Noname manuscript No.
(will be inserted by the editor)

A New Framework for GLIF Interdomain Resource Reservation Architecture (GIRRA)

Gigi Karmous-Edwards · Silvana Greco Polito · Admela Jukan · George Rouskas

Received: August 31

Abstract Many existing and emerging Scientific high-end applications (E-science) require end-to-end circuits interconnecting Grid resources for large data transfers. A few advanced networks, mainly Research and Education Networks (NRENS), such as Surfnet, National Lambda Rail and Internet 2, now provide mechanisms for end-users to reserve and provision lightpaths via middleware referred to as Network Resource Mangers (NRMs). Although, some progress has been made in automated intra-domain lightpath services, inter-domain lightpath provisioning still requires manual intervention and presents several key challenges such as scalability of topology information exchanged, consistency and scalability of information model, security of access to the resources, hybrid networking and multilayer lightpaths, and accounting and billing.

In this paper, we describe a new architectural framework called GIRRA with the goal to provide an integrated response to these challenges. We propose a new approach to model GLIF network domains and GOLEs as virtual switches and to describe their behavior, functionality, policy capabilities, and topology aggregation. We define a inter-domain path computation model to determine paths that meet constraints and access policy restrictions. We propose a security framework for authentication and authorization of users and a model for accounting and billing that aims to provide easy and secure access to the resources. Key aspects of the GIRRA solution are that it focuses on the inter-dependence between different challenges of inter-domain path provision and it is built around already existing solutions for intra-domain resource provisioning.

Keywords Interdomain networking · security · path computation · GLIF · middleware

Gigi, Silvana and Admela
Department of Electrical Engineering, Institute of Computer and Network Engineering Technische Universitt Carolo-Wilhelmina zu Braunschweig
E-mail: gigi_ke@ncsu.edu

Gigi and George
Department of Computer Science, North Carolina State University, Raleigh, NC, USA.

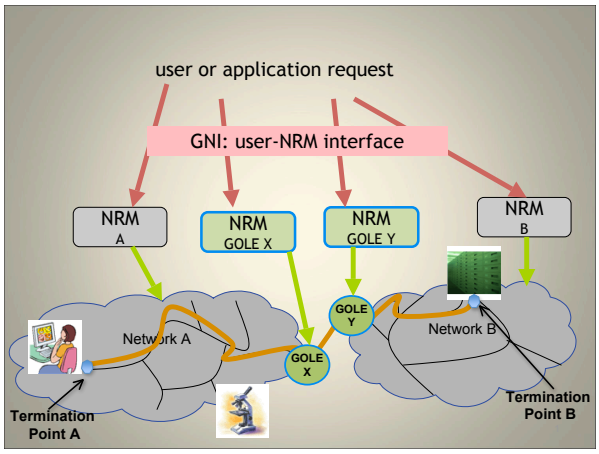

Fig. 1 Today's GLIF architecture

1 Introduction

Today many E-science researchers use applications that require high-capacity and deterministic end-to-end circuits. These existing and emerging applications [1], [2] contain large data flows of the terabyte and petabyte scale. Therefore, successful execution of these applications will need lightpath/lambda networking and on-the-fly per user/application provisioning mechanisms.

The Global Lambda Integrated Facility (GLIF) has been promoting the paradigm of Lambda networking since 2002 to help facilitate this growing class of high-end applications. In doing so, the GLIF consortium provides lambdas internationally as an integrated facility to support data-intensive scientific research, and supports middleware development for lambda networking, mostly free of charge to researchers. As described in Figure 1, GLIF resources comprise NREN network domains and GLIF Open Lambda Exchanges (GOLEs). GOLEs behave similar to Internet exchange points, in that most NRENs have static connections to one or more GOLEs. The fact that most of the NRENs are hybrid networks leads to a range of technologies available for stitching multilayered lightpaths end-to-end. The term stitching is referred to as the concatenation of different technologies into a single path, e.g.., source connected via an Ethernet partial path that is concatenated with a SONET partial path (to cross the Atlantic for example) and finally connected via Ethernet to the destination. The term multilayered in the context of this paper refers to a lightpath created across multiple network technologies with network elements supporting adaption between these technologies. An example of this is a lightpath carrying 1GB Ethernet over SONET using GFP-F. As the demand for global lightpath provisioning is increasing, the GLIF community is considering to open access to its resources to commercial applications as well. To this end, the GLIF community needs a new, user-initiated, automated and scalable inter-domain resource reservation and provisioning framework capable of handling security, accounting, and billing issues.

In recent years, the effort for automated resource provisioning in GLIF has focused on the design of software controllers known as Network Resourc Managers (NRMs).

NRMs represent pockets of automation within a domain, but inter-working solutions between NRMs for inter-domain provisioning is still an open issue. The provisioning of multi-domain network resources is challenging for multiple reasons. The hybrid nature of most of the NREN networks leads to a range of technologies available for creating multilayered lightpaths. Interoperability between different NRMs is required for multi-domain provisioning. As inter-domain path computation requires some level of topology and resource information to be exchanged between domains, a uniform description language and model is also required. Once a modeling framework is agreed upon by the resource owners, the main complexities lie with the amount and type of information that is required to be exposed by each domain, leading to scalability and security considerations. Exchange of information between domains implies a certain level of trust between domains and models for mutual authentication between them. To secure access to resources, while guaranteeing authorization-based provision, policy-based mechanisms are required. In addition, accurate accounting and billing functions are needed to facilitate payment for the provision of lightpaths.

In order to meet the complex challenge of inter-domain provisioning in GLIF, we contend that rather than solving each of these challenges independently, a holistic integrated solution must be developed, where interdependencies between key problem areas are identified and resolved. To this end, we present the design framework for GLIF resource reservations, called GLIF Interdomain Resource Reservation Architecture (GIRRA). GIRRA extends the NRM-based framework with tools to automate and secure GLIF resource provisioning in multi-domain contexts and builds on concepts currently under discussions in both the GLIF and Open Grid Forum (OGF) working groups, such as the Generic Network Interface (GNI) GLIF task force and the OGF's Network Service Interface (NSI).

Specifically, we propose an integrated solution that addresses the problem spaces of (i) model representation of domains and GOLEs and information exchange, (ii) authentication and authorization (AA) for security, (iii) inter-domain path computation, and (iv) accounting and billing.

With regards to model representation, we propose to model GLIF domains and GOLEs as virtual switches called Girra Virtual Switches (GVSs). In doing so, we capture the behavior and functionality of a network as GVS capabilities. The objective is to provide GOLE and domain information for path computation enriched with technology, security and administrative capabilities such as technology adaptation and multiplexing functions, access policy roles associated to the resources, and cost/value of the resources. These capabilities support the design of a novel multi-layer, multi-domain path computation model that encompasses security and advanced services as it allows computation based on the authorization profile of the requester, determination of the cost of the resources at the end of computation, and specification of different technological constraints for computation. The path computation model is based on an *a-priori* representation of a global GLIF topology with domains/GOLEs described as GVSs. Inter-domain coarse grain paths are first computed using this topology, and later intra-domain resources consistent with the inter-domain coarse grain path are computed independently within each domain; note that, for privacy and scalability reasons, GVS data does not include any intra-domain resource information. We assume that all intra-domain path computation and provisoning, including multilayer and technology adaptation considerations, are performed by the domains NRM and GIRRA does not interfere with existing domain/GOLE control and management. Since all resource reservation occurs during intra-domain path computation, all necessary

traffic grooming will not be considered during inter-domain path computation. The network resources are controlled and managed only by the domain/GOLE owners who are aware of other traffic running through the equipment to provide traffic grooming. The fine-grain path computation occurs only for the intra-domain path computation, which is handled by the NRMs, and therefore out of scope on the course-grain inter domain path computation. The term coarse grain is used in this paper for interdomain and only includes the domains and GOLEs involved in the path and their associated edge ports (including technologies, and policies, configurations).

