



GÉANT Automation Platform

De automatizar a orquestar la operación de red en GÉANT

Carolina Fernández (i2CAT)

XXXIII Jornadas Técnicas RedIRIS, Toledo, España
22/05/2025

Público

Introducción

Qué es GÉANT y qué está haciendo

Qué es GÉANT



Lleva la asociación de *National Research & Education Networks* (NRENs) de Europa



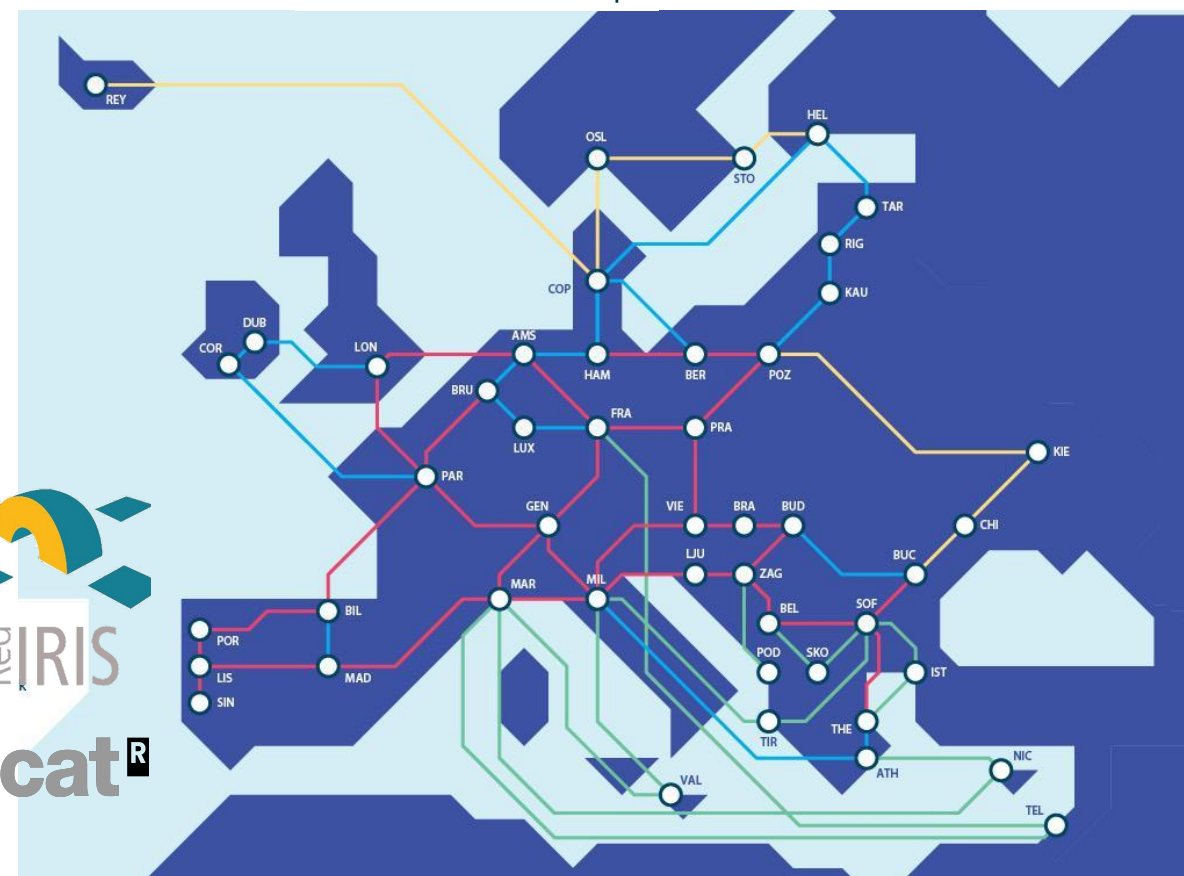
Coordina y participa en proyectos competitivos de la UE



Opera una infraestructura paneuropea

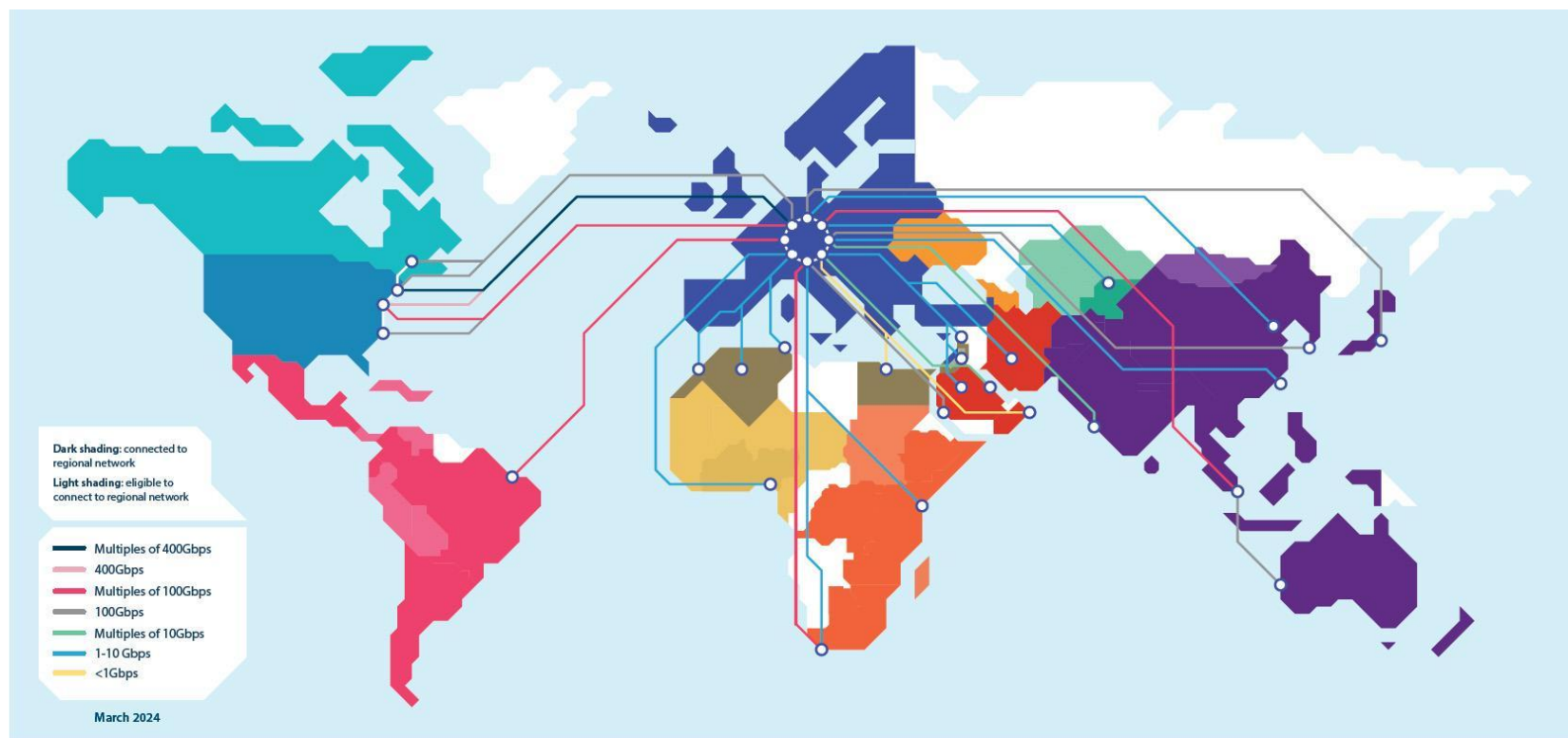


Gestiona un portafolio de servicios para investigación y educación



En Europa: 38 NRENs + NORDUnet; dando soporte a 10.000 instituciones y 50 millones de usuarios académicos

Qué es GÉANT



Es hora de actualizar los equipos de red...

- Plataforma actual: Juniper MX (960/480/204)
 - Más de 10 años de experiencia
 - Muy buena integración con Ansible
 - Servicios L3
- Nueva plataforma: NOKIA 7750SR-S – SROS [no SR Linux]



MX 960



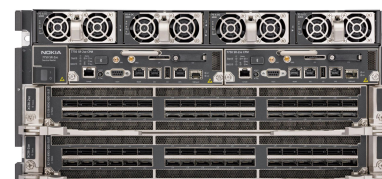
MX 480



MX 204

Ambos disponen de routers virtualizados:

- Juniper MX → vMX
- Nokia SROS → nokia_sros (*Containerlab*)



7750 SR-2se



7750 SR-7s

... Y de migrar la lógica existente a los nuevos

- Migración en 2 fases:
 - FASE 1: mover los enlaces de la red troncal a los nuevos equipos Nokia
 - Los nodos Nokia se despliegan como P/LSR (desde Q1 2024)
 - FASE 2: mover los servicios de clientes a los equipos Nokia, quitando los Juniper
 - Promoción de los nodos Nokia a PE (desde Q1 2025)
- Tras ciertas iteraciones, la operación de la red queda totalmente automatizada:
 - Los operadores ejecutan los flujos de acciones (*workflows*)
 - No se suele necesitar CLI

Diseño y herramientas

Decisión sobre procesos, modelos de datos y herramientas

Automatización y orquestación

Procesos:

- ¿Cuál es el servicio y cómo se ofrece?
- ¿Quién decide y cómo?
- ¿Cuál es el sistema autoritativo para datos concretos?
- ¿Qué más debe pasar si se da una acción?

