Annals of Emerging Technologies in Computing (AETiC)
Vol. 1, No. 1, 2017

Article

Comparing the Complexity of Two Network Architectures

Olivier Z. Zheng[1], Maaruf Ali[2,*] and Kashinath Basu[3]

[1]INTERPOL, Singapore
olivier.zheng@supinfo.com
[2]Department of Science and Technology, University of Suffolk, Ipswich, Suffolk, UK
m.ali2@uos.ac.uk
[3]Dept of Computing & Communication Technologies, Oxford Brookes University, Oxfordshire, UK
kbasu@brookes.ac.uk
*Correspondence: m.ali2@uos.ac.uk; Tel.: +44-1473 338678

Received: 21st August, 2017; Accepted: 15th September; Published: 1st October, 2017

Abstract: A Service Provider has different methods to provide a VPN service to its customers. But which method is the least complex to implement? In this paper, two architectures are described and analysed. Based on the analyses, two methods of complexity calculation are designed to evaluate the complexity of the architecture: the first method evaluates the resources consumed, the second evaluates the number of cases possible.

Keywords: Computer Networks; Internet Topology; Network Complexity; Multi-protocol Label Switching (MPLS); Virtual Private Networks (VPN).

1. Introduction

"Network complexity" - nobody can clearly give a concise definition of this notion, but everybody can "feel" the meaning behind this notion.

The RFC 3439 [1] policy document makes a relation between network design (network architecture) and network complexity.

Modern networks are bigger and ever more interconnected than before. With this growth, it is obvious that the global complexity of the network has increased too: there are more data types and hence more data to be considered when the network has to be managed, a local change can have a global effect as Jon Crowcroft explained with the problem with YouTube and a BGP update [2]; or more recently with the testing of new BGP attributes which made a disruption to the global Internet traffic [3]. Some parameters, which have increased with the growth, cannot be stopped, for instance, it is a fact that there are more and more networks, but stopping the increase of networks will stop the growth of the network. However, the complexity of the network may be controlled.

The main problem with the complexity in modern networks is that the behaviour cannot be totally predictable (the case can be compared to non-linear systems). It becomes interesting to design large complex networks where the behaviour can be predictable (the case can be compared to linear systems).

In a period where companies are trying to save resources (money, improvement of their "green-impact" on the planet) whilst increasing the efficiency of their equipment using solutions as virtualization technologies, or energy-efficient technologies - controlling the complexity of the network may be a solution. This may be achieved by optimisation of the network design, by matching the network equipment to the actual needs in order to obtain the best efficiency/complexity ratio.

One approach to reduce the network complexity is by analysing configuration files [4]: a network device has an initial level complexity, with the configuration made by a human operator visible on the configuration file of this device, there is a complexity variation. The analysis was focused on some objective values: some are device-based (line count, routing line count, policing line count, etc.), and some others are network-based (interdependencies between devices, number of networks). Unfortunately, the work on this analysis does not finish in a way to have a numeric metric for the configuration files. This approach is incomplete. It is not possible to get the different features used by protocols running on the network, and it does not take the network design as part of the network complexity.

Another one has been to compare the cost of two ways to give mobility to users on an IP network: Recursive InterNet Architecture (RINA), Locator/Identifier Separation Protocol (LISP) and Mobile IP architectures [5]. Different cost models have been implemented and they have been used under RINA, LISP and Mobile IP architectures. Those cost models have been validated using simulations, and the RINA architecture was found to have the lowest cost whilst LISP had the highest cost.

The aim is to try to define the least complex architecture for a Service Provider (SP) to provide VPN (Virtual Private Network) services to its customers. There are many ways to provide the VPN services; the focus will be on two architectures based on MPLS (Multi-Protocol Label Switching) technology:

- MPLS using LSPs (Link Switched Paths);
- MPLS over L2TPv3 (Layer 2 Tunnelling Protocol version 3).

1.1 Organisation of the Paper

A methodology to compare the complexity of two network architectures is presented from the service provider's point of view in the first part of the paper. This is carried out by two methods of calculation and by comparison of the results.

The rest of the paper is organised as follows: Section Two describes the network architectures which are compared. Then the analysis of the architectures on different levels is done in Section Three. Section Four introduces two methods of calculation of the complexity of the network architectures. Section Five concludes this paper.

