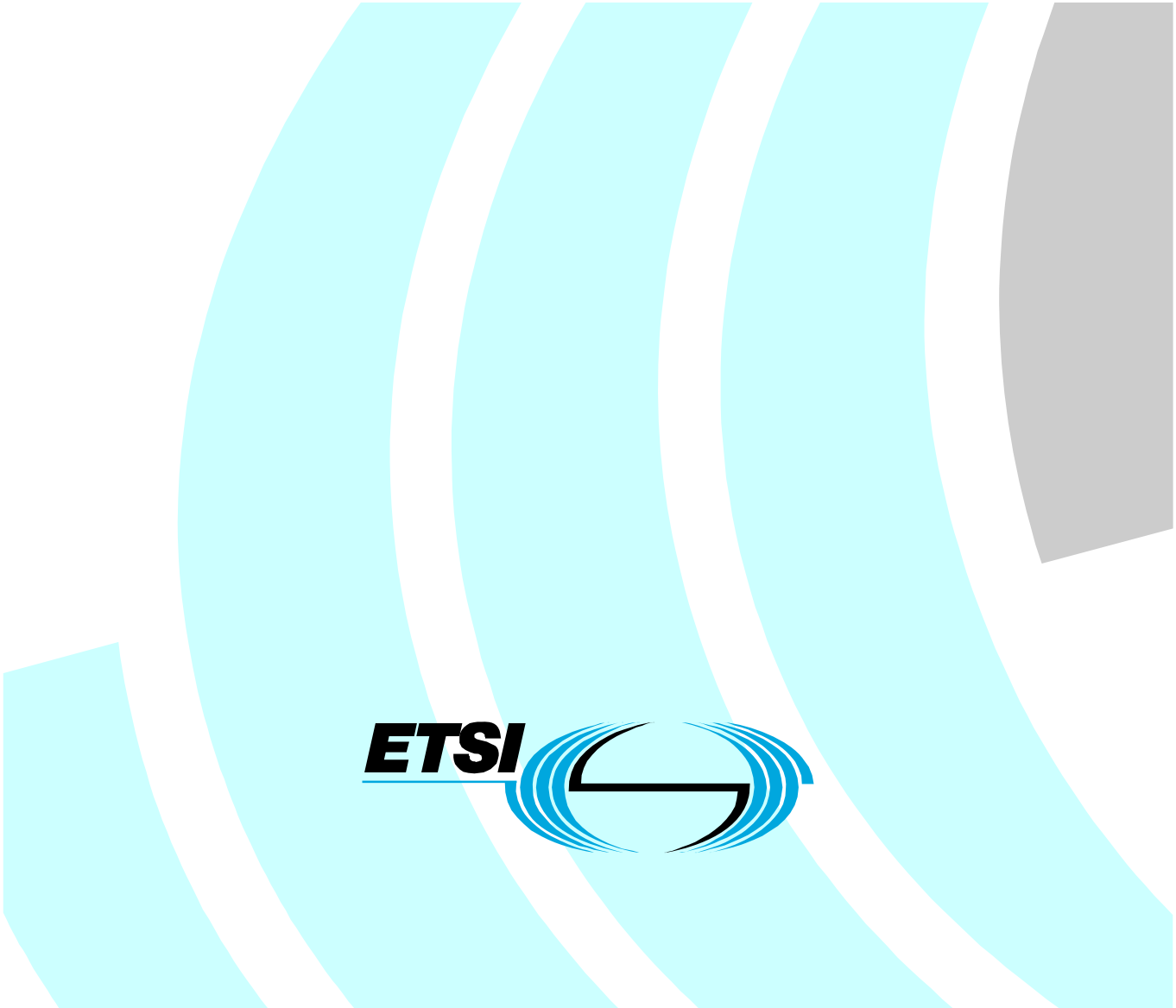
# ETSI TS 102 856-1 V1.1.1 (2011-07)

*Technical Specification*

**Satellite Earth Stations and Systems (SES);**
**Broadband Satellite Multimedia (BSM);**
**Multi-Protocol Label Switching (MPLS)**
**interworking over satellite;**
**Part 1: MPLS-based Functional Architecture**



Reference
DTS/SES-00306

Keywords
architecture, broadband, IMS, internet,
interworking, IP, MPLS, multimedia, satellite

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

# Contents

Intellectual Property Rights ..... 5
Foreword ..... 5
Introduction ..... 5
1 Scope ..... 6
2 References ..... 6
2.1 Normative references ..... 6
2.2 Informative references ..... 7
3 Definitions and abbreviations ..... 8
3.1 Definitions ..... 8
3.2 Abbreviations ..... 9
4 General ..... 10
4.1 BSM ..... 10
4.1.1 BSM Functional Architecture ..... 10
4.1.2 BSM QoS Architecture ..... 10
4.1.3 BSM Traffic Classes ..... 10
4.2 MPLS ..... 11
4.2.1 MPLS Objectives ..... 11
4.2.2 MPLS Signalling ..... 11
4.2.3 MPLS QoS Issues ..... 11
4.2.4 MPLS Traffic Engineering ..... 12
4.2.5 MPLS Encapsulation ..... 12
4.2.6 MPLS VPNs ..... 13
4.3 Functional Requirements ..... 13
5 MPLS/BSM Functional Architecture ..... 13
5.1 Scenario A: Full Interworking of MPLS ..... 14
5.1.1 Network Architecture ..... 14
5.1.2 Protocol Stack ..... 17
5.1.3 QoS Provisioning ..... 19
5.1.3.1 BSM Traffic Classes ..... 19
5.1.3.2 DiffServ ..... 20
5.1.3.3 IntServ ..... 21
5.1.4 Traffic Engineering ..... 21
5.1.5 Resiliency ..... 22
5.2 Scenario B: Interworking Using IP Tunnels ..... 23
5.2.1 Network Architecture ..... 24
5.2.2 Protocol Stack ..... 25
5.2.3 QoS Provisioning ..... 25
5.2.4 Traffic Engineering ..... 26
5.2.5 Resiliency ..... 26
6 MPLS/BSM-Specific Functional Elements ..... 26
6.1 LSR/ST ..... 26
6.2 LSR/Hub ..... 27
6.3 LSR/GW ..... 27
6.4 LSR/OBP-Sat ..... 27
**Annex A (informative): Use Cases ..... 28**
A.1 MPLS Network using Scenario A1 ..... 28
A.2 MPLS Network using Scenario B1 ..... 29
A.3 MPLS Network using Scenario A2 ..... 29
A.4 MPLS VPN using Scenario A1 ..... 30

**Annex B (informative): MPLS Transport Profile ..... 32**

**Annex C (informative): Bibliography ..... 33**

History ..... 34

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

The present document is part 1 of a multi-part deliverable covering the issues related to the use of MPLS (Multi-Protocol Label Switching) in "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM)", as identified below:

**Part 1: "MPLS-based Functional Architecture";**

Part 2: "Negotiation and management of MPLS labels and MPLS signalling with attached networks".

# Introduction

Multi-protocol Label Switching (MPLS) is employed today as a solution for delivering quality of service (QoS) on IP-based terrestrial networks by providing QoS-based routing of IP traffic, among other advanced capabilities. Compatibility between the BSM and MPLS networks should be an essential feature, for example to provide extensions and interconnectivity to terrestrial MPLS networks and/or a satellite back-up for terrestrial MPLS networks.

The ability to support MPLS efficiently and in a standardised manner over a BSM network forms the core rationale for the present document. This work on MPLS and QoS is independent of, but complementary to, the existing BSM specifications on QoS, in particular TS 102 463 [5] and TS 102 464 [6].

# 1 Scope

The present technical specifications extend and complement the existing BSM QoS functional architecture to enable transport of MPLS signalling and data flows over a BSM network in a way such that MPLS networks connected by different STs can communicate as if they were connected by standard terrestrial LSRs (label switching routers).

The present document forms part 1 of this multi-part deliverable. It defines the main architectural concepts, including the network architecture and protocol stacks, and outlines the key QoS, traffic engineering and resiliency provisions. Several architecture variants are defined and their main characteristics are analysed, also taking into account three different BSM network types.

An Annex sketches a set of use cases that illustrate different application and configuration scenarios of the present specifications.

In a separate document, TS 102 856-2 [11], the detailed procedures in BSM network entities and related signalling issues are addressed. A particular focus is placed on the fully integrated MPLS/BSM architecture as defined in the present document.

The setup of multicast MPLS paths is considered out of scope of this multi-part deliverable.

# 2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

## 2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 292: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks".

[2] ETSI TS 102 295: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; BSM Traffic Classes".

[3] ETSI TS 102 357 (V1.1.1): "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Common Air interface specification; Satellite Independent Service Access Point SI-SAP".

[4] ETSI TS 102 462: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); QoS Functional Architecture".

[5] ETSI TS 102 463: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with IntServ QoS".

[6] ETSI TS 102 464: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with DiffServ Qos".

[7] ETSI TS 102 672: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Management Functional Architecture".

[8] ETSI TS 102 673: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Performance Parameters".

[9] ETSI TS 102 675-1: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Part 1: Performance Management at the SI-SAP".

[10] ETSI TS 102 675-2: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Part 2: Performance Management Information Base".

[11] ETSI TS 102 856-2: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Multi-Protocol Label Switching (MPLS) interworking over satellite; Part 2: Negotiation and management of MPLS labels and MPLS signalling with attached networks".

## 2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Services and architectures".

[i.2] IETF RFC 1633: "Integrated Services in the Internet Architecture: an Overview".

[i.3] IETF RFC 2205: "Resource Reservation Protocol (RSVP) - Version 1 Functional Specification".

[i.4] IETF RFC 2210: "The Use of RSVP with IETF Integrated Services".

[i.5] IETF RFC 2702: "Requirements for Traffic Engineering over MPLS".

[i.6] IETF RFC 2983: "DiffServ and Tunnels".

[i.7] IETF RFC 3107: "Carrying Label Information in BGP-4".

[i.8] IETF RFC 3031: "Multiprotocol Label Switching Architecture".

[i.9] IETF RFC 3209: "RSVP-TE Extensions to RSVP for LSP Tunnels".

[i.10] IETF RFC 3270: "MPLS Support of Differentiated Services".

[i.11] IETF RFC 3564: "Requirements for Support of Differentiated Services - aware MPLS Traffic Engineering".

[i.12] IETF RFC 3630: "Traffic Engineering Extensions to OSPF Version 2".

[i.13] IETF RFC 4023: "Encapsulating MPLS in IP or GRE".

[i.14] IETF RFC 4090: "Fast Reroute Extensions to RSVP-TE for LSP Tunnels".

[i.15] IETF RFC 4124: "Protocol Extensions for Support of DiffServ-aware MPLS Traffic Engineering".

[i.16] IETF RFC 4271: "A Border Gateway Protocol 4 (BGP-4)".

[i.17] IETF RFC 4364: "BGP MPLS IP VPNs".

[i.18] IETF RFC 4577: "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP VPNs".

[i.19] IETF RFC 5036: "LDP Specification".

[i.20] IETF RFC 5586: "MPLS Generic Associated Channel".

[i.21] IETF RFC 5654 - Requirements of an MPLS Transport Profile".

[i.22] IETF RFC 5860: "Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks".

[i.23] IETF RFC 5921: "A Framework for MPLS in Transport Networks".

[i.24] IETF RFC 5950: "Network Management Framework for MPLS-based Transport Networks".

[i.25] IETF RFC 5960: "MPLS Transport Profile Data Plane Architecture".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**architecture:** abstract representation of a communications system

NOTE: Three complementary types of architecture are defined:

- Functional Architecture: the discrete functional elements of the system and the associated logical interfaces.
- Network Architecture: the discrete physical (network) elements of the system and the associated physical interfaces.
- Protocol Architecture: the protocol stacks involved in the operation of the system and the associated peering relationships.

**BSM network:** BSM subnetwork together with the BSM interworking and adaptation functions that are required to provide IP interfaces (i.e. layer 3 and below) to attached networks

**BSM subnetwork:** all the BSM network elements below the Satellite Independent Service Access Point (SI-SAP)

**control plane:** plane that has a layered structure and performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections

**label switched path:** path through one or more LSRs at one level of the hierarchy followed by a packets in a particular FEC

NOTE: This definition is taken from RFC 3031 [i.8].

**label switching router**: MPLS node which is capable of forwarding native L3 packets

NOTE: This definition is taken from RFC 3031 [i.8].

**MPLS label:** label which is carried in a packet header, and which represents the packet's FEC

NOTE: This definition is taken from RFC 3031 [i.8].

**MPLS node:** node which is running MPLS

NOTE 1: An MPLS node will be aware of MPLS control protocols, will operate one or more L3 routing protocols, and will be capable of forwarding packets based on labels. An MPLS node may optionally be also capable of forwarding native L3 packets.

