Inter-domain, on-demand VPNs mediated by a Business Layer

Fernando Matos, Alexandre Matos, Paulo Simões and Edmundo Monteiro, CISUC, University of Coimbra

ABSTRACT

VPNs are an important feature at NGN. Firstly because privacy and confidentiality each time more is a main matter; secondly, because private channels are important to qualify specific relationships between customer and providers that are a result of service mediated by a Business Layer (BL) and at last because VPNs can be the basis for many other expected value-added NGN services, like videoconference, Internet banking and multimedia applications.

VPNs have been established trough an intense human intervention, what is not in concordance with NGN perspectives. The presence of a BL helps do diminish this, however, opens discussion to some scalability issues.

At this work, we discuss how an inter-domain, on-demand VPN is effectively established with the intervention of a BL and in order to identify the advantages of this strategy we analyze performance and scalability aspects related to the BGP/MPLS VPN establishment. Based on that we conclude that this provisioning model has much more advantages than classical strategies which involve hard human intervention, moreover, this new model brings a new reality to inter-domain VPNs and that could be used as a value-added service at NGN.

I. INTRODUCTION

SERVICE PROVIDERS (SPs) are constantly faced with a high exchanging of documents and intensive human intervention when an inter-domain VPN is required. This task is becoming more complex if we consider the constant improvement on QoS requirements that customers are able to request in NGN services. The classical strategy involving exchanging of documents via fax or email are not viable to these new QoS requirements.

The adoption of a service concept where data is separated from transport [1-3] guides SPs in the direction of Service Oriented Architectures (SOA) [4] and consequently to the adoption of a BL. At this sense, a BL is an intermediary that can manage the complexity before devoted to the human exchanging of documents.

With classical strategies, documents are the basis to guarantee trust through SLAs contracted by customers and a SP. The content of this SLA could only be gathered with intense human negotiation and other contracts established with other providers, which creates a trust chain. This strategy becomes hardly manageable if more complex requirements would be included on the service requisition and that is why a BL could diminish the complexity of this task.

As NGN still lack some proof implementation of its principles, recently, some initiatives like GENI [5], FIRE [6] and NWGN [7] gained focus due to their concerning with results on real platforms and not only on simulated environments. In these strategies, service provisioning is a core task that must be accomplished with idealistic perspectives like a new Internet addressing model, classical distributed algorithms conceived as new protocols and placement of functionality on header packets. At general, those strategies would lead to an innovation at the Internet model from the scratch which means they are still on an early stage.

As already mentioned on an earlier article [8], a BL is an innovative strategy to bypass the difficult to obtain a trust chain in an inter-domain VPN, however, it is important to discuss the impacts of this new strategy. At this work we discuss the scalability impressions of inter-domain VPNs established via BLs and also present measurements that leaded us to evidence that this is perfectly viable and that SPs are faced with an opportunity to deploy new value-added services for NGN. We performed the experimental tests on the inter-domain scenario, using the RFC 4364 [9] recommendations as VPN configuration mechanism.

The motivations for these conclusions are on Section 2, where we discuss the NGN perspectives and their impacts on the conception of a new Business Model. At the Section 3, we briefly present our Global Business Framework which was previously introduced on [8]. At Section 4, we extend our GBF presentation to a scenario where an inter-domain, on-demand VPN is established and discuss some performance and scalability test results. Finally, at Section 5 we conclude the article.

II. NGN PERSPECTIVES

Historically, customers have been moved from a network based on telephony to another with improved performance. This fast integration of computers and telecommunication has changed the market scenario, moving customers and providers to the Internet. Despite this important contribution, the Internet at the beginning was faced just as a technology to make customers closer to their providers, in order that these providers would sell exclusive products.

But the technology was growing really fast and innovations were presented every time. Due to this dynamicity, customers were not more worry with products but with services. From the providers' point of view, it was time to integrate to other providers in order to reach a large spectrum of customers, and improve their revenues. However, the heterogeneity of each provider not only about technology to provide a service but also the diversity of services offered, maintain as an obstacle to reach a broadband access.

At one side providers were faced with the opportunity to enlarge their realm of services, integrating data, voice, multimedia and even emerging network services like instant messengers and broadcasting. At the other side, customers were claiming for more diversity and desiring to be able to access their services from anywhere.

