L3VPN Working Group
Internet-Draft
Updates: 4382 (if approved)
Intended status: Standards Track
Expires: April 27, 2011

Chen. Li
Lianyuan. Li
Lu. Huang
China Mobile
Ke. Ma
Hao. Tang
China Academy of Telecommunication

October 24, 2010

# MPLS Layer 3 Carrier Support Carrier Virtual Private Network Management Information Base
draft-li-network-mpls-l3vpn-csc-vpn-mib-01

## Abstract

This memo defines an portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects to configure and/or monitor Multi-protocol Label Switching Layer-3 Carrier Support Carrier Virtual Private Networks on a Multi-Protocol Label Switching (MPLS) Label Switching Router (LSR) supporting this feature.

this memo supplements RFC [4382] which focus on MPLS VPN MIB.

## Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 27, 2011.

## Copyright Notice

Table of Contents

## 1. Introduction

This memo defines an portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects to configure and/or monitor Multi-protocol Label Switching Layer-3 Carrier Support Carrier(CSC) Virtual Private Networks on a Multi-Protocol Label Switching (MPLS) Label Switching Router (LSR) supporting this feature.

This document adopts the definitions, acronyms and mechanisms described in [2547] and [4382] . Unless otherwise stated, the mechanisms of [2547] and [4382] apply and will not be re-described here.

## 2. Requirements Language

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 [RFC2119].

## 3. The MPLS-L3-CSC-VPN-MIB Objects

The MIB objects related with MPLS L3 CSC VPN are defined by mplsL3CscVpnVrfLabelSwtichTable.

This table represents the MPLS L3 CSC VPN VRF Table that are configured. A Network Management System (NMS) or SNMP agent creates an entry in this table for every MPLS L3 CSC VPN configured on the LSR being examined. The table supplements the MIB Objects in RFC 4382.

The relationship between this draft and RFC4382 can be described as the image below:

