Dynamic network service control and management techniques across multi-provider networks

by

Atsushi Taniguchi

Dissertation

submitted to the Department of Informatics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

The Graduate University for Advanced Studies, SOKENDAI
Mar. 2020

Abstract

Communication networks are now an essential infrastructure of society. Various services are constructed across multi-provider networks, which are usually configured and operated statically. Dynamic Network Service (NS) control and management across multi-provider networks enables resource utilization and operability to be provided more efficiently. This dynamic NS control and management mechanism reduces human work load and significantly improves overall work efficiency. Networks constructed across multi-provider networks are expected to be used in various services (e.g., automated driving, remote drone control, and remote surgery). For such applications, reliability is crucial to eliminate accidental emergencies. However, there is currently no established method for deploying NSs across multi-provider networks dynamically and for assessing their reliability. NS deployment across multi-provider networks should also be defined in global standardizations such as the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) Network Functions Virtualization (NFV). The current documents, however, have significant issues (e.g., overload, security, and location specification) for realistic operation scenarios of multi-provider networks. This dissertation describes four typical use cases featuring multi-provider networks (e.g., basic use case of NS deployment, modification to NS connectivity, network selection from two provider networks, and NS expansion to other provider networks) and operational flows. In this dissertation, I also proposes a scheme for exchanging network information between providers. My evaluation using the current specifications and realistic parameters revealed that an NFV Orchestrator (NFVO) could be overloaded when an NS was deployed in multi-provider networks. This dissertation thoroughly describes the multi-provider NS deployment from several practical aspects unlike the previous academic work. My proposals were adopted as a new feature of the next ETSI NFV specifications by clarifying use cases that can only be achieved with an exchange model. Another critical component to meet service requirements is the selection of an appropriate network, as the network reliability depends on the operation of each network provider. I also proposes a method that enables the lower and upper reliability to be computed in a distributed manner without requiring privacy disclosure. While this problem may seem similar to a traditional reliability evaluation assuming a single-domain network, the existence of multiple domains introduces the following two challenges. The first is the high computation complexity; i.e., network reliability evaluation, is known to be #P-complete, which has prevented reliability evaluations of multi-domain networks. The second is intra-domain privacy; i.e., network providers that never disclose internal data required for reliability evaluation. My

method is solidly based on graph theory and is supported by a simple protocol that secures intra-domain privacy. Experiments on real datasets show that the method can compute the reliability for 14-domain networks in one second. The reliability is bounded with reasonable errors; e.g., bound gaps are less than 0.1%. The privacy issue has not been studied in the long history of network reliability. This will be a key issue in the future of NSs, since multi-provider NSs have been recently discussed in standardization bodies. A feasibility evaluation is required to clarify the requirements for network path control scenarios of NS deployment across multi-provider networks. This dissertation presents a dynamic network path control scenario with dynamic inter-domain and intra-domain network path control using optical switching and control plane technologies. The focus was inter-domain network path creation, Quality of Service (QoS) recovery for protecting high priority traffic over an OIF-based User Network Interface (OIF UNI) using the policy controllers, and a failure recovery of a Label Switched Path (LSP) established over an External Network to Network Interface (ENNI). Routing problems that arose in the multi-domain network were successfully solved and the actual service activation time of inter-domain Ethernet transport services between Japanese and US domains was evaluated. The QoS recovery successfully achieved the migration of high-priority video traffic between Tokyo and Osaka with no errors within around 30 seconds. There was no packet loss for high-priority traffic flow when migrating traffic between a Multi-Protocol Label Switching (MPLS)-LSP and an Optical LSP. The link failure recovery was also confirmed by using a hierarchal LSP over a network testbed without the outflow of any control packets to an outside domain. The measured restoration time of the link failure recovery was 272 ms. This indicates that the proposed traffic control scheme can be applied to NSs that require QoS recovery within minutes with low packet loss rates in multi-provider networks.

Contents

List of Figures

List of Tables

Abbreviations

3GPP 3rd Generation Partnership Project
AS Autonomous System
ASBR Autonomous System Border Router
ASON Automatically Switched Optical Network
BF Base Flow
BGP Border Gateway Protocol
BUS Business Applications
CC Connection Controllers
CDF cumulative distribution function
CE Customer Edge
CSPF Constraint based Shortest Path First
CPE Customer Premises Equipment
CUS Customer Application Coordinator
DC Data Center
DP Domain Provider
E2E End to end
ECM Element Control and Management
EF Expedited Forwarding
EvCPE Enterprise vCPE
ETSI European Telecommunications Standards Institute
ETSI EVE ETSI Evolution Working Group
ETSI IFA ETSI Interfaces and Architecture Working Group
ERO Explicit Route Object
EVPN Ethernet VPN
FEC Forward Error Correction
GMPLS Generalized Multi-Protocol Label Switching
GMPLS-UNI GMPLS based User Network Interfaces
GR Group Report
GS Group Specification
GW Gateway
ICM Infrastructure Control and Management
IE Information Element
IETF Internet Engineering Task Force
I-NNI Internal Network to Network Interface

IP Internet Protocol
IX Internet Exchange
ISG Industry Specification Group
E-NNI External Network to Network Interface
ITU-T International Telecommunication Union-Telecommunication Standardization Sector
JGN Japan Gigabit Network
LSP Label Switched Path
MEF Metro Ethernet Forum
MEF-LSO MEF Lifecycle Service Orchestration
MEMS Micro Electro-Mechanical Systems
MPC Multi Party Computation
MPLS Multi-Protocol Label Switching
NC Network Connectivity
NE Network Elements
NFV Network Functions Virtualization
NFVI NFV Infrastructure
NFVI-PoP NFVI-Point of Presence
NFV-MANO NFV Management and Orchestration
NFVO NFV Orchestrator
NIC Network Interface Card
NMS Network Management System
NS Network Service
NSD NS Descriptor
NsDf NS Deployment Flavour
NVGRE Network Virtualization using Generic Routing Encapsulation
OAM Operation, Administration, and Maintenance
OIF Optical Internetworking Forum
OIFUNI OIF based User Network Interfaces
OLSP Optical Label Switched Path
OMS Optical Multiplex Section
ONF Open Networking Foundation
ONUG Open Networking User Group
OP Optical Path
OPS Optical Path Section
OS Operation System
OSPF Open Shortest Path First
OTN Optical Transport Network
OTS Optical Transmission Section
OTU Optical Transport Unit
OSS/BSS Operation Support System/Business Support System
OXC Optical Cross Connect
PC Permanent Connection
PCE Path Computation Element

PE Provider Edge
QoS Quality-of-Service
RD Route Distinguisher
RSVP Resource Reservation Protocol
RSVP-TE RSVP with TE Extensions
RT Route Terget
SCN Signaling Control Network
SDO Standardization Developing Organization
SLA Service Level Agreement
SOF Service Orchestration Functionality
SP Service Provider
SPC Soft Permanent Connection
STM-64 Synchronous Transport Module-64
STP Spanning Tree Protocol
TE Traffic Engineering
ToR Top of Rack
TNA Transport Network Assigned
vAPL virtual Appliance
vCPE virtual Customer Premises Equipment
vRouter virtual Router
VIM Virtualized Infrastructure Managers
VL Virtual Link
VNF Virtualized Network Function
VPN Virtual Private Network
VTEP VXLAN Tunnel End Point
VXLAN Virtual eXtensible LAN
WAN Wide Area Network
WIM WAN Infrastructure Managers

Chapter 1

Introduction

Communication networks are now an essential infrastructure of society. Communication networks consist of various kinds of networks operated by telecommunications operators, content providers, and cloud operators, and various network services (NSs) are constructed across multi-provider networks. Such multi-provider networks are usually configured and operated statically. Dynamic NS control and management across multi-provider networks provides resource utilization and reliability more efficiently. However, there is currently no established method for uniting multi-provider networks dynamically or for assessing their reliability. In this dissertation, a network architecture across multi-provider networks is described (shown in Figure 1.1). Here, NS management is responsible for meeting the service requirements across multi-provider networks and managing the life cycle of services and network instances. Network path control is responsible for controlling the network paths within a provider network. Specifically, the NS management is deployed on a per service basis, and network controllers are deployed on a per network basis. Service requests from users are sent to the NS management, which then selects the network that meets the requirements and notifies the network controller of each provider. The suitable route within the provider network is selected as a result. This dynamic NS control and management mechanism reduces human work load and significantly improve overall work efficiency. Networks constructed across multi-provider networks are expected to be used for in various services, such as automated driving, remote drone control, and remote surgery. The network through which such services flow needs a flexible and reliable network that meets the requirements. In this dissertation, network reliability across multi-provider networks is defined as the connectivity among specific terminals, i.e., the probability of connection among terminals below the Internet Protocol (IP) layer when link failure or packet loss occurs through a stochastic process, as connectivity is a necessary component for NSs to work. As such, network reliability is a fundamental metric of communication networks [1, 2, 3, 4].

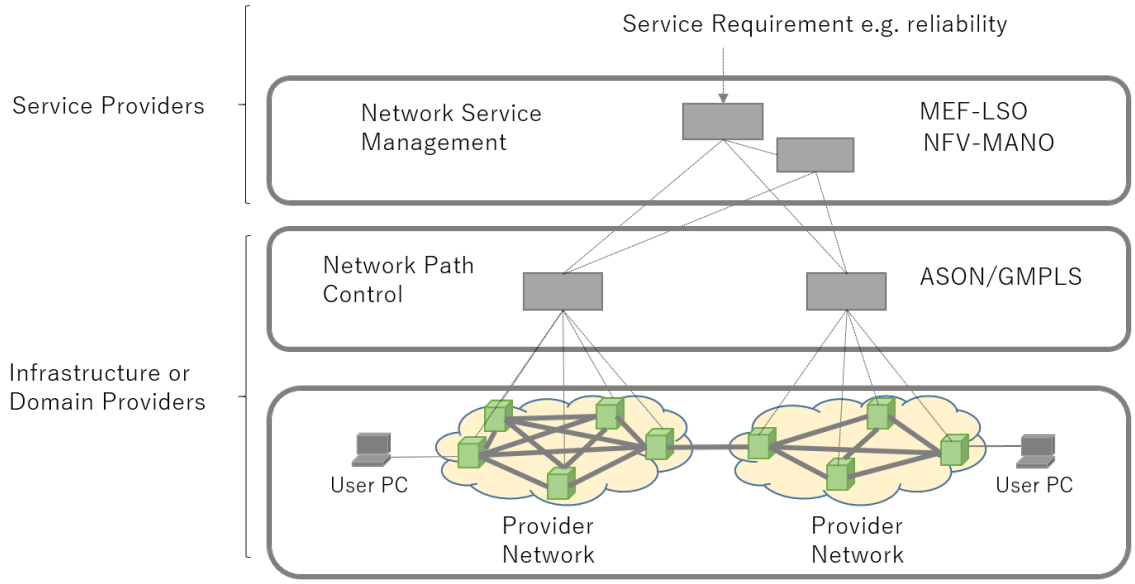


Figure 1.1: Network architecture across multi-provider networks.

1.1 Motivation

This dissertation consists of information regarding Network Service Management and Network Path Control. From the perspective of the NS management, this dissertation focuses on network information exchange among multi-provider networks and network reliability evaluation for network selection. From the perspective of the network path control, this dissertation focuses on feasibility evaluation.

1.1.1 Network Service Management

1.1.1.1 Network Information Exchange

To manage services with appropriate network reliability across multi-provider networks, each provider needs to identify the services across the providers, and know which route the services take among networks. There are two forms of a NS over multi-provider networks: an IP transit model that connects to networks provided by transit providers, and a direct peering model that connects provider networks to each other. The IP transit model enables the existing ETSI NFV Release 2 specifications to be applied without significant changes. However, inquiries about NSs that deploy / modify requests require the allocation of resources from the transit provider, making flexible network changes difficult. In contrast, the direct peering model enables NSs to be provided without affecting the transit provider network. NS deployment across multi-provider networks has also been discussed in the standardization field. The ETSI ISG for NFV proposed the use of multi-domain service orchestration in [5], and the Metro Ethernet Forum (MEF) defined

an architecture of multiple infrastructures in [6]. The 3rd Generation Partnership Project (3GPP) proposed requirements for network slicing in multi-operator scenarios for 5G in [7]. These standardization developing organizations (SDOs) communicate with each other to achieve multiple infrastructure NFV. However, a direct peering model requires a scheme that checks the identifiers showing that each provider manages the service and reflects identifiers that are not used by each provider and are generally available to the service. New schemes need to be built that take security and networking into account. In particular, a new scheme that can handle both models is required for realistic operational scenarios. Additionally, there are the following concerns,

- Overload: The IP transit model can be overloaded due to the native central-control model. Since orchestrators process network information for all providers involved in the deployment ofs, the processing load increases with the size and demand rate of the network.

- Security: If a malicious provider sends unexpected network information, the traffic might be sent to an unexpected route because of the Virtual Private Network (VPN) mechanism. Additionally, the infrastructure provider needs to prevent network information leaking. Thus, a key authentication mechanism is needed to provide the network information to the provider system.

- Location specification: According to the ETSI NFV Release 2 specifications, there are two ways to specify the location of a Virtualized Network Function (VNF): affinity and anti-affinity groups, and location constraints. The affinity and anti-affinity groups show whether two VNFs are placed in the same site (provider) or not, and the location constraints show the geographic location of a VNF. The downside is that this might result in the generation of an L2 network loop overlay.

1.1.1.2 Network Reliability of End-to-End Network

Another critical component to meet service requirements is the selection of an appropriate network, as the network reliability depends on the operation of each network provider. While this problem may seem similar to a traditional reliability evaluation assuming a single-domain network, the existence of multiple domains introduces the following challenges.

- Computation complexity: Reliability evaluation is known to be #P-complete [8, 9]. #P is the complexity class of enumeration problems associated with NP decision problems, and a #P problem must be at least as hard as the corresponding NP problem (for network reliability, the corresponding NP problem is to find *any* single network state connecting the terminals, while the #P problem is to assess *all* connected states). Of course, there is no naive decomposition in #P problems. In the face of this computational difficulty, the recent work of [10, 11, 12] succeeded in computing the reliability for networks with less than 200 links. Unfortunately, multi-domain networks must be larger than single-domain ones, so the computation issue is more

challenging. To reduce the computation burden, sampling approaches like Monte Carlo simulations have been studied [4]. Such approaches, however, provides no guarantee as to the accuracy and could result in large errors [13, 11]. This implies that the significant risk of network unreliability might be overlooked, which would cause terrible disruption in the future. Since reliability evaluation requires counting (enumerating) all network status connecting terminals, it is #P-complete.

- Intra-domain privacy: Domain providers (DPs) remain reluctant to disclose their internal information, e.g., the network topology and the link availabilities, because such disclosure might enable their competitors to learn their business strategies or attackers to find vulnerabilities. To my knowledge, no prior work has investigated this issue in the context of network reliability. [14, 15] proposed a cost minimization method for multi-domain networks that utilizes secure multi-party computation to keep internal information private. This method was designed for NP problems that can be efficiently solved by pruning the search space, but it cannot be applied to this dissertation's #P problem as I have to examine the whole search space in a unitary manner.

1.1.2 Network Path Control

1.1.2.1 Feasibility of Dynamic Network Control Scenarios across Multi-provider Networks

A feasibility evaluation is required to clarify the requirements for network path control scenarios. While IP level switching is simple, it is inefficient because it requires a physical connection in advance. Automatically Switched Optical Network (ASON) and Generalized MPLS (GMPLS) control-plane technologies are an effective solution to comply with such requirements because they enables the provisioning of lambda-based LSPs by controlling Optical Cross Connects (OXCs). In the case of a resource modification, which is one of my use cases, a change in a connectivity service's traffic volume is assumed to be in the unit of several hours. Therefore, network deployment or modifications require switching time within minutes without affecting existing services.

1.2 Related Work

This section consists of related studies and standardization.

1.2.1 Related Studies

In this section, related studies are summarized in the Network Information Exchange and Network Reliability evaluations described in the previous section respectively.

1.2.1.1 Network Information Exchange

NS deployment across multi-provider networks has been extensively studied in academia. The virtual network embedding problem, with constraints on both virtual nodes and virtual links, is known to be NP-hard. and virtual network embedding across multi-domain networks need to be provisioned across heterogeneous administrative domains managed by multiple infrastructure providers. The centralized heuristic resource allocation algorithm was proposed for allocating virtual networks involving multiple infrastructure providers [16, 17, 18]. Reference [19] proposed a centralized resource discovery mechanism for virtual network embedding across multiple providers. Reference [20] proposed the abstraction of physical resources of a domain to re-use existing embedding algorithms with minor modifications. While a centralized approach is effective in efficiently calculating resource allocation and obtaining an abstract view, the role and responsibilities to manage the centralized management are vague. Reference [21] exchanges provider resource policy information and allocates virtual resources through consensus-based auctions. Reference [22] exchanges network policy and location constraint information among providers to allocate virtual resources on the basis of policy. These previous works focused on resource allocation of virtualized resources. Reference [23] exchanges only virtual node types and associated costs between operators for virtual resource allocation. Reference [14, 15] also proposed a secure computation technique for exchanging resource information and prices among multiple providers. Therefore, given a real network, a mechanism is needed to exchange information between providers to allocate network resources. However, no work addresses practical aspects, e.g., [15] defines a protocol for NS deployment across multi-provider networks, but it does not consider interoperability with existing systems.

1.2.1.2 Network Reliability Evaluation of End-to-End Network

No work has investigated the intra-domain privacy issue in the context of network reliability evaluation. Several methods to compute network reliability have been proposed including sum-of-disjoint products [24], factoring theorem [25], decomposition method [26], and binary decision diagrams [27, 10, 11, 12]. They compute the exact reliability without partitioning the problem. No work has succeeded in computing the reliability of real networks with more than 200 links. Sampling approaches like Monte Carlo simulations [4] scale well, but the solution can deviate significantly [13, 11]. Reference [28] proposes F-Monte Carlo; it estimates the probability of rare events accurately, but it depends on the unrealistic assumption that all links would fail with *equal* probability. The most critical issue of this approach is that no guarantee is given as to solution accuracy. Non-guaranteed reliability could cause unexpected disruption of the key social infrastructure. The privacy issue has not been studied in the long history of network reliability. This will be a key issue in the future of network services, because multi-domain services have been recently discussed in the standardization bodies [6, 30]. Minimum-cost networks can be constructed securing intra-domain privacy [14, 15], but the reliability has not been studied.

1.2.1.3 Feasibility of Dynamic Network Control Scenarios across Multi-provider Networks

There are several studies that focus on achieving QoS recovery of IP traffic flows while optimizing network resource usage in ASON/GMPLS-based networks [31, 32]. In these studies, TE control is achieved by a Network Management System (NMS) or a centralized Path Computation Element (PCE), which gathers network topology information from all NEs and exchanges a portion of information with peer domains. Also, the NMS and the centralized PCE can be used as network planning and provisioning tools to initiate transport services. In this architecture, LSPs are controlled dynamically by monitoring the amount of the traffic at each monitoring point. Furthermore, a traffic monitoring server collects the traffic information, projects a traffic matrix among monitoring points, and feeds back the suggested operation to the NMS or the centralized PCE. Murayama et al. [31] proposed an optical VPN architecture based on centralized LSP traffic monitoring and an LSP routing scheme. Also, Nakahira et al. [32] reported the effectiveness of the routing of LSPs using centralized routing and NMS. The centralized scheme has global visibility of the network state and may potentially produce more optimal solutions. On the other hand, In the case of multi-provider networks, each provider must have a centralized scheme with capability to communicate with each other to exchange network information. Additionally, the role and responsibilities for managing network resources between provider networks are vague. I proposed the operational evaluation of ASON/GMPLS inter-domain capability over field network [1, 2]. Following our work, several papers have researched and standardized on automation technology for multi-provider networks by using PCE. [35].

1.2.2 Related Standards

The related standards consist of ETSI ISG NFV and MEF related to NS management across multi-provider networks, and ASON / GMPLS related to network path control of NSs across multi-provider networks.

1.2.2.1 ETSI ISG NFV

The ETSI defines an NFV reference architectural framework to manage Virtualized Network Functions (VNFs) [36]. Figure 1.2 shows the NFV reference architectural framework defined by ETSI ISG NFV. The framework consists of four function blocks: the VNF, the NFV Infrastructure (NFVI), the NFV-Management and Orchestration (MANO), and the Operation Support System/Business Support System (OSS/BSS). The VNF is an implementation of a network function. The NFVI includes virtual and hardware resources such as computation, networking, and storage; VNFs are deployed on the NFVI. The NFV-MANO manages these function blocks, which consists of the NFVO, the VNF Manager (VNFM), and the Virtualized Infrastructure Manager (VIM). The OSS/BSS coordinates the NFV framework with legacy networks. The NFVO provides an NFV NS with VNFs. The VNFM manages the VNF instances. The VIMs allocate resources on the NFVI. Figure 1.3 shows an example of an NFVI network across multiple DP administrative

domains [37, 38]. There are two ways to provide the NS across multi-provider networks. Figure 1.3 (a) shows how to unite the network resources of multi-provider networks. The VIM corresponding to the domain manages the NFVI in the domain, and the NFVO guarantees the network connection between the domains. The NFVO can manage the NS with a single VNFM across multi-provider networks. In this case, although the NFVO can control the life cycle and policy management of NSs, it manages only abstracted network information, so it can not obtain detailed network information from the domain.

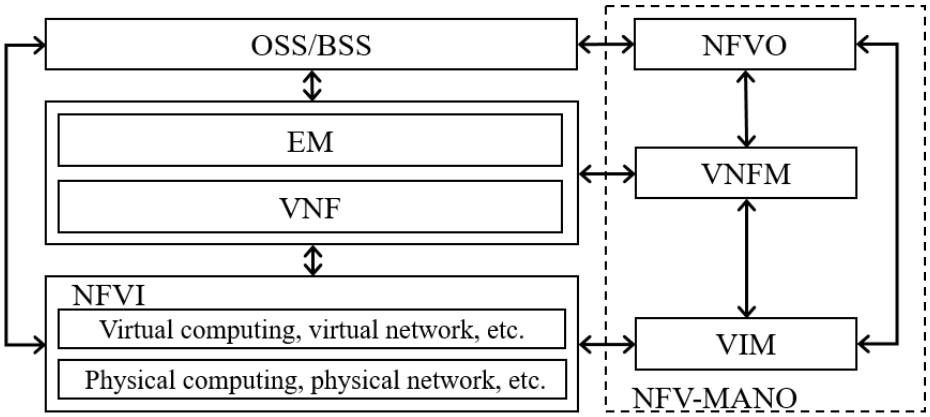


Figure 1.2: NFV reference architectural framework.

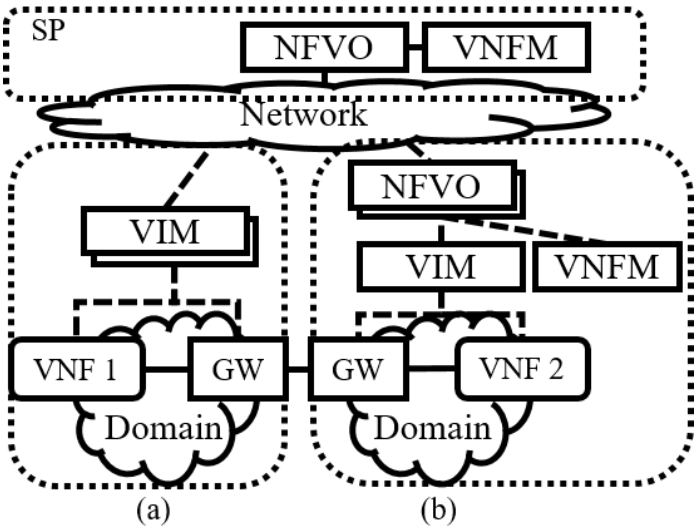


Figure 1.3: NS across multi-provider networks.

This subsection considers two types of players: Domain Providers (DPs) and Service Providers (SPs). DPs manage their own domains and evaluate the reliability of their own domains. A SP provides a NS across the domains and so must compute reliability as a whole. Figure 1.3 (b) shows how to nest the NSs of multi-domain networks. The

NFVO corresponding to the domain provides the NSs at each domain, and the SP's NFVO guarantees the network connection between the domains. This NFVO can manage the nested NS across multi-domain networks. Similar to (a), the NFVO cannot obtain detailed network information from the domain.

In the case of a NFV service among multiple managed domains through a Wide Area Network (WAN) as in Fig 1.3 (a), the NFVO has difficulty in sorting and selecting the required information because the configuration information is located in geographically separated domains that are managed by multiple infrastructure providers. Although the ETSI NFV has standardized a number of function blocks and the interface between blocks, if the placement of the configuration information is under specified, the interface of the blocks would not be decided. I, working with other ETSI NFV members, have compiled a standard report on the requirements for building NSs across multi-site and multi-provider networks as a new feature of the ETSI NFV Release 3 specification [37]. ETSI ISG NFV agreed to adopt the feature of the ETSI GR NFV-IFA022 report as the ETSI NFV Release 3 specifications, has finalized the data model specifications, and is currently working on protocol level specifications [39].

1.2.2.2 MEF

The MEF also defines the Lifecycle Service Orchestration (LSO) architecture. Figure 1.4 shows the MEF-LSO reference architecture defined by MEF. The framework consists of five components: the Customer Application Coordinator (CUS), Business Applications (BUS), Service Orchestration Functionality (SOF), Infrastructure Control and Management (ICM), and Element Control and Management (ECM). The CUS is a functional management entity in the customer domain. The BUS is an SP functionality supporting the business management layer functionality. The SOF is the set of service management and policy-based management functionalities. The ICM is the set of functionalities providing domain-specific network and topology view resource management capabilities. The ICM includes the functionality of ETSI NFV-MANO. The MEF-LSO model is a distributed model. Figure 1.5 shows an example of a network architecture over DP's administrative domains [6]. The CUS controls the SOF corresponding to each domain, and provides slices across domains by exchanging information between the SOFs of each domain. The CUS communicates with the ICM corresponding to each domain to control policy information. The CUS can send policy information to the SOF, but can not obtain detailed network information from ICM or ECM. However, The MEF has not defined MEF-LSO interface specification in detail, as the interface specification follows that of other SDOs.

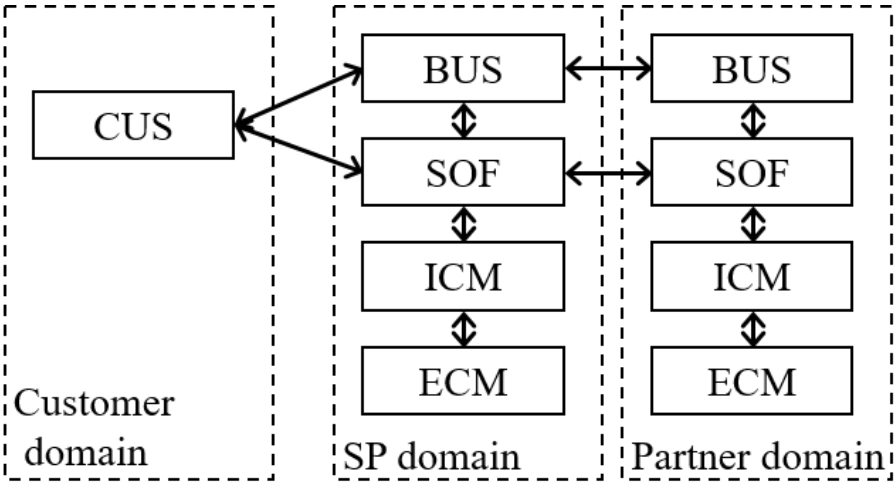


Figure 1.4: MEF-LSO Reference architecture.

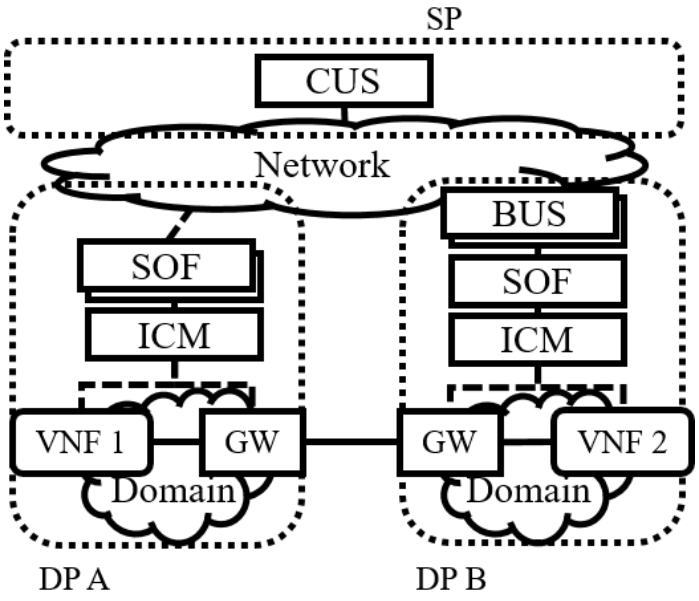


Figure 1.5: Network architecture for NS deployment across multi-provider networks managed by MEF.

1.2.2.3 ASON/GMPLS

Figure 1.6 shows termination points in optical layer network management of Type-B OXCs. The OC192/ synchronous transport module-64 (STM64) of client data is managed as an Optical Path (OP) inside the Optical Transport Network (OTN) management network. Forward Error Correction (FEC), which is added to the Optical Transport Unit (OTU) frame, provides supervisory functions to transport client data between optical channel

termination points. The OTU overhead is inserted at the termination point of every Optical Multiplex Section (OMS), which comprises a single or multiple Optical Transmission Section(s) (OTS) [40]. In the pre-OTN section, the OXCs manage the section trail without assigning a specific wavelength and define the OPS0 (Optical Path Section [OPS]) layer [41]. The Optical Cross Connect (OXC) that terminates both the OTN and pre-OTN sections converts particular alarm indication signals between the OPS0 and OMS/OTS layers to achieve seamless Operation, Administration, and Maintenance (OAM) between these sections.

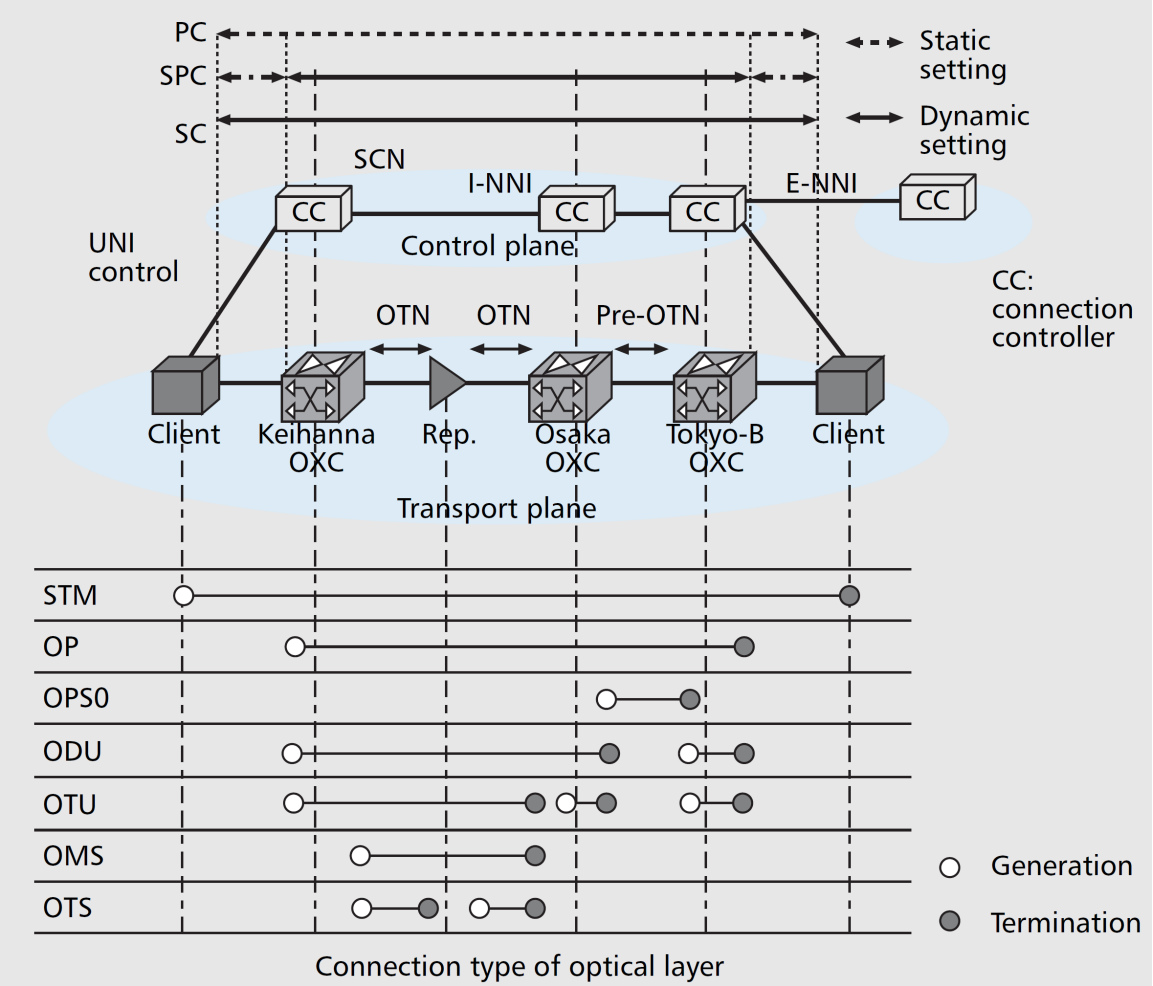


Figure 1.6: Optical layer management and ASON architecture for type B OXCs.

Figure 1.6 also outlines the ASON architecture constructed over the OXC system. The architecture and requirements of ASON are described in International Telecommunication Union- Telecommunication Standardization Sector (ITU-T) G.8080 [42]. The control plane consists of Connection Controllers (CCs) and a Signaling Control Network (SCN) to enable CCs to communicate with each other. The ASON architecture specifies three kinds of reference points, namely, Internal Network to Network Interface (I-NNI), External Network to Network Interface (E-NNI), and UNI in the SCN. On the other hand, the ITU-T

G.8080 architecture defines three types of paths. The first one is a Permanent Connection (PC). The PC path is established by statically setting each OXC. The second one is a Soft Permanent Connection (SPC). The SPC path is established by incorporating static and dynamic settings of the OXC and consists of the PC path between the OXC and client Network Elements (NEs) and a switched connection (SC) path between the edge OXCs. The third path is the SC. The SC path is established by a dynamic setting using the control-plane signaling, which is triggered by client NEs. The static PC path is used in cases where autonomous control is not required., or the network operators want to preserve network resources for static service requests from their customers. On the other hand, dynamic SPC paths and SC paths are used in cases where a client or operator wants to set the end-to-end path easily. This easy path setting can significantly reduce not only the operational burdens such as the accommodation design of the path, but also perform various types of recovery schemes.

1.3 Contributions

In this dissertation, I analyzed four operational use cases by using NSs across amulti-provider network. The use case analysis has revealed three requirements for controlling NSs across a multi-provider network.

1.3.1 Use Case Proposal for Standardization

To achieve the use case of using an NS across a multi-provider network, the interfaces connecting the provider networks need to be standardized. To that end, in this dissertation, I propose a use case to reach agreements with other operators and vendors on the needs of the use cases and the functional requirements to realize the cases. Use case analysis revealed three requirements: (1) Network information exchange for exchanging necessary resource information between multiple providers (2) A network evaluation method for selecting an appropriate network that meets service requirements, and (3) network path control for updating the connectivity among multi-provider networks. My proposal was adopted for standardization by clarifying use cases that could only be achieved by exchanging information among providers.

1.3.2 Network Information Exchange Scheme

The realization of NSs over multi-provider networks has practical issues (e.g., overload, security, location specification). In the dissertation, I propose a protocol extension to implement the proposed scheme, and evaluated aspects related to the proposed scheme from a practical perspective. Experiments with Ethernet VPN (EVPN) connections through multi-providers have clarified the parameters exchanged by the protocol. This dissertation thoroughly discusses the multi-provider NS deployment from several aspects, unlike the past academic work. My proposed idea was adopted as a new feature of the ETSI NFV

Release 3 specifications. I gave a presentation of my proposed scheme at the International Conference on Network and Service Management (CNSM) 2015 [3].

1.3.3 Network Reliability Evaluation

In this dissertation, I propose a method to partition the network size so as to yield upper and lower bounds of reliability. Each DP computes the reliability of its own domain, and the SP then unifies the results to yield the bounds for the whole network. My contributions are summarized as follows. Since there was no mechanism for secure information exchange scheme among providers, the proposed method contributed to a theory, protocols, and experiments.

- Theory: My rigorous theory enables for an effective partition. The partition reduces the problem size to decrease computation complexity. Additionally, the partition guarantees that no intra-domain information is disclosed. The theory utilizes the graph contraction technique to yield upper and lower bounds of reliability. It is worth noting that the bounds of my method have a clear advantage over the sampling approach that has no error bounds [4]; if the network is unreliable, the user will become aware of this by the *small* lower bound; alternatively, if the lower bound is high, it means that the network is confirmed to be sufficiently reliable.

- Protocol: I have defined a primitive protocol between the SP and DPs. DPs can compute the reliability of their domains without revealing their internal data. The computed reliabilities are processed by the SP using secure computation techniques. Several practical issues including inter-domain connections are also addressed.

- Experiments: My method was numerically evaluated using several real networks. While the recent work of [10, 11, 12] could deal only with networks having fewer than 200 links, my method could successfully evaluate the reliability of 14 domains with 907 links. The bound gaps are reasonably small.

This content was accepted for publication by the Institute of Electronics, Information and Communication Engineers (IEICE) Transactions on Communications and will appear in 2020 [10].

