.1–1.2 | Point-to-Point Links | | Router Loopback /Mgmt | 192.168.1.4/30 | G0/0–G0/1 | 192.168.1.5–1.6 | Router Mgmt | |

**Configurations Done**

**OSPFv2 Enabled on Routers**

* Secure OSPFv2 configuration using *ip ospf authentication message-digest.*
* Interfaces authenticated with MD5.
* Network-wide reachability tested using **PING** from HR PC to all others.

**Secure NTP Server Configured**

* NTP server at 192.168.5.9 configured.
* Devices synchronized with centralized time.

**Secure Remote Management**

* Configured TACACS+ server
* All network devices (routers & switches) use TACACS+ for remote login.

**Port Security**

* **Switch 2 and 3**:
  + Port security with 2 dynamically learned MACs per port.
  + Violation action: **restrict**.
* **Switch 1**:
  + Statically assigned MAC addresses for Admin PC and Servers.
  + Violation action: **shutdown**.

**Website Access Control**

* Only HR, IT, FINANCE, and R&D allowed to access the Web Server at 192.168.5.3.
* Configured with ACLs on router interfaces to enforce policy.