Digital Map
IETF Hackathon

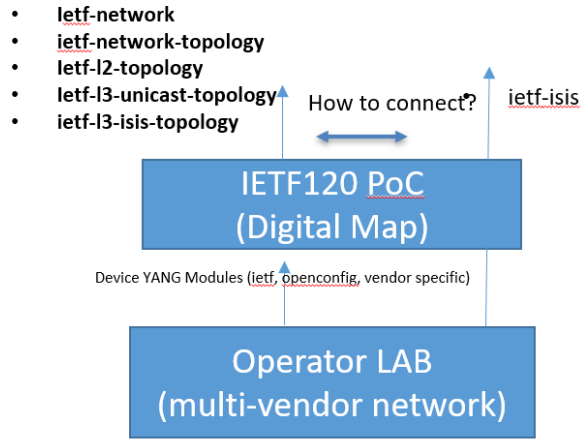
IETF 121

2–3 November 2024

Dublin, Ireland

Project Info

- The goal is to demonstrate how operators can use the IETF Topology Yang models to represent a real carrier IP/MPLS network.
- We start with one particular problem space: How to use IETF topology model to represent a real carrier network based on IS-IS and OSPF domains for planning/simulation purposes.
- We want to demonstrate if RFC8345 is the suitable standard for representing the multi-layered topology for Digital Map and show the models comparison with and without the identified gaps.
- What drafts/RFC's were involved (initial set)
  - https://www.rfc-editor.org/rfc/rfc8345 (ietf-network, ietf-network-topology)
  - https://www.rfc-editor.org/rfc/rfc8944 (ietf-l2-topology)
  - https://www.rfc-editor.org/rfc/rfc8346 (ietf-l3-unicast-topology)
  - https://datatracker.ietf.org/doc/draft-ogondio-nmop-isis-topology (ietf-l3-isis-topology)
  - https://datatracker.ietf.org/doc/rfc9130 (ietf-isis)
  - https://datatracker.ietf.org/doc/html/draft-havel-nmop-digital-map-concept
  - https://datatracker.ietf.org/doc/html/draft-havel-nmop-digital-map
  - https://datatracker.ietf.org/doc/draft-davis-opsawg-some-refinements-to-rfc8345



