WORKSHOP GARR 2024

NET MAKERS

GÉANT AUTOMATION PLATFORM (GAP)

Simone Spinelli

Géant

Come interagire da remoto

About me

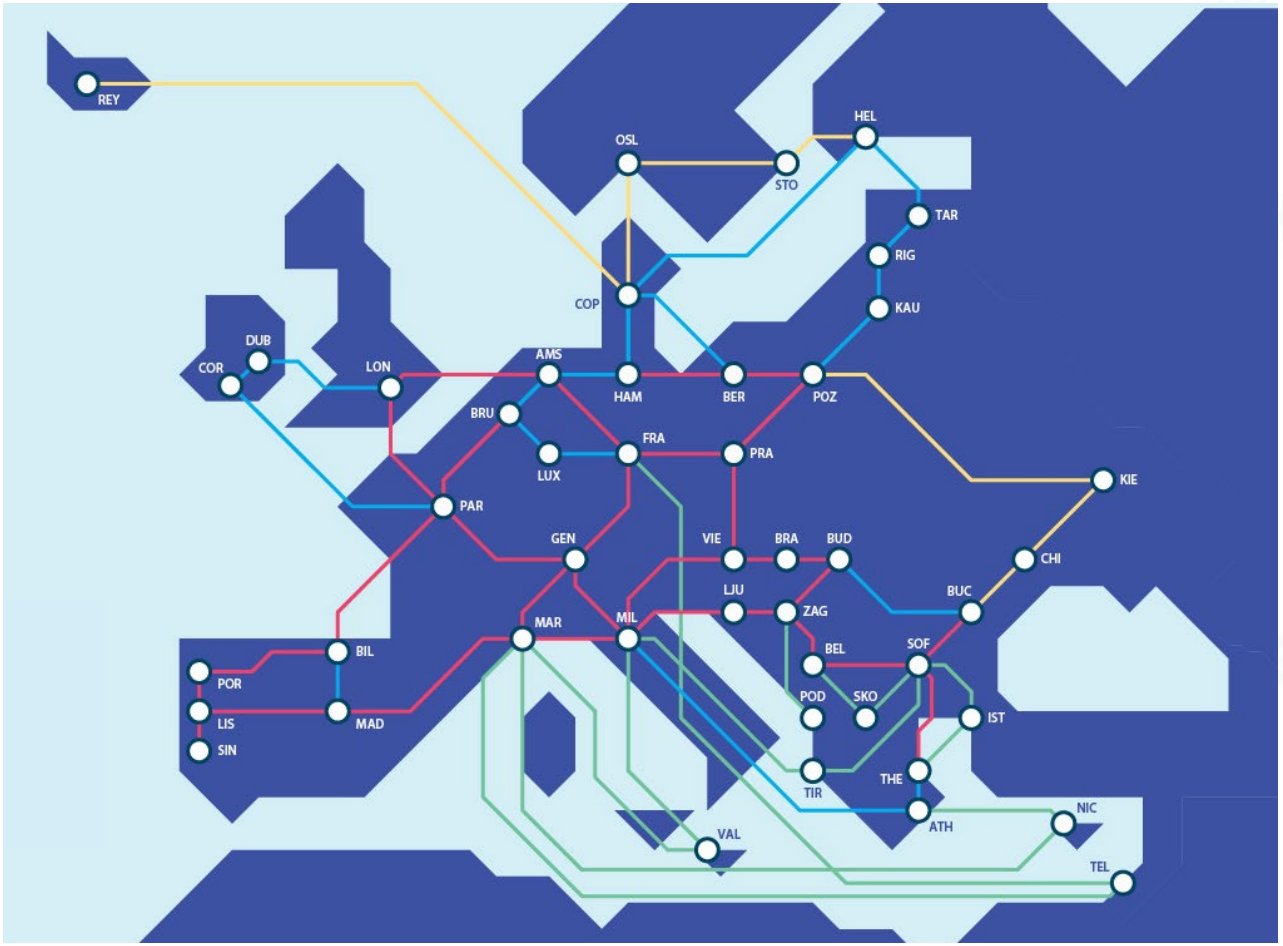
- Padre di due gemelli di 4 anni (Liam & Nora)
- ± 15 anni @Università di Pisa
- Nei Paesi Bassi dalla fine del 2016
- @Geant dal 2019, focus Network Automation

simone.spinelli@geant.org

AVVERTENZA: Ho riutilizzato slides che avevo giá, quindi molte saranno in inglese.