2. Background

MPLS using LSPs and MPLS over L2TPv3 are based on the same foundations: the Provider Edge (PE) routers run virtual instance for each customer (called VRF, for Virtual Routing Forwarding). The BGP (Border Gateway Protocol) protocol is used as the routing protocol between the VRFs and to transmit information about VPN links (for instance, the VPN label). Finally an IGP (Interior Gateway Protocol) is executed on the PE and Provider (P) routers [6], [7], [8], [9].

2.1. MPLS using LSPs

In this architecture, the SP network is an MPLS-based core network. Because of the nature of the core network, all the data are transmitted from a PE router to another PE router using the value of a label.

A label has a local scope (a router and its peers). So to create an LSP between two customers and to traverse the core network, the PE and P routers need to transmit their labels bindings to theirs peers. This task is accomplished by the LDP (Label Distribution Protocol) protocol. LDP allows for two directed routers to exchange their labels. LDP will also create LSP trees starting from each Egress PE router (from the closest router to the destination).

The process of LDP exchange is as follows: the LDP will discover the LSRs (Label Switched Routers) where the LDP are running using the LDP Hello messages sent on the 224.0.0.2 multicast IP address. This is the multicast address to contact all routers in the subnet.

Then, after that once each router has done the discovery process, two LSRs which have discovered each other first, will open an LDP session. The number of LDP sessions created between two LSRs will depend on the type of link: one session for all the frame-mode links (labels are in a per-platform label space), while there is an LDP session for each LC-ATM mode link (labels are in a per-interface label space).

After the creation of the LDP session, the LSRs will exchange their label bindings in unsolicited downstream advertisement mode. This means that the LSR will distribute the label binding to its LDP peers without knowing if they need it or not (it is like a label binding flood). All the label bindings are stocked in the LIB (Label Information Base) in the control plane of the LSR. The remote binding to the next-hop LSR is stocked in the LFIB (Label Forwarding Information Base) in the data plane of the LSR.

The Service Provider network will forward packets on the label value, this means that the LDP and the running IGP must be synchronised. If a labelled packet arrives at a link where the LDP is down, but the IGP is running, then the IGP can forward the packet because the IGP runs only on the Service Provider network and does not know the customer network (which is stored in the routing table in the VRF in the PE routers).

The transmission of the packet will be done through different stacked labels as shown in Fig. 1:

The VPN label, a label used only by the Ingress PE router to identify the correct VRF and by the Egress PE router to forward to the correct VRF.

The IGP label, a label used for the forwarding of the packet in the Service Provider network, because any unlabelled packet in this network will be dropped.

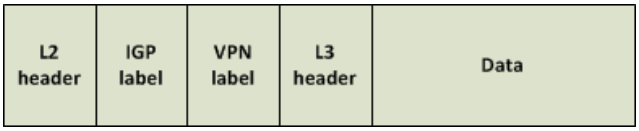

Figure 1. The packet sent to the SP in MPLS using LSPs. [11]

The LDP protocol is used to transmit the IGP label bindings by each router in the network.

2.2. MPLS over L2TPv3

In this architecture, the SP network is an IP-based core network. The problem with an MPLS-based core network was that of the case of only one part working with IP traffic [10].

The L2TPv3 protocol is an encapsulation protocol. In the MPLS VPN case, the L2TPv3 protocol is used to carry MPLS packets on IP networks.

L2TPv3 will create a tunnel point-to-multipoint for each PE router: in every L2TPv3 session, a PE router will act as a hub and the other PE routers will act as a spoke.

In the Service Provider network, an IP packet from a PE router to another PE router will contain as shown in Fig. 2:

The IP header;
The L2TPv3 header, which contains a Session ID field and a Cookie ID field;
The MPLS label, in this case corresponds to the VPN label;
The MPLS payload, which is the data for the destination host.

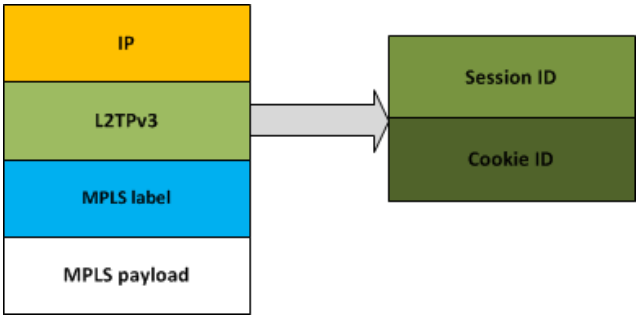

Figure 2. The packet sent in to the SP in MPLS over L2TPv3. [11]

The L2TPv3 Session ID contains a 32 bit identifier. The Session ID field is a mandatory field in the L2TPv3 header. It allows a PE router to recognize which context corresponds to the packet. The L2TPv3 cookie ID is an identifier. The Cookie ID field is an optional field, the size of the field is variable but the maximum is 64 bits.