NOTE 2: This definition is taken from RFC 3031 [i.8].

**multi-protocol label switching**: IETF working group and the effort associated with the working group

NOTE: This definition is taken from RFC 3031 [i.8].

**user plane:** plane that has a layered structure and provides user information transfer, along with associated controls (e.g. flow control, recovery from errors, etc.)

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| BA | Behaviour Aggregate |
| BGP | Border Gateway Protocol |
| BSM | Broadband Satellite Multimedia |
| CE | Customer Edge |
| DiffServ | Differentiated Services |
| DS | Differentiated Services |
| DSCP | DiffServ Code Point |
| E-LSP | Explicitly TC-encoded PHB Scheduling Class |
| FEC | Forwarding Equivalence Class |
| GRE | Generic Routing Encapsulation |
| GW | Gateway |
| HTTP | Hypertext Transfer Protocol |
| IETF | Internet Engineering Task Force |
| IntServ | Integrated Services |
| IP | Internet Protocol |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| L1 | Layer 1 |
| L2 | Layer 2 |
| L3 | Layer 3 |
| LAN | Local Area Network |
| LER | Label Edge Router |
| L-LSP | Label-Only-Inferred PHB Scheduling Class |
| LSA | Link State Advertisement |
| LSP | Label Switched Path |
| LSR | Label Switching Router |
| MPLS | Multi-Protocol Label Switching |
| NCC | Network Control Centre |
| NMC | Network Management Centre |
| NMS | Network Management System |
| OAM | Operations, Administration, and Maintenance |
| OBP | On-Board Processing |
| OPEX | Operating Expense |
| OSPF | Open Shortest Path First |
| PE | Provider Edge |
| PHB | Per-Hop Behaviour |
| PSC | PHB Scheduling Class |
| QID | Queue Identifier |
| QoS | Quality of Service |
| RSM | Regenerative Satellite Mesh |
| RSVP | Resource Reservation Protocol |
| SD | Satellite Dependent |
| SDU | Service Data Unit |
| SI | Satellite Independent |
| SI-SAP | Satellite Independent Service Access Point |
| ST | Satellite Terminal |
| TC | Traffic Class |
| TE | Traffic Engineering |
| TP | Transport Profile |
| TSM | Transparent Satellite Mesh |
| TSS | Transparent Satellite Star |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |

# 4 General

This clause identifies and briefly sketches the core technologies that need to be brought together to define an integrated MPLS/BSM architecture.

## 4.1 BSM

ETSI's Working Group SES BSM has made substantial progress over the past decade in defining an IP-based BSM network. Among the technical specifications and reports generated by the WG, TS 102 292 [1] (Functional Architecture for IP Interworking with BSM Networks) and TS 102 462 [4] (QoS Functional Architecture) are especially relevant for the present purposes.

### 4.1.1 BSM Functional Architecture

TS 102 292 [1] introduces a satellite-independent service access point, the SI-SAP interface. This interface provides the higher-layer BSM functions inside the satellite terminal with a service access point for the lower layer (satellite-specific) functions. It allows the BSM protocols developed in the satellite-independent layer (above SI-SAP) to perform over any BSM family. Moreover, the SI-SAP enables the use of standard Internet protocols directly over the BSM or with minimal adaptation to BSM physical characteristics. Any BSM functions that are required in the satellite-independent layer should be introduced without impacting Internet protocols, ideally via proxies or dedicated (protocol) managers. A detailed specification of the SI-SAP interface is provided in TS 102 357 [3].

### 4.1.2 BSM QoS Architecture

Central to the QoS capability of a BSM network is the concept of QIDs (Queue Identifier). These represent abstract queues that are defined at the SI-SAP for the purpose of transferring user data via the SI-SAP. The satellite dependent layers are responsible for assigning satellite capacity to these abstract queues according to the specified queue properties (e.g. QoS and forwarding behaviour). QIDs may be assigned statically (e.g. by management configuration) or dynamically using specific resource reservation and signalling procedures. A QID is assigned at the time when the associated queue is opened. An open queue is uniquely identified by the associated QID; in particular, the QID is used to label all subsequent data transfers via that queue. It is important to note that QIDs have only local significance at the respective interface; QID values are not communicated to entities outside the ST.

The key issue with respect to QoS provision in BSM networks concerns the mapping between QIDs and any QoS parameters or application-specific parameters that may be present at higher layers (i.e. above SI-SAP). TS 102 462 [4] does not specify such a mapping. Rather, it establishes the basic concepts to manage and control QID-related resources and their mappings to resource requirements from higher layers. For these tasks, a client-server model is defined whereby an ST QID resource manager is the client function to a centralised BSM QID manager (server) that has the overall view of all BSM resources and their assignment status. QID resources can be allocated in a variety of ways, including by static pre-configuration (via the management plane) or dynamically by control plane signalling and subsequent requests across SI-SAP.

### 4.1.3 BSM Traffic Classes

Service providers are generally not interested in the specific QoS mechanisms or in numerically quantifying QoS attributes, like maximum allowed delay or jitter, per application. Rather, it must simply be ensured that traffic entering the BSM is characterised, sorted and processed according to its characteristic. For this purpose, TS 102 295 [2] (BSM Traffic Classes) defines eight distinct traffic classes that capture and categorise the full spectrum of observed traffic characteristics. By mapping each application to a suitable BSM Traffic Class it can thus be ensured that the corresponding traffic receives the appropriate treatment by the BSM.

## 4.2 MPLS

### 4.2.1 MPLS Objectives

MPLS is an IETF mechanism (RFC 3031 [i.8]) that enables packet switched networks to operate more efficiently and under greater control by the network operator. When MPLS was first introduced in the mid-1990's, the primary goal was to provide new capabilities in IP routers to optimise overall traffic throughput and to categorise, separate and process traffic for QoS differentiation. MPLS operates between the OSI layers 2 and 3, and introduces the concept of a (unidirectional) Label Switched Path (LSP). Packet forwarding in MPLS enabled IP routers is achieved by means of an MPLS label that is attached to each packet. The MPLS label is part of an MPLS header which is introduced between the Layer 2 and 3 headers. It is important to note that an LSP is not characterized by a globally unique MPLS label; instead, labels have only local significance at a specific interface, and MPLS routers are responsible for assigning the correct label to each packet for the next hop.

Since its inception, MPLS has evolved significantly by adding new capabilities and integrating other IETF technologies. Over the years, the focus has shifted from traffic engineering to efficient and manageable service delivery that enables lower OPEX. MPLS is now probably the fastest growing technology for IP networking, both in terms of standardisation as well as actual deployment in terrestrial networks.

For the purposes of the present document, the question arises as to which elements of MPLS are potentially beneficial for BSM networks. Considering that well over 100 RFCs and active Internet Drafts currently exist, a careful reflection on the scope of an integrated MPLS/BSM network is required. This must start by identifying and characterising the major MPLS paradigms, as discussed in the following.

### 4.2.2 MPLS Signalling

Historically, MPLS was conceived as a mechanism to segregate IP traffic into distinct LSPs for QoS and traffic engineering purposes. Different LSPs would carry different types of traffic which could receive dedicated handling and forwarding by MPLS routers according to their priority. These LSPs can be established in different ways, including by dynamic signalling or by management action. All packets that are placed on a given LSP are said to belong to the same Forwarding Equivalence Class (FEC), and they receive the same treatment by the network.

Several techniques exist to generate, store and distribute MPLS labels, depending on the field of application and desired capability. The Label Distribution Protocol (LDP, see RFC 5036 [i.19]) is a simple protocol by which LSRs inform each other of the label bindings they have made to forward packets along LSPs. Here LSPs are instantiated automatically according to the underlying routing information available in IP routers. To allow for a more flexible LSP placement, RFC 3209 [i.9] (RSVP-TE: Extensions to RSVP for LSP Tunnels) extends RSVP (RFC 2205 [i.3]) by introducing traffic engineering capabilities. In that context, LSPs are referred to as "LSP tunnels." Finally, for MPLS applications involving VPNs, RFC 3107 [i.7] (Carrying Label Information in BGP-4) specifies a way in which MPLS labels can be distributed using the standard routing protocol BGP-4 (RFC 4271 [i.16]).

### 4.2.3 MPLS QoS Issues

As regards the support of QoS in MPLS networks, an obvious approach is to simply send QoS-sensitive traffic over dedicated, traffic-engineered LSP tunnels whose participating LSRs exhibit the desired pre-arranged forwarding behaviour. The issue here is how to manage such a QoS provision on a large scale. One approach would be to adopt the Internet Integrated Services (IntServ) framework and apply RFC 2210 [i.4] (The Use of RSVP with IETF Integrated Services). However, due to the well-known inherent drawbacks of IntServ, that approach has not gained much support.

Instead, the IETF has devoted a considerable amount of effort to integrating and adapting the DiffServ approach for use in MPLS. RFC 3270 [i.10] (MPLS Support of DiffServ) defines a flexible solution for supporting DiffServ over MPLS networks, thus allowing the MPLS network administrator to select how DiffServ Behaviour Aggregates (BAs) are mapped onto LSPs. A BA denotes the set of IP packets that require the same DiffServ behaviour, and therefore have the same DSCP (DiffServ Code Point) marking in the IP header's 6-bit DS Field (which is part of the 8-bit former IPv4 ToS field or the former IPv6 Traffic Class field). At each LSR, the DSCP is used to select the Per Hop Behaviour (PHB) that determines the scheduling treatment and, in some cases, drop probability for each packet. Examples of common PHBs are BE (Best Effort), CS (Class Selector), AF (Assured Forwarding), and EF (Expedited Forwarding), as listed e.g. in Annex C of TS 102 464 [6] together with their associated DSCPs. Obviously, the total space available for DSCPs (6 bits) greatly exceeds the number of useful PHBs, leaving considerable room for locally configurable (proprietary) mappings.

Now, RFC 3270 [i.10] defines two types of approaches to employing fields of the MPLS shim header for PHB encoding:

- E-LSP: In the E-LSP (Explicitly TC-encoded PHB Scheduling Class) LSP approach, the MPLS shim header's 3-bit TC field is used to indicate the packet's PHB, covering both information about the packet's scheduling treatment and its drop precedence. Note that here the MPLS label determines only the forwarding behaviour, and does not convey any QoS provisions. Also note that a PHB Scheduling Class (PSC) denotes a set of PHBs for which packets must not be reordered.

- L-LSP: In the L-LSP (Label-Only-Inferred PHB Scheduling Class) LSP approach, an MPLS label is assigned for each PHB scheduling class; the packet's drop precedence is conveyed in the MPLS TC field. In this approach, the LSR thus determines both its forwarding and its scheduling behaviour from the MPLS label.

The E-LSP and the L-LSP approaches may co-exist in any given MPLS network.

### 4.2.4 MPLS Traffic Engineering

Traffic Engineering is concerned with performance optimisation of operational networks. RFC 2702 [i.5] (Requirements for Traffic Engineering over MPLS) identifies the functional capabilities required to implement policies that facilitate efficient and reliable network operations in an MPLS network. An important concept introduced in RFC 2702 [i.5] is the MPLS traffic trunk. This is a unidirectional routable object that can be thought of as an aggregation of traffic flows of the same class which are placed inside an LSP. An LSP can contain more than one traffic trunk, and traffic trunks can be re-routed over another LSP. Furthermore, two LSPs between the same source and destination may be load shared to carry a single traffic trunk. An LSP (or set of LSPs) that carries a traffic trunk is sometimes referred to as a traffic engineered tunnel, or TE tunnel.

The routing of traffic trunks can occur via (RSVP-TE) signalling or via administrator action. In the latter case, the resulting path is called an administratively specified explicit path. An administratively specified path can be completely specified or partially specified.

Highlighting the interdependence between QoS and Traffic Engineering, RFC 3564 [i.11] (Requirements for Support of DiffServ-aware MPLS Traffic Engineering) specifies the requirements for the support of Traffic Engineering in DiffServ-aware MPLS networks. RFC 4124 [i.15] (Protocol Extensions for Support of DiffServ-aware MPLS Traffic Engineering) addresses these requirements and defines the required protocol extensions. This includes extensions to routing protocols and also to RSVP-TE signalling beyond those already specified in RFC 3209 [i.9] (RSVP-TE: Extensions to RSVP for LSP Tunnels). Further extensions to RSVP-TE are specified in RFC 4090 [i.14] (Fast Reroute Extensions to RSVP-TE for LSP Tunnels) to establish backup LSP tunnels for local repair of LSP tunnels.

### 4.2.5 MPLS Encapsulation

The core operation in MPLS networks is the forwarding of LSPs, and this operation is performed by MPLS enabled IP routers. Since non-MPLS capable IP routers cannot interpret the MPLS shim header, such routers cannot forward LSPs. However, it is possible to tunnel LSPs across a non-MPLS enabled IP network. This is done by means of MPLS encapsulation, as defined in RFC 4023 [i.13] (Encapsulating MPLS in IP or GRE).

