

SDN / Open Flow dans le projet de recherche de GEANT (GN3+)

Xavier Jeannin

GIP RENATER
23-25, rue Daviel
75013 PARIS

Résumé

Dans le cadre du projet GN3+ (avril 2013 – Mars 2015), parmi la tâche orientée prospective, JRA2T1 poursuit les activités de recherche sur Open Flow.

Les technologies SDN visent à centraliser le plan de contrôle du réseau au sein d'un serveur externe. La communauté recherche réseau est particulièrement intéressée car SDN peut relancer l'innovation en rendant facilement programmable le plan de contrôle et en permettant l'usage de matériel de commutation à faible coût. Un autre objectif est de fournir plus de souplesse dans la gestion du réseau et ainsi de mieux répondre aux besoins des utilisateurs. JRA2T1 investit sur les axes suivants : standardisation, mise en production d'un testbed OpenFlow dans GEANT, performance et monitoring, multi-domaine et SDNapps (programmation du plan de contrôle pour les besoins des applications).

RENATER collabore dans la partie monitoring, à l'adaptation du protocole IEEE 802.1ag, Ethernet OAM (Operation, Administration, and Management) et particulièrement dans la partie multi-domaine sur les aspects orientés connexion. Network Service Interface permet de gérer des services réseau multi-domaine de bout en bout en permettant à chaque réseau d'exposer de manière standardiser les ressources réseau disponibles (au sens connexion) pour des connexions multi-domaine. L'utilisation de NSI est pressentie pour permettre l'interconnexion de deux domaines Open Flow soit directement soit à travers des domaines non compatibles Open Flow. La flexibilité de NSI permet d'inclure facilement les caractéristiques d'un flow dans la définition des points d'interconnexion (Service Termination Point). Ainsi grâce à cet ajout au service de connexion de NSI, il serait possible d'interconnecter des domaines Open Flow en incluant les nouvelles fonctionnalités offertes par Open Flow.

Mots-clefs

Software Defined Network, OpenFlow

1 Introduction

Après avoir présenté le banc d'essai (testbed) Open Flow que GEANT met à disposition de la communauté recherche et enseignement, ce court article présente la partie recherche que poursuit RENATER sur la connexion de domaine Open Flow. Ce travail basé sur l'utilisation du framework « Network Service Framework » s'effectue dans le cadre de la tâche de recherche JRA2T1 du projet GN3plus.

2 GEANT Open Flow testbed

GEANT a construit un « testbed » au cours du projet GN3 pour étudier Open Flow. Ce « testbed » va être maintenant porté en production pour un usage par les chercheurs en réseau. Grâce à l'utilisation de « FlowVisor », le testbed est capable de fournir un réseau indépendant géré par un contrôleur « Open Flow » pour chaque chercheur. FlowVisor est un contrôleur OpenFlow spécial qui agit comme un proxy transparent entre les swiches OpenFlow et plusieurs contrôleurs OpenFlow. FlowVisor permet de créer des "slices" (des tranches) de réseau et d'en déléguer le contrôle à différents contrôleurs.

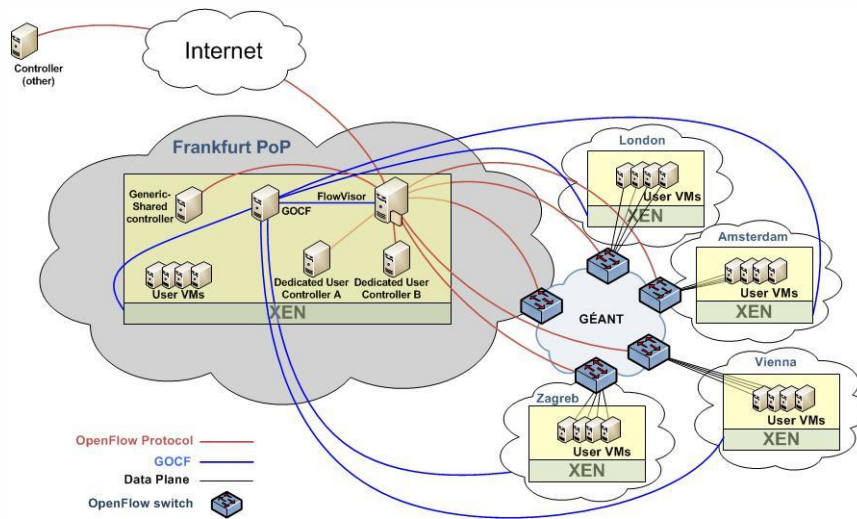


Figure 1: Vue d'ensemble du testbed GÉANT OpenFlow

L'accès se fait via une interface web <https://openflow.geant.net/> grâce à laquelle on peut