1.3.4 Feasibility Evaluation for Network Path Control

A standardization method was proposed to control network paths across multi-provider networks, but it did not evaluate actual switching times. In this dissertation, I implemented the mechanisms proposed in the standardization method and evaluated them experimentally to verify that the switching time was suitable for the use case. I conducted a field evaluation of the dynamic path control across multi-provider networks. The focus was inter-domain network path creation, QoS recovery for protecting high-priority traffic transmitted over OIF-UNI using policy controllers, and a failure recovery of LSPs established over E-NNI. Routing problems that arose in the multi-domain network were successfully solved and the

actual service activation time of inter-domain Ethernet transport services was evaluated. The QoS recovery successfully achieved the migration of high-priority video traffic with no errors from the MPLS-LSP to the cut-through Optical Label Switching Path (OLSP) and vice versa over the Japan Gigabit Network (JGN) Ⅱ network testbed within about around 30 seconds. There was no packet loss for high-priority traffic flow when migrating traffic between MPLS-LSP and optical LSPs. The link failure recovery was also confirmed by using hierarchical LSP over the network testbed without the outflow of any control packets to an outside domain. This content was presented at the European Conference on Optical Communication (ECOC) 2007 [1] and published in the IEEE Communication Magazine [2].

1.4 Outline

This dissertation consists of six chapters, shown in Figure 1.7. Chapter 2 describes my proposed use cases for coordinated control of cloud and WAN. The content is taken from my proposed use cases to the ETSI NFV report for discussing features of ETSI NFV Release 3 specifications [37]. Chapter 3 describes my proposed network information exchange scheme to achieve interoperability among the NS management systems of multiple operators, which enables scalable management while maintaining privacy within the domain. Chapter 4 describes my proposed method that efficiently computes the reliability of muti-domain networks without compromising intra-domain privacy. Chapter 5 describes the results of a feasibility evaluation of inter-domain transport path creation, intra-domain cut-through migration, and failure recovery at a field testbed. Chapter 6 summarizes the dissertation and discusses future directions of research.

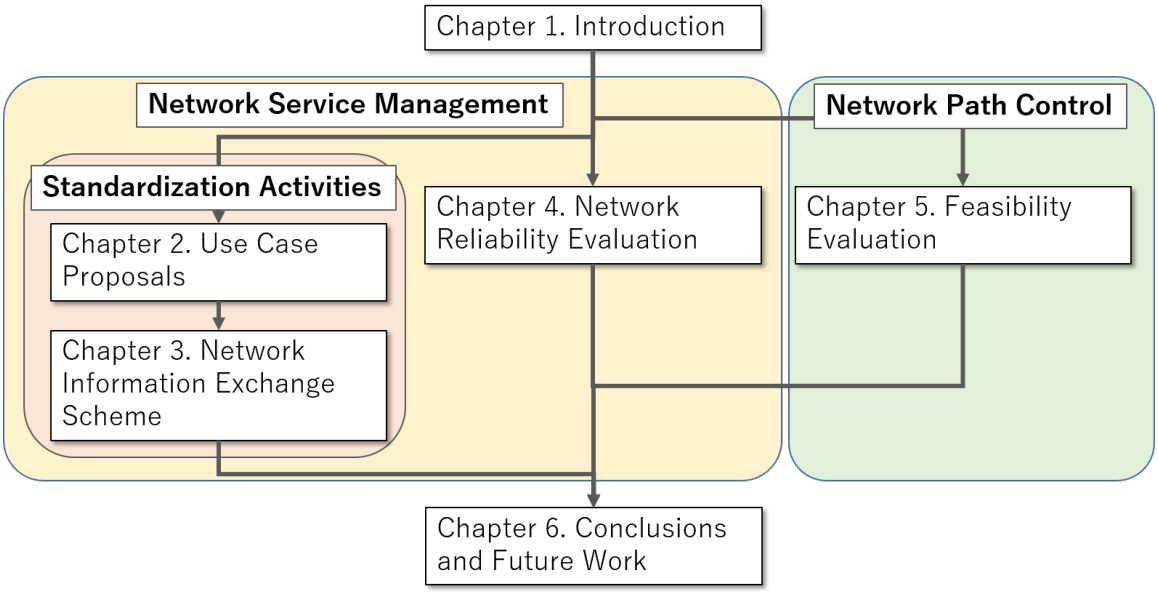


Figure 1.7: Chapter structure.

Chapter 2

Use Case Proposal for Standardization

This section describes use cases for NSs across multi-provider networks. NFV use cases are summarized in ETSI NFV [5]. NFV technologies enable flexible evolution of the home environment by reducing hardware-specific functionality with minimal cost and improved time to market, and new services can be introduced as required on a grow-as-you-need basis. The benefits derived from avoiding installation of new equipment would be amplified if the evolution of the home environment is considered with the appropriate NFV approach. By using virtual technology, the required customer premises equipment (CPE) functionality is provided by a specific provider through a multi-provider network. However, the current network and cloud services are managed individually by each provider, and the network configuration cannot be flexibly changed. As a result, the service takes longer and cannot properly handle the load on resources. Thus, I proposed four use cases to ETSI NFV that enable flexible configuration changes among their provider networks. Section 2.1 shows a basic use case of an NS across multi-site networks. Section 2.2 shows a modification to the WAN connectivity resource of a multi-site NS. Section 2.3 shows an NS for E2E enterprise vCPE (EvCPE) across two WANs. Section 2.4 shows an NS expansion to other NFVI-Point of Presences (PoPs) over WAN.

2.1 Basic Use Case of NS across Multi-site Networks

2.1.1 Introduction

This use case is discussed in the context of the EvCPE NS orchestration. As shown in Figure 2.1, the overall model focuses on two NFVI-PoPs located at two different sites connected over a shared WAN infrastructure (e.g. IP/ MPLS, optical network, etc.). A NS consisting of two VNFs is instantiated as shown in Figure 2.1. Each VNF comes from one of two groups of VNFs, namely virtual CPE (vCPE) and virtual Appliance (vAPL). Each group is installed in a different site, and the VNFs of the NS are connected across the WAN infrastructure.

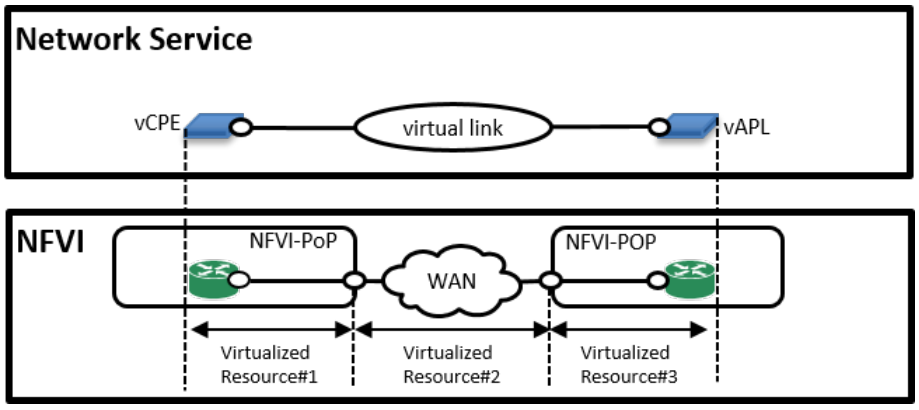


Figure 2.1: Connectivity overview for enabling NS.

The virtualized network resources for Site#1, for WAN, and for Site#2 are referred to as virtualized network resource#1, #2 and #3, respectively. The virtualized network resources assigned to the vCPE and vAPL VNFs are terminated at virtual network ports which are attached to the WAN infrastructure. As a result, a unified VL is created by combining the virtualized network resource#1, #2 and #3.

Base operational flows for deploying NSs across the two sites are examined. VNFs are deployed in each of two sites, Site#1 and Site#2 and network connectivity is configured between those sites. The VNF deployments at each site and the network connectivity between the two sites should be coordinated in such a way as to deliver a unified service. The VNFs at each site will be connected across the WAN. The connectivity of VNFs over the WAN can be performed:

(a) through gateways at each site that translate/map between the in-site and WAN virtual networks; or

(b) as an overlay network using tunnelling protocols (see clause 5.2.4.2.1 in ETSI GS NFV-EVE 005 [45]).

Examples of tunneling ling protocols typically used in data centers include Virtual eXtensible LAN (VXLAN) and Network Virtualization using Generic Routing Encapsulation (NVGRE). Tunneling protocols offer the ability to stack/aggregate different customer private networks across a provider network. Two base operational flows, namely BF#1.1 and BF#1.2, corresponds to connectivity approach a), and one base operational flow, namely BF#1.3 corresponds to connectivity approach b). These are described below. Figure 2.2 provides a more detailed view of the use case. The architectural model is derived from Figure 5.2 in [46]. It shows a multi-site model managed by a single Service Provider. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are further referred in the present use case.

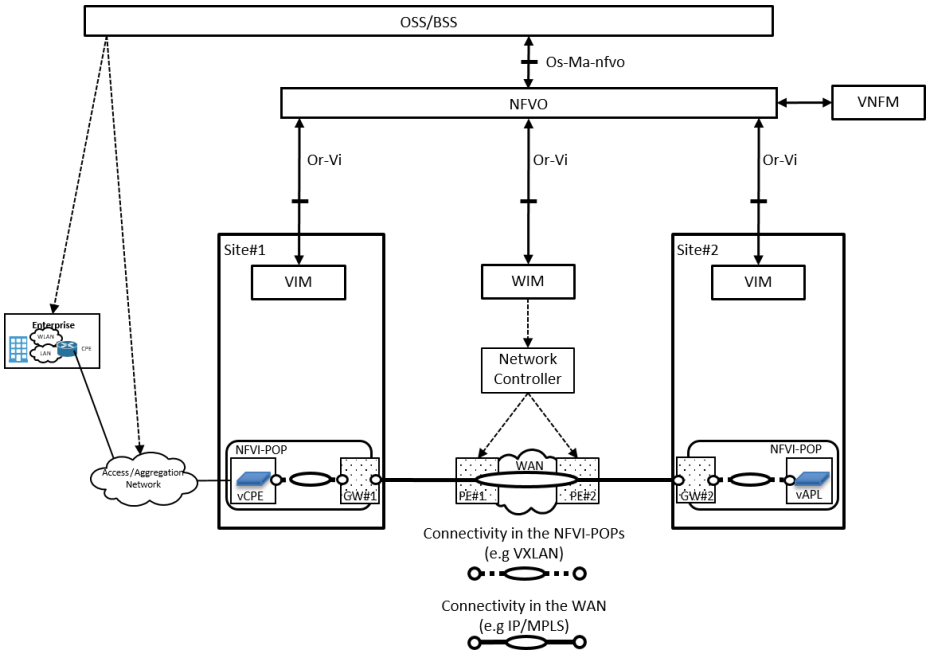


Figure 2.2: High-level view of the EvCPE service across WAN.

2.1.2 Trigger

Table 2.1 describes the use case trigger.

Table 2.1: NS for E2E Enterprise vCPE trigger base flow #1.

Trigger	Description
BF#1.1, BF#1.2 and BF#1.3	The OSS requests the NFVO to instantiate a NS with a VNF in Site#1 and another in Site#2, with these VNFs connected by a virtual link.

2.1.3 Actors and Roles

Table 2.2 describes the use case actors and roles.

Table 2.2: NS for E2E Enterprise vCPE actors and roles.

#	Actor
1	OSS/BSS
2	NFVO
3	VIM
4	Network Controller
5	WIM

2.1.4 Pre-conditions

Table 2.3 describes the pre-conditions.

Table 2.3: NS for E2E Enterprise vCPE Pre-conditions.

#	Pre-condition
1	The network between the enterprise site and Site#1 shown in Figure 2.2 works properly according to the Service Level Agreement (SLA)
2	The infrastructure of the NFVI-PoP at Site#1 and Site#2 and the network infrastructure of the WAN are also physically connected.

2.1.5 Post-conditions

Table 2.4 describes the post-conditions for base flow #1 (i.e. BF#1.1, BF#1.2 and BF#1.3).

Table 2.4: NS for Enterprise vCPE post-conditions for base flow #1.

#	Post-condition
1	An EvCPE service is installed with VNF is two sites. The vCPE is in one site and the vAPL is in another site. The virtual link between the VNF is supported across a WAN

2.1.6 Operational Flows

Table 2.5 and Table 2.5 describe the base flow #1.1 (BF#1.1) and the base flow #1.2 (BF#1.2), respectively for the approach of translating/mapping in between in-site and WAN virtual networks (see section 2.1). The BF#1.1 shows the approach of translating/ mapping between in-site and in-WAN virtual networks based on information provided by WIMs. The BF#1.2 shows the approach of translating/mapping between in-site and in-WAN virtual networks based on information provided by VIMs.

Table 2.5: NS for E2E Enterprise vCPE base flow #1.1.

#	Flow	Description
1	OSS/BSS → NFVO	Requests to instantiate a NS across Site#1 and Site#2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-nfvo*

Continued on next page.

#	Flow	Description
2	NFVO	Starts an instantiation process for the vCPE and vAPL VNFs with the VNFM(s). The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. Then the NFVO decides the location where to instantiate the vCPE and vAPL VNFs and decides to setup network connectivity between two sites across the WAN through gateways at each site translating/mapping in between in-site and WAN virtual networks.
3	NFVO → WIM	Requests to allocate virtualized resource#2 between NFVI-PoPs at Site#1 and at Site#2 with a designated bandwidth. *Interface - Or-Vi*
4	WIM → Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated bandwidth between Site#1 and Site#2. Interface - e.g. NBI for Network controllers .
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated bandwidth. The IP/MPLS path configurations are, for example, installed into gateways, PE#1, PE#2 and other provider routers in the WAN infrastructure. There are multiple options where the end points for the VNFs are installed, as discussed in ETSI GS NFV-INF 005 [47] (e.g. vSwitch, Network Interface Card (NIC), Top of Rack (ToR), virtual Router (vRouter), etc.).
6	Network Controller → WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address, VXLAN ID, and MPLS-VPN Route Distinguisher (RD) are returned.
7	WIM → NFVO	Returns the response to the virtualized resource allocation request between NFVI-PoPs at Site#1 and at Site#2. In this context, the resource identifier, which is used for identifying the virtualized resource at the WIM, and information for connecting to the WAN (e.g. IP address and VXLAN ID, and MPLS-VPN RD) are returned. *Interface - Or-Vi*
8	NFVO → VIM at Site#1	Requests to allocate the virtualized resource#1 connecting to the WAN. The NFVO sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note. *Interface - Or-Vi*
9	VIM at Site#1	Allocates the virtualized resource for connecting to the WAN at Site#1. See note.
10	VIM at Site#1 → NFVO	Returns the response for allocating the virtualized resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualized resource at the VIM. See note. *Interface - Or-Vi*

Continued on next page.

#	Flow	Description
11	NFVO → VIM at Site#2	Requests to allocate the virtualized resource#3 connecting to the WAN. The NFVO sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note. *Interface - Or-Vi*
12	VIM at Site#2	Allocates the virtualized resource connecting to WAN. See note.
13	VIM at Site#2 → NFVO	Returns the response to the request for allocating the virtualized resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualized resource at the VIM. See note. *Interface - Or-Vi*
14	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s).
15	NFVO → OSS/BSS	Returns the results of NS instantiation request.
NOTE: The set of steps 8, 9 and 10 and set of steps 11, 12, 13 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2.		

Finished.

Table 2.6: NS for E2E Enterprise vCPE base flow #1.2.

#	Flow	Description
1	OSS/BSS → NFVO	Requests to instantiate a NS across Site#1 and Site#2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-Nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL VNFs with the VNFM(s). The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. Then the NFVO decides the location where to instantiate the vCPE and vAPL VNFs and decides to setup network connectivity between two sites across the WAN through gateways at each site translating/mapping in between in-site and WAN virtual networks.
3	NFVO → WIM	Requests to allocate virtualized network resource#2 between NFVI-PoPs at Site#1 and at Site#2 with a designated bandwidth. *Interface - Or-Vi*

Continued on next page.

#	Flow	Description
4	WIM → Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated bandwidth between Site#1 and Site#2. Interface - e.g. NBI for Network controllers
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated bandwidth. The IP/MPLS path configurations are, for example, installed into gateways, PE#1, PE#2 and other provider routers in the WAN infrastructure.
6	Network Controller → WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address) are returned.
7	WIM → NFVO	Returns the response to the virtualized resource allocation request between NFVI-PoPs at Site#1 and at Site#2. In this context, the resource identifier, which is used for identifying the virtualized network resource at the WIM and the information for connecting to the WAN are returned. *Interface - Or-Vi*
8	NFVO → VIM at Site#1	Requests to allocate the virtualized resource#1 at Site#1. See note 1. *Interface - Or-Vi*
9	VIM at Site#1	Allocates the virtualized resource#1. See note 1.
10	VIM at Site#1 → NFVO	Returns the response for allocating the virtualized resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualized resource#1 and the information for connecting to the NFVI-PoP at Site#1 (e.g. IP address, VXLAN ID, and MPLS-VPN RD). See note 1. *Interface - Or-Vi*
11	NFVO → VIM at Site#2	Requests to allocate the virtualized resource#3 at Site#2. See note 1. *Interface - Or-Vi*
12	VIM at Site#2	Allocates the virtualized resource#3. See note 1.
13	VIM at Site#2 → NFVO	Returns the response for allocating the virtualized resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualized resource#3 and the information for connecting to the NFVI-PoP at Site#2 (e.g. IP address, VXLAN ID, and MPLS-VPN RD). See note 1. *Interface - Or-Vi*

Continued on next page.

#	Flow	Description
14	NFVO → WIM	Requests to update the virtualized network resource#2 at the WAN. The NFVO sends the information for connecting to the endpoints of the site#1 and site#2 for the interconnection between the two sites which is obtained in step 10 and 13. See note 2. *Interface - Or-Vi*
15	WIM → Network Controller	Request to configure the provider edge (PE) node#1 and PE node#2 at WAN. See note 2. *Interface - e.g. NBI for Network controllers.*
16	Network Controller	Configures the PE node#1 and PE node#2 at WAN. See note 2.
17	Network Controller → WIM	Returns the response for configuring the PE node#1 and PE node#2 at WAN. See note 2.
18	WIM → NFVO	Returns the response for updating the virtualized network resource#2. See note 2.
19	NFVO → VIM at Site#1	Requests to update the virtualized network resource#1 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#2 for the interconnection between the two sites which is obtained in step 13. See note 2. *Interface - Or-Vi*
20	VIM at Site#1	Configures the virtualized network resource#1. See note 2.
21	VIM at Site#1 → NFVO	Returns the response for updating the virtualized network resource#1. See note 2. *Interface - Or-Vi*
22	NFVO → VIM at Site#2	Requests to update the virtualized network resource#3 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#1 for the interconnection between the two sites which is obtained in step 10. See note 2. *Interface - Or-Vi*
23	VIM at Site#2	Configures the virtualized network resource#3. See note 2.
24	VIM at Site#2 → NFVO	Returns the response for updating the virtualized network resource#3. See note 2. *Interface - Or-Vi*
25	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s).
26	NFVO → OSS/BSS	Returns the results of NS instantiation request.

Continued on next page.

#	Flow	Description
NOTE 1: The set of steps 8, 9 and 10 and set of steps 11, 12, 13 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2. NOTE 2: The set of steps from 14 to 18, set of steps from 19 to 21 and set of steps from 22 to 24 can be executed sequentially or in parallel. That is, the procedures to configure the virtualized network resource#1, virtualized network resource#2 and the virtualized network resource#3 can be executed in parallel.		

Finished.

Table 2.3 describes the base flow #1.3 (BF#1.3) for the approach of tunneling in-site virtual networks in WAN virtual networks. The flow includes all necessary steps on setting up the connectivity assuming the case that only physical connectivity has been established (see pre-condition #2 in Table 2.3).

Table 2.7: NS for E2E Enterprise vCPE base flow #1.3.

#	Flow	Description
1	OSS/BSS → NFVO	Requests to instantiate a NS across Site#1 and Site#2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL VNFs with the VNFM(s). The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. Then the NFVO decides the location where to instantiate the vCPE and vAPL VNFs and decides to establish an interconnection between the two sites as an overlay network using tunnelling protocols. In this case, the NFVO coordinates the resources commonly used between the two sites (e.g. VXLAN Network Identifier for VXLAN, Tenant Network ID for NVGRE, VLAN ID in the C-Tag of IEEE 802.1ad [48], etc.). This coordination process can involve interaction with VIMs on the two sites to check the availability of the common resources, get information about them, and reserve them. *Interface - Or-Vi*
3	NFVO → WIM	Requests to allocate virtualized resource#2 between NFVI-PoPs at Site#1 and at Site#2 with a designated bandwidth. *Interface - Or-Vi*
4	WIM → Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated bandwidth between Site#1 and Site#2. *Interface - e.g. NBI for Network controllers* .

Continued on next page.

#	Flow	Description
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated bandwidth. The IP/MPLS path configurations are, for example, installed into gateways, PE#1, PE#2 and other provider routers in the WAN infrastructure. There are multiple options where the end points for the VNFs are installed, as discussed in ETSI GS NFV-INF 005 [47] (e.g. vSwitch, NIC, ToR, vRouter, etc.).
6	Network Controller → WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address, VLAN ID in the S-Tag of IEEE 802.1ad [48], and MPLS VPN RD) are returned.
7	WIM → NFVO	Returns the response to the virtualized resource allocation request between NFVI-PoPs at Site#1 and at Site#2. In this context, the resource identifier, which is used for identifying the virtualized resource at the WIM, and information for connecting to the WAN (e.g. IP address, VLAN ID in the S-Tag of IEEE 802.1ad [48], and MPLS-VPN RD) are returned. *Interface - Or-Vi*
8	NFVO → VIM at Site#1	Requests to allocate the virtualized resource#1 for the interconnection between the two sites. The NFVO sends information on the common resources for the interconnection between the two sites which are obtained in step 2. The NFVO also sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note 1. *Interface - Or-Vi*
9	VIM at Site#1	Allocates the virtualized resource#1 based on the information provided in step 8. See note 1.
10	VIM at Site#1 → NFVO	Returns the response to the request for allocating the virtualized resource#1 for the interconnection between the two sites. The VIM returns the information for connecting to the endpoint at the Site#1 (e.g. the address of VXLAN Tunnel End Point (VTEP) for VXLAN or the router supporting NVGRE). See note 1. *Interface - Or-Vi*
11	NFVO → VIM at Site#2	Requests to allocate the virtualized resource#3 for the interconnection between the two sites. The NFVO sends information on the common resources for the interconnection between the two sites which are obtained in step 2. The NFVO also sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note 1. *Interface - Or-Vi*
12	VIM at Site#2	Allocates the virtualized resource#3 based on the information provided in step 11. See note 1.

Continued on next page.

#	Flow	Description
13	VIM at Site#2 → NFVO	Returns the response to the request for allocating the virtualized resource#3 for the interconnection between the two sites. The VIM returns the information for connecting to the endpoint at the Site#2 (e.g. the address of VTEP for VXLAN or the router supporting NVGRE) is returned. See note 1. *Interface - Or-Vi*
14	NFVO → VIM at Site#1	NFVO requests to configure the virtualized resource#1 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#2 for the interconnection between the two sites which is obtained in step 13. See note 2. *Interface - Or-Vi*
15	VIM at Site#1	Configures the virtualized resource#1. See note 2.
16	VIM at Site#1 → NFVO	Returns the response to the request for configuring the virtualized resource#1. See note 2. *Interface - Or-Vi*
17	NFVO → VIM at Site#2	NFVO requests to configure the virtualized resource#3 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#1 for the interconnection between the two sites which is obtained in step 10. See note 2. *Interface - Or-Vi*
18	VIM at Site#2	Configures the virtualized resource#3. See note 2.
19	VIM at Site#2 → NFVO	Returns the response to the request for configuring the virtualized resource#3. See note 2. *Interface - Or-Vi*
20	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s).
21	NFVO → OSS/BSS	Returns the results of NS instantiation request.
NOTE 1: The set of steps 8, 9 and 10 and set of steps 11, 12, 13 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2. NOTE 2: The set of steps 14, 15 and 16 and set of steps 17, 18, 19 can be executed sequentially or in parallel. That is, the procedure to configure the virtualized resource at Site#1 can be executed in parallel to the procedure to configure the virtualized resource at Site#2.		

Finished.

2.1.7 Other Considerations

2.1.7.1 NS Instance Description

According to the ETSI NFV Release 2 specifications, there are two ways to control the placement of the VNFs, namely ”affinity or anti-affinity group” and ”location constraints”. The affinity or anti-affinity group describes the affinity or anti-affinity relationship applicable between the VNF instances in the NS Descriptor (NSD) [49]. The NFVO needs to select appropriate locations for the VNFs to meet the affinity or anti-affinity group. Additionally, the NFVO considers Virtual link requirements, e. g. latency, bandwidth, availability, and decides where to establish VNF.. The location constraints describe the site where the VNF is instantiated as part of the NS instantiation [50].

This subsection focuses on using the affinity or anti-affinity group to place the VNFs to different sites. Moreover, the way to utilize the ”location constraints” for VNF placement to different sites will be described. Figure 2.3 shows parameters of the NSD related to this use case. In Figure 2.3, an affinity or anti-affinity group is defined and applied to the VNF Profiles for vCPE and vAPL. Because the ”affinityOrAntiAffinity” and the ”scope” attribute of the affinity or anti-affinity group are set to ”anti-affinity” and ”NFVI-POP”, respectively (see rows in red in Table ”AffinityOrAntiAffinityGroup”), the NFVO allocates the vCPE and vAPL in different NFVI-PoPs. The NSD also specifies requirements of the Virtual Link which connects vCPE and vAPL (see rows in green in Table ”VirtualLinkDf”, ”connectivityType”, and ”VirtualLinkProfile”). Thus, the NFVO finds connectivity between those two NFVI-PoPs which satisfies the requirements.

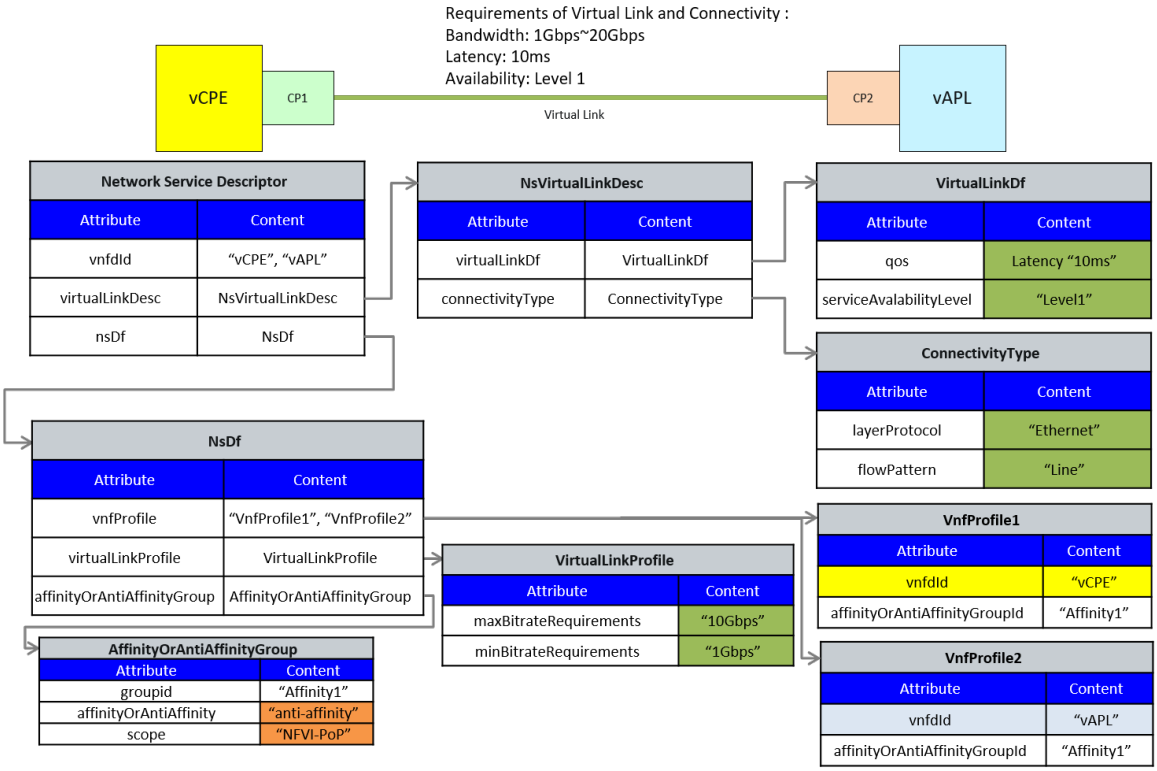


Figure 2.3: Connectivity overview for enabling NS.

2.1.7.2 Infrastructure Description

As an example Figure 2.4 shows the underlying networks for the case of the MPLS related to this use case. However, the other network architecture does not preclude for this use case. For the branch site connection case shown in Figure 2.4 a), the Customer Edge (CE) router is equivalent to GW#1 and GW#2 depicted in Figure 2.4. The Site#1 and Site#2 are connected to the IP-VPN as a customer site. The VPN routing information of the NFVI-POP are exchanged between the CE and PE routers, and also propagated to other customer sites. For the Inter Autonomous System (AS) connection case shown in Figure 2.4 b), the PE router is equivalent to GW#1 and GW#2 depicted in Figure 2.4. The Site#1 and Site#2 are identified by the AS number and are administrated by independent AS. These PE routers, which are configured as Autonomous System Border Router (ASBR), exchange the VPN routing information with each other as they are connected to other sites.

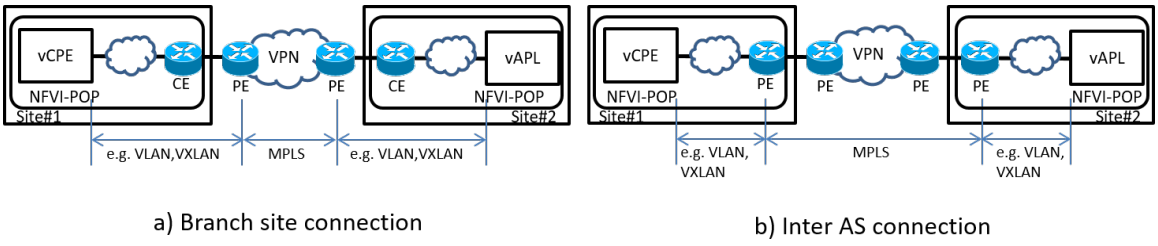


Figure 2.4: Underlying network for the case of MPLS related to an E2E EvCPE service across WAN.

2.1.7.3 Mapping of Service Instance Model to Supporting Infrastructure

Figure 2.5 shows the mapping of the service instance model to the infrastructure related to this use case. For the case of BF#1.1 and BF#1.2, the Virtual Link is directly mapped to the underlying network. On the other hand, for the case of BF#1.3, an overlay network is created over the underlying network and the Virtual Links are mapped onto the overlay network. For the case of BF#1.3, the WAN connectivity can be shared with other Virtual Links.

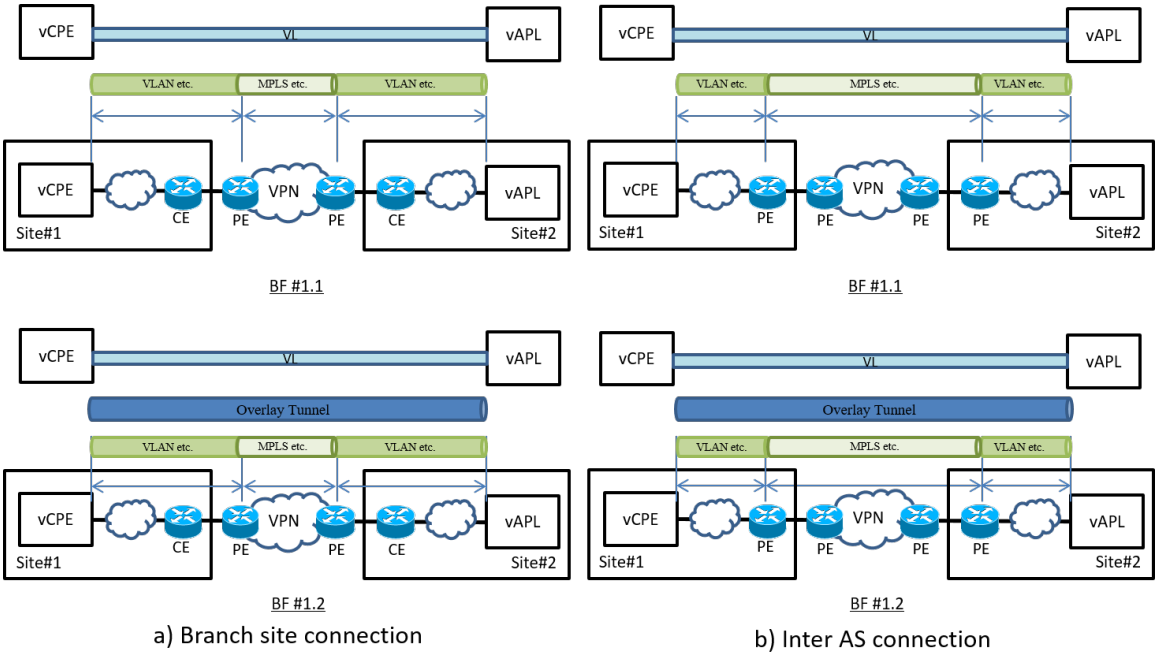


Figure 2.5: Mapping of the service instance model to the infrastructure related to this use case.

2.1.7.4 Management Architecture and Activities

This subsection represents a collection of management flows related to a sequence of a NS Instantiation. The diagram shown in Figure 2.6 provides a sequence diagram for

instantiating a connectivity service between two sites. All the flows in this subsection are informative, representing the base flow in the description.

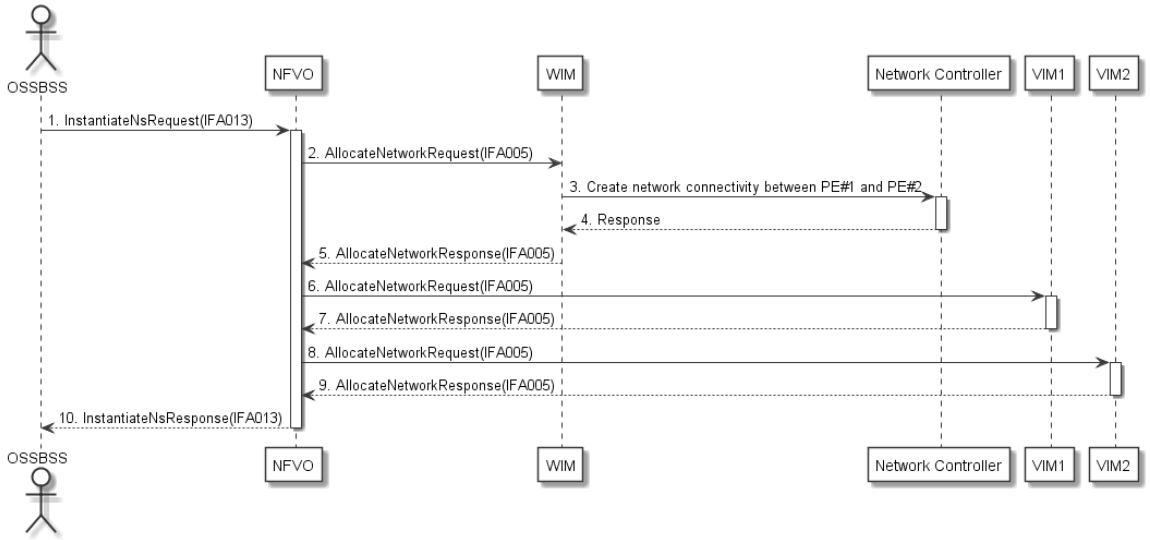


Figure 2.6: Instantiate a connectivity service.

Figure 2.7 shows a mapping of service instance Model to infrastructure related to an E2E EvCPE service across WAN. Some attributes to be discussed are introduced.

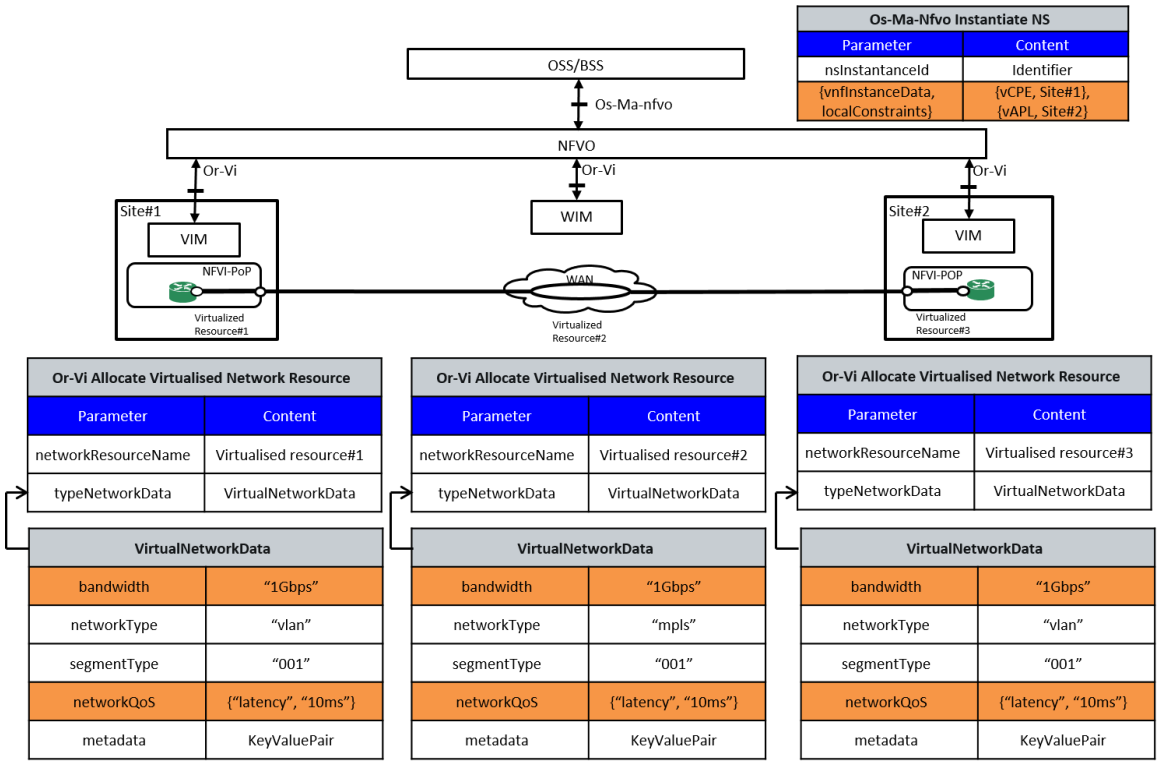


Figure 2.7: Mapping of service instance Model to infrastructure related to an E2E EvCPE service across WAN.

