Functional Overview

Automated Network Request Handling – ServiceNow

1. Introduction

The Automated Network Request Handling solution is built to streamline, standardize, and manage network-related service requests through ServiceNow.
This document explains the key input variables used during request submission and the approval workflows that control authorization.

2. Request Variables

The following catalog variables are used to gather complete and structured information, enabling smooth automation and accurate approval routing.

2.1 Request Category

- **Type:** Choice
- **Description:** Defines the type of network service being requested.
- **Examples:**
    - Network Access
    - Firewall Modification
    - VPN Access
    - Bandwidth Enhancement

- **Functional Purpose:** Determines workflow behavior and approval paths.

2.2 Business Justification

- **Type:** Multi-line text
- **Description:** Captures the business or technical reasoning behind the request.
- **Functional Purpose:** Helps approvers assess the requirement and validate compliance.

2.3 Application / Portal Information

- **Type:** Single-line text / URL
- **Description:** Identifies the system, application, or portal affected by the request.
- **Functional Purpose:** Assists the network team in understanding scope and minimizing rework.

2.4 Priority Level

- **Type:** Choice
- **Values:** Low, Medium, High, Critical
- **Description:** Indicates how urgent the request is.
- **Functional Purpose:** Determines priority handling, SLA impact, and escalation rules.

3. Approval Scenarios

Approval workflows are dynamically triggered based on parameters such as request type, urgency, and sensitivity.

3.1 Manager Approval (Standard Requests)

- **Applicable To:** Regular network service requests
- **Approval Flow:**
    - Routed to the requester's reporting manager
- **Purpose:**
    - Confirms business need and departmental alignment

3.2 Network Security Approval (High-Risk Requests)

- **Applicable To:**
    - Firewall modifications
    - VPN access
    - Sensitive network configurations
- **Approval Flow:**
    - Directed to the Network Security or Security Approval Group
- **Purpose:**
    - Ensures security policies and risk controls are enforced

3.3 Group Approval (Department-Specific Requests)

- **Applicable To:**

    - Requests associated with specific departments or network domains

- **Approval Flow:**
    - Routed to the appropriate departmental or network approval group
- **Purpose:**
    - Confirms technical feasibility and workload distribution

4. Functional Process Flow

User Submits Network Request
↓
Request Details Captured
(Request Type, Justification, Portal Information, Urgency)
↓
Flow Designer Evaluation
↓
→ Manager Approval (Standard)
→ Network Security Approval (High Sensitivity)
→ Department/Group Approval
↓
Approval Granted
↓
Request Fulfillment & Notification

5. Key Benefits

✔ Consistent and standardized request intake
✔ Automated, role-based approval process
✔ Reduced manual effort
✔ Improved governance and audit readiness
✔ Faster and more efficient service delivery

6. Conclusion

This functional design ensures efficient handling of network requests while maintaining strong governance, security controls, and operational transparency.
By utilizing structured inputs and dynamic approval workflows, the solution aligns with enterprise ITSM standards and ServiceNow best practices.