RFC 4023 [i.13] specifies two IP-based encapsulations:

a) MPLS-in-IP; and

b) MPLS-in-GRE.

In both cases, the outer, encapsulating protocol is IP. In encapsulation method (a), the MPLS packet is encapsulated with an (outer) IP header, so that the resulting IP datagram can be treated by IP routers in the usual way. In encapsulation method (b), the MPLS packet is first encapsulated with a GRE header, and the resulting packet is then encapsulated with an (outer) IP header.

### 4.2.6 MPLS VPNs

The problem of how to deliver VPN solutions over IP networks has long been debated by the IP community, including the MPLS Working Group. With RFC 4364 [i.17] (BGP MPLS IP VPNs), a stable MPLS-based solution is now available which in fact extends MPLS into a new application area. RFC 4364 i.17 describes a method by which a service provider uses an IP backbone to provide MPLS IP VPNs for its customers, i.e. the VPN providers. This method uses a peer model, in which the customer's edge (CE) routers send their routes to the service provider's edge (PE) routers. The provider network uses MPLS to tunnel customer packets across the IP backbone, and the CE-PE interface is typically running BGP (RFC 4271 [i.16]). Later, in RFC 4577 [i.18] (OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP VPNs), OSPF was allowed instead of BGP to facilitate that interconnection for some customers.

## 4.3 Functional Requirements

When considering the integration of MPLS capabilities with BSM networks, the following high-level functional requirements are identified:

1) The integrated MPLS/BSM functional architecture should support all of the features of MPLS.

2) There shall be no requirement for modification of MPLS protocols (MPLS control and data transport), i.e. MPLS should be interworked with no adaptation.

3) Any modifications to the BSM architecture should be as small as possible.

4) The documents should define a standard method of QoS mapping in order that a BSM network can provide an appropriate level of QoS differentiation for MPLS transport.

# 5 MPLS/BSM Functional Architecture

This clause defines scenarios for integrated MPLS/BSM functional architectures. The common theme in all these scenarios is that a terrestrial MPLS-based IP network is interconnected with a BSM network, thus enabling MPLS-based traffic to enter the BSM network. The different scenarios introduced below are characterised by different degrees of interworking and integration of MPLS and BSM entities, ranging from full interworking through no interworking. Depending on the degree of interworking, the character of the MPLS traffic (e.g. in terms of QoS and traffic engineering treatment) can be preserved to a larger or smaller extent. The three BSM network types TSS (Transparent Satellite Star), TSM (Transparent Satellite Mesh), and RSM (Regenerative Satellite Mesh) (see TR 101 984 [i.1]) are considered.

The following MPLS/BSM scenarios are identified:

- **Scenario A** - Full interworking
  - Scenario A1: all STs and the Hub contain an integrated LSR functionality; three variants are considered, which differ in the type of underlying BSM network: (i) TSS, (ii) TSM, and (iii) RSM.
  - Scenario A2: all STs, the Hub, and the (OBP) satellite contain an integrated LSR functionality; the BSM network is of type RSM. (Scenario A2 will not be studied in detail.)
- **Scenario B** - Interworking using IP tunnels
  - Scenario B1: using IP as the encapsulation protocol, MPLS packets are tunnelled across the unmodified BSM network. (This applies to all types of BSM networks.)
- **Scenario C** - MPLS delivered by Layer-2 ST

  Here, MPLS is transported via a satellite Layer 2 modem, i.e. the ST only contains a L2 bridge. This Scenario has thus limited relevance to the MPLS operation. In particular, the assumed model of a Layer-2 modem (L2 transport of complete Ethernet frames) means that the MPLS header information is opaque at this ST lower layer. It is also of no relevance for the BSM SI-SAP model because the SI-SAP U-plane specification defines a Layer-3 modem (transport of L3 packets). Scenario C will thus not be analysed further in the present document.

In addition to the basic functional and protocol architectures, this clause also specifies the basic concepts related to QoS provisioning, traffic engineering and resiliency for each scenario. The capabilities of the integrated MPLS/BSM functional elements for the different scenarios will be described in clause 6. Further details of scenario A (which is considered the most complete and relevant case for BSM networks) are specified in TS 102 856-2 [11].

In all architecture diagrams in this clause, the following notation is used. Large light grey rectangles placed in the background indicate the BSM network. White boxes denote BSM network entities. Any small (blue, shaded) boxes attached to these entities indicate MPLS specific functionality integrated into that entity. Any blue lines emanating from these combined entities indicate *logical* MPLS-enabled connectivity to the respective combined entity.

## 5.1 Scenario A: Full Interworking of MPLS

This clause introduces an integrated MPLS/BSM scenario whereby *full* interworking between the MPLS and BSM networks is realised (Scenario A). From an MPLS network point of view, this means that the functional characteristics of LSPs entering the BSM network do not differ from LSPs that run across terrestrial links. From a BSM network point of view, full interworking implies that the BSM network supports the set of MPLS capabilities and features, including the MPLS QoS, traffic engineering and resiliency capabilities as defined by the IETF.

Full interworking is achieved by adding the LSR functionality to BSM entities in such a way that (i) the combined entity acts as an ordinary MPLS-enabled IP router inside the MPLS network, and (ii) the BSM-internal procedures are performed as specified in the BSM standards, with the constraint that these procedures shall not interfere with MPLS procedures. This entails substantial changes to the ST (or the Hub) as currently defined. These changes are outlined in clause 6 and detailed in TS 102 856-2 [11]. In terms of the network architecture, Scenario A is thus characterised by adding the full set of MPLS functionalities to all BSM network entities that shall support LSPs. Scenario variants exist which differ only in the type of the underlying BSM network, as discussed in the following.

The following clauses specify, respectively, the network architecture, the protocol stack, and the QoS provisioning, traffic engineering and resiliency mechanisms for the Scenario A variants.

### 5.1.1 Network Architecture

Figures 5.1 to 5.3 introduce Scenario A1, which is defined in terms of fully MPLS capable ST and Hub (respectively GW) entities.

Figure 5.1 shows the architecture of Scenario A1 for the case when the BSM network is of type TSS. In this case, LSPs inside the BSM network directly interconnect the combined LSR/ST only with the LSR/Hub functional entity; LSR/ST to LSR/ST communication is only possible via a double hop through the LSR/Hub, which acts as an ordinary LSR at the MPLS (2.5) layer. In terms of interconnection with the outside MPLS network, the combined LSR/ST and LSR/Hub functional entities act as ordinary LSRs with respect to that network. Note that here the LSR/Hub is capable of acting both as a BSM-network internal (MPLS-enabled) Hub, and as an (MPLS-enabled) gateway to the terrestrial MPLS network.

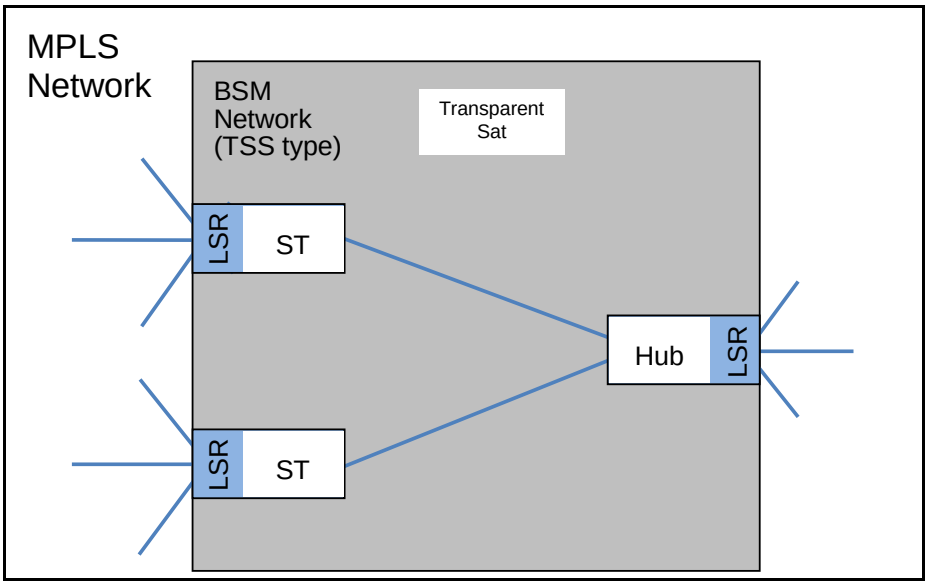



**Figure 5.1: Scenario A1 with a TSS type of BSM network**

Figure 5.2 shows the architecture of Scenario A1 for the case when the BSM network is of type TSM. As indicated in the figure, the mesh capability allows for direct, single-hop LSPs between a pair of LSR/STs, thus bypassing the LSR/Hub functional entity. For the connectivity with the terrestrial MPLS network via the LSR/Hub, the same considerations as above apply. In fact, in terms of user traffic, the Hub is just a special type of ST, so that the LSR/Hub and the LSR/ST are equivalent network entities for LSPs.

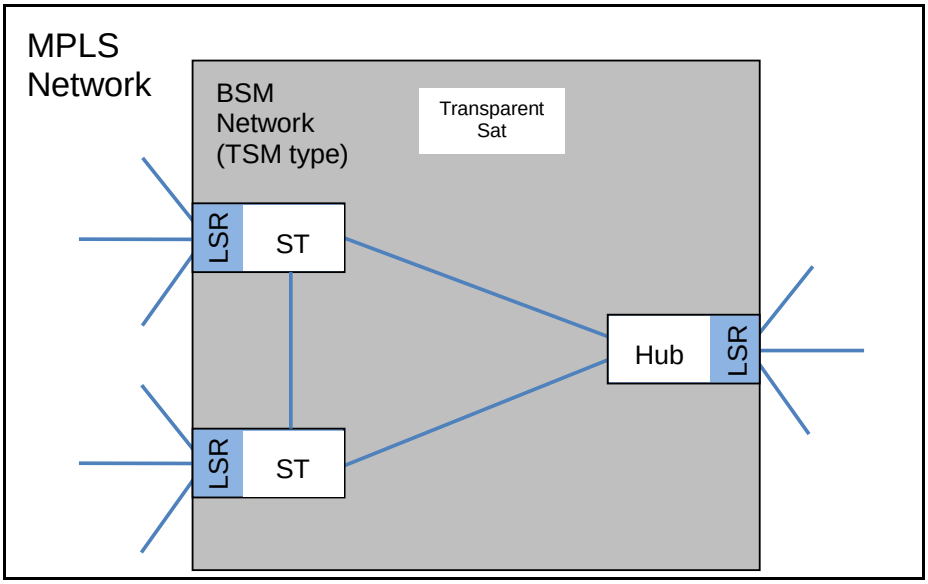



**Figure 5.2: Scenario A1 with a TSM type of BSM network**

In Figure 5.3, the architecture of Scenario A1 is depicted for the case when the BSM network is of type RSM. In such a network, no central Hub exists, and the connectivity to the terrestrial MPLS network is provided via a Gateway (GW), enhanced by the LSR functionality. In terms of MPLS connectivity, the LSR/GW functional entity plays the same role as the LSR/Hub in the TSM case, except that the GW does not connect a pair of STs (double hop); instead, for ST to ST connectivity, a BSM network of type RSM employs a single hop via the OBP satellite.

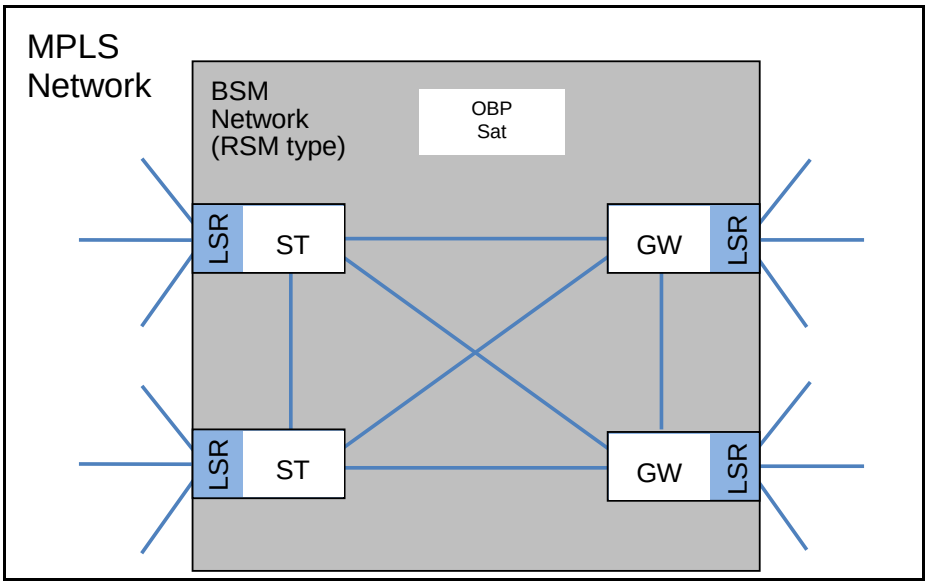



**Figure 5.3: Scenario A1 with an RSM type of BSM network**

Figure 5.3 shows two LSR/GW functional entities to illustrate the possibility of single-hop LSR/GW to LSR/GW connectivity, thus allowing the BSM network to play the role of a transit network, e.g. interconnecting two large terrestrial MPLS networks via a single LSP hop over the satellite.

