Incident Management for Network Service

draft-feng-opsawg-incident-management-00

Chong Feng(frank.Fengchong@Huawei.com)

Tong Hu(hutong@cmhi.chinamobile.com)

Luis Contreras 〔luismiguel.contrerasmurillo@telefonica.com〕
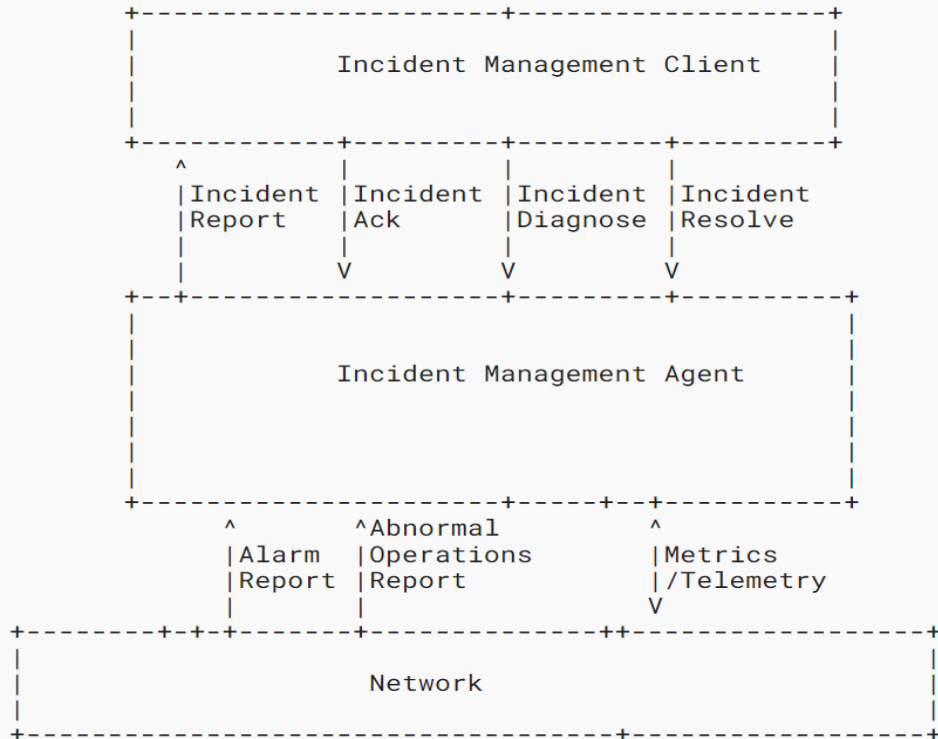
Qin Wu(bill.wu@huawei.com)

Chaode Yu(yuchaode@huawei.com)

Motivation

- The management system is overwhelmed by the frequency and quantity of alarms, KPI, trace information with the growth of new service and service complexity
    - result in low processing efficiency, inaccurate root cause identification and duplicated tickets.

- The management system is built as a silo and manages performance data, fault data, trace information separately
    - However the investigation of some faults also depends on some other data like topology data or performance data
    - It is difficult to assess the impact of alarms and/or metrics on network services

Proposed Solution Overview

Incident is the unexpected interruption of network services, degradation of network service quality or sub-health of network services.

```
+----------------------+--------------------+
|                      |                    |
|       Incident Management Client          |
|                      |                    |
|                      |                    |
+--------+----------+---------+-----------+-+
         ^          |         |           |
         |Incident  |Incident |Incident   |Incident
         |Report    |Ack      |Diagnose   |Resolve
         |          V         V           V
+--+-----------------+---------+-----------+
|                                          |
|                                          |
|       Incident Management Agent          |
|                                          |
|                                          |
|                                          |
+--------------------+-----+--+------------+
         ^           ^Abnormal        ^
         |Alarm      |Operations      |Metrics
         |Report     |Report          |/Telemetry
         |           |                V
+--------+-+-+-------+----------++----------------+
|                                                 |
|                   Network                       |
|                                                 |
+----------------------------+--------------------+
```

