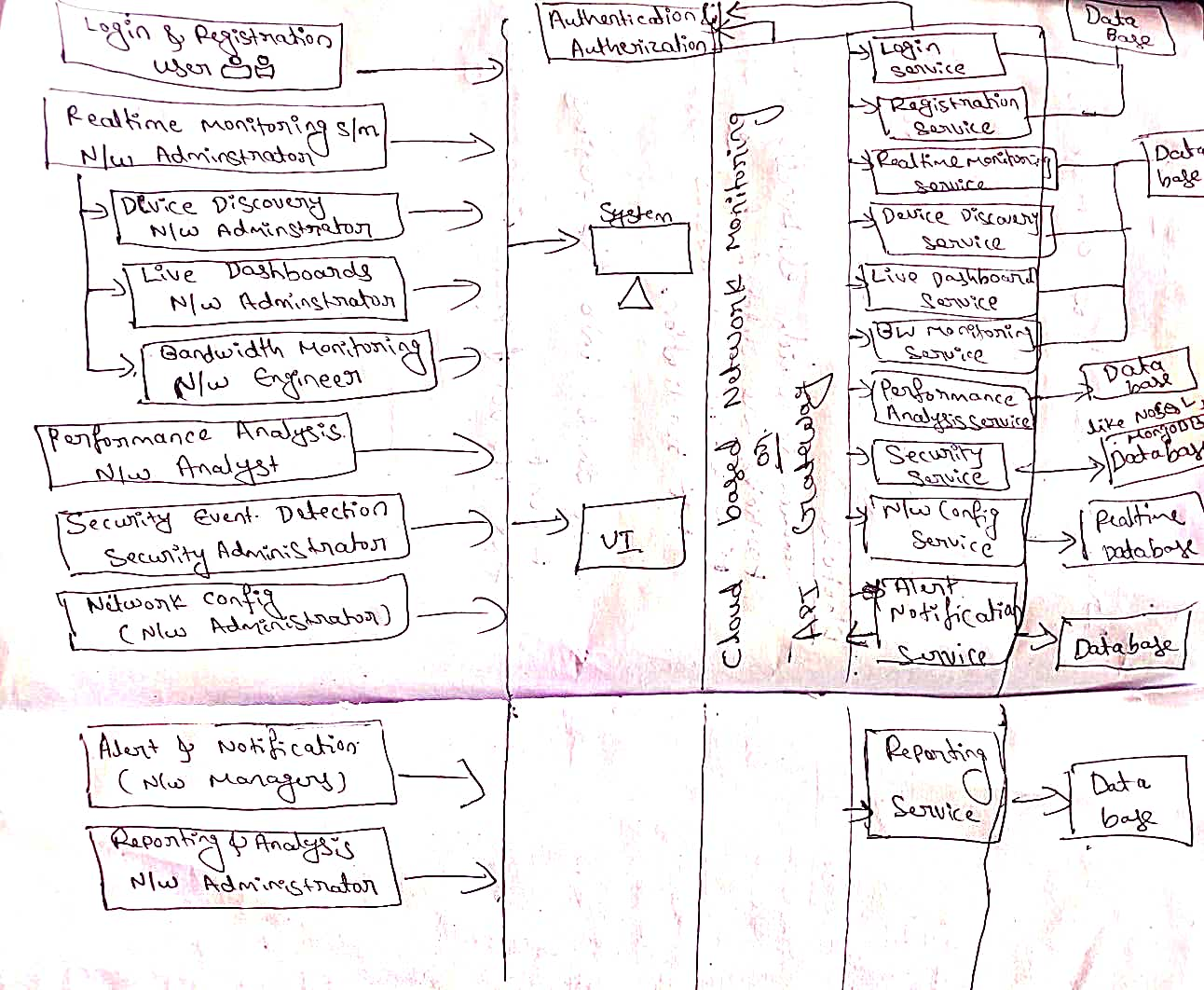
**Network Monitoring System**



### **High-Level Design (HLD) for Network Monitoring System**

#### System Overview:

The network monitoring system is designed to provide comprehensive real-time monitoring, performance analysis, security event detection, network configuration management, alerts and notifications, reporting and analytics, as well as integration with third-party tools. It ensures the efficient management and optimization of network infrastructure while maintaining security and compliance.