2.1.8 Analysis

This clause provides further analysis of Use Case #1 in terms of the connectivity services between different NFVI-PoPs and WAN infrastructure. This analysis will be done with reference to the interfaces defined over the Or-Vi reference point, which form the northbound interface for the VIM. The analysis will highlight the relevant Information Elements and their respective attributes defined over the Or-Vi reference point [51] and show how they can be utilized by the WIM in order to ensure connectivity between sites (e.g. central office). For ensuring connectivity between sites; network connectivity endpoints, virtual network ports, virtual network interfaces and virtual network resources are the essential elements. Figure 2.8 illustrates the mapping of these elements described in [51] in the context of Use Case #1. These elements are described below in the context of providing connectivity between VNFs over a WAN infrastructure. In this use case, a virtual network resource is characterized by various attributes defined over the VirtualNetwork Information Element [51]. For example, it specifies the type of the virtual network. There are multiple options to allocate the virtual network resources (e.g. vlan, vxlan, gre, etc.), which are characterized by the networkResourceTypeId, segment information (e.g. vlan identifier, vxlan identifier, gre key, etc.), the bandwidth, the network QoS attributes. On the other hand, a virtual network port is another type of endpoint and characterized by the VirtualNetworkPort Information Element in [51]. The attributes of

this information element are configured depending on the portType (e.g. L2 or L3 access ports or L1 trunk port), networkId, segmentId (e.g. vlan id, gre key), and the bandwidth (in Mbps) supported by the virtual network port. These attributes are helpful to determine the location of the attachment points to VNFs within the NFVI-PoP. The virtual network port is attached to a virtual network interface, which is a communication endpoint under a compute resource. The virtual network interface is described by the attributes of the VirtualNetworkInterface information element (e.g. networkId, networkPortId, ipAddress, etc.). Moreover, a network connectivity endpoint is an endpoint attached to an NFVI-PoP administrated by the VIM. As represented by the example, it is considered that the endpoint can be mapped onto a Network Gateway. Such a network gateway can be addressed by an attribute, the networkConnectivityEndpoint of the NfviPop Information Element. This attribute is helpful for other NFVI-PoP or N-PoP to find the location of the network gateway instance.

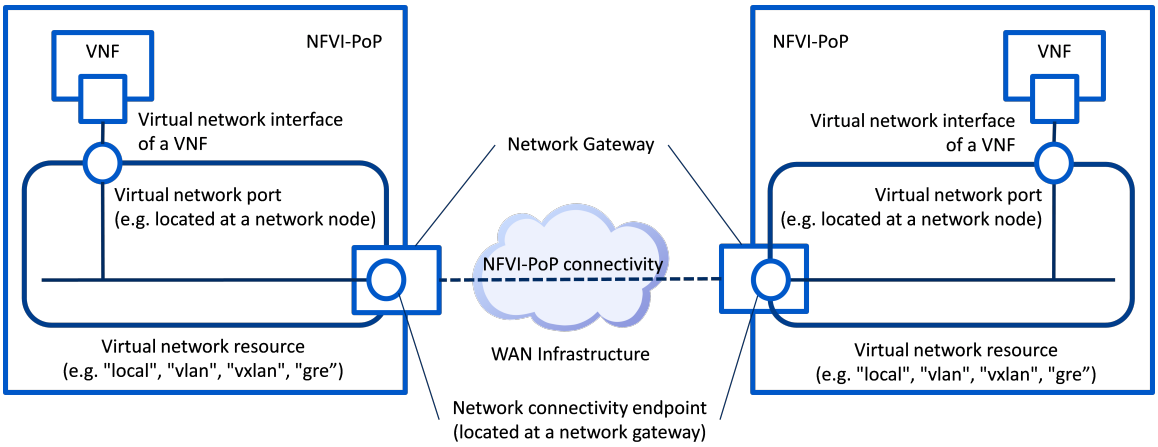


Figure 2.8: Terminology mappings from IFA 005 context to current document.

From the perspective of the infrastructure level, a network gateway of the NFVI-PoP is considered as a CE node [52] which connects branch sites. The CE can be considered as an infrastructure node in the infrastructure network domain [47], or can also be a virtualized network node. On the other hand, PE nodes are put at the edge of the WAN infrastructure, interfacing to Ex-Nf, a reference point to an external network defined in NFV Infrastructure [47]. The connectivity at the WAN infrastructure level, called WAN connectivity, is established between the provider edge nodes. The connectivity may be configured in advance or on-demand. As shown in Figure 2.9, connectivity between the NFVI-PoPs, configured between the customer edge nodes, needs to be established over the WAN connectivity.

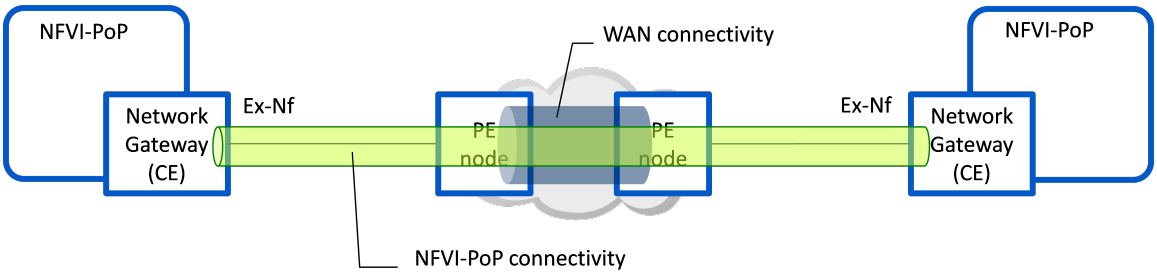


Figure 2.9: A mapping to the infrastructure.

Table 2.8 shows as examples ways of configuring the WAN and NFVI-connectivity between the NFVI-PoPs. These examples should not be limiting and more examples can be added and analyzed, if necessary.

Table 2.8: Examples for NFVI-PoP connectivity and WAN connectivity.

NFVI-PoP connectivity service	WAN Connectivity
Virtual Private LAN Service (VPLS) (layer 2 MPLS VPN) [53, 54, 55]	MPLS (L2-VPN)
VPRN (layer 3 MPLS VPN) [52]	MPLS (IP-VPN)
H-VPLS [56]	MPLS
Ethernet VPN (EVPN) [57]	MPLS
VxLAN [58]	IP-Network
NVGRE [59]	IP-Network

After the instantiation of the NS, VNFs are connected within the same or different broadcast domain as shown in Figure 2.10 and Figure 2.11.

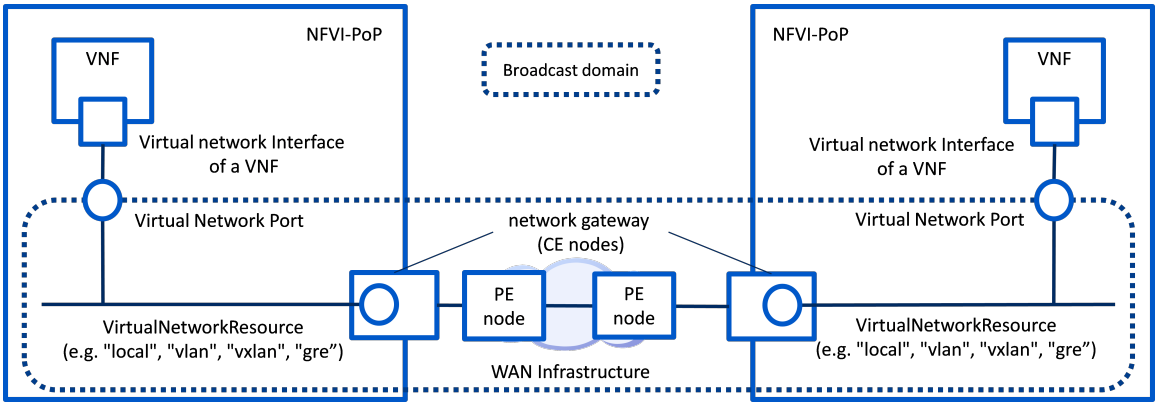


Figure 2.10: L2 connectivity between NFVI-PoPs.

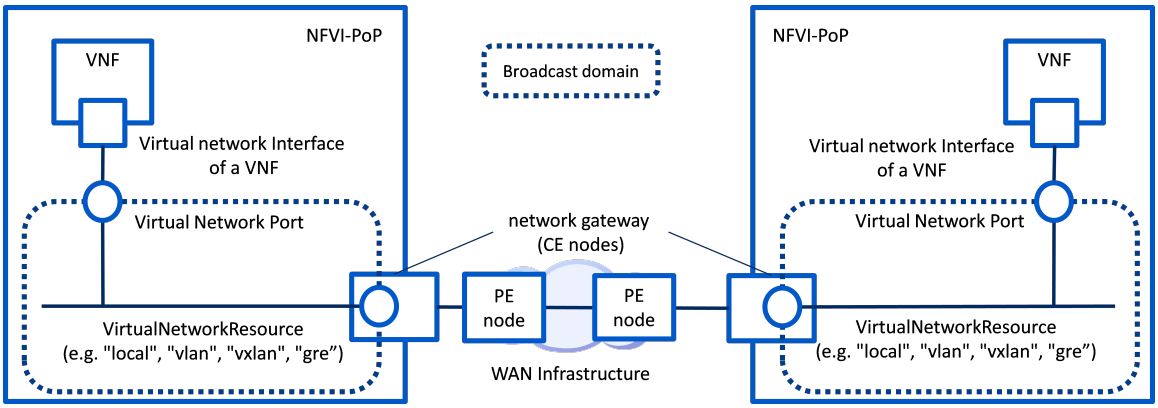


Figure 2.11: L3 connectivity between NFVI-PoPs.

It should be analyzed, from a view across all of the use cases, what information elements and attributes to manage the following resources are necessary:

- WAN connectivity
- NFVI-PoP connectivity (configurations for Ex-Nf)
- Configuration of the network gateways to interconnect virtual network resources and NFVI-PoP connectivity

In addition, the base flows in this use case indicate that it is necessary for a VIM/WIM to provide information necessary for connecting to a virtualized network resource the VIM/WIM manages. This information is consumed by other VIMs/WIMs when they connect their virtualized network resources to this one. The flow of information can be as follows:

- WIM to VIM (see steps 7, 8 and 11 of BF#1.1 in Table 2.5 and steps 7, 8 and 11 of BF#1.3 in Table 2.7). A VIM uses the information about allocated virtualized network resource on the WAN to configure a virtual network resource within its managed NFVI-PoP to connect to the virtual network resource on the WAN.
- VIM to WIM (see steps 10, 13 and 14 of BF#1.2 in Table 2.6). A WIM uses the information about the virtualized network resource within the NFVI-PoP connecting to the WAN to configure a virtual network resource within its managed WAN to connect to the virtual network resource within the NFVI-PoP.
- VIM to VIM (see steps 10, 13, 19 and 22 of BF#1.2 in Table 2.6 and steps 10, 13, 14 and 17 of BF#1.3 in Table 2.7). A VIM uses the information about other NFVI-PoP endpoints to configure the endpoint of an overlay or inter-AS connection within its managed NFVI-PoP to connect with the peered endpoint within another NFVI-PoP.

The distribution of this information is performed via NFVO as shown in the base flows. Thus, NFVO should be capable of acquiring the relevant information from the source VIM/WIM and then forward the needed information to the appropriate target VIMs/WIMs.

2.2 Modification to the WAN Connectivity Resource of a Multi-site NS

2.2.1 Introduction

Based on use case #1 in section 2.1. this subsection shows a use case on modification to the WAN connectivity resource of a multi-site NS. As introduced in use case #1, the NS in this case is for an EvCPE, which is reused in the present use case description. Within the context of such an NS (e.g. the NS for the EvCPE), the bandwidth requirement of the VL in between the VNFs may increase or decrease in accordance with, for example, the change of traffic volume of a connectivity service between Site#1 and Site#2. The WAN controller or WIM controls the bandwidth of the WAN connectivity to match the change of traffic volume between the two sites.

2.2.2 Trigger

Table 2.9 describes the use case trigger.

Table 2.9: Modification to the WAN connectivity resource.

Trigger	Description
BF	The OSS requests the NFVO to increase the capacity of an existing NS (e.g. the NS for the EvCPE) , because the workload on the current VNFs has become high.

2.2.3 Actors and Roles

Table 2.10 describes the use case actors and roles.

Table 2.10: NS for E2E Enterprise vCPE across two WANs actors and roles.

#	Actor
1	OSS/BSS
2	NFVO
3	VIM
4	Network Controller
5	WIM

2.2.4 Pre-conditions

Table 2.11 describes the pre-conditions.

Table 2.11: NS for E2E Enterprise vCPE across two WANs Pre-conditions.

#	Pre-condition
1	An E2E EvCPE service is instantiated and works properly according to the SLA. See base flow #1.1, base flow #1.2, or base flow #1.3 in section 2.1.
2	The virtual network bandwidth of WAN is limited by the capacity requirement according to NS.

2.2.5 Post-conditions

Table 2.12 describes the post-conditions.

Table 2.12: Modification to the WAN connectivity resource.

#	Post-condition
1	The capacity / bandwidth of the virtualized network resources at site#1, site#2 and WAN that consist of the NS have been increased. An EvCPE service is instantiated and works properly according to the SLA.

2.2.6 Operational Flows

Table 2.13 describes the operational flow.

Table 2.13: Modification to the WAN connectivity resource operational flow.

#	Flow	Description
1	OSS/BSS → NFVO	Requests an update to increase the capacity of the VL of an existing NS between Site#1 and Site#2. *Interface - Os-Ma-nfvo*
2	NFVO → WIM	Requests to update the network bandwidth of the virtualized resource#2 at the WAN. The NFVO sends the resource identifier which is obtained at step 7 of base flow #1.1, base flow #1.2, or base flow #1.3 in section 2.1. *Interface - Or-Vi*
3	WIM →, Network Controller	Requests to update the network bandwidth of the virtualized resource#2.
4	Network Controller	Updates the network bandwidth of the virtualized resource#2. See note. .
5	WIM → NFVO	Returns the response to update the network bandwidth of the virtualized resource#2. *Interface - Or-Vi*

Continued on next page.

#	Flow	Description
6	NFVO → VIM at site#1	Requests to update the network bandwidth of the virtualized resource#1 at site#1. The NFVO sends the resource identifier which is obtained at step 10 of base flow #1.1, base flow #1.2, or base flow #1.3 in section 2.1. See note. *Interface - Or-Vi*
7	VIM at site#1	Update the network bandwidth of the virtualized resource#1. See note.
8	VIM at site#1 → NFVO	Returns the response to update the network bandwidth of the virtualized resource#1. See note.. *Interface - Or-Vi*
9	NFVO → VIM at site#2	Requests to update the network bandwidth of the virtualized resource#3 at site#2. The NFVO sends the resource identifier which is obtained at step 13 of base flow #1.1, base flow #1.2, or base flow #1.3 in section 2.1. See note. *Interface - Or-Vi*
10	VIM at site#2	Update the network bandwidth of the virtualized resource#3. See note.
11	VIM at site#2 → NFVO	Returns the response to update the network bandwidth of the virtualized resource#3. See note.. *Interface - Or-Vi*
12	NFVO → OSS/BSS	Returns the result of the update for the NS. *Interface - Os-Ma-nfvo*
NOTE: The set of steps 6, 7, 8 and the set of steps 9, 10 and 11 can be executed sequentially or in parallel. That is, the procedure to update the network bandwidth at Site#1 can be executed in parallel to the procedure to update the network bandwidth at Site#2.		

Finished.

2.2.7 Analysis

For the modification of the WAN connectivity resource of a multi-site NS, the NFV-MANO should be able to:

- Support controlling the bitrate provided by the virtualized network resource.
  As shown in the steps #2 and #6, NFVO requests WIM and VIM to update the network bandwidth of the virtualized network resources in the WAN and within the site, respectively. In both cases for WAN and NFVI PoP virtualized network resources, controlling the bitrate to any possible value in between a minimum and a maximum may not be possible, thus only a limited number of fixed bit rates (e.g. 100 Mbps, 1 Gbps and 10 Gpbs) may be supported. The UpdateNetwork operation provided by the virtualized network resource management interface in ETSI GS NFV-IFA 005 [51] is relevant to the present use case. The

input parameter updateNetworkData of type VirtualNetworkData has the attribute ”bandwidth” which enables specifying the minimum network bandwidth (in Mbps) for a virtualized network resource. Currently, the interface applies to resources managed by the VIM within an NFVI-PoP. Similar capabilities and specification are also applicable in the case of WAN virtualized network resources managed by a WIM.

2.3 NS for E2E Enterprise vCPE across two WANs

2.3.1 Introduction

An enterprise vCPE model can be seen as a use case in ETSI GS NFV 001 [5], which provides a view of a typical large enterprise comprising headquarters facilities with a centralized corporate IT infrastructure and multiple branches connected to one another and to the enterprise headquarter. The vCPE functions can be deployed at branch sites, service provider's site, and centralized enterprise site. Those sites are interconnected with WAN connectivity service, which traditionally supported by a single infrastructure, or by multiple different network infrastructure (Open Networking User Group (ONUG) Software-Defined WAN Use Case [60]). MPLS, Internet or a pair of them are shown as examples. Derived from use case 1, this use case discusses how the NFVO maps aVL onto an appropriate WAN infrastructure, when multiple WAN infrastructures are available. In the context two virtual links, one for management plane and the other for data plane, are required for a particular NS. For the management plane the requirement is high reliability, while the requirement for the data plane is high capacity. However, the virtual links that have the required characteristics and capacity to satisfy the NS requirements are installed and available in different WAN infrastructures. The MANO should select the Virtual Links that meet best the path criteria for the NS. Thus this ability of MANO on the selection of the appropriate VLs would enable it to meet criteria such as the connectivity type (e.g. Ethernet, IP-VPN), the performance (the latency, the jitter or the bandwidth), the service availability level, etc. The following base flow is expected, but not limited:

- BF: NS deployment with two virtual links over different WAN infrastructures:
  - A pair of WAN infrastructures, namely WAN#1 or WAN#2, are connected to each site, namely Site#1 or Site#2. VNFs are deployed at the two sites in the same way as described in Use Case 1, and those are then connected with a pair of VLs belonging to the two WAN infrastructures.
  - The two WAN infrastructures combined fulfil the different requirements of the two Virtual Links such as the connectivity type, the performance, and the service availability level, etc. as required by the NS. The MANO thus selects the appropriate VLs, i.e. the Virtual Link#1 and the Virtual Link#2 from the WAN#1 and the WAN#2, respectively.

Figure 2.12 shows the connectivity overview for enabling end-to-end the NS across two WAN infrastructures. Two NFVI-PoPs are connected across two WAN infrastructures.

virtualized network resources of Virtual Link#1 and Virtual Link#2 are referred to virtualized network resource#1, #3 and #5 and virtual network resource#2, #4 and #6, respectively. The virtualized network resource #1 and #2, the virtualized network resource #5 and the virtualized network resource #6 are attached to vCPE, vAPL and monitoring, respectively. The virtualized network resource #1 and #5 and the virtualized network resource #2 and #6 are also attached to the virtualized network resource#3 and #4, respectively. As a result, the Virtual Link#1 is installed on the virtualized network resource#1, #3 and #5. And the Virtual Link#2 is installed on the virtualized network resource#2, #4 and #6.

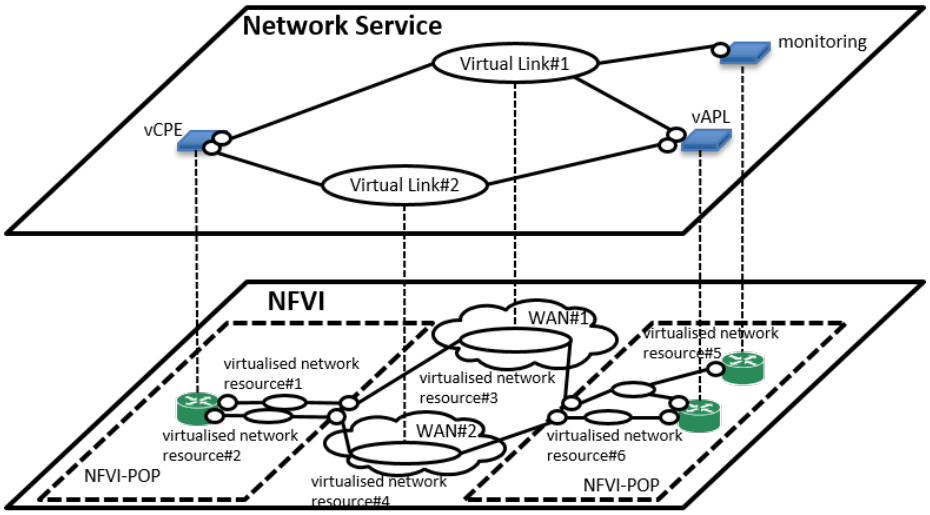


Figure 2.12: Connectivity overview for enabling End-to-End NS across two WANs.

Figure 2.13 provides an architectural view of the use case with respect to the MANO framework. It shows a multi-site model managed by a single Service Provider. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are referred to in the present use case. Here the architecture includes a WIM for each WAN. However, this does not preclude an alternative management architecture, where a single WIM may be responsible for both (or more) underlying WANs.

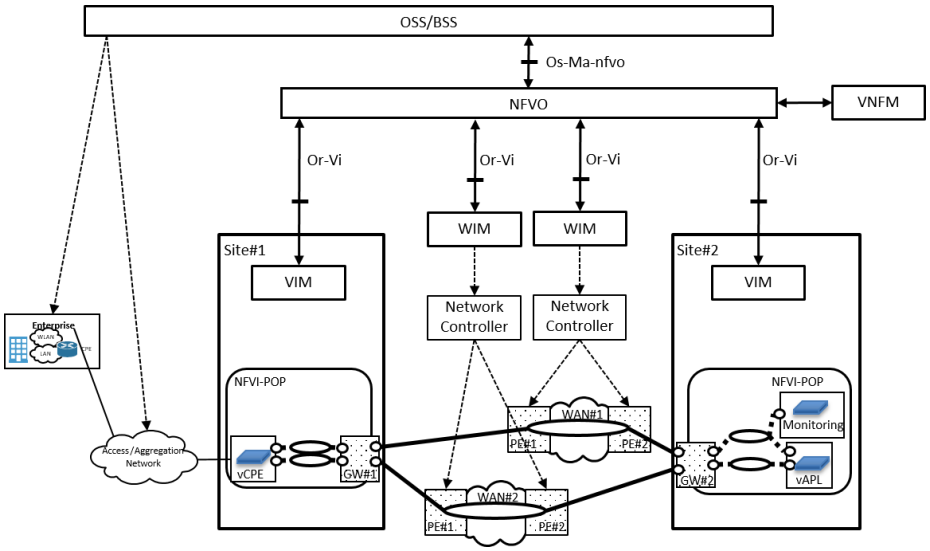


Figure 2.13: High-level use case for an E2E EvCPE service across two WANs.

2.3.2 Trigger

Table 2.14 describes the use case trigger for base flow.

Table 2.14: NS for E2E Enterprise vCPE across two WANs trigger base flow.

Trigger	Description
BF	When the NFVO is requested to instantiate VNFs in the Site#1 and Site#2 from the OSS/BSS.

2.3.3 Actors and Roles

Table 2.15 describes the use case actors and roles.

Table 2.15: NS for E2E Enterprise vCPE across two WANs actors and roles.

#	Actor
1	OSS/BSS
2	NFVO
3	VIM
4	Network Controller
5	WIM

2.3.4 Pre-conditions

Table 2.16 describes the pre-conditions for base flow.

Table 2.16: NS for E2E Enterprise vCPE across two WANs Pre-conditions.

#	Pre-condition
1	The network between the enterprise site and Site#1 shown in Figure 2.2 works properly according to the SLA.
2	The infrastructure of the NFVI-PoP at Site#1 and Site#2 and the network infrastructure of the WAN are also physically connected.

2.3.5 Post-conditions

Table 2.17 describes the post-conditions for base flow.

Table 2.17: NS for E2E Enterprise vCPE across two WANs post-conditions for base flow.

#	Post-condition
1	E2E EvCPE service is provided across the two sites. The VNF connects two Virtual Links through different WANs.

2.3.6 Operational Flows

Table 2.18 describes the base flow.

Table 2.18: NS for E2E Enterprise vCPE base flow #1.1.

#	Flow	Description
1	OSS/BSS → NFVO	Requests to instantiate a NS across Site#1 and Site#2. Designates WANs to allocate the Virtual Link#1 and #2 respectively by notifying the requirements of the VLs at NSD or input parameters. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL. NFVO decides allocation of the VLs which meet the requirements shown in step 1 in accordance with the capability and the capacity check of the WAN infrastructure shown in step 2 in Table 2.5.
3	NFVO, WIM, Network Controller, VIMs at Site#1 and Site#2	The virtualized network resources#1,#3, #5 and the virtual resource#2,#4,#6 are created according to the step 3 to step 15 of ”NS for E2E Enterprise vCPE base flow#1” (Table 2.5), respectively. WIM follow from the step 3 to step 7 but works with WIMs in the WAN#1 and WAN#2.
4	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s). The VNFs across two sites connect to the Virtual Link#1 and #2. .

Continued on next page.

#	Flow	Description
5	NFVO → OSS/BSS	Returns the results of NS instantiation request.

Finished.

2.3.7 Analysis

The objective of this analysis is to describe the instantiation procedures expressed in step 2 of Table 2.18 and highlight the main operational steps. In order to determine the location to instantiate the VNFs and VLs requested by OSS/BSS, the NFVO needs to parse the relevant NSD file to determine the location of NFVI-PoPs, and check for available network resources. In this regard the relevant attributes, parameters and contents that are required during different steps of the instantiation process are analyzed below.

NS Descriptor (NSD) Parsing

The OSS/BSS invokes an ”InstantiateNsRequest” on the NFVO to start the instantiation procedure. This request includes the parameter ”flavourId”, which is linked to the target NSD and refers to NS Deployment Flavour (NsDf) Information Element (IE) which has been on-boarded in advance. The request also includes ”locationConstraints” that defines the location constraints for the target VNFs to be instantiated as a part of the target NS. In the context of use case 2, the Virtual Links are required to be deployed in the different WAN infrastructures but the constraints for the VLs have not been specified in the current ETSI NFV Release2 specifications yet.

Determination of Location of NFVI-PoPs

The parameter ”locationContraints” in ”instantiateNsRequest” defines constraints on the basis of which NFVI-PoPs are selected for deploying the VNFs as requested by OSS/BSS. The NFVO invokes ”NfviPopNetworkInformationRequest” to the VIMs in order to retrieve NfviPop information element. This information element consists of the attribute ” geographicalLocationInfo”, which provides the information about the geographic location (e.g. geographic coordinates or address of the building, etc.) of the NFVI resources that the VIM manages. Another attribute of ”networkConnectivityEndpoint” provides the information about network connectivity endpoints. However, the content of ”networkConnectivityEndpoint” attribute has not been specified yet in the specification of the Or-Vi reference point [51]. It is expected that the ”networkConnectivityEndpoint” attribute provides information about the network interface that connects the NFVI-PoP to the WAN infrastructure, and this information is shared with the WIM.

Network Resource Identification between NFVI-PoP

The ”NsVirtualLinkDesc” IE in the NS Deployment Flavour (NsDf) IE includes ”connectivityType” and ”virtualLinkDf” attributes. The ”connectivityType” attribute has the contents of ”layerProtocol” and ”flowPattern”. The ”layerProtocol”

identifies the protocol that the VL supports (Ethernet, MPLS, ODU2, IPV4, IPV6, Pseudo-Wire, etc.) while ”flowPattern” identifies the flow pattern of the connectivity (Line, Tree, Mesh, etc.). With those contents, the NFVO can determine the type of network connectivity that should be instantiated. The ”virtualLinkDf” attribute has the contents of ”qos”. The ”qos” content has ”latency”, ”packetDelayVariation”, ”packetLossRatio”, and ”priority” values. With these values of the ”qos” content, NFVO selects WAN infrastructure which satisfies the QoS requirements. A situation may arise where the QoS requirements of Virtual Link#1 and Virtual Link#2 are satisfied by WAN#1 and WAN#2 respectively. As discussed above, a new constraint for virtual link is necessary to deploy Virtual Link#1 and Virtual Link#2 in different WAN infrastructures.

Querying for Network Status

The invocation of the ”QueryNetworkCapacityRequest” message by the NFVO can be used to retrieve information elements from VIM at Site#1, VIM at Site#2, WIM#1 and WIM#2. The message has a parameter ”resourceCriteria”, which declares the characteristics of the virtual network for which the operator may want to know the available, total, reserved and/or allocated capacity. The information provided by this parameter can thus be used to retrieve available path, resource, etc., in the VIM at Site#1, VIM at Site#2, WIM#1 and WIM#2. In use case 2, NFVO should decide how to allocate the virtualized network resources for VLs in different WAN infrastructures. By comparing attributes and contents in the target NSD and the current status of the virtualized network resources managed by VIM at Site#1, VIM at Site#2, WIM#1 and WIM#2, and by checking if the deployment model is defined in the NSD or not, the NFVO requests for resource allocations to the VIMs and the WIMs. In the operational procedure, the operational policies may contain rules that follow criteria for certain aspects. A non-exhaustive list of criteria is listed below:

- Constraints aspects:
  - The NFVO may consider constraints on location of the VNFs and VLs declared by OSS/BSS.
  - The constraints for the VLs should be declared as such whether they can be deployed in the same or different WAN infrastructures.
- WAN capacity aspects:
  - During the selection process of WAN infrastructure, the NFVO generates ”resourceCriteria” parameter, which declares capacity computation parameter for selecting the characteristics of the virtual network.
  - Explicit route declaration can be indicated which WAN infrastructure should be used.
  - WIM should have the capability to compute available network resources.
  - Network Controller should have the capability to compute available capacity if WIM does not have the capability.
- WAN connectivity aspects:

  - During the selection process of WAN infrastructure, the NFVO may require information on the type of connectivity servicesupported by the WIMs.
  - The connectivity information of the NFVO should support different types of layer protocols so that ”connectivityType” attribute can be specified with multiple options such as Ethernet, MPLS, ODU2, IPV4, IPV6, Pseudo-Wire, etc.
  - In a situation where there is no WAN connectivity between NFVI-PoPs, NFVO needs to request WIM for allocation of a new WAN connectivity.
  - WIM should be able to configure the WAN connectivity.
- NFVI-PoP Connectivity aspects:
  - In a situation where there is no NFVI-PoP connectivity between NFVI-PoPs, NFVO needs to request WIMs and VIMs for allocation of a new NFVI-PoP connectivity.
  - NFVO should be able to collect network interface information connecting to the WAN infrastructure.

2.4 NS Expansion to other NFVI-PoPs over WAN

2.4.1 Introduction

Derived from the use case 1, this use case discusses how the NFVO expands the NS to the other NFVI-PoPs over WAN for the purpose of scaling the NS. Flexible NS scaling can help save CAPEX and OPEX when traffic rapidly changes because of expected event, e.g. a scheduled event requiring additional service capacity, or unexpected event (e.g. natural disaster) requiring capacity expansion. For example, it is assumed that two NFVI-PoPs that are located in different sites are connected over the WAN infrastructure, and the NFV-MANO deploys an NS within one of the sites (the first site). When workloads of the NS cross its capacity threshold and there are not enough available resources to scale the NS within the first site, the NS scaling is resolved by expanding the NS to use resources from a second site. In such a case, the NFV-MANO manages the needed NS VLs and requests new network connectivity between the two sites to expand the NS over the two sites. As a result, the workloads can be distributed between the two sites. The following base flow is expected, but not limited:

- BF: NS expansion to other NFVI-PoPs over the WAN:
  - There are two sites, namely Site#1 and Site#2, which are physically connected over the WAN. An NS which consists of two VNFs, i.e. vCPE and vAPL#1, and a VL which connects them is deployed in Sites#1. When a trigger event such as the overload of the vAPL#1 is detected, the NFVO adds a new instance of the vAPL called vAPL#2 in Site#2, and updates the VL to connect the vAPL#2 across the WAN.

Figure 2.14 shows a connectivity overview after performing the NS expansion to other NFVI-PoPs over the WAN. By performing the NS expansion, two NFVI-PoPs are connected across a WAN infrastructure. The virtualized resource for the WAN is referred as virtualized network resource#3. A virtualized network resource#2 is created to provide network connectivity within the NFVI-PoP of Site#2. The virtualized network resource#1 in the NFVI-PoP of Site#1, which connects the vCPE and the vAPL#1, is extended to connect the WAN. As a result, the VL is extended covering the virtual network resource#1, #2 and #3.

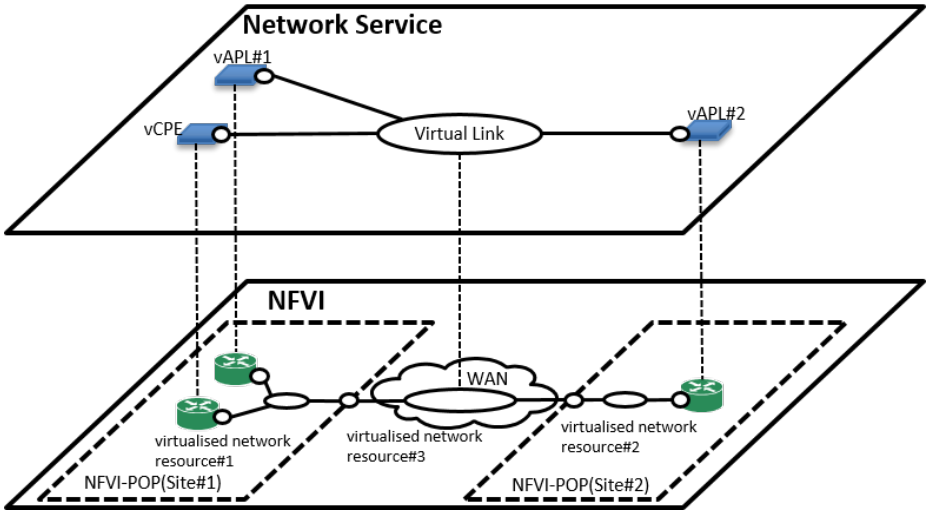


Figure 2.14: Connectivity overview for enabling NS expansion over WAN.

Figure 2.15 provides an architectural view of the use case. It shows a multi-site model managed by a single Service Provider. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are further referred to in the present use case.

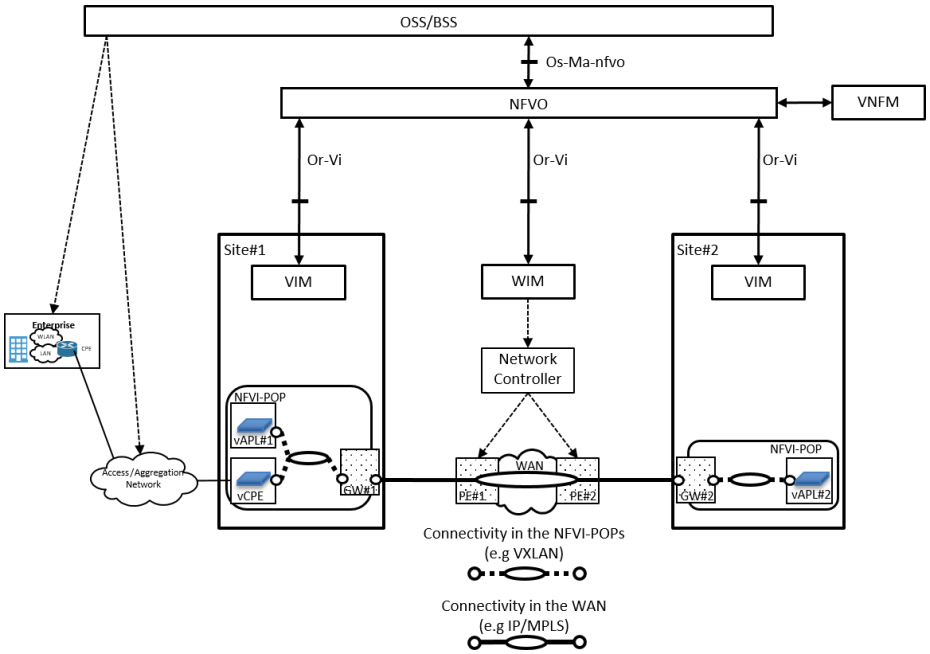


Figure 2.15: High-level use case for an NS expansion over WAN.

2.4.2 Trigger

Table 2.19 describes the use case trigger for base flow.

Table 2.19: NS expansion to other NFVI-PoPs over WAN trigger base flow.

Trigger	Description
BF	When the NFVO is requested by the OSS/BSS to scale NS to add vAPL#2 due to the OSS/BSS getting a trigger event such as an overload of the vAPL#1..

2.4.3 Actors and Roles

Table 2.20 describes the use case actors and roles.

Table 2.20: NS expansion to other NFVI-PoPs over WAN actors and roles.

#	Actor
1	OSS/BSS
2	NFVO
3	VIM
4	Network Controller
5	WIM

2.4.4 Pre-conditions

Table 2.21 describes the pre-conditions for base flow.

Table 2.21: NS expansion to other NFVI-PoPs over WAN Pre-conditions for base flow.

#	Pre-condition
1	The E2E EvCPE service is provided by the vCPE and the vAPL#1 in Site#1. The NFVO provides the virtual resource at Site#1 for the E2E EvCPE service by default.

2.4.5 Post-conditions

Table 2.22 describes the post-conditions for base flow.

Table 2.22: NS expansion to other NFVI-PoPs over WAN post-conditions for base flow.

#	Post-condition
1	The E2E EvCPE service is updated across the two sites. The VNFs in the two sites are connected over the VL through WAN infrastructure..

2.4.6 Operational Flows

Table 2.23 describes the base flow.

Table 2.23: NS expansion to other NFVI-PoPs over WAN base flow.