- sélectionner des ports sur la topologie ci-dessous, ce qui permet de créer un réseau ;
- créer des machines virtuelles qui servent de sources pour des flux réseaux ;
- créer une machine sur laquelle on installera un Open Flow contrôleur.

1. Select OpenFlow Ports 2. Select Flowspace

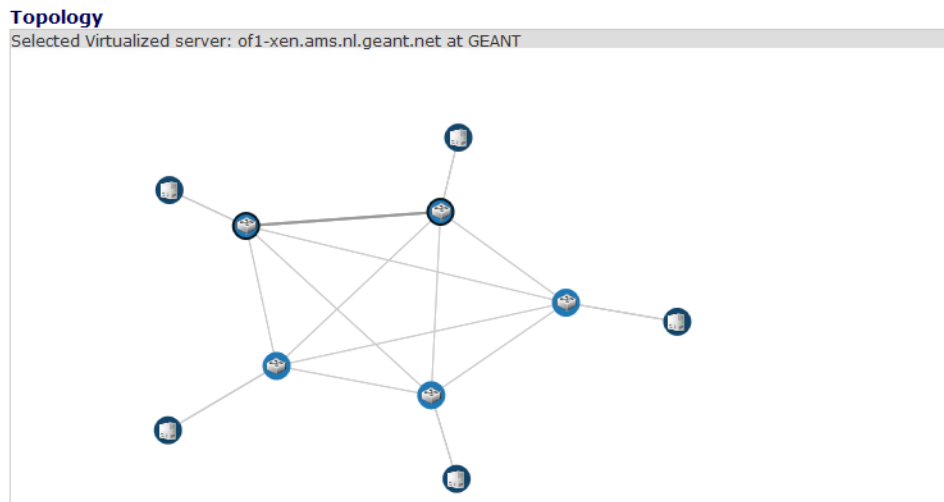


Figure 2 : interface pour la création d'un réseau géré par Open Flow

Enfin, on peut aussi configurer les flux sur les ports des switch « Open Flow » : MAC Source, MAC Destination, Ethernet Type, VLAN ID, IP Source, IP Destination, IP Protocol, TCP/UDP Source, TCP/UDP Destination.

Flowspace 1 (saved)

Field	From	To
MAC Source	<input type="text"/>	<input type="text"/>
MAC Destination	<input type="text"/>	<input type="text"/>
Ethernet Type	<input type="text"/>	<input type="text"/>
VLAN ID	111	111
IP Source	<input type="text"/>	<input type="text"/>
IP Destination	<input type="text"/>	<input type="text"/>
IP Protocol	<input type="text"/>	<input type="text"/>
TCP/UDP Source	80	<input type="text"/>
TCP/UDP Destination	<input type="text"/>	<input type="text"/>
Ports	Aggregate GEANT-OpenFlow: Port 4 on OpenFlow Switch 00:00:00:00:00:00:03 Aggregate GEANT-OpenFlow: Port 7 on OpenFlow Switch 00:00:00:00:00:00:03 Aggregate GEANT-OpenFlow: Port 8 on OpenFlow Switch 00:00:00:00:00:00:01 Aggregate GEANT-OpenFlow: Port 4 on OpenFlow Switch 00:00:00:00:00:00:01	
Delete?	<input type="checkbox"/>	

Si l'infrastructure est en place, il a noté qu'à l'heure de l'écriture de ce document, l'ensemble des outils qui permettent de gérer cette plateforme est toujours en cours de réalisation ou de déploiement.