The security framework that we integrate in GIRRA aims to secure access to the resources based on user authentication and authorization models and provides an infrastructure for resource provisioning based on collaboration between providers. We propose a federation-based trust model for GLIF providers and we provide a single and secure interface for access to the GLIF resources, accounting and billing. Users are asked to register with the federated GLIF providers for access to free services and are asked to register with a clearinghouse for access to commercial services. Registration corresponds to the submission of service level agreements (SLAs) that allow users to access resources provided by multiple providers. The trust model also allows the introduction of a collaborative model with accounting computed on the base of metering functions activated in one domain and using cost/value data advertised in the GVS representation of multiple domains.

The paper is organized as follows. In Section 2, we describe related work. In Section 3, we describe the GIRRA architecture and its design objectives. In Section 4, we introduce the GVS description model. Section 5 describes the GIRRA security framework, including its trust model and the interfaces for users to access the GLIF resources. The path computation model is presented in Section 6, while Section 7 describes the GIRRA accounting and billing framework. Finally, Section 8 provides a brief discussion and conclusion.

2 Standards and Related Work

2.1 Network Resource Managers (NRMs)

The GLIF community is an international virtual organization that promotes the paradigm of lambda (lightpath) networking based on circuit-switching. An important objective of GLIF is to enable international network connectivity along with the ability to reserve and provision lightpaths in advance and on the fly across NRENs. Note that individual domains typically employ a Network Resource Manager (NRM) to setup dynamic lightpaths between network elements within its purview. Examples of NRMs include Nortel DRAC [3], Phosphorous Harmony [4], ENL NRM [5], and DICE IDC [6]. Since these technologies have been developed independently of each other, several efforts are currently underway to enable interoperability between these NRMs. These efforts mainly entail the development of software wrappers between NRMs. While successful demonstrations of interoperability have taken place [7],[8], especially in contexts where scalability has not been critical, it is generally recognized that new control and management mechanisms are needed for dynamic provisioning of global lightpaths [9],[10].

2.2 Network Resource Information Models

Information models have been around for years. Existing models include the Common Information Model (CIM) [11] that provides an object-oriented schema for different devices but does not have a schema that represents some of the DWDM gear in a GLIF environment. The authors of [12] developed the Network Description Language (NDL) which is a modular set of schemas based on the Resource Description Format (RDF) mainly to describe networks. This functional model is based on ITU G.805 [13] with the addition of capability information. The use of NDL to represent the complex multi-layered GLIF resources has been demonstrated for the creation of a single-layer interdomain lightpath [14],[15]. This effort is now going through standardization in a new OGF working group called Network Markup Language working group (NML wg) [17]. The Stitching Framework [18] also developed an object oriented data model for inter-domain path computation. GIRRA will also build upon the efforts of the NDL team, and the work of the NML working group with a nuance of modeling a GVS, which has capabilities that are mapped from an entire domain or GOLE. A similar schema will be used to represent the GVS as the NDL representation of single physical devices.

2.3 Generic Network Interface (GNI) and Fenius Project

The GLIF consortium has been working towards a solution for interoperability between the NRMs mentioned above for several years and recently initiated a releated software development project referred to as Fenius [19]. The Fenius project is developing a single Generic Network Interface (GNI) API for experimentation. The purpose of this API is to have a single, agreed upon, user-to-network "service agent" API that can be translated to any existing single domain APIs (with existing NRMs as described above). GLIF is working closely with the OGF Network Service Interface (NSI) working group [20], which will use the experiences of the GNI API to develop the standard Network Service Interface (NSI) API. The NSI API is between a "requester agent" and a "network service agent," where the requester agent could be either a end-user or another network service agent.

2.4 AA and billing in Multi-Domain, Multi-Provider Networks

The design of a security framework for inter-domain resource provisioning in GLIF-like communities, such as GRID, is still a challenge [21],[22],[23],[24]. The heterogeneity of the GRID community is a serious challenge in defining and implementing a uniform and common security model for AA, hence most of the solutions proposed focus on interworking mechanisms between different security infrastructures deployed by the multiple GRID providers. Moreover, the insistence of GRID providers on keeping tight control of the authentication and the authorization data of their users increases the complexity of the inter-working AA models.

Outside the GRID community, lightpath provisioning with security features integrated in [25], or interworking with [27],[28], the GMPLS control plane has also been studied. In particular, [25] proposes to enhance the path computation protocol with features for AA of requesters. Most of the GRID solutions for accounting and billing refer to GRIDBanks [30],[29]. GRIDBanks obtain user usage records from

the service providers and manage the procedure for billing. The literature provides approaches [31],[32], that propose to use accounting not only to motivate resource contribution, but also to control resource sharing.

2.5 Interdomain Multilayer Path Computation

Path computation is defined as the mechanism that allows computation of optimal paths satisfying a set of user requirements. There are several existing algorithms today for path finding, however, not all of them consider multi-layer path computations as required for GLIF-type hybrid networks. With multi-layer paths, technology adaptation must be considered throughout the path finding process as a constraint. Recently, several papers have demonstrated results on the design of mechanisms and protocols for both intra- and inter-domain path computations [15],[34]. A comprehensive comparison of different interdomain models for path provisioning appears in [35], and key open issues are outlined, including interdomain topology exchanges, routing, and QoS and reliability of paths, for which no scalable solution yet exists. An important conclusion of [35] is that incorporating pre-computation models with PCE-based [33] path computation may result in a scalable solution.

Other unique approaches to address the inter-domain lightpath problem space include OBGP [37], where it is suggested to utilize the familiar layer 3 BGP framework and apply it to the optical layer for wavelength reachability across multiple domains. In [37], it was proposed that an optical domain is modeled as a distributed Layer 3 switch, controlled by "optical BGP". In [41] an alternative to the ITU's UNI/NNI concept is considered to provide a Multi-providor Federation Interface (MPFI) with a focus on policy-based requirements on services. Although a prototype of OBGP has been developed, neither approach has seen wide deployment yet.

3 GIRRA Architecture and Objectives

The proposed GIRRA architecture for automatic inter-domain resource provisioning encompasses resource description, abstraction and advertising models, multi-domain and multi-layer path computation, interfaces for secure accesses to the resources and for accounting and billing between users and the GLIF network. In the following, we first describe the objectives that have driven our design, and later we describe in detail each of its components as shown in Figure 2. We emphasize that the principle driving our design has been to reduce and simplify the information exchanged so as to facilitate interoperability among domains and a scalable path computation process.

