A Need for Multiprotocol Label Switching Operation Administration Maintenance

Last updated: June 2007

As network operators converge their existing data (ie: Asynchronous Transfer Mode (ATM) and Frame Relay) and new IP VPN and access services (Ethernet) onto a common Multiprotocol Label Switching (MPLS)-based network infrastructure, there is an increasing need for monitoring and trouble shooting capabilities of end-to-end MPLS network connectivity. Especially, when the increasing stringent Service Level Agreement (SLA) requirements are considered for end-to-end network performance, jitter, and delay, driven by new services such as VoIP and video, the ability for Service Providers to efficiently detect, isolate, and troubleshoot end-to-end network performance and connectivity has become crucial to compete in the market place today.

MPLS Traffic Engineering, Any Transport over MPLS (AToM) and MPLS IP-VPNs are examples of services for which the ability to provide SLA testing and LSP integrity checking might be mandatory. Internet Control Message Protocol (ICMP) ping and applications such as Cisco IOS Service Assurance Agent (SAA) have traditionally conducted SLA testing and LSP integrity checking; however, MPLS Operation Administration and Maintenance (OAM) now plays a crucial role. Unlike a traditional transport network which offers bi-directional connectivity, MPLS provides a unidirectional network connectivity between two label edge routers [MPLS-RFC3031] and therefore OAM would need to be adapted/extended to cater for the specific need of MPLS whilst providing at the same time, the same service and look and feel as the one achieved by OAM for traditional network infrastructure such as TDM, ATM or Frame Relay.

Traditionally, ICMP ping has been commonly used to troubleshoot IP based networks. However, as an MPLS core network does have different behavior, ICMP ping will not be able to fully troubleshoot MPLS networks and does have some shortcomings such as:

- Inability to detect MPLS data plane failure, if IP layer works fine
- Inability to provide sufficient reply data to isolate fault for an MPLS specific issue

OAM generally comprises sets of procedures that diagnose and respond to failure, and test and measure SLAs within a given network. Diagnostics and tests are applicable to both data and control plane, whereas SLA measurement is more related to data plane. MPLS OAM is primarily focused on LSP liveliness check and hop-by-hop tracing, and IP SLA is targeted for end-to-end performance measurements.

As OAM is a very large framework, it is often challenging to offer the full set of functionalities. Moreover, OAM is sometimes “forgotten” during protocol design and OAM capabilities will be available after the roll out of the technology.

This document focuses on the requirements and existing solutions for OAM in an MPLS network. It also provides a feature-by-feature comparison between two existing solutions, which can be used for fault detection, isolation, and diagnostics:Y.1711 and MPLS Ping/Trace. Lastly, this white paper will introduce some of the latest work and status at the standardization level.

Motivations and Requirements

Maintaining core integrity is a critical part of identifying MPLS OAM. It is critical that the control plane and data plane are fully in sync in order to preserve the integrity of the end-to-end label switched path.

The primary objective is to reduce operational costs by minimizing service interruptions.
The adoption of OAM mechanisms will help reduce trouble resolution time. The latter, for example, permits NOC personnel to keep up with increasing, growing MPLS network infrastructures and increasing stringent network availability requirements.

Minimal requirements include, the ability to detect and diagnose a break in the LSP data path and identify the source of the failure. Control plane /data plane integrity validation is also highly critical.

MPLS OAM should satisfy the following requirements:

- **Separation between control plane and data plane OAM**

  Although MPLS control plane OAM functions may be available, network operators cannot rely exclusively on the control-plane to detect all user-plane defects. The userplane carrying customer traffic and the control-plane carrying the signaling protocols might not necessarily have the same path, nor the same processing within the Label Switches Routers (LSRs). Therefore, a situation could arise in which the data-plane could fail without affecting the control plane.

- **Detection, diagnosis, localization of broken LSPs**

  Any OAM solution must provide the capability to diagnose and detect broken LSPs, and to isolate the failed resource in the path. This is particularly true for misbranching defects, which are particularly difficult to specify recovery actions in an LDP network.

- **LSP tunnel trace capability**

  A tracing capability function is desired. Based on past experience (see IP trace), it was shown that this function helps to troubleshoot and isolate defects.

