Functional Overview :

Automated Network Request Management – ServiceNow

1. Overview:

The Automated Network Request Management solution is designed to standardise, automate, and control network-related service requests using ServiceNow.
This functional overview outlines the **key variables** used for request intake and the **approval use cases** that govern request authorisation.

2. Variables:

The following catalogue variables are configured to capture complete and structured request information, enabling automation and accurate routing of approvals.

2.1 Request Type:

- **Type:** Choice
- **Description:** Identifies the category of network service being requested.
- **Examples:**
    - Network Access Request
    - Firewall Change
    - VPN Access
    - Bandwidth Upgrade
- **Functional Role:** Drives workflow logic and approval routing.

2.2 Justification:

- **Type:** Multi-line Text
- **Description:** Captures the business or technical reason for the request.
- **Functional Role:** Used by approvers to evaluate the necessity and compliance of the request.

2.3 Portal Details:

- **Type:** Single-line Text / URL
- **Description:** Specifies the application, system, or portal impacted by the network request.
- **Functional Role:** Provides clarity to the network fulfilment team and reduces rework.

2.4 Urgency:

- **Type:** Choice
- **Values:** Low, Medium, High, Critical
- **Description:** Indicates the time sensitivity of the request.
- **Functional Role:** Influences priority, SLA, and escalation logic.

3. Approval Use Cases:

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

3.1 Manager Approval (Standard Requests):

- **Applicable For:** Routine network requests
- **Approval Logic:**
  - Request routed to the requester’s reporting manager
- **Purpose:**
  - Ensures business justification and alignment with departmental needs

3.2 Network Security Approval (High-Sensitivity Requests):

- **Applicable For:**
  - Firewall changes
  - VPN access
  - High-risk network configurations
- **Approval Logic:**
  - Routed to the Network Security team or security approver group
- **Purpose:**
  - Enforces security policies and risk controls

3.3 Group Approval (Department-Specific Requests):

- **Applicable For:** Requests tied to specific departments or network domains
- **Approval Logic:**

    - ➔ Routed to the relevant network or department approval group
- **Purpose:**
    - ➔ Ensures technical feasibility and workload distribution

4. Functional Flow Diagram:

```
User Submits Network Request

          |

Catalog Variables Captured

(Request Type, Justification,

 Portal Details, Urgency)

          |

Flow Designer Evaluation

          |

          +--> Manager Approval (Standard)

          |

          +--> Network Security Approval (High Sensitivity)

          |

          +--> Group Approval (Department-Based)

          |

Approval Granted

          |

Request Fulfillment & Notification
```

5. Functional Benefits:

✔️ Standardised request intake
✔️ Automated and role-based approvals
✔️ Reduced manual intervention

✔️ Improved compliance and auditability
✔️ Faster and more reliable service delivery

6. Summary

This functional design ensures that network requests are processed efficiently while maintaining governance, security, and operational control.
By leveraging structured variables and dynamic approval use cases, the solution aligns with enterprise ITSM best practices and ServiceNow automation standards.