3.1 GIRRA objectives

In the design of the GIRRA architecture we have the following main objectives. First, we want to introduce a new abstraction model of network domains and GLIF GOLEs that includes not just topology information as traditional models do, but also security and functional capabilities. The key challenge in the design of this model is the abstraction of resource description that provides exhaustive information for path computation with a controlled amount of description data.

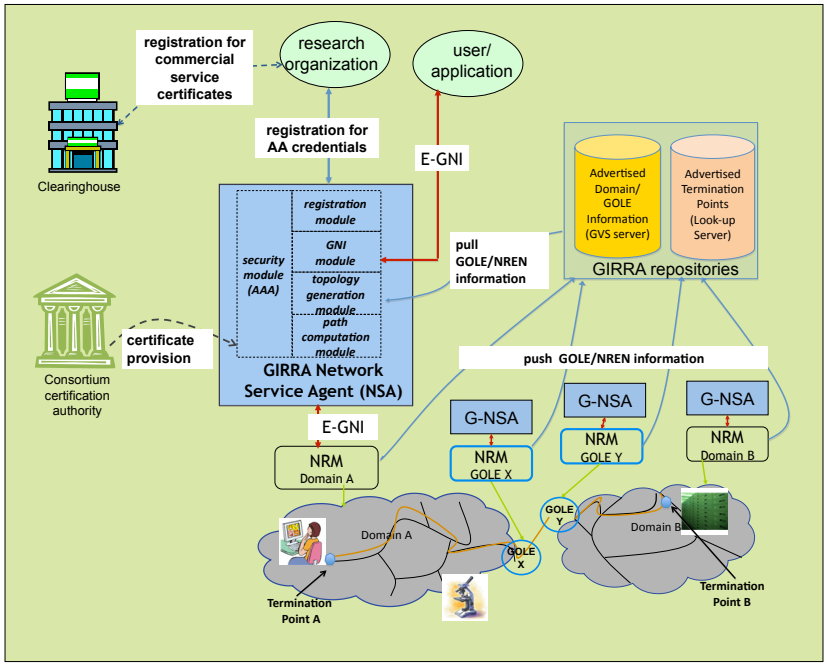

Fig. 2 GIRRA architecture and interfaces

Our second objective is to develop an advertising model with reduced traffic load for scalable exchange of information between domains. To achieve this objective we rely on the observation that key pieces of information useful for path computation, including functional and security capabilities, are relatively static.

Our third objective is about designing an inter-domain, multi-layer path computation model that builds upon existing NRM-based solutions. We assume that intra-domain resource reservations will only be conducted via the NRM of a given domain/GOLE. Inter-domain constraint-based path computations use the (mostly) static, abstracted GVS information, and take into account the authorization profile of users; the required technology adaptation and user request parameters are taken as constraints to determine the path suitable for each request.

Our fourth objective is an AA framework that allows secure access to resources according to network-imposed user authentication and path computation policies.

Lastly, we want to design an interface for access to the GLIF resources that makes the inter-domain path provisioning mechanism and the number of providers involved transparent to users, while guaranteeing accountability and billing for all the resources used.

3.2 GIRRA architectural components and interfaces

The GIRRA architecture we propose is shown in Figure 2. It is built around already existing components incuding the NRMs, the GNI interfaces that are enhanced to

achieve the GIRRA objectives and called Extended-GNI (E-GNI), and the network service agent for which a functional definition is under discussion in the OGF and GLIF working groups.

GIRRA Network Service Agent (G-NSA). The G-NSA is a key element of our architecture. It is responsible for the functions related to inter-domain and multi-layer path computation and to the access of users to the GLIF resources. We define five separate functional modules for G-NSA, namely, the registration module, the E-GNI module, the topology generation module, the path computation module, and the security module.

The registration module is responsible for verifying the identity and authorization profiles of research organizations and, more generally, of any entity interested in GLIF resources. It provides these entities with AA credentials that can be used multiple times for accessing resources.

The E-GNI module implements the interface to either the users or other G-NSAs for access to the services. On this interface, the G-NSA receives lightpath requests and interacts with the requesting entity for authentication and authorization purposes.

The topology generation module is responsible for generating a global virtual topology representing the GLIF network, using information describing domains/GOLEs stored in the repositories. This global topology is used by the computation module to compute coarse-grain inter-domain paths. In the context of this paper, coarse grain path computation refers only to the determination of which domains and GOLEs are involved in the path and their associated edge ports. It does not include detailed intra-domain path information. We assume that all intra-domain path computation and provisoning, including multilayer and technology adaptation considerations, are performed by the domains NRM and GIRRA does not interfere with existing domain/GOLE control and management systems. The path computation module also determines the finer-grain paths by concatenating the intra-domain paths computed by each NRM along the coarse-grain path. The G-NSA interacts with the NRMs to ask for and obtain these intra-domain paths.

The security module implements AAA (authentication, authorization, and accounting) functions. It is responsible for authenticating and authorizing resource requests coming through the E-GNI module. It performs accounting for resources using metering information received from the NRM. The security module also supports access policy control for resource provisioning. The path computation module interacts with the security module to verify the resources a user is authorized for that can be considered for computation.

GIRRA Virtual Switch (GVS) Repository and Termination point. Two key repositories are required for GIRRA: the GVS server and the termination point lookup server. The former collects abstracted information for each GLIF domain and GOLE representing both topology aggregation and functional capabilities/policies; the latter collects information regarding GLIF endpoints such as GLIF high-end compute, storage, or instrument resources.

Network Resource Managers (NRMs). NRMs are responsible for intra-domain path computation and reservation. There are two requirements which GIRRA assumes from the NRMs that does not exist in current NRMs: 1) the capability for pushing the GVS description information of their resources up to the repository servers and updating

it on a periodic basis; and 2) implementing metering functions and provide metering information to the GNSA for accounting.

Extended-Generic Network Interface (E-GNI). We refer to the GNI API on both the interfaces between user and G-NSA and between NRM amd G-NSA. We propose extensions to these interfaces (hence the term "extended") to add features for authentication of users on the user/G-NSA interface and for provision of metering/accounting information on the NRM/G-NSA interface. The G-NSA receives E-GNI requests from end users and can also make E-GNI requests to other NRMs via the GNI-Fenius framework.

In addition to the GIRRA components introduced above, we assume the existence of a certification authority and a clearinghouse for security and billing functions. The certification authority is responsible for issuing certificates used for AA of users and mutual authentication between domains. The clearinghouse supports accounting and billing functions and makes the heterogeneity of the GLIF providers transparent to users.

4 The GVS Description Model

Our work is motivated by the following key research questions we hope to answer:

> *Is it possible to model a network domain and GOLE as a capability-rich, topology-aggregated, virtual switch and provide enough key characteristics for this model to scale? And what is the minimum set of information that is readily available and relatively static for network administrators to easily compile, abstract, and advertise, as well as update on a periodic bases for workable solutions?*

Our modeling approach is inspired by (a) the Edge Reconfigurable Optical Network (ERON) [16] concept that enables scalable dynamic lightpath provisioning based on a mesh network of intelligent edge switches and static lightpaths, and (b) the description model of high-functioning network elements such as a MultiService Provisioning Platform (MSPP). MSPPs are described by a set of functions and capabilities that can be configured remotely. MSPP capabilities include technology adaptation, multiplexing/demultiplexing, cross-connections between pairs of interface on the same element, and restoration/protection services.