The primitive perspective of Internet which is the integration of disparate networks trough a very simple structure of protocols was not viable to handle that scenario. To get a service on everywhere customers would require QoS and specific performance parameters which conflicts with the intrinsic best effort nature of Internet. Besides, to merge so many distinct providers it was imperative to conceive an infrastructure capable to handle a huge new kind of traffic, merging data, voice, multimedia and many other formats. This is the core motivation for a new generation of networks.

ESTI, TMF and other standardization bodies already recognized this movement and are working on definitions for a new network generation, so called NGN (Next Generation Networks). Two distinct visions are accomplished at NGN services [1]: the transport and the service itself. That means there are open ways to providers build services jointly. While some providers are worry with transport issues, others are responsible to provide the core of the service.

With this new concept of service, NGN opens opportunity to, at least, three new business relationships: firstly, providers would not be more attached to one specific network or service provider; secondly, providers could work with a close cooperation in order to provider a more complex service and lastly, providers that decide to offer a service with NGN perspective, must previously be aware of their possible partners.

These relationships could not be accomplished with the classical business model for Internet where a provider is responsible for all chain of a service and where billing is a matter only of customer and one provider. As observed on [3], the determination of a new model that accomplishes these three relationships would be coherent, providing the same perception of service for every end-user and obtaining the maximum value from existent services.

NGN perspectives have been the target of standardization efforts since 2003. The first attempt came from International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) with the specification Y.20001 [10] where a first definition of NGN was conceived. According ITU-T, NGN is a packet-based network able to provide telecommunication services where transport is totally independent from service-related functions and QoS is a crucial matter to be attended.

The first standardization efforts opened a race to NGN. Other important contribution came from European Telecommunications Standards Institute (ETSI) at its working group Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN). This architecture had its first release on December 2005. As the main objective was to obtain an open strategy where distinct providers can collaborate to provide a service and where customers could reach this anywhere, anytime, TISPAN has defined two main elements at its architecture: 3rd Generation Partnership Project (3GPP) and IP Multimedia Subsystem (IMS). While IMS is a service centralizer where distinct technologies may be supported, 3GPP is an inter-carrier effort to flexibly telecommunication frontiers.

Recently, another discussion complements NGN perspectives – the future Internet. As NGN looks for architectural features improving service provisioning and customers' mobility, there was a lack for other questions underlying the future of the Internet.

A. The future Internet

The transition from a closed network to the main hub for communication and information required an undeniable evolution which is still being addressed. Complementary initiatives like GENI [6], FIRE [7] and NWGN [8] are worried with the design of a future Internet, aiming to realize not only architectural modifications but also an evaluation of NGN impact. For all these cases, it is expected a redesign of the Internet which leads to the identification of challenges.

According to [11], a lot of technological challenges are guiding many scientists around the world: the increasing pervasiveness of mobility and wireless technologies, the amount of connected devices eventually leading to sensor networks, the insatiable demand for bandwidth, location determination as an important enabler for new categories of context aware services, an infrastructure devoted to end-user services, security and resiliency augmented and an increasing demand for adaptation of services in distinct platforms with different types of contracts.

All these challenges could be embraced on an enlarged service and network management proposal. However, there are strategies not well received by the future Internet community, especially which would involve the proliferation

of new and complex protocols to act on the top layers. As stated by [3], this indiscriminate process leads to swollen Internet with reduced scalability capacities.

At this scenario one of the challenges concerns the reach of security. Privacy becomes a core feature expected on the new relationships on the future Internet. With this in mind, VPNs play an important role and at same time become an interesting service to support NGN perspectives.

III. Global Business Framework

The proposed framework was conceived as a mechanism to automate and facilitates the dynamic service provisioning in a multi-domain environment. It is intended to handle the entire life cycle of the service, since its creation and publishing until its execution and termination.

This framework is composed by three layers: Business Layer (BL), Policy Layer (PL) and Network Infrastructure Layer (NIL) (Figure 1).

