Incident Management for Network Service

draft-feng-opsawg-incident-management-03

Chong Feng(Fengchonglly@gmail.com)

Tong Hu(hutong@cmhi.chinamobile.com)

Luis Contreras （luismiguel.contrerasmurillo@telefonica.com）

Thomas Graf (thomas.graf@swisscom.com)

Qin Wu(bill.wu@huawei.com)

Chaode Yu(yuchaode@huawei.com)

Nigel Davis (ndavis@ciena.com)

Recap

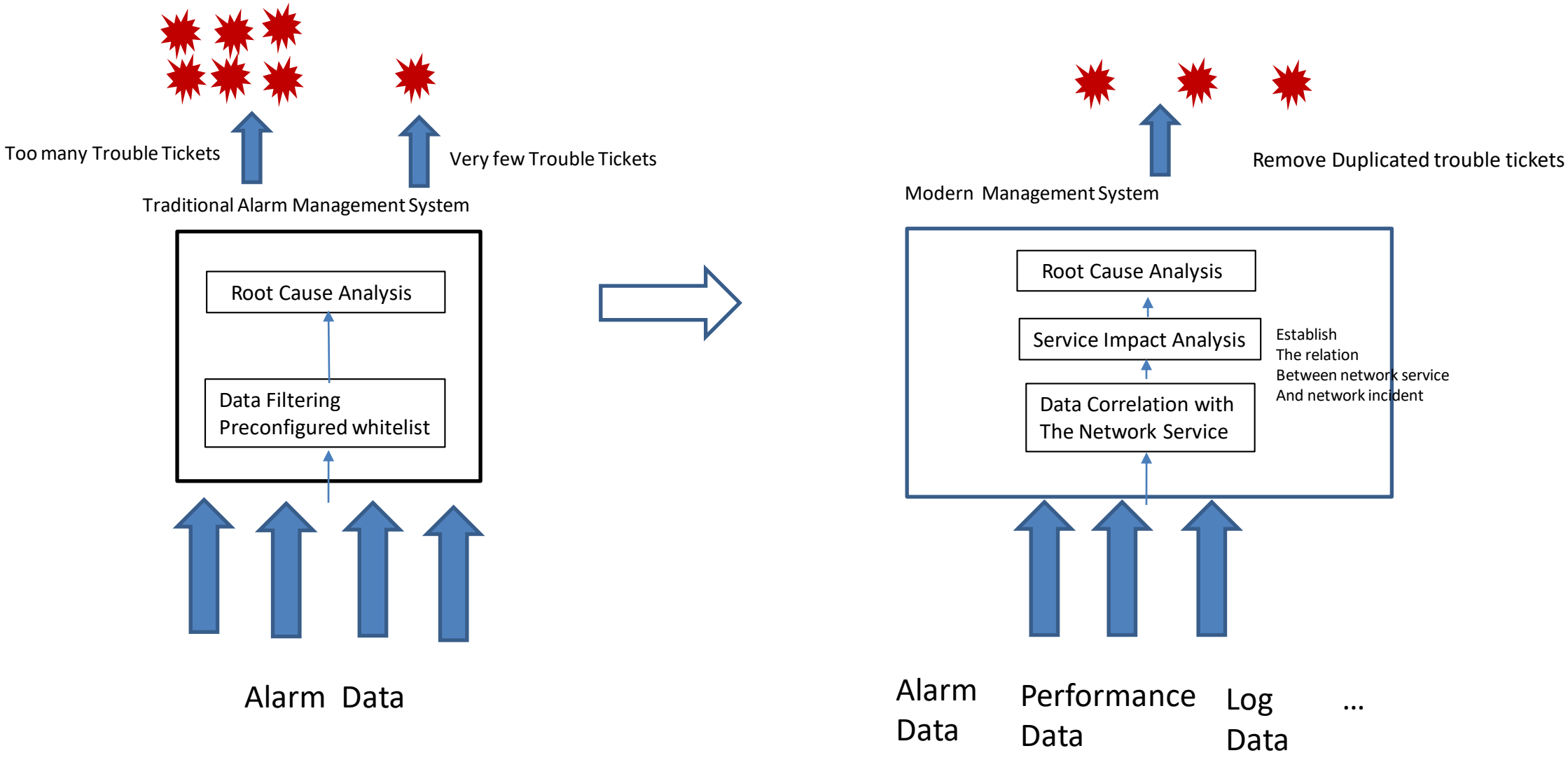
- Problem Space
  - The frequency and quantity of alarms and performance metrics data reported to OSS overwhelm the management systems
    - Traditional method such as data compression is time consuming, and labor intensive
  - Data source such as alarm, performance metrics are managed by the management system separately, difficult to assess the impact of alarms, performance metrics and other anomaly data on network services without known
    - relation across layer of the network topology data
    - or the relation with other network topology data.
- The goal of this document is to develop a network wide incident-centric solution is proposed to
  - establish dependency relation with network service
  - Establish dependency relation with network topology at different layers
  - Allow upper layer OSS has user friendly open API to investigate incident

