International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1714

(01/2007)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Operation, administration and maintenance

MPLS management and OAM framework

ITU-T Recommendation Y.1714

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	**Y.1700–Y.1799**
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation Y.1714

MPLS management and OAM framework

Summary

ITU-T Recommendation Y.1714 covers MPLS user-plane operation, administration and maintenance, control plane aspects and TMN aspects of MPLS management. Specifically, the mechanisms covered in this Recommendation are being worked on at different standard bodies mainly ITU-T and IETF.

This Recommendation focuses on MPLS technology specific OAM aspects of the TMN model of ITU-T Rec. M.3010. The Recommendation scope is limited to those components and interfaces that interface between network elements (user and control plane), and between network elements and EMS, NMS systems.

Source

ITU-T Recommendation Y.1714 was approved on 13 January 2007 by ITU-T Study Group 13 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

This Recommendation is an umbrella Recommendation to progress work on all aspects of multiprotocol label switching (MPLS) management. This Recommendation covers MPLS user-plane operation, administration and maintenance (OAM), control plane aspects, and TMN aspects of MPLS management. It is recognized that the scope of this work crosses many ITU-T Study Groups and Questions as well as other standard bodies.

Many aspects of MPLS management have been worked concurrently with the preparation of this Recommendation. Those specific aspects of management not ready for normative reference at the time of issue will be addressed via normal ITU document update procedures and are identified in this Recommendation as "for further study".

ITU-T Recommendation Y.1714

MPLS management and OAM framework

1 Scope

This Recommendation covers MPLS user-plane operation, administration and maintenance, control plane aspects and TMN aspects of MPLS management. The mechanisms covered in this Recommendation are being worked on at different standard bodies mainly ITU-T and IETF.

This Recommendation focuses on MPLS technology specific OAM aspects of the TMN model of [ITU-T M.3010]. The Recommendation scope is limited to those components and interfaces that interface between network elements (user and control plane), and between network elements and EMS, NMS systems (the 'Q' interface).

The following diagram (Figure 1) shows the scope of this Recommendation and interaction with other ITU-T Study Groups and standard bodies.

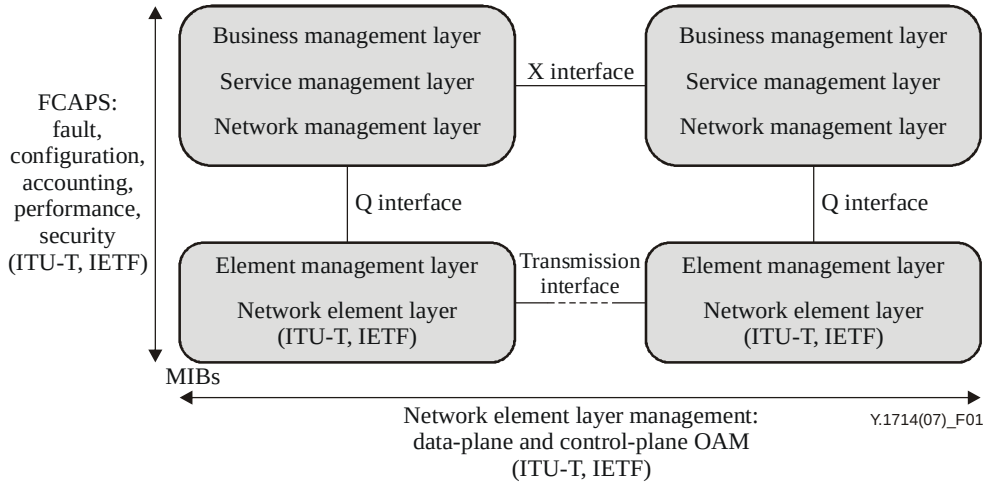

Figure 1 – Generic TMN model

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.8110] ITU-T Recommendation G.8110/Y.1370 (2005), *MPLS layer network architecture*.

[ITU-T I.610] ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

[ITU-T M.3010] ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

[ITU-T Q.933] ITU-T Recommendation Q.933 (2003), *ISDN Digital Subscriber Signalling System No. 1 (DSS1) – Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*.

[ITU-T X.84] ITU-T Recommendation X.84 (2004), *Support of frame relay services over MPLS core networks*.

[ITU-T Y.1411] ITU-T Recommendation Y.1411 (2003), *ATM-MPLS network interworking – Cell mode user plane interworking*.

[ITU-T Y.1561] ITU-T Recommendation Y.1561 (2004), *Performance and availability parameters for MPLS networks*.

[ITU-T Y.1710] ITU-T Recommendation Y.1710 (2002), *Requirements for Operation and Maintenance functionality in MPLS networks*.

[ITU-T Y.1711] ITU-T Recommendation Y.1711 (2004), *Operation and Maintenance mechanism for MPLS networks*.

[ITU-T Y.1712] ITU-T Recommendation Y.1712 (2004), *OAM functionality for ATM-MPLS interworking*.

[ITU-T Y.1713] ITU-T Recommendation Y.1713 (2004), *Misbranching detection for MPLS networks*.

[ITU-T Y.1720] ITU-T Recommendation Y.1720 (2003), *Protection switching for MPLS networks*.

[ITU-T Y.2011] ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for next generation networks*.

[IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[IETF RFC 2206] IETF RFC 2206 (1997), *RSVP Management Information Base using SMIv2*.

[IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

[IETF RFC 3036] IETF RFC 3036 (2001), *LDP Specification*.

[IETF RFC 3107] IETF RFC 3107 (2001), *Carrying Label Information in BGP-4*.

[IETF RFC 3209] IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP tunnels*.

[IETF RFC 3212] IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP*.

[IETF RFC 3478] IETF RFC 3478 (2003), *Graceful Restart Mechanism for Label Distribution Protocol*.