The common characteristic of the above scenarios of type A1 is the fully integrated MPLS capability in both the STs and the Hub (or GW), irrespective of the type of BSM network. Figure 5.4 shows Scenario A2 where the MPLS capability is additionally integrated on-board the satellite, assuming a BSM network of type RSM.

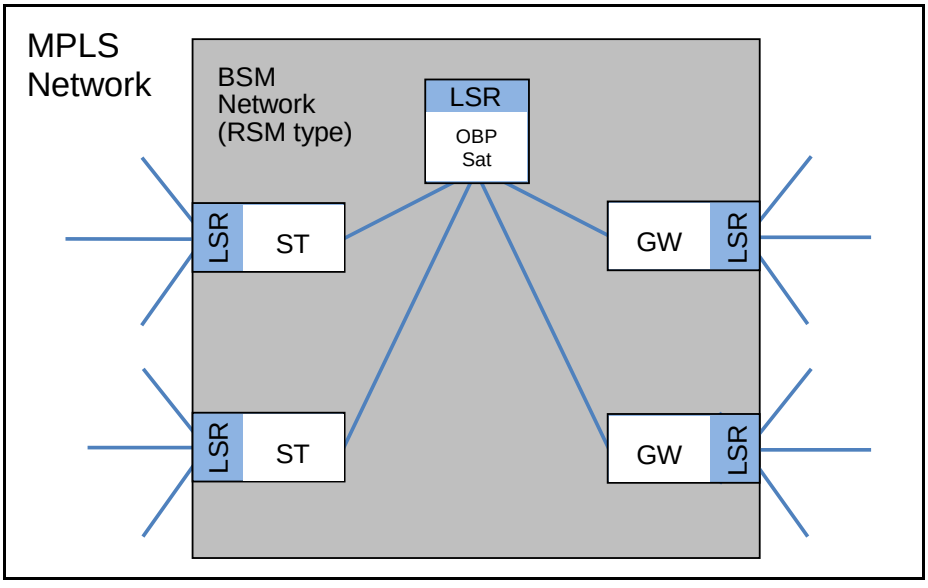



**Figure 5.4: Scenario A2 -LSR on-board (not analysed in detail)**

There are experimental satellite systems that employ on-board IP routers and therefore Scenario A2 could be foreseen as a future development of such systems. Scenario A2 will not be studied further in the present document.

Concluding this clause on variants of Scenario A, it is noted that all of the above network entities are defined as *functional* entities, and no assumptions are made regarding the degree of *physical* integration. For example, the LSR/ST, LSR/Hub and LSR/GW functional entities may each be realised as integrated physical entities. Another implementation option would be to realise a physical separation of the upper layers from the lower, satellite-dependent layers. The following clause on protocol stacks will briefly address this issue.

### 5.1.2 Protocol Stack

This clause specifies the protocol stacks for the variants of Scenario A introduced above. The discussion here is kept at a conceptual level and any details, in particular relating to SI-SAP and the procedures at the user, control and management planes, are given in TS 102 856-2 [11].

Figure 5.5 shows the protocol stack for Scenario A1 in the TSS case, assuming a physically integrated implementation of both the LSR/ST and the LSR/Hub functional entities. On the terrestrial side (left and right borders in the figure), these entities communicate via the ordinary IP protocol stack containing an embedded MPLS sublayer; on the satellite interface, communication occurs via the BSM protocol stack, which is however modified by the presence of the MPLS sublayer.

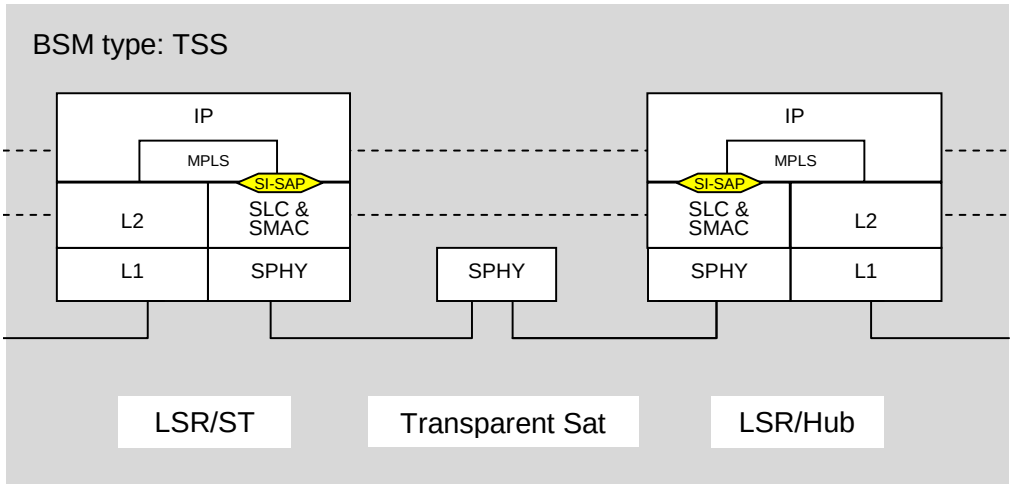



**Figure 5.5: Protocol stack for Scenario A1 with BSM type TSS; a physically integrated implementation of the BSM network entities is assumed**

The figure also highlights the BSM SI-SAP interface, which is placed between the IP/MPLS and SLC&SMAC layers. The presence of the MPLS sublayer entails certain modifications to SI-SAP, which require a careful consideration of the procedures at all three SI-SAP planes. For example, at the user plane, it must be ensured that the MPLS shim header is passed on across SI-SAP, so that it can be correctly transmitted over the air interface to the adjacent LSR. At the control plane, MPLS specific parameters and settings from the upper layer must be correctly translated into lower-layer, satellite dependent parameters so that the appropriate satellite resources can be assigned. TS 102 856-2 [11] will specify these modifications.

The fact that the MPLS sublayer in the figure does not extend across the entire width of the LSR/ST and LSR/Hub entities indicates that not all primitives between the IP layer and the lower layers pass through the MPLS sublayer. Obviously, non-MPLS packets must be processed and forwarded by these entities in the usual way.

To illustrate a possible alternative physical realisation from the one assumed in Figure 5.5. Figure 5.6 displays the protocol stack for the same scenario as above, however assuming that the BSM entities are implemented in a physically separated arrangement. As can be seen, the LSR/ST and LSR/Hub functional entities are each separated into two physical components, one forming a Layer 3 entity, and the other one forming a Layer 2 entity. The Layer 3 entity provides the IP/MPLS interface towards the terrestrial side, and the Layer 2 entity provides the satellite interface. The interconnection between these two physical entities is realised via a terrestrial LAN.

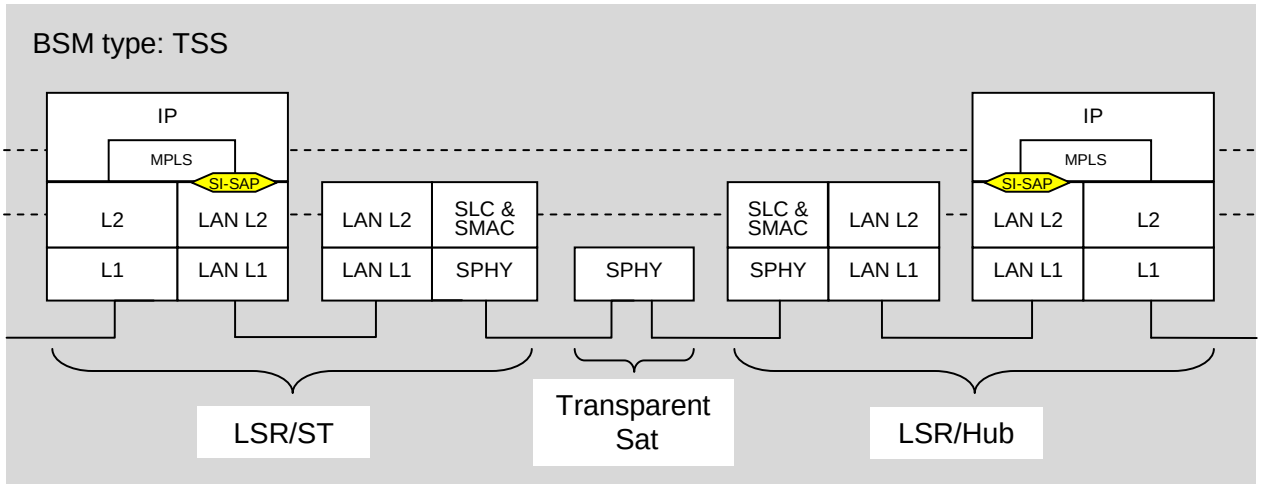



**Figure 5.6: Same as in Figure 5.5, except that a physically separated implementation of the BSM network entities is assumed**

As noted above, the present document does not specify or recommend any specific physical realisation of the combined MPLS/BSM functional entities. Both protocols stacks shown above represent compliant physical realisations of the functional entities defined here.

Figure 5.7 depicts the protocol stack for Scenario A1 for the TSM case, assuming a physically integrated implementation of both the LSR/ST and the LSR/Hub functional entities. A comparison with Figure 5.5 shows that the mesh topology, which is reflected in the fact that the rightmost entity in Figure 5.7 can be an LSR/Hub *or* an LSR/ST, does not alter the protocol stack as compared with the star topology. As already discussed in clause 5.1.1, this again shows that the Hub is just a special ST as far as the handling of user traffic is concerned. The complexities of a mesh system are confined to BSM-internal control and signalling, and this level is not represented in the present protocol stack diagrams.

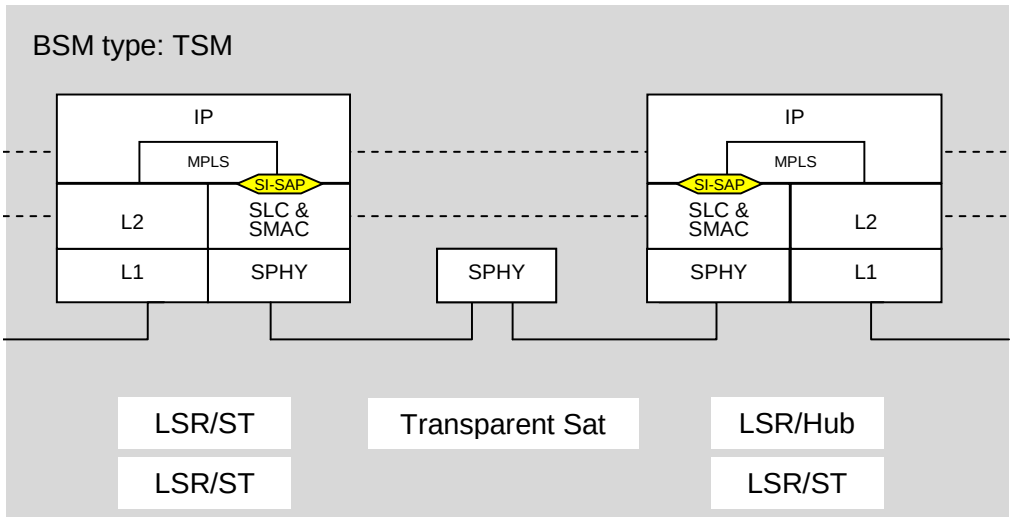



**Figure 5.7: Protocol stack for Scenario A1 with BSM type TSM (physically integrated arrangement)**

Figure 5.8 shows the protocol stack for Scenario A1 for the RSM case (physically integrated arrangement). Again, the protocol stacks for the combined MPLS/BSM entities remain unaffected by the mesh configuration. Apart from the additional connectivity relationship brought about by the LSR/GW, the only difference between Figures 5.8 and 5.7 concerns the satellite, which is regenerative in the RSM case.