As seen in Figure 3, we describe each domain/GOLE as a virtual switch, called GIRRA Virtual Switch (GVS), and we model its functionalities, behaviors, policies, and features as GVS capabilities. In doing so, we borrow concepts from remote MSPP management. For instance, an MSPP allows for the creation of a cross-connect between two ports having different technologies (e.g., SONET and Ethernet WAN), as long as an appropriate technology adaptation capability is applied to the cross-connect.

Key aspects of the GVS description model include: (a) the determination of a resource description abstraction level that provides enough information for inter-domain computation with a controlled amount of easy to elaborate data, and (b) identification of domain/GOLE functions and capabilities that are relatively static and available for network administrators to collect. Using relatively static information leads to an advertising model in which information provided once can be used for computation related to multiple requests. This causes a reduced amount of advertising information compared with per-lightpath request adverting models.

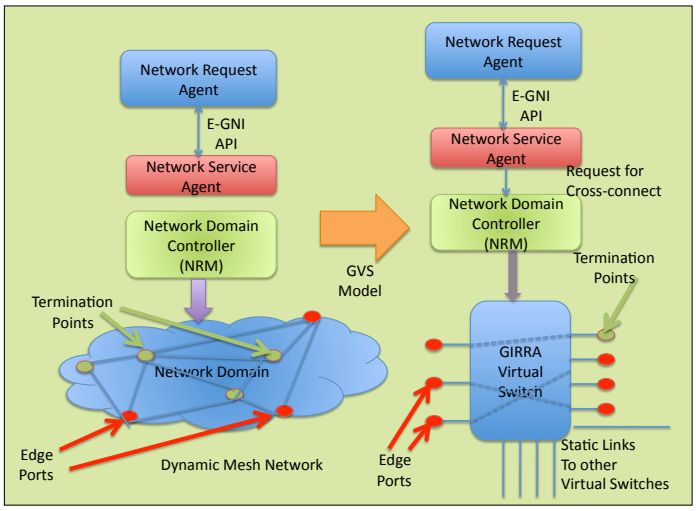

Fig. 3 Domain Modeled as GVS

GVS Description of Resources and Topology Aggregation. We propose to model an entire domain or GOLE comprising several physical network elements into a single virtual switch we termed GVS. The novel GVS model contains representation of only the domain/GOLE edge ports after topology aggregation as potential cross-connecting ports on the single virtual switch. Along with edge port representation on the GVS, we also model the functionality/policy and features of the entire domain or GOLE as GVS capabilities. To this end, we build upon existing efforts for modeling capability and ports/interfaces such as NDL, NML wg or the Stitching framework that we discussed in Section 2.2.

As described in Table 1, we propose to use URIs to identify edge ports and to advertise their interface type and technology parameters, access policy rule and pricing information. This information will be used for constraint-based path computation, for determining which resources the user is authorized to access, and for determining approximate cost values of a computed path.

Table 1 GVS Edge Port Information

Attribute	**Explanation**
URI	Uniform Resource identifier
InterfaceType	Technology of interface
Access policy rule	Who has access to resource
Pricing	High level approximations of usage costs
Technology parameters	VLAN range, MTU sizes etc.
Adjacent Port URI	Uniform Resource identifier

Capabilities Abstraction of GLIF Domains and GOLEs. Abstracting capability information of a domain/GOLE down to a single virtual switch is one of the greatest

challenges of our GIRRA approach. As shown in Table 2, we propose to describe capabilities regarding technology and cross-layer adaption supported, multiplexing and de-multiplexing capabilities, restoration capabilities and delay estimation. A domain or GOLE can claim a specific capability such as technology adaptation when it has at least one physical network element capable of providing it.

Capabilities lead to different configuration options and will be applied to the various edge port cross-connect options when making an intra-domain path request. The advertisement of these capabilities will provide the necessary information for the G-NSA path computation module to use as constraints during path computation. As an example, if a path is requested via the E-GNI API between two endpoints with different technologies (e.g., Ethernet VLAN to SONET), it will then require that specific form of technology adaptation from the G-NSA. The G-NSA path computation module will use the presence or absence of that capability advertised by a GVS during the path computation process. Doing so will assure that, when the G-NSA makes the required E-GNI request for an intra-domain partial path, the NRM of the requested domain is capable of configuring the internal network elements so as to provide the partial path with technology adaptation.

Table 2 Advertised Domain/GOLE Information in GVS Server

GVS Capabilities	**Explanation**
Technology Adaptation Type x	Client layer to Server layer
Cross Layer Adaptation x	Encapsulation form
Multiplexing/Demultiplexing Capability	Configuration values
Restoration Capability	Type of Protection or Restoration
Delay Estimation	Approximate delay to traverse Domain

Termination Points abstraction . As for edge ports of domains/GOLEs, we propose to describe termination points as ports on the corresponding GVS. As shown in Table 3, we propose to use URI to identify termination points. Other attributes follow similar parameters to the edge ports described earlier, however a novel attribute we include for our termination point model is the most preferred (followed by next most preferred, etc.) edge port. This preference parameter will be used during path computation to determine multiple paths ordered according to preference, and is one of the key simplifications in the logical topology for path computation.

Table 3 Advertised Termination Points, Look up Server

Attribute	**Explanation**
URI	Unified Resource identifier
Interface technology	type of interface
Access policy rule	who has access to resource
Pricing	high level approximations of usage
1st choice edge port	likely available dynamic path to edge port
2nd choice edge port	next likely available dynamic path to edge port
3rd choice edgeport	next likely available dynamic path to edge port

5 GIRRA security infrastructure and interfaces for lightpath provision

GIRRA includes an infrastructure to ensure secure access to resources that is based on a collaboration model between providers and involves a consortium certification authority and a clearinghouse. In this section, after introducing the GIRRA trust model, we describe the interfaces shown in Figure 2 for organizations to register with consortium and clearinghouse for provisioning of free and commercial services, respectively, and the use of the E-GNI interface for authentication and authorization of users for access to the GLIF services.

GLIF Trust Model. The entities involved in the path provision mechanism are the GLIF resource providers, the research organizations, and the users of these research organizations interested in using GLIF resources, referred as GLIF end-users. Today, GLIF end-users obtain resources on the basis of identity and research profile of the organizations they belong to. We contend that GLIF providers are inclined towards collaborating and therefore are unique in their ability to have trust relationships to build a consortium with a single secure access interface with users. As shown in Figure 4, the certification authority provides the G-NSA of each domain/GOLE with a certificate attesting the affiliation of its provider with the consortium. G-NSAs share direct bilateral trust relationships, while the trust relationship between consortium and end-users is indirect with research organizations acting as an intermediary between them. Certificates issued by the certification authority will be used to support provisioning of AA credentials that are issued by one G-NSA and can be verified by any other G-NSA. These certificates allow mutual authentication between G-NSAs.