The Cookie ID is randomly generated, and two PE routers cannot have the same Cookie ID in the same session (same Session ID). The Cookie ID is in the L2TPv3 header to give a protection against spoofing: because of the nature of the Cookie ID (random value), it is difficult for an attacker to spoof this value.

Each PE router will use some signalling to advertise the tunnel capabilities to the others PE routers.

These capabilities are sent through BGP-4. The tunnel SAFI (Subsequent Address Family Identifier) is a new BGP SAFI. It will advertise the tunnel endpoint, the endpoint IPv4 address and the next-hop IP address.

The Egress PE router can support different encapsulations; it will advertise the encapsulation that it can support in the BGP tunnel encapsulation attribute. It is in the BGP tunnel encapsulation attribute, also called the BGP SAFI-Specific Attribute (SSA), that the Session ID and the Cookie ID are transmitted. The transmission of the packet is done using:

The VPN label: as in MPLS with LSPs, the label is used by the Ingress PE router to identify the correct VRF and by the Egress PE router to forward to the correct VRF.

The IP header: the P and PE routers will use the IP destination address in the header to forward the packet to the correct Egress PE router.

The L2TPv3 header: the Egress PE router to validate the authenticity of the packet, based on the value of the Cookie ID and the Session ID.

3. Analysis of the Architectures

In this section, a qualitative comparison is done on the network architecture at both the architectural level and the configurational level.

3.1. Architectural Point of View

The two finite state machines of the PE router, corresponding to the different states taken by the PE router in the two network architectures, are close as shown in Figures 3 and 4.

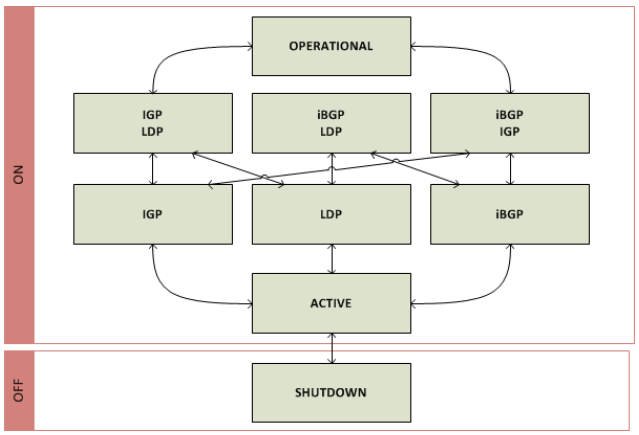

Figure 3. The finite-state machine of a PE router in MPLS using LSPs. [11]

In MPLS using LSPs (Fig. 3), the "LDP", the "iBGP LDP" and the "IGP LDP" states, which correspond to the states where the LDP protocol is running, are unique in the architecture (there are no "LDP", "iBGP LDP" or "IGP LDP" states in the MPLS over L2TPv3 finite state machine).

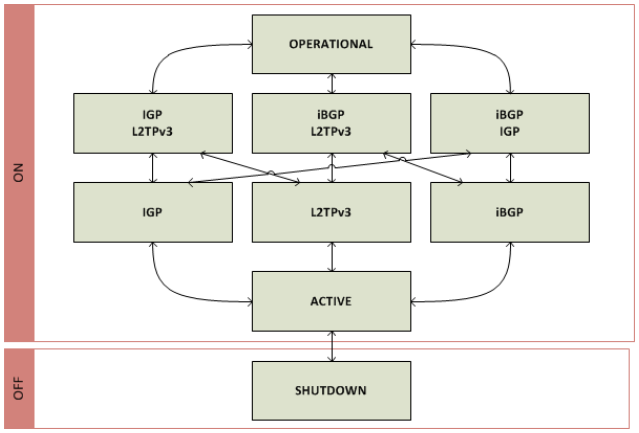

Figure 4. The finite-state machine of a PE router in MPLS over L2TPv3. [11]

In MPLS over L2TPv3 (Fig. 4), the "L2TPv3", the "iBGP L2TPv3" and the "IGP L2TPv3" states, which correspond to the states where the L2TPv3 protocol is running, are unique in the architecture (there are no "L2TPv3", "iBGP L2TPv3" or "IGP L2TPv3" states in the MPLS using LSPs finite state machine).

