**Network Monitoring System**

**User Stories and Acceptance Criteria:**

1. **Login and Registration:  
   User Story:** As a user of the network monitoring system, I want to have a seamless login and registration process to access the system securely and manage my account details effectively.

**Acceptance Criteria:**

**User Registration:**

* + Users should be able to access the registration page from the login screen.
  + The registration form should include fields for essential information such as full name, email address, and password.
  + The system should validate the email address format and ensure that the password meets security requirements (e.g., minimum length, complexity).
  + Upon successful registration, users should receive a confirmation email to verify their email address and activate their account.

**User Login:**

* + Users should be able to access the login page from the system's homepage.
  + The login form should include fields for email address and password.
  + The system should authenticate user credentials against the stored database of registered users.
  + Users should be redirected to the system's dashboard upon successful login.

1. **Real-time Network Monitoring (3.1):**

**User Story:** As a network administrator, I want to have real-time visibility into the devices connected to the network and their performance metrics.

* + **Acceptance Criteria:**
    1. The system automatically discovers and maps all devices connected to the network.
    2. Users have the option to manually add devices to the network inventory.
    3. Devices are accurately represented on the network map.
    4. The network map is continuously updated to reflect changes in the network topology.

1. **Device Discovery (3.1.1):**

**User Story:** As a network administrator, I want to ensure efficient device discovery to maintain an accurate inventory of all devices connected to the network.

* **Acceptance Criteria:**

**Automatic Device Discovery:**

* + The system should automatically scan the network infrastructure to discover all connected devices, including routers, switches, servers, printers, endpoints, and any other networked devices.
  + Devices should be accurately identified based on their MAC addresses, IP addresses, and other unique identifiers.
  + The discovery process should cover both wired and wireless devices within the network.

1. **Live Dashboards (3.1.2):**

**User Story:** As a network manager, I want to monitor network performance in real-time through customizable dashboards.

* + **Acceptance Criteria:**
    1. The system provides real-time visualizations of network performance metrics, including bandwidth usage, latency, and packet loss.
    2. Dashboards are customizable based on user roles, allowing different stakeholders to view relevant metrics.
    3. Users can configure dashboards to display specific performance metrics and KPIs.
    4. The system provides interactive features such as drill-down capabilities for deeper analysis.

1. **Bandwidth Monitoring (3.1.3):**

**User Story:** As a network engineer, I want to track bandwidth usage across devices, applications, and protocols, and receive alerts for abnormal consumption.

* + **Acceptance Criteria:**
    1. The system tracks bandwidth usage by device, application, and protocol.
    2. Users can set threshold-based alerts for abnormal bandwidth consumption.
    3. Alerts are sent via email, SMS, or in-app notifications.
    4. The system provides detailed reports on bandwidth usage patterns and trends.

1. **Performance Analysis (3.2):**

**User Story:** As a network analyst, I want to analyse network performance trends and visualize the network topology.

* + **Acceptance Criteria:**
    1. The system provides a visual representation of the entire network topology.
    2. The network map dynamically updates as new devices are added to the network.
    3. Historical performance data is stored and analyzed for trend analysis.
    4. Performance reports can be generated for specific time intervals.

1. **Security Event Detection (3.3):**

**User Story:** As a security administrator, I want to detect and respond to security threats in real-time.

* + **Acceptance Criteria:**
    1. The system includes an Intrusion Detection System (IDS) to monitor network traffic for suspicious activities and anomalies.
    2. Immediate alerts are generated for potential security breaches.
    3. Log analysis is performed on log files from network devices and servers to identify security incidents.
    4. Logs are correlated to provide insights into security events.

1. **Network Configuration Management (3.4):**

**User Story:** As a network administrator, I want to manage and monitor network configurations to ensure compliance and reliability.

* + **Acceptance Criteria:**
    1. The system automatically backs up and version controls network device configurations.
    2. Users can compare configurations to identify changes.
    3. Compliance checks are performed to ensure network configurations comply with industry standards and internal policies.
    4. Automated alerts are generated for non-compliance issues.

1. **Alerts and Notifications (3.5):**

**User Story:** As a network manager, I want to receive timely alerts for network events and performance issues.

* + **Acceptance Criteria:**
    1. Users can set up custom alerts for specific events or thresholds.
    2. Alerts are delivered via email, SMS, or in-app notifications.
    3. Alert notifications include relevant details and actionable information.

1. **Reporting and Analytics (3.6):**

**User Story:** As a network administrator, I want to generate reports and analyze network performance data.

* + **Acceptance Criteria:**
    1. The system provides pre-built reports for network health, performance, and security events.
    2. Users can generate custom reports based on user-defined criteria.
    3. Trend analysis is performed to identify potential issues and predictive analytics are used for capacity planning.

1. **Integration with Third-party Tools (3.8):**

**User Story:** As a system integrator, I want to integrate the network monitoring system with third-party tools for enhanced security intelligence.

* + **Acceptance Criteria:**
    1. The system seamlessly integrates with Security Information and Event Management (SIEM) solutions.
    2. Compatibility with popular SIEM platforms such as Splunk, ELK Stack, and ArcSight is ensured.
    3. Extensive testing is conducted to ensure compatibility with a wide range of network devices, including routers, switches, firewalls, and load balancers.

These user stories and acceptance criteria outline the requirements for a comprehensive network monitoring solution that addresses various aspects of real-time monitoring, performance analysis, security event detection, configuration management, alerts and notifications, reporting, analytics, and integration with third-party tools.