[IETF RFC 3479] IETF RFC 3479 (2003), *Fault Tolerance for the Label Distribution Protocol (LDP)*.

[IETF RFC 3811] IETF RFC 3811 (2004), *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*.

[IETF RFC 3812] IETF RFC 3812 (2004), *Multiprotocol Label Switching* (*MPLS) Traffic Engineering (TE) Management Information Base (MIB)*.

[IETF RFC 3813] IETF RFC 3813 (2004), *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*.

[IETF RFC 3814] IETF RFC 3814 (2004), *Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)*.

[IETF RFC 3815] IETF RFC 3815 (2004), *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP).*

[IETF RFC 3985] IETF RFC 3985 (2005), *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture.*

[IETF RFC 4090] IETF RFC 4090 (2005), *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*.

[IETF RFC 4221] IETF RFC 4221 (2005), *Multiprotocol Label Switching (MPLS) Management Overview*.

[IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.

[IETF RFC 4377] IETF RFC 4377 (2006), *Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks.*

[IETF RFC 4378] IETF RFC 4378 (2006), *A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM).*

[IETF RFC 4379] IETF RFC 4379 (2006), *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 control plane: [ITU-T Y.2011].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 user plane: This refers to the set of traffic forwarding components through which traffic flows.

NOTE – "User plane" is also referred to as "transport plane" in other ITU-T Recommendations.

3.2.2 network supervisory function: It is a function, which coordinates a set of mechanisms to monitor the defect state of the LSP.

3.2.3 link protection: In this type of protection, during the failure, all the LSPs using the protected link as an output interface are rerouted over the single backup LSP. A backup LSP that bypasses a single link of the protected LSP is called next hop (NHOP) bypass LSP.

3.2.4 node protection: Node protection is similar to link protection except that the destination of the backup LSP is a node further downstream the point of failure. Typically node protection is using the next node downstream the point of failure, in this case the backup LSP is known as the "next next hop (NNHOP) bypass LSP".

When a node failure occurs, the LSPs are rerouted completely around the failed node.

3.2.5 path protection: Path protection provides end-to-end protection from source to tail for a given LSP. More details can be found in [ITU-T Y.1720].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CE	Customer Edge
CsC	Carrier's Carrier
eBGP	External BGP
FEC	Forwarding Equivalent Class
FR	Frame Relay
FTN	FEC-to-NHLFE
IGP	Interior Gateway Protocol
IP	Internet Protocol
IWF	Interworking Function
LDP	Label Distribution Protocol
LSP	Label Switched Path
LSR	Label Switched Router
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmit Unit
NHLFE	Next Hop Label Forwarding Entry
NHP	Next Hop
NNHP	Next Next Hop
OAM	Operation, Administration and Maintenance
PE	Provider Edge
POS	Packet Over Sonet
RRO	Record Route Object
RSVP	Resource Reservation Protocol
TDM	Time Division Multiplexing
TE	Traffic Engineering
TMN	Telecommunications Management Network
VCCV	Virtual Channel Connectivity Verification
VPN	Virtual Private Network

5 Conventions

None.

6 Network models

The network models include the cases where MPLS based networks constitute the core part of the service networks while other layer 2 technologies (e.g., ATM, frame relay, Ethernet, etc.) are used to convey end-to-end services which are the client layer of the MPLS portion. Examples include MPLS based IP-VPN [IETF RFC 4364], ATM (or any layer 2 technologies such as Ethernet or frame relay), MPLS network, interworked network that has MPLS core network in the middle of the end-to-end layer 2 connections, and networks that convey voice signals by MPLS backbone (known as voice over MPLS).

6.1 MPLS infrastructure

[IETF RFC 3031] defines the MPLS architecture, where packets get assigned to a particular forwarding equivalent class (FEC) when entering the network. [ITU-T G.8110] is the corresponding ITU-T reference for MPLS architecture as defined in [IETF RFC 3031]. The FEC to which the packet is assigned is then encoded as a label. At subsequent hops, there is no further analysis of the packet's network layer header. Rather, the label is used as an index into a table which specifies the next hop and a new label. The old label is replaced with the new label, and the packet is forwarded to its next hop. MPLS architecture specifies that each label switched router (LSR) in the MPLS backbone informs each other of the label/FEC bindings it has made. This set of procedure is known as label distribution protocol. The label distribution protocol also encompasses any negotiations in which two label distribution peers need to engage in order to learn of each other's MPLS capabilities. Two LSRs which use a label distribution protocol to exchange label/FEC binding information are known as "label distribution peers" with respect to the binding information they exchange.

The MPLS architecture does not specify a single label distribution protocol. The choice of label distribution protocol depends on the goal to be achieved. In certain cases, it is desirable to bind label to forwarding equivalent classes which can be identified with routes to address prefixes via LDP [IETF RFC 3036], BGP [IETF RFC 3107]. Similarly, when resource reservation is required along the path, particularly those related to traffic engineering, it is desirable to set up an explicitly routed path, from ingress to egress via specific label distribution protocol such as RSVP-TE [IETF RFC 3209] or CR-LDP [IETF RFC 3212].

Support for MPLS traffic engineering LSPs between different interior gateway protocol (IGP) areas or across autonomous systems is achieved via some enhancements in the RSVP-TE signalling and label distribution protocol (see [b-IETF RFC 4105]).

MPLS architecture allows also the n–1 LSR in a label switched path to pop the label and forward the packet based on information gained from its network layer. This is known as penultimate hop popping and allows the egress LSR to perform only one lookup (instead of two lookups).

6.2 Interworking LSP

An interworking LSP is an MPLS LSP augmented with adaptation information to permit the essential attributes of a service (such as T1 leased line, ATM, or frame relay) to be emulated over a packet switched network. An interworking LSP is equivalent to a pseudowire label construct as defined in [IETF RFC 3985].