  It is expected that the path trace function returns the entire list of LSRs and links used by a certain LSP (or at least the set of LSRs/links up to the location of the defect) [hop by hop tracing]. Further, the tracing capability should include the ability to trace recursive paths, such as the use of nested LSPs, or the entrance and exit of LSPs to and from traffic-engineered tunnels. The path trace function must also be capable of diagnosing LSP mis-merging by permitting comparison of expected versus realized forwarding behavior at any LSR in the path. The path trace capability should be capable of being executed from both the head end LSR and any mid -point LSR.

- **The OAM mechanism should support Equal Cost Multi-Path (ECMP) LSPs.**

  ECMP scenarios appear when several LSPs can carry data from the head-end to the tail end. In this particular situation, the OAM mechanism should be able to exercise and verify all paths that could potentially transport data within a reasonable time frame.

  Unfortunately, there is no standard for the load-sharing algorithm, but it is important that any function be capable of detecting failures on all operational paths, as failure of any branch may lead to loss of traffic, regardless of the load-sharing algorithm

- **Ability to raise an alarm when failures are detected, without causing an alarm during a defect event in a lower layer.**

  Upon detection of a broken LSP, the correct alarm/notification should be sent to the LSRs or the network management system. For example, if the LSP is to carry Layer 2 circuits, a defect at the LSP level should not target multiple alarms at the Layer 2 level.

- **MPLS OAM functions should be backward-compatible and must support the existing infrastructure**

  MPLS is now widely deployed by Service Providers; therefore, any MPLS OAM solution must account for the existing equipment and further ensure seamless integration of this functionality.

- **Any OAM mechanism should offer SLA and performance measurement/management mechanisms**

  SLA mechanisms are required to measure different aspects of SLAs such as: jitter, latency, and packet loss. One extra parameter of interest for Service Providers is network availability and performance measurement. Performance measurement is an effective means of scanning the whole network at any time and systematically searching for errors, bottlenecks and suspicious behavior. Current transport networks rely heavily on end-to-end performance measurement which gives the operational group a very good understanding of the network behavior and performance. The definition of network availability and performance management parameters differ between providers; one may define it as a function of jitter, another of packet loss or latency.

Existing Solutions

While MPLS does provide native facilities (such as: Fast Reroute link/node protection, fault recovery, LDP graceful restart, LDP fast convergence.), which compliment the OAM framework, none of those features can detect and diagnose fault within the MPLS network. Such a tool is needed to seamlessly operate the MPLS network.

Two solutions are available: Y.1711 is a product of ITU and MPLS Ping/Traceroute a product [MPLS_PING] of the IETF. Each solution reflects the design philosophy of the community from which it originates. Note, as well that MPLS Ping/Traceroute is now part of ITU-T Y.1714 which is a generic framework on MPLS Management and OAM.

This section will quickly review the principles of each mechanism and will outline the applicability of each approach.

Y.1711

Y.1711 is based on connectivity verification packet flows, which are inserted in the network at the head-end of the LSP. Those packets are checked at the tail end. If a faulty condition is detected at the LSP, notifications are sent back to the head-end. Each LSP requires a state machine at its terminating LSRs (both head-end and tail-end LSR), which keep track of the default condition status. Those packets allow connectivity verification along the LSP being tested. This mechanism is mainly geared toward connected oriented point-to-point LSPs, like the one signaled by RSVP-TE.

This mechanism relies on the use of a specific MPLS label to identify the OAM packets. It uses Reserved label 14 [OAM_LABEL], which uniquely identifies Y.1711 OAM packets.

Therefore, OAM packets will carry two labels when transmitting within the MPLS network, the first one being the transport label and the second one label 14. One of the main requirements for an OAM mechanism is to ensure that the OAM packets use an identical path as the data packets being tested. This guarantees that the data path is alive and functional.

The mechanism defines three main packets: Connectivity Verification (CV), Forward Defect Indication (FDI), and Backward Defect Indication (BDI).