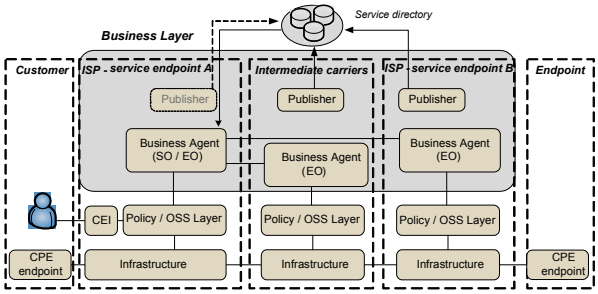


Figure 1. Global framework overview

BL is used as a collaborative environment where providers offer and negotiate services. In the architecture a service is offered by a service provider (Service Owner: SO) and is constituted by one or more service elements. These service elements are offered by providers (Element Owner: EO) and they have similar behavior than services, except they are negotiated only between providers (SO/EO) and never between customer and SO. In order to offer a service or a service element at BL, each provider needs to publish their offer in a service directory (in our case, UDDI) using the Publisher component. Both service and element service offers are described using Service Specification Templates (SST) and Element Specification Templates (EST) respectively. These templates contain detailed information about services or service elements (pricing, SLAs, etc.) and are used as reference document for service/service element publishing at UDDI and service element exchange information between SO and EO.

At the customer side, an interface named Customer Entry Interface (CEI) is used as front end to perform requisitions to the architecture. This interface can lighten the requisition task, since it hides service technical details, allowing the customer to inform only a set of specific parameters.

When a customer requests a service from a SO, the Business Agent component, which can play the role of both SO and EO, is responsible to locate elements at the UDDI and assembly them in order to build a service which satisfy the requirements asked by the customer. SO then contacts each selected EO to obtain more detailed information about the elements such as availability and price. At the EO side, it checks with the PL to verify if it can provide the element asked by the SO and if it is in accordance with the local provider policies. In this case, the EO notifies SO responding that it can provide the requested element.

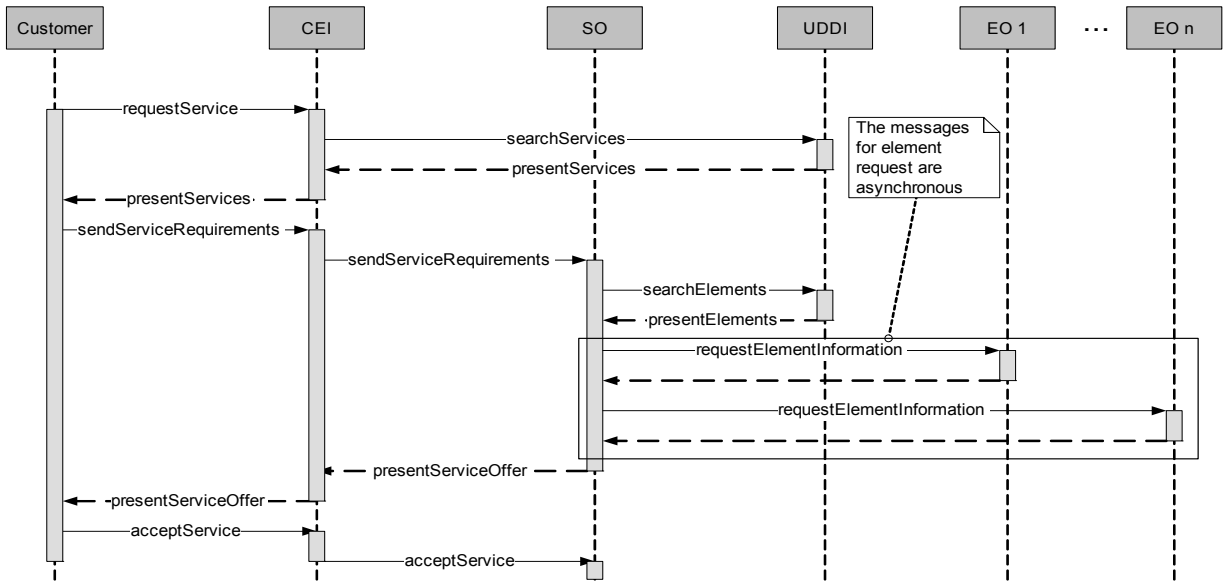
With this information, the SO is able to compose a service offer SLA to present to the customer, who can approve or reject it based on its requirements. Once the customer approves the SLA, the service setup is ready to take place. At this time, the SO must reach an agreement with the EOs. This is accomplished by the establishment of SLAs between the SO and each chosen EO.

