MPLS in Next-Generation Transport Networks

A Light Reading Webinar
Sponsored by
MPLS-TP Industry Initiative

A Research-Led, Thought-Leadership Program from Heavy Reading and Light Reading

- Ongoing editorial coverage on MPLS-TP related topics
- Heavy Reading MPLS-TP white paper
- LRTV operator interviews video

www.lightreading.com/mplstp/
Today’s Presenters

• **David Sinicrope**, Director, Standardization Development Unit IP and Broadband, Ericsson

• **Joe Whitehouse**, Director of Marketing, Network Technologies, Metaswitch

• **Luyuan Fang**, Principal Engineer, Cisco

• **Rafael Francis**, Head of Technology & Marketing, Americas, ECI Telecom

• **Michael Haugh**, Senior Product Manager, Ixia
Agenda

- Introduction to MPLS-TP and Key Drivers
  - Emerging Standards Overview
  - MPLS-TP and IP/MPLS
  - Deployment Scenarios
  - Test Requirements and Industry Milestones
  - MPLS-TP Next Steps
  - Questions & Answers
Transport Network Situation

• Currently TDM based
  – constant bit rates even when no traffic

• Network Convergence
  – Too costly to run specialized networks
  – Multiple services need to run on same network infrastructure without sacrificing quality
  – Flexibility to adapt to new types of traffic and topologies

• Fast growing services
  – Higher bandwidth demand – video
  – VPNs and Virtualization – VPNs, cloud virtualization
  – Services are packet/IP based, don’t need constant bit pipe

• Quality of Service
  – Predicable behavior and control
  – Stable and fast resiliency
  – Scalability
Why packet for the transport?

• Transport environments have a specific look and feel that must be maintained or slowly evolved to control OPEX.
• The transport network is evolving to statistical multiplexing (i.e., packet switching) to gain greater efficiency of network resources.
• Yet it must remain connection oriented for control, management and service guarantees.
• Ethernet is the predominate packet transport service, yet TDM must still be supported. Both must be supported on the same network.

…but what technology to use that meets these needs?...
Why not use MPLS?

- MPLS provides the statistical multiplexing and control needed.
- MPLS has been long deployed and proven for many services such as IP VPN, Ethernet, Frame Relay, TDM and ATM.
- MPLS designed originally to carry IP efficiently. Later extended for other service emulation, e.g., Ethernet, TDM, FR
- Provides a rich and dynamic control plane not needed for transport networks.
  - Transport environments are traditionally provisioned.

- Until recently, MPLS lacked some OAM tools familiar to transport operations. MPLS has been enhance to include these tools.

MPLS is much more than what is needed for transport. What parts of MPLS are needed specifically for the transport environment?
What is MPLS-TP?

The way forward is to create a “profile”, or subset, of existing, enhanced MPLS suited to meet transport requirements.

MPLS-TP *is* MPLS:
MPLS-TP is the subset of MPLS tailored for transport networks.
Why Unified MPLS?

• Many industry initiatives and views on MPLS and MPLS-TP.
• MPLS including MPLS-TP is being used for
  – Mobile backhaul
  – Residential Broadband Access
  – Business and Enterprise services
  – many more
• There is still a great deal of “compartmentalization” between the parts of the network where MPLS-TP is used and where more dynamic functions of MPLS are used.
  – MPLS-TP usage tends to be focused on the access and aggregation while MPLS usage tends to be focused on the aggregation and core.

Yet regardless of the network architecture, the networks need to provide end to end service with the guarantees and diagnostics as though there were a unified network.
Unified MPLS is an MPLS architecture to provide seamless services across a variety of MPLS environments. This includes consistent OAM, Network Management, Control and Resiliency functions across any type of MPLS network.

- Unified MPLS technology (including QoS, OAM, resiliency, control and management, etc.)
- Efficient delivery of any service
- Flexible and scalable network architecture
- Open and extensible solution
- Enables smooth migration paths from various legacy networks and services

* From Broadband Forum MD-258
Poll Question #1

The properties of MPLS-TP make it most suitable for deployments in what part of the network? (multiple responses allowed)

- Backbone/core
- Metro
- Access
- None of the above, MPLS-TP deployments will be minimal
Agenda

• Introduction to MPLS-TP and Key Drivers
• Emerging Standards Overview
• MPLS-TP and IP/MPLS
• Deployment Scenarios
• Test Requirements and Industry Milestones
• MPLS-TP Next Steps
• Questions & Answers
MPLS-TP Standards History

