NetSentinel – Design Document

Purpose

NetSentinel provides scalable, plug-and-play network observability by collecting, processing, and analyzing telemetry data from a wide variety of network devices (switches, routers, firewalls, etc.). It's designed for cloud, on-premise, and edge deployments.

High-Level Architecture

[Devices] → [NetProbe] → Kafka → [SentinelCore] → [AlertManager] → [Dashboards / Ops Tools]

Components

Component	Description
NetProbe	Collects ICMP, SNMP, SSH data. Performs auto-discovery.
Kafka	Central event bus. Producers: NetProbe. Consumers: SentinelCore, AlertManager.
SentinelCore	Processes and detects anomalies. Sends alerts to Kafka.
AlertManager	Routes alerts to Slack, email, webhooks, or auto-remediation.

Technologies Used

Layer	Technology
Collection	Go, SNMP, ICMP, SSH
Messaging	Apache Kafka
Processing	Go, Flink/Spark (optional)
Anomaly Detection	Rule-based initially, LSTM later
Alerts	Webhooks, Slack, Redis
Security	TLS 1.3, AES-256, RBAC

Folder Structure

```
netsentinel/ ■■■ netprobe/ # Data collection agents (ICMP, SNMP, SSH, Discovery)
■■■ kafka-service/ # Kafka integration (producer/consumer) ■■■ sentinel-core/ #
Processing and anomaly detection ■■■ alertmanager/ # Notification and escalation
■■■ dashboard/ # Optional visualization layer
```

Implementation Roadmap

Phase	Feature	Duration
1	Core ICMP/SNMP/SSH collection	2–3 weeks

2	Kafka integration	1 week
3	SentinelCore + Alerting	2–3 weeks
4	LSTM anomaly detection	2 weeks
5	Dashboard & configs	Ongoing