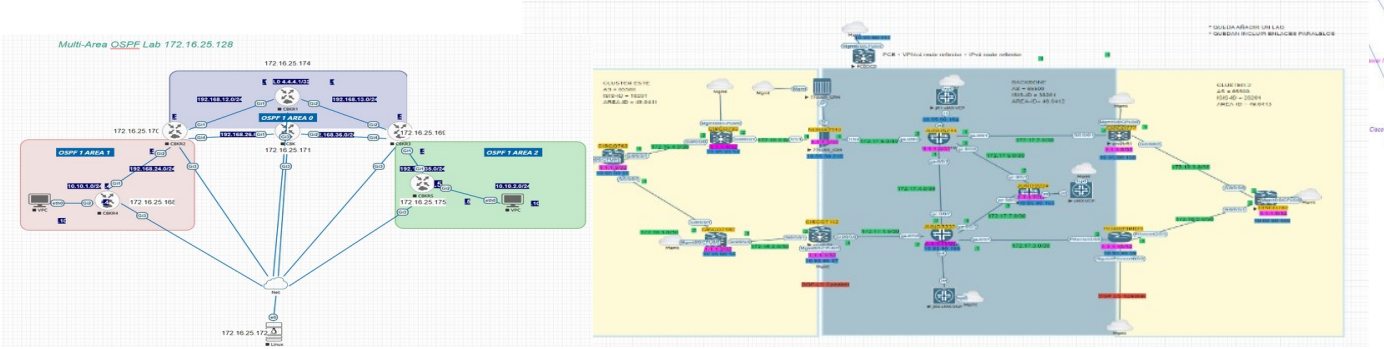
Hackathon Plan

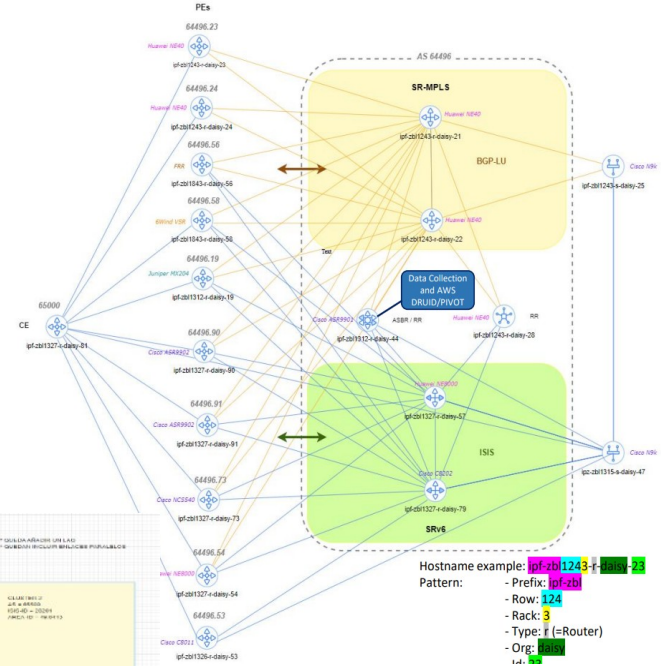
- The project has started at IETF120 Hackathon, where we focused on generic topology queries and addressed subset of gaps we identified for RFC8345 using IS-IS scenario in the operator LAB

- The objective for this hackathon is to improve the IETF120 Hackathon prototype, including:
  - How to retrieve performance metrics or configuration attributes (defined in RFC9030 or RFC9129 and retrieved via device API) northbound from the Controller via RFC8345 API and its IS-IS and OSPF Augmentation.
  - Start addressing simulation/emulation scenario.
  - Run Digital Map discovery on labs from Swisscom and Telefonica

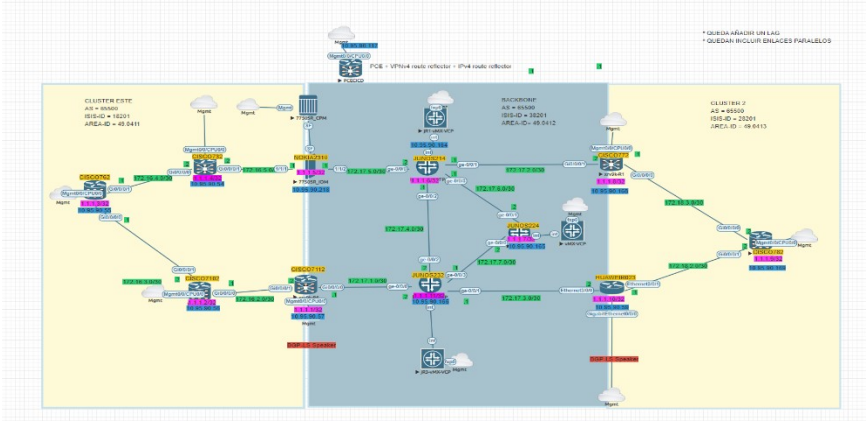
Labs used

- Collaborated with Swisscom and Telefonica to connect to their labs and map different technologies to topology using RFC8345
- Created in-house virtual labs for mapping OSPFv3 and ISIS.