After all involved parties reached an agreement, SO then sends the information needed by each EO to properly configure their equipment according to the customer requirements. At this point, EO forwards this information to PL which verifies what resources are available to provide the contracted service element. After that, PL contacts the NIL to inform which resource must be configured and sends the required information to do that, such as service parameters and local provider policies.

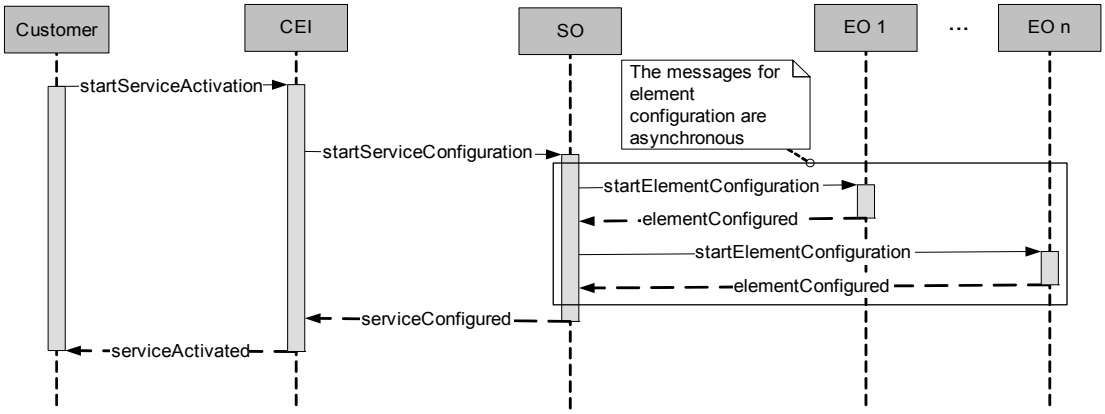
In its turn, the NIL builds a configuration script, by translating the information received from PL in equipment configuration commands. The NIL then performs a local connection (Telnet, SSH) with the equipment to execute the script. Once this configuration is performed at every EO, the service setup is finished and it is ready to be activated.

It is worth to mention that BL has a crucial role in the framework since all message exchanges between the entities involved during service provisioning occur in this layer. Figure 2 shows sequence diagrams of three of the most important use cases that happen in BL:

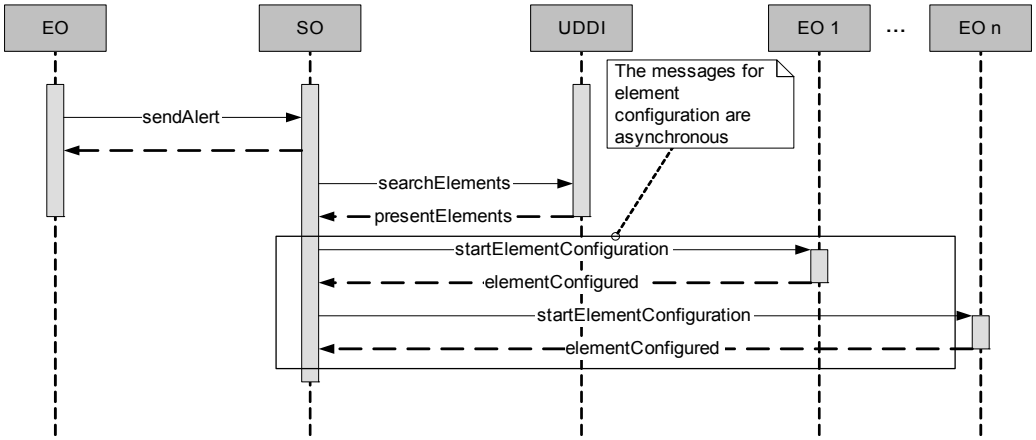
- Service requisition: During this use case, the customer initiates the service requisition. It is here that SO assembles the service offer based on the information obtained from each EO. SO also presents the service offer to the customer;
- Service activation: In this use case, the customer requests for the service activation. SO contacts each EO in order to send the service requirements;
- Service reconfiguration: In this use case, an EO sends an alert message to SO informing that some problem occurred at configuration/provisioning VPN time. SO then must search for alternatives to reestablish the VPN configuration/provisioning.



a) Service requisition



b) Service activation



c) Service reconfiguration

Figure 2. Sequence diagrams

IV. INTER-DOMAIN VPN SCENARIO

As stated before, due to the NGN and Future Internet premises, providers are forced to change their way to offer services. Some of those premises such as on-demand service provisioning and a multi-domain environment make providers to concern more about privacy and automatic service configuration. In order to show that our framework can address the mentioned subjects, we present here an inter-domain VPN scenario implemented over GBF.

