CCAMP Working Group **Kenji Kumaki**
KDDI Corporation
Zafar Ali
Cisco
Systems
Tomohiro Otani
KDDI R&D
Laboratories, Inc.
George
Swallow
Mallik
Tatipamula
Cisco
Systems

Internet Draft
Category: BCP
Expires: July 2006
January 2006

Operational, Deployment and Interworking Considerations for GMPLS

draft-kumaki-ccamp-mpls-gmpls-interworking-02.txt

Status of this Memo

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/ietf/1id-abstracts.txt.

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

Copyright Notice

Abstract

In order to deploy GMPLS technology in the existing IP/MPLS networks, various operation, deployment and interworking aspect of MPLS/GMPLS needs to be addressed.

From the deployment perspective, GMPLS architecture document lists [RFC3945] three different scenarios in which GMPLS technology can be deployed: overlay, augmented and integrated. Reference [GMPLS-mig] addresses the problem of migration from MPLS to GMPLS networks using the integrated model. This draft addresses the same problem space for augmented model and illustrates the applicability of augmented model in deploying GMPLS technology in existing IP/MPLS networks.

Another very important aspect of MPLS/GMPLS interworking is ability to effectively use GMPLS services in IP/MPLS networks. This includes ability to specify GMPLS LSPs in signaling requests based on the type of the setup desired, as well as considerations for the operation aspects of using GMPLS LSPs.

In this draft, we highlight some deployment and MPLS/GMPLS interworking requirements and propose solutions to address them. We also highlight some operation aspects and the possible solution and provide applicability statement for the available options.

Conventions used in this document

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].

Routing Area ID Summary

(This section to be removed before publication.)

SUMMARY

This document addresses some MPLS/ GMPLS deployment, operational and interworking aspects.

WHERE DOES IT FIT IN THE PICTURE OF THE ROUTING AREA WORK?

This work fits in the context of MPLS/GMPLS deployment, operational and interworking.

WHY IS IT TARGETED AT THIS WG?

This document is targeted at ccamp as it addresses some MPLS/GMPLS deployment, operational and interworking aspects.

RELATED REFERENCES

Please refer to the reference section.

Table of Contents

1. Introduction

Introduction of GMPLS technology in existing IP/MPLS networks and migration of IP/MPLS services to GMPLS core poses some new requirements that do not exist while using point to point physical links in the core network. One of the biggest challenges in today's network is "how to deploy GMPLS technology" in a manner least impact on the existing IP/MPLS networks. It is neither feasible nor desired to upgrade all existing nodes to GMPLS technology. In fact, it is required to minimize the impact of migration to GMPLS on the existing IP/MPLS network. It is also desired to respect the administrative boundaries between IP/MPLS and Optical domains.

There are several architectural alternatives including overlay, integrated and augmented models proposed in GMPLS architecture document [RFC3945]. The key difference among these models is how much and what kind of network information can be shared between packet and Optical domains. Peer model is suitable, where optical transport and Internet/Intranet Service networks are operated by a single entity. Currently, many service providers have traditionally built their networks, where Optical transport and IP/MPLS service networks belong to different operation, management, ownership. Most important thing is that service providers wants to operate and manage their networks independently, and deploy them without changing existing IP/MPLS network topologies, protocols and scalability. Overlay model is suitable for such scenario, however does not offer the benefits of peer model approach for efficient resource utilization, optimal routing and protection and restoration between IP/MPLS and Optical networks. Augmented model is suitable in this scenario, where Optical transport and IP/MPLS service networks administrated by different entities and would like to maintain a separation between IP/ MPLS and Optical layers, at the same time, get the benefits of integrated model approach.

Reference [GMPLS-mig] addresses the problem of migration from MPLS to GMPLS networks using the integrated model. This draft addresses the GMPLS deployment considerations using augmented model and illustrates how it can be used in existing IP, MPLS and non-IP/MPLS networks. In this regard, there are three different considerations taken into account while comparing these approaches. They are: Deployment considerations, routing aspects, and failure recovery considerations.