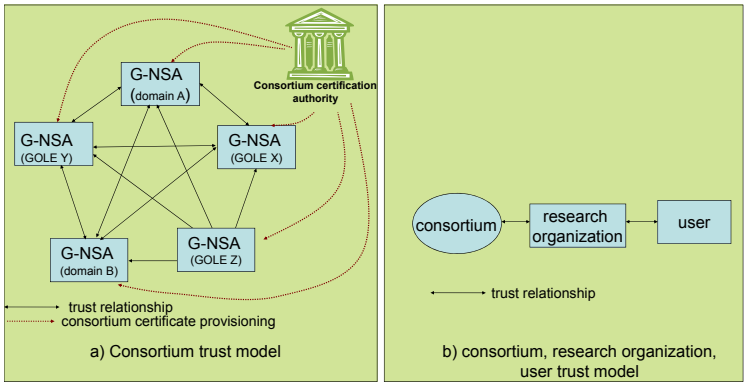

Fig. 4 GLIF Trust Model

5.1 Interface for Access to GLIF resources: Registration with the Consortium for Provision of AA Credentials

As described in Figure 2, we propose that the G-NSA registration module implements functions for registration of research organizations with the consortium. The registration model is distributed and the NSA of any domain/GOLE can handle the registration procedure acting as intermediary between the organization and all the providers of the consortium. The consortium could also decide to refer to a third provider for the registration functions and this will not invalidate the model proposed.

The functions of the G-NSA registration module are the following. It receives registration requests from the organizations, it is informed about identity and authorization profile of the requesters, it issues AA credentials for the organizations, it signs these AA credentials using its certificate, and it then provides them to the requester. Regarding the verification of the research profile and identity of the organization, we assume that the registration module can be provided with this information and we do not enter into the details of this procedure.

AA credentials. The content of the AA credentials is described in Figure 5(a). It includes authentication information, authorization information, and the ceritificate and signature of the issuer.

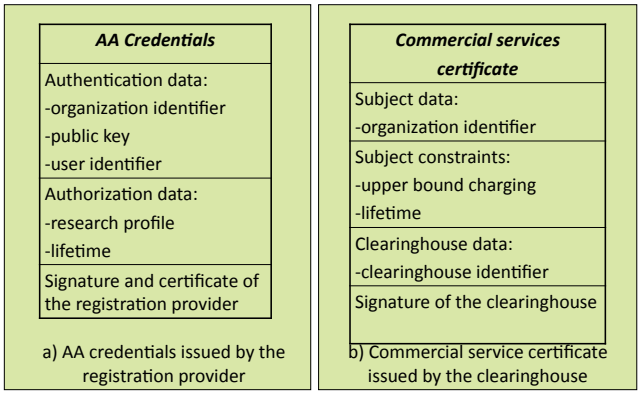

Fig. 5 AA Credentials and Commercial service certificate

The authentication information describes the identity of the research organization, its public key and the identifier of the user to which the research organization wants to allow access to the GLIF resources. The public key is included to support the mechanism for authentication of issuers of lighpath requests that will be described in Section 5.2. The user identifier is included in the AA credentials to allow the research organization to keep trace of the activities of its users. This identifier will be included in the accounting records sent to the organization. If the organization wants to allow more than one user to access the GLIF resources, it has to ask for a list of credentials, one per user.

The authorization content of the AA credentials is related to the research profile of the organization. This profile is used during path computation by the G-NSA to

validate the resources the organization is authorized to use. The authorization content of the AA credentials also includes a parameter describing their lifetime. The lifetime is negotiated between the organization and consortium and defines the time during which the credentials are valid.

5.2 Interface for access to GLIF Resources: Clearinghouse and Registration for Commercial Services

Access to commercial services requires registration of research organizations with the consortium for provision of AA credentials and registration with the clearinghouse (see Figure 2). The clearinghouse has three main functions: (a) it acts as credit certification institution of the consortium, (b) it receives payment from the organizations, and (c) it distributes this payment to all the providers on the base of accounting records metering the user service. During registration with the clearinghouse, the research organizations prove their financial state and are provided with a certificate called "commercial service certificate" asserting the registration. Users will be asked to show it any time they ask for commercial services.

Commercial Services Certificate. Figure 5(b) describes the content of the commercial service certificate. It includes information about the subject of the certificate, i.e., the research organization, information about the identity of the clearinghouse and its digital signature that guarantees data origin, integrity and non-repudiation. The information about the subject includes not only its identifier, but also constraints that can limit the use of this certificate. As an example, it may include an upper bound on charging allowed per service and its lifetime. In Section 7 we describe how this certificate is used by users to access commercial resources.

5.3 User Authentication and Extended-GNI (E-GNI) Module

The messaging proposed along the E-GNI API is shown in Figure 6(a). Authentication is performed by the G-NSA security module using the public key stored in the credentials: the user uses its private key to encrypt a nonce received from the G-NSA, and the G-NSA uses the public key carried in the credentials to verify the identity of the user through the encrypted nonce. If the verification of the user is successful, the G-NSA uses the signature on the AA credentials to verify their data origin, integrity and non-repudiation. Users can use AA credentials provided by any G-NSA to request a lightpath from any other G-NSA, since the verification of the digital signature on the AA credentials can be performed by any G-NSA.

The main advantages of the authentication method proposed for GLIF users are the following. It does not require storage of AA credentials in consortium servers and it does not require interaction between the registration G-NSA that had issued the AA credentials and the G-NSA that performs AA. The research organization is responsible for storing the AA credentials and any G-NSA of the consortium can verify their validity and use them to authenticate and authorize users locally. The locality property of this model leads to semplicity as it requires enhancements only to the E-GNI interfaces; it does not require signaling for exchange of users' AA data between providers or upgrading of the AA servers for storage of users' AA data. This model is based on the assumption that providers are inclined to share users.

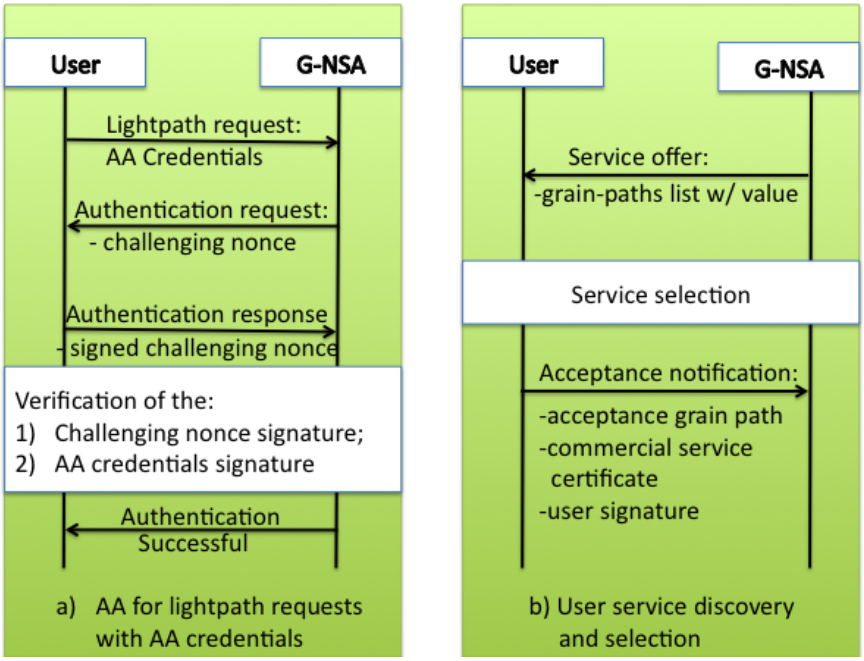

Fig. 6 User authentication and user discovery and selection service

6 GIRRA Path Computation model

We propose a path computation model that consists of four distinct steps: i) GVS logical topology generation, ii) termination point lookup and edge-port determination, iii) logical topology reduction and inter-GOLE path computation, and iv) G-NSA E-GNI requests to individual NRMs. We describe each of the steps below and provide a high level summary in Table 4.