#	Flow	Description
1	OSS/BSS → NFVO	The OSS/BSS requests to scale the NS to add the vAPL#2. *Interface - Os-Ma-nfvo*
2	NFVO	The NFVO checks the capability whether the Site#1 has enough resources for the vAPL#2. If there are not enough resources at Site#1, the NFVO then checks the capacity of Site#2 for instantiating vAPL#2. If vAPL#2 has the capacity then the NFVO will check the connectivity related capability of WAN between the NFVI-PoP at Site#1, and the NFVI-PoP at Site#2. The NFVO then decides to allocate vAPL#2 to Site#2 and setup a virtualized network resource#3 for network connection between two sites across the WAN. Then the NFVO starts an instantiation process for the vAPL#2 with the VNFM.

Continued on next page.

#	Flow	Description
3	NFVO, WIM, Network Controller	The virtualized network resources#3 for network connectivity across WAN is created according to step 3 to step 7 of ”NS for E2E Enterprise vCPE base flow#1.1” (Table 2.5).
4	NFVO, VIM at Site#2	The virtualized network resources#2 for connecting to the WAN is created according to the step 11 to step 13 of ”NS for E2E Enterprise vCPE base flow#1.1” (Table 2.5). See note.
5	NFVO → VIM at Site#1	The NFVO requests to update the virtualized resource#1 for connecting to the WAN. The NFVO sends information for connecting to the network connectivity over the WAN which is obtained in step 3. See note. *Interface - Or-Vi*
6	VIM at Site#1	The VIM at Site#1 updates the virtualized resource#1 for connecting to the WAN. See note.
7	VIM at Site#1 → NFVO	The VIM as Site#1 returns the response to the request for updating the virtualized resource#1. See note. *Interface - Or-Vi*
8	NFVO	The NFVO completes the instantiation process for the vAPL#2 with the VNFM.
9	NFVO → OSS/BSS	The NFVO returns the results of the NS scaling request.
NOTE: The step 4 and set of steps 5, 6 and 7 can be executed sequentially or in parallel. That is, the procedure to update connectivity at Site#1 can be executed in parallel to the procedure to create connectivity at Site#2.		

Finished.

2.4.7 Analysis

For the expansion of an NS to other NFVI-PoPs over WAN, the NFV-MANO should be able to:

- Update the connectivity of the NS already deployed within a site to expand the existing NS VL across the WAN.

As the use case depicts, initially, the only available NS VL was deployed within the boundary of a specific Site (e.g. NFVI-PoP), whereas after the expansion, the existing NS VL expands across the WAN. As introduced in steps 5, 6 and 7 of the operational flow in Table 2.23, the VIM should support updating the virtualized network for connecting to the WAN. Requirement Nfvo.NsU.004 of ETSI GS NFV-IFA 010 [61] specifies the capability for the NFVO to support updating the existing VL(s)/VNFFG(s) involved in an existing NS. In addition, requirement Nfvo.NsRmpbNfvo.001 of the same referred deliverable [61]

specifies the support of the capability of the NFVO to issue requests to the VIM in order to allocate, identify, update and release resources needed for the connectivity of NSs. The requirements do not detail within what boundaries/scope such an update of virtualized network resources can be performed, i.e. whether or not such an update concerns only to virtualized network resources within an NFVI-PoP. The virtualized Network Resource Management interface produced by the VIM on the Or-Vi reference point towards the NFVO specifies the UpdateNetwork operation (refer to clause 7.4.1.4 of ETSI GS NFV-IFA 005 [51]). The operation offers the capability to update different types of virtualized network resources, such as: network, subnet and network ports. The NfviPop information element (refer to clause 8.10.3 of [51]) also provides information about the network connectivity endpoints to the NFVI-PoP, which helps building the topology information relative to NFVI-PoP connectivity to other NFVI-PoP. Both, the UpdateNetwork operation as well as the NfviPoP information element are relevant to the present use case. As part of the expansion across the WAN, the existing virtualized network resource(s) within the NFVI-PoP needs to be updated to enable connectivity to the WAN through the appropriate network connectivity endpoint of the NFVI-PoP. Although it is not explicitly detailed in the use case flow, the update to enable connectivity to the WAN might require allocation of new specific virtual network resources such as network ports and network segments. However, neither the UpdateNetwork operation, nor the information elements available in the ETSI GS NFV-IFA 005 [51] specify the means on how to achieve such a connectivity expansion.

2.5 Conclusion

I have presented four typical use cases that have been accepted as a new feature of the ETSI NFV Release 3 specifications [37]. Prior to this proposal, the exchange of network information between providers was considered unnecessary, since the NFV use case focuses on a single operator case, which means that the NFV orchestrator can manage all network information. My proposal was accepted because it showed use cases involving networks from multiple providers, like we see with multihoming. Use case analysis can be summarized into three requirements: (1) Network information exchange for exchanging necessary resource information between multiple providers (2) a network evaluation method for selecting an appropriate NFVI-PoP that meets service requirements, and (3) NFVI-PoP connectivity control for updating the connectivity among multi-provider NFVI-PoPs. The ETSI GR NFV-IFA022 report [37] analyzed these use cases in more detail and summarized suggestions for improving the existing specifications.
Proposals for standardization of basic schemes for connecting multiple nfrastructures are expected to lead to vendor implementation.

Chapter 3

Network Information Exchange Scheme

This chapter numerically evaluates the NFVO load of the ETSI NFV specifications. A simple queueing model with parameters recommended in the conventional scheme shows that the waiting time can go to infinity. Thus, an interoperable architecture among multiple VIMs, which delegates a part of a slice design process to VIMs, is proposed. On the basis of the queuing model, the waiting time only grows moderately in our scheme. The chapter also discusses several aspects related to our interoperable architecture among multiple VIMs e.g., protocol extension and security, from practical perspective. Section 3.1 shows practical issues of existing specifications. Section 3.2 shows the proposed scheme that exchanges network information among multiple providers. Section 3.3 shows an example of implementing the exchanging scheme that was proposed to ETSI NFV GR IFA022.

3.1 Practical Issues

3.1.1 Response Time

To discuss the overloading issue of the ETSI NFV Release2 specifications, Figure 3.1 shows a NS deployment across multi-provider networks for IoT services [62, 5]. The WAN and Data Centers (DCs) are provided by infrastructure providers, and the NFVO is provided by a service provider. The NFVO controls network resources in the WAN and DCs through application programming interfaces. Nowadays, infrastructure providers usually operate several types of infrastructure networks, e.g., fixed and wireless networks, L2VPN, and L3VPN, and clouds. End-to-end service quality is not determined by single infrastructure, and so the quality control across multi-provider networks is key issue in 5G [63, 64]. Note that OpenStack [65], a reference implementation of VIM, does not care Network Connectivity (NC) between VIMs, the NFVO has to NC information to VIMs

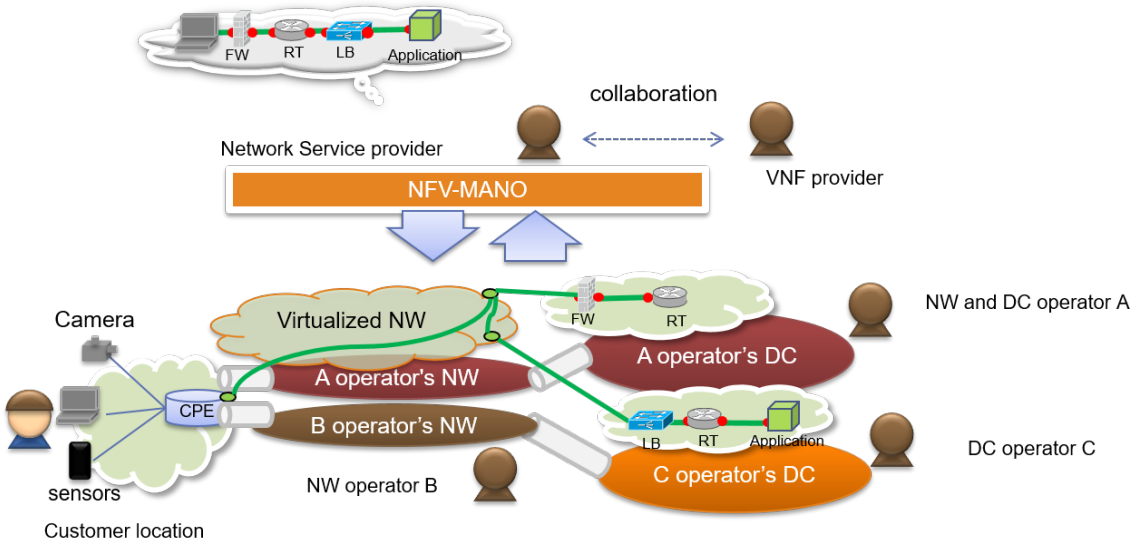


Figure 3.1: Virtual network integration as a service.

Additionally, 5G networks will be often used by IoT service providers. To reduce communication fees, IoT service providers would frequently destroy their slices in off period, which could greatly increases NS deployment requests to the NFVO. Figure 3.2 shows a queuing model that represents the existing ETSI NFV Release 2 specifications. It is modeled as the M/M/1. Poisson distribution is used to model the arrival times. The average response time, T_{nfvo}, of NS deployment is given as,

$$T_{nfvo} = \frac{1}{\mu_{nfvo} - \lambda} - \frac{1}{\mu_{vim} - \frac{\lambda}{m}} \tag{3.1}$$

where λ represents the request rate per second (or transactions per second depending on the context), $\frac{1}{\mu_{nfvo}}$ is the processing time of NFVO, $\frac{1}{\mu_{vim}}$ is that of VIM, and m is the total number of VIMs and WIMs.

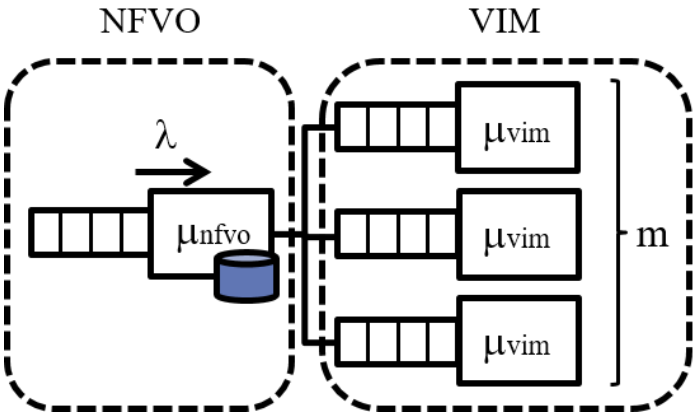


Figure 3.2: Queuing model of the existing protocol.

Figure 3.3 shows the response time, T_{nfvo}, against the request rate, λ, with parameters $\frac{1}{\lambda_{nfvo}} = 90\,ms$, $\frac{1}{\lambda_{vim}} = 10\,ms$, $m = 2$. As shown in these parameter values, much heavier load is imposed on the NFVO in the existing protocol. The horizontal axis indicates the number of transactions per second and the vertical axis shows the average response time in second. The limit of average response time as the transactions per second approaches 30 is infinity. According to [37], the number of operational flows from the NFVO to the VIM is from 10 to 13 in the case of NS among two sites across a WAN. As the number of infrastructure becomes larger than 2, the possibility of request congestion increases because of the large number of operational flows. Thus, the management load of the central-control model is not enough to achieve the NS deployment across multi-provider networks.

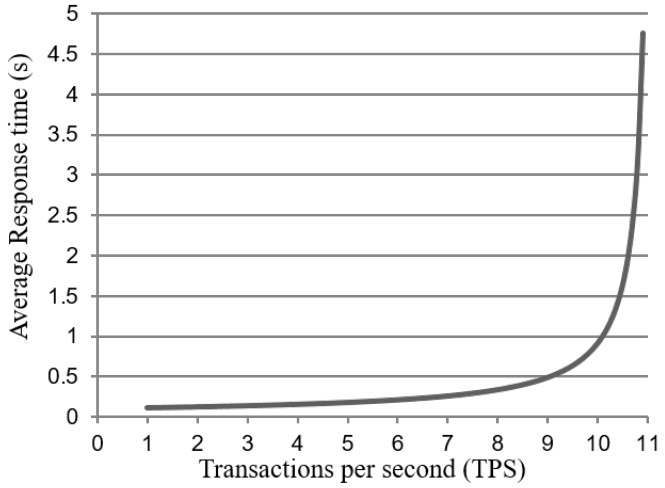


Figure 3.3: Response time in existing protocol.

The reinforcement of the NFVO facility is expected to reduce the management load. In the central-control case, the NC information is provided by the NFVO. Thus, the second term in (1) can be ignored because the processing time of the VIM is negligibly small. The first term in (1) becomes infinity. The transactions per second when the average response time becomes infinity, $\lambda*$, is given as (1), where, h_{nfvo} represents the processing time of the database and I/O at the NFVO.

$$\lambda^* = \mu_{nfvo} = \frac{1}{h_{nfvo}} \tag{3.2}$$

Figure 3.4 shows the number of the transactions per second with the processing time for the central-control model. The horizontal axis indicates the processing time of the NFVO and the vertical axis shows the transactions per second as average response time becomes infinity. If the transactions per second become larger, the faster processing of the NFVO is necessary. However, the reinforcement of facilities increases capital investment costs of service provider.

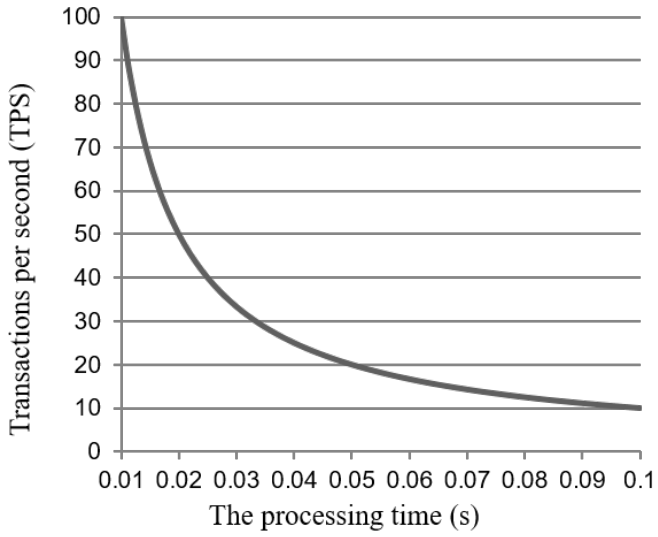


Figure 3.4: The number of the transactions per second with processing time.

3.1.2 Security

If a malicious VIM or WIM sends unexpected NC information, the traffic might be sent to an unexpected route because of the VPN mechanism. Additionally, infrastructure provider needs to prevent NC information leaking. Thus, the key authentication mechanism is needed to provide the NC information to the VIM.

3.1.3 Network Designation

Wrong location designation may cause L2 network loop among multiple infrastructure. According to the ETSI NFV Release 2 specifications, there are two ways to specify the location of a VNF: affinity and anti-affinity groups, and location constraints. The affinity and anti-affinity groups show whether two VNFs are placed in the same site (provider) or not, and the location constraints show the geographic location of the VNF. However, the overlay a L2 network loop might be generated. Figure 3.5 shows issues concerning to wrong designating locations. There are three sites, sites 1, 2, and 3. One pair, VNF 1 and 2, belongs to an anti-affinity group, and another, VNF 2 and 3, also belongs to an anti-affinity group. VNF 1 and 2 are located at site 1 and 2, respectively. When VNF 3 is requested to be deployed from the NFVO, it cannot be created at site 2 because of the anti-affinity group policy. However, VNF 3 might be created at sites 1 or 3 because the VNF 3 is not in the same anti-affinity group with the VNF 1. If the VNF 3 is created in the site 1, the network loop might be generated between the site1 and 2. The three sites are simple to explain, but if there are more sites, it would be difficult to describe an appropriate group for the VNF and the VL. Thus, the designation of appropriate location constraints is important for multiple infrastructure NS.

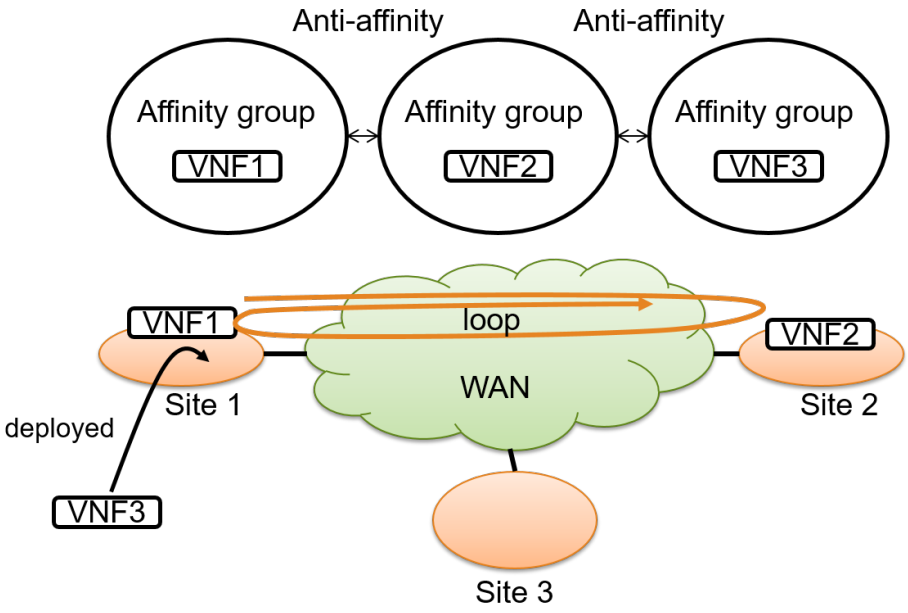


Figure 3.5: Location constraints issues.

3.2 Proposed Scheme

a) Network Information Exchange scheme

My proposal is a multisite NFV architecture for reducing the management load. Figure 3.6 shows the proposed scheme. The NFVO provides abstract network and policy information to the VIMs and WIMs in the Management plane (M-plane), and the VIMs and WIMs compute the detailed routing information. The NFVO specifies the virtual resources to be allocated by the VIM through the policy information. This information is also used to control the routing policy with respect to each NS, such as the acceptable bandwidth and delay. In my proposal, the VIM exchanges the NC information of the gateway nodes among the VIMs and WIMs.

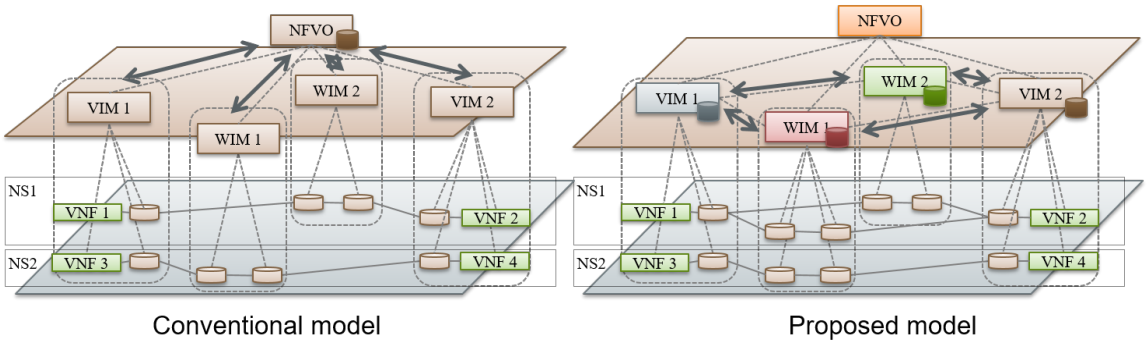


Figure 3.6: Proposed scheme coodinating across multiple DC.

Figure 3.7 shows the sequence for NS creation. The NFVO requests and receives the network topology and capabilities from the VIMs and WIMs in advance, and it creates an NC map among infrastructures. The NC map is NC information for managing the network topology and the capabilities among multiple infrastructures. The NFVO allocates relative NC-identifiers (NC-IDs) that identify NCs among DCs and WANs. If the NFVO receives a request for NS creation, the NFVO requests resource allocation to the VIMs and WIMs. The NFVO provides the NC-ID to the VIMs and WIMs. Then the VIMs and WIMs allocate resources for VNFs and the network resources of intra DC networks and WANs. Then, the VIMs or WIMs that connects to other VIMs and WIMs exchange NC-IDs. If exchanged NC-ID is the same as the ID provided by the NFVO, the VIMs and WIMs exchange NC information among VIMs or WIMs. Then, the VIMs and WIMs configure GW nodes among DCs and WANs by using the NC information. As a result, NS is created.

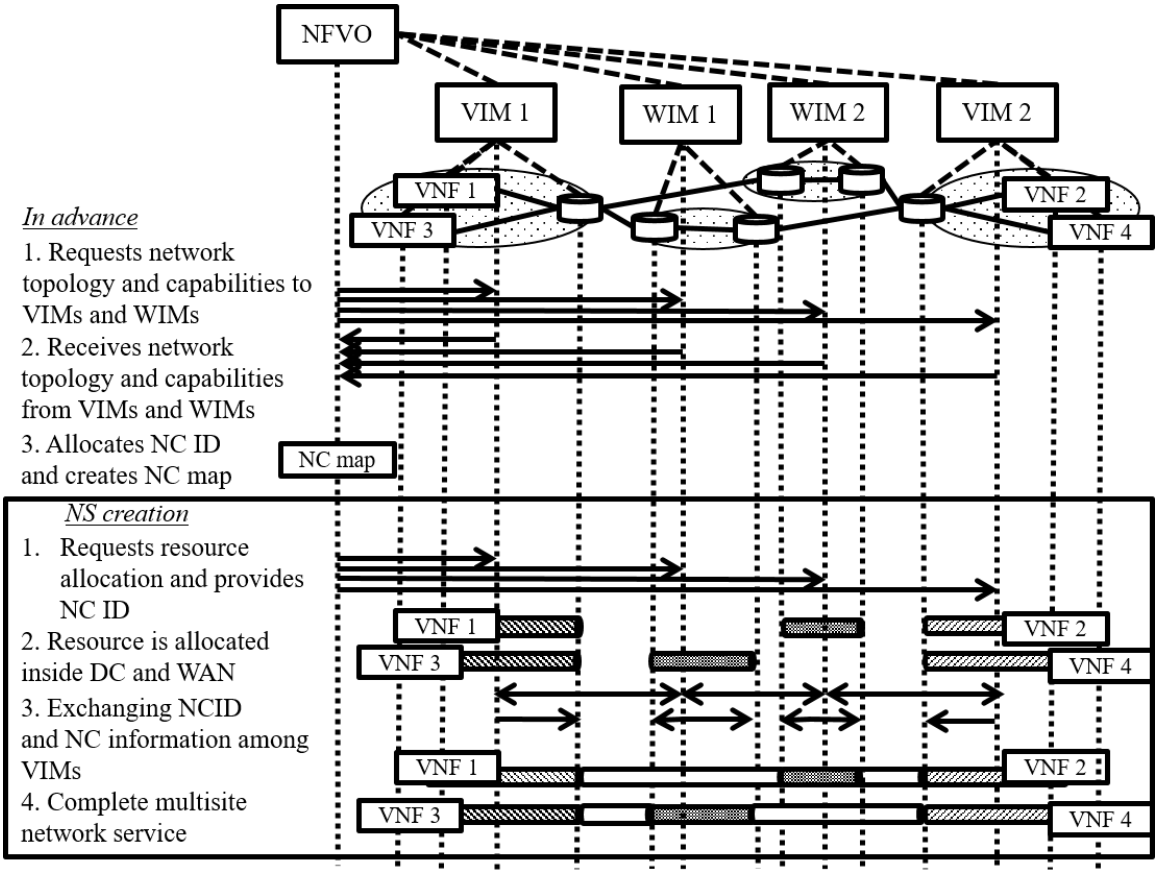


Figure 3.7: NS creation sequences.

b) Simulation Evaluation

Figure 3.8 shows the queuing model of the proposed scheme. The processing times of the VIMs and WIMs are treated as the same for sake of simplicity. In my proposal case, the NFVO queries the resource allocation to the VIM or WIM, which has the

NC database. The VIM allocates network resources and replies to the NFVO.

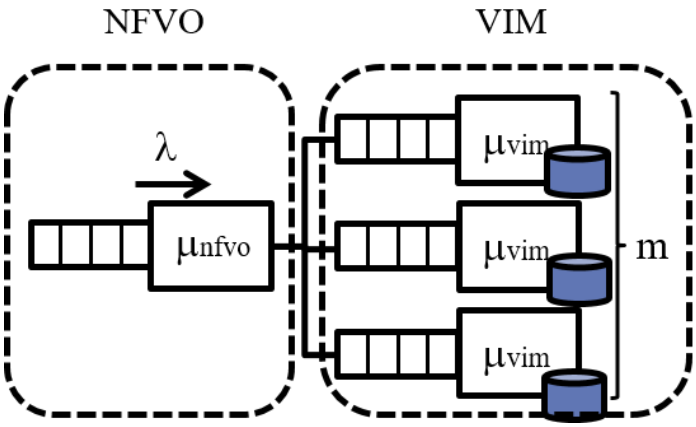


Figure 3.8: Queuing Model of proposed scheme.

In my proposal scheme, the NC information is provided by the VIM or WIM. Thus, the first term in (1) can be ignored because the processing time of the NFVO is negligibly small. The second term in (1) becomes infinity. The transactions per second as the average response time becomes infinity, $\lambda*$, is given as (1), where, h_{nfvo} represents the processing time of the database and I/O at the VIM or WIM.

$$\lambda^*|m \times \mu_{vim} = \frac{m}{h_{vim}} \tag{3.3}$$

Figure 3.9 shows the number of transactions per second with processing time for the central-control model and proposed scheme when m is equals to 2. The horizontal axis indicates the processing time of the NFVO and the vertical axis shows the transactions per second as average response time becomes infinity. My proposed scheme can reduce the transactions per second as the average response time becomes infinity.

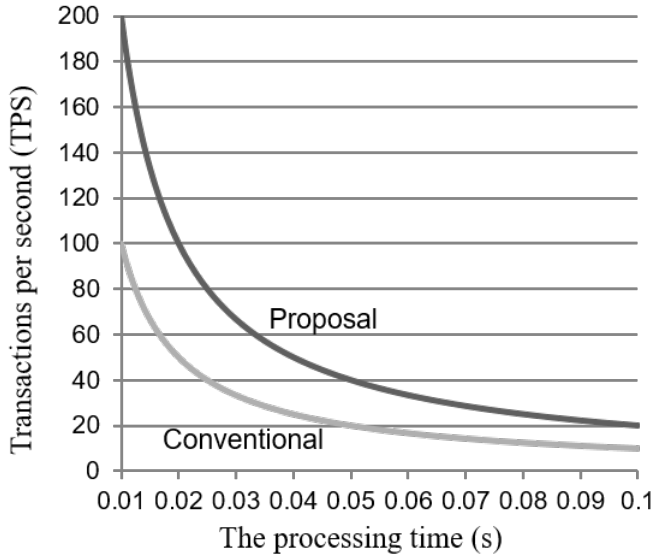


Figure 3.9: The number of the transactions per second with processing time for central-control model and proposed scheme.

Figure 3.10 shows the number of transactions per second with the number of VIM and WIMs. The horizontal axis indicates the number of VIMs and WIMs and the vertical axis shows the number of transactions per second as the response time becomes infinity. When the number of VIMs is larger, the number of transactions per second as the response time becomes infinity is longer.

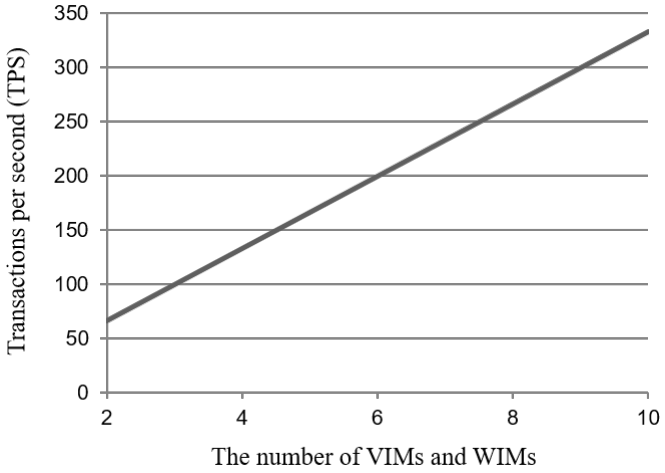


Figure 3.10: The number of transactions per second when average response time diverges.

3.2.1 Route for Exchanging Network Information

As described in the Section, exchanging configuration information among the VIMs and WIMs can achieve efficient operation. However, no official interface is available for exchanging configuration management information among VIMs and WIMs in the ETSI NFV standard [37]. Thus, an alternative way to exchange the required information for the edge nodes is conceived. In this section, I compare three routes to exchange messages in Figure 3.11 as given hereafter.

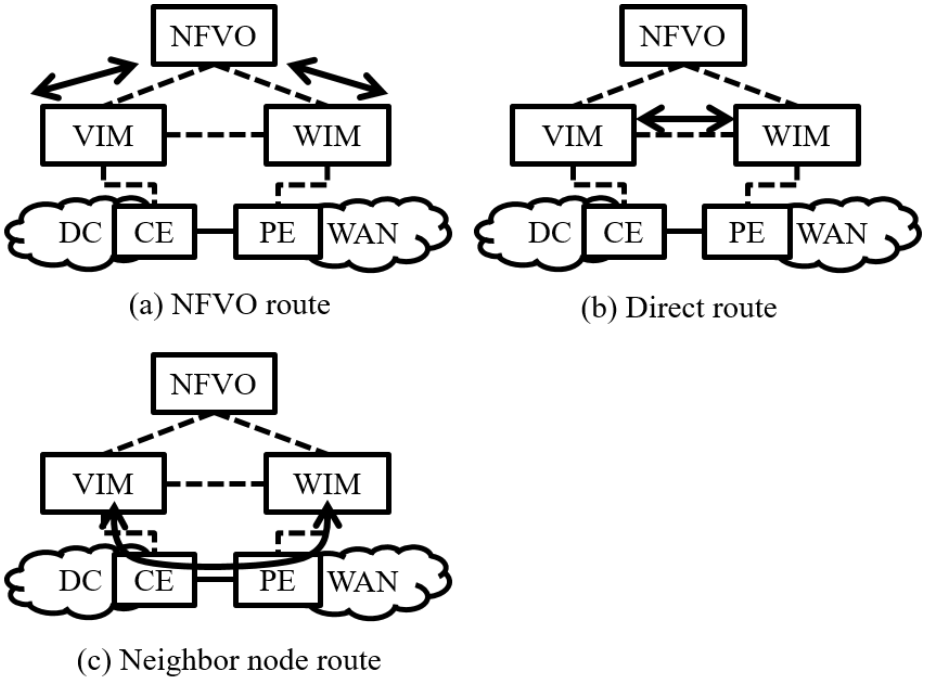


Figure 3.11: Exchange route for configuration information for VIM and WIM.

a) NFVO route a route through the NFVO

b) Direct route a route that directly connects the VIM and WIM

c) Neighbor node route a route through a link between the edge nodes

I evaluate the advantages and disadvantages of the three routes from the aspects of scalability, operation, and security.

a) Scalability

For a NFVO route, the NFVO receives a message from one VIM/WIM and forwards the message to its counterpart VIM/WIM. If the NFVO receives many queries, the load on the NFVO is concentrated. On the other hand, for a direct route, the communications between the VIM and WIM are independent of the load on the NFVO. For the case of a neighbor node route, because the exchange route of the

configuration information overlaps the user traffic in the data plane (D-plane), traffic management such as the Quality of Service (QoS) is required to prevent packet loss of the user data.

b) Operation and Management

In the case of a NFVO route, the NFVO exchanges the configuration management information through the NFVO route. Since the configuration information is private information of the infrastructure provider, the NFVO requires technology to prevent the leakage of information and mutual authentication among the NFVO and VIMs. For the case of the neighbor node route, the probability that the information will be leaked is low because of the independent communications route. For the case of the direct node, it is not realistic to establish a connection among multiple operators because the C-plane must be connected to the VIM and WIM.

Table 3.1 shows comparison results related to the exchange routes. If the management DB is located on the NFVO side, the NFVO route is suitable. If the management DB is located on the VIM side and the infrastructure is provided by multiple operators, the NFVO route or the neighbor node route is suitable. If the infrastructure is provided by a single operator, all of routes are available.

Table 3.1: Comparison results based on aspects of exchange route.

Items	NFVO route	Direct route	Neighbor node route
Scalability	Load of NFVO is concentrated	Good	Configuration of QoS is required
Operation and management	Does not affect service	Does not affect service	Does not affect service
Security	Information filtering technologies and authentification technologies are required	Control plane connection is required	Multiple operators can use this route by using VPN connection
Application	- NFVO side - Single or multiple operators	- VIM side - Single operators	- VIM side - Single or multiple operators

3.2.2 Protocols Extension for Neighbor Route

The verification and repairing scheme for NC among multiple infrastructures is needed [37]. I propose the use of BGP for exchanging NC information among VIMs and WIM to collect the NC information among multi-sites over WANs. Figure 3.12 shows the BGP connection for the Management-plane (M-plane). The BGP is enhanced

for distributing the NC information to external entities. When the NFVO requests resource allocation, the NFVO provides public VPN key for creating VPN connection for exchanging NC information. Then a VIM and WIM create M-plane VPN by using the VPN key. Then a VIM and WIM speak the BGP and create the BGP session between the VIM pairs. The BGP session passes through a link between gateway nodes at a DC and WAN. The VIMs and WIMs exchange parameters among the VIMs. Then VIMs and WIMs create C-plane BGP. Additionally, M-plane BGP is possible to verify and repair the NC between gateway nodes. Thus, the VIMs and WIMs can exchange NC information among VIMs and WIMs by using M-plane BGP.

Additionally, double key authentication mechanism used among the NFVO and VIMs is introduced for the proposed scheme. The NFVO receives NS creation request and sends network information to VIMs, namely VPN keys, and VPN information. The VPN information is encrypted by using the keys of the NFVO and the counterpart VIMs. Encrypted VPN information to the corresponding VIM is exchanged between VIM and WIM along with NC-ID information. If the counterpart VIM can decrypt VPN the information by using the VPN keys provided by the NFVO and their own key. Then the VIMs can exchange NC information with the counterpart VIMs. This mechanism prevents NC information leaking to malicious VIM and creates a secure connection among VIMs on a per NS basis.

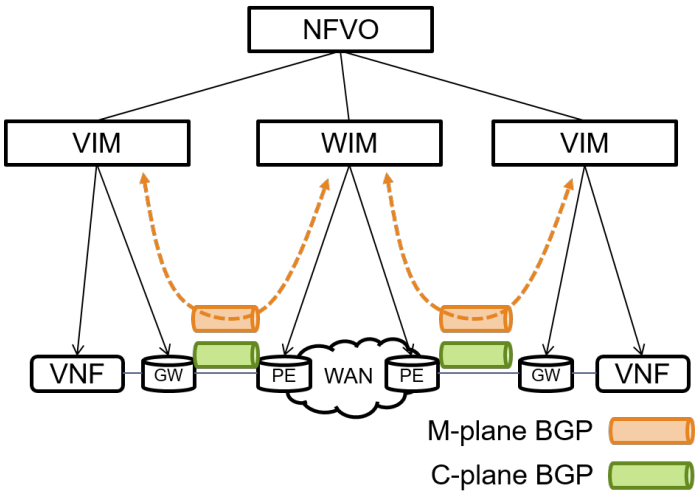


Figure 3.12: BGP connection for M-plane.

3.2.3 Descriptor Extension for Designating Location

The NFVO needs to create the data structure to provide NC information among multiple infrastructures in my proposal. Additionally, service providers need to control location of VNF in aspect of business continuity and low latency. However, the existing protocol cannot designate location by service provider as shown in section 2.1. Figure 3.13 shows the data structure that I call the NC map and the designation of location from a service provider. The NC map comprises of the availability zone and capabilities of DC and WANs.

The NC map also has NC information allocated by the NFVO, and underlay and overlay connectivity. The new descriptor, namely the NS Based infrastructure Descriptor (NSBD), is on-boarded by service provider to the NFVO in advance by using NSD. The NSBD has the combination information of the DC and the WAN and policy information. When the service provider requests the NS provisioning, the NFVO selects the NC which can satisfy the policy by using NC map. Then NFVO creates NS. If the infrastructure provider changes the location of DC, the provider doesn't need to change the available zone because the available zone is abstracted information. And if the infrastructure provider terminates the service, another infrastructure provider can satisfy the policy based on NSBD. The available zone can take over to another infrastructure provider.

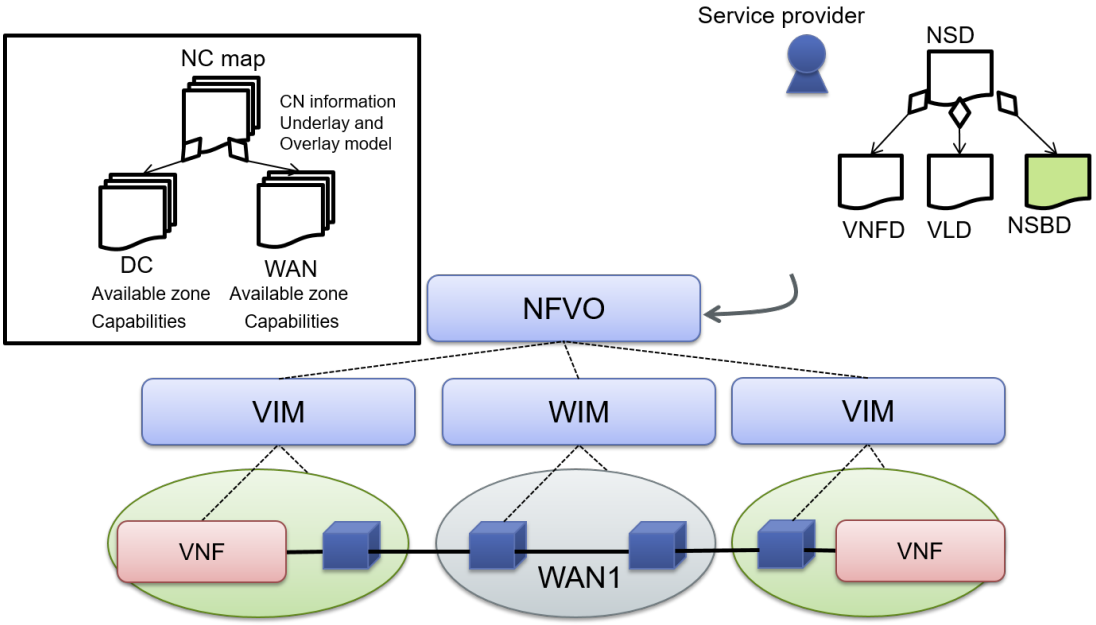


Figure 3.13: Location constraints from service provider.