Document Status

- draft-feng-opsawg-incident-management
  - v-00 was first presented in NETCONF WG and NETMOD in the IETF 116 meeting, and
    - it was suggested to align with trace context series drafts and clarify the relation with them.
  - The draft also received comments/inputs from Thomas Graf, Nigel, Luis, Med, etc
    - Regarding relation with TMF incident profile specification, Luis suggested to focus on network level on top of domain controller and add new cases on incident generation based SLO violation.
    - Thomas encouraged to add more details on multi-domain cases, e.g., one related to SRv6 Network visibility
    - Med provided good input to introduction on motivation and goal clarification.
  - V-01 was later presented in OPSAWG WG
    - Thomas and Nigel were added as coauthor
    - The relation with Alarm, TMF incident profile, Service Assurance and trace context draft were presented
    - Incident model design and update was discussed

- The latest update is v-(03), changes compared to the previous versions:
  - Motivation and goal clarification in the introduction section.
  - Revise sample use case section, keep two original cases and Add one new use cases on Incident Generation based on Luis's input.
  - Add some text to the model design overview.
  - Add reference to Precision Availability Metric defined in IPPM PAM WG document.

UC1: Duplicated trouble tickets Reduction



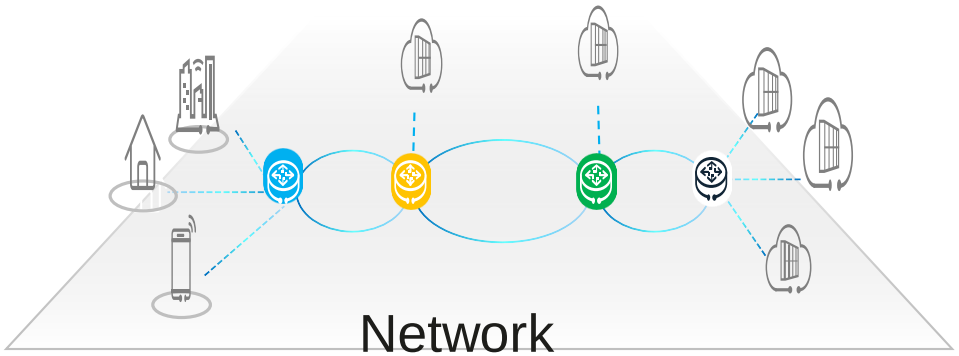
UC2: Incident Creation based on SLO violation

