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)

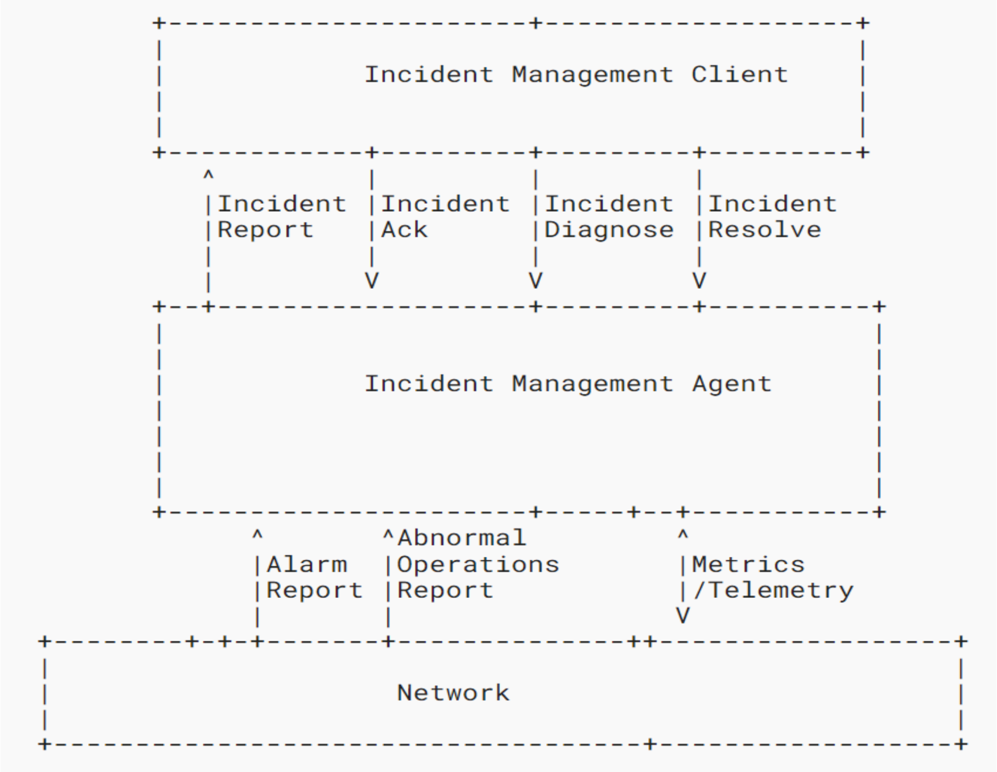
Motivation

- 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

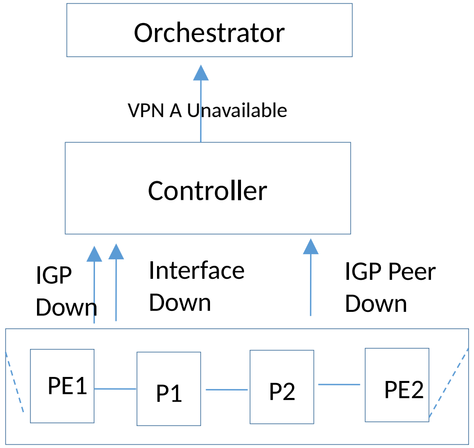
Use Cases

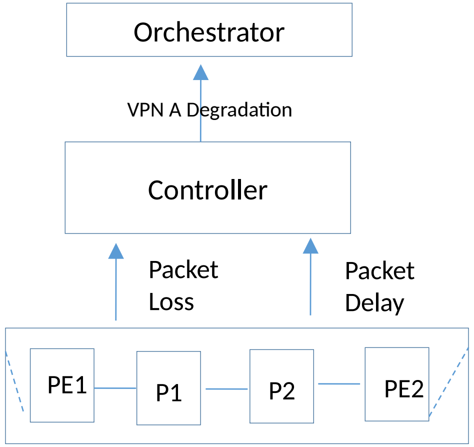
Preconfigure the relation between the network service, incident, trigger the incident when a set of alarms (e.g., IGP down) affect the service