Artefactos:

- ¿Contienen configuración?
- ¿Qué datos son estáticos o de configuración?
- ¿Qué depende de una única instancia?
- ¿De dónde vienen los datos?
- ¿Hay posibles variantes?

Automatización y orquestación

Procesos:

- ¿Cuál es el servicio y cómo se ofrece?
- ¿Quién decide y cómo?
- ¿Cuál es el sistema autoritativo para datos concretos?
- ¿Qué más debe pasar si se da una acción?

Automatización

- Ejecuta acciones atómicas:
 - Extraer datos
 - Enviar alguna configuración
 - Ejecutar algo
- Muy especializado, depende del contexto
 - Cisco/Juniper/Nokia/Linux/*
- Se enfoca al artefacto generado
- Normalmente es **donde se empieza**

Artefactos:

- ¿Contienen configuración?
- ¿Qué datos son estáticos o de configuración?
- ¿Qué depende de una única instancia?
- ¿De dónde vienen los datos?
- ¿Hay posibles variantes?

Orquestación

- Representa la lógica de negocio
- Interacciona con múltiples sistemas
- Agnóstico, independiente del contexto
- En general se ejecuta punto a punto
- Normalmente es **donde se quiere llegar**

GAP: filosofía

Ir de arriba abajo
(orquestración) es lo que
mejor nos ha funcionado.

*“Pasar de pensar en la
configuración a los
modelos abstractos”*

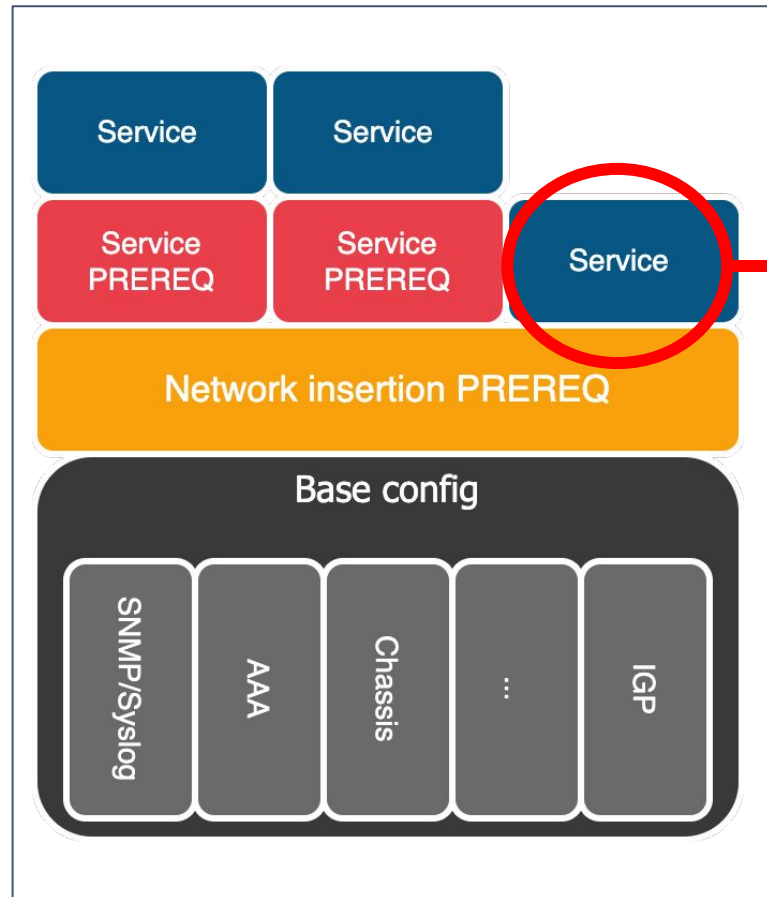
Analizar y repensar los procesos

Descomposición del nodo

Descomposición del servicio

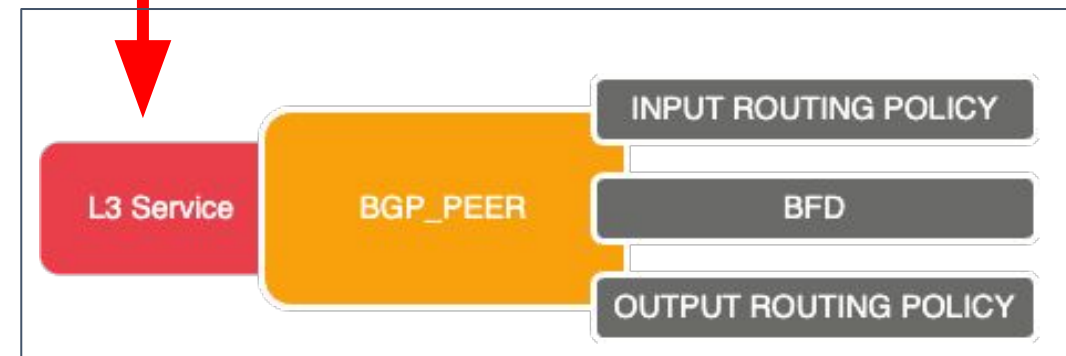
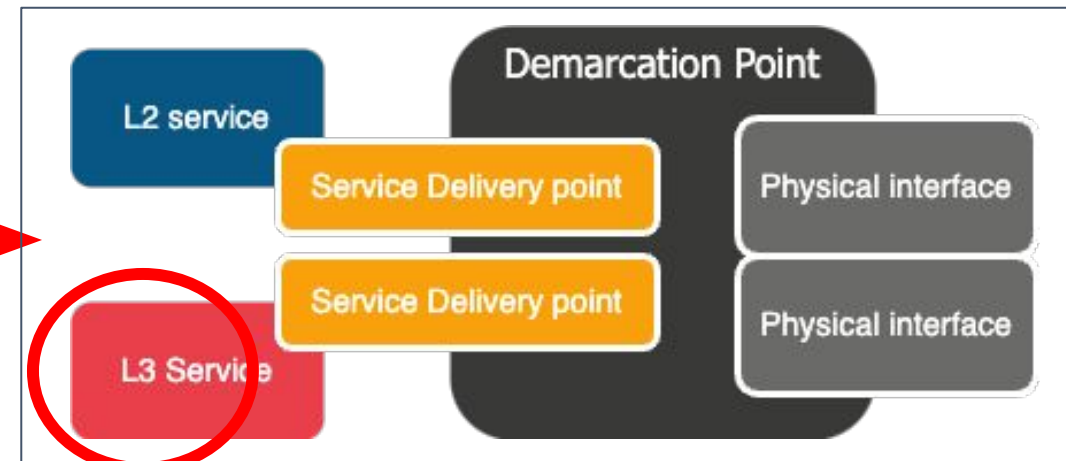
Descomposición de la configuración

GAP: filosofía (descomposición)