- Incident management is proposed to:
  - Provide consistent management of different type of data sources by aggregating various different Performance data, alarm data, trace information into the incident for the network service
    - Align with TMF724A "Incident Management API Profile "
  - Identify the relationship between the incident and the network service
    - One incident is corresponding to either one or multiple network service
    - The relationship between the incident and the network service can be preconfigured
      - E.g., derived from the relation between subservice and symptom in the Service assurance model
    - The relationship between the incident and the network service can be identified
      - Using Service Impact analysis
  - Use AI and troubleshooting API to accurately identify the root causes of device, network, and service faults and report the root causes to the O&M system of the carrier through the incident northbound interface
    - Incident report/querying
   - Incident diagnosis
    - Incident resolution

Use Cases

Preconfigure the relation between the network service, incident, trigger the incident when a set of alarms (e.g., IGP down) affect the service
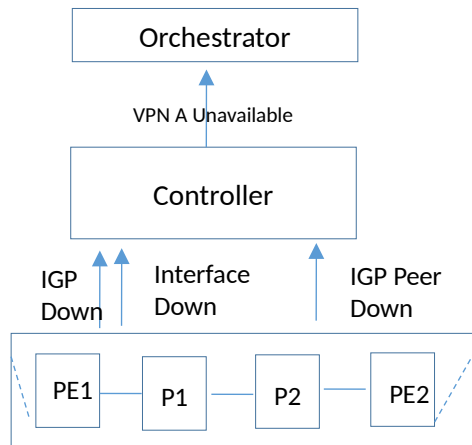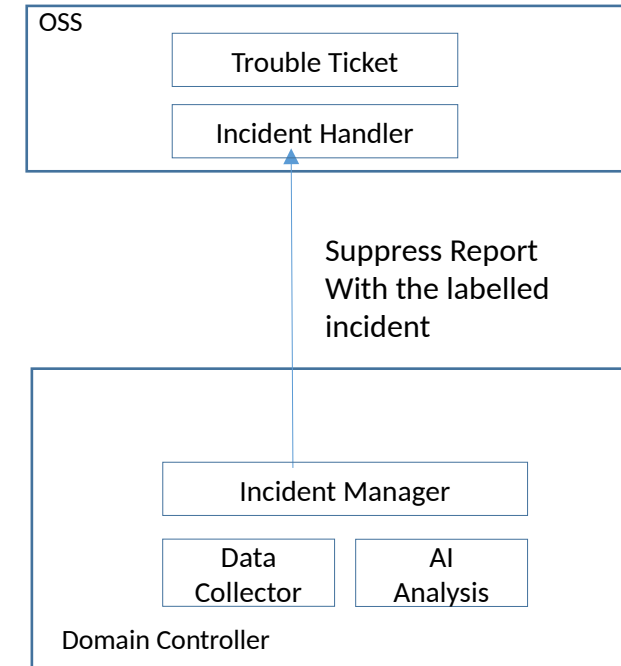
Preconfigure the relation between the network service and incident, trigger the incident when degraded service Impact user experience
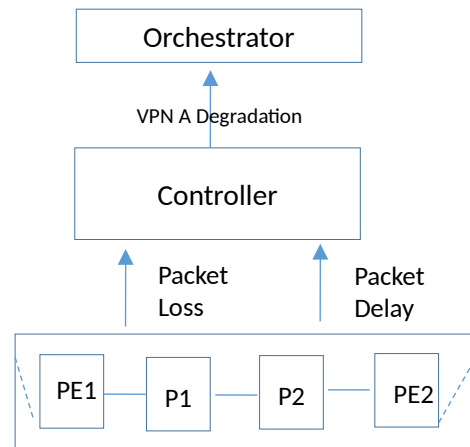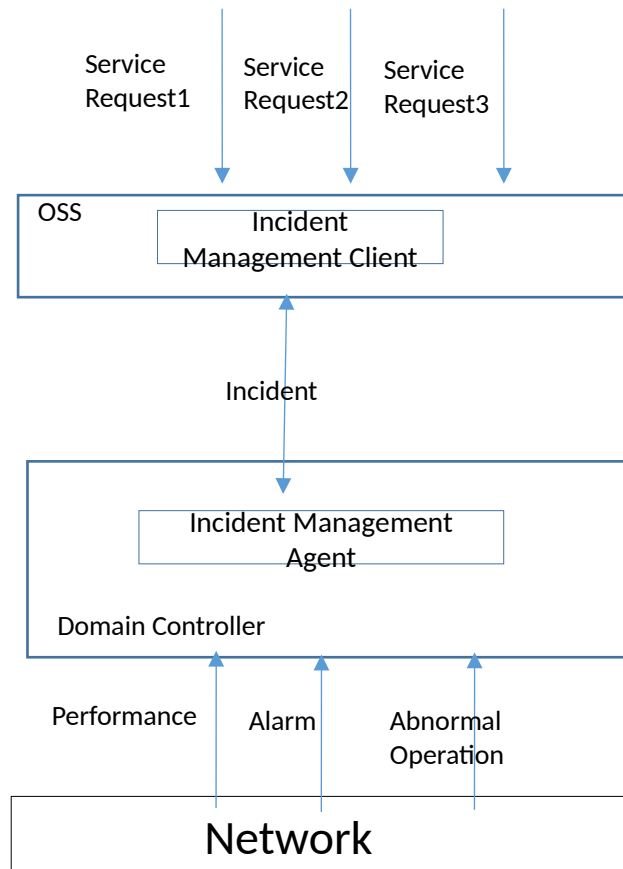
Identify the relation between the network service and the incident Dynamically based on Service Impact analysis results
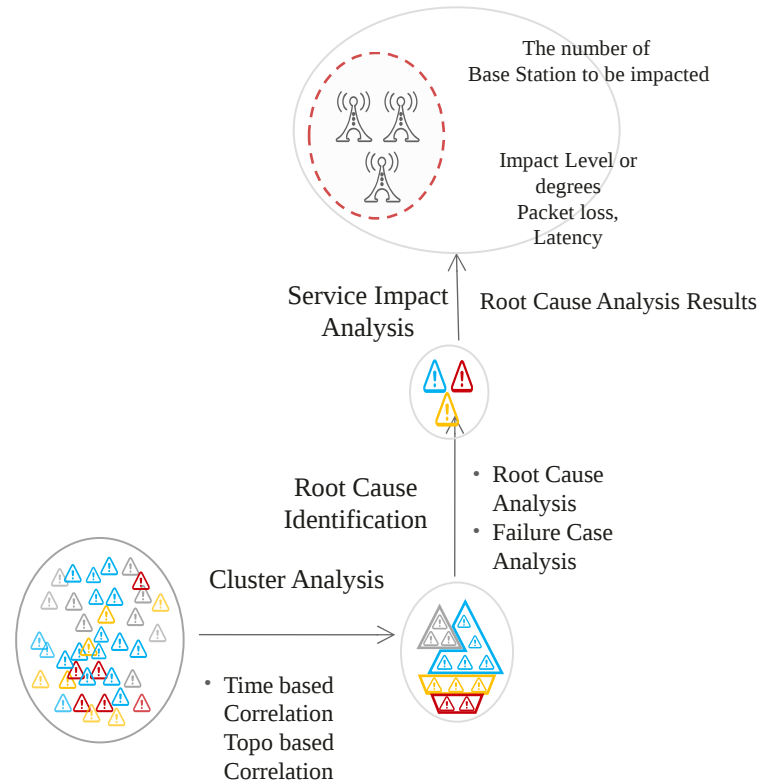
Exclude or suppress the incidents based on incident label or local policy during cutover or energy saving period