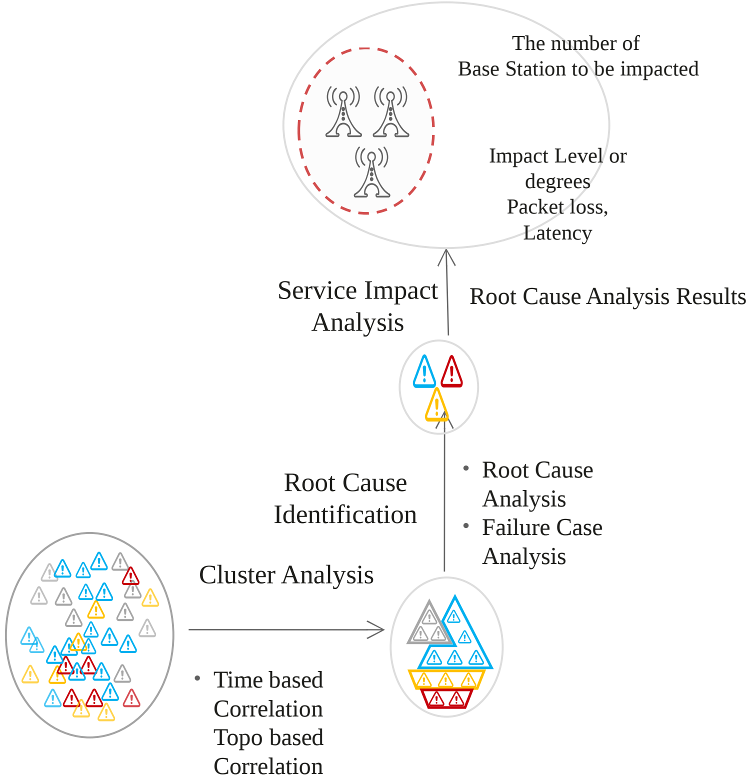
Preconfigure the relation between the network service and incident, trigger the incident when degraded service Impact user experience

Identify the relation between the network service and the incident Dynamically based on Service Impact analysis results

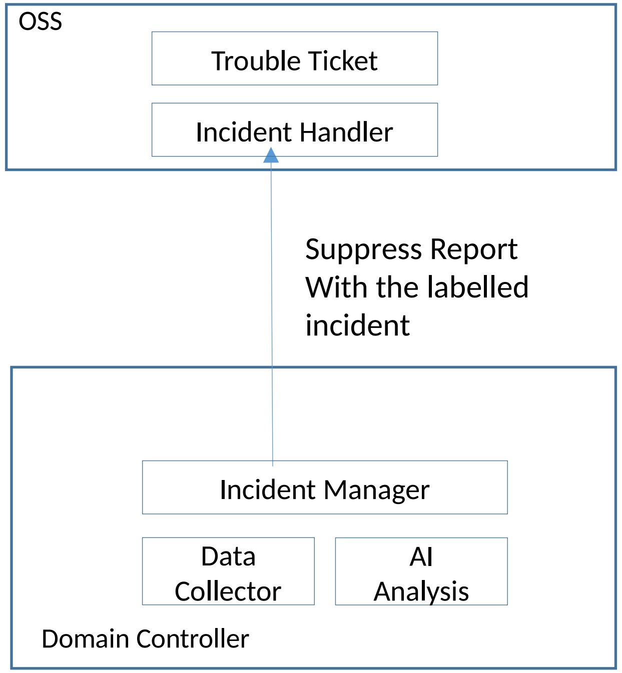
Exclude or suppress the incidents based on incident label or local policy during cutover or energy saving period