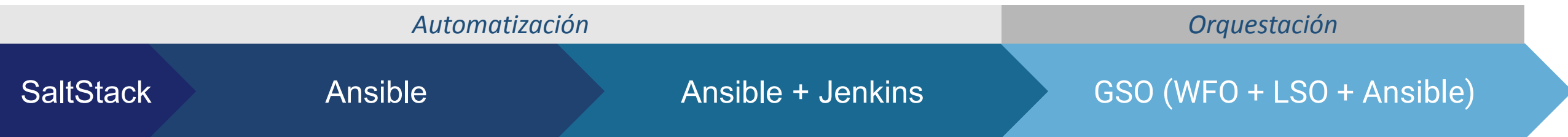
Descomposición del nodo

Descomposición del servicio



Descomposición de la configuración

De automatizar a orquestar

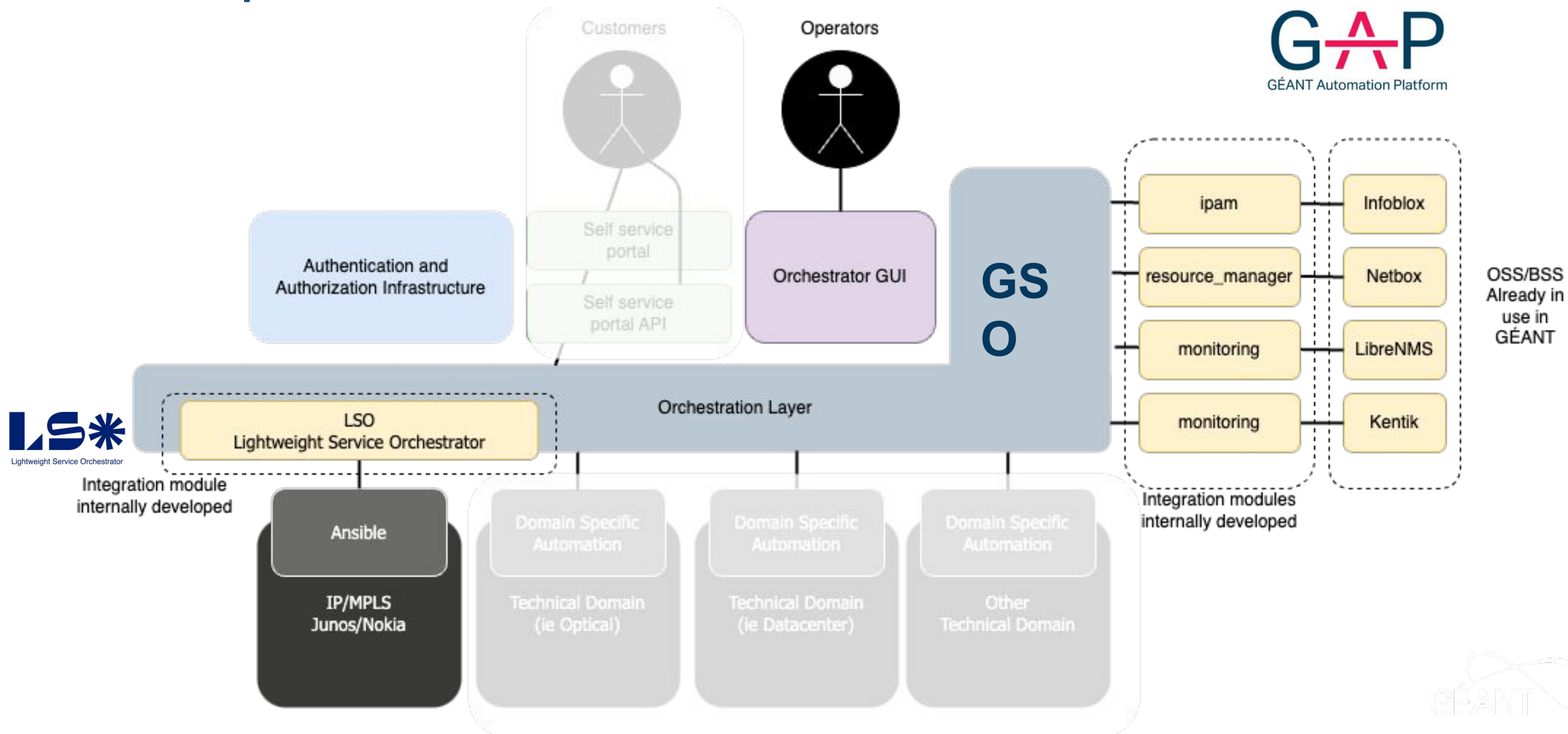


- *Ground truth*: cfg de Ansible
- Inventario versionado de *routers, switches, trunks, servicios*, etc
- Jerárquico, separado por entorno y datos dinámicos VS estáticos
- Iniciado desde Gitlab CI
 - Validación de esquemas
 - Comprobación de duplicados, diferencias y con NMS (LibreNMS)

- Jenkins *pipelines/workflows*
 - Desplegar nuevo *router*
 - Desplegar nuevo *trunk*
- Ansible *playbooks*
- Despliegue Docker: Jenkins GUI+CLI + *worker* con Ansible
- Iniciado por el operador

- GÉANT Service Orchestrator (GSO)
 - Workflow Orchestrator (WFO)
 - Lightweight Service Orchestrator (LSO)
 - Ansible *playbooks*
- Despliegue en Docker/servidor/librería
- Iniciado por el operador

GAP: arquitectura



GAP: arquitectura (LSO → Ansible)

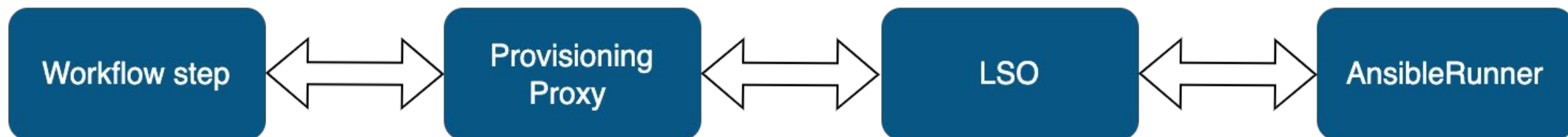
LSO

- Mucha experiencia con Ansible/Jinja
- Se decide no migrar a AWX/Tower (uso de REST)
 - Simplificar ⇒ hazlo tú mismo
 - Código abierto

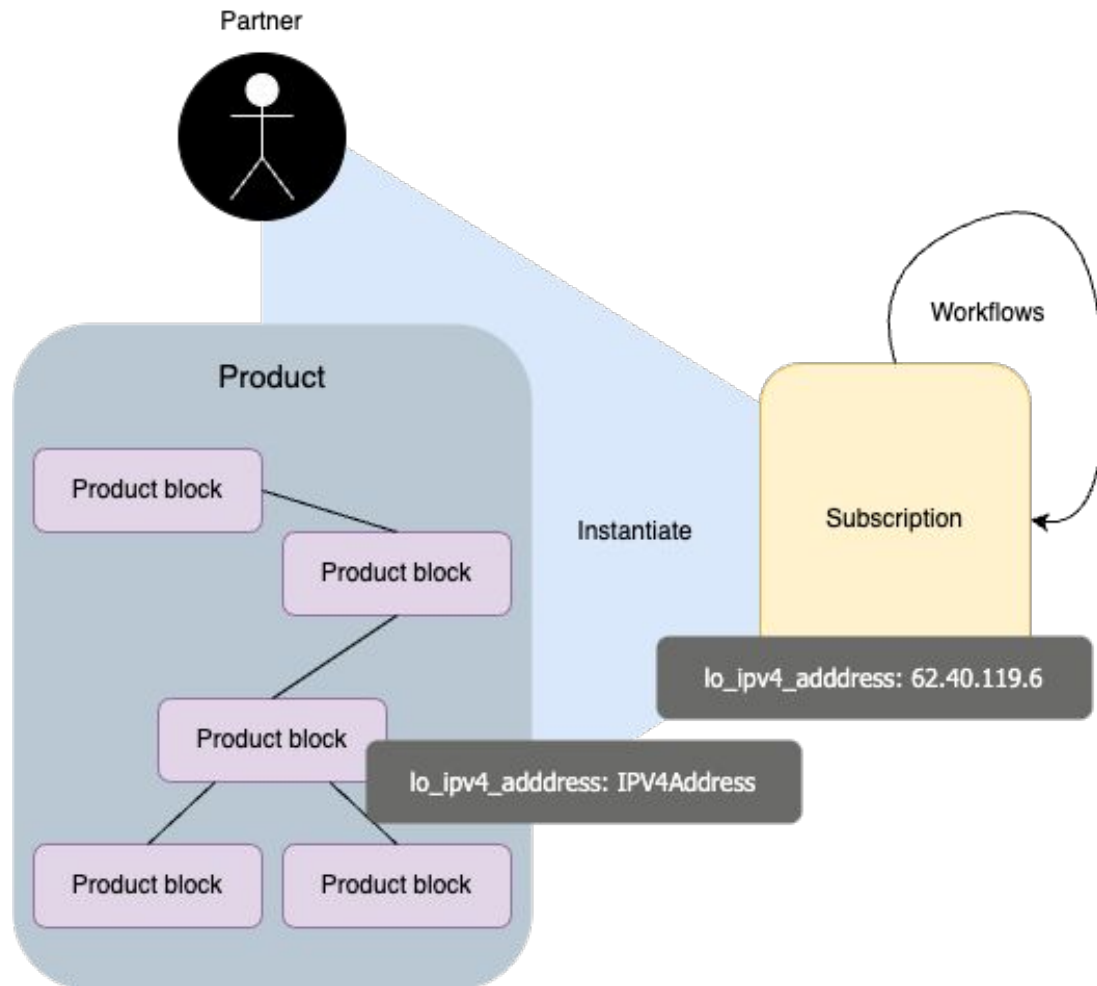


Ansible

- Un *product block* ~ un *role*
- Todo el *ground truth* (inventario, datos de red) lo envía GSO
 - Envío mínimo de datos a LSO (contexto local)