MPLS L3VPN MIB

|--MplsL3VpnObject

|----MplsL3VpnRoute

|------mplsL3VpnVrfRteTable

|--------mplsL3VpnVrfRteTable

|--------(New)mplsL3CscVpnVrfLabelSwtichTable

## 4. MPLS-L3-CSC-VPN-MIB Module Definition

```
   -- VPN VRF Label Switch Table

   mplsL3VpnVrfLabelSwitchTable OBJECT-TYPE

   SYNTAX SEQUENCE OF MplsL3VpnVrflabelSwitchEntry

   MAX-ACCESS not-accessible

   STATUS current

   DESCRIPTION

   "This table specifies per-interface MPLS L3 CSC VPN VRF Table label
   switching information.  Entries in this table define VRF label
   switching entries associated with the specified MPLS CSC VPN
   interfaces."

   ::= { mplsL3VpnRoute 2 }

   mplsL3VpnVrfLabelSwitchEntry OBJECT-TYPE

   SYNTAX MplsL3VpnVrfLabelSwitchEntry

   MAX-ACCESS not-accessible

   STATUS current

   DESCRIPTION

   "An entry in this table is created by an LSR for every label within
   the context of a specific VRF capable of supporting MPLS/BGP CSC VPN.
   The indexing provides an ordering of VRFs per-VPN interface."

   INDEX { mplsL3VpnVrfName,

   mplsL3VpnVrfLabelSwtichInLabel,

   mplsL3VpnVrfLabelSwtichOutLabel,

   mplsL3VpnVrfLabelSwtichPushLabel,

   mplsL3VpnVrfLabelSwtichNHopType,

   mplsL3VpnVrfLabelSwtichNHop,

   }
```

```
   ::= { mplsL3VpnVrfLabelSwitchTable 1 }

   MplsL3VpnVrfLabelSwitchEntry ::= SEQUENCE {

   mplsL3VpnVrfLabelSwitchInLabel MplsLabel,

   mplsL3VpnVrfLabelSwtichOutLabel MplsLabel,

   mplsL3VpnVrfLabelSwtichPushLabel MplsLabelorZero,

   mplsL3VpnVrfLabelSwtichAge Gauge32,

   mplsL3VpnVrfLabelSwitchNHop InterfaceIndexorZero,

   mplsL3VpnVrfLabelSwtichProto INTEGER,

   mplsL3VpnVrfLabelSwitchProtectLabel MplsLabelorZero,

   mplsL3VpnVrfLabelSwitchProtectNHop InterfaceIndexorZero,

   mplsL3VpnVrfLabelSwitchProtectType INTEGER,

   }

   ::= { mplsL3VpnVrfLabelSwitchTable 1 }

   mplsL3VpnVrfLabelSwitchInLabel OBJECT-TYPE

   SYNTAX MplsLabel

   MAX-ACCESS not-accessible

   STATUS current

   DESCRIPTION

   "The outer label of the packet, The label point to the remote tier_2
   PE"

   ::= { mplsL3VpnVrfLabelSwitchEntry 1 }

   mplsL3VpnVrfLabelSwitchOutLabel OBJECT-TYPE

   SYNTAX MplsLabel

   MAX-ACCESS not-accessible

   STATUS current
```

```
   DESCRIPTION

   "The new label point to the remote tier_2 PE, which will replace the
   inlabel"

   ::= { mplsL3VpnVrfLabelSwitchEntry 2 }

   mplsL3VpnVrfLabelSwitchPushLabel OBJECT-TYPE

   SYNTAX MplsLabelorZero

   MAX-ACCESS not-accessible

   STATUS current

   DESCRIPTION

   " The label point to the remote tier_1 PE, which will be pushed to
   the packet.  A value of 0 is valid and represents the scenario that
   the packet should be sent to tier_2 network"

   ::= { mplsL3VpnVrfLabelSwitchEntry 3 }

   mplsL3VpnVrfLabelSwtichAge OBJECT-TYPE

   SYNTAX Gauge32

   MAX-ACCESS read-only

   STATUS current

   DESCRIPTION

   "The number of seconds since this label switch item was last updated
   or otherwise determined to be correct. "

   ::= { mplsL3VpnVrfLabelSwitchEntry 4 }

   mplsL3VpnVrfLabelSwitchNHop OBJECT-TYPE

   SYNTAX InterfaceIndexOrZero

   MAX-ACCESS read-create

   STATUS current

   DESCRIPTION
```

"The ifIndex value that identifies the local interface through which the next hop of the packet should be forwarded. A value of 0 is valid and represents the scenario where no interface is specified."

DEFVAL { 0 }

::= { mplsL3VpnVrfLabelSwitchEntry 5 }

mplsL3VpnVrfLabelSwtichProto OBJECT-TYPE

SYNTAX INTEGER {

other (1),

LDP (2),

BGP (3),

RSVP (4),

}

MAX-ACCESS read-creat

STATUS current

DESCRIPTION

"The label distributing mechanism."

DEFVAL { other }

::= { mplsL3VpnVrfLabelSwitchEntry 6 }

mplsL3VpnVrfLabelSwitchProtectLabel OBJECT-TYPE

SYNTAX MplsLabelorZero

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

" The backup label point to the remote tier_1 PE. A value of 0 is valid and represents the scenario that there isn’t any protect path and label"

```
   DEFVAL { 0 }

   ::= { mplsL3VpnVrfLabelSwitchEntry 7 }

   mplsL3VpnVrfLabelSwitchProtectNHop OBJECT-TYPE

   SYNTAX InterfaceIndexOrZero

   MAX-ACCESS read-create

   STATUS current

   DESCRIPTION

   "The ifIndex value that identifies the backup interface through which
   the next hop of the packet should be forwarded.  A value of 0 is
   valid and represents the scenario where no interface is specified."

   DEFVAL { 0 }

   ::= { mplsL3VpnVrfLabelSwitchEntry 8 }

   mplsL3VpnVrfLabelSwitchProtectType OBJECT-TYPE

   SYNTAX INTEGER {

   other (1),

   bypass (2),

   detour (3),

   }

   MAX-ACCESS read-creat

   STATUS current

   DESCRIPTION

   "The MPLS TE fast reroute protect mechanism.  Bypass refers to
   facility backup LSP.  Detour refers to one-to-one backup LSP."

   DEFVAL { other }

   ::= { mplsL3VpnVrfLabelSwitchEntry 9 }

   -- End of MPLS-L3-CSC-VPN-MIB
```