Orchestrator

VPN A Unavailable

Controller

IGP Down | Interface Down | IGP Peer Down

PE1 — P1 — P2 — PE2

Orchestrator

VPN A Degradation

Controller

Packet Loss | Packet Delay

PE1 — P1 — P2 — PE2

The number of Base Station to be impacted

Impact Level or degrees Packet loss, Latency

Service Impact Analysis | Root Cause Analysis Results

Root Cause Identification
- Root Cause Analysis
- Failure Case Analysis

Cluster Analysis
- Time based Correlation Topo based Correlation

OSS
Trouble Ticket
Incident Handler

Suppress Report With the labelled incident

Domain Controller
Incident Manager
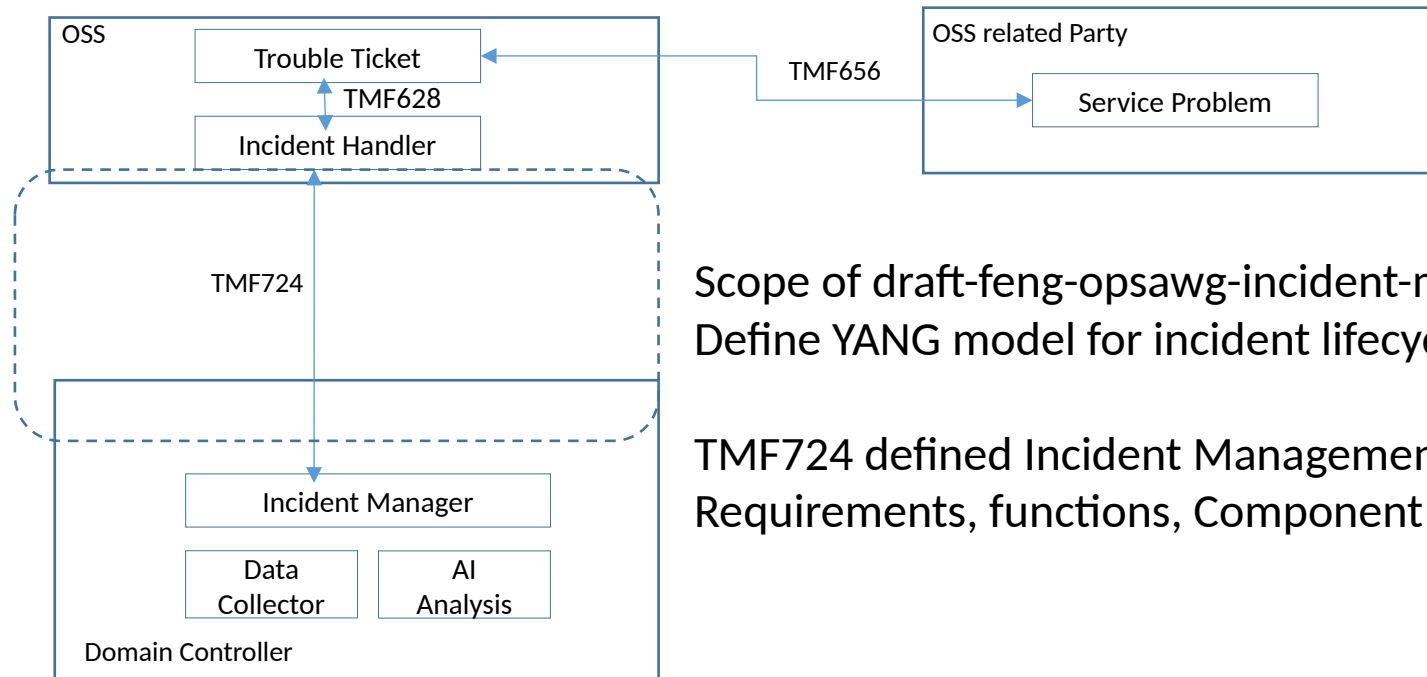Data Collector | AI Analysis

Incident vs Alarms vs Performance

- alarm information, performance anomaly information, maintenance information are used for troubleshooting to provide more fine granularity root cause analysis.

- One incident can take multiple alarms/performance metrics, abnormal operation events as input and is triggered when the service is affected.

- Multiple Services can be affected by the same incident.

Comments? Questions?

Relation with TMF Incident Management Profile

OSS

Trouble Ticket

TMF628

Incident Handler

OSS related Party

Service Problem

TMF656

TMF724

Incident Manager

Data Collector

AI Analysis

Domain Controller

Scope of draft-feng-opsawg-incident-management-00
Define YANG model for incident lifecycle management

TMF724 defined Incident Management API profile including
Requirements, functions, Component capability.

TMF656 Service Problem Management API User Guide
TMF724 Incident Management API Profile
TMF628 Performance Management API REST Specification