MPLS/GMPLS interworking is also an important aspect that needs to be considered in deploying GMPLS technology in existing IP/MPLS networks. MPLS/GMPLS interworking function refers to methods deployed for mapping between MPLS LSPs and GMPLS LSPs. From a Packet Switching Capable (PSC) network point of view, a router in the PSC network sees

GMPLS LSP (signaled in non-PSC network) as a point-to-point link. How effectively IP/MPLS networks can utilize these TE links (FA-LPSs) created in GMPLS networks is an important aspect that needs to be considered.

Resource affinity and Priority management are operational aspect that must be considered in deploying GMPLS technology. Specifically, GMPLS technology is equipped with features like resource affinity and priority management, protection and restoration. These features have some implications on how IP/MPLS networks can utilize forwarding and/or routing adjacencies established on top of GMPLS networks.
Especially, these management can be a local decision.
In this draft, we highlight these implications/requirements and propose solutions to address them. In this fashion this draft complements [GMPLS-mig] draft, which formalizes the MPLS/GMPLS interworking problem. However, [GMPLS-mig] draft does not address MPLS/GMPLS interworking problems such as a mapping between protected MPLS LSPs and protected GMPLS LSPs.

Feature richness of MPLS and GMPLS technology allows service providers to use a set of options on how GMPLS services can be used by IP/MPLS networks. However, there are some operational considerations and pros and cons associated with the individual options. This draft also highlights some operations considerations associated with use of GMPLS services by IP/MPLS networks.

2. Terminology

SP: Service provider
MPLS LSP setup request: MPLS rsvp path message
MPLS signaling request: MPLS rsvp path message

MPLS TE topology: MPLS TE database (TED)

3. MPLS/GMPLS Deployment,Operational and interworking requirements

In this section, we highlight requirements that service providers have in order to deploy GMPLS technology in existing IP/MPLS networks.

3.1 Software Upgrade Requirement

Generally speaking, it is not practical to upgrade all IP/MPLS routers to GMPLS capable routers in real SP networks due to a number of reasons. Especially, in case of accommodating enterprise customer, we do not allow IP/MPLS routers to upgrade GMPLS capable routers. This means in the real IP/MPLS networks some routers would not be upgraded to support GMPLS and some routers support would it.

3.2 Use of GMPLS network resources in IP/MPLS networks

Most SPs have different networks for various services; their GMPLS deployment plans are to have these service networks use a common GMPLS controlled optical core. We need a way to make effective use of GMPLS network resources (e.g. bandwidth) by the IP/MPLS service networks.

3.3 Interworking of MPLS and GMPLS protection

If MPLS LSPs are protected using MPLS FRR [RFC4090], when an FRR protected packet LSP is signaled, we should be able to select protected FA-LSPs from GMPLS network. In terms of MPLS protection, MPLS path message can be included some flags in FAST REROUTE object and SESSION_ATTRIBUTE object.
In terms of GMPLS protection, there are both signaling aspects [RFC3471] [RFC3473] and routing aspects [GMPLS-routing].
Protected MPLS LSPs should be able to select GMPLS protection type with the option.

3.4 Separation of IP/MPLS domain and GMPLS domain

Most SPs have had different networks for every service, where optical networks and IP/MPLS networks belong to different operation, management, ownership. Most important thing is that SPs want to operate and manage their networks independently, and deploy them without changing existing IP/MPLS network topologies, protocols and affecting scalability.

3.5 Failure recovery

Failure in optical routing domain should not affect services in

IP/MPLS routing domain, and failure can be restored/repaired
in

optical domain without impacting IP/MPLS domain and vice
versa.

4. Augmented model

Augmented Model is introduced in GMPLS Architecture document
[RFC3945]. It is a hybrid model between the full peer and
overlay

models as shown in figure1. Border nodes at the edge of IP/
MPLS

domain and optical domain receive routing information from
the

optical devices (in optical domain) and nodes (in IP/MPLS
domain).