Figure 3.14 is an example of the NSBD. The infrastructure deployment flavor shows whether the NC map is created automatically or manually. The priority parameter of WAN is used to select WAN. If the location or WAN is changed for site migration, relationship between infrastructure deployment flavor class and site class is terminated and switched to another site class.

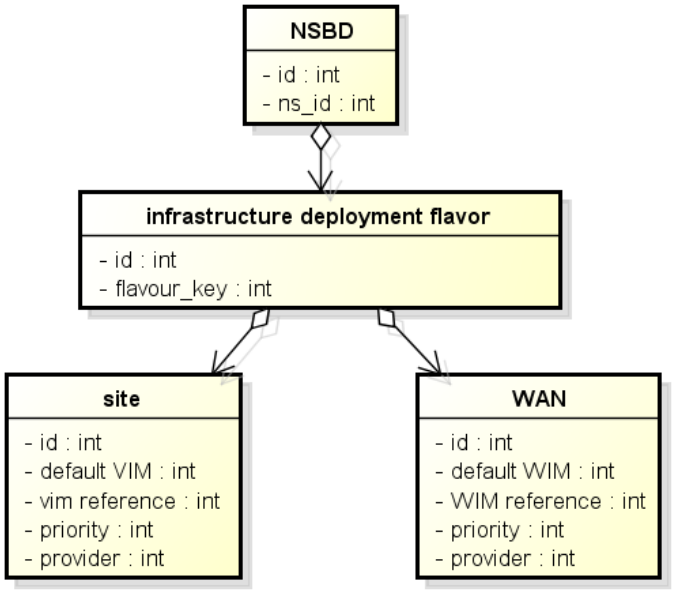


Figure 3.14: Example of NSBD.

3.2.4 Experimental Evaluation

The NC information should be verified to determine what kind of protocols is exchanged among multiple VIMs and WIMs to achieve proposed scheme. Figure 3.15 shows the emulated experimental environments. A BGP/ MPLS-VPN was used for connecting different autonomous domains. Figure 3.15 (a) shows the provider edge routers (PEs) and customer edge routers (CEs) used the experiments. The PEs and CEs were created in a virtual container by using a RYU BGP speaker [66] and Lagopus switches [67]. Figure 3.15 (b) shows an environment used to verify the parameters for exchanging among multiple infrastructures. PC1 and PC2 are Ubuntu-based PCs. The network environment was created by using virtual container technology in a single server. Multi-protocol BGP (MP-BGP) can use network resources efficiently among multi-domain networks [68]. Figure 3.16 shows the packet capture of the MP-BGP update message from BGP3 to BGP4 in Figure 3.15 (a). In this experiment, the MPLS label was set to 300 at BGP3 in *MP_REACH_NLRI*. The export route target (RT) of BGP 3 is set to 65010:101. If the import RT of the virtual routing and forwarding (VRF) at BGP4 is same as the export RT at BGP3, this route is rerouted to the VRF. In MP-BGP, the PE redistributed labeled VPN-IPv4 routes that connect to the VRF. As a result, dynamic routing is possible by using the MP-BGP. Figure 3.15 (c) shows the environment used to verify parameters for exchanging among multiple VIMs. A static route was used for connectivity among CE1 and PEs at sites 1 and 2. Internal BGP (iBGP)/MPLS-VPN was used for the sites internal connectivity between the PEs. External BGP (eBGP)/ MPLS-VPN were used for site-to-site and site-to-WAN connectivity between PEs. The local preference value was used to select WANs on a per NS basis. The local preference values from PE1 to PE2 and CE1 and that from PE2 to PE1 and CE1 at site 1 were set to 200 and 100, respectively. The

local preference values from PE7 to PE8 and CE2 and that from PE8 to PE7 and CE2 at site 2 were set to 200 and 100, respectively.

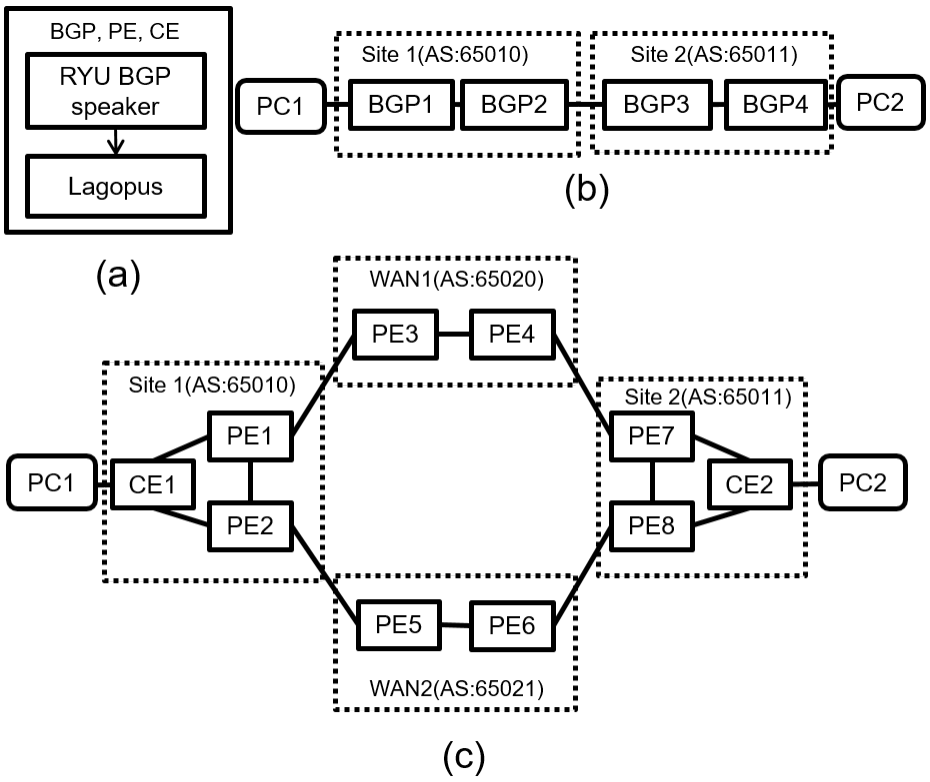


Figure 3.15: Experimental environment.

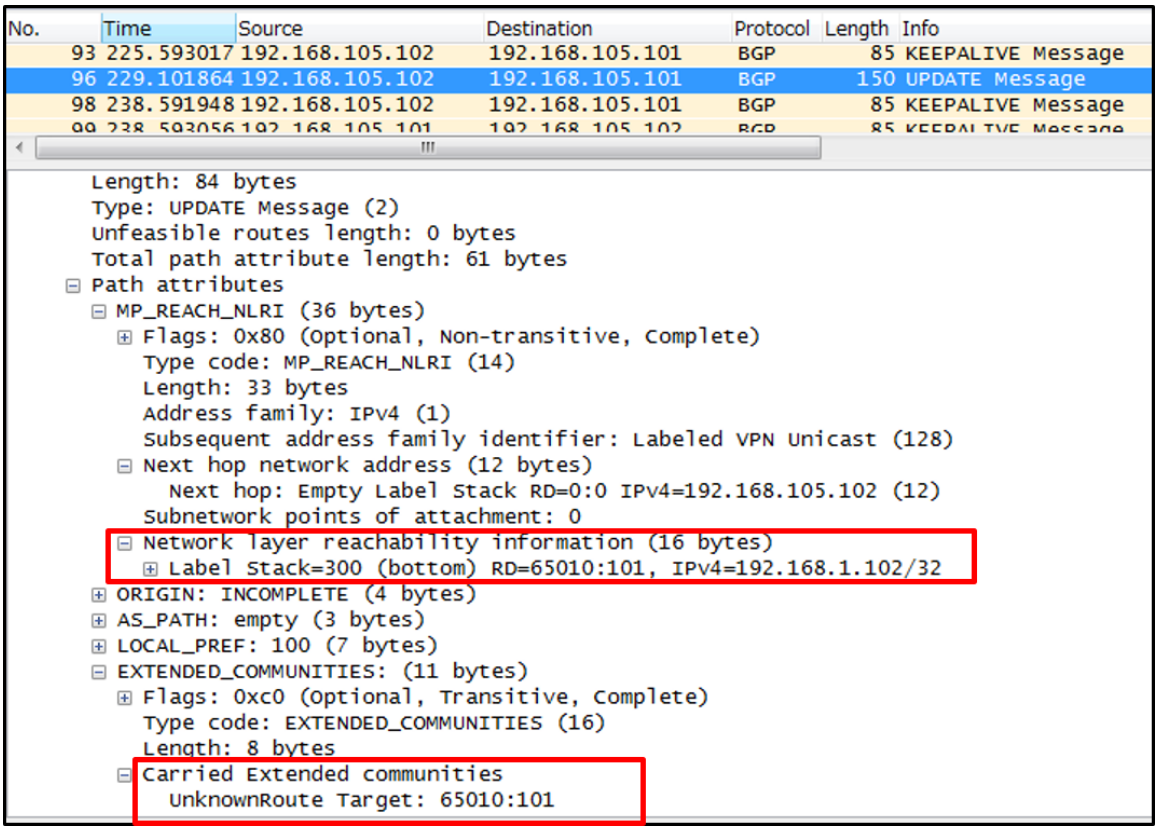


Figure 3.16: Packet capture of MPBGP update message.

Figure 3.17 shows the parameters for achieving multisite NFV across WANs. The external RT and internal RT are needed to be the same among the sites and WANs and the IP address of each neighboring PE is needed to be configured by the BGP.

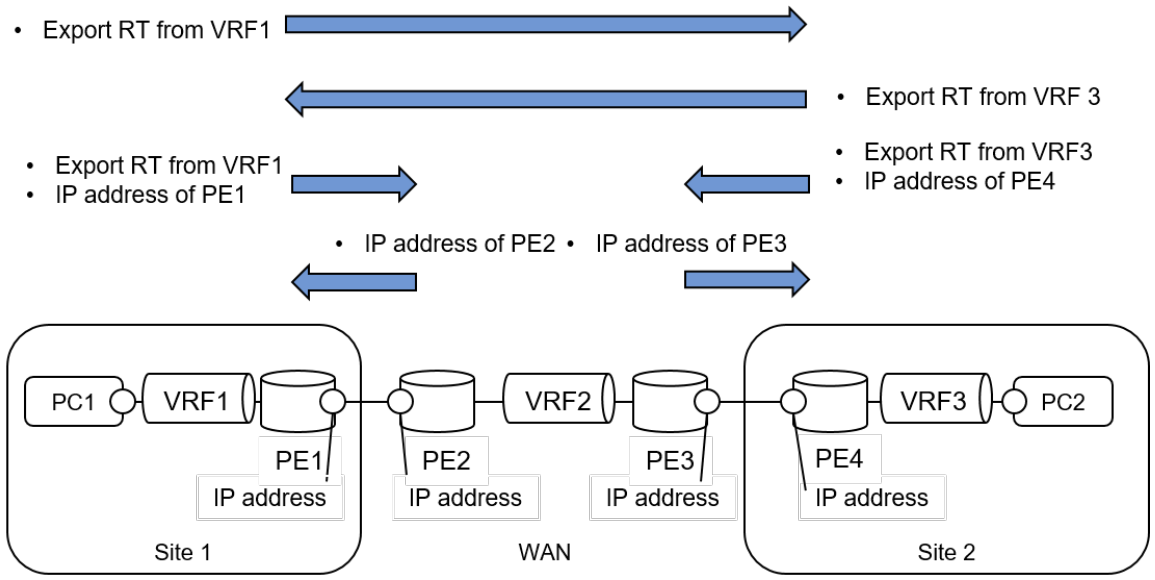


Figure 3.17: Exchange parameters for my proposed scheme..

Figure 3.18 shows an example of a message sequence for this use case. The NFVO provides VIMs and a WIM with the information of the VPN tag (xyz) and a list of their adjacent managers such as VIM or WIM. VIM1 or VIM2 creates a VPN for xyz and configures the neighboring IP addresses, RDs, and external RT. Then, the VIM1 notifies the VPN and external RT information to WIM1. Also, VIM2 notifies the VPN tag (xyz) and external RT information to WIM1. WIM1 validates the VPN tags and modifies the import RTs. Then, it notifies the tags and external RT information to the VIMs.

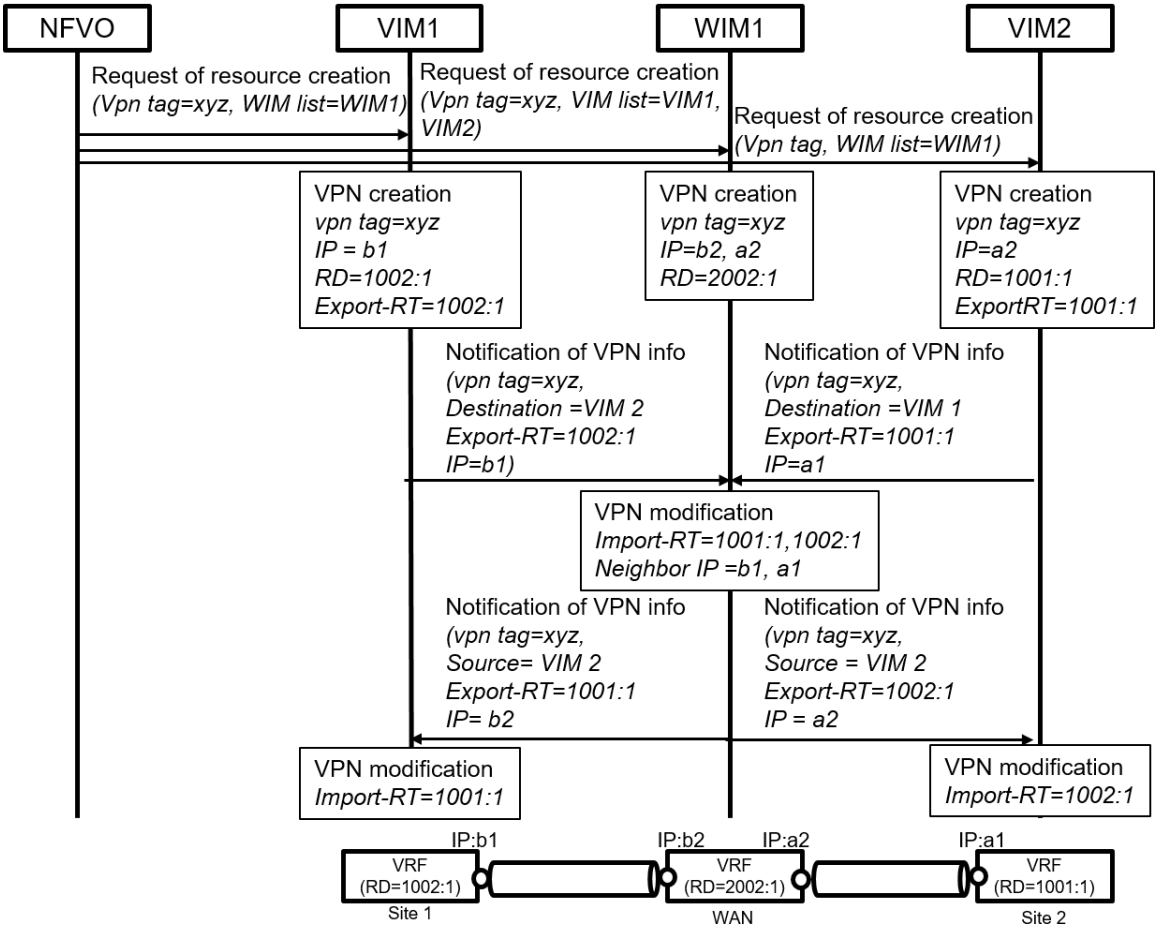


Figure 3.18: Sequence for this use case.

When the VIM receives a request for NW deletion from the NFVO, the VIM or WIM deletes the VRF and exchanges the updated RT information and the number of the RDs with its counterpart VIM or WIM. Thus, the NC information necessary to achieve my proposed scheme is verified for the NS creation over multi-provider networks.

3.3 Proposal to ETSI NFV Release 3 Specifications

My proposed mechanism allows network parameters to be exchanged among inter-VIMs with maintaining intra-network privacy for controlling the dynamic path between multiple domains. My proposed feature is presented as an implementation example rather than a the ETSI NFV Release 3 specifications. This section is taken from the ETSI NFV IFA 022 [37] appendix text proposed by the author as an implementation example.

3.3.1 Case 1: Extending a VLAN Network across WAN

3.3.1.0.1 Overview

In this case, WIM provides L2 connectivity service which connects two or more sites transparently. There are several technologies to establish L2 WAN connectivity (e.g. L2-VPN using MPLS), and this case is not limited to a particular technology. However, this case assumes that VLAN (IEEE 802.1q [69]) is used for interfaces between the WAN and an NFVI-PoP to establish NFVI-PoP connectivity. Figure 3.19 shows an overview of extending a VLAN network across WAN. The WIM allocates a virtualized network resource #2 which the WAN connectivity is mapped to. In this case, VLAN ID=id_2 is assigned to access the WAN connectivity, that is, Ethernet frames transferred between a network gateway and a PE node are tagged with the VLAN ID= id_2. The VIMs allocate virtualized network resources within a NFVI-PoP. The virtualized network resources are also mapped to a VLAN network, which in this case VLAN ID= id_1 for NFVI-PoP#1 and VLAN ID= id_3 for NFVI-PoP#2. To properly interconnect the virtualized network resource at the WAN and the virtualized network resources at the NFVI-PoPs, the VIMs configure the network gateways such that the network gateways can translate the VLAN ID of incoming/outgoing Ethernet frames. For example, the network gateway at NFVI-PoP#1 translates the VLAN ID of incoming traffic from id_2 to id_1. Similarly, the network gateway at NFVI-PoP#1 translates the VLAN ID of outgoing traffic from id_1 to id_2.

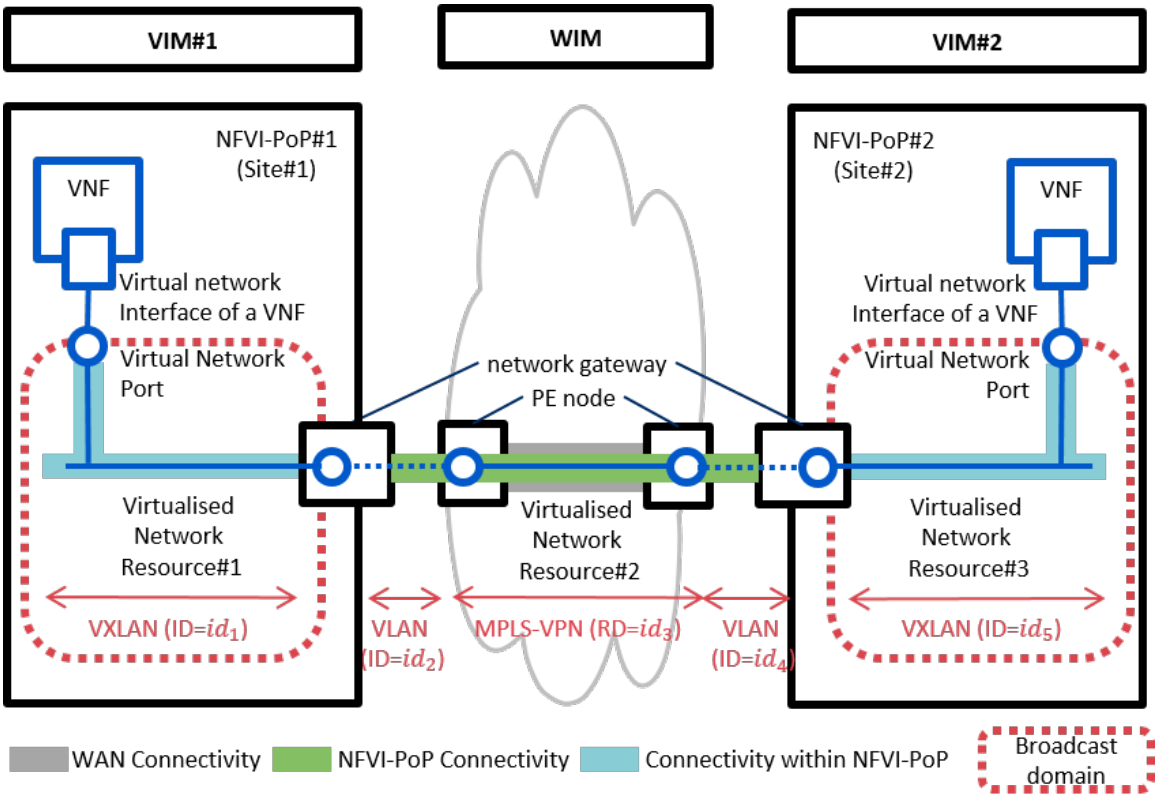


Figure 3.19: Overview of extending a VLAN network across WAN.

3.3.1.1 Properties of virtual network resources

The virtualized network resources at WAN, NFVI-PoP#1 and NFVI-PoP#2 are characterized as shown in Table 3.2. These properties are exchanged between NFVO and WIM/VIM through the Or-Vi reference point.

Table 3.2: Properties of virtualized network resources for case 1.

Virtualized Network Resource	Attribute	Example Value	Description
WAN	Connectivity type	Ethernet and Mesh	See ConnectivityType information element in clause 6.5.3 in ETSI GS NFV-IFA 014 [49].
	Network type of WAN connectivity	l2-vpn	The type of network of the WAN connectivity that maps to the virtualized network. In this case, it is L2-VPN using MPLS. See also attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Network type of NFVI-PoP connectivity	vlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Segment type	id_2	vlan identifier. See also attribute segmentType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Is shared	False	This attribute represents whether the network is shareable (for aggregation). In this case, the network is not shareable. See also attribute isShared of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
NFVI-PoP#1	Network type	vlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].

Continued on next page.

Table 3.2: Properties of virtualized network resources for case 1.

Virtualized Network Resource	Attribute	Example Value	Description
	Segment type	id_1	vlan identifier. See also attribute segmentType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
NFVI-PoP#2	Network type	vlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Segment type	id_3	vlan identifier. See also attribute segmentType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].

Finished.

3.3.1.2 Operational flow

Table 3.3 shows the operational flow for this case. It follows BF#1.1 of use case #1 in section 2.1, so Table 3.3 shows only additional description specific for this case.

Table 3.3: Operational flow (based on BF#1.1 of use case #1).

#	Flow	Description
1	OSS/BSS → NFVO	See step 1 of BF#1.1 of use case #1 in section 2.1.
2	NFVO	See step 1 of BF#1.1 of use case #1 in section 2.1.

Continued on next page.

#	Flow	Description
3	NFVO → WIM	See step 3 of BF#1.1 of use case #1 in section 2.1. In this case, the following information is passed to the WIM; • NFVI-PoPs to be connected: NFVI-PoP#1 and NFVI-PoP#2; • Connectivity type: Ethernet and Mesh; • Is shared: False; and • QoS and bandwidth information.
4	WIM → Network Controller	See step 4 to 6 of BF#1.1 of use case #1 in section 2.1. L2 WAN connectivity between the PE nodes at WAN is established for the virtualized network resource#2. Then, NFVI-PoP connectivity is prepared so that the L2 WAN network connectivity is accessible with VLAN ID= id_2 from the NFVI-PoPs. .
5	Network Controller	
6	Network Controller → WM	
7	WIM → NFVO	See step 7 of BF#1.1 of use case #1 in section 2.1. The WIM returns an indication of the network port of the WAN and VLAN ID= id_2 as information for connecting to the WAN.
8	NFVO → VIM at Site#1	See step 8 of BF#1.1 of use case #1 in section 2.1. In this case, the following information is passed to the VIM: • Information for connecting to the WAN: an indication of the network port of the WAN and VLAN ID= id_2; and • QoS and bandwidth information.
9	VIM at Site#1	See step 9 of BF#1.1 of use case #1 in section 2.1. According to the input parameters at step 8, the VIM creates the virtualized network resource#1. A VLAN network is established for the virtualized network resource#1. The VLAN ID of the network is id_1. The network gateway is configured for VLAN ID translation, i.e. the VLAN ID of incoming traffic is translated from id_2 to id_1, and the VLAN ID of outgoing traffic is translated from id_1 to id_2.
10	VIM at Site#1 → NFVO	See step 10 of BF#1.1 of use case #1 in section 2.1. The VIM returns the identifier of the virtualized network resource. The identifier will be used to attach virtual network ports to be connected with a virtual network interface of a VNF.

Continued on next page.

#	Flow	Description
11	NFVO → VIM at Site#2	See step 11 of BF#1.1 of use case #1 in section 2.1. In this case, the following information is passed to the VIM: • Information for connecting to the WAN: an indication of the network port of the WAN and VLAN ID= id_2; and • QoS and bandwidth information.
12	VIM at Site#2	See step 12 of BF#1.1 of use case #1 in section 2.1. According to the input parameters at step 11, The VIM creates the virtualized network resource#3. A VLAN network is established for the virtualized network resource#3. The VLAN ID of the network is id_3. The network gateway is configured for VLAN ID translation, i.e. the VLAN ID of incoming traffic is translated from id_2 to id_3, and the VLAN ID of outgoing traffic is translated from id_3 to id_2.
13	VIM at Site#2 → NFVO	See step 13 of BF#1.1 of use case #1 in section 2.1. The VIM returns the identifier of the virtualized network resource. The identifier will be used to attach virtual network ports to be connected with a virtual network interface of a VNF.
14	NFVO	See step 14 of BF#1.1 of use case #1 in section 2.1.
15	NFVO → OSS/BSS	See step 15 of BF#1.1 of use case #1 in section 2.1.

Finished.

3.3.1.3 Considerations

Distributed control and centralized control in VLAN ID assignment

In this case, each of the VIMs and the WIM independently assigns VLAN ID to virtualized network resources. As a result, VLAN IDs of the virtualized network resources for a VL can be different from each other. Alternatively, it is also possible that NFVO manages a pool of VLAN IDs which are commonly used among multiple NFVI-PoPs and a WAN, and assigns a single VLAN ID to the virtual network resources for a Virtual Link. In that case, the NFVO sends the VLAN ID selected by the NFVO for a VL to the WIM and the VIMs at step 3, 8 and 11 in Table 3.3 respectively.

Supporting L3 connectivity services

It is possible to enable L3 connectivity services such as DHCP on a VL which is instantiated according to the operational flow shown in Table 3.3. To enable it, additional steps are necessary for VIM#1 and VIM#2 to create a virtualized sub-network and associate it with the virtualized network resource created at step 9 or 12 of the operational flow. As described in clause 8.4.5.3 in ETSI GS NFV-IFA

005 [51], the virtualized sub-network is used to specify properties for L3 connectivity services. Because the virtualized network resources at VIM#1 and VIM#2 belong to the same broadcast domain, the L3 related parameters of the virtualized sub-networks need to be the same between VIM#1 and VIM#2.
If DHCP is enabled, it needs to assign IP addresses without overlapping between the two sites. It is FFS how to achieve it.

3.3.2 Case 2: EVPN Connection with Inter-AS among NFVI-PoPs

3.3.2.1 Overview

In this use case, the network of NFVI-PoP and WAN provide EVPN-VXLAN- and EVPN-MPLS, respectively. The NFVI-PoPs and WAN are connected by the Inter-AS option B as described in the Internet Engineering Task Force (IETF) RFC 4364 [52] and are managed by independent domains. The EVPN, which is standardized in IETF RFC 7432 [57], can advertise information of L2 (MAC) and L3 (IP) through MP-BGP. The EVPN has many benefits for efficiency, reliability, scalability, etc. on network operations. Additionally, The MPLS based network provides standard-based management tools and technologies, namely MPLS MPLS-OAM, traffic management, and QoS. By using the EVPN connection, the VNFs can communicate to each other within the same L2 broadcast domain across WAN. Figure 3.20 shows an overview of EVPN connection with Inter-AS option B among the NFVI-PoPs across WAN. In this case, The NFVI-PoP#1, NFVI-PoP#2 and WAN belong to different administrative domains. The network gateway#1 and #2 show ASBR for connecting ASes. The Ethernet frames which are sent from VNF#1 are labelled by RD which is part of destination network address, namely id1, and encapsulated by VXLAN header, namely id4 to isolate from other networks within NFVI-PoP#1. At the network gateway at NFVI-PoP#1, VPN information are exchanged from NFVI-PoP#1 domain to WAN domain by using eBGP. Then RD is re-labelled from id1 to id2 and re-encapsulated by MPLS header. Then VPN packets are transferred to NFVI-PoP#2 domain following target RT information at WAN. And at the network gateway at NFVI-PoP#2, VPN-information are distributed from WAN to NFVI-PoP#2 by using e-BGP. Then RD is re-labelled from id2 to id3, and re-encapsulated by VXLAN header, namely id5. As a result, VNF#1 of NFVI-PoP#1 and VNF#2 of NFVI-PoP#2 can communicate with each other.

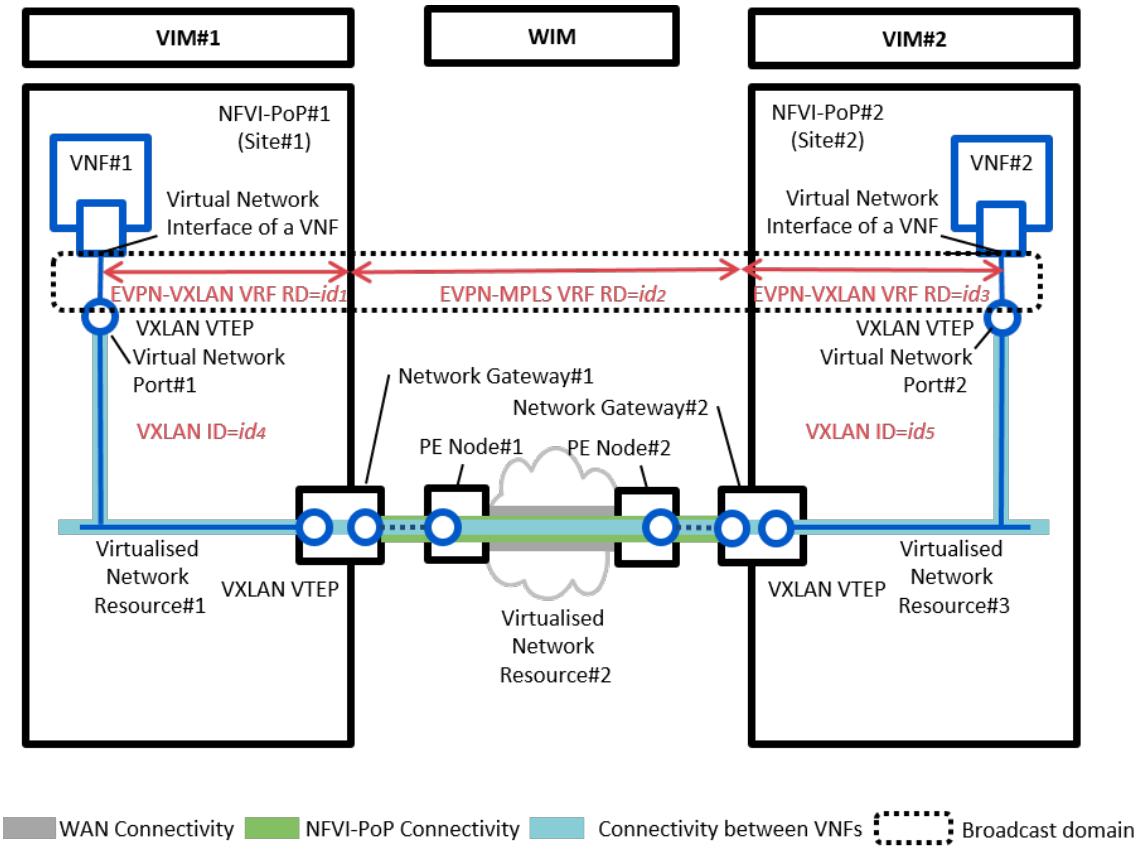


Figure 3.20: Overview of EVPN connection with Inter-AS among NFVI-PoPs.

3.3.2.2 Properties of virtual network resources

The virtualized network resources at WAN, NFVI-PoP#1 and NFVI-PoP#2 are characterized as shown in the Table 3.4. These properties are exchanged between NFVO and WIM/VIM through the Or-Vi reference point.

Table 3.4: Properties of virtualized network resources for case 2.

Virtualized Network Resource	Attribute	Example Value	Description
WAN	Connectivity type	MPLS and Mesh	See ConnectivityType information element of the NS Virtual Descriptor in clause 6.5.3 in ETSI GS NFV-IFA 014 [49].

Continued on next page.

Table 3.4: Properties of virtualized network resources for case 2.

Virtualized Network Resource	Attribute	Example Value	Description
	Network type for WAN connectivity	l2-vpn	The type of network for the WAN connectivity that maps to the virtualized network. In this example, it is Ethernet over MPLS. For details, see attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Network type for NFVI-PoP connectivity	evpn-mpls	The type of network for the NFVI-PoP connectivity that maps to the virtualized network. In this example, it is EVPN-MPLS. See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	Segment type for NFVI-PoP connectivity	id_2	This attribute indicates VRF RD for EVPN-MPLS at WAN. This attributes provided by WIM and is unchangeable from NFVO. IP packets through MPLS-VPN are encapsulated by VRF-RD. See also attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	Is shared	True	This attribute indicates whether the network is shareable (for aggregation among VLs) or not. In this use case, the network is shareable. See also the attribute isShared of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].

Continued on next page.

Table 3.4: Properties of virtualized network resources for case 2.

Virtualized Network Resource	Attribute	Example Value	Description
NFVI-PoP#1	Network type for connectivity within NFVI-PoP	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Segment type for connectivy within NFVI-PoP	id_4	This attribute indicates VXLAN ID within NFVI-PoP #1. This attributes provided by VIM#1 and is unchangeable from NFVO. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Network type for NFVI-PoP connectivity	evpn-vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Segment type for NFVI-PoP connectivity	id_1	This attribute indicates VRF RD for EVPN-VXLAN at Site#1. This attributes provided by VIM and is unchangeable from NFVO. IP packets through VXLAN-VPN are encapsulated by VRF-RD. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
NFVI-PoP#2	Network type for connectivity within NFVI-PoP	vxlan	SSee attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].

Continued on next page.

Table 3.4: Properties of virtualized network resources for case 2.

Virtualized Network Resource	Attribute	Example Value	Description
	Segment type for connectivity within NFVI-PoP	id_5	This attribute indicates VXLAN ID within NFVI PoP #2. This attributes provided by VIM#2 and is unchangeable from NFVO. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	Network type for NFVI-PoP connectivity	evpn-vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Segment type for NFVI-PoP connectivity	id_3	This attribute indicates VRF RD for EVPN-VXLAN at Site#2. This attributes provided by VIM and is unchangeable from NFVO. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].

Finished.

3.3.2.3 Operational flow

Table 3.5 shows the operational flow for this case. It follows BF#1.2 of use case #1 in section 2.1, so that Table 3.5 shows only additional descriptions specific for this case.

Table 3.5: Operational flow (based on BF#1.2 of use case #1).

#	Flow	Description
1	OSS/BSS → NFVO	See step 1 of BF#1.2 for use case #1 in section 2.1.
2	NFVO	See step 1 of BF#1.2 for use case #1 in section 2.1.

Continued on next page.

#	Flow	Description
3	NFVO → WIM	See step 3 of BF#1.2 for use case #1 in section 2.1. See note. In this case, the following information are provided to the WIM; • Connectivity type: MPLS and Mesh; • NFVI-PoPs to be connected: NFVI-PoP#1 and NFVI-PoP#2; • Network type for WAN connectivity: l2-vpn; • Network type for NFVI-PoP connectivity: evpn-mpls; • Is shared: True; and • QoS and bandwidth information.

Continued on next page.

#	Flow	Description
4	WIM → Network Controller	See step 4 to 6 of BF#1.2 for use case #1 in section 2.1. See note. EVPN-MPLS between the PE node#1 and PE node#2 is established as virtualized network resource#2. The WIM allocates VRF RD for the EVPN-MPLS, namely id_2 to itself. .
5	Network Controller	
6	Network Controller → WM	
7	WIM → NFVO	See step 7 of BF#1.2 for use case #1 in section 2.1. The WIM returns an indicatifier of virtualized network resource#2 and VRF RD, namely id_2.
8	NFVO → VIM#1	See step 8 of BF#1.2 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#1: • Network type for connectivity within NFVI-PoP: vxlan; • Network type for NFVI-PoP connectivity: evpn-vxlan.
9	VIM#1	See step 9 of BF#1.2 for use case #1 in section 2.1. According to the attributes of step 8, the VIM#1 creates EVPN-VXLAN as the virtualized network resource#1. The VIM#1configures id_1. to its own VRF RD.
10	VIM#1 → NFVO	See step 10 of BF#1.2 for use case #1 in section 2.1. The VIM returns identifiers of the virtualized network resource #1and VRF RD, namely id_1.
11	NFVO → VIM#2	See step 11 of BF#1.2 of use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#2: • Network type for connectivity within NFVI-PoP: vxlan; • Network type for NFVI-PoP connectivity: evpn-vxlan.
12	VIM#2	See step 12 of BF#1.2 for use case #1 in section 2.1. According to the attributes of step 11, The VIM#2 creates EVPN-VXLAN as the virtualized network resource#3. The VIM#2 configures id_3 to its own VRF RD.
13	VIM#2 → NFVO	See step 13 of BF#1.2 for use case #1 in section 2.1. The VIM#2 returns identifiers of the virtualized network resource#3 and VRF RD, namely id_3.

Continued on next page.