The inter-domain VPN scenario (Figure 3) is composed by three autonomous systems (AS), where each one represents a provider's domain. In each AS, there are an ASBR (Autonomous System Border Router) and a PE (Provider Edge) router that is connected to a CE (Customer Edge) router. In this scenario, a BGP/MPLS VPN is established among three PE routers

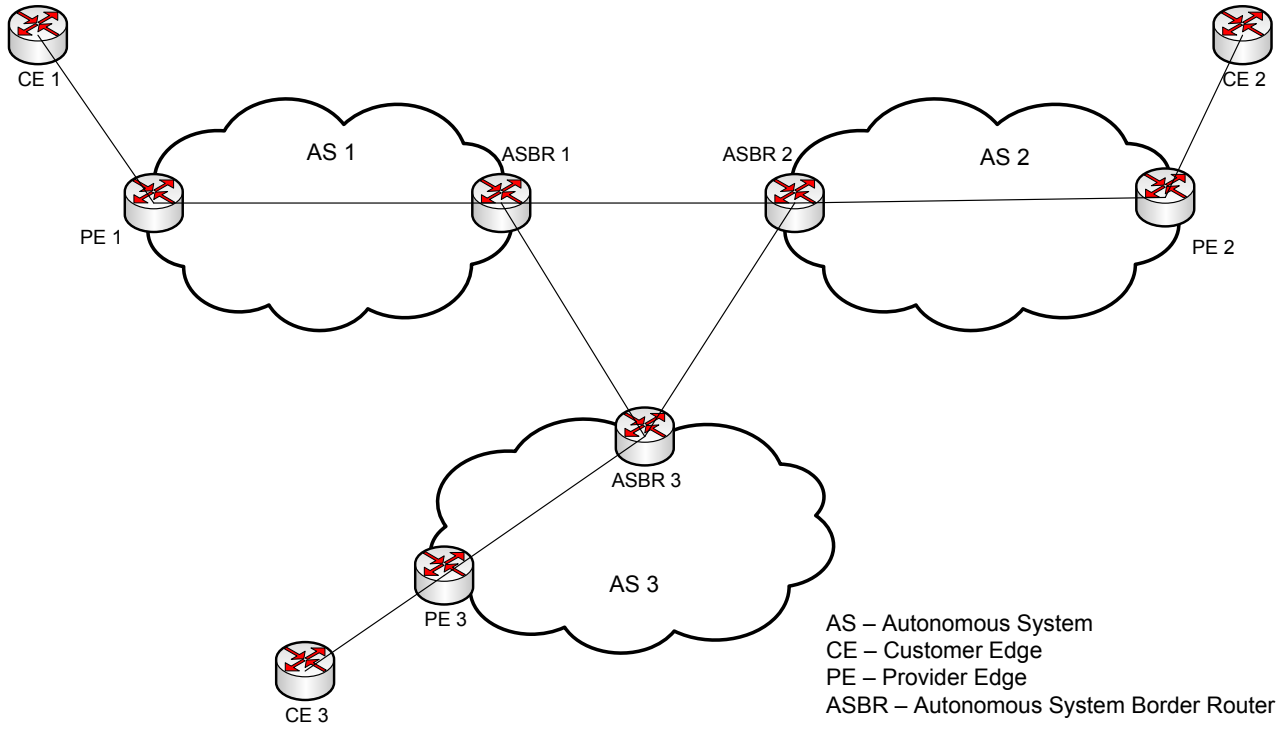


Figure 3. Topology of the inter-domain VP scenario

When a customer requests a VPN service to GBF, some of the parameters he must inform are the endpoint addresses. Based on this information, the SO is able to search for providers which can provide and end-to-end connection among the endpoints. Obviously, in this case an important factor to consider when searching for providers is whether they are able to reach each endpoint. After SO finds the potential providers, probably, there will be more than one possible path among the endpoints to choose. To resolve this, SO uses local configuration parameters and requirements informed by the customer, such as QoS parameters and price. In our scenario we considered only two parameters:

- Number of hops: Maximum number of hops that can exist between a pair of endpoints. This parameter is defined by the SO.
- Price: The maximum price the customer wants to pay for the service. This parameter is defined by the customer.