- **CV flows** are generated at the head-end and terminated on the tail-end of the LSP being tested every second. The CV packet contains a unique Trail Termination Source Identifier (TTSI), which is composed of the head-end LSR identifier and the LSP identifier.
- **FDI** is generated by any LSR that detects a defect. Its purpose is to inform all LSRs downstream of the defect about the defective condition. FDI is useful in the case of nested LSPs.
- **BDI flow** informs the head-end LSR that there is a defect at the LSP's tail-end LSR.

Further, Y.1711 assumes that there is an existing return path between the tail-end and the head-end. This return path can be either in band (LSP from Tail-end to Head-end LSRs) or out of band (ie: IP connection between Tail-end Head-end LSRs).

The OAM payload packet includes the OAM Function Type (1 octet), which identifies the packet type (ie: CV, FDI, BDI), the specific OAM function type data, TTSI (20 octets), and a BIP16 (2 octets) error detection mechanism. BIP 16 is close to the CRC function used for SONET, and necessitates heavy processing. Y.1711 OAM packets have a minimum payload length of 44 octets, which is similar to the length of ATM cells. CV, FDI, and BDI payload are shown in the figures below. Note that FDI and BDI payload includes a "Defect Type" and "Defect Location". Four possible defect types are defined in the MPLS network. Refer to [Y.1711] for additional information.

Table 1. FigureY.1711/1:CV payload structure

Function Type (01Hex)	Reserved (all 00Hex)	LSP Trail Termination Source Identifier	Padding (all 00Hex)	BIP16
1 octet	3 octets	20 octets	18 octets	2 octets

Table 2. Figure Y.1711/2: FDI payload structure

Function Type (02Hex)	Reserved (00Hex)	Defect Type	TTSI (optional, if not used set to all 00Hex)	Defect Location	Padding (all 00Hex)	BIP16
1 octet	1 octet	2 octets	20 octets	4 octets	14 octets	2 octets

Table 3. Figure Y.1711/3: BDI payload structure

Function Type (03Hex)	Reserved (00Hex)	Defect Type	TTSI (optional, if not used set to all 00Hex)	Defect Location	Padding (all 00Hex)	BIP16
1 octet	1 octet	2 octets	20 octets	4 octets	14 octets	2 octets

TTSI is defined as appending a 16 octet LSR ID IPv6 address followed by a 4 octet LSP Tunnel ID. For LSR, which does not have an IPv6 address, the IPv4 address is used after re-writing+padding it to fit within the 16 octets field. The 4 octets LSP ID field is most of the time, not enough to use for native information.

Table 4. Figure Y.1711/3: TTSI value

LSR ID	LSP ID
16 octets	4 octets

The use of the TTSI field requires a unique space to be managed across applications, and assumes that the LSRs should track the TTSI IDs within the database, therefore increasing memory requirements for those nodes. TTSI also implies that LSP IDs should be added to all forms of MPLS signaling.

Dealing with Equal Cost Multi Paths (ECMP)

When ECMPs exist within the MPLS network from the head-end to the tail-end, it is not possible to predict how the Load Balancing (LB) algorithm will “spread” the data across the multiple paths. When dealing with MPLS packets, some LB algorithm may use the IP information in the packet as a decision criterion, while others might use the inner MPLS label for a forwarding decision. Therefore, double labeling does not guarantee that the OAM packets are currently testing the data path. This violates one of the main requirements.

Penultimate Hop Popping and Non-compliant Routers

One can observe the protocol design to realize that the label (label 14), which identifies the OAM payload is used to carry the information up to the tail-end of a given LSP. When the MPLS network uses Penultimate Hop Popping (PHP), for the sake of optimization, the tailend LSR expects to receive an unlabeled packet from his upstream neighbor LSR. In this configuration, the use of the OAM label assumes that the tail-end LSR will pop and process this label+packet, even while using PHP. This requires a behavior change at the tail-end LSR level. Consider that PHP is widely used across the deployed MPLS network.

MPLS Ping/Traceroute

When an LSP fails to deliver user traffic, the failure cannot always be detected by the MPLS control plane. For the MPLS data plane verification, as a natural progression, the IP data plane verification tools (ie: ping and trace route) are extended to work on the MPLS networks. The MPLS Ping/Traceroute, modeled after the ping/traceroute paradigm: ping (ICMP echo request [ICMP]), is used for connectivity verifications, and traceroute is used for hop by-hop fault localization and path tracing.