#	Flow	Description
14	NFVO → WIM	See step 14 of BF#1.2 for use case #1 in section 2.1. In this case, the following attributes are provided to the WIM; • Information for connecting to virtualized network resource #1: id_1; and • Information for connecting to virtualized network resource #3: id_3.
15	WIM → Network Controller	See step 15 of BF#1.2 for use case #1 in section 2.1.
16	Network Controller	See step 16 of BF#1.2 for use case #1 in section 2.1. The WIM adds id_1 and id_3 to the import RT list at the PE node#1 and the PE node#2.
17	Network Controller → WIM	See step 17 of BF#1.2 for use case #1 in section 2.1.
18	WIM → NFVO	See step 18 of BF#1.2 for use case #1 in section 2.1.
19	NFVO → VIM#1	See step 19 of BF#1.2 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#1: • Information for connecting to virtualized network resource #3: id_3
20	VIM#1	See step 20 of BF#1.2 for use case #1 in section 2.1. The VIM#1 adds id_3 to the import RT list at the network gateway#1.
21	VIM#1 → NFVO	See step 21 of BF#1.2 for use case #1 in section 2.1.
22	NFVO → VIM#2	See step 22 of BF#1.2 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#2: • Information for connecting to virtualized network resource #1: id_1
23	VIM#2	See step 23 of BF#1.2 for use case #1 in section 2.1. The VIM#2 adds id_1 to the import RT list at the network gateway#2.
24	VIM#2 → NFVO	See step 24 of BF#1.2 for use case #1 in section 2.1.
25	NFVO	See step 25 of BF#1.2 for use case #1 in section 2.1.

Continued on next page.

#	Flow	Description
26	NFVO → OSS/BSS	See step 26 of BF#1.2 for use case #1 in section 2.1.
NOTE: Once a L2-VPN is established, the establishment of a virtualized network resource and allocation of VRF RD at steps from step 3 to step 7 can be skipped when allocating other Virtual Links between the NFVI-PoPs.		

Finished.

3.3.3 Case 3: VXLAN Connection over L3 WAN Connectivity between NFVI-PoPs

3.3.3.1 Overview

In this case, L3-VPN at WAN is used to provide an IP based underlying network among two or more NFVI-PoPs, and overlay tunnels with VXLAN are created over the underlying network to provide L2 connectivity for VLs. It is supposed that the L3-VPN autonomously manages TE according to QoS and bandwidth requirements from the NFV-MANO, and exchanges the routing information of each NFVI-PoP by using BGP or Open Shortest Path First (OSPF). The VXLAN creates L2-based broadcast domains for VLs and allows NFV-MANO to specify IP addresses to the VNFs independently from the address spaces of the underlying network. There are several options in terms of end points of VXLAN based overlay networks; i.e. the location of VTEPs. In this case, the VTEPs are placed on vSwitches on hosts and VXLAN based overlay networks are terminated at virtual network ports connected to the virtual network interfaces of the VNFs. Figure 3.21 shows an overview of a VXLAN connection over L3 WAN connectivity between two NFVI-PoPs. The WIM creates an L3-VPN between NFVI-PoP#1 and NFVI-PoP#2. In this case, the WIM is responsible for IP address assignment for the network between the network gateway of NFVI-PoP and a PE node of the WAN. That is, when establishing an L3-VPN, the WIM generates IP addresses for external ports of the network gateways and the PE nodes and then passes these IP addresses to the VIM#1 and the VIM#2 to properly configure the addresses and routing information (i.e. next-hop) of the network gateways. In this specific example, the WIM assigns 172.16.1.2/24 and 172.16.2.2/24 to the external ports of the network gateways #1 and #2 and 172.16.1.1/24 and 172.16.2.1/24 to the PE nodes #1 and #2, respectively. In the NFVI-PoPs, 192.168.1.1/24 and 192.168.2.1/24 are statically allocated to the internal ports of the network gateways respectively. When establishing a VXLAN connection, the VIMs assign IP addresses to virtual network ports for VXLAN VTEPs. In this specific example, the VIMs assign 192.168.1.2/24 and 192.168.2.2/24 to the virtual network ports #1 and #2, respectively. Then the VIM#1 and VIM#2 configure VXLAN VTEPs on virtual network port#1 and #2 to provide L2 connectivity (ID= id1) for VNFs in NFVI-PoP#1 and NFVI PoP#2. As a result, NFV-MANO can assign the IP addresses to virtual network interfaces of the VNFs according to the NSD, in this specific example, 10.10.0.1/24 and 10.10.0.2/24 are assigned to virtual network interafaces#1 and #2 respectively. When the VNF#1 sends Ethernet

frames to the VNF#2, these frames are encapsulated with the VXLAN headers and outer IP/UDP headers by virtual network port#1. The destination address of the outer IP header is set to the IP address of peered virtual network port#2 (i.e. 192.168.2.2). Then the IP packets are delivered to virtual network port#2 over the IP based underlying network. The VXLAN header and outer IP/UDP headers of the IP packets are removed by virtual network port#2 and then the unwrapped Ethernet frames are forwarded to the VNF#2.

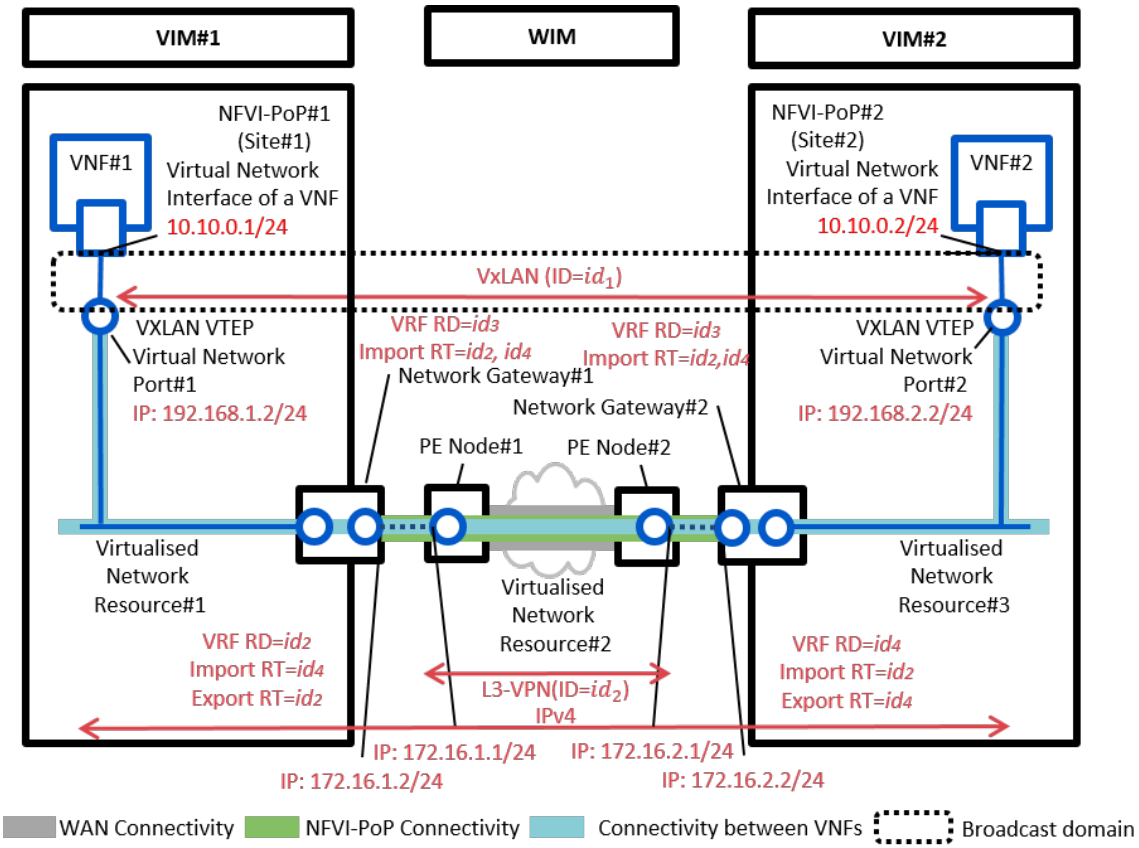


Figure 3.21: Overview of VXLAN connection between NFVI-PoPs over L3 WAN connectivity.

3.3.3.2 Properties of virtual network resources

The virtualized network resources at WAN, NFVI-PoP#1 and NFVI-PoP#2 are characterized as shown in the Table 3.6. These properties are exchanged between NFVO and WIM/VIM through the Or-Vi reference point.

Table 3.6: Properties of virtualized network resources for case 3.

Virtualized Network Resource	Attribute	Example Value	Description
WAN	Connectivity type	IPv4 and Mesh	See ConnectivityType information element of the NS Virtual Descriptor in clause 6.5.3 in ETSI GS NFV-IFA 014 [49].
	Network type for WAN connectivity	l3-vpn	The type of network for the WAN connectivity that maps to the virtualized network. In this example, it is L3-VPN using MPLS. For details, see attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	Network type for NFVI-PoP connectivity	IPv4	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	Segment type for NFVI-PoP connectivity	none	See also attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	Is shared	True	This attribute indicates whether the network is shareable (for aggregation among VLs) or not. In this use case, the network is shareable. See also the attribute isShared of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
NFVI-PoP#1	Network type	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].

Continued on next page.

Table 3.6: Properties of virtualized network resources for case 3.

Virtualized Network Resource	Attribute	Example Value	Description
	Segment type	id_1	VXLAN network identifier. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [51].
	scope	multi-site	The scope of the area which the network covered. ”multi-site” means this network is extended to other sites.
NFVI-PoP#2	Network type	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	Segment type	id_1	VXLAN network identifier. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [51].
	scope	multi-site	The scope of the area which the network covered. ”multi-site” means this network is extended to other sites.

Finished.

3.3.3.3 Operational flow

Table 3.7 shows the operational flow for this case. It follows BF#1.3 of use case #1 in section 2.1, so Table 3.7 shows only additional descriptions specific for this case.

Table 3.7: Operational flow (based on BF#1.3 of use case #1).

#	Flow	Description
1	OSS/BSS → NFVO	See step 1 of BF#1.3 of use case #1 in section 2.1.

Continued on next page.

#	Flow	Description
2	NFVO	See step 1 of BF#1.3 for use case #1 in section 2.1. NFVO decides to create the VXLAN and selects an identifier of VXLAN (ID= id_1) for connecting VNFs at NFVI-PoP#1 and NFVI-PoP#2.
3	NFVO → WIM	See step 3 of BF#1.3 for use case #1 in section 2.1. See note 1. In this case, the following attributes are provided to the WIM: • Connectivity type: IPv4 and Mesh; • NFVI-PoPs to be connected: NFVI-PoP#1 and NFVI-PoP#2; • Network type for WAN connectivity: l3-vpn; • Network type for NFVI-PoP connectivity: IPv4; • Is shared: True; and • QoS and bandwidth information.
4	WIM → Network Controller	See step 4 to 6 of BF#1.3 for use case #1 in section 2.1. See note 1. L3-VPN between the PE node#1 and #2 is established as virtualized network resource#2. The WIM allocates IP addresses, namely 172.16.1.1/24 and 172.16.2.1/24 to the PE node#1 and #2. It also selects IP addresses, namely 172.16.1.2/24 and 172.16.2.2/24 to be assigned to the external port of the network gateways of NFVI-PoP#1 and #2, respectively.
5	Network Controllor	
6	Network Controller → WIM	
7	WIM → NFVO	See step 7 of BF#1.3 for use case #1 in section 2.1. See note 1 The WIM replies an identifier of virtual network researce#2 and IP addresses, namely 172.16.1.2/24 and 172.16.2.2/24, to be assigned to the external ports of the network gateways. It also replies IP addresses of the PE nodes, namely 172.16.1.1/24 and 172.16.2.1/24.

Continued on next page.

#	Flow	Description
8	NFVO → VIM#1	See step 8 of BF#1.3 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#1: • Information for connecting to the WAN: 172.16.1.2/24 to be assigned to the external port of the network gateway#1 and 172.16.1.1/24 of the PE node#1 for configuring a next-hop of the network gateway#1; • Network type for NFVI-PoP: vxlan; • Scope: multi-site; and • QoS and bandwidth information.
9	VIM#1	See step 9 of BF#1.3 for use case #1 in section 2.1. According to the attributes of step 8, the VIM#1 creates the virtualized network resource#1. The VIM#1 allocates the specified IP address, namely 172.16.1.2/24 to the external port of the network gateway#1 and adds a next hop (i.e. 172.16.1.1/24) to the routing table of the network gateway#1. The VIM#1 also allocates an IP address, namely 192.168.1.2/24 to the virtual network port#1 for VXLAN VTEP.
10	VIM#1 → NFVO	See step 10 of BF#1.3 for use case #1 in section 2.1. The VIM returns identifiers of the virtualized network resource #1and IP address of the virtual network port#1, namely 192.168.1.2/24.
11	NFVO → VIM#2	See step 11 of BF#1.3 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#2: • Information for connecting to the WAN: 172.16.2.2/24 to be assigned to the external port of the network gateway#2 and 172.16.2.1/24 of the PE node#2 for configuring a next-hop of the network gateway#2; • Network type for NFVI-PoP: vxlan; • Scope: multi-site; and • QoS and bandwidth information.

Continued on next page.

#	Flow	Description
12	VIM#2	See step 12 of BF#1.3 for use case #1 in section 2.1. According to the attributes of step 11, The VIM#2 creates the virtualized network resource#2. The VIM#2 allocates the specified IP address, namely 172.16.2.2/24 to the external port of the network gateway#2 and adds a next hop (i.e. 172.16.2.1/24) to the routing table of the network gateway#2. The VIM#2 also allocates an IP address, namely 192.168.2.2/24 to the virtual network port#2 for VXLAN VTEP.
13	VIM#2 → NFVO	See step 13 of BF#1.3 for use case #1 in section 2.1. The VIM#2 returns identifiers of the virtualized network resource and IP address of virtual network port#2, namely 192.168.2.2/24.
14	NFVO → VIM#1	See step 14 of BF#1.3 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#1; • Segment type for NFVI-PoP: id_1; and • VTEP address of NFVI-PoP#2 obtained at step 13: 192.168.2.2/24. See note 2.
15	VIM#1	See step 15 of BF#1.3 for use case #1 in section 2.1. According to the attributes of step 14, the VIM#1 configures VTEP at the virtual network port#1 (ID = id_1 and the destination address= 192.168.2.2/24).
16	VIM#1 → NFVO	See step 16 of BF#1.3 for use case #1 in section 2.1.
17	NFVO → VIM#2	See step 17 of BF#1.3 for use case #1 in section 2.1. In this case, the following attributes are provided to the VIM#2: • Segment type for NFVI-PoP: id_1; and • VTEP address of NFVI-PoP#1 obtained at step 10: 192.168.1.2/24. See note 2.
18	VIM#2	See step 18 of BF#1.3 for use case #1 in section 2.1. According to the attributes of step 17, the VIM#2 configures VTEP at the virtual network port#2 (ID = id_1 and the destination address = 192.168.1.2/24).
19	VIM#2 → NFVO	See step 19 of BF#1.3 for use case #1 in section 2.1.
20	NFVO	See step 20 of BF#1.3 for use case #1 in section 2.1.

Continued on next page.

#	Flow	Description
21	NFVO → OSS/BSS	See step 21 of BF#1.3 for use case #1 in section 2.1.
NOTE 1: Once a L3-VPN is established, the steps from step 3 to step 7 can be skipped when allocating other VLs between the NFVI-PoPs. NOTE 2: The VXLAN has several options like unicast mode/multicast mode/ BGP control plane to exchange addresses of VTEPs. In this case, it is assumed that the VXLAN uses unicast mode.		

Finished.

3.4 Conclusion

I detailed the overloading issue of the existing protocol and proposed a novel interoperable architecture among multiple VIMs for reducing the NFVO load. Additionally, practical issues including security and protocol extensions were thoroughly discussed. The proposed mechanism for exchanging parameters between VIMs has been accepted as an implementation of the ETSI NFV Release 3 specifications. My efforts on the request congestion management and multiple WAN connections represent an innovative solution for achieving NS deployment across multi-provider networks. Suggestions on exchange parameters were introduced.

My comparison of the centralized and the distributed models shows that the distributed model is more effective in terms of load, security, and location issues.

Chapter 4

Network Reliability Evaluation

In this section, I propose a method that efficiently computes the reliability of multi-domain networks without revealing intra-domain privacy. The selection of an appropriate network is critical component as the network reliability depends on the operation of each network provider. While this problem may seem similar to a traditional reliability evaluation assuming a single-domain network, calculating network reliability across multi-domains introduces computational complexity and intra-domain privacy challenges. Our method enables us to partition the problem so as to yield upper and lower bounds of reliability. Each DP computes the reliability of their domain, and the SP then unifies the results to yield the bounds for the whole network. Section 4.1 formalizes the problem addressed. Section 4.2 establishes the theory, while Section 4.3 describes the protocol. Section 4.4 reports our experiments and their results.

4.1 Problem Statement

This subsection provides the problem statements needed for understanding my advances. Section 4.1.1 defines my network model, and Section 4.1.2 describes the problem raised by reliability evaluations of multi-domain networks.

4.1.1 Network Model

This subsection does not focus on any specific type of network. Networks can be physical, logical, or any mixture, as long as they can be represented as my model described below. A network is represented as undirected graph $G = (V, E)$, where V is a set of nodes and E is a set of links. The whole network is partitioned into *domains*, and the domains are numbered; the set of domain numbers is denoted by $D = \{1..|D|\}$. Node set V is partitioned following the domains; i.e.,

$$\bigcup_{i \in D} V_i = V,$$
$$V_i \cap V_j = \emptyset \qquad\qquad i, j \in D\ (i \neq j).$$

Domain i is defined as the induced subgraph, $G[V_i]$.

Nodes connecting to another domain are called *border* nodes, and the set of border nodes is defined as $B \subset V$. Because every border node belongs to a single domain (from the partition definition), I can consider a function $f_B : B \to D$ and f_B is surjective (i.e., every domain has at least one border node). The set of domain i's border nodes, i.e., $B \cap V_i$, is a vertex separator[1] for the domain and the others.

The service provided by the SP consists of nodes named *terminals*. The terminal set is defined as $T \subset V$. In this section, I assume that every domain has at least one terminal, so the surjective function $f_T : T \to D$ is considered. Without loss of generality, I assume that every terminal is not a border node; i.e., $T \cap B = \emptyset$ (if not, I can cleave the border terminal into the border-only node and a new terminal, and then connect them with a perfect link; the new terminal is not connected to the neighbors of the border node).

Given network G, let $m = |E(G)|$. The m-dimensional binary vector $\boldsymbol{x} = \{x_1, \ldots, x_m\} \in \{0, 1\}^m$ is used to represent the current status of the links; if $x_i = 0$, then link $e_i \in E$ has failed; otherwise, e_i is available. I assume that every link e_i independently fails with probability $1 - p_i$, where $p_i \in [0, 1]$ is the probability that e_i is available. Nodes are regarded as perfect. Given status $\boldsymbol{x}$, the corresponding subgraph, $G(\boldsymbol{x}) \subseteq G$, is defined by $V(G(\boldsymbol{x})) = V$ and $E(G(\boldsymbol{x})) = \{e_i \in E : x_i\}$.

Network reliability is defined as follows. Given network G with T, the set, $\mathcal{G}(G, T)$, of subgraphs connecting the terminals is,

$$\mathcal{G}(G, T) = \{G(\boldsymbol{x}) \subseteq G : G(\boldsymbol{x}) \text{ connects } T\}.$$

Note that I allow detour paths, which connect terminals in the same domain via another domain (this issue is discussed in Section 4.3.1). Network reliability $R(G, T)$ can be considered as the total probability of connecting the terminals,

$$R(G, T) = \sum_{G(\boldsymbol{x}) \in \mathcal{G}(G,T)} \prod_{i \in \{1..m\}} [x_i p_i + (1 - x_i)(1 - p_i)], \tag{4.1}$$

where the product term is the probability that the network is in $G(\boldsymbol{x})$.

I assume that DP i knows $G[V_i]$. I also assume that the SP figures out how to connect the domains, i.e., $G[B]$ (or the contracted graph of $G[B]$, as is discussed in Section 4.2.2). Note that inter-domain connections are often very complicated to grasp even if I limit ourselves to those used by the service, so I address this concern in Section 4.3.1.

4.1.2 Reliability Evaluation for Multi-domain Networks

My problem is defined as follows.

Problem. *Whether SP efficiently compute $R(G, T)$, with the same accuracy as the conventional methods under the information constraint, i.e., $G[V_i]$ is known only to DP i while $G[B]$ is known only to the SP.*

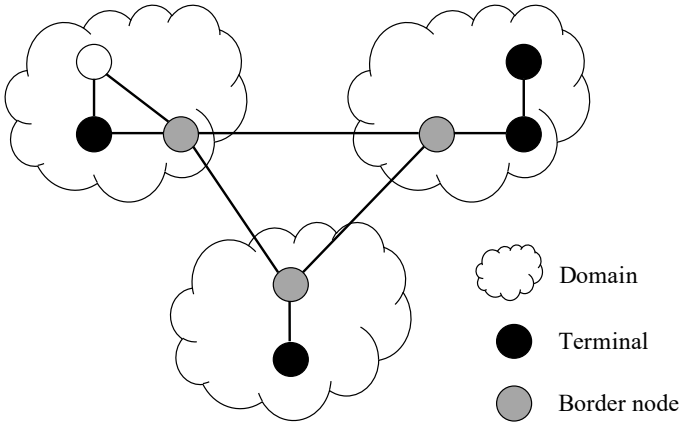
[1] A subset, $S \subset V$, of nodes is a *vertex separator* for nonadjacent nodes $u, v \in V$, if the removal of S from the graph separates u and v into distinct connected components.

4.2 Theory

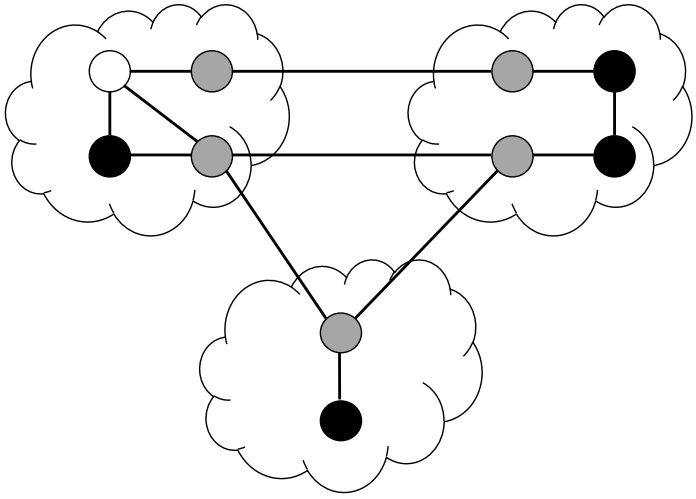
This subsection establishes a theory that yields lower and upper bounds of reliability. The problem is partitioned to reduce computation complexity and also to secure intra-domain privacy. The theory is developed in two steps as follows (Figure 4.1).

(a) Section 4.2.1: Compute the exact value of $R(G, T)$ when f_B is bijective; i.e., every domain has just a single border node, $\forall i \in \{1..|D|\}, |B \cap V_i| = 1$.

(b) Section 4.2.2: Compute $R(G, T)$ with the bounds when f_B is surjective; this is the general case.



(a) Single border node.



(b) General case.

Figure 4.1: Problem instances.

4.2.1 ingle Border Node

Lemma 1. *Every subgraph connecting the terminals also connects all the border nodes.*

$$\mathcal{G}(G,T) = \mathcal{G}(G,T \cup B).$$

Proof. Because the right side of the equation connects T, we have $\mathcal{G}(G,T) \supseteq \mathcal{G}(G,T \cup B)$.

I then prove the converse, $\mathcal{G}(G,T) \subseteq \mathcal{G}(G,T \cup B)$, by contradiction. Assume that there exists a border node $b \in B$ that is disconnected from some of T in a subgraph of $\mathcal{G}(G,T)$. Without loss of generality, I assume the border node is in domain i, i.e., $b \in V_i$. Because b is the single border node in the domain (f_B is bijection in Problem 1), $\{b\}$ is a vertex separator for the domain, which implies that several terminals are disconnected from/to the domain. This contradicts the fact that the subgraph is in $\mathcal{G}(G,T)$. □

Corollary 1. *From* (4.1) *and Lemma 1, I have,*

$$R(G,T) = R(G,T \cup B).$$

Lemma 2. *The link set is partitioned into the domains and the backbone.*

$$E(G[B]) \cup \bigcup_{i \in D} E(G[V_i]) = E, \tag{4.2}$$

$$E(G[V_i]) \cap E(G[V_j]) = \emptyset \qquad i, j \in D\ (i \neq j), \tag{4.3}$$

$$E(G[V_i]) \cap E(G[B]) = \emptyset \qquad i \in D. \tag{4.4}$$

Proof. From the definition of my network model, for each link $e = \{u, v\}$, the ends are either in a domain ($u, v \in V_i$) or are borders ($u, v \in B$). □

I define the *join* operation over two sets of subgraphs, following family algebra [70]. Given two sets of subgraphs, $\mathcal{G}_1 = \mathcal{G}(G_1, T_1)$ and $\mathcal{G}_2 = \mathcal{G}(G_2, T_2)$, their join is defined, as follows,

$$\mathcal{G}_1 \sqcup \mathcal{G}_2 = \Big\{ (V(G_1) \cup V(G_2), E(G_1') \cup E(G_2')) : \\ G_1' \in \mathcal{G}_1, G_2' \in \mathcal{G}_2 \Big\}.$$

Lemma 3. *The set of subgraphs connecting the terminals is given as the join between the domains and the backbone.*

$$\mathcal{G}(G, T \cup B) = \mathcal{G}(G[B], B) \sqcup \bigsqcup_{i \in D} \mathcal{G}(G[V_i], (T \cup B) \cap V_i).$$

Proof. I first prove $\mathcal{G}(G, T \cup B) \supseteq \mathcal{G}(G[B], B) \sqcup \bigsqcup_{i \in D} \mathcal{G}(G[V_i], (T \cup B) \cap V_i)$. The first term of the right side, $\mathcal{G}(G[B], B)$, indicates that all the border nodes are connected in every subgraph. The second term, $\mathcal{G}(G[V_i], (T \cup B) \cap V_i)$, indicates that all the terminals in domain i are connected to the border node in every subgraph. Hence, every joined subgraph in the right side connects all the terminal and the border nodes, which implies the left side.

I then prove the converse: $\mathcal{G}(G, T \cup B) \subseteq \mathcal{G}(G[B], B) \sqcup \bigsqcup_{i \in D} \mathcal{G}(G[V_i], (T \cup B) \cap V_i)$. In each subgraph of the left side set, every border node is a distinct node separator for a singleton. Cutting the subgraph at the border nodes (without removing them), each piece connects either the border nodes or the border node with terminals in the domain. Note that G is covered by the union of $G[B]$ and $G[V_i]$'s in the right side from (4.2). Thus, the right side is implied. □

Lemma 4. *Network reliability is partitioned as follows,*

$$R(G, T \cup B) = R(G[B], B) \prod_{i \in D} R(G[V_i], (T \cup B) \cap V_i).$$

Proof. In Lemma 2, each subgraph in the left side, $G' \in \mathcal{G}(G, T \cup B)$, is cut into the domains and the backbone in the right side. From (4.3) and (4.4), no link is shared between the domains and the backbone. Thus, the reliability of the whole network is simply given as the product of reliabilities for the domains and for the backbone. □

Theorem 1. *Reliability of multi-domain networks can be partitioned into those of the domains and the backbone.*

$$R(G, T) = R(G[B], B) \prod_{i \in D} R(G[V_i], (T \cup B) \cap V_i).$$

Proof. From Corollary 1 and Lemma 4. □

4.2.2 General Case

Lemma 5.

$$\mathcal{G}(G, T) \supseteq \mathcal{G}(G, T \cup B).$$

Proof. Same as the former half of Lemma 1. □

Lemma 5 implies that several border nodes can be bypassed in (b), unlike Lemma 1.

Let $G' = (V', E')$ be the graph where border nodes in the same domain are *contracted* (Fig. 4.2). Contraction of a pair of nodes produces a new graph in which the two nodes are merged; their links are left as they are (some of them could be parallel links). Let $B' \subset V'$ be the set of new border nodes after the contraction.

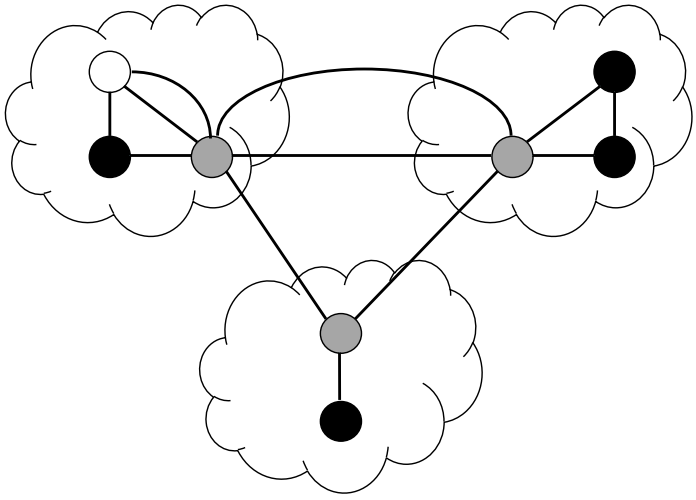


Figure 4.2: Contraction of border nodes. This graph is the contracted graph, G', of Figure 4.1b. The three border nodes form the set, B'.

Corollary 2. *Associating a contracted node with any of original nodes, there is the injection, f_V, between the new and original vertex sets,*

$$f_V : V' \to V.$$

Corollary 3. *There is the bijection, f_E, between the new and original link sets,*

$$f_E : E(G'[B']) \cup \bigcup_{i \in D} E(G'[V_i']) \to E.$$

Based on Corollaries 2 and 3, nodes and links in a contracted graph are associated with those in the original graph, if needed; i.e., new links are associated with the availability of the original ones.

Lemma 6. *The set of connected subgraphs is a superset of the join between the domains and the contracted backbone.*

$$\mathcal{G}(G, T \cup B) \supseteq \mathcal{G}(G'[B'], B') \sqcup \bigsqcup_{i \in D} \mathcal{G}(G[V_i], (T \cup B) \cap V_i).$$

Proof. The second term of the right side, $\mathcal{G}(G[V_i], (T \cup B) \cap V_i)$, indicates that in domain i all the border nodes are connected. In this case, it is sufficient that the backbone connects one of border nodes for each domain; i.e., from Corollary 2, it is sufficient that all the contracted border nodes are connected, which is the first term, $\mathcal{G}(G'[B'], B')$, in the right side. □

Theorem 2. *The lower bound of the reliability is given as,*

$$R(G, T) \geq R(G'[B'], B') \prod_{i \in D} R(G[V_i], (T \cup B) \cap V_i). \tag{4.5}$$

Proof. From Lemma 5 and Lemma 6. □

Lemma 7.

$$\mathcal{G}(G,T) \subseteq \mathcal{G}(G',T).$$

Proof. From Corollary 2, if there is a path in G, there also is a path in G'. □

Lemma 8. *In the contracted network, the set of connected subgraphs is a subset of the join between the domains and the backbone.*

$$\mathcal{G}(G',T) = \mathcal{G}(G'[B'],B') \sqcup \bigsqcup_{i\in D} \mathcal{G}(G'[V_i'],(T\cup B')\cap V_i').$$

Proof. Because the contracted graph, G', has a single border node in every domain, I have an identical lemma, $\mathcal{G}(G',T) = \mathcal{G}(G',T\cup B')$, with Lemma 1. Replacing $\mathcal{G}(G',T)$ with $\mathcal{G}(G',T\cup B')$ in Lemma 8, which can be proved in the same way of Lemma 3. □

Theorem 3. *The upper bound of the reliability is given as,*

$$R(G,T) \le R(G'[B'],B') \prod_{i\in D} R(G'[V_i'],(T\cup B')\cap V_i'). \tag{4.6}$$

Proof. From Lemma 7 and Lemma 8. □

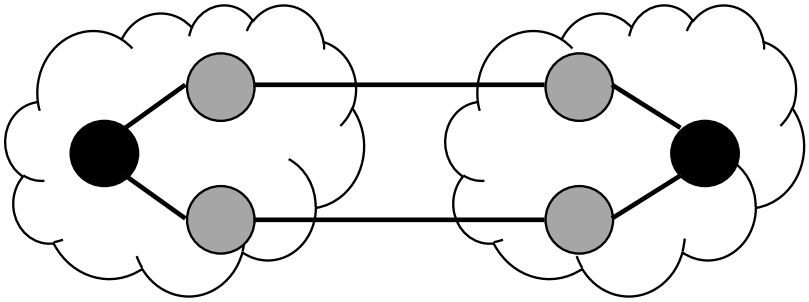
4.2.3 Examples

Figure 4.3 illustrates how the lower and upper bounds deviate from the exact value. Figure 4.3a is the network considered, and Figure 4.3b gives the corresponding contracted graph. Figure 4.3c shows several subgraphs included in the set of connected subgraphs for the lower bound (i.e., the right side of Lemma 6), the set for the exact value ($\mathcal{G}(G,T)$), and the set for the upper bound (the right side of Lemma 8).

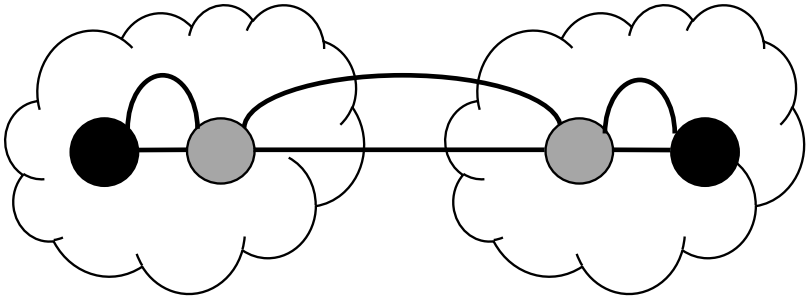
- Exact value (the center column). The top two subgraphs are connected, while the bottom one is disconnected (X-mark indicates the subgraph is not included in the set of connected subgraphs). Thus, the top two are included in $\mathcal{G}(G,T)$, and the bottom one is not.

- Upper bound (the right column). The subgraphs shown are derived from the center column of the same row. The three subgraphs seem all connected, but the bottom one is actually not, as shown in the center column; this false positive leads to overestimation. Because no false negative happens as discussed in my theory, it can be used in determining the upper bound.
  The following observation allows us to expect tight upper bounds. Because false positive subgraphs are actually disconnected, they are likely to have many failed links. If link availabilities are small, the probabilities of these subgraphs is expected to be very small; given link availabilities of 99%, i.e., $p_i = 0.99$, the probability that the network is in the bottom state of Figure 4.3c is $0.99^3 \times 0.01^3 = 0.00000097029$. Thus, false positive subgraphs do not impose significant errors on the upper bound.

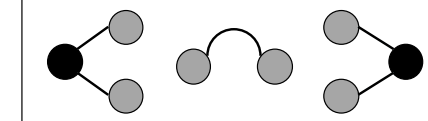
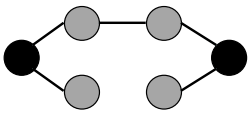
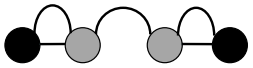
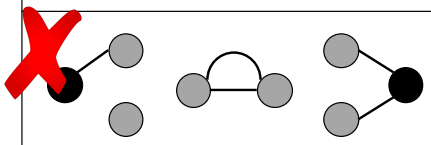
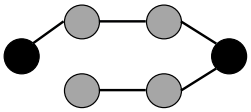
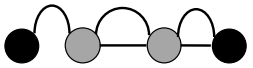
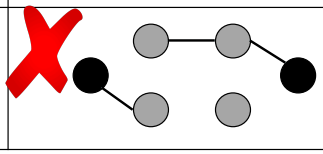
- Lower bound (the left column). The subgraphs are separated according to the domains, because inter-domain graphs are contracted, while intra-domain graphs are not; in each piece of each subgraph, terminals and border nodes should be connected. Although only the top subgraphs seem connected, the middle one is actually connected as shown in the center column; this false negative leads to underestimation, and it can be used for the lower bound.



(a) A network.



(b) Contracted graph.

Lower bound (right side of Lemma 6)	Exact value ($\mathcal{G}(G,T)$)	Upper bound (right of Lemma 8)
		
		
		

(c) Several subgraphs included in the sets of lower bound, exact value, and upper bound.

Figure 4.3: Subgraphs used to describe how the bounds deviate from the exact value.

4.3 Practice

This subsection addresses the practical issues whose solutions are needed for actual deployment. After discussing inter-domain connections in Section 4.3.1, Section 4.3.2 defines a primitive protocol between an SP and DPs to compute the reliability bounds of Theorems 2 and 3. This subsection aims at showing that a basic protocol can be defined for my theory; further elaboration for specific services will be done in the future.

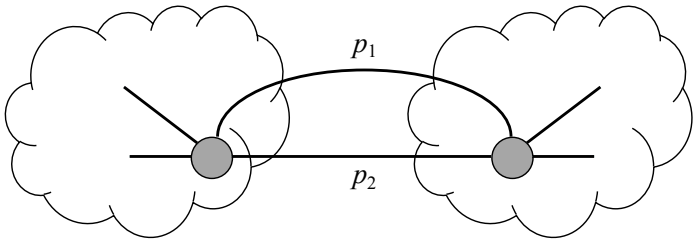
4.3.1 Inter-domain Connections

In my network model, I assume that the SP can utilize the contracted graph of inter-domain network, $G'[B']$, which is included in (4.5) and (4.6). I first discuss the determination process of $G'[B']$, for (I) standardized specifications like ETSI NFV [37, 38] and (II) the general case.

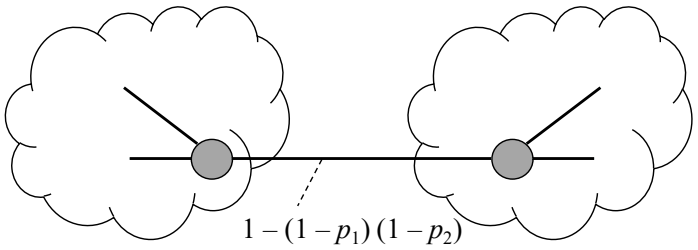
(I) The ETSI NFV Release 3 specifications allow SPs to retrieve adjacency between domains that join the NFV infrastructure [37]. Thus the SP in my method can determine the topology of $G'[B']$ based on this adjacency.