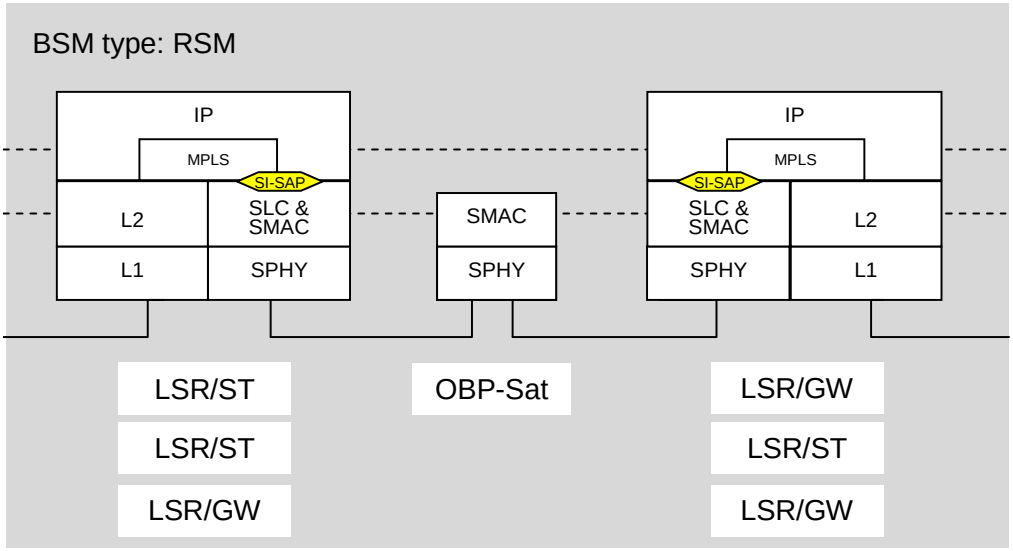



**Figure 5.8: Protocol stack for Scenario A1 with BSM type RSM (physically integrated arrangement)**

## 5.1.3 QoS Provisioning

The problem of how to introduce QoS awareness in BSM networks is addressed in the three technical specifications TS 102 462 [4] (QoS functional architecture), TS 102 464 [6] (Interworking with DiffServ QoS) and TS 102 463 [5] (Interworking with IntServ QoS). The central theme in these specifications concerns the mapping and translation of QoS-specific higher (mostly IP)-layer parameters and procedures to the satellite-dependent, lower layers. The eventual goal is to enable the satellite-dependent layers (below SI-SAP) to implement and deliver the QoS as communicated and demanded by the higher layers (above SI-SAP).

This relationship between the layers above and below SI-SAP is significantly altered by the presence of an MPLS sublayer, which is located between the SI-SAP interface and the IP layer. It should be noted, however, that only a certain set of procedures involve the MPLS sublayer, namely those dealing with the control of LSPs and the forwarding of traffic within LSPs. Only MPLS packets, i.e. packets that contain an MPLS shim header, are in fact passed through the MPLS sublayer and are processed and routed according to MPLS specifications. Ordinary (non-MPLS) IP packets either bypass the MPLS sublayer, or - if they pertain to the setup and control of LSPs - invoke procedures inside the MPLS sublayer.

The following clauses address three different QoS approaches that have been considered for BSM networks, and specify their application to the fully integrated MPLS/BSM case. These three approaches are the BSM Traffic Classes, the DiffServ model, and the IntServ model. The following provisions pertain to all variants of Scenario A.

### 5.1.3.1 BSM Traffic Classes

As mentioned in the clauses 4.1.2 and 4.1.3, the BSM traffic classes were constructed for the purpose of capturing and categorising a wide spectrum of observed traffic characteristics. They do not correspond to any specific Internet QoS model. In fact, for a given QoS model (e.g. DiffServ, IntServ, or any proprietary or future model), a scheme or mapping must be defined to allocate the correct BSM traffic class, and thus QoS treatment at the SD layers, to each traffic component that requests a model-specific QoS treatment at the higher layers. No such mapping has however been specified so far, leaving this as an implementation choice.

The same considerations apply in the case when an MPLS sublayer is present. The interaction of the higher layers with the SD layers (across SI-SAP) strongly depends on the nature of the QoS model, e.g. whether or not IP packets carry a QoS-specific marking, or whether or not a QoS model-specific signalling system is present. In any case, at the SI-SAP interface, criteria must be established and enforced that ensure that all components of the user traffic - independent of how they are classified - are assigned to the appropriate BSM Traffic Classes. In that respect, therefore, MPLS does not add to the complexities of mapping QoS characteristics and demands between layers. Such mappings are left as an implementation or configuration choice to the network operator.

### 5.1.3.2 DiffServ

Figure 5.9 illustrates the relationship between the IP layer, the BSM SD layer, and the MPLS sublayer for the case when the DiffServ model is used at the IP layer. No distinction is made here between the user, control and management planes. For each layer, certain key parameters that are relevant in the present context are listed in the figure. The vertical double arrows indicate specifications that govern the respective relationship. The relationship between the IP layer and the SD layers (across SI-SAP) is defined by the BSM specification TS 102 464 [6] (Interworking with DiffServ QoS). The relationship between the IP layer and the MPLS sublayer is defined by the IETF specification RFC 3270 [i.10] (MPLS Support for DiffServ). Finally, this multi-part deliverable deals with the relationship between the MPLS sublayer and the SD layers (across SI-SAP).

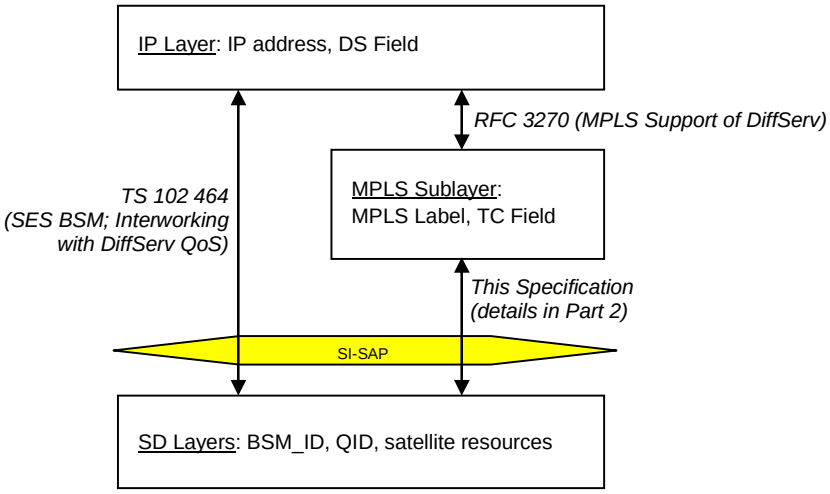



**Figure 5.9: Illustration of the scope and relationship of QoS-related specifications for the case of DiffServ**

**IP Layer to MPLS Sublayer Mapping**

As discussed in clause 4.2.3, RFC 3270 [i.10] specifies two approaches for mapping the DS field onto MPLS fields, and these are the E-LSP and the L-LSP approach. Both approaches may be used in the present context. Since these approaches may coexist in a given LSR, the MPLS sublayer must keep a memory that records, for each active LSP, whether the E-LSP or the L-LSP approach applies. This is necessary in order to obtain a correct interpretation of the contents of the MPLS label and the MPLS TC field.

**MPLS Sublayer to SD Layers Mapping**

As concerns the translation and mapping of the QoS settings from the MPLS sublayer across SI-SAP down to the SD layers, the QoS functional architecture for BSM networks as defined in TS 102 462 [4] shall be applied. This involves the concept of QIDs, which denote abstract queues defined at the SI-SAP for transferring user data via the SI-SAP. In terms of the SD layers, each QID represents a specific capability of the underlying BSM network to transmit packets across the satellite, expressed by a specific set of parameters such as bitrate, delay, jitter and packet loss probability. It is the responsibility of the BSM network to implement these capabilities, and to assign and manage the associated QIDs. TS 102 462 [4] specifies an architecture for assigning and managing QIDs that allows for both static and dynamic assignments, as well as centralised and distributed management architectures. Since these provisions are independent of the details of the SI layers above SI-SAP, they also apply for the present case.

Furthermore, recognising that TS 102 464 [6] already defines the interworking of DiffServ-enabled (non-MPLS) IP networks with BSM networks, the provisions in that TS can serve as a template for the present problem. Specifically, while TS 102 464 [6] is concerned with the mapping of DSCPs to QIDs, the present document is concerned with the mapping of the MPLS TC field (in the E-LSP case), respectively the MPLS label and the MPLS TC field (in the L-LSP case) to the QIDs.

Consequently, the problem of introducing DiffServ into integrated MPLS/BSM networks is thus reduced to the task of mapping the MPLS label and the MPLS TC field to the appropriate QIDs so that these data packets receive the correct treatment by the SD layers. The required procedures for this task are analogous to those specified in TS 102 464 [6].

A more detailed specification, focusing on the control plane, is given in TS 102 856-2 [11].

#### 5.1.3.3 IntServ

IntServ is an IETF architecture (defined in RFC 1633 [i.2]) that supports guaranteed QoS in IP networks. In contrast to DiffServ, the IntServ model relies on a resource reservation protocol, RSVP (defined in RFC 2205 [i.3]), to request and reserve the required resources along the path. An RSVP request contains the so-called "flowspec," which specifies the desired QoS for a specific packet flow.

IntServ thus allows for the explicit reservation of (guaranteed) resources within IP routers per flow, however at a considerable cost in terms of memory and processing in routers. This leads to poor scalability and manageability, so that IntServ is not used widely in today's IP networks.

Since IntServ is not considered the primary choice for implementing a QoS orientation in IP networks, the following provides only a brief outline of a possible approach for an integrated MPLS/BSM architecture based on IntServ.

In analogy to the previous figure for DiffServ, Figure 5.10 illustrates the relationship between the various involved layers for the case when the IntServ model is used. It is noted that a BSM specification (TS 102 463 [5]) is available that defines the relationship between the IP (and higher) layers and the SD layers, and that no IntServ-specific RFC exists at the interface between the IP (and higher) layers and the MPLS sublayer. This latter observation is a consequence of the fact that, unlike DiffServ, IntServ does not introduce any packet markings which would need to be mapped to the MPLS shim header. At the same time, the absence of an RFC at this interface indicates that the IETF does not specify how IntServ flows are to be mapped onto LSPs. This issue is thus considered an implementation choice.

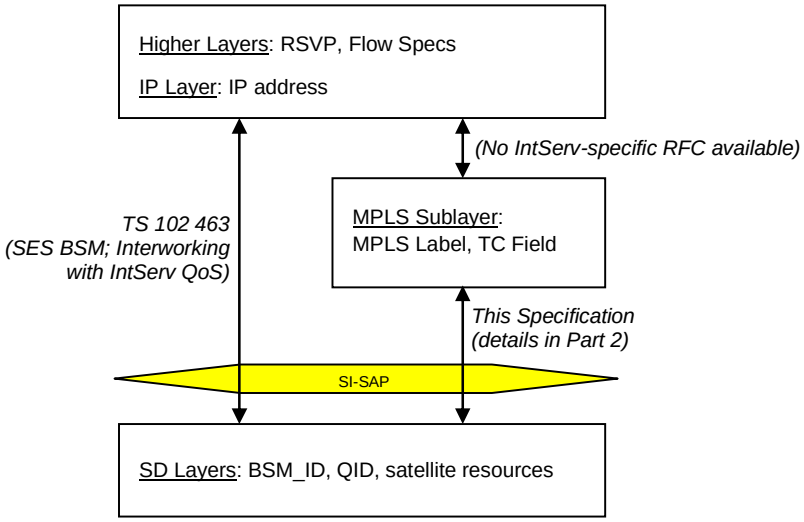



**Figure 5.10: Illustration of the scope and relationship of QoS-related specifications for the case of IntServ**

The BSM specification TS 102 463 [5] defines how the IntServ model shall be integrated with BSM networks. The key issues concern the mapping of the IntServ service classes and associated styles of traffic and QoS characterisation onto the BSM service model, and the mapping of RSVP procedures onto BSM signalling. Both issues are separate and independent of both MPLS signalling (LSP set-up) and MPLS packet forwarding, so that they do not interfere with each other. However, as mentioned above, the question remains as to how IntServ flows are to be mapped onto LSPs. This is left as an implementation choice which can be decided by the network operator in conjunction with traffic engineering choices. For all other issues, the provisions in TS 102 463 [5] should be employed where applicable.

A more detailed specification, focusing on the control plane, is given in TS 102 856-2 [11].

### 5.1.4 Traffic Engineering

As discussed in clause 4.2.4, traffic engineering in MPLS networks deals with the problem of mapping traffic trunks onto LSPs with the objective to optimise network resource utilisation and traffic performance. Since, in Scenario A, all BSM network entities that process IP traffic are fully MPLS-capable routers, all IETF specifications relating to MPLS TE are directly applicable. This is due to the fact that, from an MPLS networking point of view, terrestrial links differ from BSM satellite links only in terms of the lower-layer (L1 and L2) techniques. Owing to the special properties of satellite links, however, certain issues arise when applying IETF TE mechanisms.