LSP ping and LSP traceroute provide diagnostics and troubleshooting capabilities for MPLS LSPs. These tools provide basic building blocks for the MPLS OAM capabilities. This enables verification of the MPLS data plane consistency.

LSP ping is a data plane verification tool that verifies the LSP connectivity, and the integrity of the MPLS network. During the verification, ping packet reaches the end of the path, at which point it is sent to the control plane of the egress LSR, which then verifies that it is indeed an egress for the FEC. Currently, the following FECs are supported: LDP IPv4 prefix, LDP IPv6 prefix, RSVP IPv4 Session Query, RSVP IPv6 Session Query, VPN IPv4 prefix, VPN IPv6 prefix.

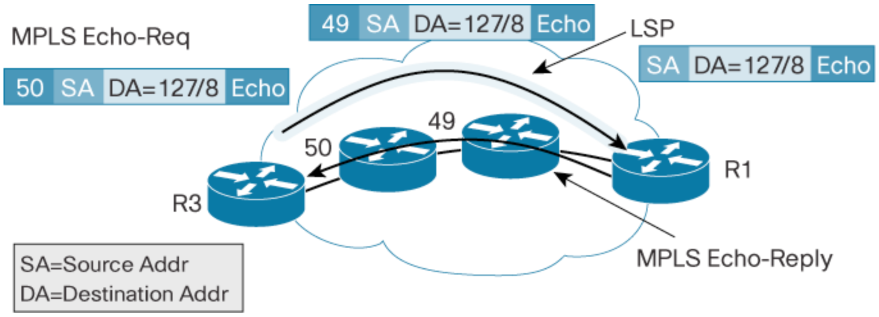
This mechanism is flexible enough to facilitate support of new FECs.

Ping mode can test the integrity of connectivity via the verification on the Forward Equivalence Class (FEC) entity between the ping origin and the egress node for this particular FEC. This test is carried out by sending an MPLS echo request along the same data path as other packets belonging to this FEC as shown in Figure Ping/1.

As such, it is forwarded like any packet that belongs to that FEC. The MPLS echo request contains information about the FEC whose MPLS path is being verified.

Once the MPLS request packet reaches the end of the path, the egress LSR verifies that it is an egress for the FEC and notifies the node that originated the MPLS echo request, with the appropriate return code.

Figure 1. Figure Ping/1: MPLS Ping/Traceroute Operation



LSP traceroute is a data plane verification tool that traces LSP paths in the MPLS network. In the trace route LSP verification, the packet is sent to the control plane of each transit LSR, which performs various checks to ensure that it is indeed a transit LSR for this path.

Traceroute mode is mainly used in fault isolation. Traceroute operation is performed via a manipulation on the TTL (starting at 1 and increment by 1). The LSR issuing the LSP trace originates an MPLS Echo-Request packet with a TTL starting at 1. In addition an object called “Downstream TLV” is also added to the Echo-Request packet. The packet is sent to the control plane of each transit LSR, which performs various checks, including one that determines if it is a transit LSR for this path. Furthermore, each transit LSR also returns extra information related to the FEC being tested (ie: label bound to the FEC, list of each interface over which this FEC could be forwarded) via the Downstream mapping object. This information helps in checking the control plane against the data plane, for example making sure that forwarding matches what the routing protocol determined as the path.

Theory of Operations

An MPLS echo request is a UDP packet that is sent to a target router using the appropriate label stack that is associated with the LSP to be tested. The destination address of the MPLS echo request UDP packet is different from the address used to select the label stack.

It is not used for forwarding. Instead, the IP destination address is defined as a 127/8 address and used to:

- Force the packet to be consumed by the router where a LSP breakage occurs
- Force processing of the packet at the terminal point of the LSP if the LSP is intact
- Influence load balancing during forwarding when the transit routers use destination address in the IP header for load balancing

A MPLS echo reply is sent in reply to a MPLS echo request. The mechanism allows the use of a different return path, which can be specified by the node that sends the echo request packet. Echo reply can be forwarded as an IP packet or MPLS LSP to the LSR that originates the MPLS echo request.

The MPLS echo request and replies are both UDP packets. This packet is MPLS forwarded (mainly for the echo request) within the MPLS network. Figure 2 illustrates the UDP packet payload.