The state "iBGP", which corresponds to the state where the BGP protocol is running, is in both architectures: in MPLS using LSPs and in MPLS over L2TPv3. But the BGP protocol does not realize the same function in each architecture: in MPLS using LSPs, the BGP protocol is used to exchange the routing information related to the VPNs (vpnv4 prefixes and RTs) between the different PE routers; in MPLS over L2TPv3, the BGP protocol is used to exchange the routing information related to the VPNs too (vpnv4 prefixes and RTs), but also information about the L2TPv3 tunnel.

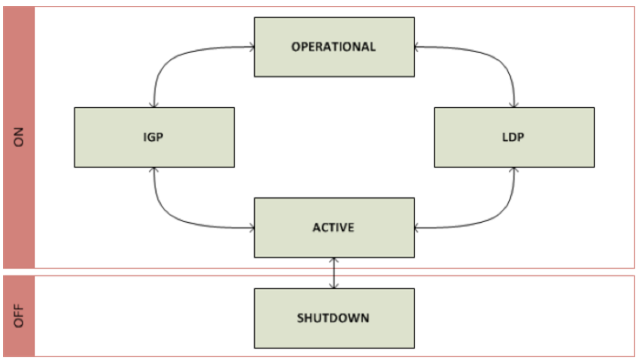

Figure 5. The finite-state machine of a P router in MPLS using LSPs. [11]

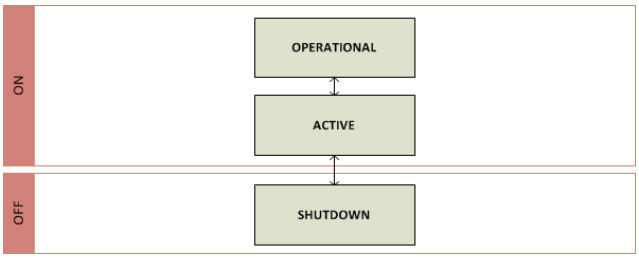

Figure 6. The finite-state machine of a P router in MPLS over L2TPv3. [11]

For the P routers, the difference is more obvious than for the PE routers (Figs. 5 and 6). It is explained because the MPLS over L2TPv3 uses directly the BGP protocol to distribute the VPN labels instead of using the LDP protocol as it is done in MPLS using LSPs. The drawback of MPLS using LSPs is that P routers participate in the LSPs; it is for this reason why there are more states in MPLS using LSPs.

In *the PE router – PE router links*: the MPLS over L2TPv3 architecture has more protocols (BGP and L2TPv3) running at this level than the MPLS using LSPs architecture (which only has BGP operating).

In *the PE router – P router links*: the MPLS using LSPs architecture has more protocols (IGP and LDP) running at this level than the MPLS over L2TPv3 architecture (which only has IGP operating).

In *the P router – P router links*: the MPLS using LSPs architecture has more protocols (IGP and LDP) running at the level than the other architecture (which only has IGP operating).

3.2 Configuration point of view

The required configuration steps (the strict minimum configuration steps required to configure the label distribution, which is the main difference between the two architectures) to configure the desired architecture on the PE and on the P router have been compared. To do it in an objective way, the comparison of the configuration steps have been done based on the configuration guide of two different manufacturers operating systems: Cisco IOS XR from Cisco Systems and JunOS from Juniper Networks [12], [13], [14].

Table 1. Configuration steps of a PE router in the architectures. [11]

MPLS using LSPs	**MPLS over L2TPv3**
Enable MPLS	Enable MPLS
Customer Facing Interface VRF	Global VRF
Enable the LDP protocol	Route-policy
Configure the LDP discovery	Customer Facing Interface VRF
Configure the LDP active/passive targeted	Configure BGP (RiV)
	Enable the L2TPv3 multipoint tunnel

There are a lots of configuration steps on a PE router working in the MPLS using LSPS and in MPLS over L2TPv3 as summarised in Table 1. However, the configuration of the PE router in MPLS over L2TPv3 seems to be more complex than the configuration of the PE router in MPLS using LSPs - because most configuration steps in MPLS over L2TPv3 have a bigger scope than the configuration steps in MPLS using LSPs. For instance, the configuration of the VRFs and the BGP protocol have a global scope (the effects of the configuration are on the router and on the network) whereas in the configuration of the LDP protocol, the L2TPv3 multipoint tunnel have a local scope (the effects of the configuration are directly on the interfaces).