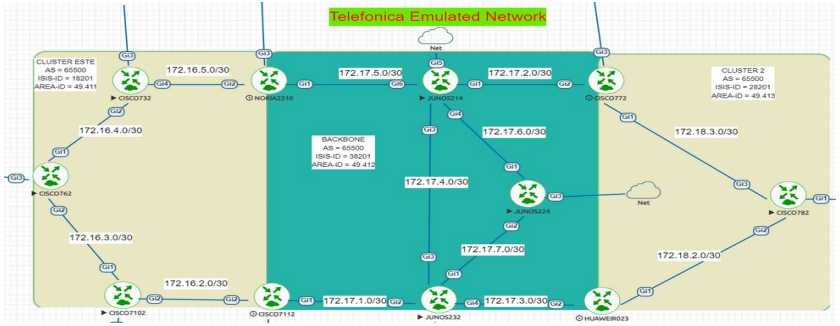




Hackathon LAB



Real Net



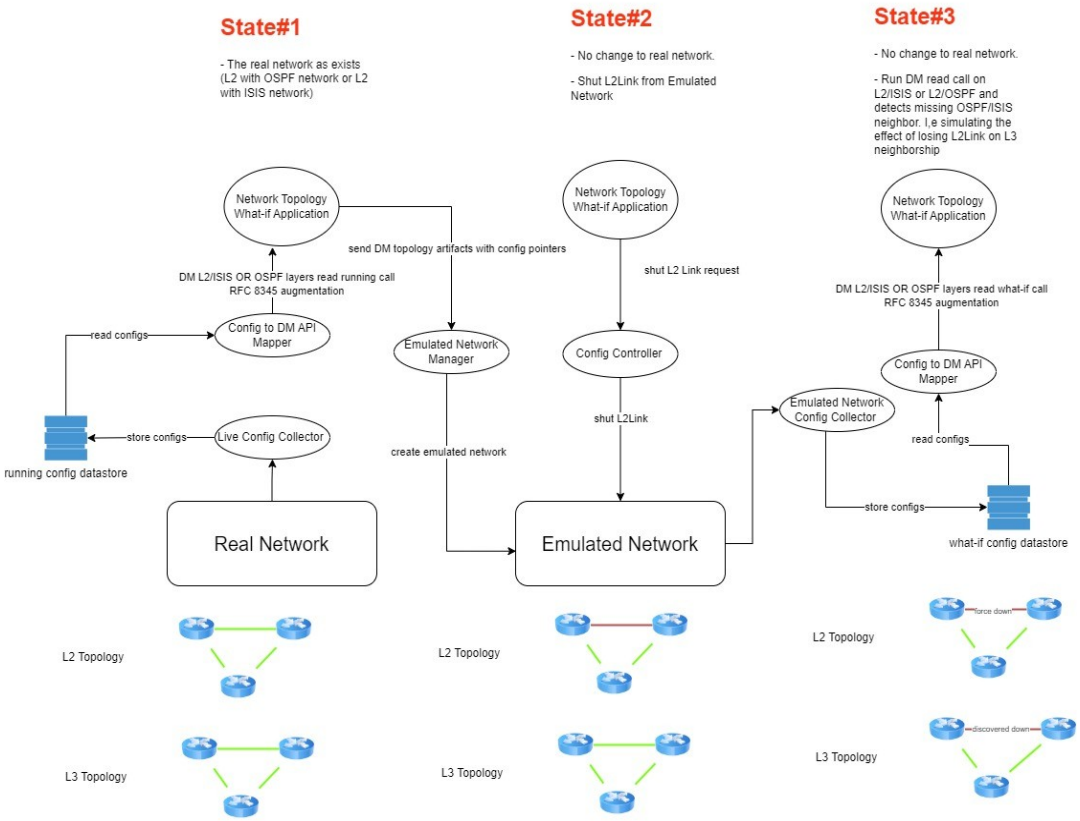
emulated

We used this multi-vendor ISIS ***Telefonica*** Operator LAB for real-time discovery

Real Topology & configs were used to build the emulated network (all discovered before the Hackathon and simulated for this Hackathon)