#### Components and Features:

1. **Real-time Network Monitoring:**
   * Continuously monitors the network for performance metrics, security events, and configuration changes.
   * Provides real-time visibility into the network status, device health, and traffic patterns.
   * **Device Discovery:**
   * Use ARP scanning for device discovery.
   * Allow manual addition through a simple form in the UI.
   * Automatically discovers and maps all devices connected to the network using protocols like SNMP, ICMP, or LLDP.
   * Supports manual device addition for comprehensive coverage of all network devices.

* **Live Dashboards:**
  + Real-time visualizations of network performance metrics such as latency, packet loss, bandwidth usage, and device status.
  + Customizable dashboards based on user roles, providing relevant insights for different stakeholders.
  + Use Chart.js for real-time visualizations.
  + Implement basic role-based access control in the frontend.
* **Bandwidth Monitoring:**
  + Tracks bandwidth usage by device, application, and protocol.
  + Sets alerts for abnormal bandwidth consumption to facilitate proactive management and optimization.
  + Utilize SNMP for bandwidth monitoring.
  + Implement threshold-based alerts using simple scripting.

1. **Performance Analysis:**
   * Network topology mapping using distributed graph databases like Neo4j.
   * Store historical performance data in a time-series database like Influx DB.
   * **Network Topology Mapping:**
     + Provides a visual representation of the entire network topology.
     + Dynamically updates the network map as new devices are added.
   * **Historical Performance Data:**
     + Stores and analyses historical performance data for trend analysis and capacity planning.
     + Generates performance reports for specific time intervals to identify patterns and optimize network performance.
2. **Security Event Detection:**
   * Advanced IDS using machine learning models for anomaly detection.
   * Log analysis using ELK Stack for centralized log management.
   * **Intrusion Detection System (IDS):**
     + Monitors network traffic for suspicious activities and anomalies.
     + Triggers immediate alerts for potential security breaches to enable rapid response.
   * **Log Analysis:**
     + Analyses log files from network devices and servers to identify security incidents.
     + Correlates logs to detect and mitigate security threats effectively.
3. **Network Configuration Management:**
   * Automated configuration backup using Git for version control.
   * Compliance checks using automated configuration drift detection.
   * **Configuration Backup:**
     + Automatically backs up and version controls network device configurations.
     + Compares configurations to identify changes and ensure consistency.

* **Compliance Checks:**
  + - Ensures network configurations comply with industry standards and internal policies.
    - Performs automated checks and triggers alerts for non-compliance to maintain security and compliance posture.

1. **Alerts and Notifications:**
   * Send alerts via email using a simple SMTP library.
   * Provides customizable alerts for specific events or thresholds.
   * Delivers alerts via email, SMS, or in-app notifications to notify administrators and stakeholders promptly.
   * Customizable alerts with integrations with popular messaging platforms like Slack or Microsoft Teams.
2. **Reporting and Analytics:**
   * Advanced reporting using business intelligence tools like Tableau or Power BI.
   * Trend analysis using machine learning algorithms for predictive analytics.
   * **Pre-built Reports:**
     + Offers standard reports for network health, performance, and security events.
     + Supports custom report generation based on user-defined criteria for in-depth analysis.
   * **Trend Analysis:**
     + Analyses performance trends to identify potential issues and predict future network requirements for capacity planning.
3. **Integration with Third-party Tools:**
   * Seamless integration with popular SIEM solutions via APIs.
   * Automated compatibility testing using continuous integration pipelines.

* **SIEM Integration:**
  + - Provides seamless integration with SIEM solutions such as Splunk, ELK Stack, and ArcSight for enhanced security intelligence.
  + **Network Device Compatibility:**
    - Ensures compatibility with a wide range of network devices, including routers, switches, firewalls, and load balancers.
    - Develops plugins or adapters for common network equipment brands to facilitate integration and interoperability.

#### Integration and Scalability:

* The system is designed with modular components that can be easily integrated with third-party tools and scalable to accommodate growing network environments.
* APIs and integration points are provided for seamless integration with existing infrastructure and third-party systems.
* Horizontal scalability is achieved through distributed architecture and containerization for efficient resource utilization and high availability.

#### Security:

* Implements robust security measures to protect sensitive data and ensure the integrity of the monitoring system.
* Utilizes encryption for data transmission, access controls for user authentication, and audit trails for tracking system activities.
* Regular security audits and updates are conducted to address emerging threats and vulnerabilities.

#### Conclusion:

This high-level design provides a comprehensive overview of the network monitoring system, outlining its key components, features, integration points, scalability, and security measures. By incorporating these features into a cohesive system, the network monitoring solution enables administrators to effectively monitor, analyse, and manage network infrastructure while ensuring security, compliance, and scalability.