An interworking LSP is intended to provide the necessary functionality to emulate the service with the required degree of faithfulness. Any switching, translation or other operation requiring knowledge of the payload semantics is the responsibility of the interworking function.

Figure 2 illustrates the generic reference model for a "native service" (NS) over MPLS where the "native service" can be any of ATM, frame relay, TDM, Ethernet, etc.

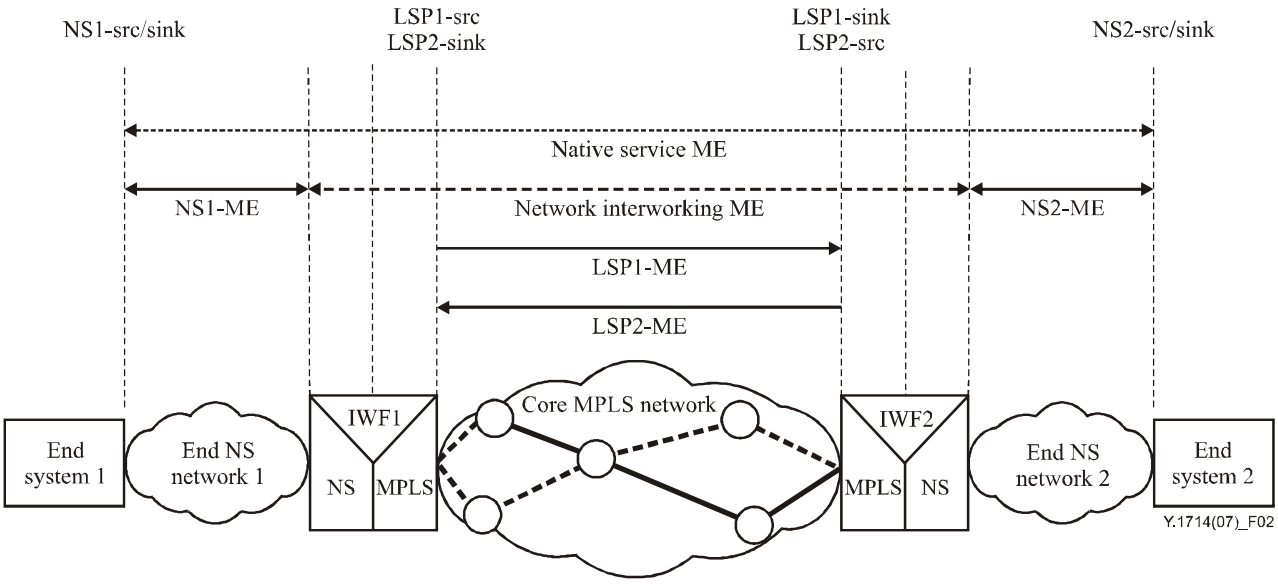

Figure 2 – Reference model for interworking LSP networks

The required functions of interworking LSPs include encapsulating service-specific bit-streams, cells or PDUs arriving at an ingress port, and carrying them across a path or tunnel. In some cases, it is necessary to perform other operation such as managing their timing and order, to emulate the behaviour and characteristics of the service to the required degree of faithfulness.

From the perspective of an end system, the interworking LSP is characterized as an unshared link or circuit of the chosen service.

Figure 2b describes the reference architecture for interworking LSP networks based on [b-ITU-T G.805] functional model.

[ITU-T Y.1711] and MPLS LSP ping and LSP trace define OAM mechanisms for the transport LSP. However, the interaction procedures at an interworking function between the transport LSP and the native service are for further study.