Based on this information, border node keeps the optical and
IP/MPLS

routing domain topology information in separate topology
database. No

routing information from the router region is carried into
the

optical region and vice versa. These are quite useful
aspects from

MPLS/GMPLS deployment, operations as well as interworking requirements.

```
                                             |        Optical Transport          |
                                             |            Network                |
                        +---------+  +---------+     +--------+  +--------+
+--------+   +---------+
                        |        |  |        |     |       |  |       |
|        |   |         |
                        | IP/MPLS+--+ Border +--+--+ OXC1  +--+ OXC2  +-+--+
Border +---+ IP/MPLS |
                        | Service|  | Node   |     |       |  |       |    |
Node   |   | Service |
                        | Network|  |        |     |       |  |       |
|        |   | Network |
                        +-----+--+  +---+----+     +-----+-+  +---+---+
+--------+   +---------+
```

Figure 1. Augmented Model

4.1 Routing in Augmented Model

Augmented model maintains a separation between optical and routing topologies; unlike integrated model approach, where topology information is shared between IP/MPLS and Optical domains. Nonetheless, as the border node has full knowledge of the optical network, it can compute routes for GMPLS LSPs within the optical domain. This allows augmented model to be more efficient in resource utilization than overlay model, such that router and optical domain resource can be optimized. At the same time, it can yield more efficient use of resources, similar to the full peer model. In the full peer model, however, since all the devices in optical and routing domains share the same topology and routing information with same IGP instance, it requires all the devices within peer model to be MPLS/GMPLS aware.

4.2 Failure Recovery in Augmented Model

Both integrated model and augmented model offer a tighter coordination between IP/MPLS and optical layers, which helps to resolve uncorrelated failures. This is unlike overlay model, which offers no coordination between optical and IP/MPLS layers; consequently a single failure in one layer may trigger uncorrelated failures in the other domain, which may complicate the fault handling.

Another important aspect in augmented model is failure transparency, i.e., a failure in an optical network does not affect operations at a router network and vice versa. Specifically, failure in the optical domain does not affect services in routing (IP/MPLS) domain, and failure can be restored/repaired in optical domain without impacting IP/MPLS domain and vice versa. Where as in peer model, since optical

and IP/MPLS domains share the same topology and routing
information,
failure in optical domain is visible to IP/MPLS domain and
vice versa.

4.3 Management in Augmented model

Currently, many SPs have traditionally built their networks,
where
Optical transport and IP/MPLS service networks belong to
different
operation, management, ownership. In augmented model, each
network
administrator can operate and manage his network
independently
because this model maintains a complete separation between
these
networks.

4.4 GMPLS Deployment Considerations

In the integrated model, since all the devices in optical and
routing
domains share the same topology and routing information with
same IGP
instance, it requires all the devices within peer model to be
MPLS/GMPLS aware. Reference [GMPLS-mig] discusses various
aspects of
migration from MPLS to GMPLS technology using integrated
model.

In augmented model, as shown in figure 1, devices within
optical and
its routing domains have no visibility into others topology
and/or
routing information, except the border nodes. This will help
augmented model to accommodate both MPLS based or non-MPLS
based
service networks connected to border nodes, as long as Border
node in
augmented model can support GMPLS control plane.

One of the main advantages of the augmented model in the
context of
GMPLS deployment is that it does not require existing IP/MPLS
networks to be GMPLS aware. Only border nodes need to be

upgraded with the GMPLS functionality. In this fashion, augmented model renders itself for incremental deployment of the optical regions, without requiring reconfiguration of existing areas/ASes, changing operation of IGP and EGP or software upgrade of the existing IP/MPLS service networks.

4.5 Applicability of real/virtual FA-LSP

Real/Virtual FA-LSPs discussed in [GMPLS-mig] are equally applicable to the integrated and augmented models. Specifically, in augmented model, the border node can advertise virtual GMPLS FA-LSPs into IP/MPLS networks and can establish the LSP statically or dynamically on as needed basis. The only additional requirement posed by the augmented model is to have at least one full routing adjacency over the GMPLS LSP, such that TE topology exchange for the individual service network can happen.