GSO: modelos de datos

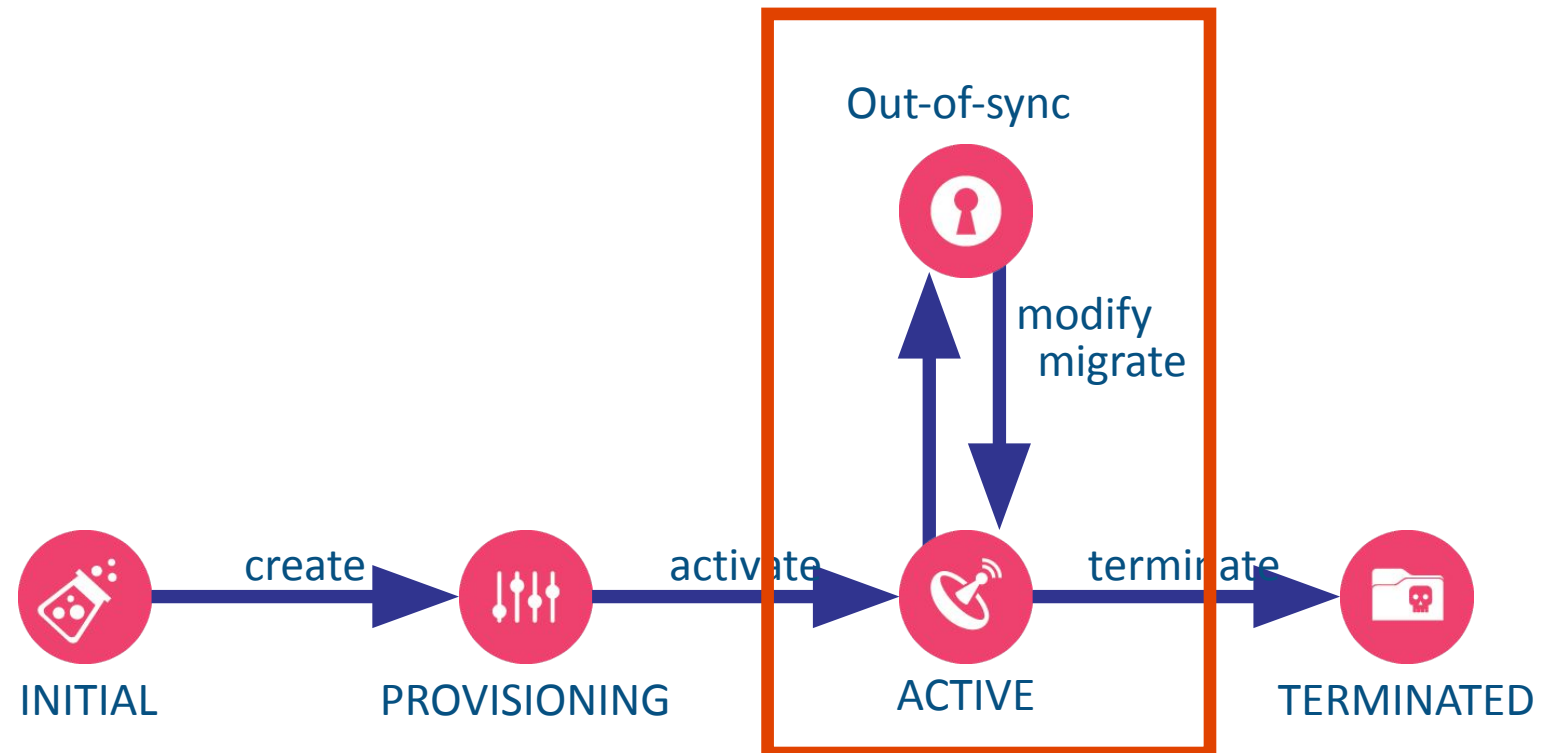


Workflow Orchestrator se alinea con esta filosofía

- *Product*: conjunto de *product blocks*
- *Product block*: objetos abstractos con atributos
- *Subscription* (servicio): instancia de un producto ofrecido a un cliente
- *Workflow*: modifica el ciclo de vida de la suscripción

GSO: ciclo de vida del servicio

Ciclo de vida de una suscripción (servicio) – gestionado desde un *workflow*



GSO: *templates* (ejemplo)

```
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 "$@$%D_}+D#$$^#^<$"; ## SECRET-DATA
    export [ ps-BOGONS ps-to-SURF1-nren ];
    peer-as 1103;
    bfd-liveness-detection {
        minimum-interval 3000;
        multiplier 3;
    }
}
```

Configuración de vecino BGP en *template* (Jinja)

- Usado en los *workflows* de *routers*

```
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 %}
}
```

GSO: servicios (ejemplo)

Subscriptions

- *Site*
- *Router*
- *Switch*
- *IP trunk*
- *Sesión BPG*
- *Circuito L2*
- *Servicio core L3*
- ...

GEANT Service Orchestrator

Test - GSO 2.24.dev2187, Available 12.10

Engine is RUNNING

Start / Subscriptions

Subscriptions

Active Terminated Transient All

Search...

Edit columns Export

ID	Description	Status	In Sync	Product tag	Customer	Customer abstr
00eb948d	Router rt1.kyo.jp.lab.office.geant.net	active	✓	RTR	GEANT Association	GEANT
5ef5a4a5	IP trunk KYO TOK, geantL_s_kid:GS-00003	active	✓	IPTRUNK	GEANT Association	GEANT
f2e10190	IP trunk SEN TOK, geantL_s_kid:GS-00001	active	✓	IPTRUNK	GEANT Association	GEANT
54903db8	Router rt1.sen.jp.lab.office.geant.net	active	✓	RTR	GEANT Association	GEANT
ed4b6864	Router rt1.tok.jp.lab.office.geant.net	active	✓	RTR	GEANT Association	GEANT
8b95d42b	Site in Kyoto, Japan	active	✓	SITE	GEANT Association	GEANT
48484a2e	Site in Tokyo, Japan	active	✓	SITE	GEANT Association	GEANT
772889d3	Site in Sendai, Japan	active	✓	SITE	GEANT Association	GEANT
6d9d8897	Site in Amsterdam, Netherlands	active	✓	SITE	GEANT Association	GEANT
76fd8654	Site in Anezzo, Italy	active	✓	SITE	GEANT Association	GEANT
c9de48ee	Site in Santurce, Spain	active	✓	SITE	GEANT Association	GEANT
ac9e4e6f	Router rt0.pis.it.lab.office.geant.net	active	○	RTR	GEANT Association	GEANT
752c9969	Site in 's-Gravenhage, Netherlands	active	✓	SITE	GEANT Association	GEANT

© 2020 - workflow-orchestrator.org

GSO: *workflows* por servicio (ejemplo)

Product block: IP trunk

Workflows

- Migrar
- Desplegar
- Modificar interfaz IP *trunk*
- Modificar métrica ISIS
- Borrar

Tareas

- Validar configuración IP *trunk*

The screenshot displays the GEANT Service Orchestrator (GSO) web interface. The main header shows the GSO logo and version information: "Test - GSO 2.24.dev2301, Available 1.1.10". The left sidebar contains navigation links: "New subscription", "Start", "Subscriptions", "Workflows", "Tasks", "Metadata", "Settings", and "Maps". The main content area shows the configuration for a specific subscription: "IP trunk SEN TOK, geant_s_sid:GS-00001". The "Product blocks" section lists the components of the IP trunk service, including "IpTrunkBlock", "IpTrunkSideBlock", "IpTrunkInterfaceBlock", "RouterBlock", and "SiteBlock". A "Modify workflow" dropdown menu is open, showing options like "Migrate on IP Trunk", "Deploy TWAMP", "Activate an IP Trunk", "Modify IP Trunk Interface", "Modify GSN metric", "Validate IP trunk configuration", and "Terminate workflow". The "Tasks" section shows a list of tasks, including "Validate IP trunk configuration" and "Terminate workflow".

