MPLS Working Group
Internet-Draft
Intended Status: Experimental RFC
Expires: August 2013

Shankar Raman
Balaji Venkat Venkataswami
Gaurav Raina
Vasan Srini
IIT Madras
Bhargav Bhikkaji
Dell-Force10

February 18, 2013

SNMP based Provider-Provisioned label for Lawful Intercept in L3 VPNs
draft-balaji-mpls-li-thru-label-dis-snmp-01

Abstract

In models of Single-AS and inter-provider Multi- Protocol Label Switching (MPLS) based Virtual Private Networks (VPNs) Lawful Intercept is a key requirement. For example, MPLS-based Layer 3 VPN models do not have any provider provisioned methods of lawful intercept that are comprehensive, quick and easy to provision from one single point. More particularly the auto-provisioning of lawful intercept for all sets of streams travelling between VPN sites and consequent re-direction of these streams to the appropriate government network has not been covered without multiple instances of having to configure the intercept at various points in the network both in the Single-AS case and the Inter-Provider VPN case.

In this paper, we propose a technique which uses a set of pre-defined labels called Lawful Intercept labels and a method for provisioning lawful intercept amongst the various PE devices using these labels both in the Single-AS and the inter-provider VPN cases. A single point of action is the key to this idea. The intercepted traffic is mirrored on a PE or a whole set of PEs or on all the PEs participating in the VPN. A technique called the Domino-effect provisioning of these Label-based Provider Provisioned Lawful Intercept mechanism is also outlined. This differs from [1] in that there is explicit use of a secure SNMP mechanism to provision the labels for Lawful Intercept at the various PEs instead of a MP-BGP update.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that

other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Table of Contents

1 Introduction

Multi-Protocol Label Switching (MPLS) [6] technology uses fixed size labels to forward data packets between routers. By stacking labels, specific customer services such as Layer 3 Virtual Private Networks (L3-VPNs) based on Border Gateway Protocol (BGP) extensions are widely deployed in the Internet. BGP-based MPLS L3-VPN services are provided either on a single Internet Service Provider (ISP) core or across multiple ISP cores. The latter cases are known as inter-provider MPLS L3-VPNs which are broadly categorized and referred to as models: "A", "B" and "C".

In all the above cases both Single-AS and inter-provider VPN cases for Layer 3 VPNs it is important that the provider or multiple providers have a co-ordinated mechanism of lawfully intercepting traffic to and from Provider Edge Routers (PEs) belonging to one or more VPN instances for the VPN instance as a whole or for a specific subnet / prefix.

This paper outlines a label-based Provider Provisioning technique that helps to provide a single point of action for lawfully intercepting through traffic mirroring or other such techniques of data flowing to and from one or more PEs or all of the PEs that constitute a particular VPN instance. More than one VPN instance may be configured with this technique. Also Enhanced Remote SPAN with GRE keying mechanism is used to transport the intercepted packets to a Lawful Intercept device where it may be examined and analyzed by Government Authorities.

In the spirit of RFC 2804 and given that RFC 3924 that already exists, this mechanism can be considered from the point of view of an Experimental draft. No other opinion is professed except to document this as a possible method to use in times of crisis and emergency. In the spirit of 2804 which states and we quote...

- On the other hand, the IETF believes that mechanisms designed to facilitate or enable wiretapping, or methods of using other facilities for such purposes, should be openly described, so as to ensure the maximum review of the mechanisms and ensure that they adhere as closely as possible to their design constraints. The IETF believes that the publication of such mechanisms, and the publication of known weaknesses in such mechanisms, is a Good Thing."

End of Quote.

Hence we submit this document for review in the spirit of what is said above.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Methodology of the proposal

2.1 PRE-REQUISITES FOR THE LABEL-BASED Provider-Provisioned SCHEME for LI

In this section, we briefly review the pre-requisites for applying this technique in terms of the PE configuration and the control-plane exchanges needed for our proposed scheme.

2.1.1 Configuring Lawful Intercept for a specific VPN instance on a specific PE

The regular mechanisms using SNMP using the TAP-MIB can be used to configure the requirement to intercept traffic going to and from a given PE router. This very mechanism is used to initiate the scheme mentioned in this document.

2.1.2.1 PE configuration

Various configurations are needed on the PEs to implement the label based Lawful Intercept scheme. A set of pre-defined labels called the Lawful Intercept labels are provided for a VPN instance that is configured on the PE. In the simplest case one single Lawful Intercept label may be used per VPN instance . In this draft, we assume that a single label based lawful intercept is used per VPN instance per PE for cases where the whole VPN site traffic needs to be trapped. For cases where specific flows are required to be monitored section 2.2.4 outlines the necessary actions to be taken.

2.1.3 Control and data-plane flow

Initially, the usual control plane exchanges take place where the labels configured for the Layer 3 VPN instance between the various PEs participating for that VPN instance are exchanged securely over the control-plane.

Appropriate Lawful Intercept labels are configured or a knob that allocates them automatically is configured. These labels are not exchanged at the time when the LI based mechanism is not in place, meaning the TAP-MIBs are not yet setup for LI for a VPN instance.