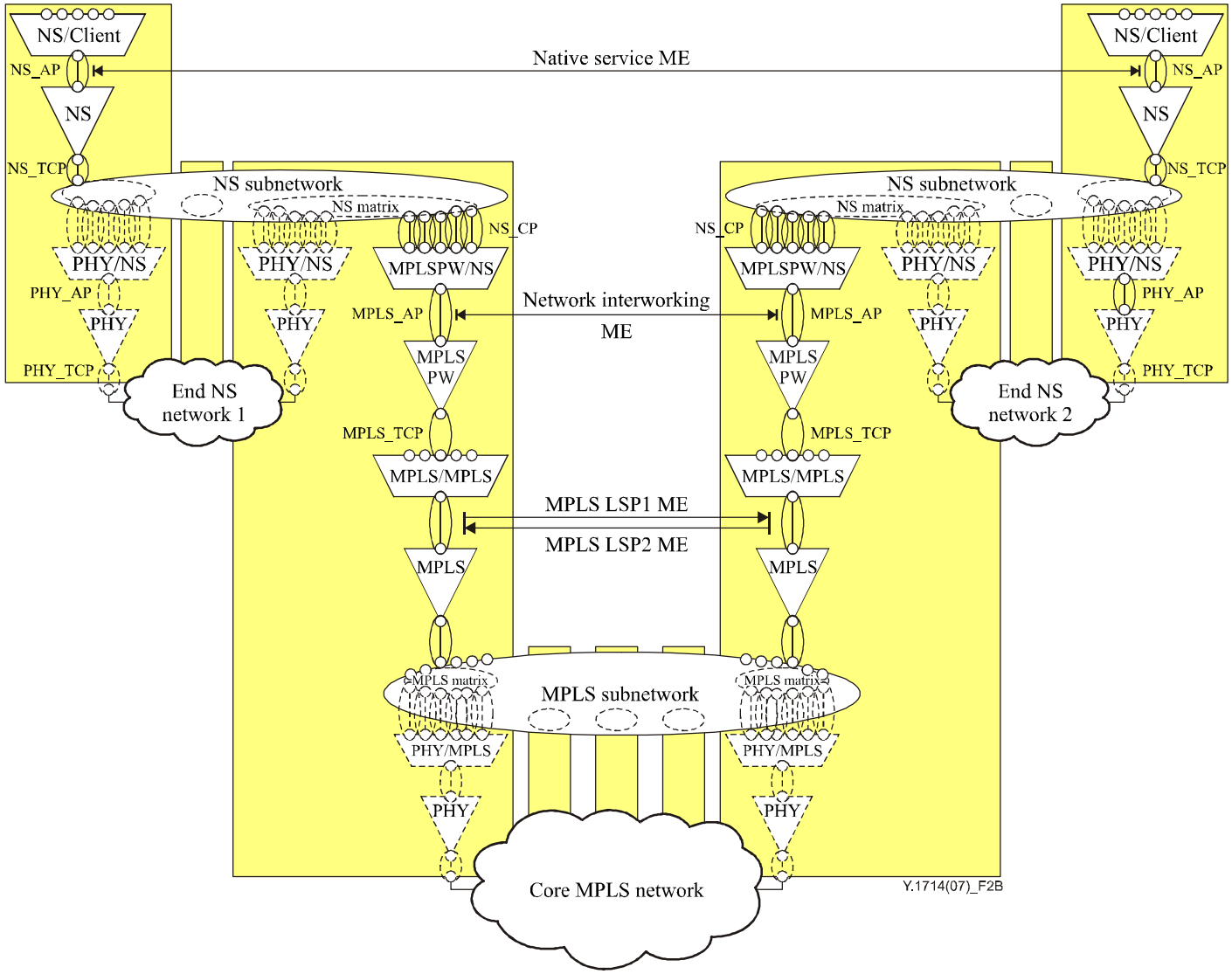

Figure 2b – Reference architecture for interworking LSP networks based on G.805

6.3 ATM-MPLS network

Figure 2 applied to ATM defines the generic reference model for ATM-MPLS network interworking. MPLS OAM functions and those of client layer should be independent of each other. [ITU-T Y.1712] recommends an ATM/MPLS specific instantiation. In this case, OAM functions for ATM networks are defined by [ITU-T I.610] and [ITU-T Y.1711] defines OAM for MPLS. Diagnostic functions are for further study.

NOTE – [ITU-T Y.1712] also documents OAM IWF procedures for the layer network interworking (service interworking) scenario that is outside the scope of this Recommendation.

6.4 L3 VPN MPLS networks

[IETF RFC 4364] describes a method by which an MPLS backbone can be used to provide IP VPNs (virtual private networks). This method uses a "peer model", in which the customers' edge routers ("CE routers") send their routes to the backbone edge routers ("PE routers"). BGP is then used in the core to exchange the routes of a particular VPN among the PE routers that are attached to that VPN. This is done in a way which ensures that routes from different VPNs remain distinct and separate, even if two VPNs have an overlapping address space. Figure 3 illustrates the L3 VPN relationship in an MPLS environment.