Step I: GVS Logical Topology Generation. The G-NSA topology generation module uses the domain/GOLE description data, stored in the GVS server, to create a global logical topology representing the GLIF network. As shown in Figure 7, this topology provides a mesh-based view of the network having switches (GVSs) with capabilities interconnected with static interdomain links.

Step II: Termination Point Lookup and Edge-port Determination. The first function the G-NSA performs to serve a lightpath request is the lookup of information about its endpoints, that is, the URIs included in the E-GNI request, from the GIRRA repository server (see Section 4).

This information allows the G-NSA to discover the source (ingress) and destination (egress) domains and to identify the possible edge connections in each domain for the

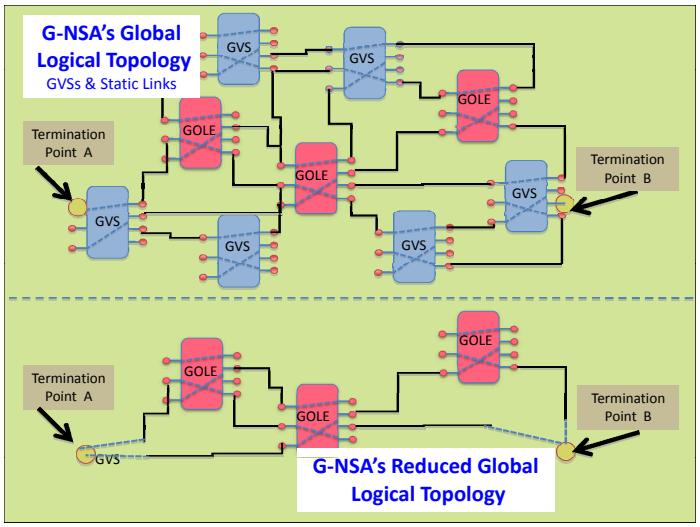

Fig. 7 Global Logical Topology and Reduced Logical Topology

specified termination points. Each termination point lookup data includes the most preferred intra-domain paths to the most likely edge-ports of its domain. This is the key information that helps start the coarse-grain global inter-domain path computation, since the specific edge ports will relay the adjacent GOLE. The G-NSA also uses the technology type of the endpoints to determine if there is a mismatch of technology types between the two termination points. If so, then the G-NSA considers the technology adaptation capability of the GVSs as a path computation constraint.

At this stage of the process, the G-NSA has determined the ingress and egress domains and the adjacent GOLEs each domain connects to (see Figure 7). Both domains now are represented by one or more partial paths from the specified termination point to the advertised edge ports.

Step III: Logical Topology Reduction (LTR) and inter-GOLE Path Computation. Once the egress and ingress domains have been determined by Step II, if both domains connect to the same GOLE, then the path is determined and is composed of the ingress domain, the GOLE and the egress domain. Otherwise, a path has to be computed to join the edge ports identified in the egress and ingress domains. This path will include only GOLEs acting as exchange points, as the GLIF network is mostly composed by NRENs interconnecting to one or more GOLEs.

The number of potential inter-GOLE paths can be high depending on the GVS topology. To reduce the number of these paths, we introduce the concept of logical topology reduction (LTR), a function that takes place in the logical topology module. This function makes use of the termination endpoint information on preferred intra-domain paths to edge ports and their adjacent domain/GOLEs to determine paths. Constraint-based policies allow to exclude paths with resources that do not meet these constraints. During this step, the path computation model also activates the function for verification of the authorization profile of the user to determine the resources they are authorized to access on the basis of the access policy rule advertised in the modeling

GVS. Resources the user is not authorized to access are eliminated from the topology, further reducing the complexity of path computation. Figure 7 shows an example of path computation with LTR. In this example, the number of GVSs has been significantly reduced by eliminating all domain GVSs that are not the ingress domain or the egress domain. This reduction in potential paths is based on the assumption that it is more efficient to create an interdomain path via GOLEs (open exchange points) rather than traversing another network domain. The example further reduces the number of potential paths by utilizing the preferred edge port information provided in the end point table. This information provides the path computation with starting edge points at the ingress domain and duplicates a similar starting edge point at the egress domain. These starting edge points limit the number of GOLEs to interconnect through.

Step IV: GNSA E-GNI Requests to Individual NRMs. Once the coarse-grain global path is computed in Step III, the G-NSA uses the E-GNI API to make intra-domain, partial-path requests to the NRMs of each of the domains and GOLEs involved in the coarse-grain path. The specification for each path request is collected from both the original end user requests and the edge ports advertised via the GVS server. A collection of these pieces of information results in a fully specified lightpath request for each domain and GOLE in the path. The G-NSA will have more than one computed path to try to reserve in case of failed attempts. It is critically important for the G-NSA to use a two-phase commit for all resource requests in the requested path. In other words, each GOLE and domain must provide a positive reply to the reservation before the G-NSA can request for the resources to be committed. If one of the domains or GOLEs provide a negative reply to the partial path request, then the G-NSA must repeat the process with one of several alternate lightpaths. Once all domains and GOLEs provide a positive reply, the G-NSA sends a commit to each of them to provision the lightpath.

Table 4 GNSA Path Finding Algorithm

	GVS Logical Topology
1	GNSA has already retrieved all advertised GVSs and static links information
2	GNSA created a global logical topology
	Termination Point Lookup and Edge-port Determination
3	GNSA receives E-GNI request for path A to B
4	GNSA does lookup for termination point A and B
5	GNSA retrieves termination point information for both A and B
6	GNSA takes point A and first choice edge port and places a static link between A and edge port
7	repeats step 6 for point B
8	GNSA substitutes domain A with a static link between point A and 1st choice edge port in Domain A
9	GNSA substitutes domain B with a static link between point B and 1st choice edge port in Domain B
	Logical Topology Reduction (LTR) and inter-GOLE path computation
10	GNSA removes remaining Domain GVS from logical topology
11	GNSA asks if edge port for Domain A connects to the same GOLE as domain B?
12	If step 11 is true than global path computation is complete Path: A-¿ GOLE-¿B
13	If step 11 is not true than use path computation to find remainder of path via GOLEs
14	steps 6 through 13 may be repeated until exhaust the combination of edge ports in lookup server
	GNSA E-GNI requests to individual NRMs
15	NSA then uses E-GNI to make path request from each domain and GOLE in global path
16	GNSA relies on a two-phase commit before the path is established and ready for the user to use

7 Service Discovery, Accounting, Metering and Billing System

To describe the accounting model proposed for GIRRA, we divide the accounting cycle in three steps, namely, service discovery and selection, metering, and accounting and billing.