Emulated Network is used in the context to run what-if scenario and demonstrate

Hackathon what-if Scenario

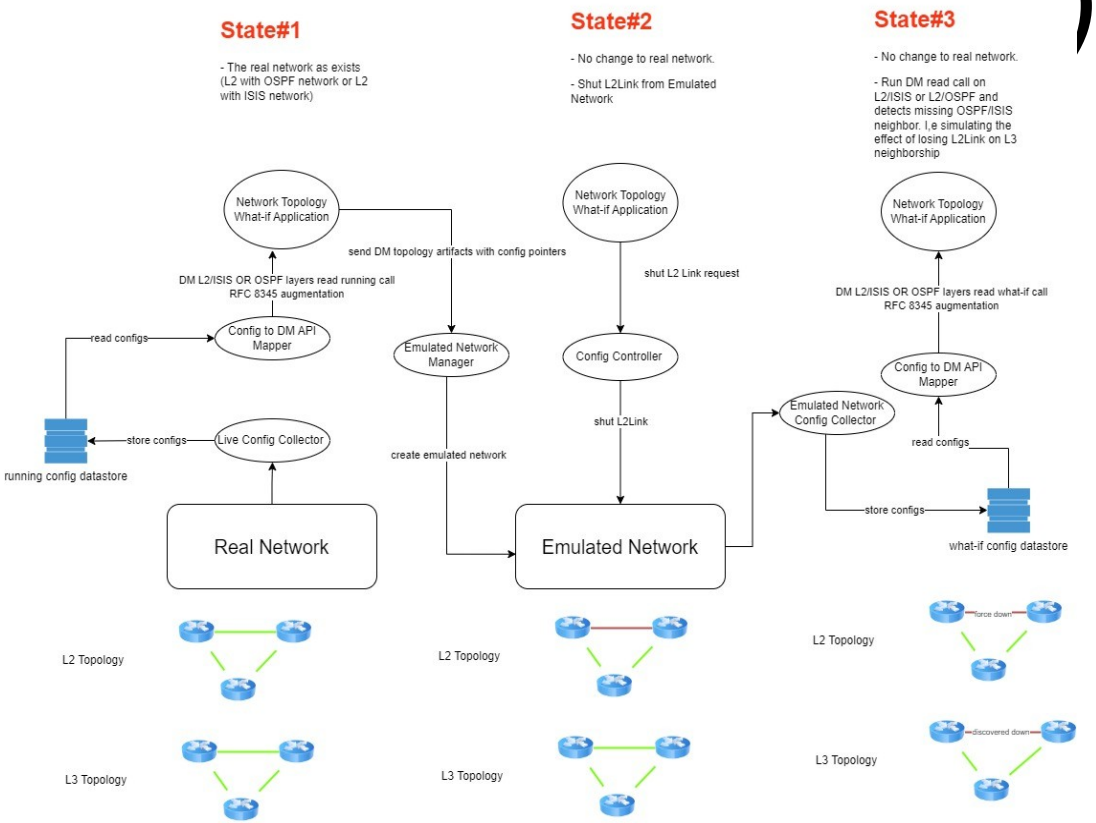


Scenario: Find impact on topology upon changing interface state

Data Collection: using the Digital Map, we extract comprehensive data from a real network, including details of nodes, links, networks, and interfaces. Each element would be associated with its configuration metadata (e.g., XPath, categories, and other properties).

Network Emulation: construct a virtualized, emulated version of the real network using the collected topology and configuration

Hackathon what-if Scenario (Cont.)



Configuration Management: The network application will have the capability to send write requests, such as shutting a specific L2 link, which would automatically trigger corresponding configuration changes on the emulated network device.

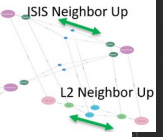
Result Validation: After making changes to the emulated network, re-read the network state using the Digital Map API, validating that higher-layer elements (like an OSPFlink/ISISLink) are

Hackathon what-if Scenario (before change)

Digital Map API [draft-ogondio-nmop-isis-topology]

c[illegible]o get isis links under network “isis:49.0413”

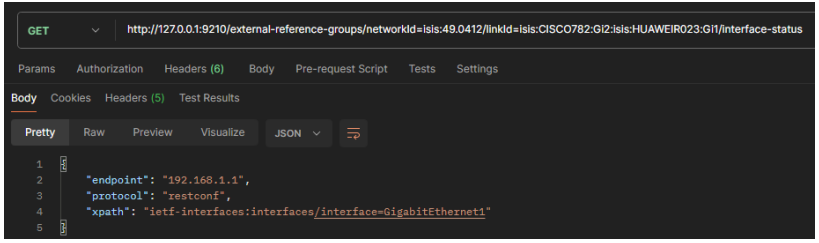
1




```
[
  {
    "link-id": "isis:CISCO782:Gi2:isis:HUAWEIR023:Gi1"
  },
  {
    "link-id": "isis:CISCO782:Gi3:isis:CISCO772:Gi1"
  }
]
```

2

Get the refs to retrieve link status



se the refs from (2) to build REST request to get interface status

3

```
### sample CONFIG API call to get interface GigabitEthernet1 status for 192.168.1.1
POST http://localhost:9220/configmanager/device/mock-operations/run
Accept: application/json
Content-Type: application/json

{
    "operation_type": "get_interface",
    "xpath": "ietf-interfaces:interfaces/interface=GigabitEthernet1",
    "endpoint": "192.168.1.1"
}
```

4

Interface u
response

```
{
  "ietf-interfaces:interface": [
    {
      "enabled": true,
      "ietf-ip:ipv4": {
        "address": [
          {
            "ip": "172.17.7.1",
            "netmask": "255.255.255.252"
          }
        ]
      },
      "ietf-ip:ipv6": {},
      "name": "GigabitEthernet1",
      "type": "iana-if-type:ethernetCsmacd"
    }
  ]
}
```

Hackathon what-if Scenario (after change)