3 Utilisation de NSF pour interconnecter des domaines OpenFlow

3.1 Bref rappel sur Network Service Framework (NSF)

Le « NSF » est un framework qui permet la fourniture de services réseau dans un contexte multi-domaine. NSF traite le réseau comme un service en cachant aux utilisateurs la complexité réseau. Les ressources réseaux sont exposées grâce à l'interface « Network Service Interface » (NSI) et le « Network Service Agents » gère les demandes de ressources réseau, fournissant ainsi un « plan de service ».

Le « Network Resource Manager » (NRM), pour sa part, a autorité sur le réseau local et gère les demandes de service pour le réseau local.

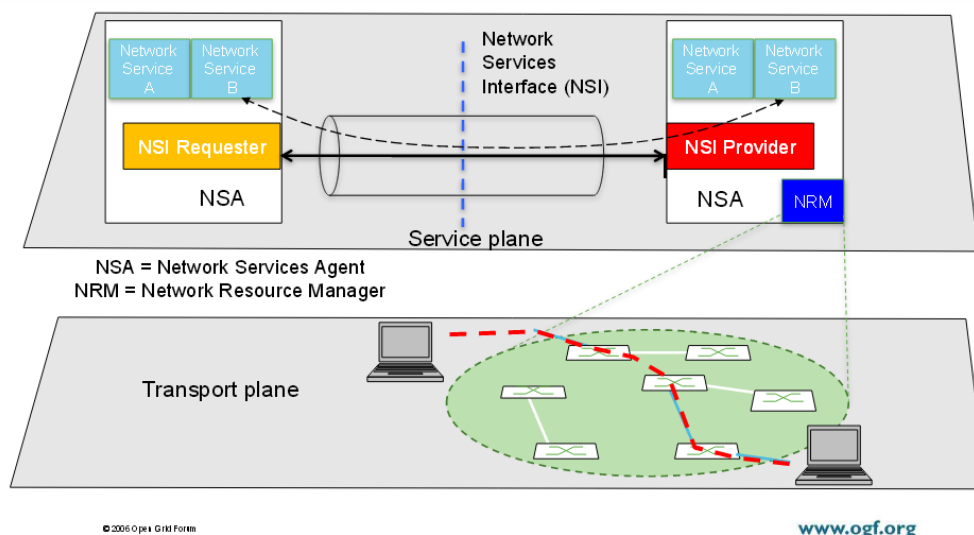


Figure 3: OGF NSI Framework

Voici quelques définitions d'éléments importants du Network Services Framework et utilisées par le protocole « NSI »:

- NSI Network Services – Services permettant le monitoring, le contrôle de ressources réseau. Le Connection Service utilisé pour la gestion de connexion point-to-point est un exemple de NSI Network Services ;

- Network Service Agent – Logiciel qui demande et fournit des Network Services grâce une Network Service Interface ;
- Network Service Interface – Une interface fournissant une session sécurisée et fiable afin de permettre un échange entre deux NSA concernant les services réseau disponibles dans les 2 domaines ;
- Network topology representation – représentation topologique inter-réseau utilisée par NSI ;
- Network service plane – liste des NSA et session NSI associées entre ces NSA.

3.2 NSF et l'Open Flow multi-domaine

NSF a été créé particulièrement pour faciliter la mise en œuvre de deux contextes :

- lorsque les demandes des ressources réseau sont initiées par les applications (Grid, ...)
- des réseaux qui veulent partager leurs ressources pour étendre ses services et améliorer les performances.

Ces deux contextes correspondent au contexte Open Flow multi-domaine

3.3 Network Connection service

NSI supporte plusieurs services réseau dont le service réseau de connexion (Network Connection – NC) qui permet l'établissement de « circuit réseau » à travers différents domaines gérés par des fournisseurs différents. C'est l'un des services réseaux de NSF les mieux spécifiés et implémentés. Nous pensons que le service Network Connection (NC) est un bon candidat pour réaliser une interconnexion de domaine Open Flow.

L'Open Grid Forum a défini le Connection Service (CS) et le protocole NSI permet la réservation, la création, la gestion, et la suppression d'une connexion réseau tout en supportant des mécanismes d'authentification et d'autorisation.