Service discovery and selection. We propose a discovery and selection service that provides users with information about the technological properties and price of the different solutions suitable for their requests at the end of coarse-grain computation, and allows users to select one. The computation of the price of the paths is based on the value of resources, defined as cost per unit of time, advertised in the modeling GVS. The G-NSA, during path computation, collects the approximate costs of the resources along the computed paths to determine the overall costs (sum of the value of the resources used in each domain) which it provides to the end user. The discovery and selection procedure is described in Figure 6(b). If the path includes commercial resources, the user has to includes the commercial certificate issued by the clearinghouse in the message, to allow the G-NSA to verify if the user is authorized to access them. The user signs the acceptance notification message to guarantee its data origin, integrity and non-repudiation. The G-NSA holds the acceptance notification as proof against payment and provides it to the clearinghouse along with the accounting records related to the resources used by the user.

Metering. Metering is the procedure to measure the amount of resources used by a service for accounting. In GIRRA, the metering information required are the "starting time" and the "time length" of the lightpath connection. As these are the same in any domain, we propose to deploy the metering functions just in the access domain of the the user. We assume the access NRM controls metering and provides metering data to the G-NSA through the E-GNI interfaces.

Accounting computation and billing. The G-NSA uses the metering data and information about the value of the resources of a computed path to issue accounting records describing connection starting time and length, the value of the resources in each domain and their cost, and the total cost of the path. The G-NSA sends the accounting records regarding the user activity to the user. The accounting records are also provided to the clearinghouse if the service provided is a commercial one. In this case, the clearinghouse will handle payment for the resources by the user and will distribute the price to providers on the basis of what is described in the accounting records.

8 Discussion and Conclusions

In this paper, we described our proposed GIRRA solution for interdomain lightpath provisioning. We aligned our solution with current activities in standard bodies and forums, while introducing new design features necessary for providing a holistic solution set encompassing resource description and advertising models, path computation, interfaces for authenticated and authorized access to the services, and accounting and billing. GIRRA is based on proven concepts that exist today in remote management of complex network elements such as MSPPs. We described a model for description of GLIF resources based on a virtual switch representation, and a provision framework

with secure access to resources provided by multiple providers. A federation-based trust model allows providers to join into a consortium for the provisioning of inter-domain lightpaths, supports advertisement of GVSs information for inter-domain path computation, and provides users with transparent access to resources from multiple providers.

Our approach simplifies inter-domain path computation by introducing a two-stage path process that includes the determination of an end-to-end coarse-grain inter-domain path followed by NRM-based intra-domain path computation. Complex intra-domain path computations and reservations remain under the scope and control of existing NRMs. Our design of the E-GNI API facilitates this two-stage path computation model. The global coarse-grain path computation takes place over GIRRA's logical topology, uses the logical topology reduction mechanism, and is based on compilation of key information abstracted from network domains and GOLEs that are filtered on the basis of constraints provided by users and security access functions. We also considered the issue of accounting and billing, and we proposed a model that makes users aware of the different resources suitable for their needs, and provides guarantees of accountability and billing for the resources provided by each provider to serve a lightpath. Finally, GIRRA was built around existing efforts and aims to support the discussion on inter-domain provision of standardization bodies as OGF.

In GIRRA, we followed the philosophy that minimal information coupled with simplified access to it often leads to a higher degree of sustainability and interoperability. We focused on abstraction of relatively static information to describe resources and reduced the requirement for NRM interoperability by forcing information exchange via a push/pull mechanism with repositories. While this increases scalability, the accuracy and freshness of the information greatly decreases resulting in possibly false positive path computations. Similarly, consistency issues may arise by asynchronous topology generation and serving of lightpath requests. Another important assumption that has driven the GIRRA design is that GLIF providers are inclined to collaborate and to share users. This assumption implies that all participants agree to the proposed model and that users agree to make their profile available to all GLIF providers. Another aspect unexplored in GIRRA is about GVS and termination point advertisements that should be automatic to avoid mis-configuration errors. Therefore, the GIRRA architecture introduced in this paper raises several questions we plan to investigate on in our future work. In particular, we plan to study the scalability, complexity and performance of the model proposed and the trade-offs between them. We will continue to refine the level of abstraction of domain capabilities and topology aggregation. We will investigate the privacy issues arising from the user sharing concept. We will explore the use of the PerfSONAR framework for the GIRRA repositories and interface protocols for the push and pull information exchange, as well as for providing a framework for monitoring lightpaths.

Acknowledgements The authors would like to thank Mohit Chamania, Xiaomin Chen, Erik-Jan Bos, Cees De Laat, Freek Dijkstra, Jeroen van der Ham, Evangelos Haniotakis, Chin Gook,Jerry Sobieski, John Volbretch, and all the participants of the OGF NSI working group, Network Markup Language working group and GLIF's GNI API task force in the Technical and Control working group for the insightful debates and discussions. This work was partially supported by Deutsche Forschungsgemeinschaft (DFG) under support code JU2757/-1/1. This work was also partially supported by SURFnet.