- Started as T-MPLS in the ITU (2006)
- Became IETF & ITU joint effort in December 2008
  - To be standardized in the IETF
  - MPLS Interoperability Design (MEAD) team formed
    - Disbanded in October 2009
- Notable standards/drafts
  - RFC 5654 – Requirements of an MPLS Transport Profile
  - RFC 5860 – Requirements for OAM in MPLS-TP
  - RFC 5921 – A Framework of MPLS in Transport Network
  - RFC 5960 – MPLS TP Data Plane Architecture
  - draft-ietf-mpls-tp-oam-framework / draft-ietf-mpls-tp-oam-analysis
  - draft-ietf-ccamp-mpls-tp-cp-framework
What is MPLS-TP?

Data Plane
MPLS Bidirectional P2P and P2MP LSPs
- No LSP merging
GACCh: Generic Associate Channel
GAL: Generic Associate Label
PW (SS-PW, MS-PW)

Control Plane
NMS provisioning option
GMPLS control plane option
PW control plane option

OAM
In-band OAM
Fault management:
- Proactive CC/CV: BFD based
- Ping and trace: LSP ping based
- Alarm Suppression and Fault Indication
  - AIS, RDI, LDI, and CFI
Performance monitoring: Loss and Delay

MPLS Based OAM

MPLS Protection

Resiliency
Deterministic path protection
Sub-50ms switch over
- 1:1, 1+1, 1:N protection
- Linear protection
- Ring protection

MetaSwitch Networks
MPLS-TP Control Plane

- draft-ietf-ccamp-mpls-tp-cp-framework
- MPLS-TP paths may be dynamically or statically provisioned
  - RFC 5654 includes migration from mgt to control plane ownership
- Based on well-established G.8080 ASON architecture
- GMPLS for provisioning of LSPs (RFCs 3945, 3471, 3473)
- T-LDP for provisioning of PWs (RFC 4447, segmented-PW)
- Control plane benefits
  - Reduced cost, increased availability, quicker set up time
Some Leading SPs’ View on the MPLS-TP OAM

• Why Single OAM Solution?
  – Multi-solutions increase the cost of development and deployment
  – Multi-solutions create the complexity and inter-operability issues

• Why MPLS-based MPLS-TP OAM?
  – SPs need end-to-end MPLS based OAM. MPLS is widely deployed already, MPLS-TP OAM needs to maintain compatibility
  – IETF MPLS-based MPLS-TP OAM tools meet transport requirements
  – IETF is the MPLS design authority, MPLS protocols need to be defined in IETF to ensure integrity of MPLS and the Internet
  – Production deployment must use Standards based solutions
### MPLS based MPLS-TP OAM Tools

- MPLS based MPLS-TP OAM address all Transport Network Requirements specified by ITU-T and IETF.
- The protocols are defined in IETF and under standardization by IETF and ITU-T

<table>
<thead>
<tr>
<th>OAM Functions</th>
<th>Proactive</th>
<th>On Demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuity Check (CC)</td>
<td>Extended BFD</td>
<td>Extended LSP Ping</td>
</tr>
<tr>
<td>Connectivity Verification (CV)</td>
<td>Extended BFD</td>
<td>Extended LSP Ping</td>
</tr>
<tr>
<td>Alarm signal</td>
<td>AIS/RDI</td>
<td>N/A</td>
</tr>
<tr>
<td>Fault Localization</td>
<td>LDI</td>
<td>Extended LSP Ping</td>
</tr>
<tr>
<td>Remote integrity</td>
<td>Extended BFD</td>
<td>Extended LSP Ping</td>
</tr>
<tr>
<td>Performance Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss/Delay measurement</td>
<td>LM and DM tools</td>
<td>New Loss Measurement and Delay Measurement</td>
</tr>
</tbody>
</table>
## MPLS-TP OAM Standardization

- **2008**
  - ITU-T G.8114 – using Y.1731 based OAM for T-MPLS, was withdrawn in ITU-T
  - IETF/ITU-T Consensus: T-MPLS terminated; MPLS-TP Joint Work started: IETF to develop protocols; ITU-T to derive reqs and integrate IETF definitions

- **2011**
  - ITU-T G.8113.1 – using Y.1731 based OAM (under label 13 instead of 14)
  - ITU-T G.8113.2 – using MPLS based OAM defined in IETF