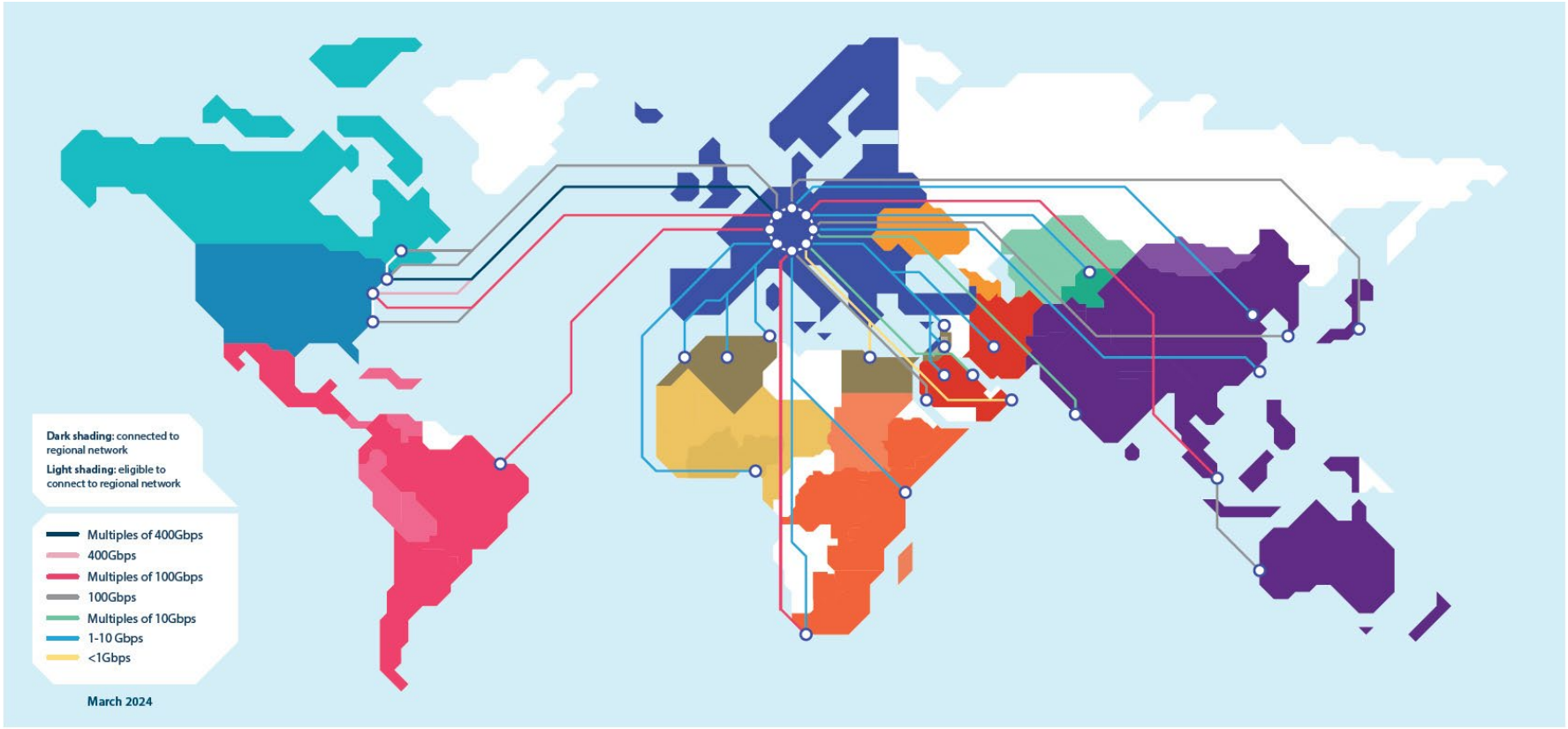
About Géant

- Runs a membership association for Europe's National Research & Education Networks (NRENs)
- Coordinates and participates in EC-funded projects
- Operates a pan-European e-infrastructure
- Manages a portfolio of services for research & education



In Europe: 38 NRENs + NORDUnet, supporting 10,000 institutions and 50 million academic users

About Géant



Canada & USA | Latin America | Europe | North Africa & Eastern Mediterranean | West & Central Africa | Eastern & Southern Africa | Central Asia | Asia-Pacific | Other R&E Networks

GÉANT Networks · Services · People

Co-funded by the European Union

geant.org

Network Automation @GÉANT

- Started in 2019 as a “nice to have”
- First Saltstack, then Ansible, then Ansible + Jenkins
- Now stable with:
  - Workflow Orchestrator
  - Ansible
  - LSO - Lightweight Service Orchestrator: API around ansible, “does nothing”.

Necessità fa virtù

- Current platform: Juniper MX (960/480/204)
  - 10+ years of experience
  - Very good integration with Ansible
- New platform is NOKIA 7750SR-S – SROS [not SR Linux]:
- Migration will be in 2 phases:
  - PHASE1: Nokia nodes deployed as P/LSR (starts Q1 2024)
  - PHASE2: Nokia nodes promoted to PE (starts Q3 2024)
- Totally automated:
  - Operators run workflows
  - No CLI needed in sunny days

NOKIA

7750 SR-2se

7750 SR-7s

Orchestrazione & Automazione

Processes:

- What is the service and how do you deliver it?
- Who decides? And how?
- What is the authoritative system for a specific data?
- Anything else that must happen because of your action?

Artifacts:

- Is it config?
- What is static/design?
- What depends from the single instance?
- Where is the data coming from?
- What are the possible variants?

Orchestrazione & Automazione

Processes:

- What is the service and how do you deliver it?
- Who decides? And how?
- What is the authoritative system for a specific data?
- Anything else that must happen because of your action?

Artifacts:

- Is it config?
- What is static/design?
- What depends from the single instance?
- Where is the data coming from?
- What are the possible variants?

Automation

- Executes atomic actions:
  - Push some config
  - Gather data
  - Execute something
- Highly specialized, dependent from the context (Cisco/Juniper/Nokia/Linux/*)
- The focus is the artifact itself
- Typically, **where we all start**

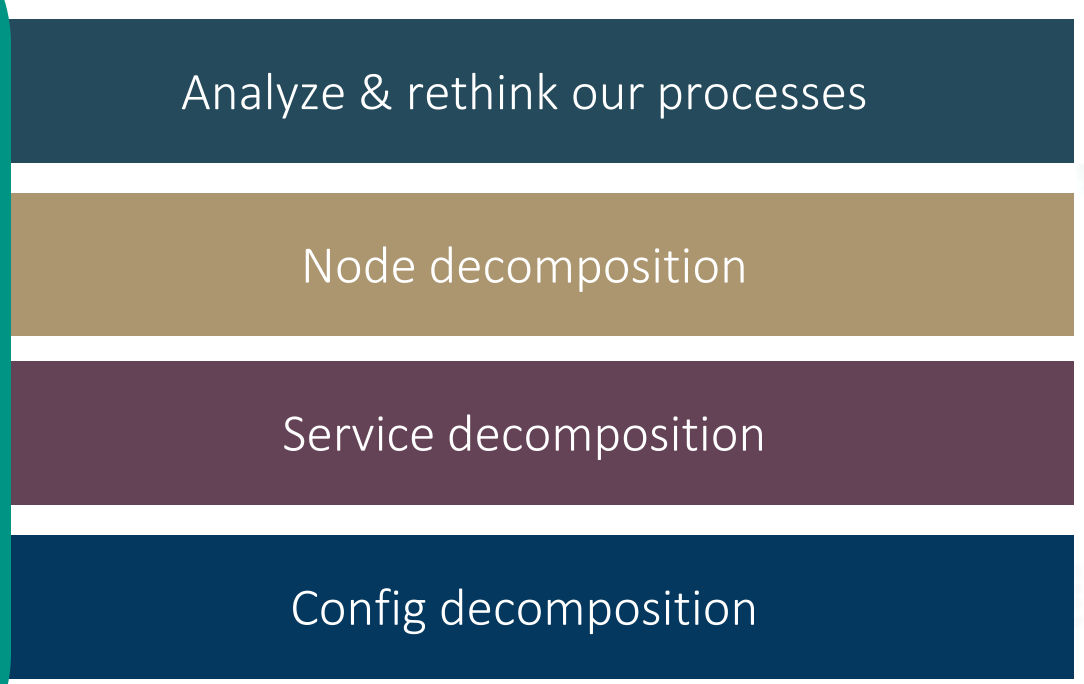
Orchestration

- Represent the business logic
- Interacts with multiple systems
- Agnostic to the context
- Generally, end-to-end
- Typically, **where we want to be**

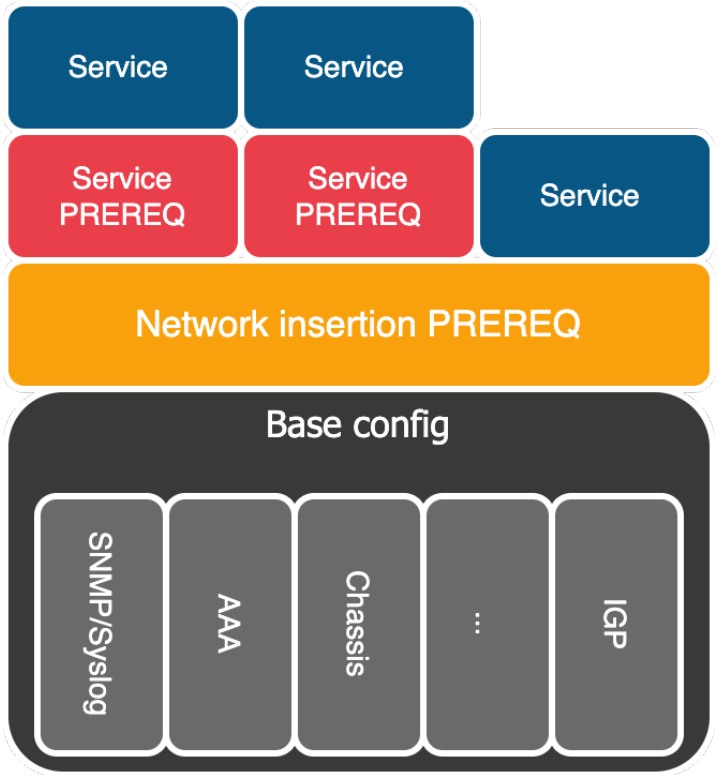
Filosofia

Approaching top to bottom (Orchestration) has been a winning choice for us.