## 5. Security Considerations

MPLS-L3-CSC-VPN-MIB is useful for monitoring of MPLS LSRs supporting L3. MPLS CSC VPN. This MIB module can also be used for configuration of certain objects, and anything that can be configured can be incorrectly configured, with potentially disastrous results.

mplsL3CscVpnVrfLabelSwtichTable contain objects which may be used to provision L3VPN switch interfaces and configuration. Unauthorized access to objects in the tables, could result in disruption of traffic on the network. This is especially true if these VRFs have been previously provisioned and are in use. The use of stronger mechanisms such as SNMPv3 security should be considered where possible. Specifically,SNMPv3 VACM and USM MUST be used with any v3 agent which implements this MIB module. Administrators should consider whether read access to these objects should be allowed, since read access may be undesirable under certain circumstances.

## 6. IANA Considerations

It is no necessary to request new IANA code in the draft.

## 7. Acknowledgments

This document has benefited from discussions and input from Lilianyuan, Ma Ke, Huang Lu,Tang Hao, and Li Zhenqiang.

## 8. Normative References

[RFC4382] Nadeau, T. and H. van der Linde, "MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base", RFC 4382, February 2006.

## Authors' Addresses

Chen Li
China Mobile
Unit2, Dacheng Plaza, No. 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
P.R. China

Email: lichenyj@chinamobile.com

Lianyuan Li
China Mobile
Unit2, Dacheng Plaza, No. 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
P.R. China

Email: lilianyuan@chinamobile.com

Lu Huang
China Mobile
Unit2, Dacheng Plaza, No. 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
P.R. China

Email: huanglu@chinamobile.com

Ke Ma
China Academy of Telecommunication
No.52 HuaYuanBeiLu
Beijing 100191
P.R. China

Email: make@mail.ritt.com.cn

Tang Hao
China Academy of Telecommunication
No.52 HuaYuanBeiLu
Beijing 100191
P.R. China

Email: tanghao@mail.ritt.com.cn

So et al
Verizon



# VPN Extensions for Private Clouds
draft-so-vepc-00.txt

## 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

## Copyright and License Notice

Abstract

This contribution addresses the service providers requirements to support Cloud services interworking with the existing MPLS-based L2 and L3 VPN services. Maintenance of virtual separation of the traffic, data, and queries must be supported for the VPN customers that are conscious of end-to-end security features and functions that VPN technologies provide today.

Table of Contents

# 1 Introduction

Data center, WAN/MAN, and the end user are three of the components that make up the Cloud in the vision of Cloud Computing. However, the existing technologies often treat each component as black boxes, detached from each other. This fact limits the overall cohesiveness of an end-to-end service. For example, the network often views the data center as a black box, meaning the network has no control or visibility (from a standards point-of-view) into the data center.

As a network provider, a Cloud-service product may be offered across multiple data centers globally, some of which may be owned by a network provider while others may be owned by a partner/vendor. In addition, multiple Cloud-Service products can be offered in the same data centers. A list of the problems that this situation is causing the network provider/operator, especially for the existing VPN customers, is presented below. These must be addressed immediately, in order for service providers to persuade the existing VPN customers to leverage the deployed Cloud-based services.

## 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 Cloud Customer End to End Separation

## 2.1. VPN Traffic Segregation Requirements

The success of VPN services in the enterprise and the government world is largely due to its ability to virtually segregate the customer traffic at layer 2 and layer 3. The lower the layer that segregation can be maintained, the safer it is for the customers from security and privacy perspectives. Today data centers segregate the customer traffic at layer 7 (application), and there is no standard for extending the VPN into data center. Network service providers view the VPN extension into data center, allowing traffic segregation per VPN, an essential necessity to the success of Cloud-Services in the enterprises and government markets. Cloud-Applications (or the virtualization function) SHOULD have the ability to get access to VPN (including Layer 2/3 VPN) services, to segregate different Cloud-Services traffic trough the network.