For example, the list of basic attributes of traffic trunks introduced in RFC 2702 [i.5] was developed having only terrestrial links in mind. Traffic trunk attributes (e.g. traffic parameters, priority, pre-emption, resilience, and policing attributes) are assigned to a traffic trunk for the purpose of influencing its behaviour and applying the correct treatment by the network entities. A traffic trunk that crosses a satellite link will pick up additional attributes such as an extended transmission delay and a risk of interference and interception, among other attributes. An implementation may benefit from provisions that explicitly account for these satellite-specific features. Since traffic trunk attributes can be assigned either by administration action or by signalling protocols (e.g. RSVP-TE), adding the satellite-specific attributes to the standard list of traffic trunk attributes will have an impact on existing IETF specifications. A detailed analysis of these issues is however beyond the scope of the present document.

In the discussion of MPLS TE so far, no specific reference was made to QoS provisions, which may be present in an integrated Scenario-A MPLS/BSM network (see clause 5.1.3). If the IETF MPLS TE procedures are applied without regard to QoS provisions (e.g. DiffServ markings), the full potential of both concepts cannot be exploited effectively. RFC 3564 [i.11] addresses this issue by defining requirements for the combined use of QoS and TE mechanisms in a DiffServ-aware MPLS network. In this way, traffic engineering can be performed at a per-class level rather than on an aggregate basis across all DiffServ classes of service. The combined and coordinated use of DiffServ and TE is referred to as "DiffServ-aware Traffic Engineering (DS-TE)."

RFC 3564 [i.11] mentions examples of networks which would particularly benefit from DS-TE, such as:

i) networks where bandwidth is scarce;

ii) networks with significant amounts of delay-sensitive traffic; and

iii) networks where the relative proportion of traffic across classes of service is not uniform.

Integrated MPLS/BSM networks may fall into some of these categories, depending on the particular usage scenario.

Use of the above TE features is optional for Scenario A.

### 5.1.5 Resiliency

As part of the overall TE framework, resiliency is concerned with the robustness, survivability and (automatic) restorability of a network in the event of a variety of possible failure modes. Concerning MPLS networks, resilience features appear in several TE-specific IETF specifications already mentioned in the previous clause, including the resilience attribute of a traffic trunk (RFC 2702 [i.5]) and the RSVP Hello extension (RFC 3209 [i.9]). The resilience attribute determines the behaviour of a traffic trunk when a fault occurs along the path through which the traffic trunk traverses. The RSVP Hello extension provides a transport-layer mechanism (involving a Hello message) that enables RSVP-TE nodes to detect when a neighbouring node is not reachable.

Existing IETF specifications also define protocol extensions to ensure that local fault conditions can be propagated throughout the MPLS network. For the present purposes, RFC 3630 [i.12] (Traffic Engineering Extensions to OSPF Version 2) and RFC 4090 [i.14] (Fast Reroute Extensions to RSVP-TE for LSP Tunnels) are particularly relevant.

RFC 3630 [i.12], also referred to as OSPF-TE, starts from the requirements for MPLS TE (RFC 2702 [i.5]) and specifies extensions to the OSPF protocol version 2 to support intra-area TE. Specifically, to enhance the resiliency of an MPLS network, certain extended link attributes are added to the list of standard link attributes for incorporation into a router's traffic engineering database. These extended link attributes are contained in a newly defined Link State Advertisement (LSA), which is called the Traffic Engineering LSA. The essential elements of the TE LSA are the respective link's maximum bandwidth, maximum reservable bandwidth, and unreserved bandwidth. Following standard OSPFv2 procedures, the TE LSA is flooded throughout the OSPF area whenever certain criteria (e.g. significant bandwidth changes) are met.

RFC 4090 [i.14] defines RSVP-TE extensions to establish backup LSP tunnels for local repair of LSP tunnels. These mechanisms enable the fast redirection of traffic onto backup LSP tunnels in the event of a failure. In order to meet the timing requirements of real-time services (such as VoIP), the backup LSP tunnels are computed and signalled in advance of the failure, thus achieving restoration times of a few tens of milliseconds. Two distinct methods are defined for the protection of both links and nodes during network failure. The *one-to-one backup method* creates detour LSPs for each protected LSP at each potential point of local repair. The *facility backup method* creates a bypass tunnel to protect a potential failure point; by taking advantage of MPLS label stacking, this bypass tunnel can protect a set of LSPs that have similar backup constraints. Obviously, this latter method is ideally suited to protect links that carry a higher probability of failure, such as a satellite link in the case of adverse atmospheric conditions or interference. To protect a satellite link, a bypass tunnel would be created around the affected (e.g. uplink) LSR/ST to use an alternate LSR/ST or a terrestrial link. By design, that bypass tunnel would carry all LSPs that use the affected satellite link.

Since the present integrated MPLS/BSM network (Scenario A) involves only fully MPLS-compliant LSRs, all these IETF specifications are directly applicable. In order for these resiliency procedures to work properly also in the case of a (potentially changeable or unstable) satellite link, a mechanism must be in place that constantly monitors its properties. For a BSM network, this is achieved by the BSM Network Management System (B-NMS) (see [7] to [10]).

Use of the above resiliency features is optional for Scenario A.

## 5.2 Scenario B: Interworking Using IP Tunnels

This clause introduces an MPLS/BSM scenario whereby no direct interworking between the MPLS and BSM network is foreseen (Scenario B). The sole objective here is to ensure that the LSP is tunnelled across the BSM network, thus enabling it to emerge intact at the other side. Consequently, no explicit MPLS specific treatment is possible inside the BSM network.

Tunnelling of LSPs across IP networks has been introduced in clause 4.2.5. These techniques will be applied to BSM networks in the next clause. The following clauses address the protocol stack and issues concerning QoS provisioning, traffic engineering and resiliency.

### 5.2.1 Network Architecture

Figure 5.11 depicts the architecture of Scenario B1, using a BSM network of type TSS as an example. The following considerations however apply to all types of BSM network. The figure first of all shows that all BSM entities remain unaffected by MPLS. In fact, the encapsulation or decapsulation procedures are performed by RFC 4023 [i.13] capable LSRs that are connected to the BSM stations, but are considered to lie outside of the BSM network. These LSRs form the tunnel heads (encapsulating role) or tunnel tails (decapsulating role). The dashed (blue) lines in the figure denote IP tunnels that contain the encapsulated LSPs. From the MPLS network point of view, the pair of encapsulating and decapsulating LSRs are adjacent routers, separated by a single MPLS hop. From the BSM network point of view, the ST (or Hub) receives ordinary IP traffic from the terrestrial side, which it processes and routes according to the BSM standard; due to the encapsulation, the BSM network is transparent to MPLS.

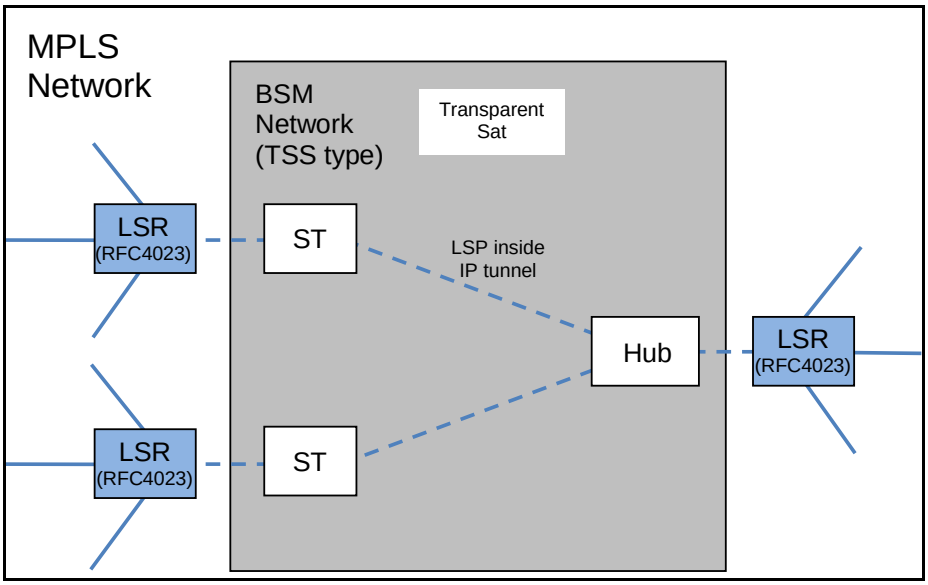



**Figure 5.11: Scenario B1 - MPLS tunnelling across the BSM network (see text)**

As discussed in clause 4.2.5, RFC 4023 [i.13] specifies two IP-based encapsulations. Figure 5.12 illustrates these two methods in terms of the header(s) added to the MPLS packet. In both cases, the resulting packet is a standard IP datagram that can be processed by the (unchanged) BSM network in the usual way.


a) MPLS Encapsulation in IP b) MPLS Encapsulation in GRE

**Figure 5.12: Illustration of the two MPLS encapsulation methods specified in RFC 4023 [i.13]**

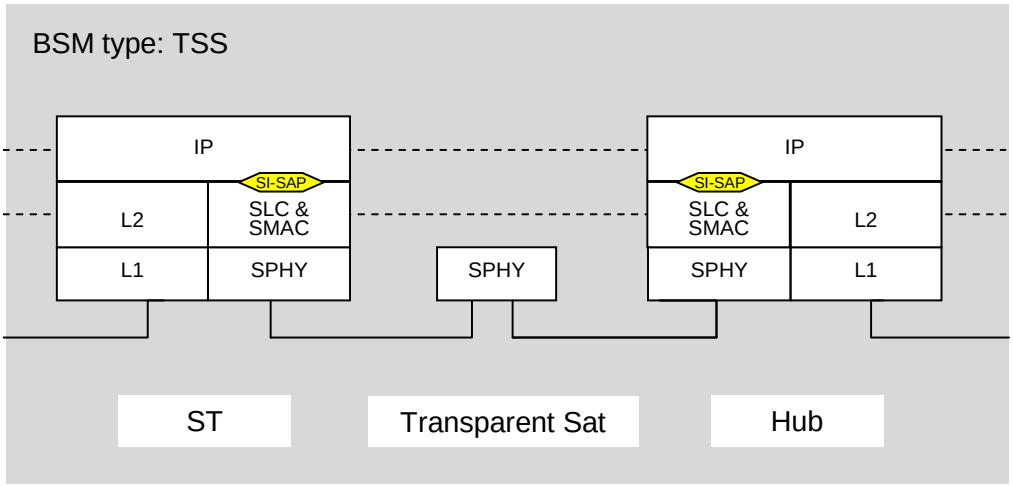
The GRE header in method (b) contains only optional fields such as a GRE checksum and GRE key and sequence number fields. Since these fields are not considered beneficial in the case of MPLS encapsulation, RFC 4023 [i.13] views method (a) as the preferred choice, unless certain conditions apply (see RFC 4023 [i.13]).

As to the contents of the encapsulating IP header, RFC 4023 [i.13] specifies that the source and destination addresses shall be set to the addresses of the encapsulating and decapsulating LSRs, respectively. An encapsulating LSR must thus have knowledge of the decapsulating LSRs IP address, and it must be aware that the decapsulating LSR is actually capable of decapsulating the relevant protocol(s). This knowledge may be conveyed to the encapsulating LSR by manual configuration, or by means of some discovery protocol.

Concluding, in the absence of any specific constraints that suggest other solutions, MPLS encapsulation in IP (according to RFC 4023 [i.13]) is considered the preferred choice for tunnelling MPLS packets across BSM networks.

### 5.2.2 Protocol Stack

Figure 5.13 shows the protocol stack for Scenario B1. Since the BSM network is transparent to MPLS, the protocol stack remains unchanged with respect to the original BSM stack, and no MPLS functionality is present inside the BSM network. Note that the fact that the IP layer encapsulates MPLS affects neither the protocol stack nor any procedures inside the BSM network.




NOTE: Here the IP layer represents the encapsulating IP protocol.

**Figure 5.13: Protocol stack for Scenario B1 with BSM type TSS**

### 5.2.3 QoS Provisioning

Since the BSM network is transparent for MPLS, BSM entities have no access to the MPLS shim header and are thus unable to realise any specific QoS requirements that may be encoded in the MPLS TC field and/or the MPLS label. In order to provide specific QoS guarantees to the tunnelled portion of the LSP, therefore, the tunnel head, i.e. the encapsulating LSR, must take action.