### MPLS OAM Approaches

<table>
<thead>
<tr>
<th>MPLS OAM Approaches</th>
<th>IETF: MPLS based OAM</th>
<th>ITU-T: Y.1731 based OAM - G.8113.1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IETF Support</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>ITU-T Support</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Inter-op with IP/MPLS</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Trace/ping Functions</strong></td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
MPLS-TP OAM Standards Status

- Core protocols are under WG last calls to become RFCs
- IETF Chair Russ Housley stated at IETF 79 and IETF 80 meetings: IETF only supports single OAM solution for MPLS-TP

• ITU-T determined in Feb. 2011 for G.8113.1 to enter Traditional Approval Process, contingent on IETF Code Point assignment; and continue work with IETF to standardize MPLS based MPLS-TP OAM.

- Standardizing by IETF and ITU-T
- Pending to approval in ITU-T
- Contingent on IETF Code Point assignment
- Not supported by IETF
The Importance of Using Standard Solution

- MPLS-TP carries OAM packet in-band through Generic Associated Channel architecture (RFC 5586)

```
+-----------------+-----------------+-----------------+
| LSP Label       | GAL             | Payload         |
+-----------------+-----------------+-----------------+
| Generic Associated Channel Label (GAL) | Identifies G-ACh packet, reserved label (Value = 13) |
| Associated Channel Header (ACH) | Channel Type indicates protocol - Assigned by IANA |
```

- Channel Type/Code Point needs to be assigned by IETF as standard
- G.8113.1 does not have IANA (Internet Assigned Numbers Authority) assigned Code Point due to lack of IETF consensus
- Risk of using experimental code point is **Code Point Collision**
  - “It can lead to interoperability problems when the chosen value collides with a different usage, as it someday surely will.” RFC 3692 (2004)
Standards-based Unified MPLS Architecture

End to End Cisco PRIME Management

Access
- CPT 50
- Pre-Aggregation
- RBS
- Any Access Technology Mapped into MPLS-TP

Metro
- CPT 200/600
- Packet Transport Aggregation
- CPT 50

Core
- CPT 600
- ARS 9000
- CRS
- IP/MPLS Core and Service Edge

Unified MPLS

MPLS-TP Aggregation/Access

IP/MPLS Core and Service Edge

Multi-Service Edge

Corporate
- Utility

Legacy

Residential

Any Access Technology Mapped into MPLS-TP

Multi-Service Edge

MPLS-TP Aggregation

Unified MPLS
Agenda

• Introduction to MPLS-TP and Key Drivers
• Emerging Standards Overview
• MPLS-TP and IP/MPLS
• Deployment Scenarios
• Test Requirements and Industry Milestones
• MPLS-TP Next Steps
• Questions & Answers
Extending MPLS into the Metro / Access

- Mobile
- Enterprise
- Residential

- Ethernet
- TDM
- ATM
- MPLS LSP

CUSTOMER  METRO ACCESS  METRO CORE  CORE EDGE
Extending MPLS into the Metro / Access
Extending MPLS into the Metro / Access

Enterprise Mobile

Residential

Ethernet TDM ATM MPLS LSP

10,000s 1,000s 100s

IP/MPLS or MPLS-TP?

CUSTOMER METRO ACCESS METRO CORE CORE EDGE
IP/MPLS or MPLS-TP?

- Both will play a role in NG Ethernet transport solutions
- Choice of one or both depends on a number of factors

MPLS-TP “static” mode

IP/MPLS

Both will play a role in NG Ethernet transport solutions and the choice of one or both depends on a number of factors.
### Transport-friendly MPLS-TP

<table>
<thead>
<tr>
<th>Strengths</th>
<th>MPLS - TP</th>
<th>IP/MPLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>“Transport” network paradigm</strong></td>
<td></td>
<td><strong>Automated provisioning/protection</strong></td>
</tr>
<tr>
<td><strong>Operationally simpler</strong></td>
<td></td>
<td><strong>Scalable to Regional / Global</strong></td>
</tr>
<tr>
<td>- skills NMS-oriented</td>
<td></td>
<td><strong>Widely deployed</strong></td>
</tr>
<tr>
<td>- routing protocol skills not required</td>
<td></td>
<td><strong>Well-standardized control plane</strong></td>
</tr>
<tr>
<td><strong>Easier on equipment resources</strong></td>
<td></td>
<td><strong>Points of heavy service concentration</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Multi-vendor environments</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Service Edge / IP core</strong></td>
</tr>
<tr>
<td><strong>Deployment Scenarios</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access layer, limited path diversity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Simple, inexpensive “spoke” devices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Networks with centralized IP intelligence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access / Metro</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Advantages of MPLS-TP for Mobile Backhaul