GSO: *workflows* en acción

Primer paso: dar información

- Lado del IP *trunk* a reemplazar
- Seleccionar nuevo *endpoint*
- Interfaz LAG de Netbox

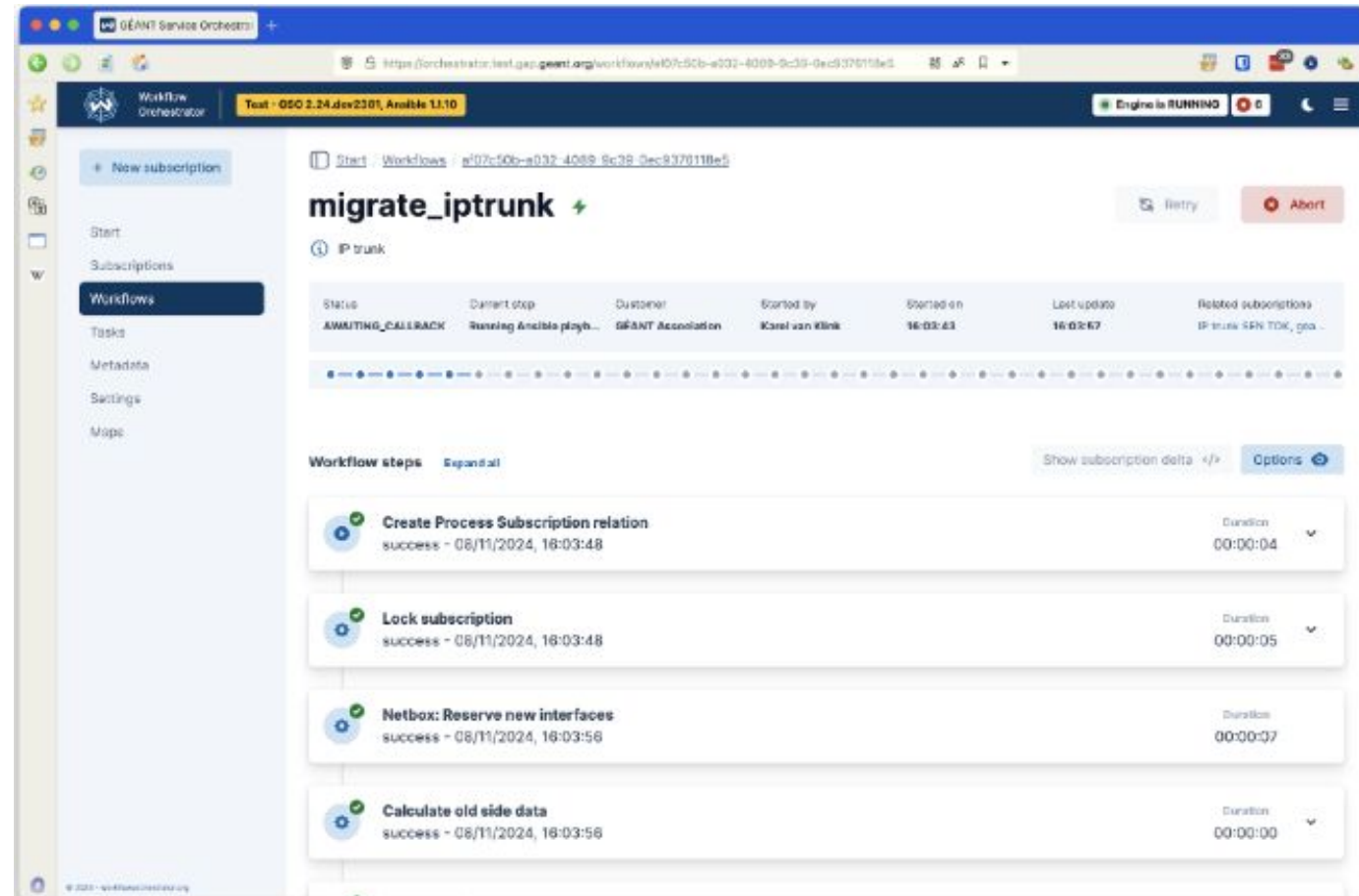
The screenshot shows a web browser window with the URL `https://orchestrator-test.gap.geant.org/workflows/new/migrate_iptrunk?ts.subscribe=tsid42c10135...`. The page is titled "GEANT SERVICE DISCOVERY" and has a sidebar with "Settings" and "Maps". The main content area is titled "User input" and contains the following sections:

- User input**: "Please submit the form to start this workflow"
- Subscription GS-00001 from rt1.san.jp.lab.office.geant.net to rt1.tok.jp.lab.office.geant.net**
- Insert the Ticket number that covers this activity ***: A text input field containing "TT#2024111246263847".
- Select the side of the IP trunk to be replaced ***: A dropdown menu with "Router rt1.san.jp.lab.office.geant.net" selected. Below it are two other options: "Router rt1.san.jp.lab.office.geant.net" and "Router rt1.tok.jp.lab.office.geant.net".
- Migrating to a different Site**: A checkbox labeled "Migrating to a different Site" which is checked.
- Restore BGP metric to original value**: A checkbox labeled "Restore BGP metric to original value" which is checked.
- Buttons**: "Cancel" and "Next" buttons at the bottom.

GSO: *workflows* en acción

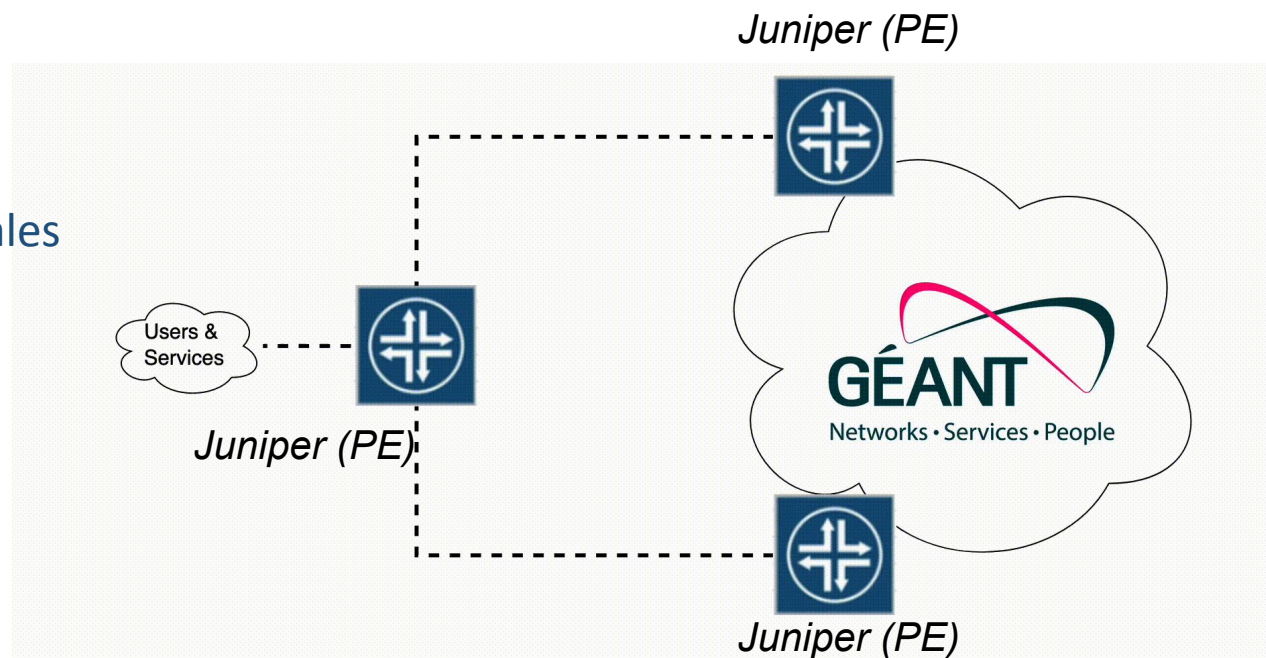
IP *trunk* (workflow: migración)

1. Registrar servicio
2. Bloquear servicio
3. *Netbox*: reservar interfaces
- ...
23. Actualizar IPAM
24. Actualizar modelo de suscripción
- ...
32. Fin



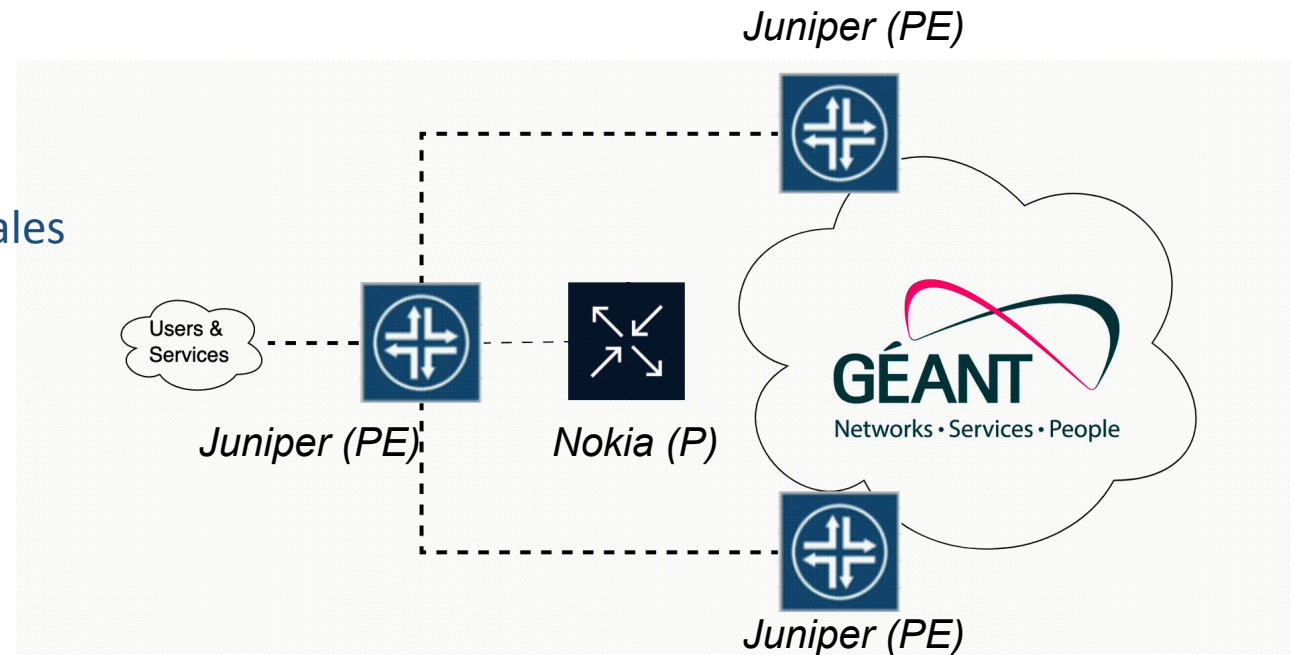
GSO: *workflows* (migración de *router*)