Suppose we want to establish a connection between the endpoints *A* and *B* using the providers *x*, *y*, *z*, and *w*. Figure 4 shows a graph representing how these providers are physically interconnected. Between each connection of the graph, there is a weight. In this case they represent the cost (price) to establish the connection.

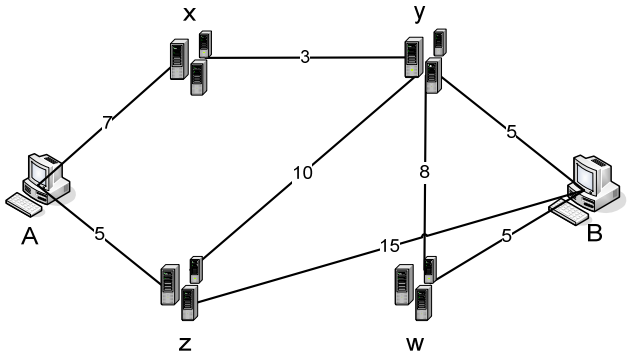


Figure 4. Connection graph

SO creates a list with all possible paths between *A* and *B*. However, the creation of this list follows some rules. For this example we applied a constraint in the number of hops (maximum of two hops). Thus, the created list has the paths (*A*, *x*, *y*, *B*), (*A*, *z*, *y*, *B*), and (*A*, *z*, *B*). Neither the path (*A*, *x*, *y*, *w*, *B*) nor the path (*A*, *z*, *y*, *w*, *B*) appear in the list because they have more than two hops. Again, SO can apply others parameters to select the best path. In this case, SO uses the price parameter, which is calculated by the sum of intermediary prices along the paths, choosing the path with the lower price (A, x, y, B).

To validate the inter-domain VPN scenario, we implemented a prototype and performed some evaluation tests, such as performance and scalability tests.

A. Implementation Aspects

The service directory used was the UDDI API jUDDI. The entire BL was implemented in Java and Web Services were used as the technology for service invocation and communication between providers. To enable the customer to request the VPN service, a web-based application (B2C Portal) was designed. This application hides service technical details and only asks for high level requirement information.

A simple PL was implemented to receive service requisitions from BL and to check if the service requirements are in accordance with the local provider policies in order to provide the service element. Concerning the NIL, we used the Dynamips Cisco router emulator and the Dynagen front-end to emulate routers to be configured at VPN provisioning. When the NIL receives the information from PL, it builds a configuration script. PL then opens a Telnet/SSH connection with each router in the emulator, in order to execute the script, thus configuring the VPN. This VPN configuration follows the RFC-4364 (BGP/MPLS VPNs) recommendations.

B. Evaluation Tests

In order to evaluate the inter-domain VPN provisioning, we performed two types of tests. First of all we executed performance tests at two use case scenarios: a) a single VPN configuration, where a customer requests for a VPN establishment; and b) a reconfiguration of a VPN, due to some difficulty at EO side. Table 1 summarizes the times observed at the tests, showing the main operations performed in each use case and their respective times. Table 1 is organized in a way that an operation may have sub-operations below it. It is worth to note that the sum of times of the sub-operations will not be necessarily equal to the time of the upper operation. This happens because an operation has other sub-operations not worth to mention, such as database access or logging.

As showed in Table 1a, the time to establish a VPN (service activation) is about 3 minutes. However, it is important to point that during the tests we observed that approximately 98% of this time is due to BGP stabilization and VRF configuration. The GBF related task times are only about 2% of the total time. If we count with the time of service requisition, the GBF task times increase to about 4%. Similar behavior happens with the times presented in Table 1b, where the GBF related tasks represent about 1.6% of the total establishment time. In both cases we believe that they are acceptable times to handle a customer activation requisition. Moreover, as mentioned before, a router emulator (Dynamips) was used during tests, which can substantially reduce the performance. As stated by the emulator author, it achieves a performance of 1 kpps, whereas the oldest NPE router model might achieve 100 kpps.