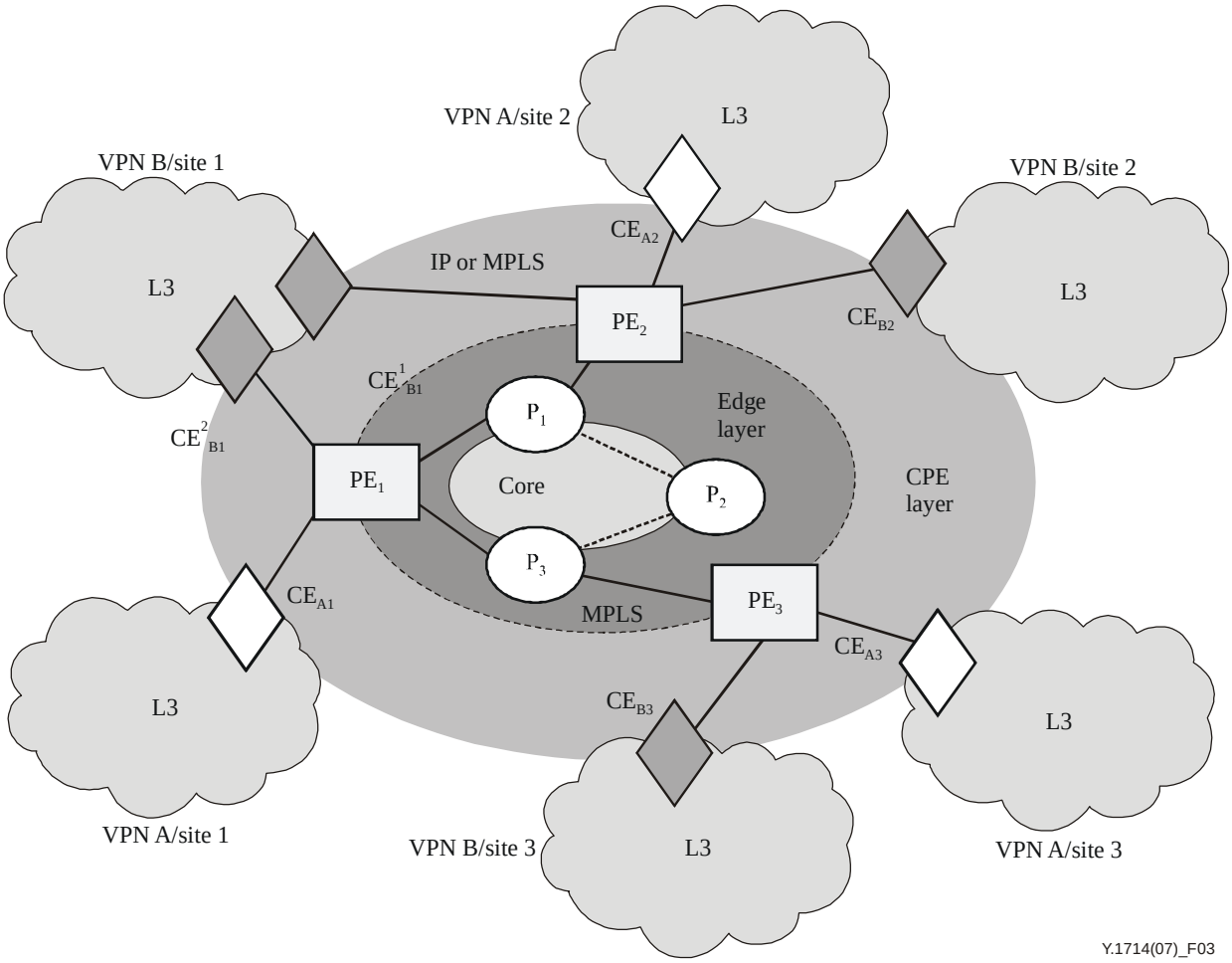

Figure 3 – Reference model for L3 VPN over MPLS network

The VPN sites might be also sometime a network of a service provider, which will then offer VPN service to its end customers. In this case, it is necessary that the CE routers support MPLS. This model is known as carrier's carrier (CsC). The principal is the exact same as for the "normal" MPLS L3 VPN. Similarly, although the VPN may be a transit network for routes outside of the customer's VPN, it does not normally participate in routing exchange for those external routes. There is no actual peering between the PE and the CE. The provider portion of the VPN does not appear as a distinct autonomous system to the routing system nor counts separately in transit metrics. The CE only needs to distribute routes that are internal to the VPN to the PE. Non-BGP speakers in the customer network are expected to have default routes to the customer's BGP speakers.

A further variation of the MPLS L3 VPN is the situation where two sites of a VPN are connected to different autonomous systems (this might be the case, for example, when the VPNs are connected to two different service providers).

There are four methods to provide L3 VPN MPLS connectivity between autonomous systems:

1) Virtual routing forwarding-to-virtual routing forwarding connections at the autonomous system border routers.
2) eBGP redistribution of labelled VPN-IPv4 routes from AS to neighbouring AS.
3) Multihop eBGP redistribution of labelled VPN-IPv4 routes between source and destination ASs, with eBGP redistribution of labelled IPv4 routes from AS to neighbouring AS.
4) To improve scalability, one can have the multi-hop eBGP connections exist only between a route reflector in one AS and a route reflector in another.

6.5 L2 VPN MPLS networks

For further study.

7 Related Recommendations and context

NOTE – This clause does not apply to the interworking LSP.

7.1 User plane aspects

7.1.1 Requirements for MPLS user-plane management

[ITU-T Y.1710] and [IETF RFC 4377] provide requirements for MPLS user plane management. [IETF RFC 4378] provides framework for MPLS user plane management.

7.1.2 MPLS availability definition and fault management mechanisms

One of the following mechanisms can be used for fault management:

1) [ITU-T Y.1711] provides a point-to-point availability definition and defines supporting protocol tools for availability measurement, fault detection, and fault notification (including alarm management).
2) Bidirectional forwarding detection (BFD) is a protocol intended to detect faults in the bidirectional path between two forwarding engines, with potentially very low latency, and can be used in addition to MPLS LSP ping for detection of data plane failures. A description is provided in Appendix IV.
3) [ITU-T Y.1561] defines parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability, and availability of packet transfer over an LSP on a multiprotocol label switching (MPLS) network. The defined parameters apply to end-to-end, point-to-point and multipoint-to-point LSP, and to any MPLS domain that provides or contributes to the provision of packet transfer services.

7.1.3 MPLS misbranching detection

FEC-CV, specified in [ITU-T Y.1713], provides a mechanism to detect data plane misforwarding of packets between LSPs not monitored via Y.1711 mechanisms, and between unmonitored and monitored LSPs.

7.1.4 Diagnostic tools

One of the following mechanisms can be used as a diagnostic tool depending on the label switched path:

1) LSP ping [IETF RFC 4379] can be used for data plane ping and trace capability. LSP ping is a diagnostic tool that can be used to verify unidirectional connectivity as well as path tracing of MPLS label switched paths. LSP ping is an UDP/IP based tool that applies to both point-to-point and multipoint-to-point LSPs. Furthermore, it has capabilities to support ECMP and PHP.

2) Virtual channel connectivity verification (VCCV) in conjunction with LSP ping may be used as a diagnostic tool over interworking LSPs. VCCV provides a mechanism to diagnose data plane misforwarding of packets between interworking LSPs. This is accomplished by providing a control channel associated with each interworking LSP. A description is provided in Appendix II.

3) LSR self test defines a means of self test for a label switched router (LSR) to verify that its data plane is functioning for certain key multiprotocol label switching (MPLS) applications including unicast forwarding based on LDP and traffic engineering tunnels based on RSVP-TE. A description is provided in Appendix II.

7.1.5 Defects

[ITU-T Y.1711] defines MPLS defects which reflect:

– Absolute loss of connectivity between the trail source and sink points.

– Misforwarding problems that have an absolute impact on the transfer characteristics of one or more P2P LSPs.

[ITU-T Y.1713] augments this list with defects observed via the misforwarding of LSPs and hence mis-forwarding of OAM probes for unmonitored LSPs (P2P or MP2P) that indirectly indicate absolute loss of connectivity between a source and sink point in the network.

There are additional defect conditions that are not explicitly path related and may only impact a portion of the traffic transported by an LSP. These may not be measurable via the use of OAM probing techniques for fault management as they manifest themselves as performance management problems. These will not be reflected as defects in the absolute connectivity sense but would impact the availability models defined in [ITU-T Y.1561] as they will appear as errored packet outcomes. These are:

7.1.5.1 MTU exceeded

MPLS does not have a fragmentation mechanism and the MTU of the current LSP for a FEC is not always known at the LSP ingress. This results in packets in the core that cannot be fragmented and cannot be forwarded. These will appear to the management system as discarded packets via the LSR MIB performance tables.