- Fits transport operational model
  - Integration with existing transport solution
- Simpler cell site device
- Simplified service provisioning
- Fault resiliency
  - Mesh topology protection for LTE
Border Node, aka “Signaling Gateway”

- Unified MPLS enables end-to-end services across static and dynamic domains with a gateway function
- In pseudowire-based backhaul, multi-segment pseudowires are used
  - Static, MPLS-TP segments
  - Dynamic IP-MPLS segments
  - Gateway interconnects or “stitches” the two
Signaling Gateway Approaches

**VPLS/VSI bridging**
- Ethernet bridging b/w MPLS domains
- MAC learning disabled for E-LINE
- Benefit: multipoint support

**Pseudowire switching**
- Tie static and dynamic pseudowires together as a single connection
- Uses multi-segment pseudowires
- Benefit: Multi-service support
Agenda

- Introduction to MPLS-TP and Key Drivers
- Emerging Standards Overview
- MPLS-TP and IP/MPLS
- Deployment Scenarios
- Test Requirements and Industry Milestones
- MPLS-TP Next Steps
- Questions & Answers
# MPLS-TP Test Challenges

## Phase 1: Is this a viable technology?

<table>
<thead>
<tr>
<th>MPLS-TP Function</th>
<th>Functional Verification</th>
<th>Interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSPs and PW encapsulation</td>
<td>• G-Ach/GAL encapsulation</td>
<td>• Message exchange (correct encoding and interpretation)</td>
</tr>
<tr>
<td></td>
<td>• Control Word (CW) inclusion</td>
<td>• Label switching</td>
</tr>
<tr>
<td>LSPs and PW establishment</td>
<td>• Static label assignment</td>
<td>• Interoperability of static SS-PW and dynamic SS-PW</td>
</tr>
<tr>
<td></td>
<td>• Dynamic provisioning</td>
<td>• Label space compatible</td>
</tr>
<tr>
<td>OAM: Continuity Check (CC) &amp; Connectivity Verification (CV)</td>
<td>• OAM message generation @ various intervals</td>
<td>• OAM message exchange</td>
</tr>
<tr>
<td></td>
<td>• Failure detection</td>
<td>• CC/CV sessions established</td>
</tr>
<tr>
<td></td>
<td>• On-demand LSP connectivity verification</td>
<td>• Ping encoding follows G-ACh Channel Type+ Echo or G-ACh Channel Type + IP/UDP/Echo?</td>
</tr>
<tr>
<td>On-demand Alarm Generation and Fault Notification</td>
<td>• Alarm generation and detection</td>
<td>• Alarm encoding and interpretation</td>
</tr>
<tr>
<td></td>
<td>• Generation of AIS/LDI/LCK/PW Status</td>
<td>• AIS suppression state</td>
</tr>
<tr>
<td></td>
<td>• Auto generation of RDI</td>
<td>• Alarm propagation</td>
</tr>
<tr>
<td></td>
<td>• CCCV Pause/Resume</td>
<td></td>
</tr>
<tr>
<td>Automatic Protection Switching (APS)</td>
<td>• Ingress, Egress and Transit Node</td>
<td>• PSC interoperability</td>
</tr>
<tr>
<td></td>
<td>• Different protection modes</td>
<td>• Switchover time measurements per LSP/PW</td>
</tr>
<tr>
<td>MPLS-TP and MPLS Interworking</td>
<td>• OAM status translation</td>
<td>• End to end service verification</td>
</tr>
<tr>
<td></td>
<td>• CW handling</td>
<td>• MS-PW (mix of MPLS-TP and IP/MPLS segments)</td>
</tr>
</tbody>
</table>
Testing DUT as Ingress PE Router

Key Use Cases to test:
1. MPLS-TP OAM interoperability
2. Continuity Check Interoperability
3. PSC interoperability
4. Validate APS commands and performance
5. Switchover time measurement based on traffic loss
6. < 50 ms switchover time in various protection mode
Testing DUT as Ingress PE Router