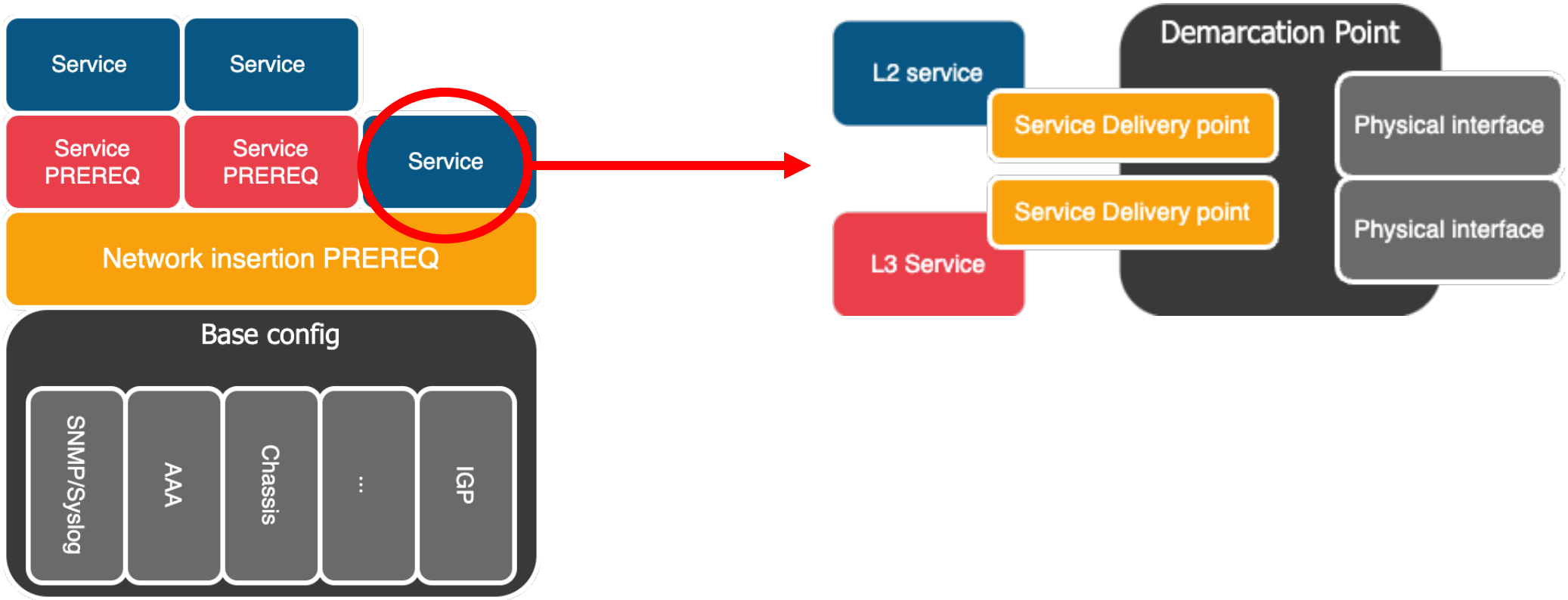
“Shift our thinking from lines of config to abstract models”