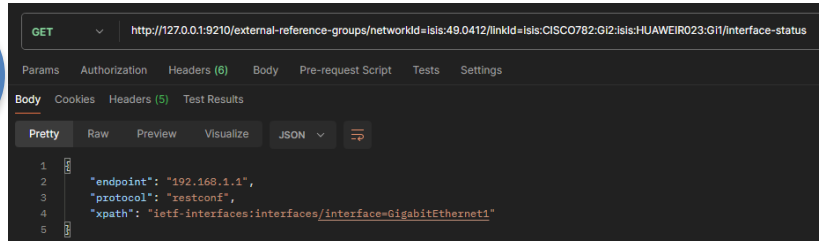
Digital Map API draft-ogondio-nmop-isis-topology
call to get isis links under network “isis:49.0413

1

```
[
  {
    "link-id": "isis:CISCO782:Gi2:isis:HUAWEIR023:Gi1"
  }
```

Get the refs to retrieve link status

2



e the refs from (2) to build REST request to get interface status

3

```
### sample CONFIG API call to get interface GigabitEthernet1 status for 192.168.1.1
POST http://localhost:9220/configmanager/device/mock-operations/run
Accept: application/json
Content-Type: application/json

{
    "operation_type": "get_interface",
    "xpath": "ietf-interfaces:interfaces/interface=GigabitEthernet1",
    "endpoint": "192.168.1.1"
    }
```

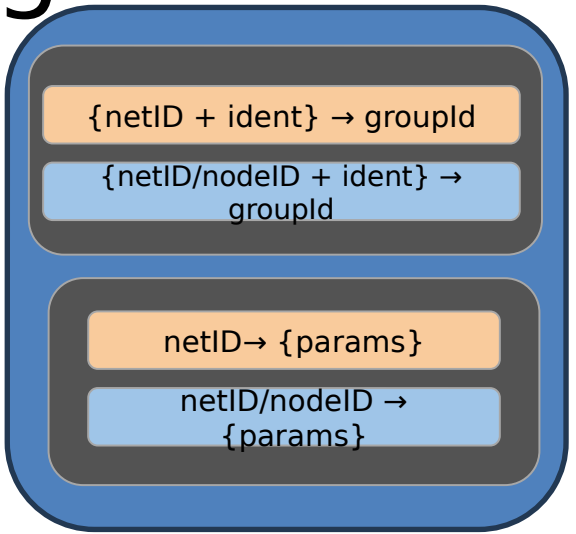
4

Interface down respo

```
{
  "ietf-interfaces:interface": [
    {
      "enabled": false,
      "ietf-ip:ipv4": {
        "address": [
          {
            "ip": "172.17.7.1",
            "netmask": "255.255.255.252"
          }
        ]
      },
      "ietf-ip:ipv6": {},
      "name": "GigabitEthernet1",
      "type": "iana-if-type:ethernetCsmacd"
    }
  ]
}
```

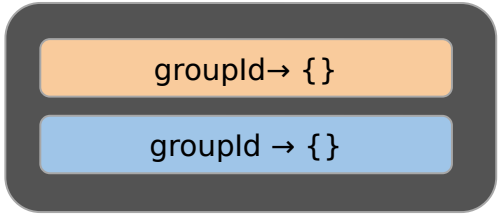
Linking Topology to Configuration

Retrieve config using RFC8345



App

Digital Map



What was achieved

- Discovered L2 and ISIS topology for multi-vendor network and built relationship between different layers
  - ISIS Areas modelled as ietf-networks (not currently supported in RFC8345 as it does not allow for links between network)
- Built an emulated lab and did a what-if scenario showing impact of config change on topology.
- Explored candidate options to link topology to other domains
  - In this hackathon we used “configuration” domain.
- Mapped different device models to the network wide topology models and retrieved them via IETF Topology API
- digital-map-exp/digital-map-public (github.com)

What next (IETF 122)

- Add more layers:
  - BGP, SRv6
  - Explore other candidate options to other domains (config, inventory, etc)
- Add more operator LABs (already started collaboration with Bell Canada)

Team members

- Sherif Mostafa (sherif.mostafa@huawei.com)
- Olga Havel (olga.havel@huawei.com)
- Vivekananda Boudia (vivekananda.boudia@insa-lyon.fr)
- Oscar Gonzalez De Dios (oscar.gonzalezdedios@telefonica.com)
- Yannick Buchs (yannick.buchs@ swisscom.com)
- Daniel Voyer (daniel.voyer@bell.ca)
- Benoit Claise (benoit.claise@huawei.com)
- Pierre Francois (pierre.francois@insa-lyon.fr)