Les services multi-domaine doivent être capables de fonctionner sur un ensemble hétérogène de technologies utilisées pour le plan de forwarding. Dans NSI, la notion de connexion est abstraite, et les messages NSI sont basés sur un schéma flexible capable de spécifier des contraintes particulières de la connexion. Les contraintes de la connexion seront évaluées afin de les comparer avec les technologies disponibles dans les réseaux locaux traversés. Un pathfinder au sein de NSI est en charge de créer ce chemin en fonction des contraintes. C'est par cette méthode que NSI veut fournir un « plan de service » permettant fournir une connexion à travers des technologies de transport hétérogène.

Il est important de relever le rôle des Service Termination Point (STP) placés à la bordure des réseaux. Chaque STP décrit une connexion possible entre deux STP dans le réseau. L'interconnexion de deux STPs entre deux domaines crée la connexion entre ces deux domaines. La réunion de ces deux STPs connectés crée un Service Demarcation Point (SDP).

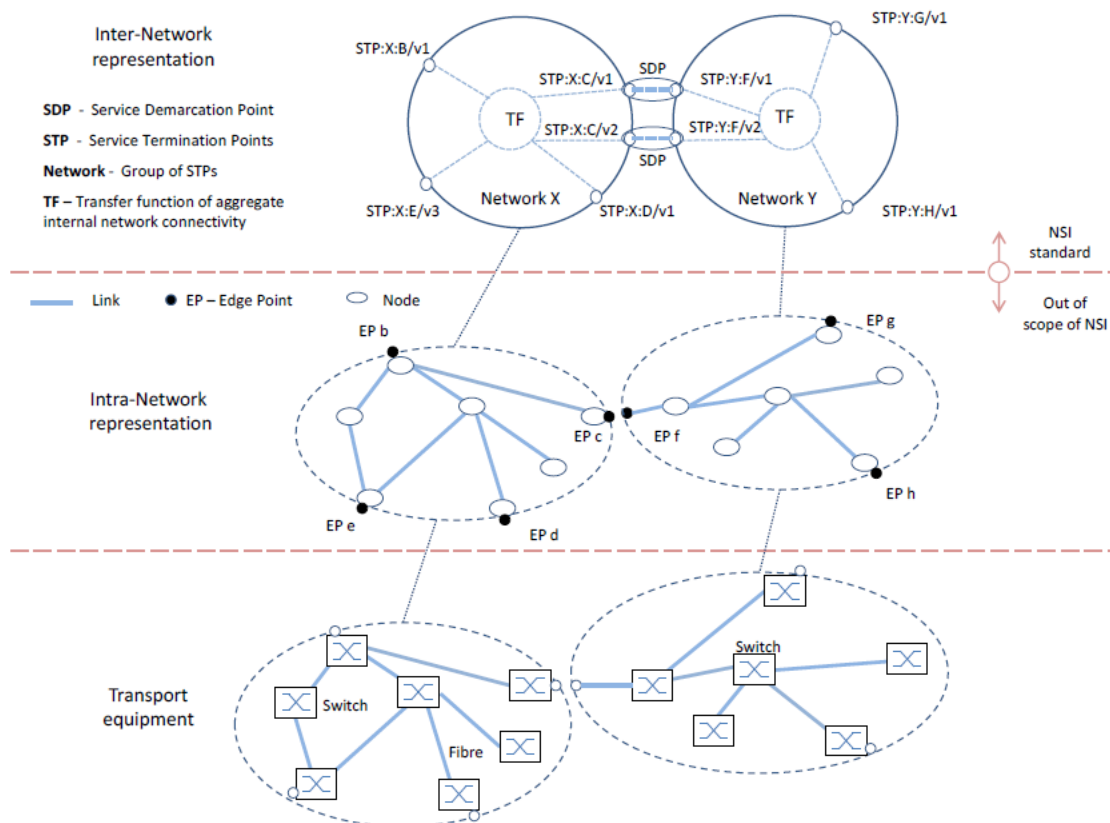


Figure 4 : NSI-CS décrit les connexions réseau possibles en bordure de celui-ci

3.4 Usage possible de NSF pour la connexion multi-domaine Open Flow

Plusieurs arguments poussent à utiliser NSF and NSI-CS pour la connexion multi-domaine Open Flow :

- NSF séparent le plan de contrôle du data plane comme Open Flow ;
- NSF est un framework inter-domaine
 - qui fait abstraction du service de transport,
 - qui est un modèle distribué,
 - dont le « provisioning » au niveau des réseaux locaux est découplé de NSI et est fourni par le “network resource manager” (NRM),
 - qui inclut la sécurité car celle-ci est présente dans NSI ;
- NSI-CS est spécialement conçue pour fournir de manière transparente un canal de communication d’un point à un autre.

