Cross-Domain Orchestration to enable Service Assurance

Noam Ben-Gal

Solutions Architect, Software Integration and Orchestration Practice, CITT Advanced Services

July 9, 2015

Overview

Think about a network that is complete, with one interface to all devices and single set of operational tools to support it, think how easy it would be to provide service assurance and guarantee SLAs…

With Cisco NSO Cross Domain Orchestration solution this is possible, introducing a “bridge” to control the multi-silos environments by orchestrating services across domains, no hassle of device centric interfaces but worry only about your end customer services offering.

Such a solution with proper design will hold insides and outsides of the services orchestrated so Service Assurance system (OSS) can leverage as input to its impact containers. this top to bottom approach really focused on the end service instead of dealing with topology calculation and accuracy and/or correlation rules complexity.

The usual

- Multiple management domain leads to multiple operation domains acting as isolated silos. this leads to complex to impossible end to end monitoring, capacity fault correlation and RCA.
- This also leads to OPEX increase over the years with separate operation teams and lack of communication between them, each team is responsible and accountable for its own domain.
- Hard to impossible to provide cross platforms Business Service health and impact to guarantee top most SLA.

CPE domain manager

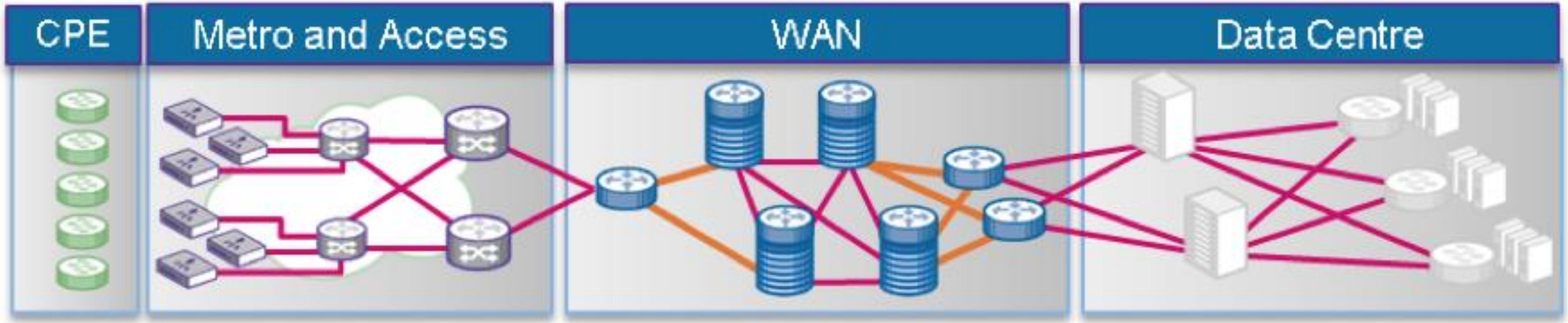
Optical Domain manager

Access Domain Manager

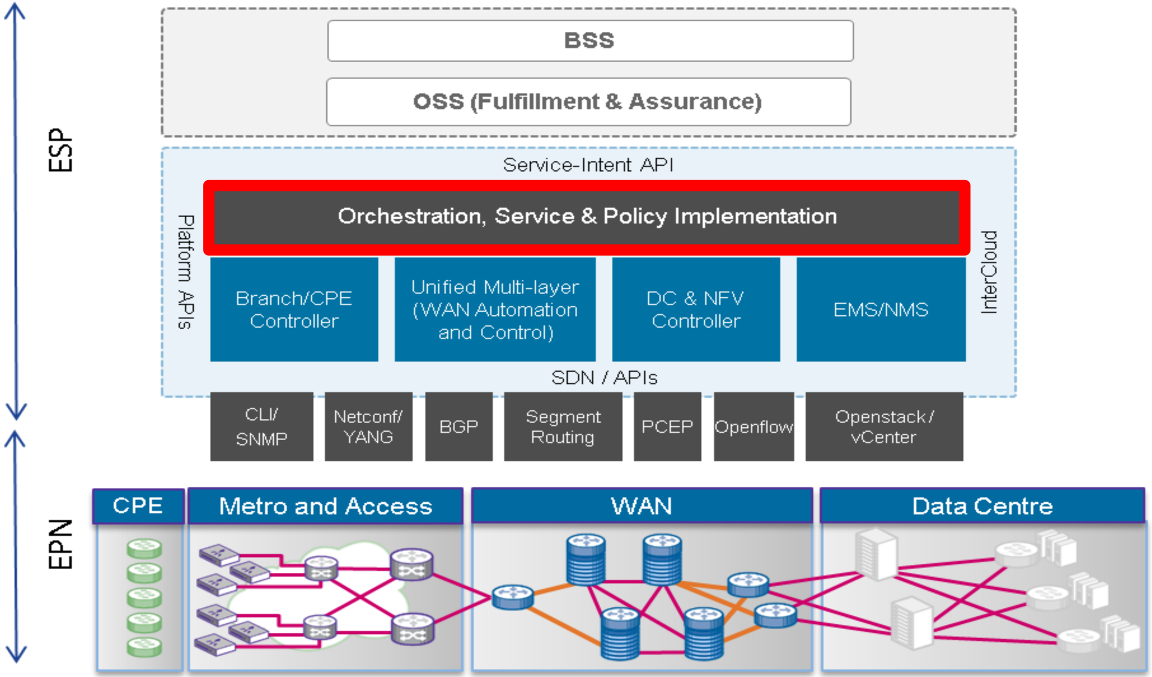
WAN Domain Manager

DC Domain Manager

Multiple instrumentation and interfaces: TL1, Cobra, CLI (Telnet/SSH), SNMP, Netconf…

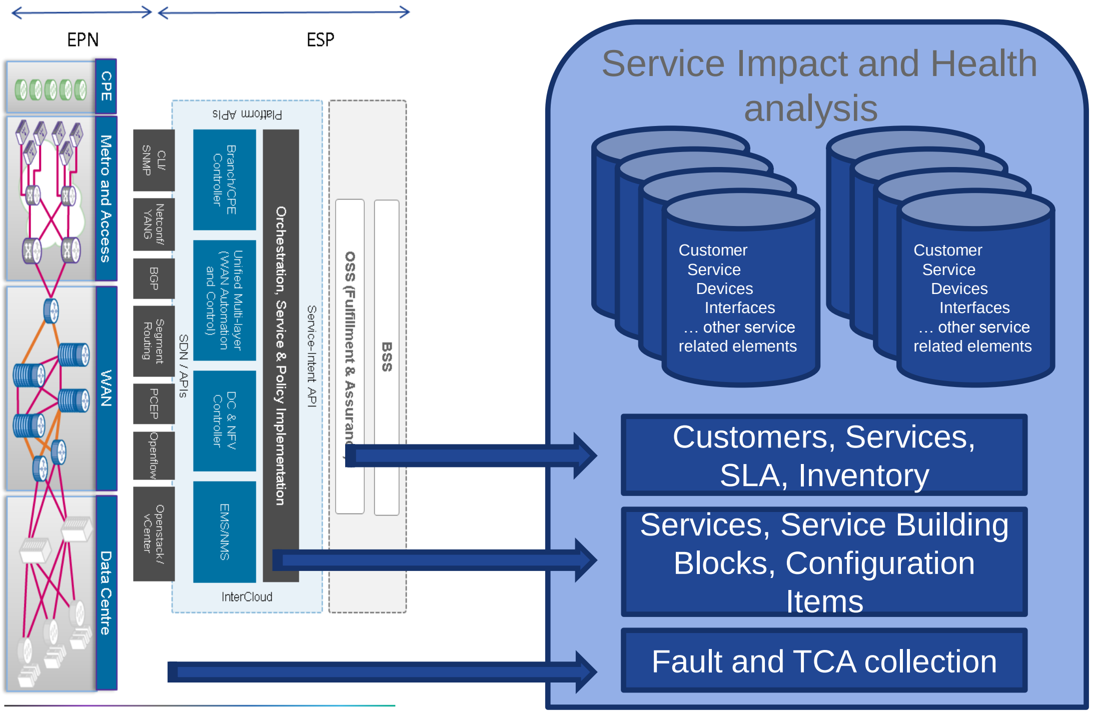


Proposed solution – Cross-Domain Orchestrator



Place cross domain cross functional Orchestration Engine that will have End-to-End visibility of all Domain Managers and devices on the southbound and business logic service representation on the north bound. this will provide centralize repository of all services, service building blocks and configuration items.