4.6 Applicability of FA Utilization

There are several possible schemes for determining how many FAs to provision, when to enable the FAs, and whether to choose FAs of virtual FAs as discussed in [GMPLS-mig] for integrated model. These aspects of FA Utilization are equally applicable to augmented model, with intelligence of FA Utilization implemented at the border node.

4.7 Bundling FA-LSP

In augmented model, it is also possible to bundle GMPLS FA-LSPs at the border nodes. Since IP/MPLS network will only see a bundled link with TE or IGP attributes, operations on the bundled link, e.g., adding a new component link, failure of a component link, etc., are completely transparent to the rest of the network.

5. MPLS/GMPLS Interworking aspects

This section outlines some MPLS/GMPLS interworking aspects.

5.1 Static vs. signaling triggered dynamic FA-LSPs

From signaling perspective, clearly there are two alternatives in which setup for GMPLS tunnel can be triggered: Static (pre-configured) and Dynamic (on-demand based on signaling setup request).

Decision to establish new Static GMPLS LSPs are made either by the operator or automatically (e.g., using features like TE auto-mesh). In either case, Static FA-LSP are established and advertised prior to setup of MPLS LSPs using them in the ERO. In case of static FA-LSP, if MPLS LSP setup request cannot be satisfied by existing

Static FA-
LSPs, it is rejected.

Dynamic FA-LSP is triggered by MPLS LSP setup request for an MPLS LSP.
Please note that dynamic FA-LSPs can be virtual FAs from routing
perspective. In either case, LSP creation from signaling perspective
is triggered by the MPLS RSVP Path message received at a MPLS/GMPLS
border router.

In the case of Static or Virtual FA-LSPs, the FA may be specified in
an ERO encoded as strict ERO. In the case where FA-LSPs are dynamic
and are not advertised as virtual links in the MPLS TE topology, MPLS
signaling request contains a loose ERO, and GMPLS LSP selection is a
local decision at the border router. In the case of Static or Virtual
FA-LSPs, a signaling request may also be encoded as loose ERO.

When the border router receives the signaling setup request and determines that in order for it to expand the loose ERO content, it needs to create GMPLS FA-LSP. Consequently, it signals a GMPLS LSP respecting MPLS/GMPLS signaling interworking aspects discussed in this sections. Once the GMPLS FA-LSP is fully established, the ERO contents for the MPLS signaling setup request are expanded to use the GMPLS LSP and signaling setup for the FA-LSP are carried in-band of the GMPLS LSP. The GMPLS LSP can then also be advertised as an FA-LSP in MPLS TE topology or an IGP adjacency can be brought up on the GMPLS LSP.

5.2 MPLS/GMPLS LSP Resource Affinity Mapping

In terms of signaling aspects, both MPLS and GMPLS LSPs are signaled for specific resource class affinities [RFC3209], [RFC3473]. This can be viewed as "colors". In terms of routing aspects, resource classes are associated with links and advertised by routing protocol in IP/MPLS domain [RFC3630] and GMPLS domain, respectively.

A real or virtual GMPLS FA-LSP or a full Routing Adjacency (RA) over GMPLS LSP can be advertised as TE-links with resource class. In this case, MPLS routers can select a GMPLS FA/RA that has a specific color.

If MPLS signaling request contains a loose ERO, and GMPLS LSP selection is a local decision at the border router. This is possible for the cases when GMPLS LSP is not advertised into IP/MPLS networks. In this case, any mapping combination may be defined manually and dynamically based on some policies at the border router.

5.3 MPLS/GMPLS LSP Priority Mapping

In terms of signaling aspects, both MPLS and GMPLS LSPs are signaled for specific setup and hold priority [RFC3209], [RFC3473], based on the importance of traffic carried over them. For proper operation of the network, it is desirable to create/use GMPLS LSPs of specified setup and hold priority, based on the setup and hold priority of the MPLS LSPs using them. In terms of routing aspects, unreserved bandwidth sub-TLV is used for the amount of bandwidth not yet reserved at each of the eight priority levels in MPLS domain [RFC3630] and max lsp bandwidth at priority 0-7 in interface switching capability descriptor sub-TLV is used for the amount of bandwidth that can be reserved at each of the eight priority levels in GMPLS domain [GMPLS-ospf-routing].