- Despliegue/eliminado de un *router* Juniper o Nokia en modo P o PE
 - Configuración base
 - Actualización de malla (*mesh*) iBGP
 - OSS/BSS
- Migración de enlaces del *core*
 - Incluyendo comprobaciones funcionales
 - Limpiar configuración antigua
 - Alineamiento parcial de OSS/BSS
 - Duración: de ½ día a 30 minutos
- Promoción de P a PE
 - Más mallas (*meshes*)
 - Otros OSS/BSS
- FASE 1 completa



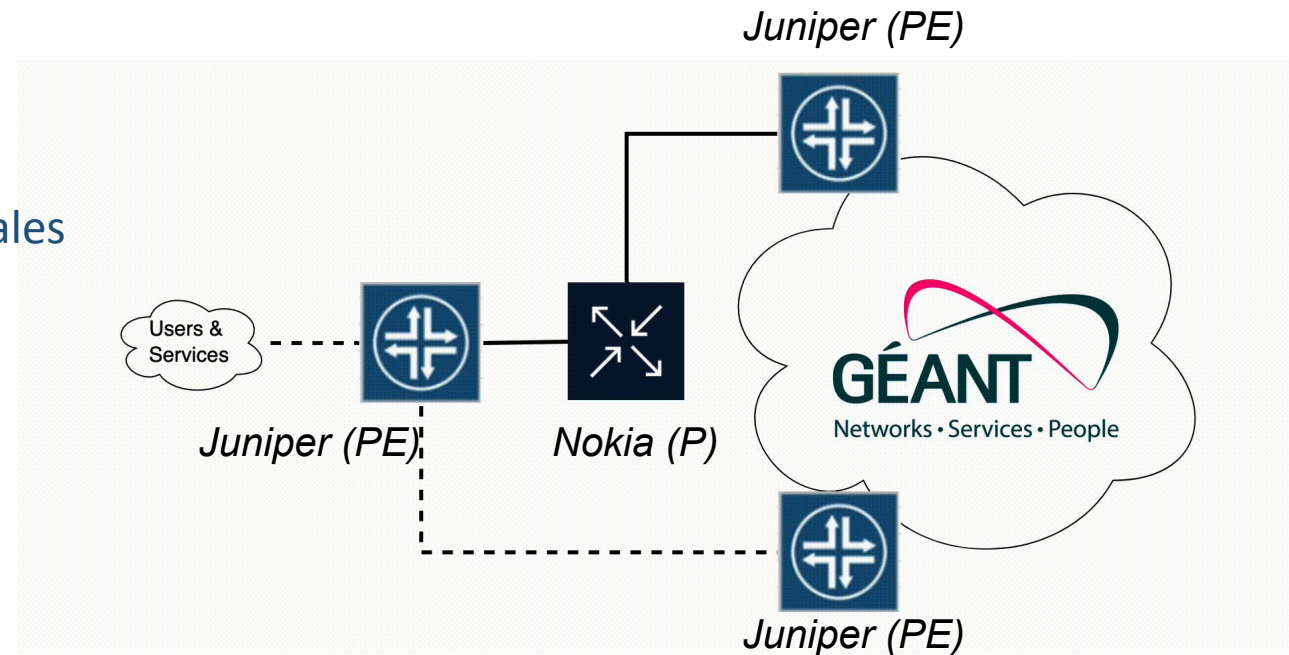
GSO: *workflows* (migración de *router*)

- **Despliegue/eliminado de un *router* Juniper o Nokia en modo P o PE**
 - Configuración base
 - Actualización de malla (*mesh*) iBGP
 - OSS/BSS
- **Migración de enlaces del *core***
 - Incluyendo comprobaciones funcionales
 - Limpiar configuración antigua
 - Alineamiento parcial de OSS/BSS
 - Duración: de ½ día a 30 minutos
- **Promoción de P a PE**
 - Más mallas (*meshes*)
 - Otros OSS/BSS
- FASE 1 completa



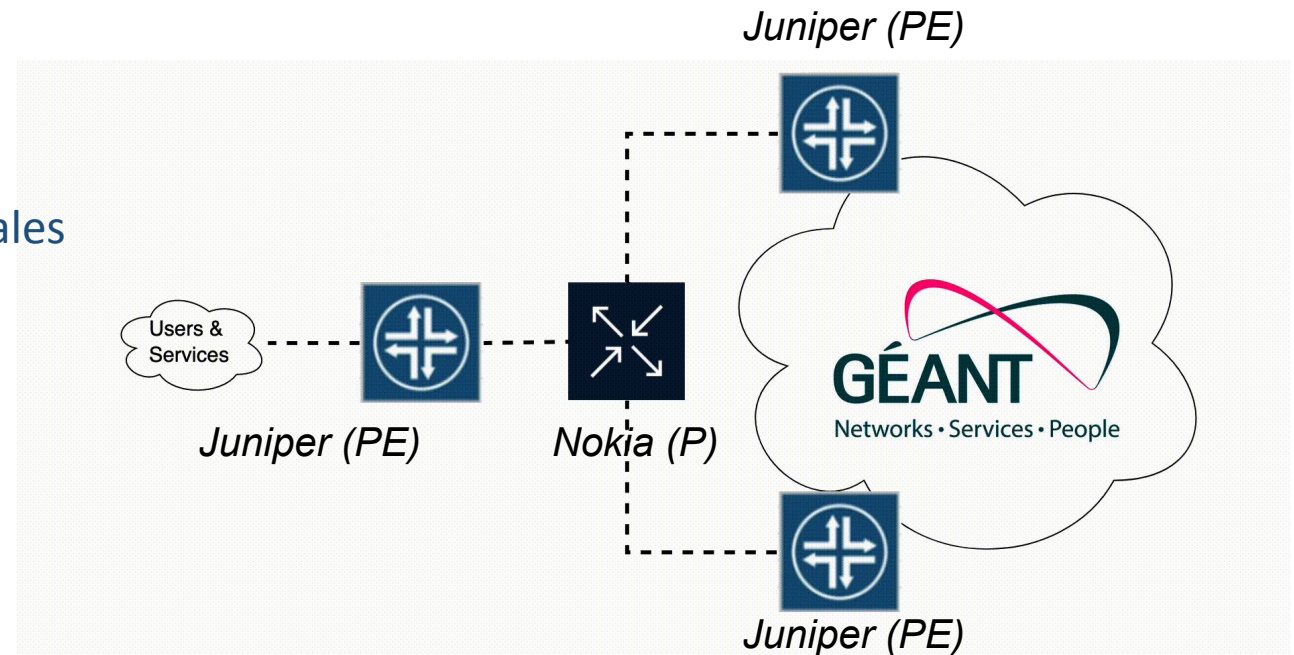
GSO: *workflows* (migración de *router*)

- Despliegue/eliminado de un *router* Juniper o Nokia en modo P o PE
 - Configuración base
 - Actualización de malla (*mesh*) iBGP
 - OSS/BSS
- **Migración de enlaces del *core***
 - Incluyendo comprobaciones funcionales
 - Limpiar configuración antigua
 - Alineamiento parcial de OSS/BSS
 - Duración: de ½ día a 30 minutos
- Promoción de P a PE
 - Más mallas (*meshes*)
 - Otros OSS/BSS
- FASE 1 completa