The second type of test we performed was scalability test, where the GBF must handle 10 simultaneous requisitions to VPN establishment. In Table 2 we can see that while the number of requisitions was increased by ten times, the time GBF took to handle all the requisitions, and consequently, to establish the ten VPNs increased only about 46%. This comparison shows that GBF is capable to handle a considerable increase of requisitions without significant performance degradation.

Operation	Time (sec)
Service requisition	3.9478
Search at UDDI	3.0057
EOs selection	0.3605
Service activation	142.3289
SO-EOs communication	1.4156
Routers configuration	0.865267

a) Configuration time for 1 VPN

Operation	Time (sec)
Service reconfiguration	128.0315
Search at UDDI	3.0118
EOs selection	0.1692
Service activation	124.3486
SO-EOs communication	0.9971
Routers configuration	0.710133

b) Reconfiguration time for 1 VPN

Table 1. Performance test times

Nº of VPN requisitions	Time (sec)
1	146.2767
10	207.9083

Table 2. Scalability test times

V. Conclusion

Inter-domain VPN establishment is a time-consuming task, since it requires a substantial human intervention and a considerable exchange of documents between SPs. With the advent of NGN service paradigms, this task might be even more burdensome due to QoS requirements the customers ask for.

In this article we presented a framework capable of provide on-demand inter-domain VPNs. This framework uses a Business Layer to automate every step concerning the service provisioning, since its publication and discovering in a service directory until its establishment. Those VPNs are valuable mechanisms to provide NGN services over the Internet, since they guarantee traffic isolation based on some QoS requirements, which contributes to privacy supporting.

During the inter-domain VPN test scenario, we faced some time performance limitations because we used a router emulator, and not real equipment, to configure the VPNs. Even so, it was possible to verify that the framework Business Layer can handle a VPN requisition in a considerable short time. Moreover, during the scalability tests, we verified that GBF can handle an increasing number of VPN requisitions without performance degradation.

Considerable work still must be done in order to make GBF a robust platform for service provisioning. Our main concerns are about security and QoS, since these are some of the cornerstones for the service provisioning over the future Internet. However, we believe that our framework can be a valuable mechanism for SPs to achieve their goals concerning inter-domain scenarios.

REFERENCES

[1] N. Morita, “Introduction to NGN Functional Architecture”. Proc. of the 10th IEEE/IFIP Network Operations and Management Symposium (NOMS’2006), Vancouver, April 2006.

[2] I. Grida et al., “Service Definition for Next Generation Networks”. Proc. of the Int. Conf. on Systems and Int. Conf. on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), April 2006.

[3] C. Lee; D. Knight, "Realization of the next-generation network," in IEEE Communications Magazine, vol.43, no.10, pp. 34-41, Oct. 2005.

[4] C. Mathew; K. Laskey; F. McCabe; P. Brown and R. Metz. “OASIS Reference Model for Service Oriented Architecture 1.0.” 2007. Available from: http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.html.

[5] G. Goth, “Will GENI be a magic lamp or a dim bulb?”in IEEE Internet Computing, vol. 9, issue 6, 2005 pp. 7 - 9.

[6] A. Gavras, A. Karila, S. Fdida, M. May and M. Potts, “Future Internet research and experimentation: the FIRE initiative”. Proceedings of SIGCOMM Computer Communications Rev. 37, 3, Jul. 2007, pp. 89-92.

[7] T. Aoyama, "A new generation network — beyond NGN —," First ITU-T Kaleidoscope Academic Conference on Innovations in NGN: Future Network and Services, 2008. K-INGN 2008. , vol., no., pp.3-10, 12-13 May 200.

[8] A. V. Matos, F. M. Matos, P. A. Simões, E. Monteiro, “Framework for the Establishment of Inter-Domain, On-Demand VPNs ”. Proceedings of IEEE/IFIP Network Operations and Management Symposium (NOMS 2008). April, 2008.

[9] E. Rosen, E. and Rekhter, Y.,, BGP/MPLS IP Virtual Private Networks (VPNs) - RFC 4364. 2006.

[10] ITU-T Rec. Y.2001, “General Overview of NGN,” Dec. 2004.

[11] R. Jian, "Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation," Proceedings of Military Communications Conference -MILCOM 2006 , Oct. 2006, pp.1-9.