In an MPLS/GMPLS interworking, if a GMPLS LSP is advertised into IP/MPLS networks as an FA/RA, an LSR in the packet network can see it a TE-link with unreserved bandwidth as advertised by the border router. In this case, MPLS routers can select links that meet a bandwidth depending on a priority level.

If MPLS signaling request contains a loose ERO, the GMPLS LSP selection is a local decision at the border router. This is possible in the case where GMPLS LSP is not advertised as an FA into IP/MPLS networks.
In this case, following approaches are possible for mapping setup and hold priority of MPLS LSPs to GMPLS FA-LSPs. These mapping functions can be applied, either manually or dynamically, depending on some policies at the border router.

1) Exact Match: In this case setup and hold priority of the GMPLS FA-LSP is same as setup and hold priority of MPLS LSP using it. In other words, GMPLS LSP Priority set = MPLS LSP Priority set.

2) Better Priority: In this case GMPLS FA-LSP can be of setup and hold priority equal better than the MPLS LSP using it. In other words, GMPLS LSP Priority set <= MPLS LSP Priority set.

3) Dynamic Priority for GMPLS LSP: In this case priority of GMPLS LSP is dynamically changed based on priority of the MPLS LSPs using it. In other words, GMPLS LSP Priority set = min (MPLS LSP Priority set).

4) Any to Any Mapping Matrix: Based on some policies, it is possible to have an any-to-any mapping for MPLS/GMPLS priority mapping at the MPLS/GMPLS border router.

5) No Priority Management in GMPLS core: In this simple minded approach all GMPLS LSPs can be establish with setup and hold priority of "0", i.e., the GMPLS LSPs are already set as better match. In this case, priority management is handled purely at MPLS layer, with GMPLS network providing L1 connectivity without priority management.

5.4 Signaling Protected MPLS LSPs

When MPLS LSPs are protected using MPLS-FRR mechanism [RFC4090] and it may be desired to signal MPLS LSP such that it uses protected GMPLS tunnel FA-LSPs. In this section we discuss MPLS/GMPLS interworking aspect for protected MPLS LSPs.

In the case of loose ERO, where selection of GMPLS FA-LSP is a left for the border nodes and "One-to-One backup desired" or "facility backup desired" flag of the FAST REROUTE object, "Local protection desired" and/or "bandwidth protection desired" and/or "node protection desired" flag of the SESSION_ATTRIBUTE object is set, the border router SHOULD try to map the signaling setup request to a GMPLS LSP which is protected within GMPLS domain. However, in the case of strict ERO, the selection of GMPLS FA-LSP is based on the contents of the ERO and these flags are ignored.

When a GMPLS LSP is advertised as FA or RA in MPLS network, Protection Capabilities attribute of the Link Protection Type is a sub-TLV of the Link TLV can be used for selecting GMPLS LSP of desired protection capability.

6. Operational Considerations

In this section, we discuss some operational considerations and pros and cons associated with the individual options listed in Section 5.3.

6.1 Applicability of the Priority Management Options

In section 5.3, various options from exact match to no priority management in GMPLS network are discussed. This section provides an applicability of these options.

The benefit of Priority Management in GMPLS Core comes at the cost of bandwidth fragmentation. E.g., in simplest approach of exact match, we need at least as many GMPLS LSPs, as there are priority combination in the network, while the other extreme of no priority management in GMPLS network does allow full aggregation of MPLS traffic on GMPLS FAs, i.e. avoids bandwidth fragmentation. If IGP adjacency is to be established over the GMPLS LSPs, having more GMPLS LSP leads to more links in the IGP/IP topology. The same is true of MPLS TE topology with the exception that FA-LSPs can be bundled to avoid flooding of multiple TE links.

With priority management within GMPLS network, there is a danger of creating oscillations in the IP/MPLS network using GMPLS. This is because when a new FA-LSP is established based on a local routing decision made at the border router; we can have undesirable preemption affecting MPLS LSPs carried over the GMPLS LSP that is being preempted. This can have cascading affect leading to oscillations on the operation of MPLS traffic.