OSS

2. Use SAP model and VPN PM model to establish service topology view And Path Quality View

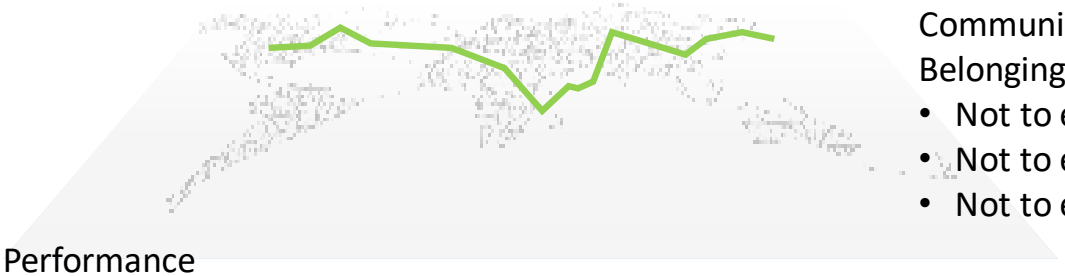
Network Controller
（Domain Controller）

1.Collect Topo data, Network Performance Data and Flow Statistics Data



3. Monitor service flow across end to end connectivity between VPN Site A, VPN Site B, VPN Site C

Service Topology



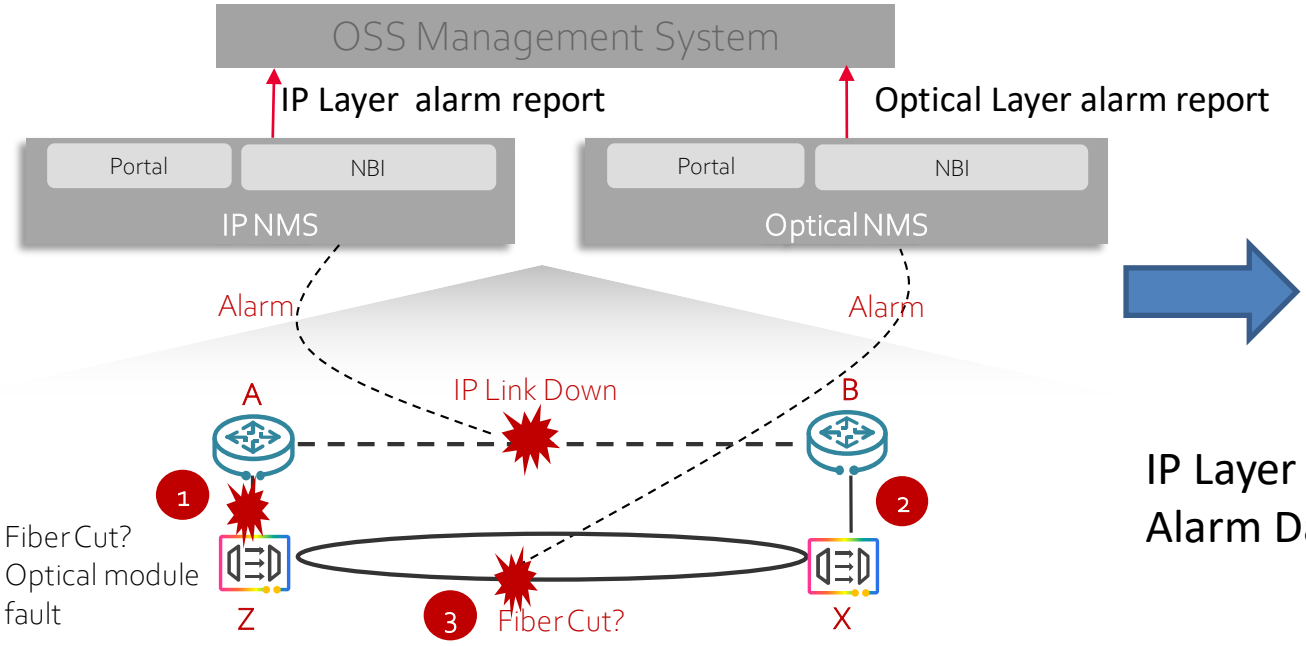
End to End SLO Objective for service flow Communicated between several vpn sites Belonging to the same L3VPN Service

- Not to exceed 30 ms for any packet;
- Not to exceed 25 ms for 99.999% of packets;
- Not to exceed 20 ms for 99% of packets.