Figure 2. Figure Ping/2: MPLS Echo Request/Reply UDP Payload

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Version Number        |         Must Be Zero          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Message Type |   Reply mode  |  Return Code  | Return Subcode|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sender’s Handle                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    TimeStamp Sent (seconds)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  TimeStamp Sent (microseconds)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  TimeStamp Received (seconds)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                TimeStamp Received (microseconds)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            TLVs ...                           |
.                                                               .
.                                                               .
.                                                               .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Message Type field identifies whether the UDP payload is an MPLS echo request or MPLS echo reply.

The sequence number is assigned by the originator of the MPLS echo request and returned in the MPLS echo reply unchanged. It enables users to track of any lost echo request packets.

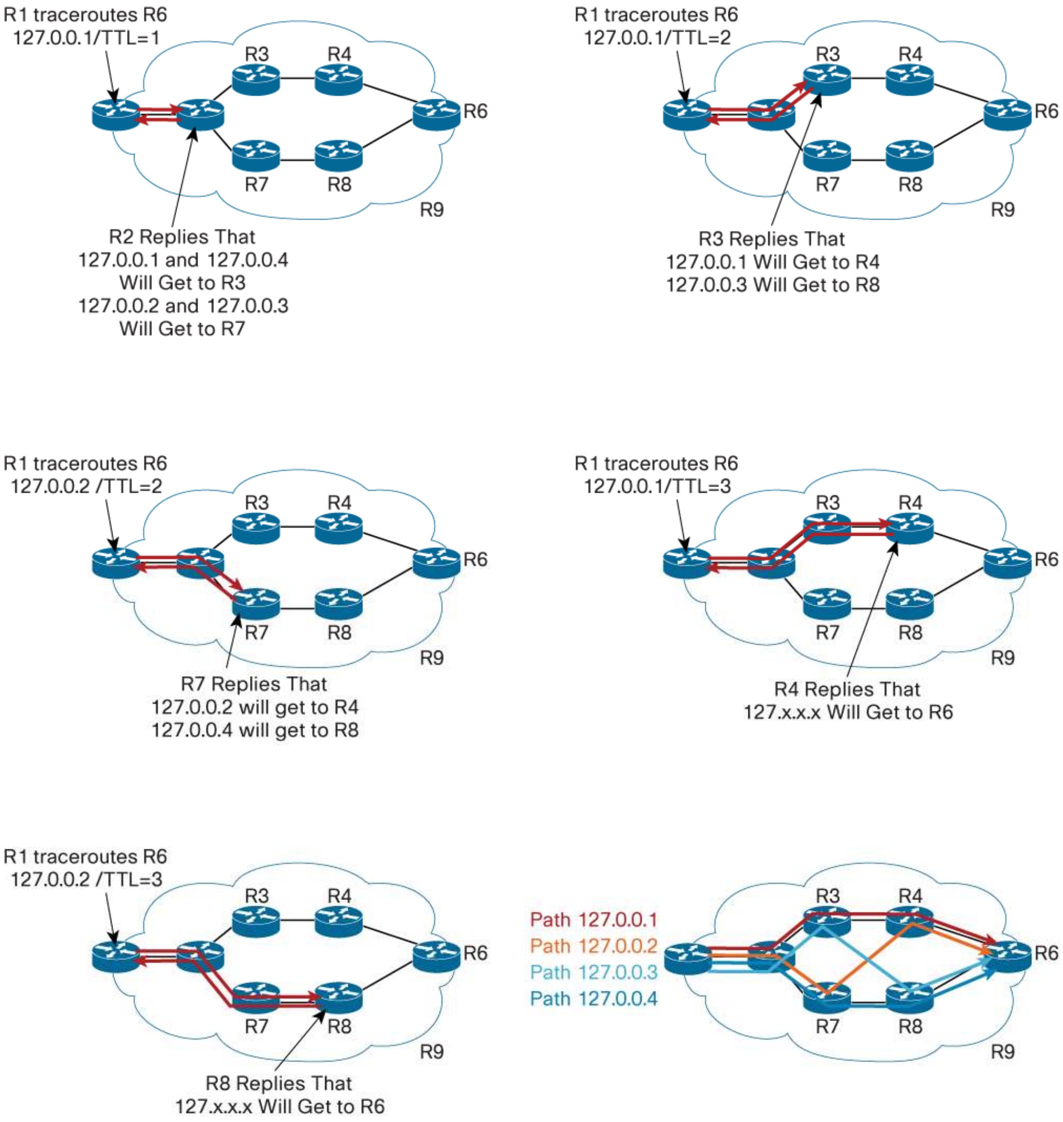
For more information regarding MPLS ping packet payload, refer to [MPLS-PING].