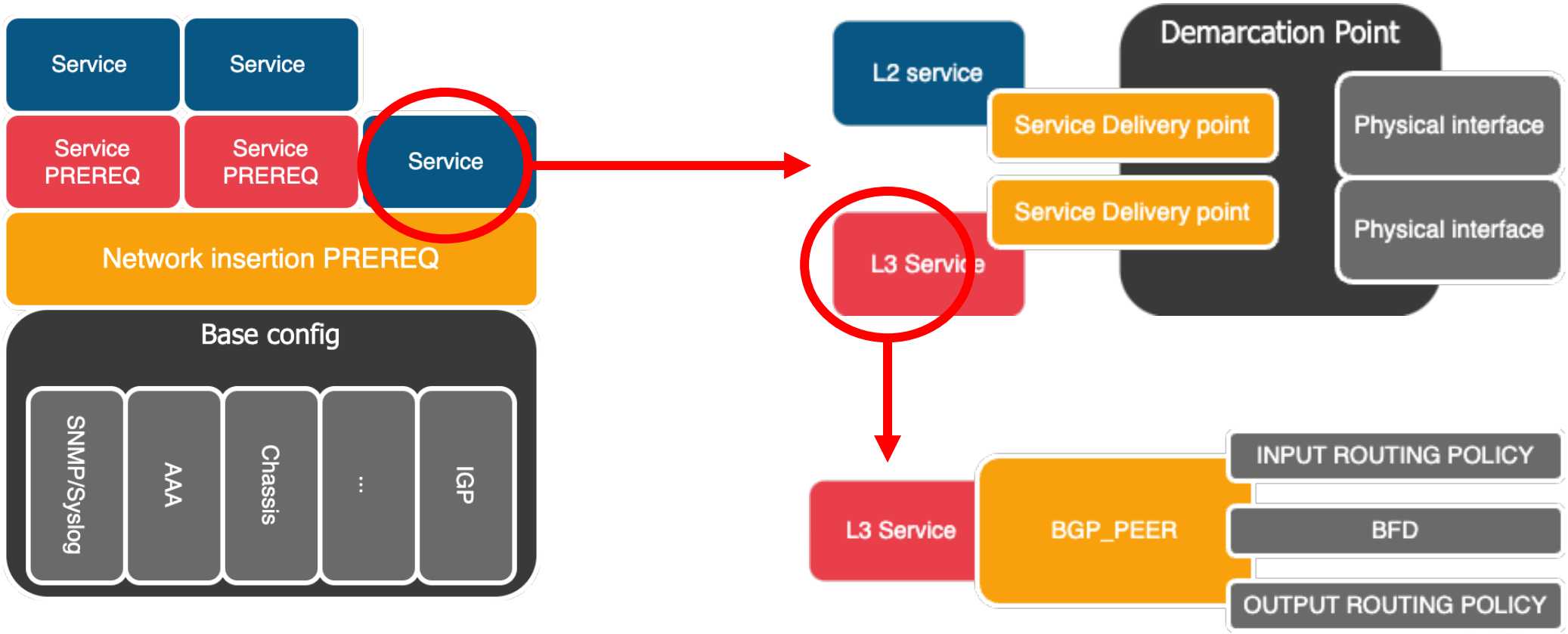
Scomposizione



E scomposizione



E ancora scomposizione



Che porta questo…

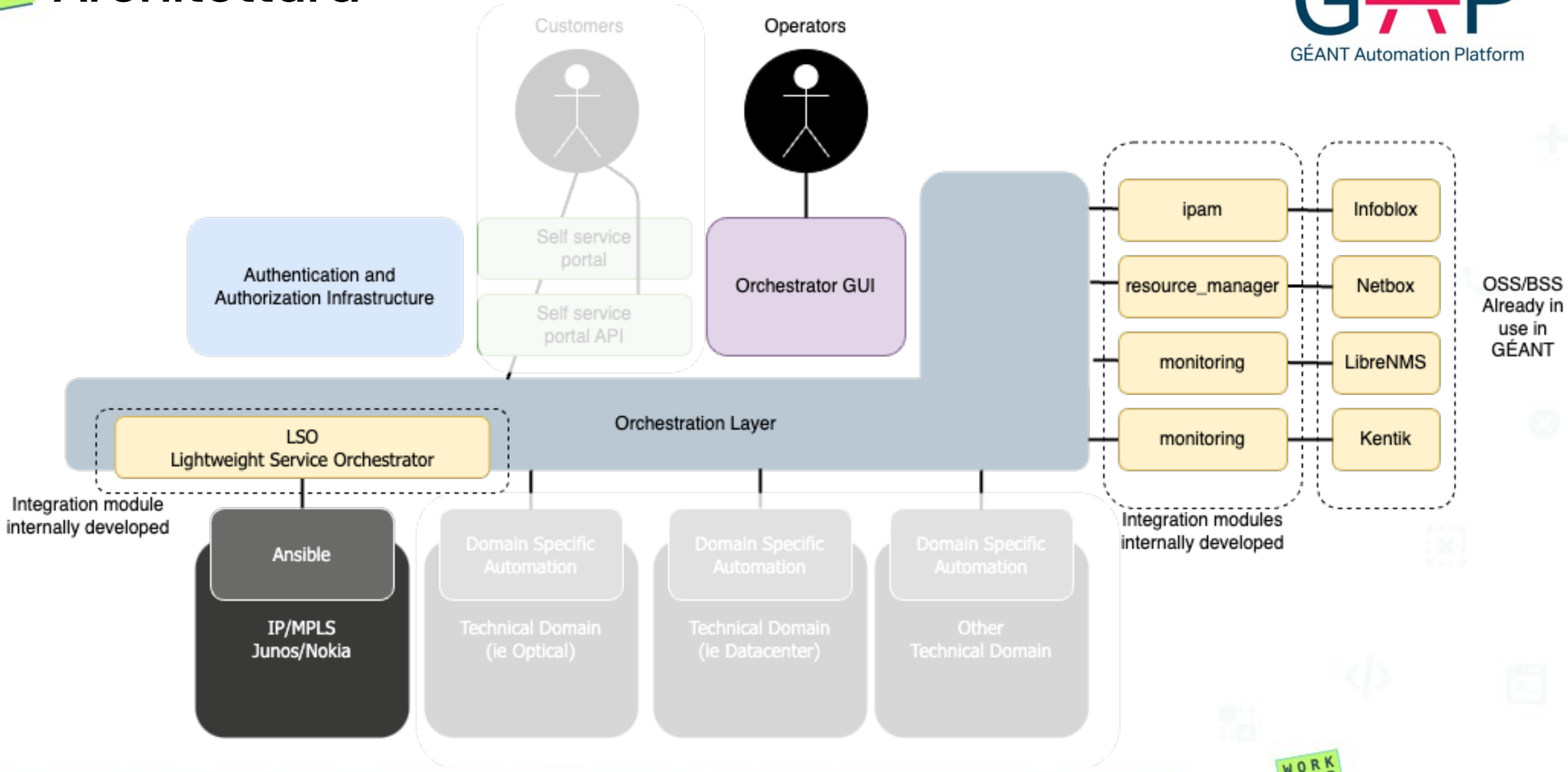
```
neighbor 1.2.3.4 {
    description "-- Peering with SURF  --";
    accept-remote-nexthop;
    out-delay 10;
    import [ ps-BOGONS ps-RPKI-RE-PEER ps-from-SURF1-nren ];
    authentication-key "$@$%DGKND#$%^#^%$"; ## SECRET-DATA
    export [ ps-BOGONS ps-to-SURF1-nren ];
    peer-as 1103;
    bfd-liveness-detection {
        minimum-interval 3000;
        multiplier 3;
    }
}
```

A diventare questo:

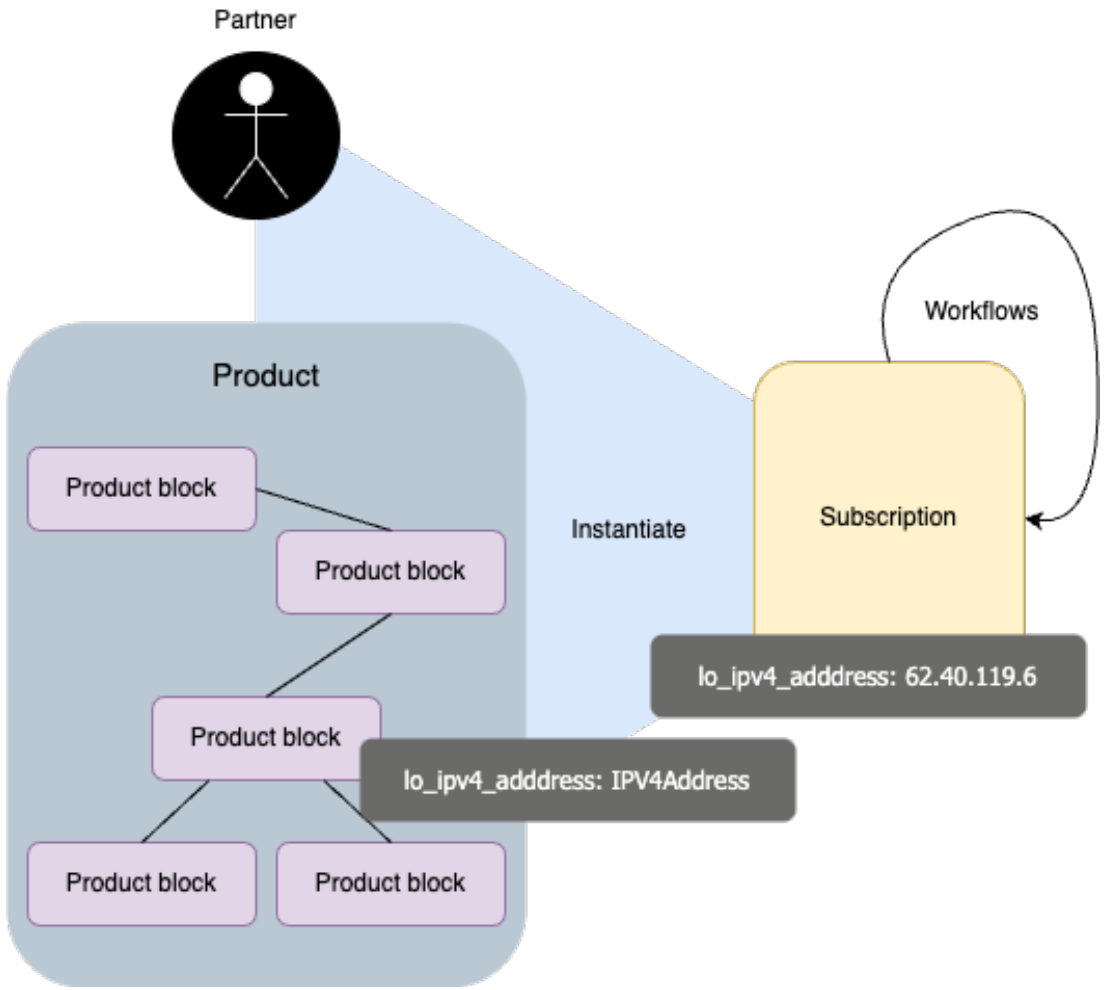
```
neighbor {{ neighbor.ipv4_address }} {
    description "-- Peering with {{org.name}}  --";
    accept-remote-nexthop;
    out-delay 10;
    import [ ps-BOGONS ps-RPKI-RE-PEER {{ org.import_policy }} ];
    authentication-key ”{{ neighbor.auth_key }}"; ## SECRET-DATA
    export [ ps-BOGONS {{ org.export_policy} } ];
    peer-as {{ org.as_number }};
{% if neighbor.features.bfd_enable == True %}
    bfd-liveness-detection {
        minimum-interval {{ bfd.minimum_interval }};
        multiplier {{ bfd.multiplier }};
    }
{% endif %}
}
```