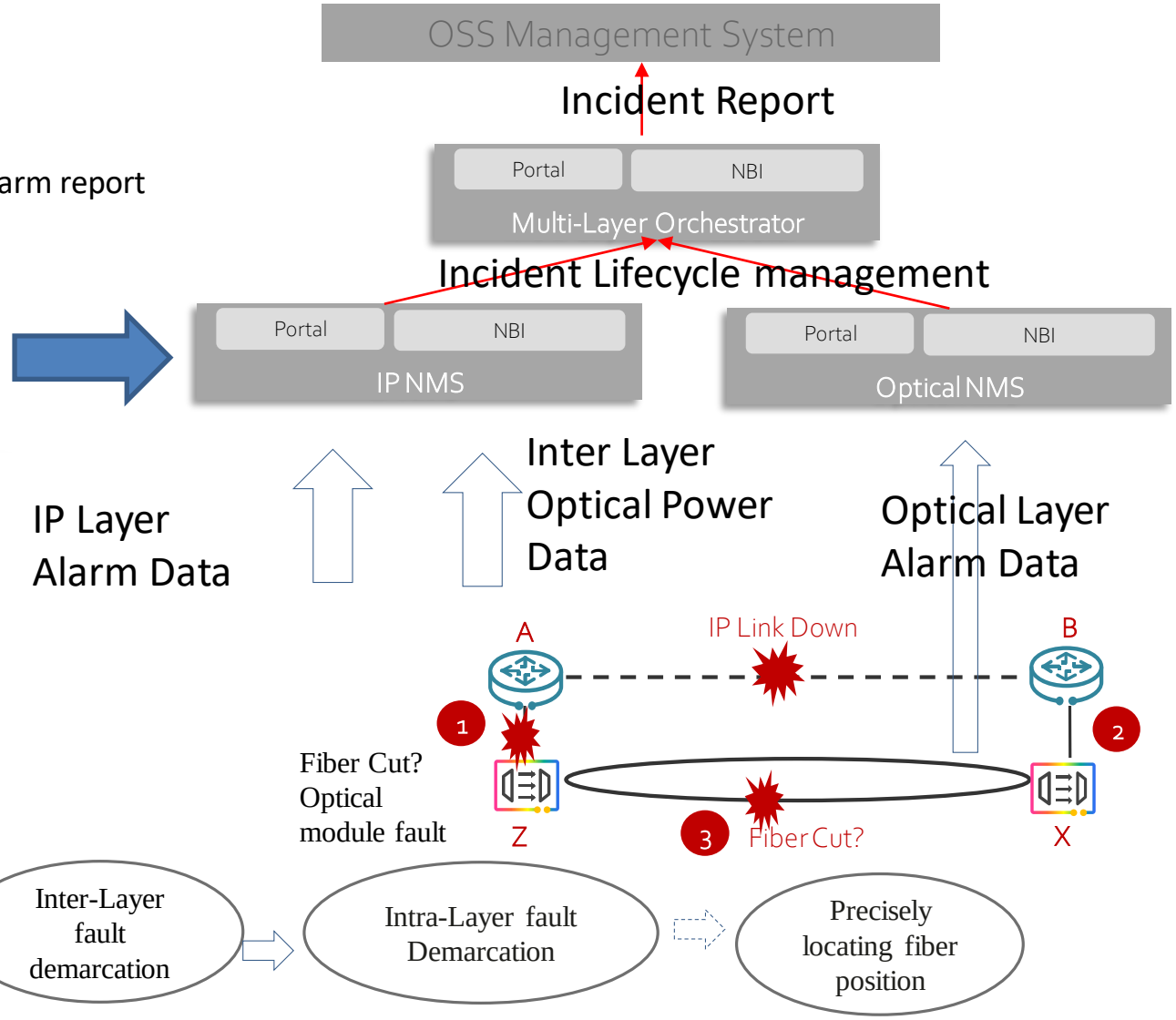
4. Upon SLO is violated, the incident will be generated by Network Controller to report to OSS

UC3: Multi-Layer Fault Management

IP layer link-down, w/o multi-team collaboration, long locating time



Difficult fault Demarcation：Fault is happened in optical network or in the inter-layer link? Which side occurred, 1 or 2?



Model Design Overview

```
module: ietf-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? int:incident-priority
        +--ro status? enumeration
        +--ro ack-status? enumeration
        +--ro category? identityref
        +--ro detail? string
        +--ro resolve-advice? string
        +--ro sources
        ...
        +--ro root-causes
        ...
        +--ro root-events
        ...
        +--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
```

Describe relation with network service

Describe with Network Topology and Network Domain

```
rpcs:
  +---x incident-acknowledge
  ...
  +---x incident-diagnose
  ...
  +---x incident-resolve

notifications:
  +---n incident-notification
     +--ro incident-id?
             -> /inc:incidents/inc:incident/inc:incident-id
     ...
     +--ro time? yang:date-and-time
```

Provide Open API between OSS and Domain Specific Controller to exchange Incident information

Next Step

- Request WG adoption?
- **Key value of network incident management**
  - **Reduce trouble ticket duplication to** improve incident diagnosis efficiency and low O&M requirements
  - **Assess impact of alarm, log, KPI data on network service to** improve network maintenance efficiency.
  - Correlate with network topo to provide multi-layer, multi-domain network observability
- Explore how model parameters can be extended to support L3VPN service unavailability monitoring
- **Address** any issues raised in this meeting