Appropriate ports that will mirror these LI intercepted frames are set up and pre-provisioned with links to the devices that will analyze the data when such interception occurs.

Once the secure control-plane exchanges are completed, normal traffic starts to flow. It is possible then that an event occurs which results in a PE being configured for Lawful Intercept to take place. Such an event could be a police tipoff, external intelligence inputs and other events. The exact set of events that will trigger LI are outside the scope of this document. Once the PE (which we will call the dPE) is configured with this, the control plane in this case SNMP then sends over the LI label to the other PEs of the same VPN instance in the form of a secure SNMP PDU with the relevant details such as

a) Prefix for which LI is to be enforced

b) Actual LI label to be used

c) DominoEffectTrigger Flag (OFF or ON)

These other PEs called the sPEs (or the source PEs for short), then install this LI label to be the inner label or the VPN service label in their packets they send to the dPE. Appropriate ACLs configured for intercepting packets coming into the dPE with the LI label route the traffic to the mirroring port on the dPE. This is then encapsulated in a GRE tunnel and sent over to the Government network after suitable encryption if necessary.

2.2 Domino-effect technique

In this case called the Domino-effect technique, all sPEs receiving control plane exchanges with an indication that a LI label is being requested to be installed on them in turn also send their respective LI labels to other PEs in distinct control plane exchanges through SNMP. This will result in the entire VPNs traffic being monitored at the various participating PEs for that VPN.

As already mentioned appropriate Access Control Entries (ACEs) in the PEs will direct the traffic coming in with these LI labels to the mirroring ports, one or more if any.

The inner label information is mapped to a GRE key and the mirrored packets at the intercepting dPE are sent with this GRE key in place with of course the GRE encapsulation to the analyzing network devices. Additional information as to which sPE the traffic came from is thus added to the packet in the form of the GRE key. The exact means of this technique is upto the implementer to take up.

2.2.0 Per-Prefix label to Per-VRF LI label

If the configuration on the dPE is to disseminate per-prefix labels then the introduction of the LI label is such that it (the LI label) is advertised as a an aggregate per-VRF label so that all of the traffic is bunched together in the transmit and/or the receive direction to the dPE and from the dPE pivoting around an appropriate single LI label so that it can be easily trapped by the ACE entry in the dPE (and if the domino is triggered in the sPEs as well) to get mirrored onto one or more ports.

2.2.1 Algorithm 1 Control-plane dPE algorithm

```
Require:
* K Valid Lawful Intercept labels per VPN for FECs to be monitored
* If in case the whole VPN site then a single label
* else specific LI labels for each prefix to be monitored
at required granularity as per VRF route entries.

Begin
Get event that triggers configuration in the TAP-MIB;

Get TAP-MIB configured particulars about which VPN and whether
    FlagTriggerDominoEffect is set;

packet = makeSNMPpacket(K[VPN Instance or FECinVPN],
                    FlagTriggerDominoEffect);

For all sPEs in the VPN

CP-SendPacket(sPE[j], Secure-SNMP, packet);

endFor
End
```

2.2.2 Algorithm 2 Control-plane sPE algorithm

```
Require: None
Begin
SNMPpacket = CP-ReceivePacket(dPE); // from dPE
Label = ExtractLabel(SNMPpacket); // extract LI label
if (Label is LI label as indicated by SNMP ObjectID information) then
   Set Label in Forwarding table for the VPN;
endif
FlagTriggerDominoEffect = ExtractFlags(SNMPpacket);
if (FlagTriggerDominoEffect) then
   Run Algorithm 1 on the sPE (as the dPE);
End
```

2.2.3 Algorithm 3 Data-plane dPE algorithm

```
Require: None

Begin
packet = DP-ReceivePacket(Interface);
if ((Label of packet is == LI label for VPN) &&
    (ACL configured for the said Label))
then

   mirror packet with all information after mapping
   VPN label to GRE key which indicates dPE;

   Encapsulate packet in GRE header and mirror it
   to appropriate port;

endif
End
```

2.2.4 Monitoring specific flows

There would be a necessity to monitor specific flows headed towards and from a subnet or a specific IP address within a site. This monitoring would be needed to be done at all sites to which this subnet or specific IP address within the monitored VRF communicates with. For this specific purpose the LI label may be sent from the dPE to the sPEs (with say the DominoEffectTrigger Flag set) for the specific prefix / subnet / IP address. Though the specific IP address cannot be trapped with a prefix entry with the LI label alone, specific Access Control Lists may be setup at all dPEs where the monitoring takes place to trap the specific IP address in particular. The flexibility lies with both the LI label based on prefix and the consequent Access Control List configured collaboratively working together to monitor the specific IP address or even subnet / prefix.

The algorithm in 2.2.1 to 2.2.3 apply for the specific flow monitoring cases as well.