Faire correspondre le modèle Open Flow et NSF :

- la fonction NRM correspond bien à celle de contrôleur SDN ;
- le contrôleur SDN peut être enrichi pour supporter NSI et ainsi remplir la fonction de NSA pour open flow domaine. Une autre solution consisterait à enrichir un NSA pour être capable de communiquer avec un open flow contrôleur via l’interface north bound (interface entre le contrôleur Open Flow et le switch Open Flow, et entre les applications et le contrôleur Open Flow). NSI pourrait être utilisée pour « provisionner » la connexion et fournir cette connectivité pour établir une connexion inter-réseau qui passerait par ce domaine SDN ;
- NSI pourrait être utilisée comme interface the east/west (interface inter-contrôleur) pour permettre l’échange entre deux contrôleurs SDN de deux réseaux administrés par la même entité ou deux entités qui collaborent.

Ainsi le contrôleur SDN couplé avec le protocole NSI pourrait interagir avec d’autres réseaux.

L’un des plus importants points qu’il faut considérer dans l’usage de NSI pour interconnecter des domaines Open Flow est la manière dont va être établie la correspondance entre toutes les connexions possibles offertes par un domaine Open Flow et les STP de NSI.

3.5 Cas d'utilisation

3.5.1 Cas 1: Connecter deux domaines Open Flow non adjacents

Dans ce cas, le protocole NSI-CS va être utilisé pour réserver et établir la connexion demandée.

Les possibilités de « provisioning » de ressources réseau ne sont pas les mêmes dans un domaine Open Flows et dans un domaine non Open Flow. Par exemple, dans un domaine Open Flows, on peut avoir un flux caractérisé par le VLAN 111 et le port TCP 80 et qui se traduit par un STP (STP 111-80). Comme un domaine non Open Flow ne peut fournir ce type de connexion sur un de ces STP, il est nécessaire de faire correspondre le STP qui offre la connexion sur le VLAN 111 avec le STP 111-80. La connexion pour un flux demandant VLAN 111 et le port 443, deviendrait alors impossible.

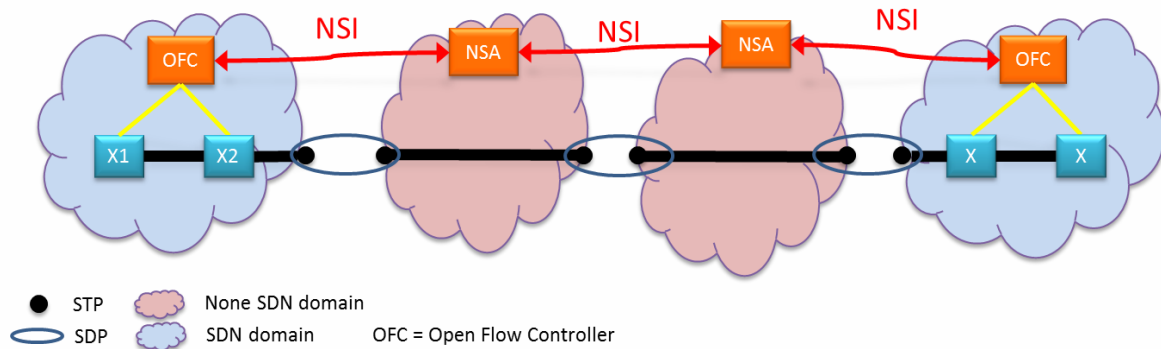


Figure 5 : Connexion de deux domaines Open Flow non adjacents

3.5.2 Cas 2: Connecter deux domaines non Open Flow à travers des domaines Open Flow

Dans ce cas, le domaine open-flow fournit le transit pour des domaines non Open Flow.