7.1.5.2 Congestive packet loss

Congestive packet loss occurs when the offered load on a link exceeds the link capacity and is sustained such that the available buffering is exceeded at an LSR in the forwarding path. These will appear to the management system as discarded packets via the LSR MIB performance tables.

7.1.5.3 Misordering

Misordering is instrumented for interworking LSPs that employ a control word containing a sequence number. Frequently implementations will discard PDUs received out of sequence, therefore misordering will appear as packet discard at the egress interworking LSR. Packets discarded due to out of order delivery are not specifically counted in any of the currently defined MIBs, therefore these will appear identically to congestive loss in the network to the management system.

NOTE – These are not explicitly identified as misordering discards in the current management information models.

7.2 Data plane recovery mechanisms

7.2.1 MPLS layer protection switching

Protection can be either end-to-end (path protection) or local (fast reroute).

7.2.1.1 Path protection

[ITU-T Y.1720] describes a path protection mechanism for 1+1 and 1:1 scenarios.

Shared mesh mechanisms whereby protection resources are shared between multiple working entities are for further study.

7.2.1.2 Local protection via fast reroute mechanism

Fast reroute, as described in [IETF RFC 4090], is a mechanism to address link and node failure using local repair. It could be used to protect multiple LSPs using a single backup tunnel. Furthermore, it has capabilities to reroute LSPs independently. Fast reroute has also the capability to support identical bandwidth between protected and protection LSPs. Fast reroute applies only to RSVP-TE signalled LSPs.

7.3 Control plane aspects

7.3.1 Detection of control plane failures

Detection of control plane failures is for further study.

7.3.2 Recovery from control plane failures

Specified procedures exist to recover from non-catastrophic control plane outages without having to interrupt the data plane connectivity and re-instantiate data plane state.

Control plane recovery for LDP signalling protocol can be achieved by means of graceful restart, as described in [IETF RFC 3478] combined with failover mechanism outlined in [IETF RFC 3479].

For BGP session, as specified in [IETF RFC 4364], graceful restart for MPLS allows to minimize the negative effects on MPLS forwarding caused by the label switching router's control plane restart.

7.3.3 Control plane diagnostic tools

RSVP-TE record route object (RRO), as described in [IETF RFC 3209], provides information indicating the actual routing of a P2P LSP set up with RSVP-TE. RRO can be compared with data plane diagnostic tool output.

7.4 Management aspects

7.4.1 MPLS textual conventions (MPLS TC) MIB

MPLS TC MIB contains textual conventions to represent commonly used MPLS management information. The textual conventions should be imported by MIB modules which manage MPLS networks [IETF RFC 3811].

7.4.2 MPLS management overview

The MPLS management overview document [IETF RFC 4221] describes the management architecture for MPLS and indicates the inter-relationships between the different MIB modules used for MPLS network management. Appendix III provides further details on the different MIB modules.

7.4.3 MIBs for user plane management

7.4.3.1 MPLS label switching router MIBs

The MPLS data plane is managed with the MPLS label switched router MIB [IETF RFC 3813]. It describes managed objects to configure and/or monitor an MPLS label switched router.

7.4.3.2 FTN MIB

The LSR FTN (FEC-to-NHLFE) MIB which directs the mapping of FECs onto LSPs in an LSR is managed via the FTN MIB [IETF RFC 3814].

It describes managed objects for defining, configuring and monitoring forwarding equivalence class (FEC) to next hop label forwarding entry (NHLFE) mappings and corresponding actions for use with multiprotocol label switching.

7.4.4 MIBs for control plane management

7.4.4.1 MPLS label distribution protocol MIBs

The MPLS label distribution protocol (LDP) control plane is managed with the label distribution protocol MIB [IETF RFC 3815].

7.4.4.2 MPLS-TE MIB

The MPLS-traffic engineering (MPLS-TE) control plane is managed via the MPLS-TE MIB [IETF RFC 3812].

7.4.4.3 RSVP MIB

The RSVP MIB defines a portion of the management information base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing the resource reservation protocol (RSVP) within the interface attributes defined in the integrated services model [IETF RFC 2206].

7.5 Security

This Recommendation introduces no new security issues into the MPLS architecture. The reader is directed to the specific specifications referred herein for specific security issues.

7.5.1 User plane management functions

For BGP/IP or MPLS IP VPNs [IETF RFC 4364], the data plane traffic separation is achieved by the ingress PE prepending a VPN-specific label to the packets. The packets with the VPN labels are sent through the core to the egress PE, where the VPN label is used to determine the correct VPN. Given the addressing, routing and traffic separation across a BGP/MPLS IP VPN core network, it can be assumed that this architecture offers in this respect the same security as comparable layer-2

VPNs such as ATM or frame relay. It is not possible to intrude from a VPN or the core into other VPNs through the BGP/MPLS IP VPN network, unless this has been configured specifically. Between two non-intersecting layer 3 VPNs of a VPN service, it is assumed that the address space between different VPNs is entirely independent. This means that, for example, two non-intersecting VPNs must be able to both use the 10/8 network (non-pubic address) without any interference.

In addition, traffic from one VPN must never enter another VPN. This includes separation of routing protocol information, so that also routing tables are separate per VPN.

Specifically:

- Any VPN must be able to use the same address space as any other VPN.
- Any VPN must be able to use the same address space as the MPLS core.
- Traffic from one VPN must never flow to another VPN.
- Routing information, as well as distribution and processing of that information, for one VPN instance must be independent from any other VPN instance.