Architettura

GÉANT Automation Platform



WorkflowOrchestrator



In WorkflowOrchestrator works the same:

- We think in terms of products: a composition of product blocks
- Product blocks are abstract objects that have attributes
- An instance of a product, instantiated for someone is a subscription.
- Workflows manipulate the subscription modifying the lifecycle state

Workflow Orchestrator Programme

- All code is licensed under Apache 2.0
- Setup under the Commons Conservancy
- All Intellectual Property remains at each member company
- Membership levels:
  - Partner
  - Graduate
  - Sandbox
- Mainly NREN's and networking use case but other use-cases as well

https://workfloworchestrator.org/

LSO & Ansible

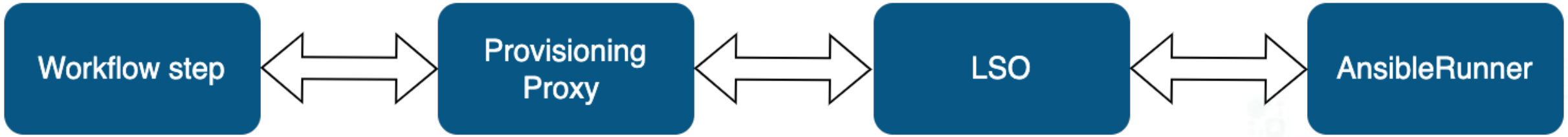
LSO

- Lots of internal experience with Ansible/Jinja
- No wish to move to AWX/Tower
- Keep it simple -> Do it yourself

Ansible

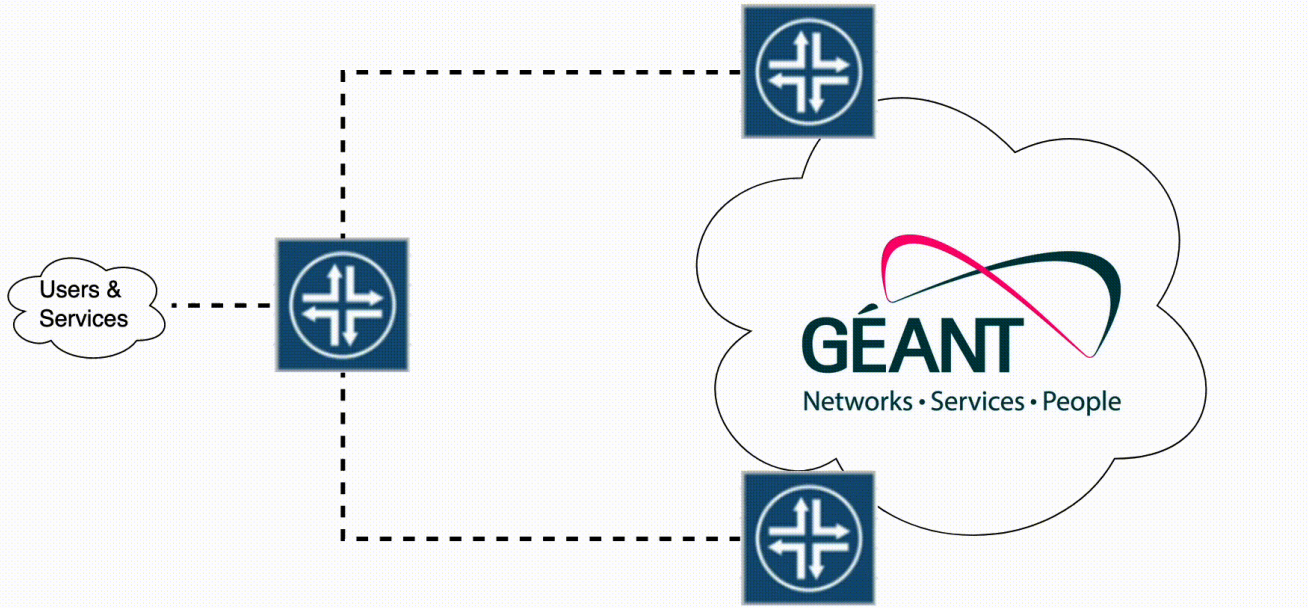
- One product block <-> One role
- Templates shared when sensible
- No canonical inventory

Lightweight Service Orchestrator



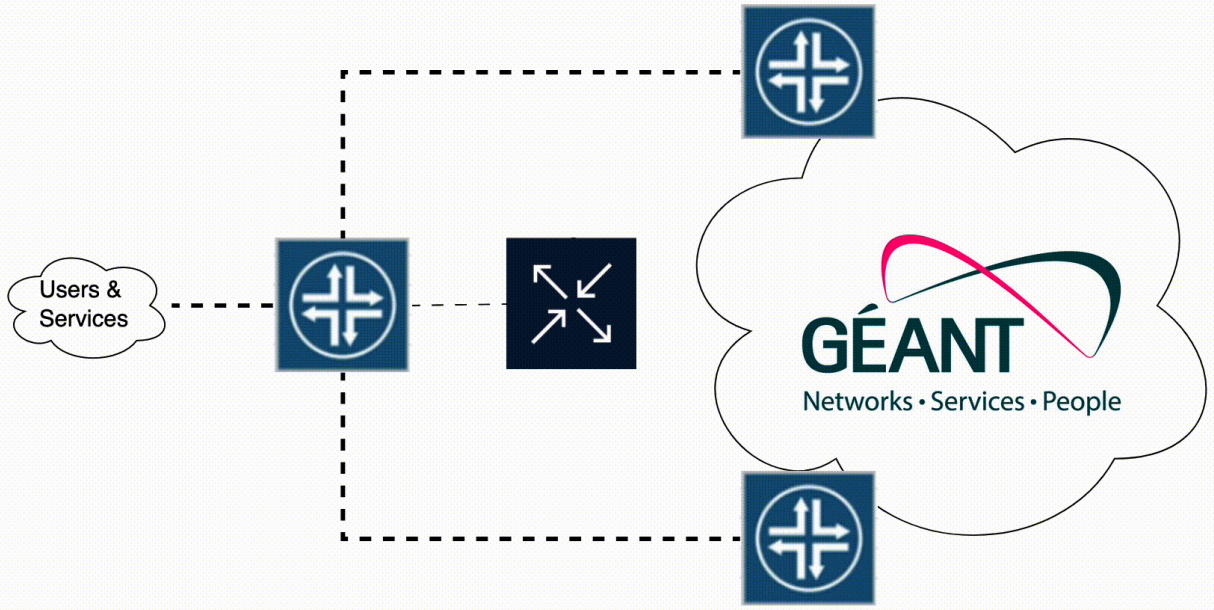
…al momento:

- Deployment/removal of a Juniper or Nokia router in P or PE mode:
  - Base config
  - iBGP mesh update
  - OSS/BSS
- Core link Migration:
  - Including functional checks
  - Old config cleanup
  - Partial OSS/BSS alignment
  - Takes now 30 min instead of ½ day
- Promotion from P to PE
  - More meshes
  - Other OSS/BSS
- PHASE1 totally covered.