2.2.5 Hierarchalizing the GRE key

The GRE key can be organized in a hierarchy with respect to site and PE information for a provider who is providing the label based lawful intercept. Since the GRE key is a 32 bit entity, the site could be 20 bit ID with the Provider edge router providing the facility being indicated by a 12 bit identifier. The source IP address being the indicator of the provider / ISP who is providing the facility the hierarchy in the GRE key would indicate the location and the PE device from where the frames are being trapped. The intercepting

authority could thus figure out in the clutter of information as to where the encapsulated frames are being emanated from. A common registry for the site identifier could be provided and set in the GRE key information thus dilineating information coming from different PE devices in different locations. It is suffice to say that a 20 bit identifier for the site could cover the location. In turn the site identifier could be broken into Country code and Zip code as well in the registry.

2.4 CONCLUSION AND FUTURE WORK

Additionally this same idea can be applied for L2-VPNs as well. A future draft in this area will be published in due course.

2.5 ACKNOWLEDGEMENTS

The authors would like to acknowledge the UK EP-SRC Digital Economy Programme and the Government of India Department of Science and Technology (DST) for funding given to the IU-ATC.

3 Security Considerations

Encryption of the packets funneled to the analyzing devices needs to be considered.

4 IANA Considerations

Appropriate SNMP MIB particulars need to be drawn up to support this mechanism. Vendor specific MIBs are a good choice to deploy this scheme. That way IANA indicators would not have to be provided to exchange the set of values that Algorithm 1,2 outlines in order to implement this scheme like if say BGP were to be used for the control plane exchanges.

5 References

5.1 Normative References

5.2 Informative References

[1] Shankar Raman et.al, "Label based Provider-Provisioned Lawful Intercept for L3 VPNs", draft-balaji-mpls-lawful-intercept-thru-label-dis-02.txt, Work in Progress, August 2012.

[1a] S. Alouneh, A. En-Nouaary and A. Agarwal, "MPLS security: an approach for unicast and multicast environments", Annals of Telecommunications, Springer, vol. 64, no. 5, June 2009, pp. 391-400, doi:10.1007/s12243-009-0089-y.

[2] M. H. Behringer and M. J. Morrow, "MPLS VPN security", Cisco Press, June 2005, ISBN-10: 1587051834.

[3] B. Daugherty and C. Metz, "Multiprotocol Label Switching and IP, Part 1, MPLS VPNS over IP Tunnels", IEEE Internet Computing, May-June 2005, pp. 68-72, doi: 10.1109/MIC.2005.61.

[4] L. Fang, N. Bita, J. L. Le Roux and J. Miles, "Interprovider IP-MPLS services: requirements, implementations, and challenges", IEEE Communications Magazine, vol. 43, no. 6, June 2005, pp. 119-128, doi: 10.1109/MCOM.2005.1452840.

[5] C. Lin and W. Guowei, "Security research of VPN technology based on MPLS", Proceedings of the Third International Symposium on Computer Science and Computational Technology (ISCSCT 10), August 2010, pp. 168-170, ISBN- 13:9789525726107.

[6] Y. Rekhter, B. Davie, E. Rosen, G. Swallow, D. Farinacci and D. Katz, "Tag switching architecture overview", Proceedings of the IEEE, vol. 85, no. 12, December 1997, pp. 1973-1983, doi:10.1109/5.650179.

[7] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, Standard Track, February, 2006.

[8] T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, "Introduction to algorithms", 3rd edition, MIT Press, September 2009, ISBN-10:0262033844.

[9] C. Semeria, "RFC 2547bis: BGP/MPLS VPN fundamentals", Juniper Networks white paper, March 2001.

[10] Advance MPLS VPN Security Tutorials [Online], Available: "http://etutorials.org/Networking/MPLS+VPN+security/Part+II+Advanced+MPLS+VPN+Security+Issues/", [Accessed: 10th December 2011]

[11] Inter-provider MPLS VPN models [Online], Available: "http://mpls-configuration-on-cisco-iossoftware.org.ua/1587051990/ ch07lev1sec4.html", [Accessed 10th December 2011]

[12] Davari.S et.al, Transporting PTP messages (1588) over MPLS networks, "http://datatracker.ietf.org/doc/draft-ietf-tictoc-1588overmpls/?include_text=1", Work in Progress, October 2011.

[RFC3924] Baker, F., Foster, B., and C. Sharp, "Cisco Architecture for Lawful Intercept in IP Networks", RFC 3924, October 2004.

Authors' Addresses

Shankar Raman
Department of Computer Science and Engineering

IIT Madras
Chennai - 600036
TamilNadu
India

EMail: mjsraman@cse.iitm.ac.in

Balaji Venkat Venkataswami
Department of Electrical Engineering
IIT Madras
Chennai - 600036
TamilNadu
India.

EMail: balajivenkat299@gmail.com

Prof.Gaurav Raina
Department of Electrical Engineering
IIT Madras
Chennai - 600036
TamilNadu
India.

EMail: gaurav@ee.iitm.ac.in

Bhargav Bhikkaji
Dell-Force10
350 Holger Way
San Jose
CA
USA

Email: Bhargav_Bhikkaji@dell.com

Vasan Srini
Department of Computer Science and Engineering
IIT Madras
Chennai - 600036
TamilNadu
India.

EMail: vasan.vs@gmail.com