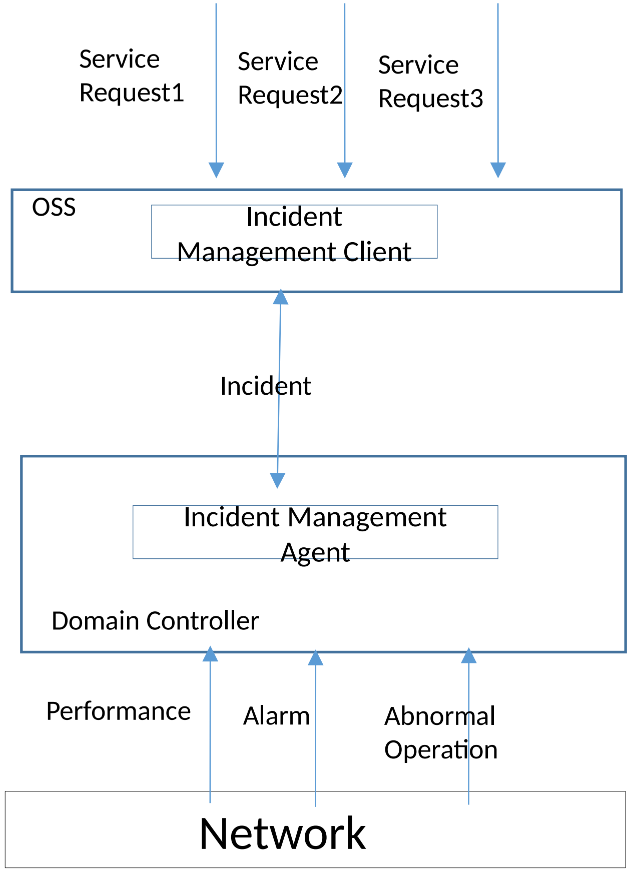




The number of Base Station to be impacted
Impact Level or degrees Packet loss, Latency
Service Impact Analysis
Root Cause Analysis Results
Root Cause Identification
• Root Cause Analysis
• Failure Case Analysis
Cluster Analysis
• Time based Correlation Topo based Correlation

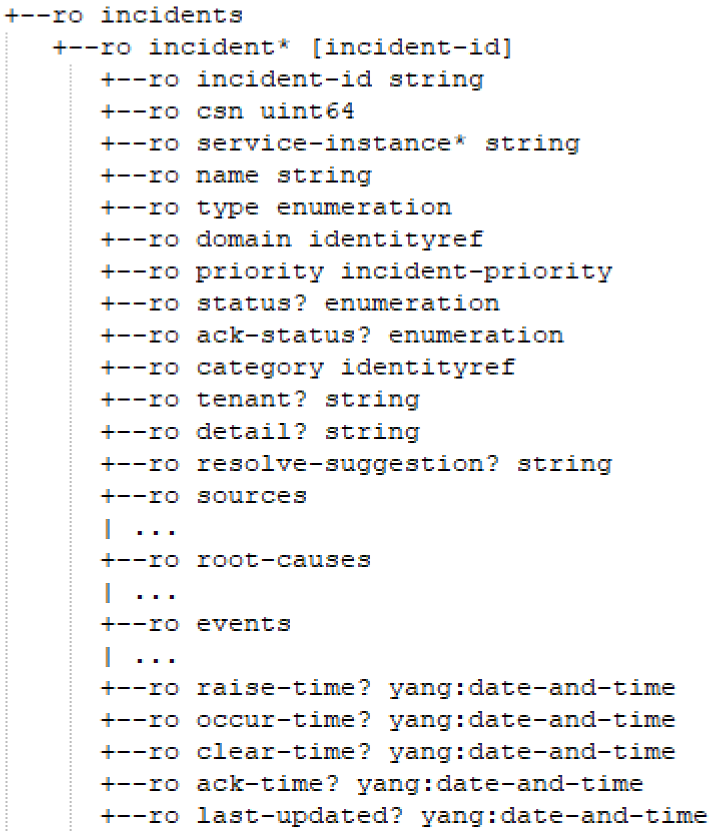


Incident vs Alarms vs Performance



- 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.

Data Model for Incident

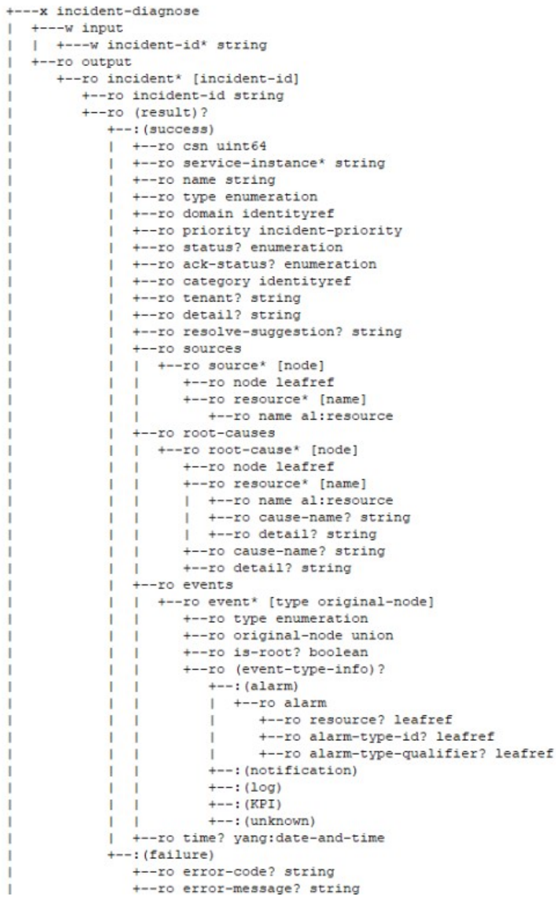


```
+--ro incidents
   +--ro incident* [incident-id]
      +--ro incident-id string
      +--ro csn uint64
      +--ro service-instance* string
      +--ro name string
      +--ro type enumeration
      +--ro domain identityref
      +--ro priority incident-priority
      +--ro status? enumeration
      +--ro ack-status? enumeration
      +--ro category identityref
      +--ro tenant? string
      +--ro detail? string
      +--ro resolve-suggestion? string
      +--ro sources
      | ...
      +--ro root-causes
      | ...
      +--ro events
      | ...
      +--ro raise-time? yang:date-and-time
      +--ro occur-time? yang:date-and-time
      +--ro clear-time? yang:date-and-time
      +--ro ack-time? yang:date-and-time
      +--ro last-updated? yang:date-and-time
```