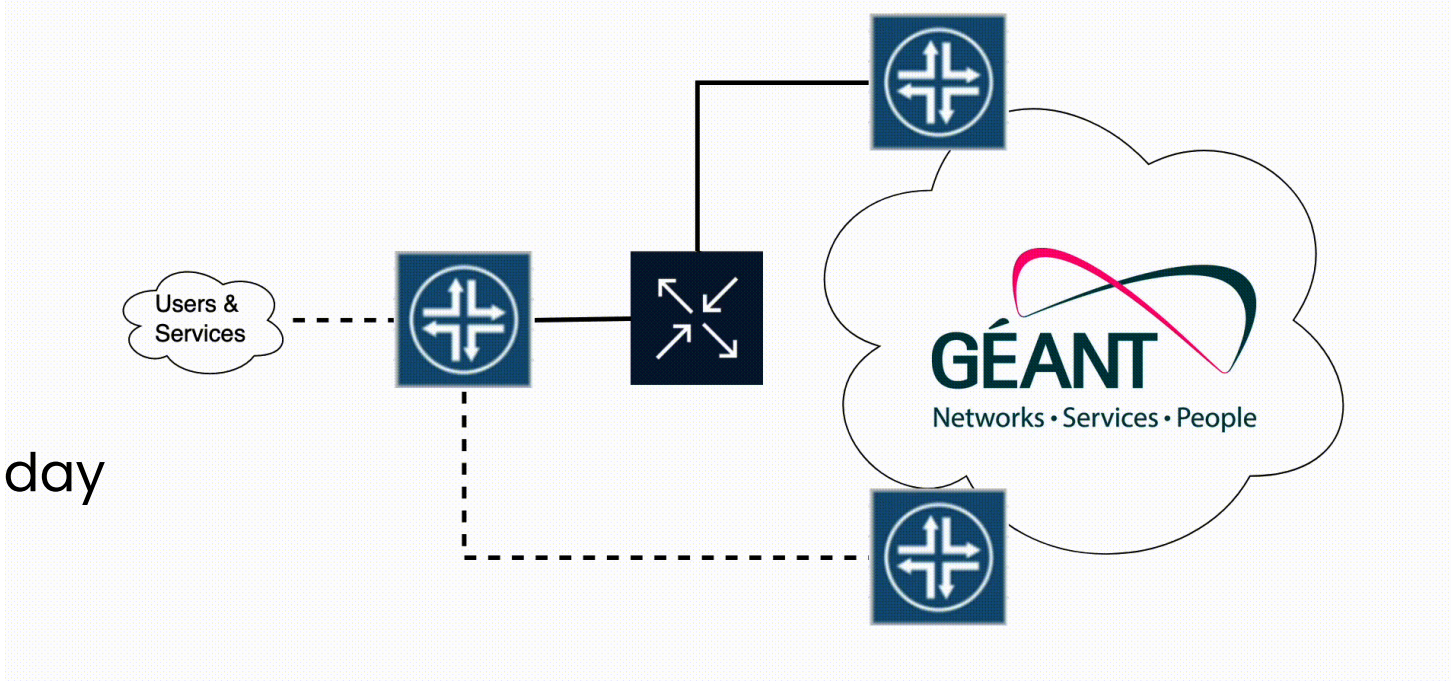
…al momento:

- Deployment/removal of a Juniper or Nokia router in P or PE mode:
  - Base config
  - iBGP mesh update
  - OSS/BSS
  - First core link
- Core link Migration:
  - Including functional checks
  - Old config cleanup
  - Partial OSS/BSS alignment
  - Takes now 30 min instead of ½ day
- Promotion from P to PE
  - More meshes
  - Other OSS/BSS
- PHASE1 totally covered.



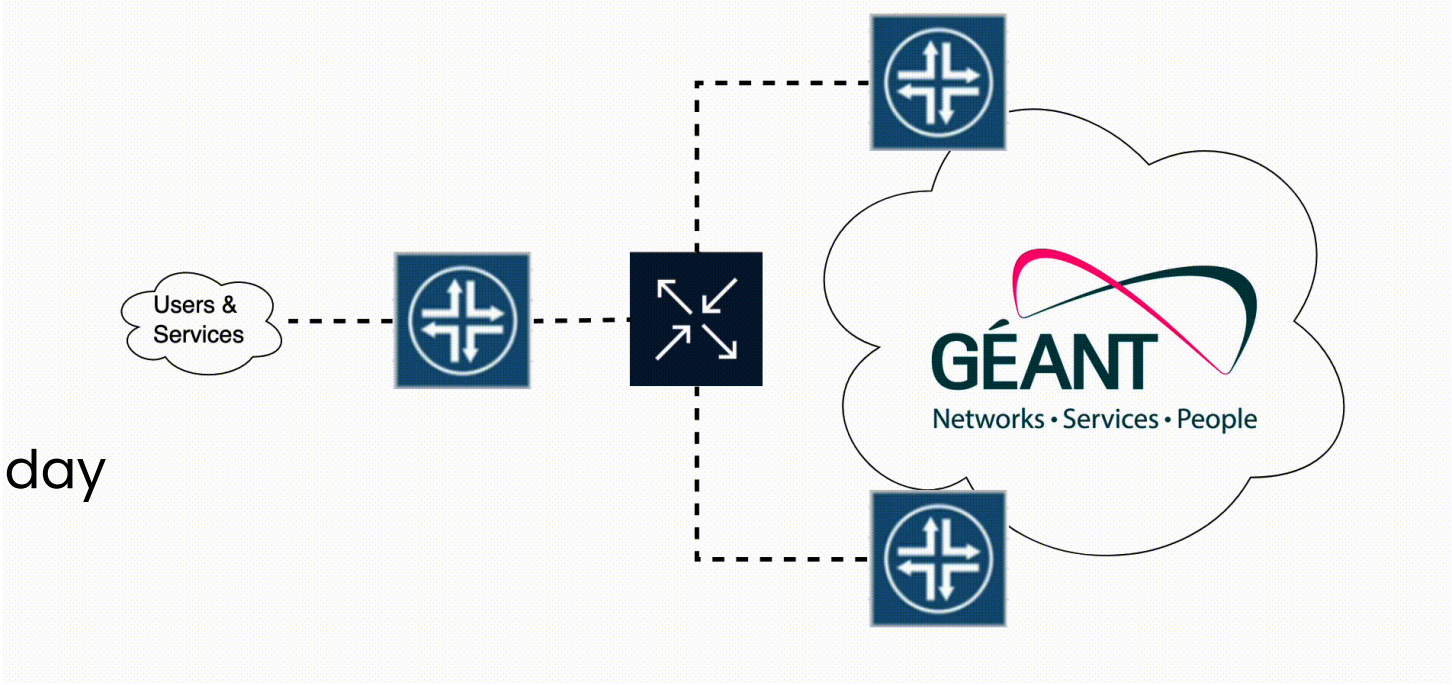
…al momento:

- Deployment/removal of a Juniper or Nokia router in P or PE mode:
  - Base config
  - iBGP mesh update
  - OSS/BSS
- **Core link Migration:**
  - Including functional checks
  - Old config cleanup
  - Partial OSS/BSS alignment
  - Takes now 30 min instead of ½ day
- Promotion from P to PE
  - More meshes
  - Other OSS/BSS
- PHASE1 totally covered.