Dealing with Equal Cost Multi Paths (ECMP)

Frequently, LSPs for a given FEC may have multiple “next hops” at transit LSRs. LSPs may have backup paths, detour paths, and other alternative paths to take in the case of a failure in the primary LSP. It is useful if MPLS echo requests can exercise all possible paths. This, while desirable, may not be practical, as the algorithms that a given LSR uses to load balance packets over alternative paths may be proprietary.

In order to achieve some degree of coverage on alternate paths, MPLS ping/trace may use the mechanism outlines in [MPLS-PING] where the destination address in the echo-request packet might be chosen into the 127/8 address range. This address might affect load balancing when the LSR uses the destination address in the IP header as a decision for load balancing.
This mechanism might be acceptable in tracing a single path (Path Trace) out of all the possible paths from ingress to egress. However, this is clearly not sufficient where it might be required to probe and trace all existing ECMP paths (TreeTrace). More latitude is offered via the Downstream mapping TLV object which allows for each transit LSR to provide information about how each of its downstream routers can be exercised. The ingress can then send MPLS echo requests that exercise these paths. Note that [MPLS_PING] does not provide a standardized method to finding all the possible ECMP LSPs from the ingress to egress LSRs. Therefore, the TreeTrace algorithm and output (number of ECMP paths found) might be different from one implementation to the other.

Figure 3. Figure Ping/3: Path/Tree Trace Example (from left to right, top to bottom)



Non-compliant Routers

As MPLS ping/trace should be compatible with the existing infrastructure, if the egress LSR for the FEC Stack being pinged does not support MPLS ping, then no reply will be sent. If in “traceroute” mode, a transit LSR does not support MPLS ping, then no reply will be forthcoming from that LSR for some TTL (ie: “n”). The LSR originating the echo request should try sending the echo request with TTL=n+1, n+2,…, n+k in the hope that some transit LSR further downstream may support MPLS echo requests and reply.

Support for Other Topologies

The need for broad coverage as well as the requirements for new services (such as triple play, video) are pushing the carriers/Service Providers to interconnect their networks and deploy point to multipoint services such as multicast capabilities.

The solution outlined so far in [MPLS_PING] and [Y.1711] provide support for point-to-point networks confined within a single domain or single provider. Some work is underway to extend those tools to support point-to-multipoint topologies [MPLS_P2MP_PING]. Similarly, due to the need for end-to-end OAM in inter carrier/inter-as MPLS networks, the MPLS Ping/trace tool is being augmented to cater to inter-as/inter-domain [MPLS_INTER_PING].

Table 5. Y.1711 vs. MPLS Ping/Trace Quick Functionality Overview

	Y.1711	**MPLS Ping/Trace**
	Need "probably" new hardware (scalability, TTSI handling, …)	**Uses existing hardware**
Applicability	• Pt-to-Pt connection oriented LSP ie: RSVP-TE • Detect LSP mismerge, misbranching	• LDP, RSVP-TE, any other MPLS signaling. • Detect FEC consistency (ie: LSP misbranching, label to FEC mapping problem) • Troubleshooting: hop by hop tracing and problem localization
ECMP friendly	No, use Reserved Label, might affect Load Balancing	Yes both Pathtrace and TreeTrace. However, TreeTrace discovery, as outlines in [MPLS_PING] is based on basic ECMP algorithm that will explore all 127/8 address range. [Note: Cisco supports a more efficient ECMP path discovery]
PHP friendly	No, use Reserved Label, affect tail-end behavior	Yes
Support for other Topologies		
Point-to-Multipoint	No	See [MPLS_P2MP_PING]
Inter Carrier/Inter-AS	No	See [MPLS_INTER_PING]
Frequency	Packet injection frequency every 1s	Frequency as per operator request
Scalability	• Requires management of TTSI • Head-end, Tail-end need to keep track of LSP state machine	• Use native information • No state machine, echo reply contains code which is interpreted by operator and/or management platform
Error detection mechanism (packet integrity)	BIP 16 calculation	IP CRC
Service Level Agreement	No	No
Performance Monitoring	No	No