Proposed solution – Service Impact and Health



Service Impact and Health analysis

Customer
Service
Devices
Interfaces
… other service
related elements

Customer
Service
Devices
Interfaces
… other service
related elements

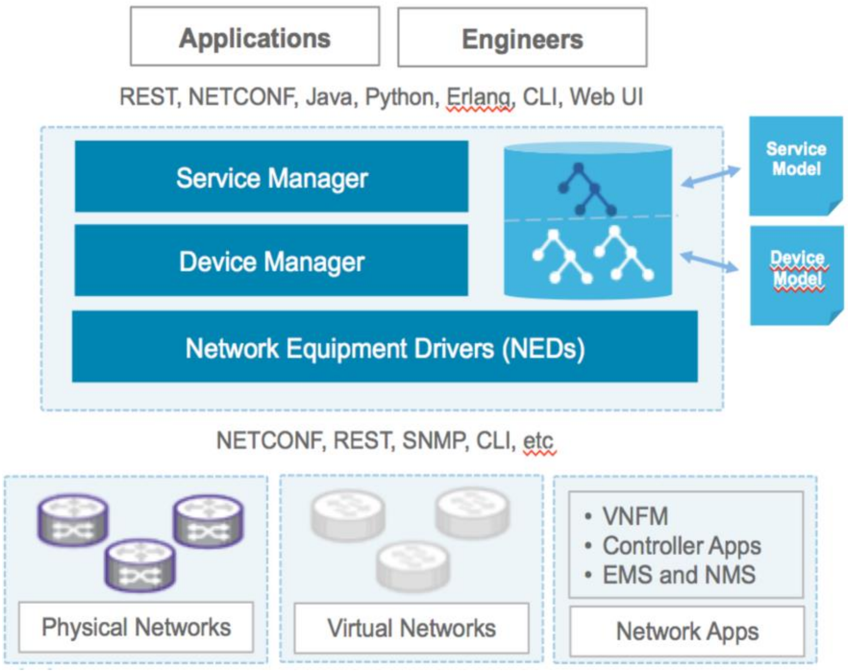
Customers, Services, SLA, Inventory

Services, Service Building Blocks, Configuration Items

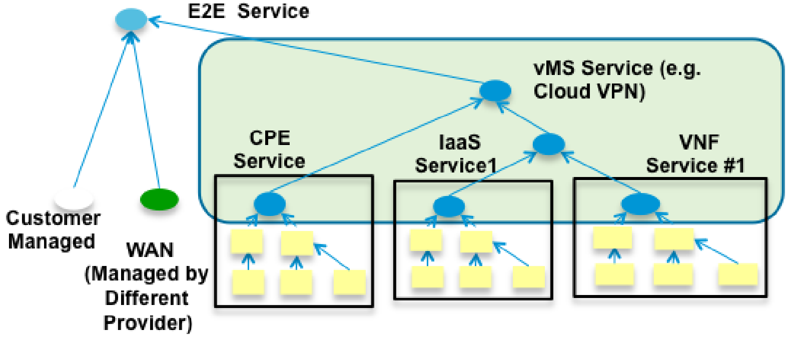
Fault and TCA collection

Service Monitoring/Assurance system will leverage the NSO repository creating impact containers. Once fault or performance metric arrive it will be associated to the relevant container for the impact and health analysis.