The configuration of P routers in MPLS using LSPs is definitively more complex than the configuration over L2TPv3: there is nothing to configure on P routers in MPLS over L2TPv3 as shown in Table 2.

Table 2. Configuration steps of a P router in the architectures. [11]

MPLS using LSPs	MPLS over L2TPv3
Enable MPLS Enable the LDP protocol Configure the LDP discovery Configure the LDP active/passive targeted	No configuration required

4. Mathematical Formulæ

In this section, a quantitative comparison is done on the architectures based on the qualitative analysis done in the previous section, two methods have been designed to evaluate the complexity of the architecture. For more details about the calculation, refer to reference [11].

4.1. Method #1

This method has been designed on the idea that to quantify the complexity and to compare the complexity of two architectures is equivalent to quantifying and comparing the complexity of the differences between the two architectures. The differences in the protocols between the two architectures are:

the BGP protocol;
the LDP protocol;
the L2TPv3 protocol.

To summarise the principle of this method:

$$C = C_{BGP} + C_{LDP} + C_{L2TPv3} \quad (1)$$

With C representing the global complexity, C_{BGP} the complexity of the BGP protocol, C_{LDP} the complexity of the LDP protocol and C_{L2TPv3} the complexity of the L2TPv3 protocol.

In this method, the complexity will be measured in the space dimension, which is the memory space occupied by the running protocols. The architecture will represent the complexity of the protocols being actually executed in the architecture under investigation.

While the memory space does not change a lot from one platform to another, the complexity in the time domain may be dependent on multiple parameters. This is the primary reason why the complexity will not be measured in the time dimension.

The analysis will be an asymptotic survey of the complexity based on the increase in the number of PE routers in the network. The analyses will analyse the growth of the complexity in the network from a network with no PE router to a network with infinity of PE routers.

A model, which represents the memory consumption, has been simulated for each protocol running on the architectures.

For the BGP protocol, the study shows that the memory consumption and hence the complexity, will depend on the number of customers per PE router, c ~~c~~, and the number of prefixes per customer, a ~~a~~. When the product $a \times c$ ~~$a \times c$~~ is below 100, the complexity of BGP is higher in MPLS over L2TPv3. When it is above 100, the complexity of BGP is almost the same on these two

architectures. The fact that the performance of BGP is more complex in MPLS over L2TPv3 is explained by the situation that the BGP will transmit more information in this particular architecture.

With the case of the LDP protocol, the simulation shows that the complexity of LDP in MPLS using LSPs is higher than in MPLS over L2TPv3. This result is not a surprise and is expected and quite normal because the LDP protocol is not running in the MPLS over the L2TPv3 network architecture. The simulation also shows that the complexity will depend on the number of P routers in the network.

For the L2TPv3 protocol, the simulation result shows that the complexity of L2TPv3 in MPLS over L2TPv3 is higher than in MPLS using LSPs. Again the result is expected because the L2TPv3 protocol is not running in the MPLS using LSPs architecture.

Referring to equation (1), the complexity of the MPLS using LSPs architecture is given by:

$$C = C_{BGP} + C_{LDP} \quad (2)$$

and the complexity of the MPLS over L2TPv3 architecture is:

$$C = C_{BGP} + C_{L2TPv3} \quad (3)$$

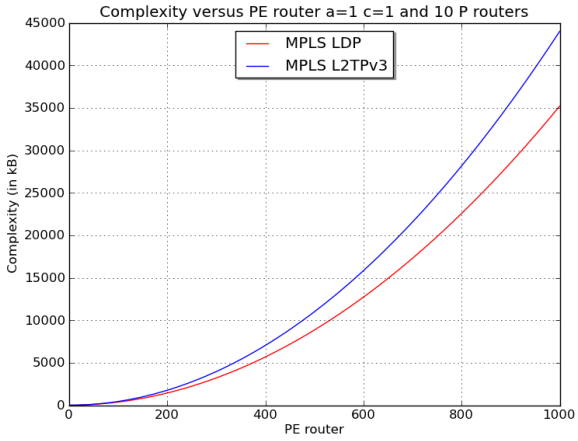

Figure 7. Complexity versus PE router with $a = 1$, $c = 1$ and 10 P routers.