An incident instance is identified by incident-id, associated with one or more network instances, and contains some critical members.

- Incident-id: the identifier of an incident instance, it MUST be unique in the whole system.
- Domain: it indicates the domain where the incident instance occurs. Such as RAN, OTN, PTN, etc.
- Category: it indicates the component where the incident instance occurs. Such as power system, line card, protocol, etc.
- Priority: indicates the priority of this incident instance.
- Sources: indicates the objects that have symptoms related to an incident instance. Such as down interface, high CPU, etc.
- Root-causes: indicates the root cause objects related to a incident instance.
- Events: the events associated with an incident instance, including alarms, logs, KPIs and other events.

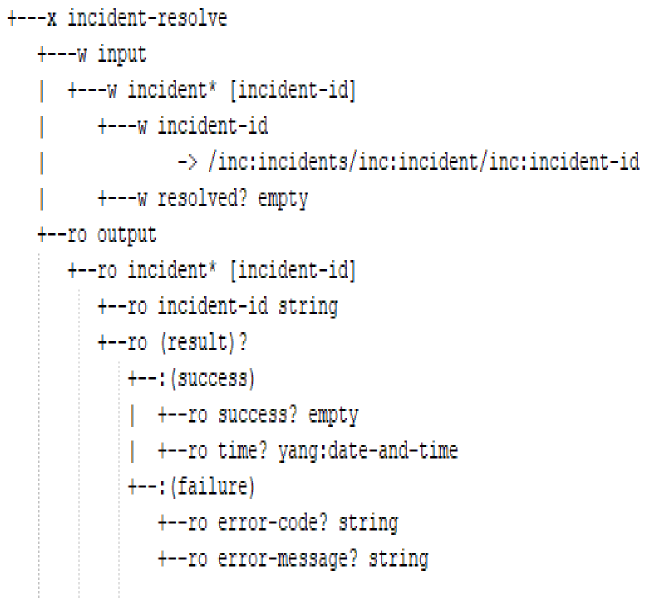
Incident Diagnosis



```
+---x incident-diagnose
|  +---w input
|  |  +---w incident-id* string
|  +--ro output
|     +--ro incident* [incident-id]
|        +--ro incident-id string
|        +--ro (result)?
|           +--:(success)
|           |  +--ro csn uint64
|           |  +--ro service-instance* string
|           |  +--ro name string
|           |  +--ro type enumeration
|           |  +--ro domain identityref
|           |  +--ro priority incident-priority
|           |  +--ro status? enumeration
|           |  +--ro ack-status? enumeration
|           |  +--ro category identityref
|           |  +--ro tenant? string
|           |  +--ro detail? string
|           |  +--ro resolve-suggestion? string
|           |  +--ro sources
|           |  |  +--ro source* [node]
|           |  |     +--ro node leafref
|           |  |     +--ro resource* [name]
|           |  |        +--ro name al:resource
|           |  +--ro root-causes
|           |  |  +--ro root-cause* [node]
|           |  |     +--ro node leafref
|           |  |     +--ro resource* [name]
|           |  |     |  +--ro name al:resource
|           |  |     |  +--ro cause-name? string
|           |  |     |  +--ro detail? string
|           |  |     +--ro cause-name? string
|           |  |     +--ro detail? string
|           |  +--ro events
|           |  |  +--ro event* [type original-node]
|           |  |     +--ro type enumeration
|           |  |     +--ro original-node union
|           |  |     +--ro is-root? boolean
|           |  |     +--ro (event-type-info)?
|           |  |        +--:(alarm)
|           |  |        |  +--ro alarm
|           |  |        |     +--ro resource? leafref
|           |  |        |     +--ro alarm-type-id? leafref
|           |  |        |     +--ro alarm-type-qualifier? leafref
|           |  |        +--:(notification)
|           |  |        +--:(log)
|           |  |        +--:(KPI)
|           |  |        +--:(unknown)
|           |  +--ro time? yang:date-and-time
|           +--:(failure)
|              +--ro error-code? string
|              +--ro error-message? string
```

- Incident diagnose rpc can be used to find root causes.
- Possible diagnosis methods include link reachability detection, link quality detection, alarm/log analysis, and short-term fine-grained monitoring of network quality metrics, etc.