6.2 Applicability of the Signaling Triggered Dynamic FA-LSP

In this section, we discussed applicability of static vs. dynamic FA-LSPs. It is important to realize that we can have FA-LSPs that are created dynamically based on triggers like configuration, link utilization level, etc. However, in the context of this document, such FA-LSPs are considered as static FAs. In this document, the term dynamic FA-LSPs are used for FA-LSPs that are triggered by RSVP Path message for MPLS LSP.

Signaling triggered dynamic FA-LSPs are addressing a problem space where traffic pattern cannot be predicted or objective is to optimize operations of the network based on actually signaled request rather than predicted use of the network resource (i.e., off-line traffic engineering).

The problem with the use of signaling triggered dynamic FA-LSPs is that we loose ability to better aggregate the traffic request at the border routers. This leads to potential cases of bandwidth fragmentation inside GMPLS core, which has disadvantages discussed in Section 6.1. Furthermore, signaling triggered dynamic FA-LSPs coupled with preemption can lead to oscillations in the operation of the network. This is because when a new FA-LSP is dynamically established based on a local routing decision made at the border router; we can have undesirable preemption affecting MPLS LSPs carried over the GMPLS LSP that is being preempted. This can have cascading affect leading to oscillations on the operation of MPLS traffic.

7. Backward Compatibility Note

The procedure presented in this document is backward compatible with [RFC3630], [RFC3784], [RFC3209] and [RFC3473].

8. Security Considerations

This document does not introduce new security issues.

9. Intellectual Property Considerations

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information

10.Acknowledgement

The author would like to express the thanks to Arthi Ayyangar for helpful comments and feedback.

11.Reference

11.1 Normative Reference

[RFC3209] "Extensions to RSVP for LSP Tunnels", D. Awduche, et al, RFC 3209, December 2001.

[RFC3630] Katz, D., Kompella, K. and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, September 2003.

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

[GMPLS-mig] "IP/MPLS - GMPLS interworking in support of IP/

MPLS to
GMPLS migration", draft-oki-ccamp-gmpls-ip-interworking-05.txt, D.
Brungard, et al, February 2005.

[RFC3945] "Generalized Multi-Protocol Label Switching (GMPLS)
Architecture",RFC 3945, E. Mannie,October 2004.

11.2 Informative Reference

[GMPLS-routing] "Routing Extensions in Support of Generalized Multi-
Protocol Label Switching", draft-ietf-ccamp-gmpls-routing-09.txt
(work in progress), October 2003.

[GMPLS-ospf-routing] "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching", draft-ietf-ccamp-ospf-gmpls-extensions-12.txt (work in progress), October 2003.

[RFC2205] "Resource Reservation Protocol (RSVP) - Version 1, Functional Specification", RFC 2205, Braden, et al, September 1997.

[RFC3471] "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, L. Berger, et al, January 2003.

[RFC3473] "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, L. Berger, et al, January 2003.

[RFC4090] "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, Pan, et al, May 2005.

12. Author's Addresses

Kenji Kumaki
KDDI Corporation
Garden Air Tower
Iidabashi, Chiyoda-ku,
Tokyo 102-8460, JAPAN
E-mail : ke-kumaki@kddi.com

Zafar Ali
Cisco systems, Inc.,
2000 Innovation Drive   Phone: 613 254 3498
Kanata, Ontario   Email: zali@cisco.com
Canada K2K 3E8

Tomohiro Otani
KDDI R&D Laboratories, Inc.
2-1-15 Ohara Kamifukuoka   Phone: +81-49-278-7357
Saitama, 356-8502. Japan   Email: otani@kddilabs.jp

George Swallow
Cisco Systems, Inc.
1414 Massachusetts Ave,

Boxborough, MA 01719
Phone: +1 978 936 1398
Email: swallow@cisco.com

Mallik Tatipamula
Cisco systems, Inc.,
170 W. Tasman Drive
San Jose, CA 95134 Phone: 408 525 4568
USA. Email: mallikt@cisco.com

13.Full Copyright Statement