References

1. G. Karmous-Edwards, Global e-Science collaboration, Computing in Science and Engineering, vol. 7, no. 2, March-April 2005, pp. 6774.
2. Editors: F. Travostino and J. Mambretti and G. Karmous-Edwards,*Grid Networks: Enabling Grids with Advanced Communication Technology*, Wiley, 2006
3. *DRAC* , www.nortel.com/drac/
4. Alexander Willner, Christoph Barz, Joan Antoni Garcia Espin, Jordi Ferrer Riera, Sergi Figuerola, Peter Martini *Harmony - Advance Reservations in Heterogeneous Multi-domain Environments*, Networking 2009: book chapter: 871-882, Springer Berlin / Heidelberg
5. L. Battestilli,Gigi Karmous-Edwards, et al., *EnLIGHTened Computing: An Architecture for Co-allocating Network, Compute, and other Grid Resources for High-End Applications*, Proceedings of IEEE Honet'07, Dubai, UAE, November 2007
6. Chin P. Guok, David W. Robertson, Evangelos Chaniotakis, Mary R. Thompson, William Johnston, Brian Tierney, *A User Driven Dynamic Circuit Network Implementation*, IEEE International workshop on Distributed Autonomous Network Management Systems, DANMS08
7. T. Lehman, J. Sobieski, B. Jabbari, *DRAGON: A Framework for Service Provisioning in Heterogeneous Grid Networks*, IEEE Communications Magazine, pp. 84-90, March 2006
8. S. Thorpe, Gigi Karmous-Edwards, et al., *G-lambda and EnLIGHTened: Wrapped In Middleware Co-allocating Compute and Network Resources Across Japan and the US*, Proc. IEEE Gridnets 2007, October 2007
9. Admela Jukan, Gigi Karmous-Edwards, *Optical Control Plane for the Grid Community: A Tutorial*, IEEE Communications Surveys and Tutorials, 3rd quarter, 2007
10. A. A. Saleh, J. M. Simmons, *Evolution Toward the Next-Generation Core Optical Network* Journal of Lightwave Technology, vol. 24, no. 9, pp. 3303-3321, September 2006.
11. *Common Information Model*, www.dmtf.org/standards/cim/
12. , Jeroen van der Ham, Freek Dijkstra, Paola Grosso, Ronald van der Pol, Andree Toonk, Cees de Laat, *A Distributed Topology Information System for Optical Networks Based on the Semantic Web*, Elsevier Journal of Optical Switching and Networking, Vol. 5, Issue 2-3, pp. 85-93, June 2008.
13. ITU-T Rec. G805, Generic functional architecture of transport networks, March 2000.
14. Li Xu, Freek Dijkstra, Damien Marchal, Arie Taal, Cees de Laat, *A Study on Declarative Multi-Layer Path Finding Based on Semantic Network Descriptions*, ONDM 2009 - 13th Conference on Optical Network Design and Modeling, IFIP conference proceedings, Braunschweig, Germany, Feb 2009.
15. Fernando Kuipers, Freek Dijkstra, *Path Selection in Multi-Layer Networks* , Elsevier Computer Communications, Vol. 32, 2009, pp. 78-85
16. Gigi Karmous-Edwards, Arun Viswanath, Douglas Reeves, Lina Battestilli, Priyanka Vegesna, George N. Rouskas, *Edge-Reconfigurable Optical Networks (ERONs): Rationale, Network Design, and Evaluation*, IEEE/OSA Journal of Lightwave Technology, vol. 27, no. 12, pp. 1837-1845, June 15, 2009.
17. Network mark-up language working group (NML-WG). URL: http://www.ogf.org/gf/group info/view.php?group=nml-wg
18. Alberto Escolano ,Andrew Mackarel, Damir Regvart, Victor Reijs, Guy Roberts, Hrvoje Popovski, *Deliverable DJ3.5.3:Report on Testing of Technology Stitching*, URL http://www.terena.nl/activities/tf-ngn/tf-ngn21/reijs-bluenet.pdf
19. *Global Lambda Integrated Facility Website* , http://www.glif.is/working-groups/controlplane/
20. Network Service Interface working group (NSI-WG). URL: http://www.ogf.org/gf/group info/view.php?group=nsi-wg
21. X. Ni and J. Luo, *A clustering Analysis Based Trust Model in Grid Environment Supporting Virtual Organizations*, International Conference on Advanced Networking and Applications, Okinawa, Japan, March 2008
22. Y. Demchenko, A. Wan, M. Cristea and C. Laat, *Authorisation Infrastructure for On-Demand Network Resource Provisioning*, International Conference on GRID Computing,Tsukuba, Japan, September 2008
23. S. Shirasuna, A. Slomisnki, L. Fang and D. Gannon, *Performance Comparison of Security Mechanisms for Grid Services*, International Conference on GRID Computing, Pittsburgh, USA, September 2004

24. Y. Demchenko, C. De Laat, O. Koeroo and D. Groep, *Re-thinking Grid Security Architecture* , International Conference on eScience, Indiana, USA, December 2008
25. S. Greco Polito, M. Chamania and A. Jukan *Extending the Inter-domain PCE Framework for Authentication and Authorization in GMPLS Networks*, International Conference on Communications, Dresden, Germany, June 2009
26. S. Greco Polito, H. Schulzrinne and A. Forte *Inter-provider AAA and Billing of VoIP Users with Token-based Method*, GLobal Information Infrastructure Symposium, Marocco, July 2007
27. R. Douville, J.-L. Le Roux, J.-L. Rougier and S. Secci, *A Service Plane over the PCE Architecture for Automatic Multidomain Connection-Oriented Services*,Vol. 46, No. 6, pp. 94-102, June 2008
28. L. Gommans, F. Dijkstra, C. de Laat, A. Taal, A. Wan, T. Lavian, I. Monga and F. Travostino, *Applications drive secure lightpath creation across heterogeneous domains*, IEEE Communications Magazine, Vol. 44, No. 3, pp. 100-106, March 2006 Symposium, Marocco, July 2007
29. E. Elmroth, P. Gardfjll, O. Mulmo, and T. Sandholm, *An OGSA-Based Bank Service for Grid Accounting Systems*,Lecture Notes in Computer Science (LNCS) 3732 - Springer, pp. 1051-1060, 2006
30. A. Barmouta and R. Buyya *GridBank: A Grid Accounting Services Architecture (GASA) for Distributed Systems Sharing and Integration*,International Parallel and Distributed Processing Symposium,Nice (France),April 2003
31. Y. Qiu and J. Adu *An Accounting and Charging System for Grid*,International Joint Conference on Artificial Intelligence, Hainan Island (China), April 2009
32. Yi Liang, Zheng Zhang, Jianping Fan, Dan Meng *PhoenixAccount: A grid accounting system for the distributed resource sharing*,International Conference on Grid and Cooperative Computing, Shenzhen (China), October 2008
33. JP. Vasseur, JL. Le Roux, Path Computation Element (PCE) Com- munication Protocol (PCEP), IETF Internet Draft, http://www.ietf.org/ internet- drafts/draft- ietf- pce- pcep-13.txt, Aug. 2008
34. T. Lehman, Xi Yang, C.P. Guok, N.S.V. Rao, A. Lake, J. Vollbrecht, N. Ghani, *Control Plane Architecture and Design Considerations for Multi-Service, Multi-Layer, Multi-Domain Hybrid Networks*, IEEE High- Speed Networks Workshop 2007, pp. 67-71r
35. Mohit Chamania and Admela Jukan, *A Survey of Inter-Domain Peering and Provisioning Solutions for the Next Generation Optical Networks*, IEEE Communications Surveys and Tutorials, First quarter, 2009
36. F. Dijkstra and C. de Laat, Optical Exchanges, In Proc. of GRIDNETS, 2004.
37. B.S. Arnaud, R. Hatem, W. Hong, M. Blanchet, F. Parent, Optical BGP Networks, www.canarie.ca/canet4/library/c4design/opticalbgpnetworks.pdf
38. O. Audouin, D. Barth, M. Gagnaire, C. Mouton, P. Vicat-Blanc Primet, D. Rodrigues, L. Thual, and D. Verchre, *CARRIOCAS project: Towards Converged Internet Infrastructures Supporting High Performance Distributed Applications*, IEEE/OSA Journal of Lightwave Technology, Vol. 27 Issue 12, pp.1928-1940 (2009)
39. Pascale Vicat-Blanc Primet, Sebastien Soudan, and Dominique Verchre, *Virtualizing and scheduling optical network infrastructure for emerging IT services*, Journal of Optical Communications and Networking, Vol. 1, Issue 2, pp. A121-A132
40. ITU-T Rec. G8080/Y. 130411 (2001) Architecture for the Automatic Switched Optical Networks (ASON).
41. S. Tomic and A. Jukan, MPFI: The multi-provider network federation inter- face for interconnected optical networks, IEEE Global Telecommunications Conference (GLOBECOM02), vol. 3, 17-21 Nov. 2002, pp. 23652369