## 2.2. Potential Solution

### 2.2.1. VPN Gateway Managed Connection Segregation

One possible way to achieve this is to have each Cloud-Application

setup connections with the VPN gateways, while the gateways attach each connection to corresponding VPN. Each Cloud-Application SHALL be transmitted over a pre-defined set of connections, and each VPN utilizing the application SHALL be transmitted over a sub-set of application connections. In this case, each Cloud-Application SHALL maintain its own independent routing table. This is possible for some current operating systems, which already support multiple routing instances for its TCP/IP stack.

2.2.2 solution using Provider Backbone Bridging (PBB) and Shortest Path Bridging (SPB)

Ethernet and VLANS are the standard L2 connectivity model throughout the data center environment. As such the IEEE has been working on numerous projects to simplify and extend traditional Ethernet models for scale and flexibility. Additionally the IEEE has projects looking at new attachments models for Virtual Machines (VM’s) to become more autonomic and secure for environments that include wholly owned and multi-tenant.

Although VLAN and PPPoE are different types of connections, the two methods described above are fundamentally the same. Consequently, it is possible to generalize the descriptions above to cover both the cases.

2.2.3 VPN Gateway Controlled Traffic Flow

It is also possible for each Cloud-Application to acquire access to L2/L3 VPN with one shared routing table supported on the server. One way to do that is to have the VPN gateway manage the traffic flow instead of other way around. In that case, the VPN gateway has the VRF table and the destination server connection address. Once the server receives the traffic, it determines intra-data center destination based on the application. So the control sequence is VPN first, and then application. The control sequence for the first two methods described above is application first, and then VPN.

2.2.4 Inter-VPN Interworking

L2/L3 VPN based MPLS network can also be deployed in the data center to manage the intra-data center traffic flow. The data center VPN structure can be set up in such a way that each external VPN can be mapped to a unique internal VPN.

2.3. Cloud Services Virtualization

2.3.1. Cloud Virtualization Requirements

Today data center virtualization is totally handled by data center servers and hypervisors. The entire process is invisible to the underlying networks. The virtualization function including application server and virtual machine (VM) allocation and assignment, disk space allocation, traffic loading and balancing, QoS assignments, and so on. There shall be a way that the network can influence some virtualization functions that are important to the concept and spirit of the VPN.

- The Private Cloud provisioning and management system SHALL have the ability to dedicate a specific block of disk space per services per VPN.

- Each VPN SHALL have the exclusive access to the dedicated block of disk space.

- Each VPN SHALL have the ability to indicate the mechanism used to prevent the unwanted data retrieval for the block of disk space after it is no longer used by the VPN, before it can be re-used by other parties.

- Each VPN SHALL have the ability to request a dedicated VM with certainly CPU capability, amount of memory and disk space.

- The VPN SHALL have the ability to request dedicated L2/3 network resources within the data center such as bandwidth, priorities, and so on.

- The VPN SHALL have the ability to hold the requested resources without sharing with any other parties.

## 2.4. Cloud Services Restoration

Today, data center restoration and diversity designs are not necessarily linked to the network restoration and diversity design. This results in over-redundant design, wasting money and resources, and may cause traffic oscillation and service and performance degradation. This problem is particularly important to the VPN traffic, which is usually highly performance sensitive. The VPN extension SHOULD be able to indicate how the restoration is handled across layers, so that a unified end-to-end design and optimization can be achieved.

Furthermore the restoration capability awareness needs to be scalable, meaning problems occur in one area of the Cloud SHALL NOT affect all other areas of the Cloud involved. This way each component of the Cloud can scale independently without causing systemic failures and/or allowing a single failure to cascade across

the Cloud.

### 2.5 Other Non-VPN Specific Areas

There are a number of known technology gaps preventing the data centers, networks, and the end users from interworking together in providing optimized and seamless end-to-end services. Although those areas are beyond VPN, they impact the VPN-based cloud services significantly. Those areas are listed below, but they are beyond the scope of this draft.

#### 2.5.1. Cloud Traffic Load-Balancing and Congestion Avoidance

Todays Cloud traffic balancing and congestion avoidance is purely data center based. The network condition is not taken into consideration. The VPN extension SHOULD support the network condition to be used for the traffic balancing and congestion avoidance decision-making.

