Cisco Network Administrator - Project 6

Project: Build Enterprise Network (Single Site)

Project Planning & Management

Objectives:

- Design and implement a secure and efficient enterprise network.
- Configure and manage network devices to ensure connectivity and security.
- Utilize industry-standard tools such as Cisco Packet Tracer and GNS3.

Project Phases:

1. **Initiation & Requirement Analysis**
   - Define project scope and objectives.
   - Identify hardware and software requirements.
   - Establish a timeline and key milestones.
2. **Planning & Design**
   - Create a network topology diagram.
   - Assign roles and responsibilities.
   - Develop a risk management plan.
3. **Implementation**
   - Set up routers, switches, and end devices.
   - Configure VLANs, security policies, and routing protocols.
   - Test network connectivity.
4. **Testing & Optimization**
   - Conduct troubleshooting and performance analysis.
   - Optimize configurations for efficiency.
5. **Deployment & Documentation**
   - Finalize network setup.
   - Prepare documentation for future reference and maintenance.

Risk Management:

- **Hardware Failure:** Have backup devices and configurations.
- **Configuration Errors:** Perform step-by-step testing.
- **Security Threats:** Implement strong authentication and monitoring.
- **Project Delays:** Regular progress tracking and adjustments.

Requirements Gathering

Stakeholder Analysis

- **Network Administrators:** Need a scalable and manageable network.
- **Employees:** Require secure and reliable connectivity.
- **IT Security Team:** Ensures network security and compliance.
- **Management:** Seeks cost-effective and high-performance solutions.

User Stories & Use Cases

- **As a network admin,** I want to configure VLANs to segment network traffic securely.
- **As an employee,** I need seamless access to internal and external resources.
- **As a security analyst,** I want real-time network monitoring to detect threats.
- **As an IT manager,** I need documentation for future maintenance.

Functional Requirements

- Support for VLANs, trunking, and inter-VLAN routing.
- Implementation of dynamic routing protocols (OSPF, EIGRP, RIP).
- DHCP configuration for dynamic IP allocation.
- Network Address Translation (NAT) for internet access.
- Access Control Lists (ACLs) for security.
- Firewall and Intrusion Detection/Prevention Systems (IDS/IPS).
- SNMP and Syslog for network monitoring.

Non-functional Requirements

- **Performance:** Ensure low-latency communication between devices.
- **Security:** Apply encryption and authentication mechanisms.
- **Usability:** Provide a user-friendly configuration and monitoring interface.
- **Reliability:** Ensure redundancy and failover mechanisms.

Week 1: Build Internal Network

Tasks:

- Install internal network using Cisco switches, routers, devices, and a server.

Deliverables:

- Use Cisco Packet Tracer & GNS3.
- Design should contain:
  - 3 Routers
  - 2 Distribution Switches (DSW)
  - 4 Access Switches (ASW)

    - 20 PCs
    - 1 Server

Week 2: Configuration for Access & Distribution Switches

Tasks:

- **Configuration for Access Switches:** Manually configure four access layer switches.
- **Configuration for Distribution Switches:** Manually configure two distribution switches.

Deliverables:

- **Basic Configuration:**
    - Set hostname.
    - Enable secret and VTY password (Cisco).
    - Configure welcome message.
    - Encrypt all passwords.
    - Create VLANs:
        - VLAN 10 (Sales)
        - VLAN 20 (IT)
        - VLAN 30 (HR)
        - VLAN 40 (Management)
    - Assign ports to VLANs on access switches:
        - F0/1-5 → VLAN 10
        - F0/6-10 → VLAN 20
        - F0/11-15 → VLAN 30
        - F0/16-20 → VLAN 40
    - Configure trunk ports.
    - Configure EtherChannel using PAgP.
    - Set DSW 1 as Root Bridge for VLANs 1, 10, and 20.
    - Set DSW 2 as Root Bridge for VLANs 30 and 40.
    - Configure access ports as portfast on access switches.
    - Protect access ports from unexpected BPDU.
    - Configure port security on access switches.
    - Save configuration to NVRAM.

Week 3: Configuration for Routers

Tasks:

- Configure basic settings (hostname, passwords, banners).

- Configure IP addresses on router interfaces.
- Implement static and dynamic routing (OSPF, EIGRP, or RIP).
- Set up DHCP for dynamic IP allocation.
- Configure NAT for internet access.
- Apply access control lists (ACLs) for security.
- Test connectivity and troubleshoot issues.

Deliverables:

- Fully configured routers with proper IP addressing.
- Functional routing protocols ensuring network communication.
- DHCP, NAT, and ACL configurations in place.
- Connectivity test results and troubleshooting documentation.

Literature Review

Feedback & Evaluation

-

-

-

Suggested Improvements

- **Scalability Enhancements:** Implementing redundant links and load balancing to improve network performance and ensure failover capabilities.
- **Security Enhancements:** Upgrading firewall rules, improving access control policies, and implementing multi-factor authentication.
- **Performance Optimization:** Tuning routing protocols and VLAN configurations for better data flow efficiency.
- **Monitoring Improvements:** Adding automated network monitoring tools with real-time alerts for potential threats or failures.
- **Documentation Enhancement:** Providing clearer network diagrams, configuration details, and troubleshooting guides for future maintenance.

Final Grading Criteria

-

-