Le contrôleur Open Flow (OFC) joue le rôle de NRM et deux scenarios sont possibles :

- l'OFC peut échanger avec un NSA ;
- l'OFC intègre un NSA.

NSI va être utilisée pour « provisionner » la connexion et fournir cette connectivité pour établir une connexion inter-réseau. Ici aussi, la correspondance entre toutes les connexions possibles offertes par un domaine Open Flow et les STP de NSI est un point clé. Les deux scénarios seront testés :

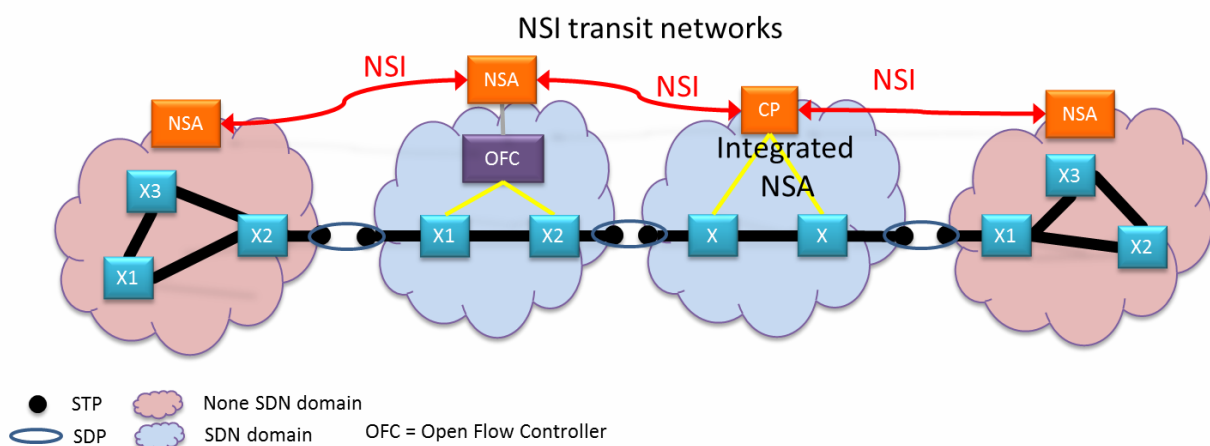


Figure 6 : Connexion de deux domaines non Open Flow à travers des domaines Open Flow

3.6 Perspectives

Premièrement, dans la définition de la requête d'une nouvelle connexion dans la nouvelle version NSI Connection Service v2.0, le champ 'anyAttribute' a été ajouté en prévision pour de futures extensions technologiques. Ce qui correspond à notre cas pour Open Flow et nous permet ainsi d'ajouter les spécificités d'une « connexion pour des domaines Open Flow ». Nous envisageons d'utiliser ce champ pour décrire un flow au sein de la connexion. D'autre part, il a été spécifié qu'au sein des domaines qui ne sont pas en mesure de traiter ces nouvelles extensions, l'agent NSI ignorera cette option à la place de rejeter la requête.

Deuxièmement, l'utilisation d'une connexion au niveau 2 permet à deux domaines Open Flow de communiquer à travers des domaines non-Open Flow tout en préservant la possibilité de mettre en place la définition des flots dans les domaines Open Flow. Ce type de connexion est pour autant non optimale ; par exemple, un domaine Open Flow devra utiliser une connexion VLAN 111 pour interconnecter deux domaines pour une requête de connexion pour le VLAN 111 et le port TCP 80 et ne pourra après plus satisfaire une nouvelle requête pour le VLAN 111 et le port TCP 8080.

La requête pour interconnecter deux domaines Open Flow sera donc une requête de connexion niveau 2 (Ethernet, VLAN ou une connexion point à point générique) enrichie des attributs spécifiques à un domaine Open Flow. Le domaine non Open Flow pourra fournir la connexion de niveau 2 et si le domaine est Open Flow alors il prendra en compte les informations du champ 'anyAttribute'.

La prochaine étape de ce travail sera d'implémenter les différents éléments de cette solution.