From a security point of view, the basic requirement is to avoid that packets destined to a host within a given VPN reach a host with the same address in another VPN or the core, or get routed to another VPN even if the host address does not exist there.

7.5.2 Control plane management functions

Control plane management functions are for further study.

7.5.3 Management plane

Management plane security is for further study.

7.6 OAM relationship between client layers and MPLS server layer

Network interworking and service interworking are within the scope of this clause.

7.6.1 IP-MPLS interworking

IP ping and IP traceroute based on Internet control message protocol [IETF RFC 792] can be used across the interworking point. Other IP-MPLS interworking mechanisms are for further study.

7.6.2 ATM-MPLS interworking

[ITU-T Y.1712] defines interworking procedures between networks based on [ITU-T I.610] and [ITU-T Y.1711] for ATM over MPLS (as defined in [ITU-T Y.1411] or similar procedures).

7.6.3 FR-MPLS interworking

1) **Frame relay 1:1 mode**

   OAM interworking for FR-MPLS in 1:1 mode is for further study.

2) **Frame relay port mode**

   The PVC status indication as defined in [ITU-T Q.933] is transported transparently between the PEs. However, mapping of a failure of the MPLS transport LSP is for further study in [ITU-T X.84].

7.6.4 Ethernet-MPLS interworking

OAM interworking for Ethernet-MPLS is for further study.

7.6.5 Voice-MPLS interworking

OAM interworking and management aspects are for further study.

8 MPLS TMN aspects

8.1 MPLS network supervisory function

MPLS network supervisory function coordinates the MPLS network management functions that fall within the scope of this Recommendation. These functions include:

- MPLS label switch path fault detection and diagnostics;
- diagnostic tools;
- MPLS layer protection switching;
- MPLS layer rerouting;
- MPLS MIBs.

Appendix I

Detection of data plane defects

(This appendix does not form an integral part of this Recommendation)

Data plane defects fall into three categories, transmission interface failures, node failures and path failures.

I.1 Detection of transmission interface failures

Link layer failure manifests itself as loss of light/carrier or higher order faults such as framing or error detection failures. Similarly some transport networks that carry MPLS (e.g., for packet over sonet (POS) as outlined in [b-IETF RFC 1619]) provide their own OAM (e.g., LCP ECHO).

I.2 Detection of node failures

Traditionally, failure of control plane adjacencies has been used to "proxy" detection of forwarding plane and to detect node failures. This technique makes sense in networks based on a connectionless forwarding but makes less sense in networks based on connection-oriented (either packet or circuit switched) forwarding mode or those where the control and data planes are disjoint. Examples include:

- *LDP [IETF RFC 3212]/CR-LDP [IETF RFC 3209] Adjacency*

  LDP incorporates a hello exchange that is used to artificially add traffic between LDP/CR-LDP peers in the absence of other traffic. This is combined with an activity timeout.

- *RSVP-TE [IETF RFC 3209] Adjacency*

  RSVP TE has been augmented with a hello exchange between peer RSVP-TE entities that can be used to detect failure.

- *IGP/EGP Adjacency*

  OSPF [b-IETF RFC 2328] etc. all have hello exchanges.

However, the explosion of software complexity and increasing sophistication of control plane implementation has led to a trend whereby control plane protocol elements may uniquely fail without impacting forwarding. Further, they do so more frequently than the types of failures that control plane fault detection (e.g., keep-alives) originally proxied detection for.

What has evolved is an operational decoupling (or at least deferral) of the "fate sharing" between the control plane and the forwarding plane, and the definition of mechanisms to ensure transactional integrity and recovery of state of the control plane across control plane specific failures. This has led to distinct definitions of recoverable and unrecoverable node failures. Detection of an unrecoverable node failure has been delayed on the assumption that recoverable node failure (with associated survival of the forwarding plane) is the more common scenario. Support of control plane restart is usually negotiated between peers and such negotiation includes establishing hold off times to allow for graceful restart. [IETF RFC 3478] is an example of decoupling of control and forwarding plane.

I.3 Detection of path failures

Path failures manifest themselves in multiple forms:

- Breaks in the path caused by serving level/layer defects.
- Breaks in the path caused by current level defects.
- Misdirection of the path via unintended merging with another path.
- Misdirection of the path via unintended mislabelling of the path such that the downstream LSR does not have an incoming label map (ILM) entry for the path.
- In case of Y.1711 OAM CV messaging, identifying the CV PDU in a no-ILM condition and extracting the TTSI from the CV PDU provides identification of the defective LSP.

Appendix II

Diagnostic tools

(This appendix does not form an integral part of this Recommendation)

II.1 Virtual channel connectivity verification

Virtual channel connectivity verification (VCCV), as described in [b-pwe3-vccv], supports connection verification applications for PWs regardless of the underlying public service network technology. VCCV makes use of IP-based protocols to perform operations and maintenance functions. This is accomplished by providing a control channel associated with each PW. A network operator may use the VCCV procedures to test the network's forwarding plane liveliness.

II.2 Label switched router self test

Label switched router self test, as described in [b-mpls-lsr-self-test], provides the capability to verify that its data plane is functioning for certain key multiprotocol label switching (MPLS) applications, including unicast forwarding and traffic engineering tunnels. A new loopback forwarding equivalency class type is defined to allow an upstream neighbour to assist in the testing at very low cost. MPLS verification request and MPLS verification reply messages are defined to do the actual probing.

MPLS echo request and MPLS echo reply messages LSP ping messages are extended to do the actual probing. The pings are sent to an upstream neighbour, looped back through the LSR under test and intercepted, by means of TTL expiration by a downstream neighbour. Extensions to LSP ping are defined to allow the downstream neighbour to report the test results.