RFC 4023 [i.13] addresses this issue for the case of DiffServ, and refers to RFC 2983 [i.6] (DiffServ and Tunnels). It is stated that the DS field of the encapsulating header may be determined, at least partially, by the BA of the MPLS packet. Note that the BA is encoded in the MPLS TC field and/or the MPLS label, depending on the employed encoding approach (E-LSP or L-LSP). This mapping must be performed according to pre-configured or signalled rules. In any case, these procedures and mapping rules shall ensure that the encapsulating IP header is constructed in such a way that the BSM entities treat the IP datagrams according to the QoS requirements expressed in the encapsulated MPLS packet. To process and forward these IP datagrams, the BSM entities will naturally follow exactly the same procedures as with native IP datagrams that contain no encapsulated MPLS packets. Since the interaction of DiffServ with IP tunnels does not involve any BSM-specific provisions, no further discussion is required here.

As regards the application of the IntServ QoS model to Scenario B, it is observed that, as in the case of DiffServ, the tunnel heads and tails are the only potential points of interaction between MPLS and IntServ/RSVP. However, given that no RFC exists to govern that interaction, the mapping of IntServ flows onto LSPs is an implementation choice. At the same time, it must be stated that the encapsulating LSR (tunnel head) shall nevertheless ensure that its IP tunnel across the BSM network conforms to the QoS demands as specified in the RSVP's flowspec that applies to that tunnel. To communicate these demands to the BSM network, the encapsulating IP protocol may employ any QoS mechanism that is understood by the BSM entities.

In conclusion, providing QoS in BSM networks in the frame of Scenario B does not impose any requirements beyond those defined in existing BSM specifications. In particular, QoS shall be provided according to the BSM QoS functional architecture as defined in TS 102 462 [4], and no modifications are foreseen to support the present tunnelling scenario.

### 5.2.4 Traffic Engineering

Traffic engineering in a Scenario-B MPLS/BSM network can be performed using the same procedures and mechanisms as in ordinary MPLS networks (and in Scenario A). In contrast to Scenario A, however, the BSM stations (ST, Hub, GW) are not MPLS capable, thus requiring functionally separated LSRs to be introduced outside the BSM network. As a consequence, the IP tunnel carrying the LSP across the BSM network (one MPLS hop) consists of three physical links, i.e. two terrestrial and one satellite link. Since traffic engineering relies heavily on the properties of links, it is crucial that this special (hybrid) MPLS hop is properly characterized in the TE database. Apart from these constraints, the considerations and provisions given for the case of Scenario A (see clause 5.1.4) apply.

### 5.2.5 Resiliency

Similarly, the resiliency procedures described for the case of Scenario A (see clause 5.1.5) also apply for Scenario B. Again, however, the peculiar architectural feature of Scenario B that the MPLS hop across the BSM network consists of three physical links, constrains the flexibility of TE/resiliency actions that exists in Scenario A. In particular, a degradation or failure of the satellite link would render all three physical links that constitute the MPLS hop unusable by MPLS TE/resiliency, thus forcing a wider detour or longer bypass tunnel around the failure. In order for these repair procedures to work properly, it must be ensured that these constraints are correctly represented in the TE database and signalled accordingly by OSPF-TE and RSVP-TE. A detailed analysis of these issues is however beyond the scope of the present document.

# 6 MPLS/BSM-Specific Functional Elements

In this clause the various functional entities of the MPLS/BSM scenarios introduced in the previous clause will be briefly described and their key features summarised. TS 102 856-2 [11] will define the involved user, control, and management plane procedures in detail.

## 6.1 LSR/ST

The LSR/ST is a BSM functional network entity that provides MPLS-based interworking between the BSM network and a premises network. It combines the role of an LSR (MPLS-enabled IP router) with that of a BSM ST. Specifically, when communicating with other LSRs, this entity behaves like an ordinary LSR, and when communicating with other BSM entities, it acts like a BSM ST (with certain modifications, see below).

In its role as an LSR, the LSR/ST entity performs the functions of an MPLS node, in particular label swapping and MPLS packet switching, and it also acts like an ordinary IP router when receiving non-MPLS (IP) packets. When placed at the edge of an MPLS domain, the LSR performs the functions of an MPLS edge node, i.e. inserting and removing MPLS labels. Such a node is referred to as a Label Edge Router (LER).

In its role as a BSM ST, the LSR/ST entity handles both the BSM-internal control and signalling procedures (including exchanges with the NCC), as well as the processing and forwarding of BSM network traffic. While the basic BSM functional architecture as defined in TS 102 292 [1] remains unchanged, the presence of an MPLS sublayer causes certain modifications at the SI-SAP interface as defined in TS 102 357 [3]. In particular, at the user plane, the SDU of the data transport primitives must include both the MPLS shim header and the IP datagram (instead of only the IP datagram). At the control plane, several services need to be modified, especially relating to the fact that the address resolution and resource reservation parameters must now be derived from the MPLS sublayer instead of the IP layer, and that MPLS signalling needs to be handled. A detailed description of these issues is given in TS 102 856-2 [11].

As the present document deals with the *functional* architecture of an integrated MPLS/BSM network, no assumptions are made regarding the *physical* integration of network entities. In particular, the LSR/ST may be realised as a single, integrated physical entity or separated into (e.g. two distinct physical entities). Clause 5.1.2 (Figure 5.6) presents an example of a physically separated arrangement, where the IP/MPLS functions are implemented by a Layer 3 entity, and the BSM-related functions are implemented by a Layer 2 entity.

## 6.2 LSR/Hub

The LSR/Hub functional entity appears in network topologies where double-hops occur between remote stations. The LSR/Hub relays this double-hop traffic by means of MPLS switching, thus acting like an ordinary LSR. In terms of its role as a BSM station, the LSR/Hub is capable of both receiving traffic from, and transmitting traffic to remote satellite stations, thus behaving like an ordinary BSM Hub at the SD layers.

In addition to the (BSM-internal) Hub functionality, the LSR/Hub also provides MPLS-based interconnection to external networks.

As the LSR/Hub may be viewed as an LSR/ST with an additional (BSM-internal) traffic relay capability, the LSR/ST features summarised in the previous clause also apply here. This includes the note on the physical implementation of the functional entities.

## 6.3 LSR/GW

The LSR/GW functional entity provides MPLS-based interworking between the BSM network and external networks. It thus provides the same basic functions as the LSR/ST, both in terms of its role as an LSR and as a BSM station. The capabilities described for the LSR/ST in clause 6.1 thus also apply for the LSR/GW.

## 6.4 LSR/OBP-Sat

The LSR/OBP-Sat functional entity appears in Scenario A2 in clause 5.1 (Figure 5.4), where a BSM network of type RSM is assumed. As this scenario is not analysed in detail in the present document, the LSR/OBP-Sat will not be discussed further here.

# Annex A (informative): Use Cases

This annex presents examples of basic use cases of MPLS/BSM Scenarios A and B.

## A.1 MPLS Network using Scenario A1

Figure A.1 shows how a fully MPLS enabled (Scenario A1) BSM network of type TSS can be used to interconnect terrestrial MPLS networks. In this use case, two remote MPLS networks (labelled A and B) are each connected to an LSR/ST, and MPLS Network C is connected to the LSR/Hub. In a typical application, Networks A and B would be remote enterprise networks, and Network C would be the public Internet. A geographically distributed enterprise with remote locations A and B and a central site (headquarter) inside C could thus be interconnected by means of BSM-based LSPs.

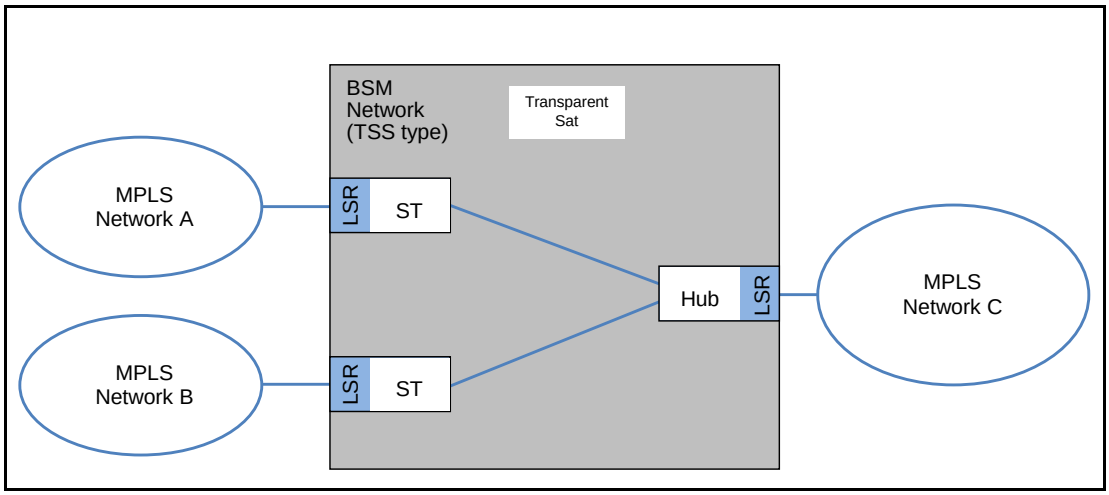



**Figure A.1: Interconnection of terrestrial MPLS networks via an MPLS-enabled BSM network of type TSS (Scenario A1)**

The following types of MPLS connectivity are supported in this use case:

- Connectivity A - B: Interconnection of (remote) MPLS networks A and B via a double satellite hop.
- Connectivity (A, B) - C: Interconnection of MPLS networks A and B to a (public) provider MPLS-enabled Network C via a single satellite hop.

Using standard MPLS procedures or, if available, MPLS TE techniques for enhanced features, an arbitrary mesh of LSPs with dedicated capabilities and QoS properties can thus be established between the sites. For example, HTTP traffic, video streaming and VoIP could be separated by configuring different sets of LSPs with the appropriate distinct capabilities. If resiliency features are enabled in the network, detour LSPs or bypass tunnels (not shown in the figure) could be foreseen to protect critical traffic components against, e.g. degradation or failure of the satellite link. A bypass tunnel could start from the affected LSR/ST and run either to an alternate modem or, if available, use a terrestrial link to bypass the satellite link.

## A.2 MPLS Network using Scenario B1

Figure A.2 shows the same use case as Figure A.1, except that the MPLS/BSM integration Scenario B1 (instead of A1) is employed. As can be seen, Scenario B1 requires an encapsulating IP tunnel to be established across the (unmodified) BSM network, with the tunnel ends placed in RFC 4023 [i.13] capable LSRs. These (encapsulating/decapsulating) LSRs can be considered to be part of the interconnected MPLS networks. Any QoS or MPLS TE procedures that may be required for the LSPs crossing the BSM network are invoked by the RFC 4023 [i.13] capable LSRs. Similarly, if a bypass tunnel is required to protect critical traffic across the BSM network, the necessary resiliency procedures are the responsibility of these LSRs. As compared to the previous case for Scenario A1, this typically involves a longer detour, since the ST (or Hub) is not MPLS capable.

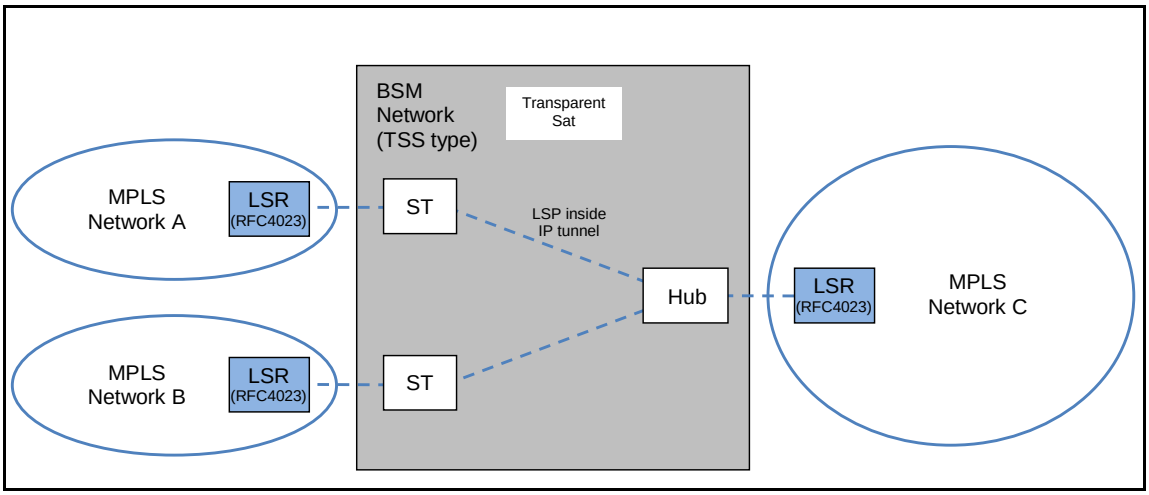



**Figure A.2: Interconnection of terrestrial MPLS networks using Scenario B1**

## A.3 MPLS Network using Scenario A2

Figure A.3 shows a further use case, involving Scenario A2 and assuming a BSM network of type RSM. The OBP-based full-mesh topology of the BSM network supports more flexible types of (single-hop) interconnectivity.