The bridge

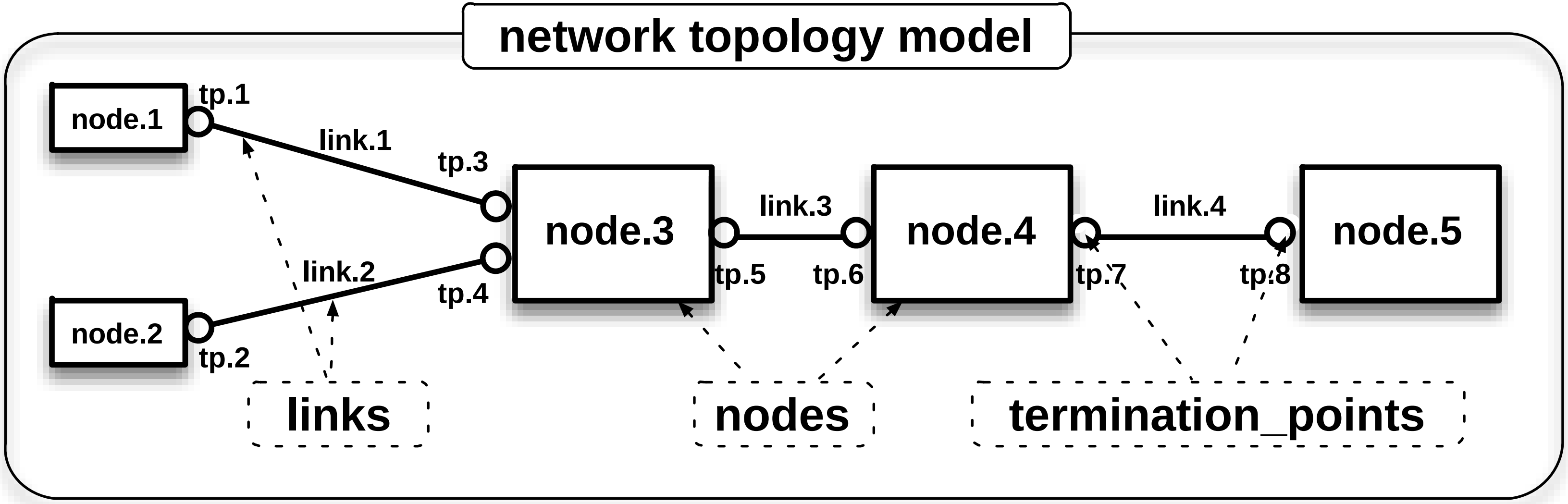


- Cisco's NSO and multi-domain architecture brings service agility and differentiation for multi domain applications. A common architecture and declarative service definitions across domains simplifies the end-to-end service lifecycle. Domain specific capabilities are abstracted with domain specific controllers tied together with NSO to bring service coherency and agility.



Example: Network Topology Fundamental Constructs

Nodes, Links, Termination Points



- Based on the draft: draft-clemm-i2rs-yang-network-topo-04.
- Topology Comprises a set of Nodes and Links.
- Model is on-boarded to the Physical and Virtual Infrastructure.

YANG Structure

```
module: network
   +--rw network* [network-id]
      +--rw network-id           network-id
      +--ro server-provided?     boolean
      +--rw network-types
      +--rw supporting-network* [network-ref]
      |  +--rw network-ref    leafref

      +--rw node* [node-id]
      |  +--rw node-id                 node-id
      |  +--rw supporting-node* [network-ref node-ref]
      |  |  +--rw network-ref    leafref
      |  |  +--rw node-ref       leafref
      |  +--rw lnk:termination-point* [tp-id]
      |     +--rw lnk:tp-id                          tp-id
      |     +--rw lnk:supporting-termination-point*
                        [network-ref node-ref tp-ref]
      |        +--rw lnk:network-ref    leafref
      |        +--rw lnk:node-ref       leafref
      |        +--rw lnk:tp-ref         leafref
```

```
+--rw lnk:link* [link-id]
      +--rw lnk:link-id           link-id
      +--rw lnk:source
      |  +--rw lnk:source-node    leafref
      |  +--rw lnk:source-tp?     leafref
      +--rw lnk:destination
      |  +--rw lnk:dest-node    leafref
      |  +--rw lnk:dest-tp?     leafref
      +--rw lnk:supporting-link* [network-ref link-ref]
         +--rw lnk:network-ref    leafref
         +--rw lnk:link-ref       leafref
```

Conclusion

- Cross Domain Orchestration is a key for bridging the gap of the multiple management domains, it acts as the source of true for service data and its construction across the network
- The legacy approach of service monitoring and assurance is typically bottom-up approach where the domain managers need a detailed knowledge on the domain components and its status, using the central orchestration and central service repository enable a top-to-bottom approach where only service related items are monitored for impact and health. this drastically decrease the complexity of understanding the relations between components and either maintain accurate “topology” or complex correlation rules
- This approach is built upon BigData analytics approach where accuracy of the data is driven from its scale, so as many sources/data inputs we have our analysis become more accurate, with this approach we can place big data log aggregation (like Splunk, LogStash) to collect the multiple sources and sore them on analytics engine (Splunk, ElasticSearch) so Service Impact application can retrieve and analyze the data and its association to the impact model built by the representation of Cisco NSO Service models.

CISCO