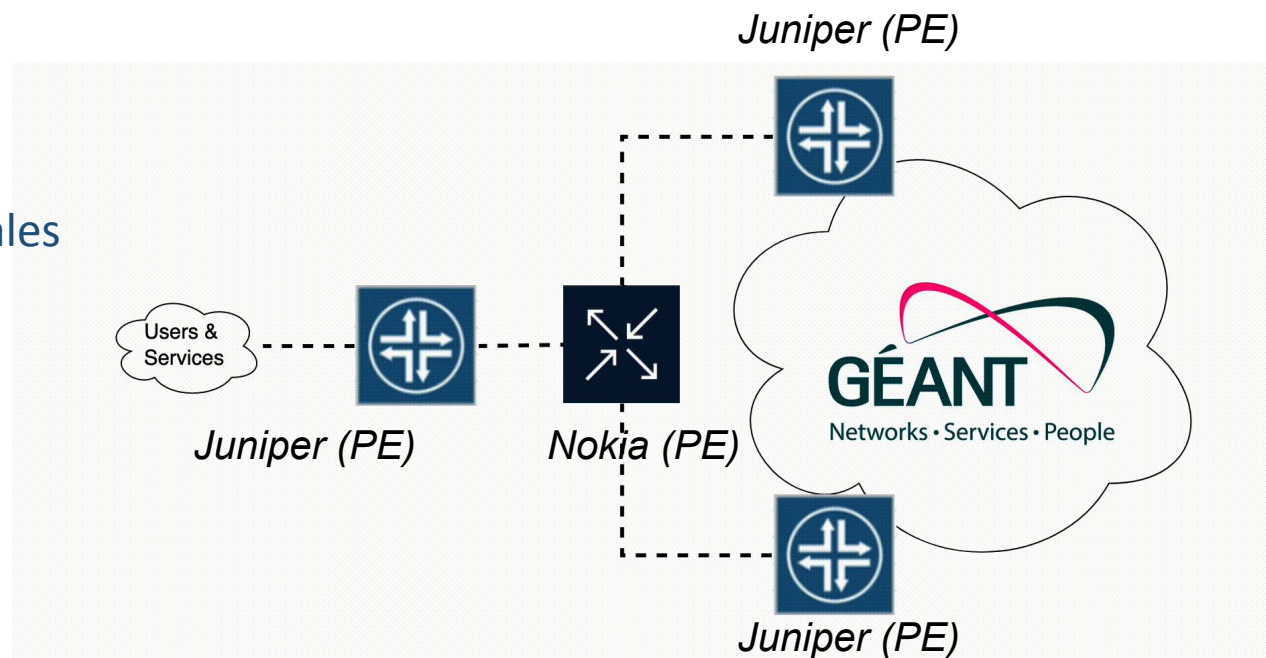
GSO: *workflows* (migración de *router*)

- Despliegue/eliminado de un *router* Juniper o Nokia en modo P o PE
 - Configuración base
 - Actualización de malla (*mesh*) iBGP
 - OSS/BSS
- **Migración de enlaces del *core***
 - Incluyendo comprobaciones funcionales
 - Limpiar configuración antigua
 - Alineamiento parcial de OSS/BSS
 - Duración: de ½ día a 30 minutos
- Promoción de P a PE
 - Más mallas (*meshes*)
 - Otros OSS/BSS
- FASE 1 completa



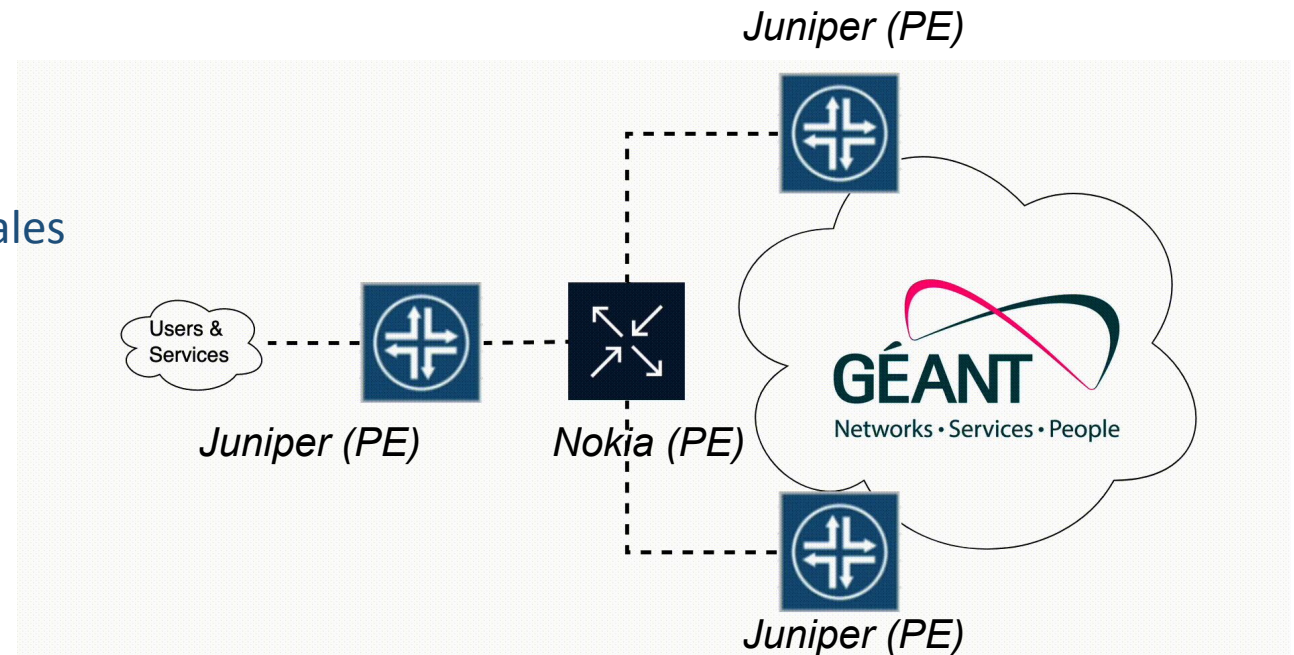
GSO: *workflows* (migración de *router*)

- Despliegue/eliminado de un *router* Juniper o Nokia en modo P o PE
 - Configuración base
 - Actualización de malla (*mesh*) iBGP
 - OSS/BSS
- Migración de enlaces del *core*
 - Incluyendo comprobaciones funcionales
 - Limpiar configuración antigua
 - Alineamiento parcial de OSS/BSS
 - Duración: de ½ día a 30 minutos
- **Promoción de P a PE**
 - Más mallas (*meshes*)
 - Otros OSS/BSS
- FASE 1 completa



GSO: *workflows* (migración de *router*)

- Despliegue/eliminado de un *router* Juniper o Nokia en modo P o PE
 - Configuración base
 - Actualización de malla (*mesh*) iBGP
 - OSS/BSS
- Migración de enlaces del *core*
 - Incluyendo comprobaciones funcionales
 - Limpiar configuración antigua
 - Alineamiento parcial de OSS/BSS
 - Duración: de ½ día a 30 minutos
- Promoción de P a PE
 - Más mallas (*meshes*)
 - Otros OSS/BSS
- **FASE 1 completa**



Derivados

Subproductos derivados del desarrollo de GAP

GAP: derivados

Maps

Vista rápida de la red

Moodi

Métricas y evaluación
durante el despliegue
automatizado

CaaS

Sandbox para un
despliegue fácil de
dispositivos virtuales

Se presentará en TNC'25 (09-13/06/2025)

GAP: derivados (Maps)

Visualización de la red operada mediante GAP:

- Permite explorar GAP
- Resumen del diseño de red
- Muestra diferentes aspectos:
 - Capacidad
 - Métrica ISIS
 - Planificación IP
 - IDs (*sites, routers, etc*)