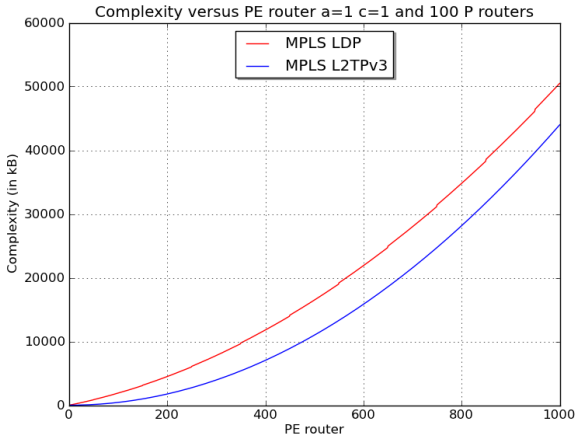

Figure 8. Complexity versus PE router with $a = 1$, $c = 1$ and 100 P routers.

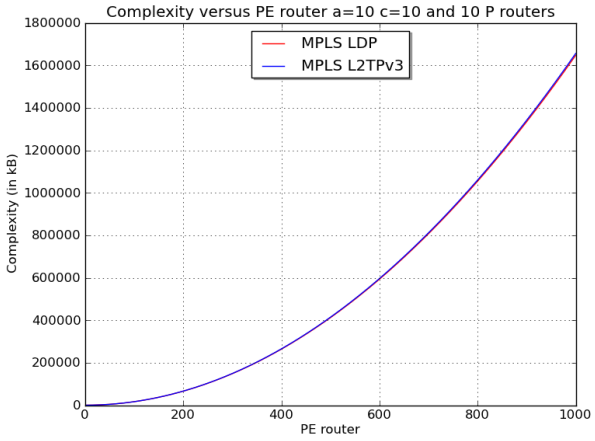

Figure 9. Complexity versus PE router with a = 10, c = 10 and 10 P routers.

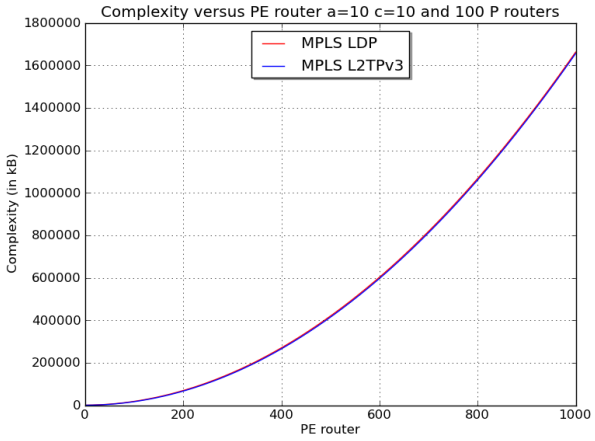

Figure 10. Complexity versus PE router with a = 10, c = 10 and 100 P routers.

When $a \times c = 100$ (in Figures 9 and 10), the complexity of the network does not have a difference between the two architectures. In a network with ten P routers or with 100 P routers, it is not possible to distinguish clearly which architecture is the best in terms of performance.

Whereas when $a \times c = 1$, as shown in Figures 7 and 8), it is visually easy to clearly distinguish the difference between the two architectures:

- In the network with a few P routers (10 P routers in Figure 7), from 0 to 200 PE routers, there is not an architecture less complex than another one, but from 200 to 1000 PE routers, choosing the architecture based on MPLS using LSPs may be the better choice.
- In the network with a lot of P routers (100 P routers in Figure 8), from 0 to 1000 PE routers, it is definitively better to choose the architecture based on MPLS over L2TPv3.

About this first method, measuring the complexity by measuring the differences, working on the differences from the two architectures, it is not a perfect method: the MPLS using L2TPv3 architecture, the packet uses the IP header to traverse the transit network; but in MPLS using LSPs, the packets use the IGP label to traverse the transit network. The LDP protocol has been analysed, but the IGP protocol has been ignored, because it accomplishes the same function in the two architectures (it allows the IP reachability of all nodes in the Service Provider's network).

4.2. Method #2

The idea here is to consider the network as a set of sub-groups. Based on this consideration, to evaluate the complexity of the entire network, it is the same thing as evaluating the complexity of each subgroup individually.

From the analysis already carried out in Section 3, three groups can be distinguished in these two architectures:

- A group focused on the PE router – PE router links;
- A group focused on the PE router – P router links;
- A group focused on the P router – P router links.