Incident Resolution

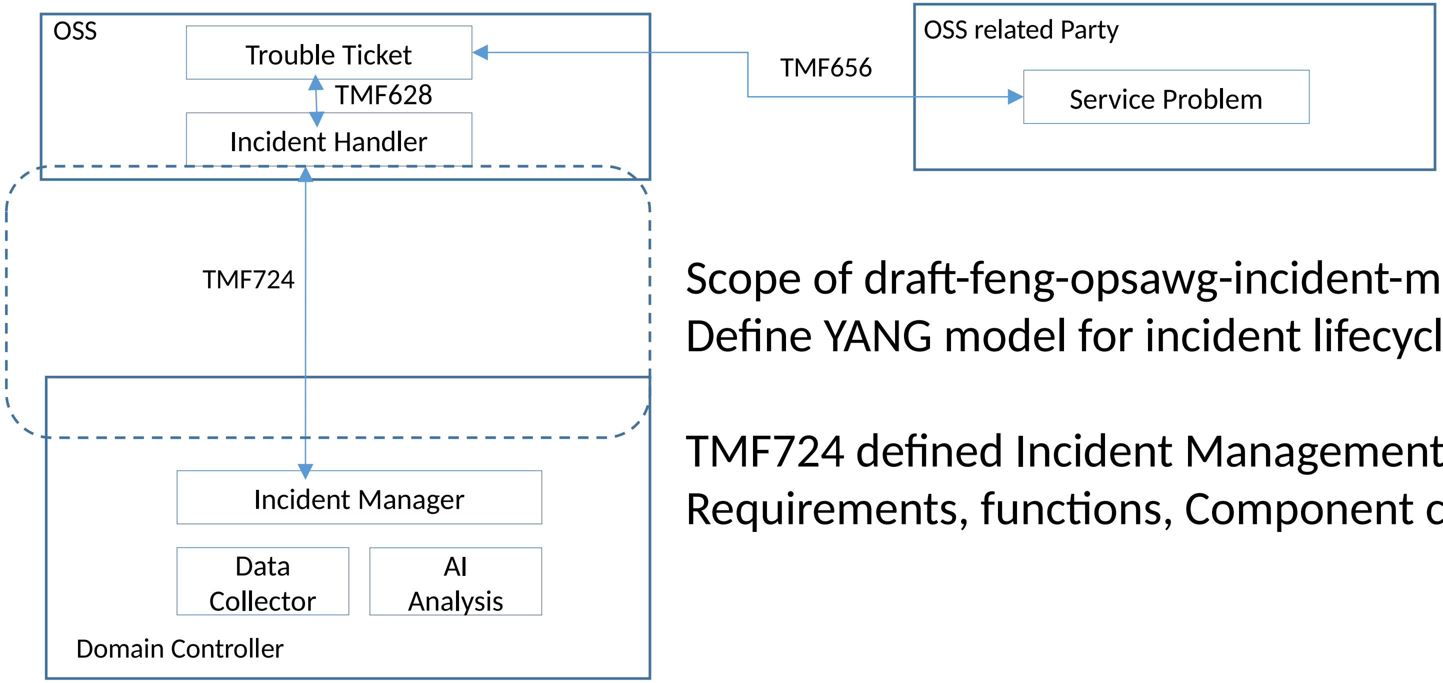


```
+---x incident-resolve
   +---w input
   |  +---w incident* [incident-id]
   |     +---w incident-id
   |             -> /inc:incidents/inc:incident/inc:incident-id
   |     +---w resolved? empty
   +--ro output
      +--ro incident* [incident-id]
         +--ro incident-id string
         +--ro (result)?
            +--:(success)
            |  +--ro success? empty
            |  +--ro time? yang:date-and-time
            +--:(failure)
               +--ro error-code? string
               +--ro error-message? string
```

- After the root cause is diagnosed, the client MAY resolve the incident.
- The client MAY choose resolve the incident by invoking other functions, such as routing calculation function, configuration function, dispatching a ticket or asking the agent to resolve it.

Comments? Questions?

Relation with TMF Incident Management Profile



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