MPLS Ping/Trace is a natural progression for the operators who have been using the IP data plane verification tools. Further, MPLS Ping/Trace addresses the OAM requirements as outlined by Service Providers and mostly allow the use of the existing equipment without hardware changes.

OAM for Value Added Services

MPLS networks become more common with increased Layer 2 and Layer 3 VPN traffic types and different voice and data applications. The ability for Service Providers to verify the LSP data plane integrity, identify and isolate MPLS forwarding problems, becomes critical for offering these services.

MPLS VPN

When offering value-added services (ie: MPLS VPN), the Service Provider can leverage a set of OAM tools, including IP ping/traceroute, VRF aware ping and traceroute, MIBs, and MPLS Ping/Trace.

Each tool can be used independently for verification and troubleshooting. An example of troubleshooting sequence for VPN might be:

- Use IP Ping/Trace from the CE to assess connectivity at the VPN level
- Use VRF aware Ping/Trace to assess connectivity between PE at the VPN level
- Use MPLS Ping/Trace to assess LSP liveliness between PE
- Simultaneous MPLS related MIBs at the LSR of interest can be gathered for useful information/parameters

AToM: Any Transport over MPLS

As network operators deploy pseudowire services, the ability to provide end-to-end fault detection and diagnostics for an emulated pseudowire service is critical for the network operator. In the case of Any Transport over MPLS (AToM), the pseudowire used to provide Layer 2 emulated service uses the MPLS tunnel as shown in Figure AToM/1.

Verification of the underlying tunnel (ie: the transport tunnel, MPLS) is specific to MPLS and should not be handled by the pseudowire OAM component.

Connection verification of the emulated service between two CEs should be performed using the native mechanisms provided by the emulated services running between the CEs. As an example, ATM OAM such as connectivity checks will be used through the OAM F4, F5 cells, when running an ATM emulated service between two CEs.

Furthermore, tight interaction is needed between the MPLS transport level OAM and the pseudowire OAM in order to provide end-to-end OAM fault detection and diagnostics. Such interaction covers OAM state mapping [OAM-MSG]…

One of the available solutions is Virtual Circuit Connection Verification (VCCV), which is intended to provide connectivity verification of a pseudowire VC.

When MPLS is used as the transport technology, VCCV capabilities are negotiated during the VC establishment. VCCV leverages the MPLS Ping encapsulation to convey the information between the end-point PEs via the L2 Circuit ID TLV, which contains the VCID to be verified along with the IDs of the two end-point PEs.