In this second method, measuring the complexity as a set of subgroups, the memory consumption will not be considered as the measure of complexity, instead, the complexity will be taken as the number of possible cases between the two routers.

To summarise this method:

$$C = C_{PE\text{-}PE} + C_{PE\text{-}P} + C_{P\text{-}P} \quad (4)$$

With: C representing the global complexity,

$C_{PE\text{-}PE}$ the complexity of the $PE - PE$ router links group, $C_{PE\text{-}P}$ the complexity of the $PE - P$ router links group and $C_{P\text{-}P}$ the complexity of the $P - P$ router links group.

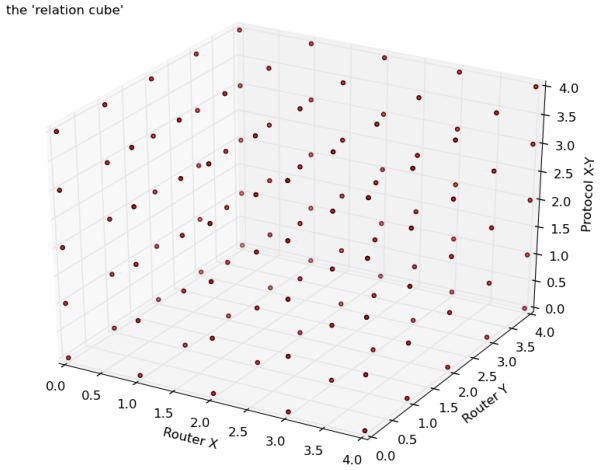

Figure 11. A "relation cube", where the routers X and Y have five different states and the protocols X-Y have five different combinations. [11]

This second method also introduces the utilisation of the "Relation Cube". In the group $X - Y$, the "Relation Cube" represents all the possible combinations: state of the router X, state of the router Y, protocol between X and Y, as shown in Fig. 11.

By using the "Relation Cube", the complexity $C_{X\text{-}Y}$ of the group $X - Y$ is equal to:

$$C_{X-Y} = n_X n_Y \times R_X \times R_Y \times P_{X-Y} \quad (5)$$

With: n_X being the number of routers X in the network; n_Y the number of routers Y in the network;

R_X the number of states that a router X can take;

R_Y the number of states that a router Y can take and $P_{X\text{-}Y}$ the number protocols (and which protocol) running between a router X and a router Y.

The analyses will be done on the relative approach, which means on the evolution of the percentage of PE routers in the network. Because the network analysed contains only PE and P routers, it is easy to determine the part of the P routers in the network.

In the group PE router – PE router links, the MPLS over L2TPv3 architecture is more complex than in the other architecture.

In the two others groups, the MPLS using LSPs architecture is more complex than the MPLS over L2TPv3 architecture.

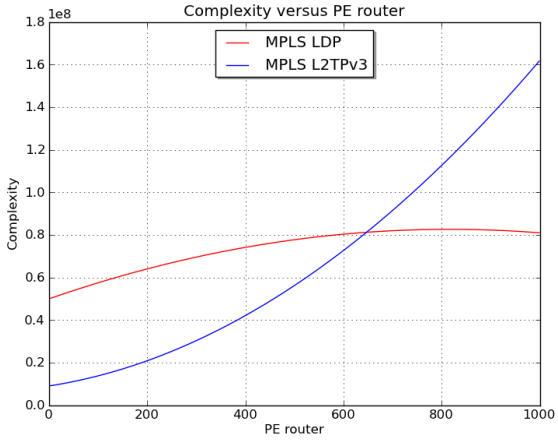

Figure 12. Complexity versus PE router.

In Figure 12, there is an intersection between the line representing the complexity in an architecture based on MPLS using LSPs and the line representing the complexity in an architecture based on MPLS over L2TPv3.

The complexity is the same on the two architectures, for a network containing about 647 PE routers (64.7% of the network are PE routers).

So:

- From 0% to 64.7% of PE routers in the network, the architecture based on MPLS using LSPs is more complex than the architecture based on MPLS over L2TPv3. It is preferable to choose MPLS over L2TPv3: for instance, if there are only two PE routers, it is better to configure MPLS over L2TPv3 than to configure the LDP protocol on all the routers.
- Above 64.7% of PE routers in the network, the architecture based on MPLS over L2TPv3 is more complex than the architecture based on MPLS using LSPs. Hence it is preferable to choose MPLS using LSPs: for instance, if there are only two P routers, it is simpler to configure MPLS using LSPs than to configure a L2TPv3 tunnel on each PE router (998 PE routers).