#### 2.5.2. QoS Synchronization

It is required that the virtualization functions QoS requirement SHOULD be synchronized with VPN service.

#### 2.5.3 Cross Layer Optimization

The VPN resource requested by the server CAN be optimized by statistical multiplexing of the resource. For example, for each VPN resource, it is possible to configure committed BW for each QoS resources and peak BW for best effort traffic, and the peak BW resources CAN be shared by different VPN service.

#### 2.5.4 Automation end to end Configuration

The automatic end-to-end network configuration will reduce the operational cost and also the probability of occurrence of mis-configuration. The VPN Extension SHALL support the automatic end-to-end network configuration.

### 2.6. End-to-End Quality of Experience (ETE-QoE)

Quality of experience (QoE) management refers to maintaining a set of application /service layer parameters within certain threshold with an objective to retain the user experience for a specific service. Very often when new underlying technologies and/or mechanisms are introduced for implementing the same services (voice, data, video, messaging, etc.), opportunities exist to improve the user experiences. Conversely the user experience may suffer unless the appropriate transport level parameters that significantly impact

the QoE are monitored and managed.

## 2.7. OAM Considerations

The VPN Extension solution MUST have sufficient OAM mechanisms in place to allow consistent end-to-end management of the solution in existing deployed networks. The solution SHOULD use existing protocols (802.3ag, Y.1731, BFD) wherever possible to help with interoperability of existing OAM deployments.

## 2.8. Work Item Considerations in IETF Clouds

In VPN extension to private Clouds, various application level parameters, protocol level parameter, and service monitoring parameters may need to be defined, and the results of monitoring may need to be exchanged periodically. In private cloud environment, since the resources exist in one or co-operative administrative domain, it is easier to monitor and manage the application and transport level parameters for the underlying resources. In some cases, proactive mechanisms can be readily implemented before user experiences degrade to the level of annoyance. In public and hybrid (a smart combination of private and public) clouds it is required to derive a list of mutually agreed upon monitoring and management parameters. Active monitoring using virtual agents and resources is also possible. However, allocation of resources and placement of the virtual agent including the amount of traffic generated for QoE management, and the exchange of the desired information back and forth need to be achieved.

## 3 Security Considerations

The VPN extension SHOULD support variety of security measures in securing tenancy of virtual resources such as resource locking, containment, authentication, access control, encryption, integrity measure, and etc. The VPN extension SHOULD allow the security to be configure end-to-end on a per VPN per-user bases. For example, the Virtual Systems MUST resource lock resources such as memory, but must also provide a cleaning function to insure confidentiality, before being reallocated.

VPN extension for private Clouds SHOULD specify an authentication mechanism based on an authentication algorithms (MD5, HMAC-SHA-1)for both header and payload. Encryption MAY also be use to provide confidentiality.

Security boundaries MAY also be create to maintain domains of TRUSTED, UNTRUSTED, and Hybrid. Within each domain access control techniques MAY be uses to secure resource and administrative domains.

## 4 IANA Considerations

None

## 5 References

### 5.1 Normative References

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

### 5.2 Informative References

None

## Author’s Addresses

Ning So
Verizon Inc.
2400 N. Glenville Rd.,
Richardson, TX 75082

ning.so@verizonbusiness.com

Henry Yu
tw telecom
10475 Park Meadows Dr.
Littleton, CO 80124
henry.yu@twtelecom.com

John M. Heinz
CenturyLink
Phone: 913-533-2115
john.m.heinz@centurylink.com

Paul Unbehagen
Alcatel-Lucent
8742 Lucent Boulevard
Highlands Ranch, CO 80129
paul.unbehagen@alcatel-lucent.com

Mike Mangino
Alcatel-Lucent
8742 Lucent Boulevard
Highlands Ranch, CO 80129
mike.mangino@alcatel-lucent.com

Bhumip Khasnabish
ZTE USA, Inc.
33 Wood Ave. S., 2nd Flr
Iselin, NJ, USA
Tel.:1-781-752-8003
Email: vumip1@gmail.com

Lizhong Jin
ZTE Corporation
889, Bibo Road
Shanghai, 201203, China
Email: lizhong.jin@zte.com.cn