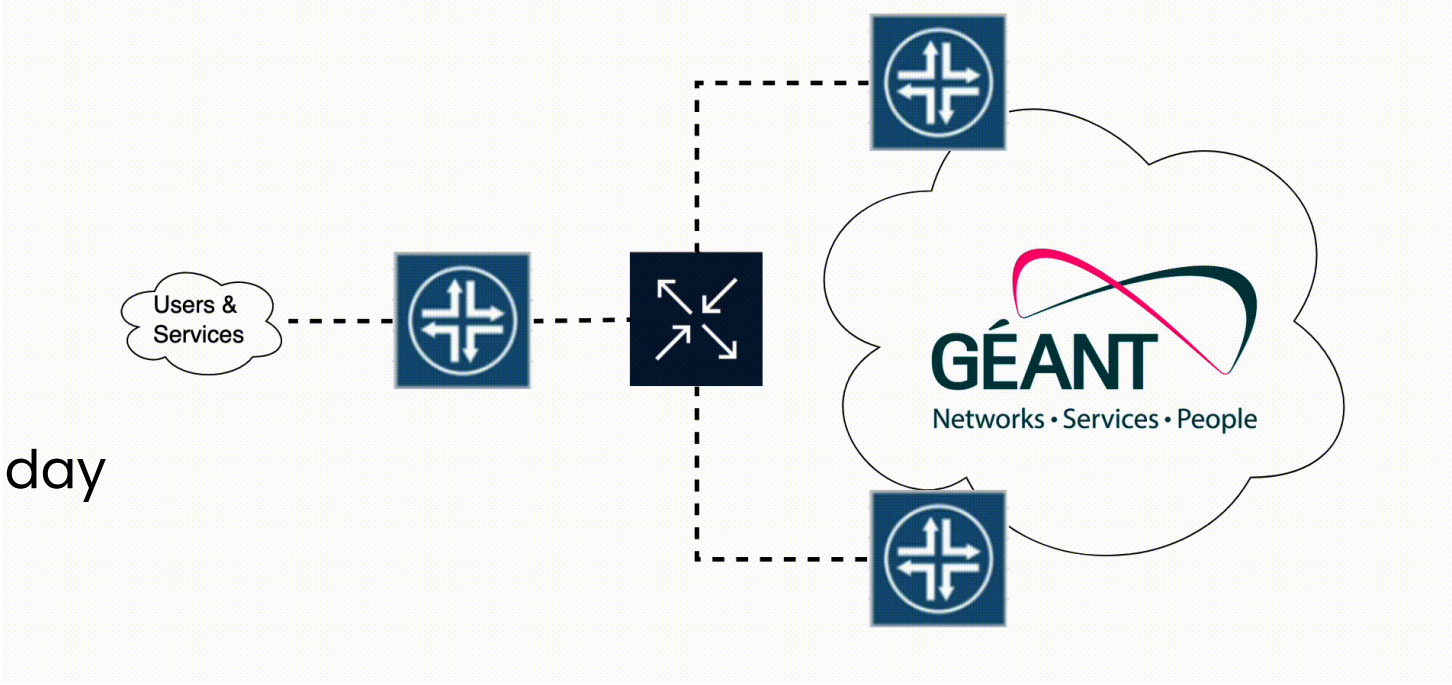
…al momento:

- Deployment/removal of a Juniper or Nokia router in P or PE mode:
  - Base config
  - iBGP mesh update
  - OSS/BSS
- **Core link Migration:**
  - Including functional checks
  - Old config cleanup
  - Partial OSS/BSS alignment
  - Takes now 30 min instead of ½ day
- Promotion from P to PE
  - More meshes
  - Other OSS/BSS
- PHASE1 totally covered.



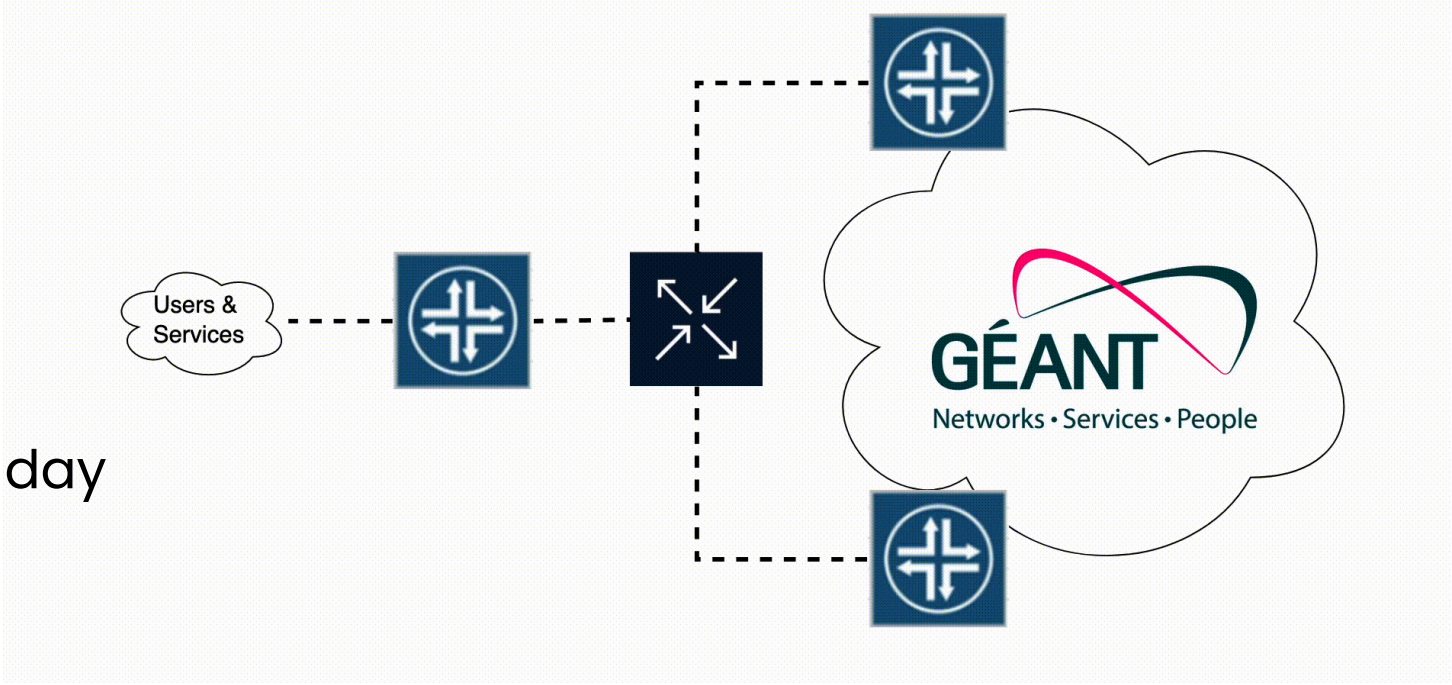
…al momento:

- Deployment/removal of a Juniper or Nokia router in P or PE mode:
  - Base config
  - iBGP mesh update
  - OSS/BSS
- Core link Migration:
  - Including functional checks
  - Old config cleanup
  - Partial OSS/BSS alignment
  - Takes now 30 min instead of ½ day
- **Promotion from P to PE**
  - More meshes
  - Other OSS/BSS
- PHASE1 totally covered.