Figure 4. Pseudo Wire Operation Reference Model

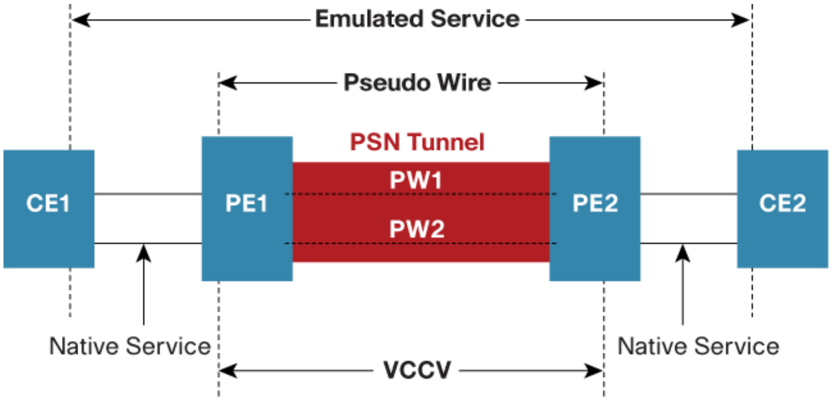


Table 6. OAM Solutions Quick Functionality Overview

	Y.1711	MPLS Ping/Trace	VCCV
	Need “probably” new hardware (scalability, TTSI handling, …)	**Uses existing hardware**	Uses existing hardware. Based on implementation, hardware changes might be required to support the two VCCV modes: in band, router alert
Applicability	• Pt-to-Pt connection oriented LSP, ie: RSVP-TE • Detect LSP mismerge, misbranching	• LDP, RSVP-TE, any other MPLS signaling. • Detect FEC consistency (ie: LSP misbranching, label to FEC mapping problem) • Troubleshooting: hop by hop tracing and problem localization	• VC connectivity check • Check VCs attachment point between two PEs for a given VC • Support ATM, Frame Relay, PPP, Ethernet
ECMP friendly	No, use Reserved Label, might affect Load Balancing	Yes Basic ECMP algorithms in draft –03 that will explore all 127/8 address range. Waiting for optimized tree-trace algorithm	Not applicable
PHP friendly	No, use Reserved Label, affect tail-end behavior	Yes	Not applicable
Scalability/Frequency	Packet injection frequency every 1s	Frequency as per operator request	Frequency as per operator request
	Requires management of TTSI	Use native information	Use native information
	BIP 16 calculation	IP CRC	IP CRC
	Head-end, Tail-end need to keep track of LSP state machine	No state machine, echo reply contains code which is interpreted by operator and/or management platform	No state machine, echo reply contains code which is interpreted by operator and/or management platform
Service Level Agreement	No	No	No

Note: This table does not show built in solutions, including MPLS Fast Reroute, Link and Node Protection used with RSVP-TE tunnels, LDP Graceful Restart, RSVP-TE Graceful Restart. These are already available and currently used in the existing deployed network.

As a conclusion, due to the operational challenges encountered by Service Providers as they deploy MPLS networks (including the provisioning, fault management, maintenance, performance, and optimization of the MPLS deployment), OAM is definitely a critical component in achieving the stringent service level agreement required by the value added services. Cisco, leveraging its internal domain experience, is actively promoting the implementation of industry standards tools. It is also working closely with customers to understand and solve problems related to managing MPLS networks. The tools presented in this paper (MPLS Ping/Trace, VCCV) constitute part of the building blocks for MPLS Fault, Configuration, Accounting, Provisioning, and Security (FCAPS) being offered by Cisco IOS MPLS Embedded Management tools.

Platform Availability

Cisco supports industry standard MPLS Ping/Trace along with Tree trace option for multi path topology and VCCV for pseudowire. Note that, at this time, Y.1711 is not supported.

For more information regarding per platform support, please refer to the MPLS Embedded Management roadmap which is available on http://cco.cisco.com

Reference

[MPLS-RFC3031] IETF, RFC 3031, ‘Multiprotocol Label Switching Architecture’, January 2001

[OAM-LABEL] IETF, RFC 3429, ‘Assignment of the ‘OAM Alert Label’ for Multiprotocol Label Switching Architecture (MPLS) Operation and Maintenance (OAM)’, November 2002

[Y.1711] ITU-T draft Recommendation Y.1711, “MPLS OAM mechanism”, Geneva, Switzerland, Feb 2002

[Y.1714] ITU-T draft Recommendation Y.1714, “MPLS Management and OAM Framework”, Geneva, Switzerland, Aug 2006

[REQUIR] IETF, RFC4377, ‘Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks’, February 2006

[MPLS-PING] IETF, RFC4379, ‘Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures’, February 2006

[VCCV] IETF, ‘Pseudo Wire (PW) Virtual Circuit Connection Verification’, draft-ietf-pwe3-vccv-13.txt, March 2007

[MPLS-P2MP-PING] IETF, ‘Detecting Data Plane Failures in Point-to-Multipoint Label Switching (MPLS), Extensions to LSP Ping ‘, draft-ietf-mpls-p2mp-lsp-ping-03.txt, March 2007

[MPLS-INTER-PING] IETF, ‘Detecting MPLS Data Plane Failures in Inter-AS and inter-provider Scenarios ‘, draft-ietf-mpls-interas-lspping-00.txt, March 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-409690-00 6/07