Corre dentro de la GUI de WFO

- Componente Typescript



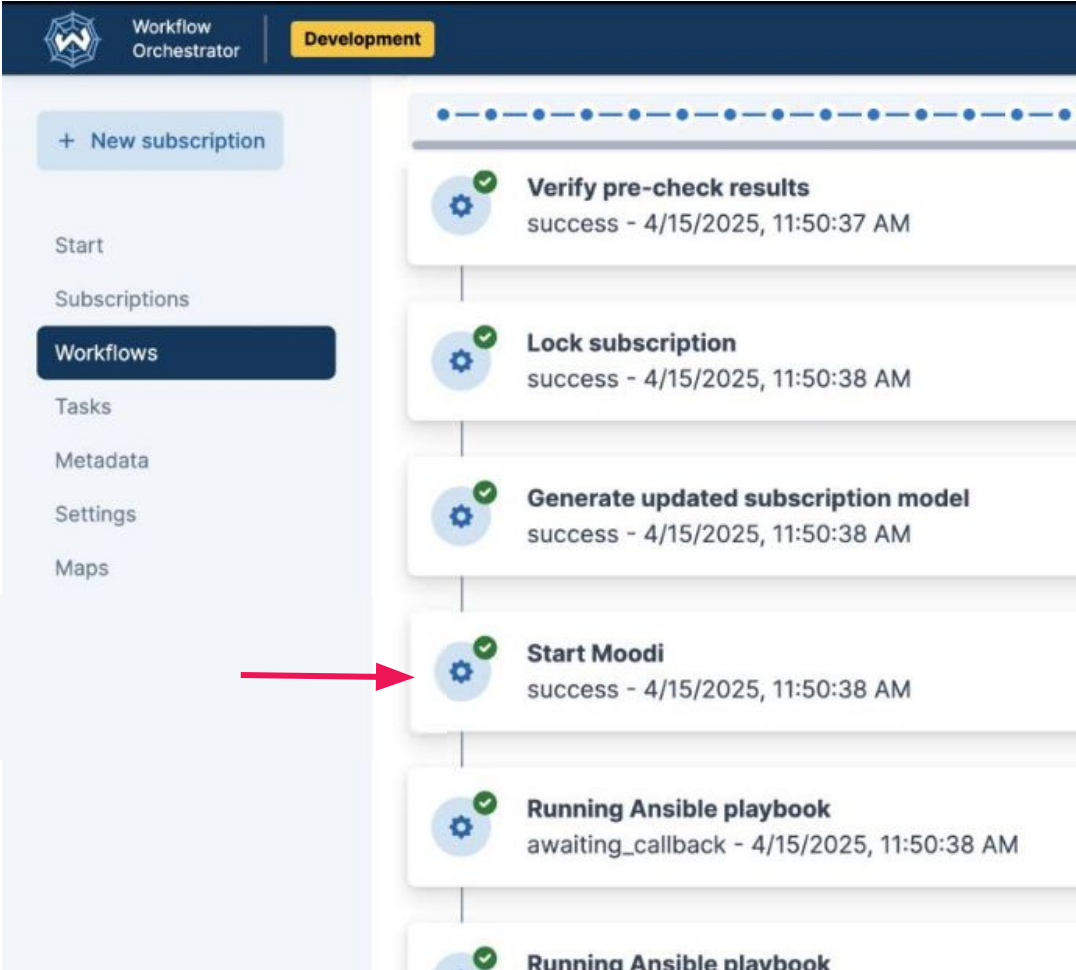
GAP: derivados (Moodi)

Se necesitan más métricas y comprobaciones durante la migración del servicio

- Usar Ansible *playbooks* por cada PRE/POST *check* de un *workflow* es costoso
- Buen soporte para GNMlc en dispositivos Nokia
- Tener telemetría cada segundo es muy valioso, pero necesita mucho espacio → Limitada a ciertos flujos
- ¿Qué datos extraer? Se describen en GAP (DB)

Corre como parte de los *workflows* de GSO

- Monitorización bajo demanda: GNMlc + Prometheus + Grafana



The screenshot displays the 'Workflow Orchestrator' interface. On the left is a sidebar with navigation links: 'Start', 'Subscriptions', 'Workflows' (highlighted), 'Tasks', 'Metadata', 'Settings', and 'Maps'. The main panel shows a workflow execution log for a 'Development' environment. The log consists of a sequence of steps, each with a gear icon, a green checkmark, and a status message with a timestamp. A red arrow points to the 'Start Moodi' step. The steps are:

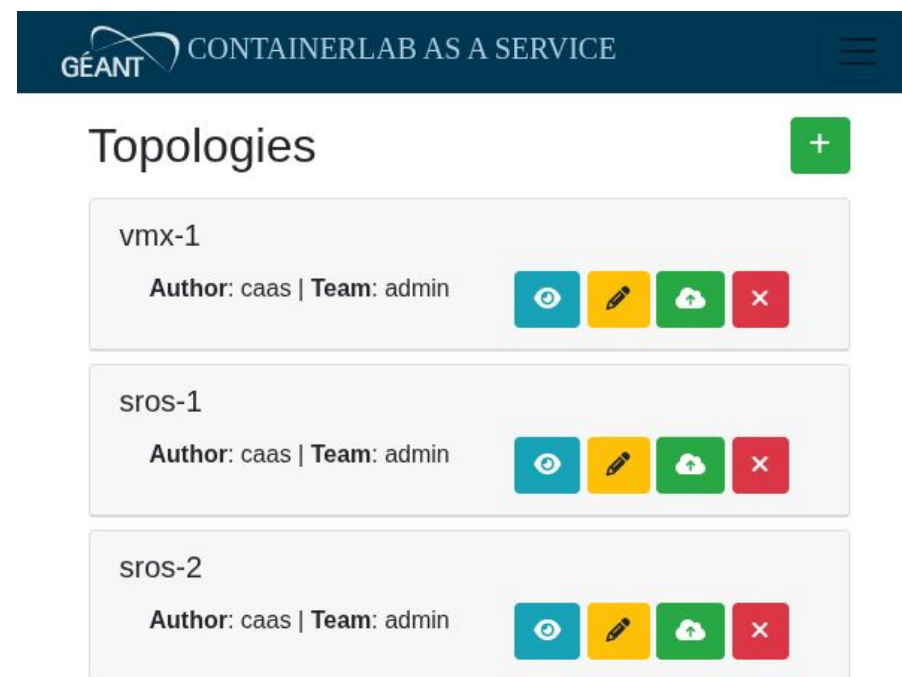
- Verify pre-check results
success - 4/15/2025, 11:50:37 AM
- Lock subscription
success - 4/15/2025, 11:50:38 AM
- Generate updated subscription model
success - 4/15/2025, 11:50:38 AM
- Start Moodi
success - 4/15/2025, 11:50:38 AM
- Running Ansible playbook
awaiting_callback - 4/15/2025, 11:50:38 AM
- Running Ansible playbook

GAP: derivados (CaaS)

Caas: Containerlab-as-a-Service

Simulación de *routers* y otros entornos de vendedores mayoritarios de forma virtualizada

- Soporte para Nokia SROS, Juniper vMX y otros (Cisco, Aruba, etc)
- Despliegue y configuración automáticos
 - En algunos casos requiere configuración de inicio y licencia
- Acceso mediante GUI
- Gestión de grupos y usuarios para separar las *sandboxes*

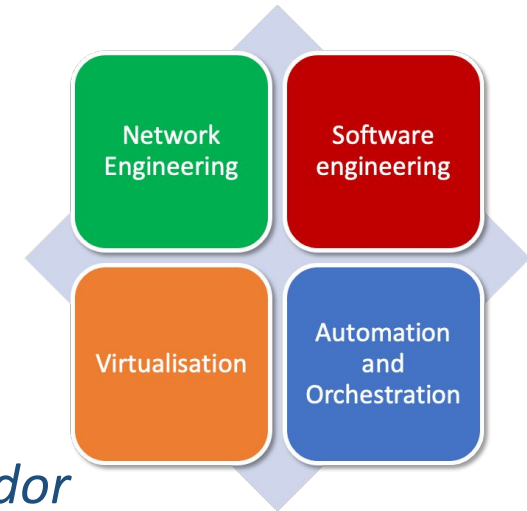


Conclusiones

Reflexiones sobre lo aprendido y qué hay a partir de ahora

Lecciones aprendidas

- Un equipo multidisciplinar como enfoque de base:
 - Ingeniería de red y de *software*
 - Operación rápida, por lo general, y contribuciones precisas
- La dificultad radica en definir los procesos, no en el código:
 - Considerar diversos actores interesados
 - Modelado de datos para llegar a servicios agnósticos del *vendor*
 - Configuraciones únicas (*snowflake*) donde menos se las espera
 - Acordar y adaptar la manera de trabajar
- Este rediseño y remodelado sientan las bases para nuevas opciones:
 - Subproductos interesantes
 - Observabilidad
 - Informes
 - Nuevos servicios a clientes



Nuevos frentes a considerar

- Nuevos dominios tecnológicos a orquestar conjuntamente
- Visibilidad granular de servicios y sus componentes:
 - Gestión de incidentes
 - Monitorización
- Auto provisionamiento (*self-service*)
 - Para socios de GÉANT
 - Con una perspectiva multi-dominio
- Enfoque hacia plataforma como punto único de gestión:
 - Se integra con la funcionalidad de otras partes de negocio
 - Visión cada vez más completa

Workflow Orchestrator *Programme*

- Todo el código queda licenciado bajo Apache 2.0
- Funciona bajo *Commons Conservancy*
- Cada organización mantiene su propiedad intelectual
- Niveles de membresía:
 - *Partner*
 - *Graduate*
 - *Sandbox*
- Sobre todo NRENs y usos de caso de redes – pero hay más



<https://workfloworchestrator.org/>



Enlaces útiles

Workflow Orchestrator (WFO)

- Documentación base: <https://workfloworchestrator.org/orchestrator-core>
- Workflow Orchestrator *Programme*: <https://workfloworchestrator.org>
- Ejemplo: <https://github.com/workfloworchestrator/example-orchestrator>
- Discord: <https://discord.gg/fQkQn5ajFR>

Ejemplos de modelados de otras NRENs

- GNA-G (*Network Automation WG*): <https://github.com/gna-g/NAWG>
- NRENs europeas: <https://wiki.geant.org/display/NETDEV/Mapping+Use+Cases>
- GÉANT (GAP): <https://gitlab.software.geant.org/goat/gap>

Contactadnos en
goat@geant.org



GOVT





Gracias por vuestra atención

www.geant.org



Co-funded by
the European Union