…al momento:

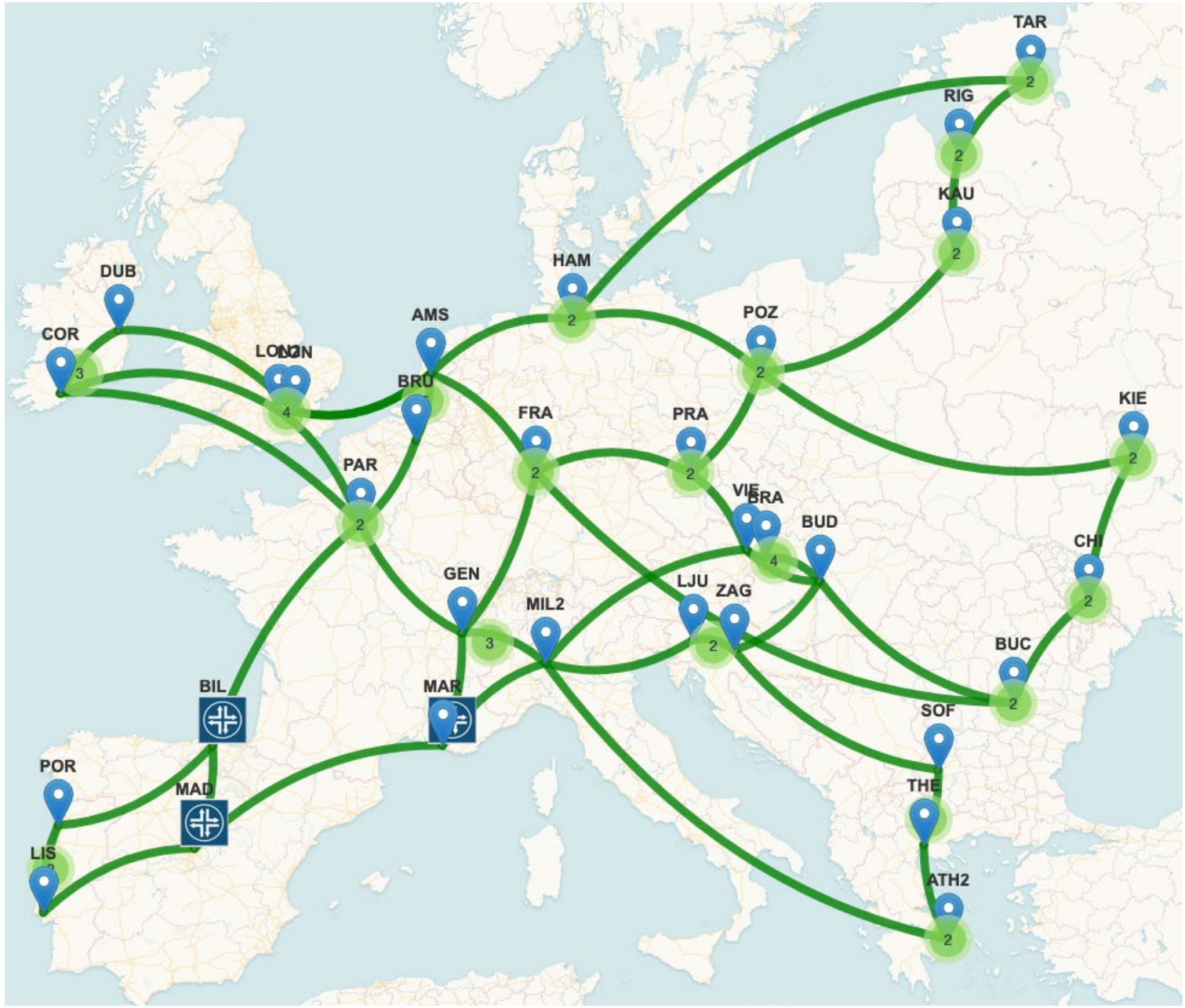
- Deployment/removal of a Juniper or Nokia router in P or PE mode:
  - Base config
  - iBGP mesh update
  - OSS/BSS
- Core link Migration:
  - Including functional checks
  - Old config cleanup
  - Partial OSS/BSS alignment
  - Takes now 30 min instead of ½ day
- Promotion from P to PE
  - More meshes
  - Other OSS/BSS
- **PHASE1 totally covered.**



Derivati: maps

Una visualizzazione della rete, dal punto di vista di GAP:

- Puo' aiutare ad esplorare GAP
- Sintetizza il design di rete
- Mostra diversi aspetti della rete stessa:
  - Capacita'
  - ISIS metric
  - IP planning
  - IDs



Derivati: moodi

Durante la migrazione dei servizi avremo bisogno di piú metriche & checks:

- Usare Ansible per fare PRE/POST checks é costoso
- Il supporto di GNMIc su NOKIA funziona bene
- 1 sec di risoluzione é complicato a lungo termine ma ha senso se e' per un breve momento (un workflow)
- Cosa collezionare é descritto in GAP

=> Monitoring on Demand: GNMIc + Prometheus + Grafana

Cosa abbiamo imparato

- Un team cross-funzionale é un approccio vincente:
  - Network Engineering & Software Engineering
  - Feedback veloce e preciso
  - In genere, piú velocitá
- La cosa difficile non sta nello scrivere codice, ma nel definire I processi:
  - Tanti stakeholders interessati
  - Cambiamento nel modo di lavorare.
- Il re-design e la modellazione pongono le basi per fare ancora di piú:
  - Sottoprodotti/derivati interessanti
  - Observability
  - Reporting
  - Nuovi servizi

L’appetito vien mangiando…

- Nuovi domini tecnologici da orchestrare insieme
- Granulare visibilitá dei servizi e dei loro componenti:
  - Gestione degli incidenti
  - Monitoring
- Self-service
  - Per i nostri partners
  - In ottica multi-dominio
- Approccio sempre piú a “piattaforma”:
  - Offre funzionalitá ad altre parti del business
  - Visione sempre piú olistica

Link Utili

Opensource foundation - Workflow Orchestrator Programme:

- https://workfloworchestrator.org

Demo Orchestrator - Containing our best practices:

- https://github.com/workfloworchestrator/example-orchestrator
- https://demo.workfloworchestrator.org
- https://netbox.demo.workfloworchestrator.org

Examples of other NREN modelling:

- GNA-G Network Automation Working Group: https://github.com/gna-g/NAWG
- GEANT: https://gitlab.software.geant.org/goat/gap

Orchestrator-core documentation:

- https://workfloworchestrator.org/orchestrator-core

Grazie!

Domande?