(II) In the general case, I consider *logical connections* between domains; i.e., a logical connection could be a sequence of physical links if the domains are not adjacent. This is because, in reliability evaluation, I do not need to recognize how nodes are connected; it is sufficient to know the probability that two nodes can communicate. The SP, hence, assumes that an inter-domain connection exists in $G'[B']$ if terminals in the two domains would directly exchange messages in the SP's service.

Next, I discuss the availability estimation for inter-domain connections (this discussion is applicable for (I) and (II)). In my protocol, the inter-domain availabilities are estimated by DPs and are given to the SP, as will be shown in Section 4.3.2. Although there could be multiple inter-domain connections between domains as shown in Figure 4.1b, these links are not necessarily distinguished if the contracted graph, $G'[B']$, is considered. This is because the set, M, of multi-links is equivalent in reliability evaluations to a single one with availability of $1 - \prod_{i \in M}(1 - p_i)$, as shown in Figure 4.4. Thus, it is sufficient for DPs to estimate the probability that the two domains can communicate. This inter-domain availability could be estimated as follows: periodically in advance, domains continue to exchange active probes between their border nodes, so as to use the success probability as the availability; or, upon receiving a request for the availability, domains examine their history of BGP updates to compute how often their counterparts were seen through BGP, because BGP messages represent the communicability between domains [71].



(a) Multi-links in $G'[B']$ of Figure 4.2.



(b) Single link.

Figure 4.4: (a) Multi-links between a pair of border nodes. (b) Corresponding connection equivalent to (a) in terms of availability.

In my model, even if terminals in the same domain have no path within the domain, they are allowed to be connected via a path that detours outside the domain. Although these detoured paths are forbidden by BGP, they could be utilized if overlay networks were established between terminals of different domains.

4.3.2 Protocol

This subsection defines a primitive protocol that computes the reliability bounds in a distributed manner. The protocol is defined for (b). The protocol also runs for (a); in this case, the contracted graph is identical with the original one, so the lower and upper bounds match.

The protocol assumes the following initial states.

- SP: the number of terminals to be placed in domain i is fixed; a secure channel is established with DP i.
- DP i: $G[V_i]$ is fixed.

Figure 4.5 illustrates the protocol sequence. First, the SP notifies DP i of the number of terminals and of domains accessed from domain i. DP i then determines the nodes hosting the terminals are placed ($T \cap V_i$ has fixed). DP i finds the border nodes to the other domains ($B \cap V_i$ has fixed), and estimates availabilities for the inter-domain connections; the availabilities are sent to the SP ($G'[B']$ is fixed).

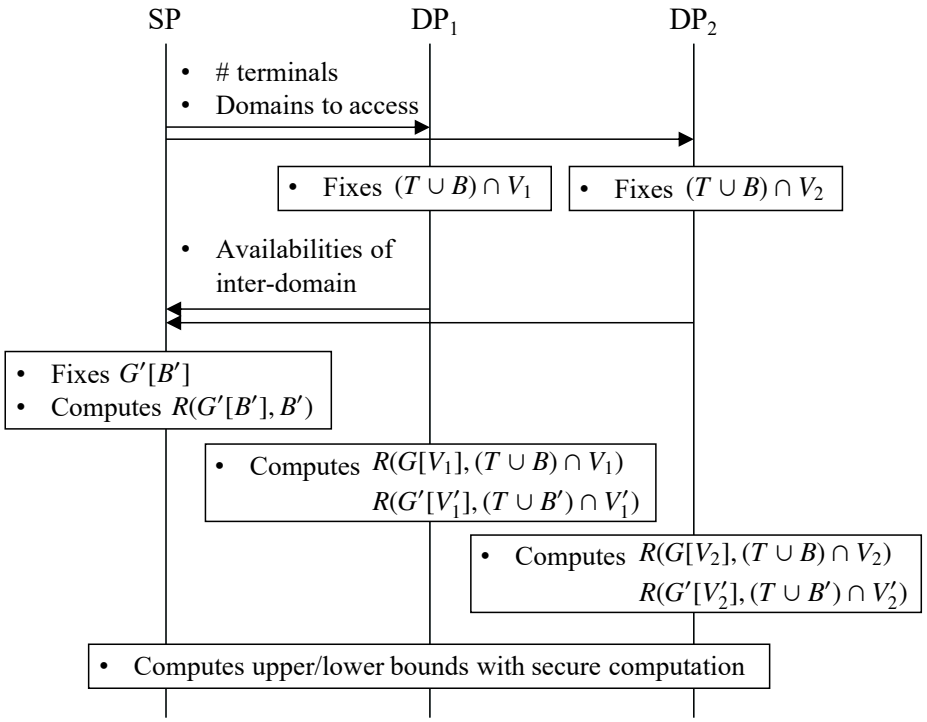


Figure 4.5: A protocol between the SP and two DPs, which computes the reliability bounds.

Finally, SP computes $R(G'[B'], B')$, while DP i computes $R(G[V_i], (T \cup B) \cap V_i)$ and $R(G'[V_i'], (T \cup B') \cap V_i')$; these partial reliabilities are secretly multiplied using secure computation techniques, such as secure multi-party computation [72] and homomorphic encryption [73] (these secure computation techniques allow computation while keeping the inputs private). In this way, no intra-domain information is disclosed in the protocol.

This section described an example of the computation procedure assuming the use of Multi Party Computation (MPC). The computation is performed by *participants*, i.e., the SP and DPs in my protocol; the SP is called 0-th participant, while DP j is called j-th participant. Every partial reliability is divided into *shares* based on cryptographic theory. Each participant is allocated a share of partial reliability, but the partial reliability can be reconstructed only when a sufficient number of shares are combined; individual shares are of no use on their own. I assume that the participants do not collude with each other. In this section, a share of reliability R allocated to participant j is denoted by $[[R]]_j$. In the ordinary use of MPC, arithmetic operations are performed over shares, and only the result is reconstructed.

I discuss only the lower bound using Figure 4.6, as the upper bound can be computed in a similar fashion. For readability, the lower bound (i.e., the right side of (4.5)) is denoted by R^L. The partial reliability of an inter-domain network is denoted by $R_0^L = R(G'[B'], B')$, while the partial reliability of domain i is denoted by $R_i^L = R(G[V_i], (T \cup B) \cap V_i)$. The lower bound is then written as $R^L = \prod_{i \in \{0\} \cup D} R_i^L$. Because summation is more efficient than multiplication in MPC [14], the multiplication is converted to a summation by taking the logarithm of reliabilities, i.e., $\log R^L = \sum_{i \in \{0\} \cup D} \log R_i^L$. The participants generate the shares

for their partial reliability, as follows,

$$\begin{aligned}&\textsc{MpcDivide}(\log R_i^L)\\ =&\{[[\log R_i^L]]_0, [[\log R_i^L]]_1, \ldots, [[\log R_i^L]]_{|D|}\}.\end{aligned}$$

The shares with subscript j are gathered by participant j, who executes MPC summation over the shares,

$$\begin{aligned}&\textsc{MpcSum}([[\log R_0^L]]_j, [[\log R_1^L]]_j, \ldots, [[\log R_{|D|}^L]]_j)\\ =&[[\log R^L]]_j.\end{aligned}$$

The SP gathers the shares of the lower bound and reconstructs it, as follows,

$$\begin{aligned}&\textsc{MpcReconst}([[\log R^L]]_0, [[\log R^L]]_1, \ldots, [[\log R^L]]_{|D|})\\ =&\log R^L.\end{aligned}$$

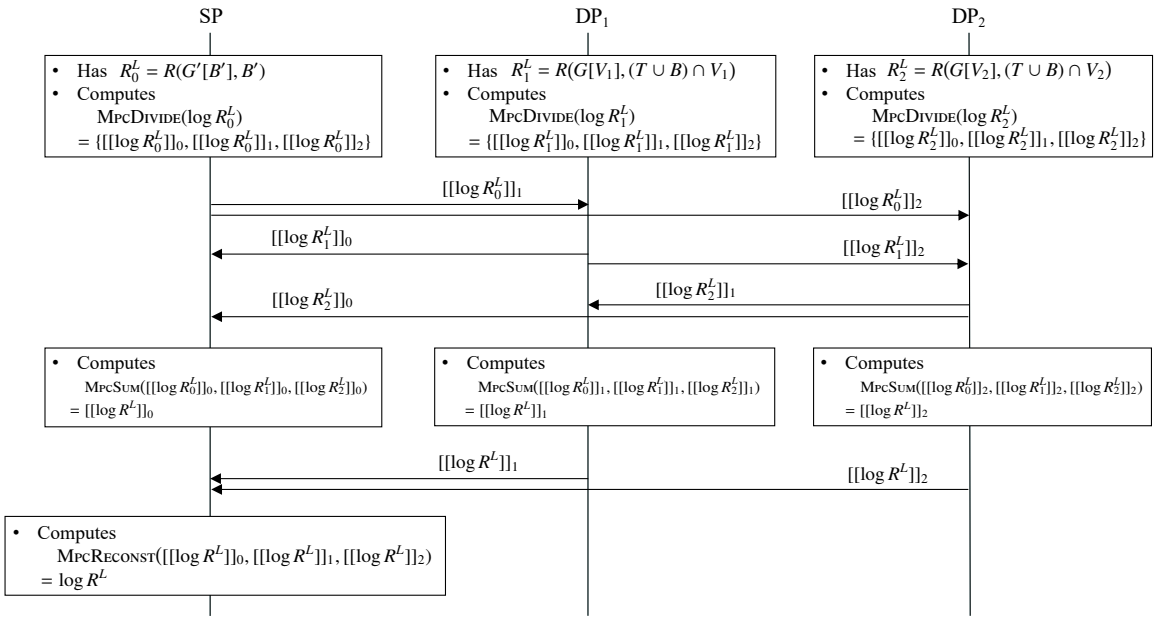


Figure 4.6: An example of MPC for the lower bound in my protocol.

The protocol overhead is briefly discussed assuming the use of MPC. Reference [14] states that the primary overhead of MPC is transmission, not computation, because transmission is slower than arithmetic operations by an order of magnitude. By taking the logarithm of partial reliabilities, I can convert the multiplication in (4.5) and (4.6) into a summation, as described above. Summation requires just two parallel transmissions, i.e., distribution of partial reliabilities and collection of results in MPC. In total, my protocol has just four stages of parallel transmission: SP's notification, DPs' replies, and two transmissions for MPC, as shown in Figures 4.5 and 4.6.

Further elaboration of the protocol, e.g., authentication and key exchange, is left as future work, because it depends on service details.

4.4 Experiments

This section uses real datasets to assess my method in terms of computation costs (Section 4.4.1) and bound gaps (Section 4.4.2). Because the protocol overhead is not significant as discussed in Section 4.3.2, it is not measured.

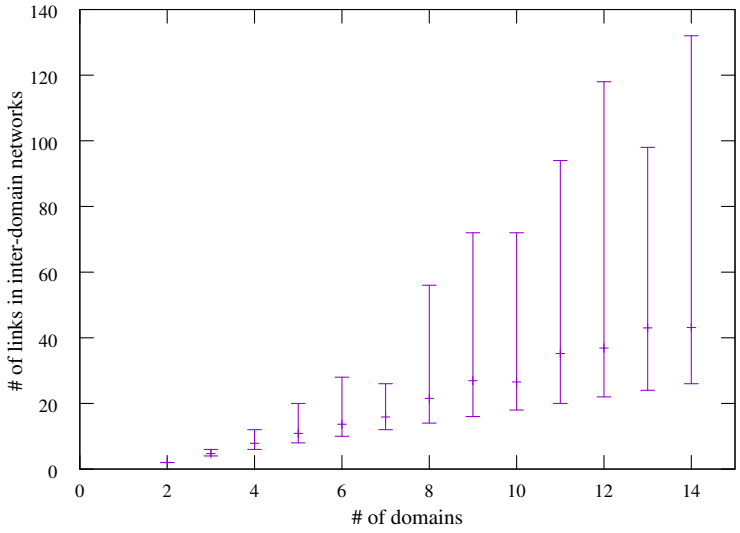
To the best of my knowledge, no method can evaluate reliability while securing intra-domain privacy, so there is no direct benchmark. As a baseline, I use hiliteCan existing reliability evaluation method [10, 11, 12], hiliteCthat discloses domain internal data in computing the exact reliability of the whole network. Because the existing method computes the exact value, it is used to assess the reliability bounds of my method.

Domains are randomly chosen from the real networks in Table 4.1 [74]. Each domain has one or two terminals and two or four border nodes; terminals and border nodes are randomly chosen. Domains are connected assuming active-active configuration of border nodes (e.g., the upper domains in Figure 4.1b). Inter-domain topologies are sampled from an AS-level network [2]; I randomly choose a starting domain (AS), from which I visit the specified number of domains in the breadth first order, then I reconstruct every link between the visited domains if existed in the original network. The number of domains ranges from 2 to 14. For each number of domains, 30 topologies are generated. For each topology, an inter-domain topology is sampled; as described above; as a result, every domain pair has a link with probability of 31.7% in my experiments. The maximum topology includes 907 links with 14 domains. Inter-domain and whole topologies, i.e., $G[B]$ and G, respectively, are summarized in Figure 4.7; for each number of domains, the average is represented by marks, and the minimum and maximum are indicated by the line whiskers. Link availabilities are uniformly and randomly determined. Parameters are summarized in Table 4.2. Each problem instance is specified for a pair of topology and availability range.

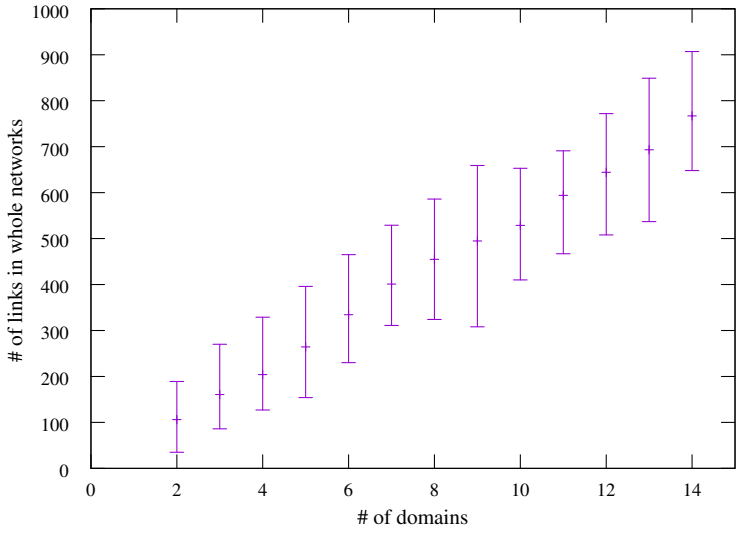
[2] `http://irl.cs.ucla.edu/topology/`

Table 4.1: Statistics of real networks used as intra-domains.

Network	$\|V\|$	$\|E\|$
Oxford	20	26
Funet	26	30
Darkstrand	28	31
Sunet	26	32
Shentel	28	35
Bren	37	38
NetworkUsa	35	39
IowaStatewideFiberMap	33	41
PionierL1	36	41
LambdaNet	42	46
Intranetwork	39	51
RoedunetFibre	48	52
Ntelos	47	58
Palmetto	45	64
UsSignal	61	78
Missouri	67	83
Switch	74	92
VtlWavenet2008	88	92
RedBestel	84	93
Intellifiber	73	95
VtlWavenet2011	92	96
Oteglobe	83	99



(a) # of links in inter-domain networks.



(b) # of links in whole networks.

Figure 4.7: The numbers of links (a) in inter-domain networks $G[B]$, and (b) in whole networks G.

Table 4.2: Parameter ranges.

# of terminals per domain	{1, 2}
# of border nodes per domain	{2, 4}
# of domains	{2, 3, ..., 14}
Link availability	(0.99,1), (0.999,1), or (0.9999,1)

The existing reliability evaluation method [10, 11, 12], which is also used in my method

to compute partial reliabilities, is implemented in C++ using the internal library of [75][3]. Graph manipulation including contraction is implemented in Python. Computation was conducted on a single core of a Core i7-8550U 1.8 GHz with 5 GB RAM.

4.4.1 Computation Costs

This subsection evaluates my method and the existing method in terms of computation time and memory usage. Because my method runs in parallel for the SP and DPs, I take the *maximum* of computation time and memory usage. The existing method has to run as a single process, because no distributed algorithm has been found for it. Computation was executed with a time limit of 120 [s].

Figure 4.8 shows the Cumulative Distribution Function (CDF) of computation time. My method consistently lies to the left of the existing method, which implies that my method is more efficient thanks to my partition theory. My method solved all the instances, while the existing method only solved 66% of them. Figure 4.9 shows the CDF of memory usage. My method required around less than 255 MB of memory to solve all the instances (the small deviation shown in my method means that my method requires a much smaller amount of memory compared to the amount that the OS process allocated by default). On the contrary, the existing method cannot complete even with 5 GB of memory.

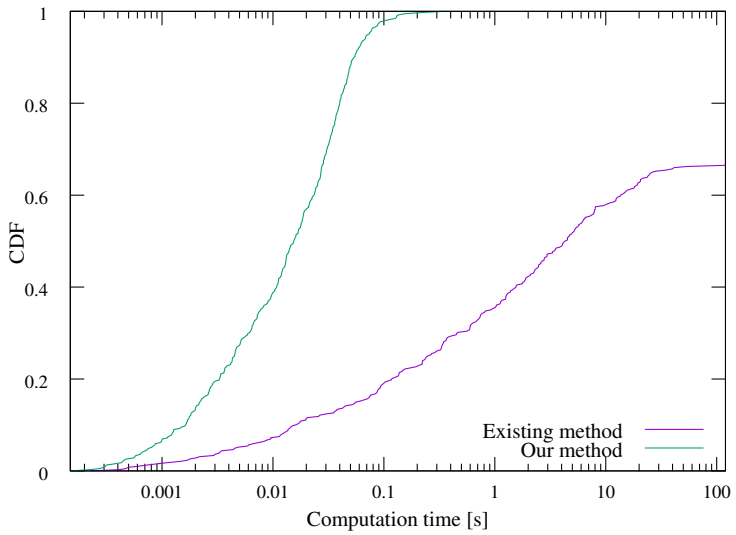


Figure 4.8: CDF of computation time.

[3] http://graphillion.org/

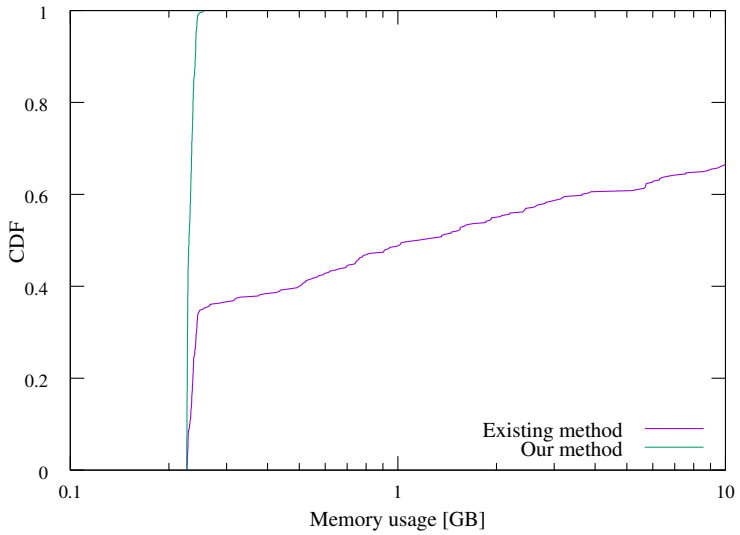


Figure 4.9: CDF of memory usage.

Figure 4.10 plots the computation time against the number of domains, while Fig. 4.11 demonstrates similar results for memory usage. For each number of domains, the average is represented by marks, and the minimum and maximum are indicated by the line whiskers. My method scales very well, while the existing method scales poorly; the existing method could not solve several instances for six or more domains. This is because the existing method incurs exponential growth in the amount of time and memory against the number of domains, due to the nature of #P problems.

It is worth noting that even if the results of my method were multiplied by the number of domains, my method would still outperform the existing method for large domain numbers.

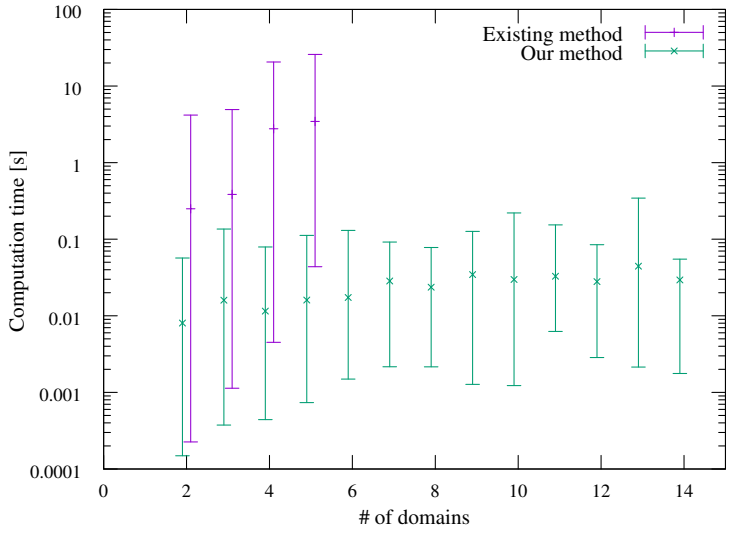


Figure 4.10: Computation time versus the number of domains.

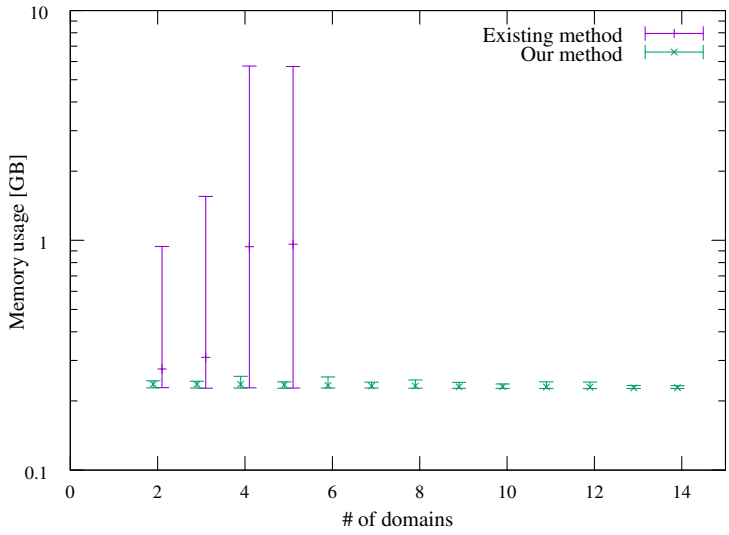


Figure 4.11: Memory usage versus the number of domains.

4.4.2 Bound Gaps

Figure 4.12 shows the gap between lower and upper bounds of my method. For each number of domains, the average is represented by marks, and the minimum and maximum are indicated by the line whiskers. The average gaps are less than 0.1 for link availabilities in (0.99,1), and they are less than 0.001 for those in (0.9999,1). The gaps grow slightly with large domain numbers, but the growth is slow.

I examine lower and upper bounds separately in Figure 4.15. The figure shows lower and upper bounds for link availabilities in (0.9999,1), which are plotted against the exact reliability computed by the existing method; I had similar results for other availability ranges. Points indicate lower and upper bounds for each instance; points below the line of $y = x$ correspond to the lower bounds, while these above the line are the upper bounds. The lower bounds have larger errors than the upper bounds. This is because the right side of Lemma 6 places a strong restriction on intra-domain reliability, i.e., all of the border nodes have to be connected, which could exclude several connected subgraphs. Note that while the upper bounds seem coincident with exact values, they are not; the discussion in Section 4.2.3 explains that upper bounds are tight.

Although my method has errors, they are bounded. This is a key advantage of my method against the existing sampling approach [4]; the bounds allow us to confidently judge whether the network is reliable enough.

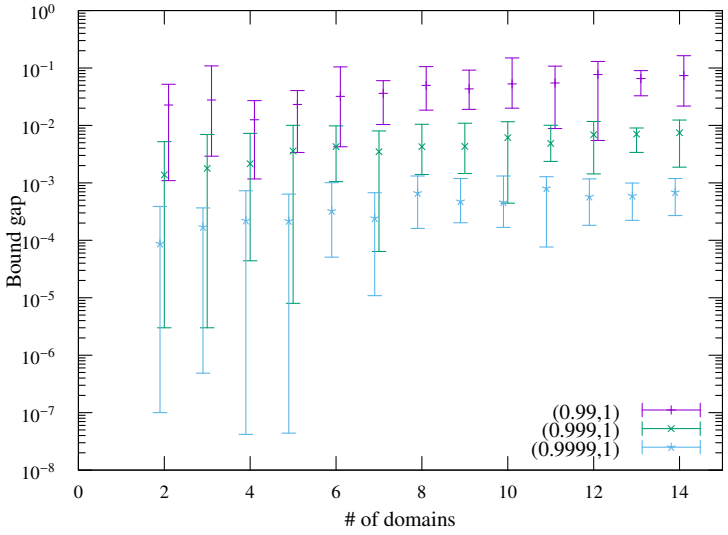


Figure 4.12: Bound gaps versus the number of domains.

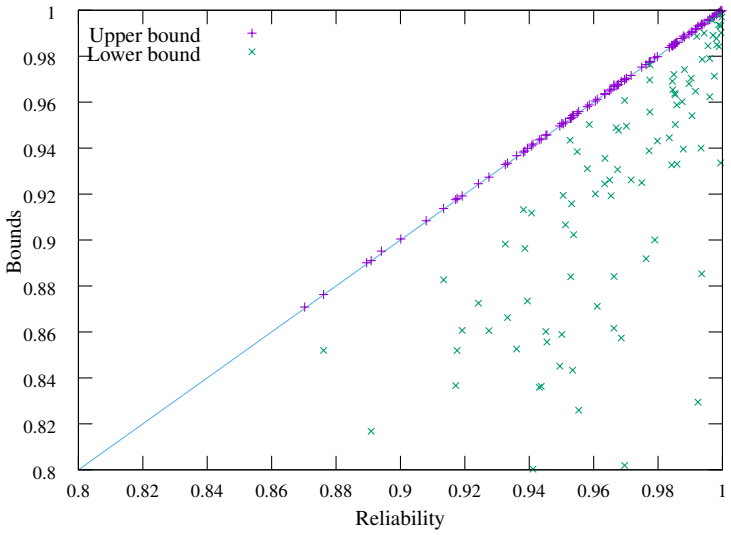


Figure 4.13: Lower and upper bounds versus the exact reliability for link availabilities in (0.99,1).

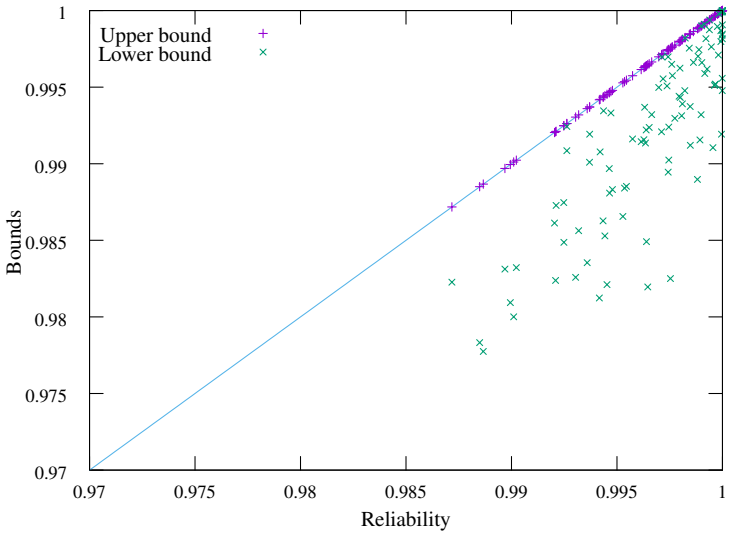


Figure 4.14: Lower and upper bounds versus the exact reliability for link availabilities in (0.999,1).

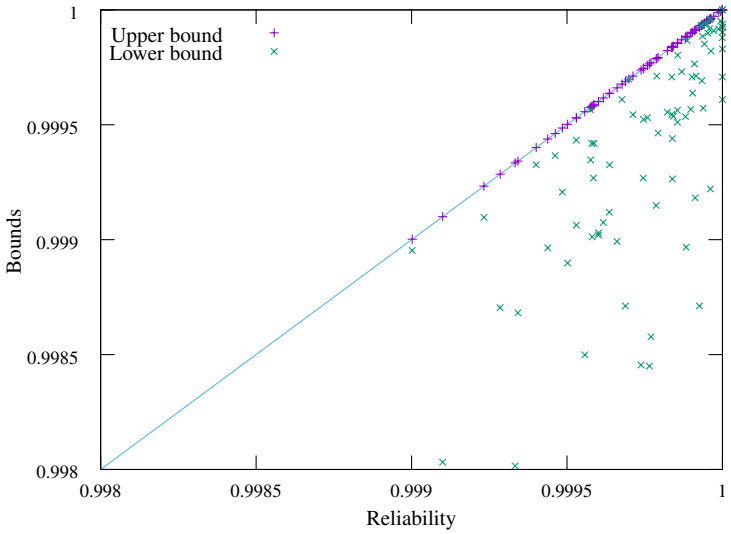


Figure 4.15: Lower and upper bounds versus the exact reliability for link availabilities in (0.9999,1).

4.5 Conclusion

In this section, I proposed a method to compute lower and upper bounds of reliability for multi-domain networks, without disclosing intra-domain information. The problem is

partitioned into subproblems for each domain, which are privately solved by each domain. The partial results, collected using secure computation techniques, were processed to yield the bounds. Experiments indicated that our method scales very well to support 14 domains with 907 links. The bound gaps are less than 0.001 with high availability links of 0.9999.

Chapter 5

Feasibility Evaluation of Network Path Control

Since the resource change use cases that change the traffic volume of connected services can take up to a few hours, network deployment or change requires switching time within minutes to avoid affecting existing services. This chapter describes the field evaluation of dynamic path control across multi-provider networks, such as creating inter-domain network paths, QoS recovery, and LSP failure recovery. Section 5.1 shows Ethernet Transport Path Creation over three domain networks. Section 5.2 shows QoS TE and Failure Recovery of an intra-domain network.

5.1 Ethernet Transport Path Creation over three domain Networks

5.1.1 Experimental Network

Figure 5.1 shows the three OXC domain network configuration consisting of Domain A and B in Japan and Domain C in the US. Each domain in JGN Ⅱ has three OXCs from different vendors, called type-A OXC and type-B OXC, respectively [76]. Domain A comprises multiple ASBR-OXCs, because type-A OXCs in Domain A were connected to IP routers with GMPLS based UNIs (GMPLS-UNIs) or OIF-UNIs. The domain of the Enlightened testbed in the US comprises three OXCs. During the experiment, the OXC in Osaka was used as an ingress node. Egress nodes were provided using the OXCs in Kanazawa in Domain B, and Baton Rouge or Raleigh in Domain C. A packet generator was equipped in both ingress and egress locations, and the traffic flow was transported from an egress node (Baton Rouge, Raleigh or Kanazawa) to the ingress node (Osaka). The STP in L2SW was activated in the US, and was inactive in Japan. Thus, the STP convergence time is not included in the activation time of the Ethernet Transport service in Japan.

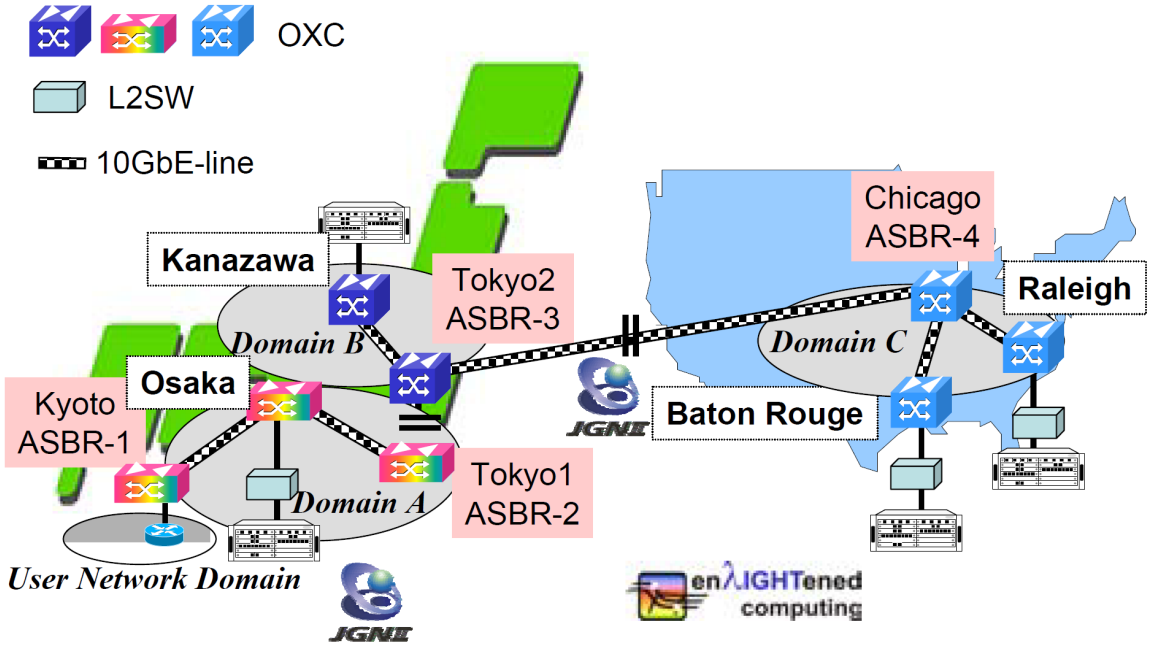


Figure 5.1: Experimental network configuration.

5.1.2 Experimental Results

I measured the activation time of Ethernet transport service over optical LSPs, which are connected to two different egress nodes through either three or two domains. The issue of the gateway node selection was solved by injecting the gateway node information toward destination into the ingress domain. The ingress node then calculates a route to the gateway node within the ingress domain. Hence, I successfully confirmed inter-domain Resource Reservation Protocol (RSVP) signalling. As shown in Figure 5.2, the ingress node automatically inserted a numbered TE link address into Explicit Route Object (ERO) of the RSVP messages to reach a proper gateway node to create the inter-domain optical LSP, even though there were multiple ASBR-OXCs in the ingress domain. Figure 5.3 (a) shows measured traffic flow carried over the LSP between Raleigh and Osaka over three domains. The generated traffic was set to the UDP flow of 800 Mbit/s with measured time resolution of 0.5s. The total service activation time of the Ethernet transport services between Raleigh and Osaka was 31 s (signalling time: 4 s, linkup time of Ethernet connectivity: 5s, L2SW STP time: 22 s.). On the other hand, Figure 5.3 (b) shows that between Kanazawa and Osaka. The total service activation time over two domains was 10 s including signalling time: 4.5 s, linkup time of Ethernet connectivity: 5.5 s. In this case, the STP is not used. From these results, I expect that I would be able to create a path between Raleigh and Osaka in around 10 s, if the STP of L2SW were not used inside the US domain.

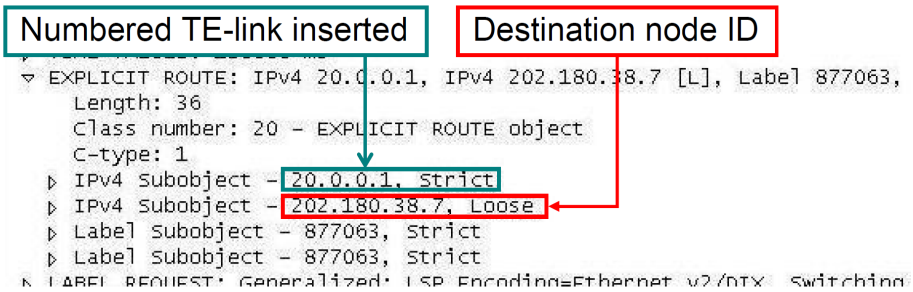


Figure 5.2: Captured signalling message for the interdomain LSP at the ingress node.

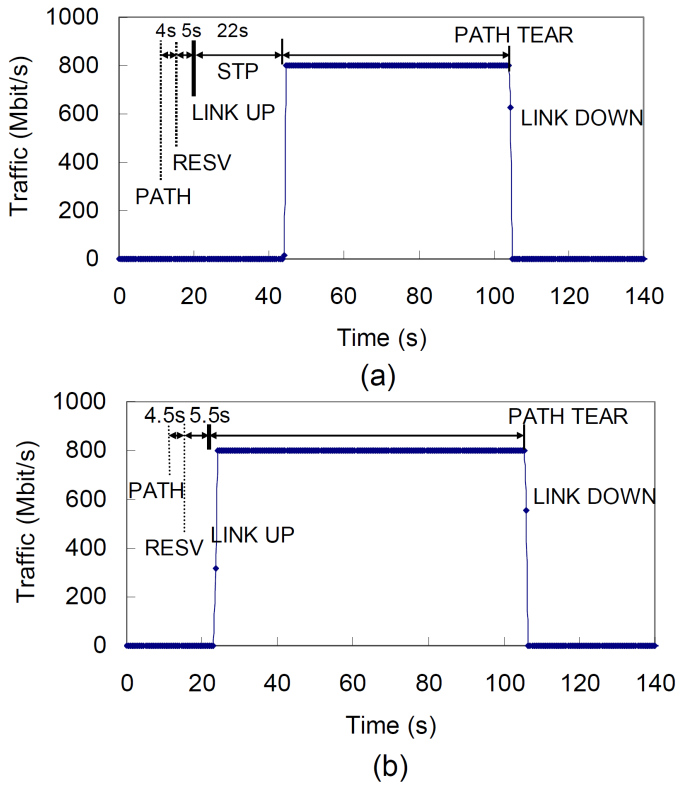


Figure 5.3: Measured time evaluation of traffic flow over LSPs from (a) Raleigh and (b) Kanazawa to Osaka.