About this method, the utilization of the "relation cube" allows a generic calculation.

5. Conclusions

Although the MPLS over L2TPv3 offers some interesting security features and a lower complexity than the architecture based on MPLS using LSPs - it is actually the architecture based on MPLS using LSPs, which is widely implemented in practice.

The next step in this work will be to formalize the methods in an objective and structured way by investigating other types of architectures in order to derive some general characteristics of the network complexity.

Acknowledgments: We would like to thank Mr. Michael Behringer, now with Stealth Mode, Nice Area, France, formerly distinguished engineer at Cisco Systems for all his advice.

References

[1] R. Bush and D. Meyer, "Some Internet Architectural Guidelines and Philosophy", http://tools.ietf.org/html/rfc3439 (accessed 21st Aug., 2017)

[2] J. Crowcroft, "Internet Failures: an Emergent Sea of Complex Systems and Critical Design Errors?", The Computer Journal, vol. 53, no. 10, 2010. (accessed 21st Aug., 2017) https://pdfs.semanticscholar.org/aba4/bba76cb4edf7455145f15ee56e975ab1eec2.pdf

[3] E. Romijn, "RIPE NCC and Duke University BGP Experiment", http://labs.ripe.net/Members/erik/ripe-ncc-and-duke-university-bgp-experiment and

http://morse.colorado.edu/~epperson/courses/routing-protocols/handouts/ripe-bgp-experiment-gone-awry.pdf (accessed 21st Aug., 2017)

[4] M. Behringer, "Network Complexity - SP Sec Forum 2010", 2nd Nov., 2010. http://networkcomplexity.org/wiki/images/b/b9/Behringer_-_SP_Sec_Forum_2010_-_Complexity.pdf (accessed 21st Aug., 2017)

[5] V. Ishakian, J. Akinwumi and I. Matta, "On the Cost of Supporting Multihoming and Mobility", 2009. http://rina.tssg.org/docs/RINAvsLISP-BUCS-TechReport_June_2009.pdf (accessed 21st Aug., 2017)

[6] K. Muthukrishnan and A. Malis, "RFC 2917 - A Core MPLS IP VPN Architecture", September 2000. http://tools.ietf.org/html/rfc2917 (accessed 21st Aug., 2017)

[7] L. Anderson and T. Madsen, "RFC 4026 - Provider Provisioned Virtual Private Network (VPN) Terminolog", March 2005. http://tools.ietf.org/html/rfc4026 (accessed 21st Aug., 2017)

[8] E. C. Rosen and Y. Rekhter, "RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs)", February 2006. http://tools.ietf.org/html/rfc4364 (accessed 21st Aug., 2017)

[9] Y. Rekhter and E. Rosen, "RFC 3107 - Carrying Label Information in BGP-4", May 2001. http://tools.ietf.org/html/rfc3107 (accessed 21st Aug., 2017).

[10] M. W. Townsley, "MPLS over Various IP Tunnels - presentation at the NANOG 30 - Miami, 10th Feb., 2004", 2004. http://www.nanog.org/meetings/nanog30/presentations/townsley.pdf (accessed 21st Aug., 2017)

[11] O. Zheng, "Comparing the Complexity of Two Network Architecture", MSc dissertation, 2011, Dept. of Computing and Communications Technologies, Oxford Brookes University, Wheatley, Oxfordshire, UK.
http://www.academia.edu/1190111/Comparing_the_Complexity_of_Two_Network_Architectures (accessed 21st Aug., 2017)

[12] Cisco Systems, "Implementing MPLS Label Distribution Protocol on Cisco IOS XR Software", https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/iosxr_r3-7/mpls/configuration/guide/gc37ldp.html (accessed 21st Aug., 2017)

[13] Cisco Systems, "Implementing MPLS VPNs over IP Tunnels on Cisco IOS XR Software", https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/iosxr_r3-7/mpls/configuration/guide/gc37vpip.html (accessed 21st Aug., 2017)

[14] Juniper Networks, "MPLS Applications Configuration Guide Release 12.3", https://www.juniper.net/documentation/en_US/junos12.3/information-products/pathway-pages/config-guide-mpls-applications/index.html (accessed 21st July, 2017).