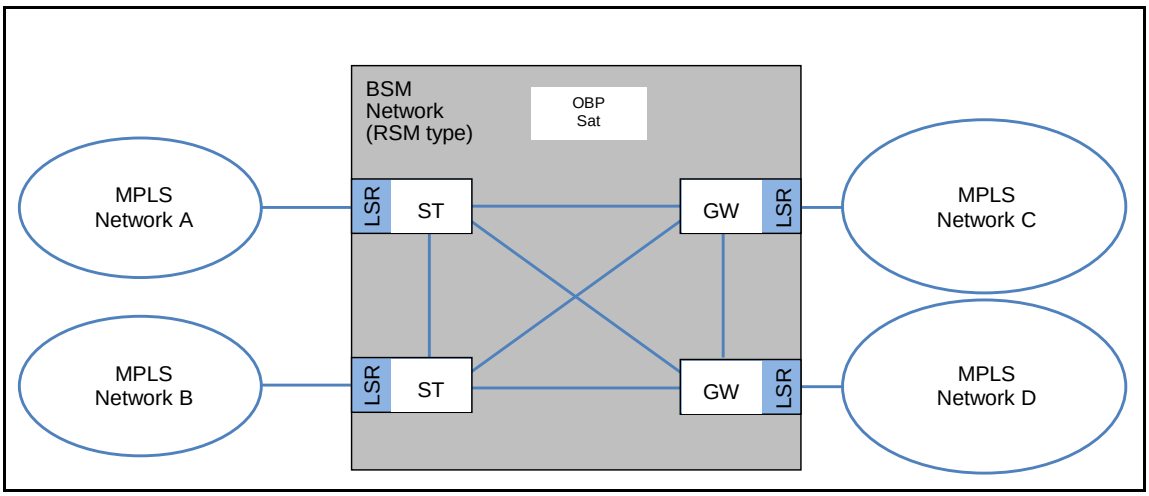



**Figure A.3: Interconnection of terrestrial MPLS networks via an MPLS-enabled BSM network of type RSM (Scenario A2)**

Specifically, the following types of connectivity are supported (all involve a single satellite hop):

- Connectivity A - B: Interconnection of (remote) MPLS networks A and B.
- Connectivity (A, B) - (C, D): Interconnection of MPLS networks A and B to (large) provider MPLS-enabled networks C and D.
- Connectivity C - D: Interconnection of (large) MPLS networks C and D.

This use case can thus also be employed to carry large amounts of provider MPLS traffic to bridge great geographical distances between two MPLS provider networks. Obviously, the great flexibility and control enabled by MPLS (QoS differentiation, TE capabilities, resiliency features) provides significant advantages to providers, as compared with non-MPLS enabled satellite links.

## A.4 MPLS VPN using Scenario A1

The above use case examples involved hybrid MPLS networks, i.e. MPLS networks that contain both terrestrial and satellite links. They dealt with connectivity configurations between nodes that are all MPLS capable.

In the following use case, an MPLS enabled BSM network is used to provide an IP VPN to ordinary (non-MPLS) customer IP networks. This is sketched in Figure A.4, whereby an MPLS/BSM Scenario A1 and a BSM network of type TSS are assumed. As can be seen, here the LSR/ST functional entities, which are the points of attachment for the customer IP networks, assume the role of Label Edge Routers (LER).

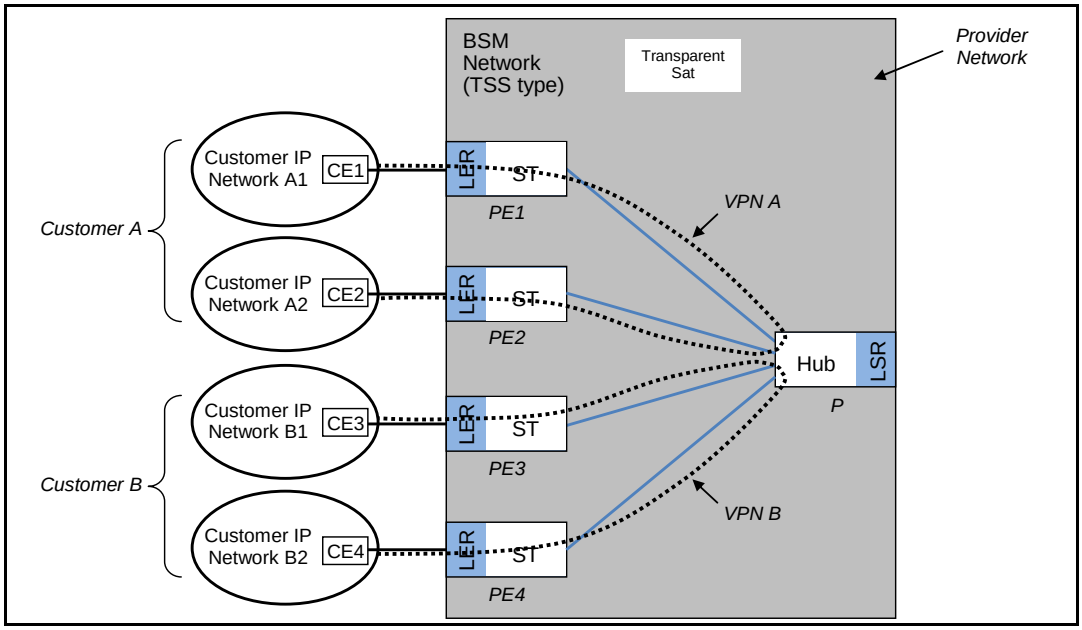



**Figure A.4: Interconnection of remote customer IP networks by realising an IP VPN based on an MPLS-enabled BSM network of type TSS (Scenario A1)**

This use case is derived from RFC 4364 [i.17], which defines the MPLS procedures within an IP backbone that enable the backbone to provide IP Virtual Private Networks (VPNs) to attached IP networks. clause 4.2.6 summarises the key features. For the purposes of the present use case, the BSM network plays the role of the IP backbone, which in this example contains five MPLS nodes, namely four PE (Provider Edge) nodes (LER/ST), and one P (Provider) node (LSR/Hub). The customer IP networks are attached to the BSM network's PE nodes via ordinary IP nodes called CE (Customer Edge) nodes.

According to RFC 4364 [i.17], BGP (RFC 4271 [i.16]) and extensions thereof are used to distribute the routes within the Provider Network, and establish the required LSPs accordingly. These mechanisms ensure both scalability and security of VPN-internal communication. In particular, communication security is intrinsically guaranteed by the separation of LSPs, so that systems in one VPN cannot gain access to systems in another VPN. This is so despite the fact that any given PE or P router can of course support more than one VPN concurrently.

As regards the provision of QoS and TE capabilities for MPLS/BGP VPNs, no adverse interactions are identified (see RFC 4364 [i.17], section 14). TE actions could even be employed to establish LSPs with particular QoS characteristics between particular pairs of sites, if that is desirable.

This use case shows how a fully MPLS enabled BSM network can be employed to provide high-quality IP VPNs to attached customer IP networks. Apart from the requirement to support certain IETF specifications in the MPLS portions of the BSM nodes, there is no impact on the BSM network.

In a variant of the above use case, the MPLS label domain can be extended from the provider (BSM) network into the customer network. As depicted in Figure A.5, this places the LER in the customer network, so that the LSR/ST entity does not need to perform LER functions. This reduces that processing load on the LSR/ST, but on the other hand introduces MPLS functionality into the customer IP networks.

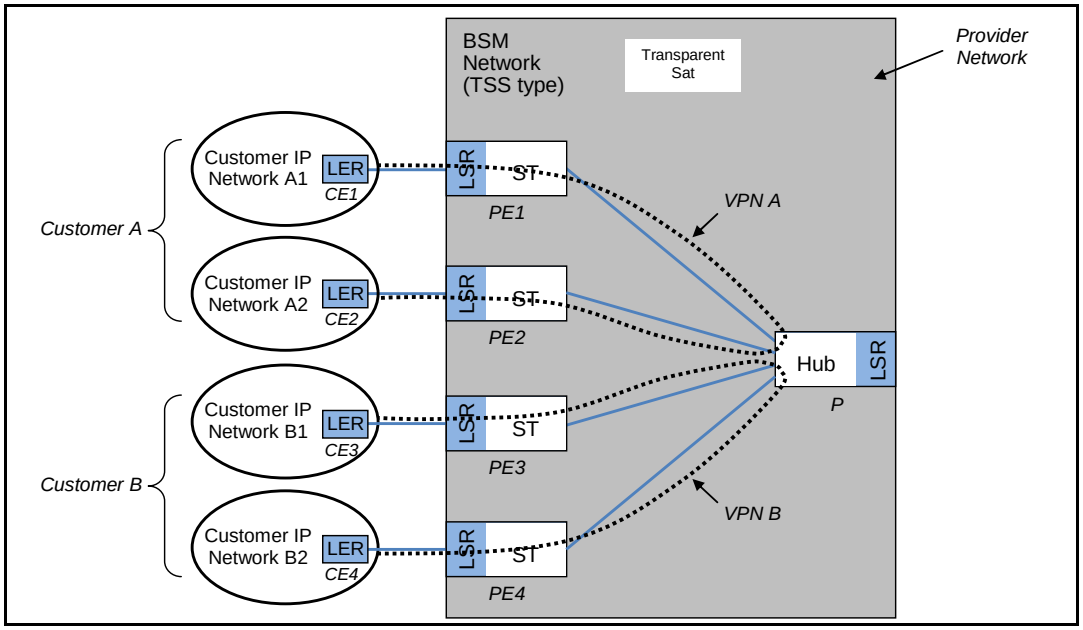



**Figure A.5: Same as in Figure A.4, except that the customer networks each contain an LER, thus extending the MPLS label domain into the customer networks**

# Annex B (informative): MPLS Transport Profile

As a rapidly maturing packet technology, MPLS is already playing an important role also in transport networks and related services. However, not all of MPLS's capabilities and mechanisms are needed and/or consistent with transport network operations. There are also transport technology characteristics that are not currently reflected in MPLS. Therefore, both the IETF and the ITU-T identified the need to define an MPLS Transport Profile (MPLS-TP). This work is now being pursued in a joint effort.

MPLS-TP enables the deployment of packet-based transport networks that efficiently scale to support packet services in a simple and cost-effective way. MPLS-TP combines the necessary existing capabilities of MPLS with additional minimal mechanisms in order that it can be used in a transport role. MPLS-TP has the same objectives and is thus based on some of the same architectural concepts as existing transport network technologies such as SDH, SONET and OTN.

A number of RFCs have already been published on the subject, and even more are in an Internet Draft status. Some key published RFCs are listed below:

- RFC 5586 [i.20] - MPLS Generic Associated Channel
- RFC 5654 [i.21] - Requirements of an MPLS Transport Profile
- RFC 5860 [i.22] - Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks
- RFC 5921 [i.23] - A Framework for MPLS in Transport Networks
- RFC 5950 [i.24] - Network Management Framework for MPLS-based Transport Networks
- RFC 5960 [i.25] - MPLS Transport Profile Data Plane Architecture

The extensions provided to MPLS by the MPLS-TP project are aimed primarily at addressing the operational, administrative, and management needs of transport operators. MPLS-TP is also enhanced to meet transport network resiliency requirements.

The potential use of MPLS-TP in a satellite networking context has received very limited attention so far. This is probably due to the currently still evolving state of MPLS-TP, and the fact that transport networks are typically concerned with traffic volumes that far exceed the capabilities of satellite networks. Nevertheless, it seems worthwhile to study, e.g. whether or not (MPLS enabled) BSM networks could benefit from some of the MPLS-TP features. For example, it is conceivable that current OAM, network management, traffic engineering and resiliency procedures could be significantly enhanced by incorporating certain features already defined in MPLS-TP. Such an analysis is however beyond the scope of the present document.

# Annex C (informative): Bibliography

ETSI TR 101 985: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite".

IETF RFC 3468: "Decision on MPLS signalling protocols".

IETF RFC 3468: "The MPLS WG decision on signalling protocols".

IETF RFC 3479: "Fault Tolerance for LDP".

IETF RFC 3945: "GMPLS Architecture".

IETF RFC 3985: "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture".

IETF RFC 4204: "Link Management Protocol (LMP)".

IETF RFC 4875: "RSVP-TE for PtMP TE LSPs".

IETF RFC 5462: "MPLS Label Stack Entry - EXP Field renamed to Traffic Class Field".

# History

| Document history | | |
|---|---|---|
| V1.1.1 | July 2011 | Publication |
| | | |
| | | |
| | | |
| | | |