5.2 QoS TE and Failure Recovery

5.2.1 JGN II Network Testbed

The JGN II network testbed had been operated by the National Institute of Information and Communications Technology (NICT) since April 2004 to promote R&D activities related to advanced networking technologies [76, 77]. One main R&D target includes the operational evaluation of GMPLS inter-carrier networking technologies considering

the prevalence of inter-carrier MPLS transport services such as MPLS-VPN services. On the other hand, the JGN Ⅱ network testbed also provides various types of NSs such as the Ethernet connection service (L2 service) and IP connection service (L3 service), as well as optical wavelength service based on the ASON/GMPLS controlled OXCs. Figure 5.4 shows an overview of the GMPLS network in the JGN Ⅱ network testbed. The network consists of two domains constructed using two different types of OXCs called the Type-A OXC and Type-B OXC. Type-A OXCs comprise three-dimensional Micro Electro-Mechanical Systems (3DMEMS) in optical switch fabric, and Type-B OXCs employ planar light wave circuits (PLCs) controlled by the thermal effect. The Type-A OXC equipped in the northern part of the network cross-connects gigabit or STM-64 optical paths, whereas the Type-B OXC equipped in the southern part cross-connects STM-64 optical paths. In the southern network domain, Type-B OXCs support integrated management of the optical switch fabric and wavelength multiplexed fiber links. Type-B OXCs can isolate in a sophisticated way the failure of optical switches, fiber links, or optical amplifiers based on ITU-T G.872 OTN architecture. Also, Type-B OXCs support two kinds of section architecture, namely, the OTN section and the pre-OTN (synchronous digital hierarchy/ synchronous optical network (SDH/SONET) based wavelength division multiplexing) section.

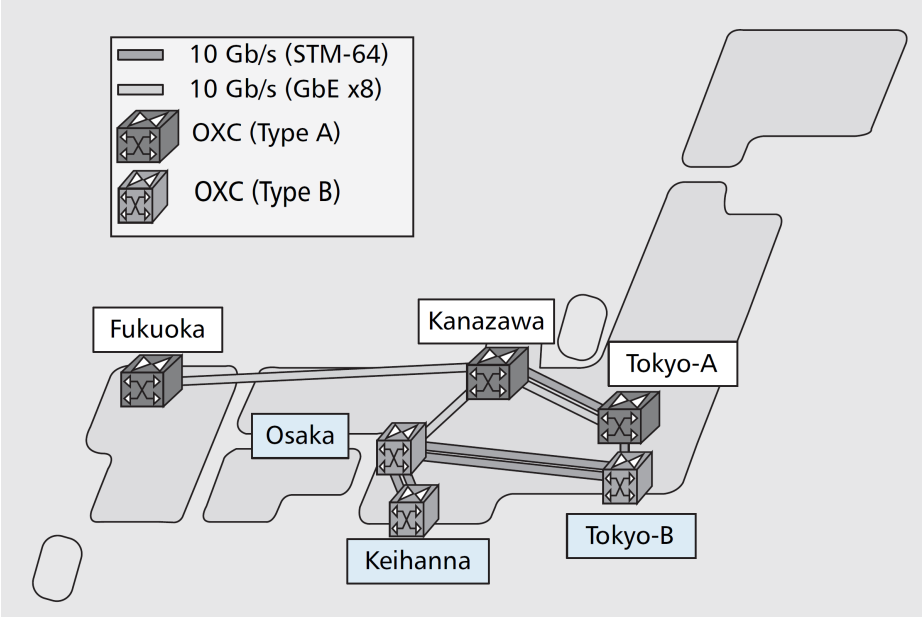


Figure 5.4: GMPLS network configuration of JGN Ⅱ.

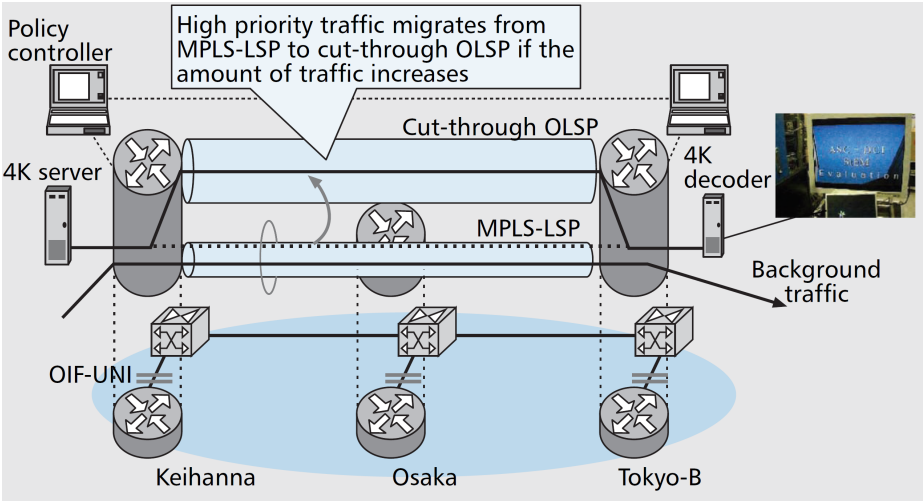
5.2.2 Target of Experimental Studies

The main target of this study is the feasibility evaluation of the TE capability of the ASON/GMPLS control-plane technology to control the QoS of IP traffic flows that traverse over multi-domain networks and various types of reference points. Specifically, this study focuses on the feasibility evaluation of QoS recovery using dynamic cut-through

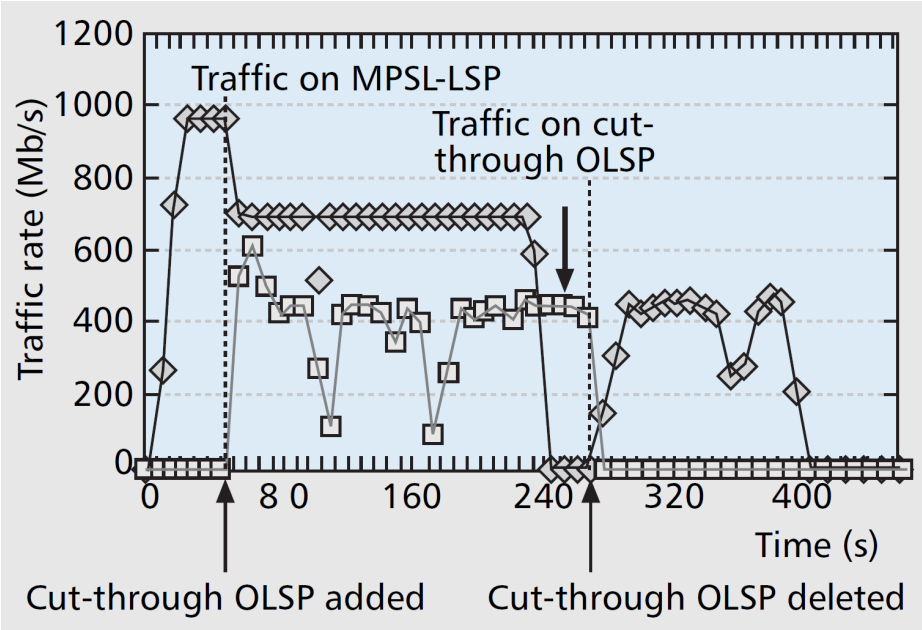
OLSP creation and link failure recovery by restoration, making use of the inherent ASON/GMPLS control-plane functionality and the state-of-the art OXC and OTN technologies. QoS recovery link and failure recovery represent the fundamental motivation behind deploying the ASON/GMPLS control-plane technologies in the Research and Educational (R&E) testbed community. Additionally, implementing even part of these promising functionalities will pave the way to new types of services in commercial networks.

5.2.3 Experiment over JGN II Network Testbed

Figure 5.5 a shows details of the experimental configuration over the JGN II network testbed. As shown in the figure, the testbed in the trial comprises OXCs and routers at three locations, Keihanna, Osaka, and Tokyo-B, which are 500 km apart. In this experiment, 4K digital cinema is used as an example of a broadband application that requires optical networks to satisfy QoS requirements such as the GMPLS network. The NTT Network Innovation Laboratories are promoting and developing the 4K digital cinema system [78]. The 4K super high definition images used in the system have roughly 4,000 horizontal and 2,000 vertical pixels, offering approximately four times the resolution of the high definition (HD) television format and 24 times that of a standard broadcast TV signal. The system mainly consists of a 4K streaming server, decoder, and projector. I utilized two types of paths in the JGN II network testbed to confirm the traffic engineering mechanism. One is an MPLS-LSP whose bandwidth is 1 Gb/s Ethernet. The other type of path is a cut-through OLSP between Keihanna and Tokyo, which cuts through an intermediate router in Osaka.



(a)



(b)

Figure 5.5: a) Experimental configuration in JGN II network; b) traffic monitors during the migration of 4K traffic between MPLS-LSP and cut-through OLSP.

In the actual experiment, initially both the 4K digital cinema traffic, which is given higher priority, and the background best effort traffic are transmitted from the router in Keihanna to the router in Tokyo through the router in Osaka. The policy controllers are configured with threshold bandwidth $R_{thh}(\alpha)$ $(= \alpha \times Bw)$ for the purpose of moving the appropriate traffic flows from the MPLS-LSP to the cut-through OLSP and for the opposite case, $R_{thl}(\alpha)$. Here, α is the threshold parameter set according to the operational policy, and Bw is the MPLS-LSP bandwidth [79]. According to the configuration, the policy controllers for the QoS recovery determine when the cut-though OLSP is set up/torn

down by monitoring the traffic flows on the MPLS-LSP. These controllers also manage the routing functionality in the routers so that the 4K traffic flow, as expedited forwarding (EF) traffic, can use the cut-through OLSP, and other traffic can use the MPLS-LSP. When the traffic flow in the MPLS-LSP exceeds $R_{thh}(\alpha)$, the 4K digital cinema traffic migrates automatically from the MPLS-LSP to the cut-through OLSP controlled by the policy controllers. Each policy controller monitors the volume of traffic flow every eight seconds. For the threshold bandwidth of $R_{thh}(\alpha)$ and $R_{thl}(\alpha)$, the upper threshold parameter a was set to 80 percent of the bandwidth of the MPLS-LSP, and the lower threshold parameter was set to 30 percent of the bandwidth.

Traffic monitoring data during the migration of the 4K digital cinema traffic flow between the MPLS-LSP and the cut-through OLSP is shown in Figure 5.5b. The amount of 4K digital cinema traffic is approximately 450 Mb/s, and the total amount of background traffic is 700 Mb/s. The policy controllers require approximately 16 seconds to make the determination to set up or tear down the cut-through OLSP. As shown in Figure 5.5b, the 4K digital cinema traffic flow successfully moved from the MPLS-LSP to the cut-through OLSP when the background traffic was injected at eight seconds, and moved back from the cut-through OLSP to the MPLS-LSP when the background traffic was terminated at 248 seconds. Each migration takes approximately 32 seconds, including the determination time of the policy controller and the time to physically set up/tear down the cut-through OLSP. In both cases, I confirmed that there was no confusion in the video images when migrating the 4K digital cinema traffic flow and that the QoS recovery of the 4K digital cinema traffic was successfully achieved.

5.2.4 Link Failure Recovery Experiment

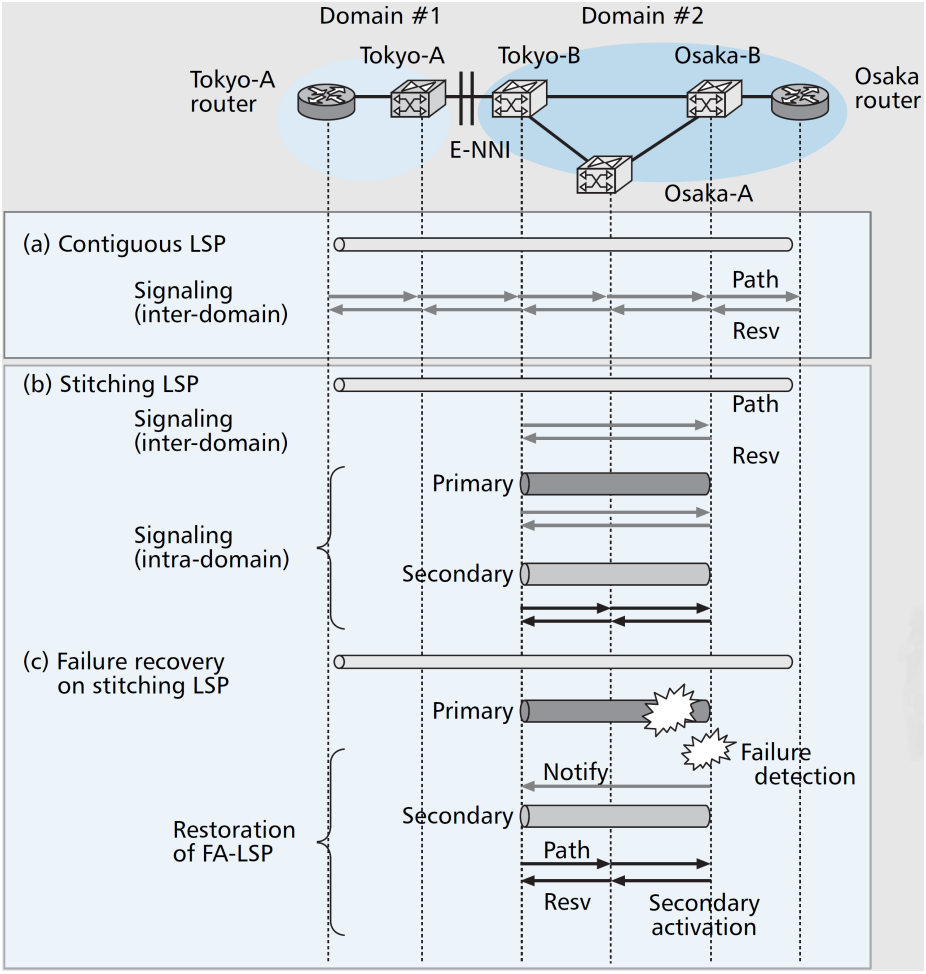
Next I conducted a link failure recovery experiment. I focused in particular on the link failure recovery of intercarrier LSPs. This section describes the requirements for inter-carrier LSP recovery and evaluate the stitching LSP architecture to meet these requirements.

5.2.4.1 Requirement for Inter-carrier LSP Recovery

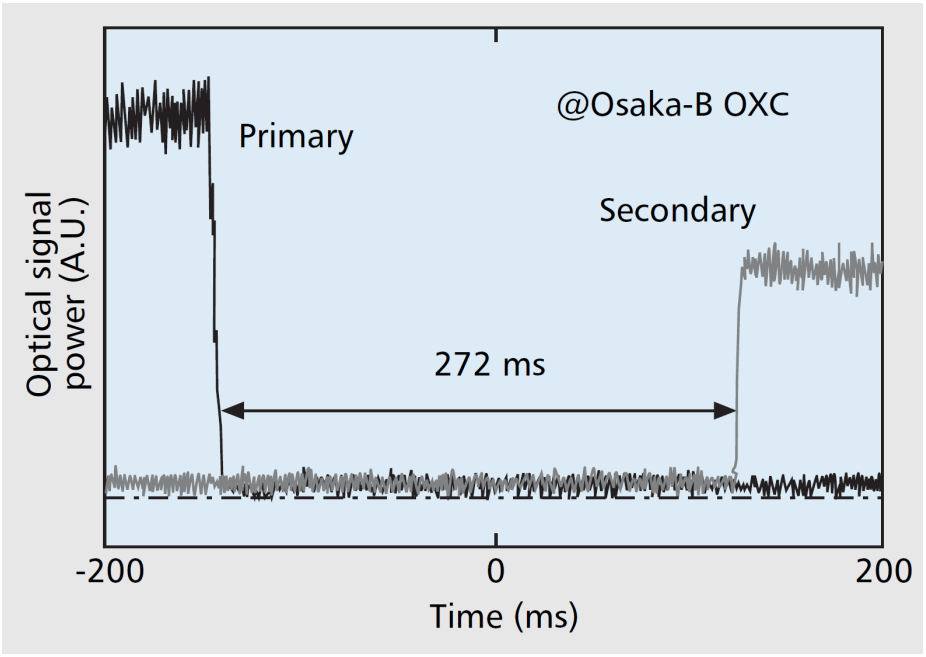
Considering the basic inter-carrier operational environment, independent LSP control in each domain is desired. Furthermore, it is desired to support not only end-to-end LSP recovery operation, but also recovery operation on a domain-to-domain basis to prevent the failure affecting one domain to another. The logically hierarchical LSP architecture is an effective solution to enhance the independency of LSP control in each carrier domain while ensuring end-to-end LSP control over multiple carrier domains.

The stitching architecture prevents undesired outflow of the link failure information to other domains in a sophisticated way. Figure 5.6a shows the logical architecture of a single layer (contiguous) LSP and hierarchical (stitching) LSP compared from the viewpoint of the intercarrier operation [80]. In the case of contiguous LSPs, the operation is very simple, and this case is suitable for a single operator multi-domain environment, because only a single session must be maintained. On the other hand, in the case of a stitching LSP,

to manage and control inter-carrier LSPs on a domain-to-domain basis, the end-to-end LSP is logically configured by stitching intracarrier LSPs to each other. By introducing a stitching mechanism to control the intra-carrier LSPs, even inter-carrier TE can be treated as intradomain TE while eliminating the requirement for any LSP control messages to other domains.



(a)



(b)

Figure 5.6: a) LSP architecture and RSVP with TE Extensions (RSVP-TE) signaling session of contiguous LSP and stitching LSP, and link failure recovery on stitching LSP; b) measured optical signaling power of primary and secondary paths.

5.2.4.2 Experiment over LSP JGN Ⅱ Network Testbed

Figure 5.6a shows the network configuration over the JGN Ⅱ network testbed comprising two operational domains connected by 10-Gb/s SDH/SONET links. I evaluated both contiguous and stitching LSPs using the testbed. During the evaluation, the OSPF-TE was running in each domain, but routing information was not dynamically exchanged between carrier domains.

I evaluated the stitching LSP creation in conjunction with network restoration on a domain-to-domain basis. To create an inter-carrier end-to-end LSP, an intra-carrier LSP was initially established from Tokyo-B to Osaka-B and then, advertised as a forwarding adjacency (FA) to make the created intra-carrier LSP a virtual TE link. Subsequently, the intercarrier LSP was successfully created by stitching the intracarrier LSP. The restoration operation of inter-carrier LSPs also was evaluated. Intra-carrier LSP failure recovery is achieved by the RSVP-TE-based end-to-end restoration protocol. Due to the introduction of the stitching LSP architecture, a failure along even the inter-carrier LSP affects only the stitched FA-LSP within a domain, and the session can be maintained, although the end-toend RSVP restoration operation caused the LSP to fail during a disruption. In the experiment, optical signal failure was caused by cutting the fiber link from the Tokyo-B OXC to the Osaka-B OXC. I successfully confirmed subnetwork restoration on a domain-to-domain basis at 272 ms as shown in Figure 5.6b. By introducing a hierarchical signaling mechanism, independent network operation in different domains can be achieved without affecting the end-to-end RSVP-TE session in an actual operational environment.

5.3 Conclusion

My evaluation clarifies the inter and intra-domain traffic engineering capabilities, namely, the inter-domain path creation, QoS recovery by dynamically creating cut-through OLSPs, and link failure recovery of the OLSPs. The activation time of interdomain path creation and QoS recovery indicates that the proposed traffic control scheme can be applied to NSs that require QoS recovery within minutes with the low packet loss rates in multi-provider networks. Link failure recovery was also confirmed by using hierarchal LSP over the JGN Ⅱ network testbed.

Chapter 6

Conclusions and Future Work

A novel method for uniting multi-provider networks dynamically or for assessing their reliability was proposed. My scheme can handle an IP transit model and direct peering models for realistic operational scenarios and can solve practical issues: overload, security, and location specifications. Additionally, my proposed multi-domain network reliability evaluation showed the same accuracy as existing methods without intra-domain network information. Moreover, network control scenarios, i.e., inter-domain path generation, intra-domain switching, and disaster recovery, were evaluated and demonstrated that the use case was feasible. A mechanism for exchanging parameters to connect network domains was proposed and has been accepted by the ETSI GR NFV-IFA022 standard report [37]. This result will help improve the efficiency and operability of networks and lead to further improvements in services. Future work will assume a specific use case and identify which parameters need to be exchanged for operation, administration, and maintenance.

- Specific use cases:
  Although the use cases of vCPE were evaluated, ETSI NFV proposes a number of use cases that require different functional requirements [5]. For example, in the VNF forwarding graph use case, sharing the cost and delay information of network links and nodes among providers enables appropriate places to launch VNFs. Thus, It is necessary to analyze the use case clarify what information needs to be exchanged among providers.

- Operation, administrative and maintenance:
  Various studies has been conducted on resource allocation mechanisms as shown in the related work. However, assuming real operation, the function of maintenance and monitoring must also be required. Exchanging operational, administrative, and maintenance parameters can help you quickly understand network conditions and failure recovery. There is no mechanism to detect network anomalies from other providers on another provider's network due to intra-domain privacy. Thus, if there is a mechanism to share the network status between providers, it may be possible to predict failures in advance.

Acknowledgements

My heartfelt appreciation goes to Prof. Shigeo Urushidani whose provided me with the valuable opportunity to study as a Ph.D. student under his guidance. I am also indebted to Prof. Takashi Kurimoto and Prof. Atsuko Takefusa, whose comments made an enormous contribution to my work. I am very grateful to Dr. Takeru Inoue of NTT Network Innovation Laboratories for his valuable cooperation in my experiments. I would like to thank Kohei Mizuno and Katsuhiro Shimano of NTT Network Innovation Laboratories for a grant that made it possible to complete this study. Finally, I would like to express my gratitude to my family for their moral support and warm encouragement.

Bibliography

[1] F. Moskowitz, "The analysis of redundancy networks," *Transactions of the American Institute of Electrical Engineers, Part I: Communication and Electronics*, vol. 77, no. 5, pp. 627–632, 1958.

[2] L. Fratta and U. G. Montanari, "A boolean algebra method for computing the terminal reliability in a communication network," *IEEE Transactions on Circuit Theory*, vol. 20, no. 3, pp. 203–211, 1973.

[3] F. T. Boesch, A. Satyanarayana, and C. L. Suffel, "A survey of some network reliability analysis and synthesis results," *Networks*, vol. 54, no. 2, pp. 99–107, 2009.

[4] I. B. Gertsbakh and Y. Shpungin, *Models of network reliability: analysis, combinatorics, and Monte Carlo*. CRC press, 2009.

[5] "ETSI GS NFV001 V1.1.1 Network Functions Virtualisation (NFV); Use Cases," ETSI ISG NFV, 2015.

[6] "Service Operations Specification MEF 55 Lifecycle Service Orchestration (LSO): Reference Architecture and Framework," MEF, 2016.

[7] "3GPP TS 28.530 V15.2.0 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Management and Orchestration; Concepts, use cases and requirements (Release 15)," 3GPP, 2019.

[8] L. G. Valiant, "The complexity of enumeration and reliability problems," *SIAM Journal on Computing*, vol. 8, no. 3, pp. 410–421, 1979.

[9] M. O. Ball, "Computational complexity of network reliability analysis: An overview," *IEEE Transactions on Reliability*, vol. 35, no. 3, pp. 230–239, 1986.

[10] M. Lê, M. Walter, and J. Weidendorfer, "Improving the Kuo-Lu-Yeh algorithm for assessing two-terminal reliability," in *Proc. of European Dependable Computing Conference*, pp. 13–22, 2014.

[11] T. Inoue, "Reliability analysis for disjoint paths," *IEEE Transactions on Reliability*. Accepted.

[12] J. Kawahara, K. Sonoda, T. Inoue, and S. Kasahara, "Efficient construction of binary decision diagrams for network reliability with imperfect vertices," *Reliability Engineering & System Safety*, vol. 188, pp. 142 – 154, 2019.

[13] M. Nishino, T. Inoue, N. Yaasuda, S. ichi Minato, and M. Nagata, "Optimizing network reliability via best-first search over decision diagrams," in *Proc. of IEEE Conference on Computer Communications*, INFOCOM, pp. 1817–1825, 2018.

[14] T. Mano, T. Inoue, K. Mizutani, and O. Akashi, "Virtual network embedding across multiple domains with secure multi-party computation," *IEICE Transactions on Communications*, vol. E98.B, no. 3, pp. 437–448, 2015.

[15] T. Mano, T. Inoue, D. Ikarashi, K. Hamada, K. Mizutani, and O. Akashi, "Efficient virtual network optimization across multiple domains without revealing private information," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 477–488, 2016.

[16] I. Houidi, W. Louati, W. B. Ameur, and D. Zeghlache, "Virtual network provisioning across multiple substrate networks," *Computer Networks*, vol. 55, no. 4, pp. 1011–1023, 2011.

[17] Y. Xin, I. Baldine, A. Mandal, C. Heermann, J. Chase, and A. Yumerefendi, "Embedding virtual topologies in networked clouds," in *Proceedings of the 6th international conference on future internet technologies*, pp. 26–29, ACM, 2011.

[18] K. Guo, Y. Wang, X. Qiu, W. Li, and A. Xiao, "Particle swarm optimization based multi-domain virtual network embedding," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 798–801, IEEE, 2015.

[19] B. Lv, Z. Wang, T. Huang, J. Chen, and Y. Liu, "Virtual resource organization and virtual network embedding across multiple domains," in *2010 International Conference on Multimedia Information Networking and Security*, pp. 725–728, IEEE, 2010.

[20] I. Vaishnavi, R. Guerzoni, and R. Trivisonno, "Recursive, hierarchical embedding of virtual infrastructure in multi-domain substrates," in *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*, pp. 1–9, IEEE, 2015.

[21] F. Esposito, D. Di Paola, and I. Matta, "A general distributed approach to slice embedding with guarantees," in *2013 IFIP Networking Conference*, pp. 1–9, IEEE, 2013.

[22] F. Samuel, M. Chowdhury, and R. Boutaba, "PolyViNE: policy-based virtual network embedding across multiple domains," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–23, 2013.

[23] D. Dietrich, A. Rizk, and P. Papadimitriou, "Multi-provider virtual network embedding with limited information disclosure," *IEEE Transactions on Network and Service Management*, vol. 12, no. 2, pp. 188–201, 2015.

[24] J. M. Wilson, "An improved minimizing algorithm for sum of disjoint products (reliability theory)," *IEEE Transactions on Reliability*, vol. 39, no. 1, pp. 42–45, 1990.

[25] A. Satyanarayana and M. K. Chang, "Network reliability and the factoring theorem," *Networks*, vol. 13, no. 1, pp. 107–120.

[26] J. Carlier and C. Lucet, "A decomposition algorithm for network reliability evaluation," *Discrete Applied Mathematics*, vol. 65, no. 1, pp. 141 – 156, 1996. First International Colloquium on Graphs and Optimization.

[27] K. Sekine, H. Imai, and S. Tani, "Computing the Tutte polynomial of a graph of moderate size," in *Proc. of International Symposium on Algorithms and Computation*, pp. 224–233, 1995.

[28] E. Canale, F. Robledo, P. Romero, and P. Sartor, "Monte Carlo methods in diameter-constrained reliability," *Optical Switching and Networking*, vol. 14, pp. 134–148, 2014.

[29] "Network Functions Virtualization – White paper on NFV priorities for 5G," ETSI ISG NFV, 2017.

[30] C. J. Bernardos, L. M. Contreras, I. Vaishnavi, R. Szabo, X. Li, F. Paolucci, A. Sgambelluri, B. Martini, L. Valcarenghi, G. Landi, D. Andrushko, and A. Mourad, "Multi-domain network virtualization," Internet-Draft draft-bernardos-nfvrg-multidomain-05, Internet Engineering Task Force, 2018. Work in Progress.

[31] J. Murayama, T. Tsujimoto, K. Matsui, K. Matsuda, and H. Ishii, "Traffic-driven optical IP networking architecture," *IEICE transactions on communications*, vol. 86, no. 8, pp. 2294–2301, 2003.

[32] Y. Nakahira, "Traffic driven IP optical path rearrange network system using PSC/LSC multi-layer GMPLS," *ECOC, Sep., 2004*, 2004.

[33] A. Taniguchi, S. Okamoto, J. H. Moore, Y. Sameshima, W. Imajuku, T. Otani, and Y. Okano, "Transpacific ethernet transport over GMPLS-based three administrative-domain photonic networks," in *33rd European Conference and Exhibition of Optical Communication*, pp. 1–2, VDE, 2007.

[34] A. Taniguchi, Y. Sameshima, S. Okamoto, T. Otani, Y. Okano, Y. Tsukishima, and W. Imajuku, "Operational Evaluation of ASON/GMPLS Interdomain Capability over a JGN II Network Testbed," *IEEE Communications Magazine*, vol. 46, no. 5, pp. 60–66, 2008.

[35] F. Paolucci, F. Cugini, A. Giorgetti, N. Sambo, and P. Castoldi, "A survey on the path computation element (pce) architecture," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1819–1841, 2013.

[36] "ETSI GS NFV 002 V1.1.1 Network Functions Virtulisation (NFV); Architectural Framework," ETSI ISG NFV, 2013.

[37] "ETSI GR NFV-IFA 022 V3.1.1 Network Functions Virtualisation(NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services," ETSI ISG NFV, 2018.

[38] "ETSI GR NFV-IFA 028 V3.1.1 Network Functions Virtualisation(NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains," ETSI ISG NFV, 2018.

[39] "ETSI GR NFV-IFA 032 V3.2.1 Network Functions Virtualisation(NFV) Release 3; Management and Orchestration; Interface and Information Model Specification for Multi-Site Connectivity Services," ETSI ISG NFV, 2018.

[40] "Interfaces for the Optical Transport Network (OTN)," ITU Rec. G.709/Y.1331, 2003.

[41] Y. Koike, T. Toide, A. Sutoh, M. Murakami, and K. Oda, "Intelligent and reliable photonic cross-connect system based on overlay model," *Journal of lightwave technology*, vol. 25, no. 6, pp. 1356–1371, 2007.

[42] "Architecture of Automatically Switched Optical Network (ASON)," ITU Rec. G.8080/Y.1304, 2006.

[43] A. Taniguchi, T. Yamazaki, Y. Yoshida, T. Kawabata, N. Sakaida, and T. Shimizu, "Impact of management data placement in NFV service coordinated across multiple datacenters and WANs," in *2015 11th International Conference on Network and Service Management (CNSM)*, pp. 406–409, IEEE, 2015.

[44] A. Taniguchi, T. Inoue, K. Mizuno, T. Kurimoto, A. Takefusa, and S. Urushidani, "Efficient reliability evaluation of multi-domain networks with secure intra-domain privacy," *IEICE Transactions on Communications*, vol. E103-B, no. 4, p. 12 pages.

[45] "ETSI GS NFV-EVE 005 V1.1.1 Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework," ETSI ISG NFV, 2015.

[46] "ETSI GS NFV-MAN 001 V1.1.1 Network Functions Virtualisation (NFV); Management and Orchestration," ETSI ISG NFV, 2014.

[47] "ETSI GS NFV-INF 005 V1.1.1 Network Functions Virtualisation (NFV); Infrastructure; Network Domain," ETSI ISG NFV, 2014.

[48] "IEEE STD 802.1ad Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges," tech. rep., 2005.

[49] "ETSI GS NFV-IFA 014 V2.1.1 Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Network Service Templates Specification," ETSI ISG NFV, 2016.

[50] "ETSI GS NFV-IFA 013 V2.4.1 Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification," ETSI ISG NFV, 2018.

[51] "ETSI GS NFV-IFA 005 V2.1.1 Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification," ETSI ISG NFV, 2016.

[52] "IETF 4364 BGP/MPLS IP Virtual Private Networks (VPNs)," tech. rep., 2006.

[53] "IETF 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks," tech. rep., 2006.

[54] "IETF 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," tech. rep., 2007.

[55] "IETF 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling," tech. rep., 2007.

[56] "IETF 7080 Virtual Private LAN Service (VPLS) Interoperability with Provider Backbone Bridges," tech. rep., 2013.

[57] "IETF 7432 BGP MPLS-Based Ethernet VPN," tech. rep., 2015.

[58] "IETF 7348 Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," tech. rep., 2014.

[59] "IETF 7637 NVGRE: Network Virtualization Using Generic Routing Encapsulation," tech. rep., 2015.

[60] "ONUG Software-Defined WAN Use Case – A white paper from the ONUG SD-WAN Working Group," tech. rep., 2014.

[61] "ETSI GS NFV-IFA 010 V2.1.1 Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Functional requirements specification," ETSI ISG NFV, 2016.

[62] W. Shen, M. Yoshida, K. Minato, and W. Imajuku, "vConductor: An enabler for achieving virtual network integration as a service," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 116–124, 2015.

[63] J. Bartelt, P. Rost, D. Wubben, J. Lessmann, B. Melis, and G. Fettweis, "Fronthaul and backhaul requirements of flexibly centralized radio access networks," *IEEE Wireless Communications*, vol. 22, no. 5, pp. 105–111, 2015.

[64] H. Raza, "A brief survey of radio access network backhaul evolution: Part II," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 170–177, 2013.

[65] "Openstack." `https://www.openstack.org/`. (Accessed on 10/02/2019).

[66] "Ryu SDN Framework." `http://osrg.github.io/ryu/`. (Accessed on 10/02/2019).

[67] "Lagopus switch and router." `http://www.lagopus.org/`. (Accessed on 10/02/2019).

[68] Y. E.Rosen, "BGP/MPLS IP VPNs," Internet-Draft draft-ietf-rfc254/bis-03.txt, Internet Engineering Task Force, 2004.

[69] "ANSI/IEEE Standard 802.1Q IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks," tech. rep., 1998.

[70] D. E. Knuth, *The Art of Computer Programming, Volume 4A, Combinatorial Algorithms, Part 1*. Addison-Wesley Professional, 1st ed., 2011.

[71] J. Rexford, J. Wang, Z. Xiao, and Y. Zhang, "BGP routing stability of popular destinations," in *Proc. of 2nd ACM SIGCOMM Workshop on Internet Measurment*, IMW '02, pp. 197–202, 2002.

[72] O. Goldreich, *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2004.

[73] C. Gentry, *A Fully Homomorphic Encryption Scheme*. PhD thesis, Stanford, CA, USA, 2009. AAI3382729.

[74] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The internet topology zoo," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 9, pp. 1765–1775, 2011.

[75] T. Inoue, H. Iwashita, J. Kawahara, and S. Minato, "Graphillion: software library for very large sets of labeled graphs," *International Journal on Software Tools for Technology Transfer*, vol. 18, no. 1, pp. 57–66, 2016.

[76] T. Otani, Y. Sameshima, S. Okamoto, and Y. Okano, "GMPLS/OXC network testbed of JGN II," in *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006.*, pp. 6–pp, IEEE, 2006.

[77] Y. Sameshima, T. Ohara, and Y. Okano, "Nation-wide GMPLS/OXC networking experiments over JGN II test bed," in *Optical Transmission Systems and Equipment for Networking V*, vol. 6388, p. 638801, International Society for Optics and Photonics, 2006.

[78] T. Yamaguchi, M. Nomura, K. Shirakawa, and T. Fujii, "SHD movie distribution system using image container with 4096/spl times/2160 pixel resolution and 36 bit color," in *2005 IEEE International Symposium on Circuits and Systems*, pp. 5918–5921, IEEE, 2005.

[79] Y. Tsukishima, A. Hirano, N. Nagatsu, T. Ohara, W. Imajuku, M. Jinno, Y. Takigawa, K. Hagimoto, L. Renambot, B. Jeong, J. Leigh, T. DeFanti, A. Verlo, and L. Winkler, "The first application-driven lambda-on-demand field trial over a US nationwide network," in *Optical Fiber Communication Conference*, p. PDP48, Optical Society of America, 2006.

[80] A. Farrel, J. Vasseur, and A. Ayyangar, "A framework for inter-domain multiprotocol label switching traffic engineering," *draft-ietf-ccamp-inter-domain-framework-06 (work in progress)*, 2006.

Publication lists

[1] A. Taniguchi, S. Okamoto, J. H. Moore, Y. Sameshima, W. Imajuku, T. Otani, and Y. Okano, "Transpacific ethernet transport over GMPLS-based three administrative-domain photonic networks," in *33rd European Conference and Exhibition of Optical Communication*, pp. 1–2, VDE, 2007.

[2] A. Taniguchi, Y. Sameshima, S. Okamoto, T. Otani, Y. Okano, Y. Tsukishima, and W. Imajuku, "Operational Evaluation of ASON/GMPLS Interdomain Capability over a JGN II Network Testbed," *IEEE Communications Magazine*, vol. 46, no. 5, pp. 60–66, 2008.

[3] A. Taniguchi, T. Yamazaki, Y. Yoshida, T. Kawabata, N. Sakaida, and T. Shimizu, "Impact of management data placement in NFV service coordinated across multiple datacenters and WANs," in *2015 11th International Conference on Network and Service Management (CNSM)*, pp. 406–409, IEEE, 2015.

[4] A. Taniguchi, T. Yamazaki, Y. Yoshida, T. Kawabata, N. Sakaida, and T. Shimizu, "A study on placement of management data of network functions and their managers when they are placed among multiple data centers (in Japanese)," *IEICE technical report*, vol. ICM2015-1, pp. 77–82.

[5] A. Taniguchi, Y. Minami, T. Kawabata, N. Sakaida, and T. Shimizu, "A study on data modeling for abstraction of management data when NFV service are placed among multiple datacenters (in Japanese)," *IEICE technical report*, vol. ICM2016-56, pp. 19–24.

[6] "Network Functions Virtualization – White paper on NFV priorities for 5G," ETSI ISG NFV, 2017.

[7] "ETSI GR NFV-IFA 022 V3.1.1 Network Functions Virtualisation(NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services," ETSI ISG NFV, 2018.

[8] Y. Minami, A. Taniguchi, T. Kawabata, N. Sakaida, and K. Shimano, "An architecture and implementation of automatic network slicing for microservices," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–4, IEEE, 2018.

[9] A. Taniguchi, T. Inoue, K. Mizuno, T. Kurimoto, A. Takefusa, and S. Urushidani, "Efficient Reliability Evaluation of Multi-Domain Networks with Secure Intra-Domain Privacy (in Japanese)," *IEICE technical report*, vol. 119, no. 196, 2019.

[10] A. Taniguchi, T. Inoue, K. Mizuno, T. Kurimoto, A. Takefusa, and S. Urushidani, "Efficient reliability evaluation of multi-domain networks with secure intra-domain privacy," *IEICE Transactions on Communications*, vol. E103-B, no. 4, p. 12 pages.