Appendix III

MPLS management capabilities

(This appendix does not form an integral part of this Recommendation)

III.1 MPLS data plane management

The MPLS label switched router MIB (LSR MIB) is designed to satisfy the following requirements and constraints:

1) The MIB supports LSP establishment via an MPLS signalling protocol (where the LSP parameters are specified using this MIB at the head end of the LSP and end-to-end LSP establishment is accomplished via signalling). The MIB also supports manually configured LSPs (i.e., those for which label associations at each hop of the LSP are provisioned by the administrator via this MIB).
2) The MIB supports the enabling and disabling of MPLS capability on MPLS capable interfaces of an LSR.
3) The MIB allows resource sharing between two or more LSPs, i.e., it allows specification of sharing of bandwidth and other LSR resources between different LSPs.
4) Both per-platform and per-interface label spaces are supported.
5) MPLS packets can be forwarded solely based on an incoming top label [IETF RFC 3031], [b-IETF RFC 3032].
6) Support is provided for next-hop resolution when the outgoing interface is a shared media interface. In the point-to-multipoint case, each outgoing segment can reside on a different shared media interface.
7) The MIB supports point-to-point, point-to-multipoint and multipoint-to-point connections at an LSR.
8) For multipoint-to-point connections, all outgoing packets can have the same top label.
9) For multipoint-to-point connections, the outgoing resources of the merged connections can be shared.
10) For multipoint-to-point connections, packets from different incoming connections can have distinct outgoing label stacks beneath the (identical) top label.
11) In the point-to-multipoint case, each outgoing connection has a distinct label stack including the top label.
12) All the members of a point-to-multipoint connection can share the resources allocated for the ingress segments.
13) The MIB provides cross-connect capability to "pop" an incoming label and forward the packet with the remainder of the label stack unchanged and without pushing any labels ("pop-and-go") [b-IETF RFC 3032].
14) The MIB supports persistent as well as non-persistent LSPs.
15) Performance counters are provided for in-segments and out-segments as well as for measuring MPLS performance on a per-interface basis.

III.2 MPLS LDP control plane management

The MPLS label distribution MIBs for user plane management are based on four main objects. These MIB modules are the MPLS-LDP-MIB, the MPLS-LDP-GENERIC-MIB, the MPLS-LDP-ATM-MIB and the MPLS-LDP-FRAME-RELAY-MIB.

1) The MPLS-LDP-MIB defines objects which are common to all LDP implementations.
2) The MPLS-LDP-GENERIC-MIB defines layer 2 per platform label space objects for use with the MPLS-LDP-MIB.
3) The MPLS-LDP-ATM-MIB defines layer 2 asynchronous transfer mode (ATM) objects for use with the MPLS-LDP-MIB.
4) The MPLS-LDP-FRAME-RELAY-MIB defines layer 2 frame-relay objects for use with the MPLS-LDP-MIB.

The MPLS-LDP-MIB module must be implemented and at least one of the layer 2 MIB modules must be implemented.

As an example, if an LSR implementation wants to support LDP utilizing a layer 2 of Ethernet, then the MPLS-LDP-MIB and the MPLS-LDP-GENERIC-MIB modules would be implemented.

If an LSR implementation wants to support LDP utilizing a layer 2 of ATM, then the MPLS-LDP-MIB module must be implemented and the MPLS-LDP-ATM-MIB module would be implemented.

If an LSR implementation wants to support LDP utilizing a layer 2 of FRAME-RELAY, then the MPLS-LDP-MIB module would be implemented and the MPLS-LDP-FRAME-RELAY-MIB module would be implemented. An LDP implementation that utilizes all three layer 2 media (Ethernet, frame relay, and ATM) would support all four MIB modules.

Appendix IV

Fault management

(This appendix does not form an integral part of this Recommendation)

IV.1 Bidirectional forwarding detection

Bidirectional forwarding detection (BFD), as described in [b-bfd-base] [b-bfd-mpls], provides a means to detect a MPLS LSP data plane failure similar to MPLS LSP ping [IETF RFC 4379]. However, the control plane processing required for BFD control packets is smaller than the processing required for LSP ping messages. A combination of LSP ping and BFD can be used to provide faster data plane failure detection and/or make it possible to provide such detection on a greater number of LSPs.

Bibliography

[b-ITU-T G.805] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

[b-IETF RFC 1619] IETF RFC 1619 (1994), *PPP over SONET/SDH*.

[b-IETF RFC 2328] IETF RFC 2328 (1998), *OSPF Version 2*.

[b-IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

[b-IETF RFC 4105] IETF RFC 4105 (2005), *Requirements for Inter-Area MPLS Traffic Engineering*.

[b-bfd-base] IETF draft, *Bidirectional Forwarding Detection*, draft-ietf-bfd-base-06.txt, March 2007.

[b-bfd-mpls] IETF draft, *BFD for MPLS LSPs*, draft-ietf-bfd-mpls-04.txt, March 2007.

[b-ccamp-inter-domain-framework] IETF draft, *A Framework for Inter-Domain MPLS Traffic Engineering*, draft-ietf-ccamp-inter-domain-framework-06.txt, August 2006.

[b-mpls-bgp-mpls-restart] IETF draft, *Graceful Restart Mechanism for BGP with MPLS*, draft-ietf-mpls-bgp-mpls-restart-05.txt, August 2005

[b-mpls-lsr-self-test] IETF draft, *LSR Self Test*, draft-ietf-mpls-lsr-self-test-07.txt, May 2007.

[b-pwe3-oam-msg-map] IETF draft, *Pseudowire (PW) OAM Message Mapping*, draft-ietf-pwe3-oam-msg-map-05.txt, March 2007.

[b-pwe3-vccv] IETF draft, *Pseudo Wire Virtual Circuit Connectivity Verification*, draft-ietf-pwe3-vccv-14.txt, July 2007.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007