Source: Ixia IxNetwork Application Traffic Statistics

<table>
<thead>
<tr>
<th>MPLS Current Label Value (Outer, Inner)</th>
<th>Tx Frames</th>
<th>Rx Frames</th>
<th>Frames Delta</th>
<th>Loss %</th>
<th>Packet Loss Duration (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before Switchover</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>101</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>102</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>103</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>104</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>105</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>106</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>107</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>108</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>109</td>
<td>58,183,106</td>
<td>58,183,106</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>After Switchover</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>59,099,137</td>
<td>59,099,137</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>201</td>
<td>59,099,137</td>
<td>59,099,136</td>
<td>1</td>
<td>0.000</td>
<td>0.105</td>
</tr>
<tr>
<td>202</td>
<td>59,099,137</td>
<td>59,099,137</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>203</td>
<td>59,099,137</td>
<td>59,099,137</td>
<td>1</td>
<td>0.000</td>
<td>0.105</td>
</tr>
<tr>
<td>204</td>
<td>59,099,137</td>
<td>59,099,137</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>105</td>
<td>59,099,137</td>
<td>59,099,136</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>106</td>
<td>59,099,137</td>
<td>59,099,136</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>107</td>
<td>59,099,137</td>
<td>59,099,136</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>108</td>
<td>59,099,137</td>
<td>59,099,136</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>109</td>
<td>59,099,137</td>
<td>59,099,136</td>
<td>0</td>
<td>0.000</td>
<td>0.000</td>
</tr>
</tbody>
</table>

LoC error injected only to the first 5 LSPs

IxiaNetowrk Per-Flow Traffic Statistics

Per LSP/PW Switchover Time

Source: Ixia IxNetwork Application Traffic Statistics
MPLS-TP: Future Testing...

Phase 2: Is this a compelling technology?

- Performance Verification and Benchmarks
  - Can MPLS-TP deliver carrier grade services?
    - Scale: service scale of LSP/PW
    - Reliability: protection switching, recovery sub 50ms
    - CoS: deliver service levels to meet SLAs
    - Performance: forwarding performance, low latency, low delay variation (jitter)
    - Management: OAM (active and on demand) and MIB support
      - Support static provisioning via NMS
      - Support dynamic provisioning
Testing with Scalability

Key Use Cases to test:
1. Simulate large number of working and protecting LSP/PW
2. Working/Protecting on the same port or different ports
3. Running Continuity Check on all working and protecting LSP/PWs at various interval including 3.33ms
4. Enable advance OAM features such as Performance Monitoring (LM, DM) and on-demand CV (LSP Ping and Traceroute)
5. End to end traffic with different rate and frame sizes
6. Validate maximum PW/LSP capacity
March 2011: Service Provider Demo: Sub-50 msec failover

- Demonstrate MPLS-TP OAM
  - BFD
  - LDI
  - AIS/RDI
- Fault insertion (fiber fail along working LSP route)
  - Sub-50 msec failover

Cisco/Ixia MPLS-TP Demo at Verizon
Industry Milestones

- MPLS 2010 Public Interoperability Demo (October 2010, Washington DC)

- MPLS-TP static LSP establishment
- MPLS-TP data plane verification
- Exchange BFD CC messages
- Use of BFD CC to identify failures
- Use of PSC
- Functionality of protection modes

First multi-vendor standards-based MPLS-TP interoperability testing

Industry Milestones

- MPLS and Ethernet World Congress - EANTC Public Multi-Vendor Interoperability Test and Public Showcase (Feb 2011, Paris)

MPLS-TP interop test with Ixia, Cisco, Ericsson, Huawei, Hitachi, and Metaswitch

- BFD Continuity Check at various intervals
- BFD Continuity Check with slow start
- IETF Linear APS
  - Bidirectional 1:1
  - Failover time at 100 ms and 3.33 ms interval
- BFD LoC induced protection switchover
- BFD on-demand LSP ping
- PW Status OAM
- MPLS-TP and MPLS interworking
  - control word interoperability

Test validates interworking between transport domains
http://www.eantc.de
Poll Question #2

When do you expect to see significant strategic deployment of MPLS-TP by numerous operators?

- Before the end of 2011
- In 2012
- In 2013
- In 2014
- Unsure / do not expect to see significant deployments of MPLS-TP
MPLS-TP Next Steps: Roundtable Discussion

- **David Sinicrope**, Director, Standardization Development Unit IP and Broadband, Ericsson
- **Joe Whitehouse**, Director of Marketing, Network Technologies, Metaswitch
- **Luyuan Fang**, Principal Engineer, Cisco
- **Rafael Francis**, Head of Technology & Marketing, Americas, ECI Telecom
- **Michael Haugh**, Senior Product Manager, Ixia
Q&A Session

Please submit your questions!