

Project Design Phase

Solution Architecture

Date:	21-12-2025
Team ID:	
Project Name:	Automated Network Request Management in ServiceNow
Maximum Marks:	4 Marks

Solution Architecture

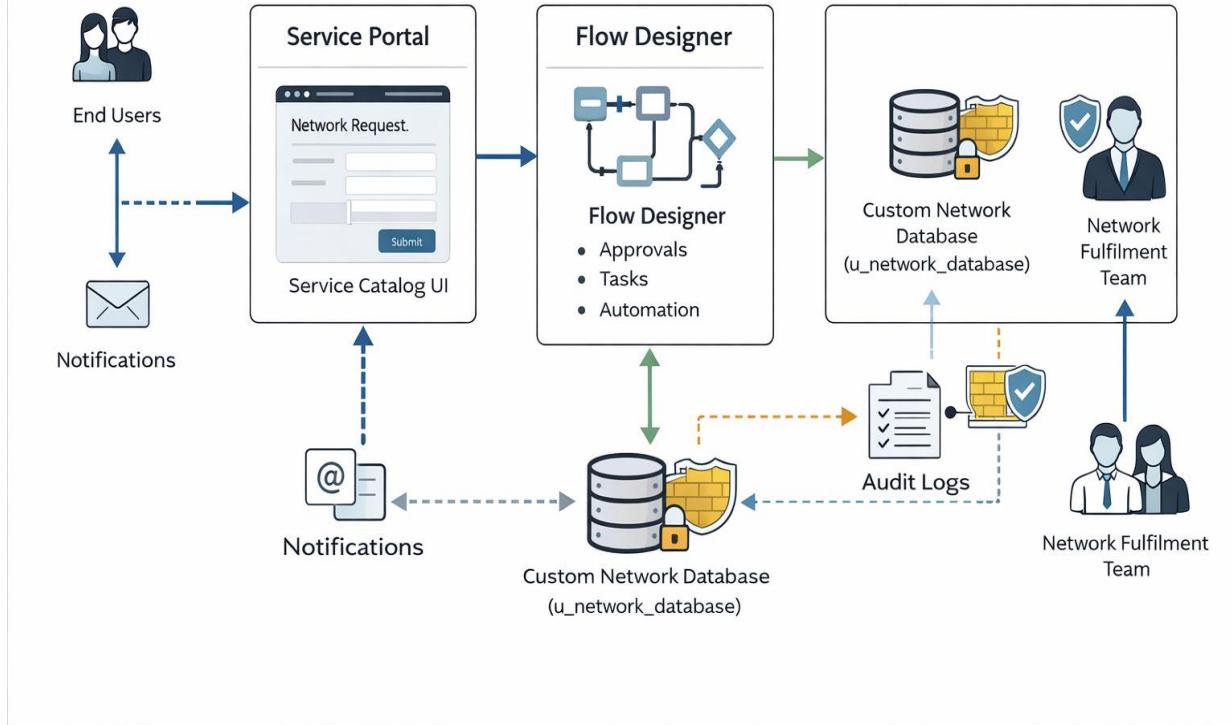
Solution architecture defines the high-level structure of the Automated Network Request Management system and explains how business requirements are transformed into a technical solution using the ServiceNow platform. It acts as a blueprint that connects business objectives with system components, workflows, and data architecture.

The primary goals of the solution architecture are to:

- Provide an efficient and automated platform for managing network-related service requests.
- Reduce manual effort and errors through standardized workflows and automation.
- Enable real-time visibility and tracking of network requests.
- Ensure compliance, security, and auditability through role-based access and approval mechanisms.
- Support scalability and future enhancements within the ServiceNow ecosystem.

Example - Solution Architecture Diagram:

Solution Architecture Diagram



Architectural Components

1. User Interface Layer

- ServiceNow Service Portal acts as the front-end interface.
- End users submit network requests through a structured Service Catalog.
- Dynamic forms and variable sets capture accurate request details.

2. Application Layer

- Service Catalog Items define different network request types.
- UI Policies and Client Scripts control dynamic behavior and validations.
- Flow Designer manages request lifecycle automation and approvals.

3. Workflow & Approval Layer

- Automated approval flows route requests to managers or network teams.
- Conditional logic ensures approvals are completed before fulfillment.

- Notifications are triggered at each stage of the request lifecycle.

4. Data Layer

- Custom Network Database table (u_network_database) stores request data.
- Catalog variables are mapped to structured fields for reporting and audits.
- Audit logs track approvals, updates, and status changes.

5. Security & Access Control Layer

- Role-based Access Control Lists (ACLs) restrict read/write permissions.
- Approval enforcement ensures compliance with IT and security policies.
- System logs provide traceability and accountability.