TOMORROW starts here.
Deploying MPLS Traffic Engineering

BRKMPL-2100

Santiago Álvarez
Distinguished Technical Marketing Engineer
Agenda

- Technology Overview
- TE and QoS
- Traffic Protection
- Bandwidth optimization
- Centralized Tunnel Creation and Control
- General Deployment Considerations
Technology Overview
MPLS TE Overview

• Introduces explicit routing
• Supports constraint-based routing
• Supports admission control
• Provides protection capabilities
• Uses RSVP-TE to establish LSPs
• Uses ISIS / OSPF extensions to advertise link attributes
How MPLS TE Works

- Link information Distribution*
  - ISIS-TE
  - OSPF-TE
- Path Calculation (CSPF)*
- Path Setup (RSVP-TE)
- Forwarding Traffic down Tunnel
  - Auto-route (announce / destinations)
  - Static route
  - PBR
  - PBTS / CBTS
  - Forwarding Adjacency
  - Pseudowire Tunnel select
Link Information Distribution

- Additional link characteristics
  - Interface address
  - Neighbor address
  - Physical bandwidth
  - Maximum reservable bandwidth
  - Unreserved bandwidth (at eight priorities)
  - TE metric
  - Administrative group (attribute flags)

- IS-IS or OSPF flood link information

- All TE nodes build a TE topology database

- Not required if using off-line path computation
Path Calculation

- TE nodes can perform constraint-based routing
- Tunnel head end generally responsible for path calculation
- Constraints and topology database used as input to path computation
- Shortest-path-first algorithm ignores links not meeting constraints
- Tunnel can be signaled once a path is found
- Not required if using offline path computation
TE LSP Signaling

- Tunnel signaled with TE extensions to RSVP
- Soft state maintained with downstream PATH messages
- Soft state maintained with upstream RESV messages
- New RSVP objects
  - LABEL_REQUEST (PATH)
  - LABEL (RESV)
  - EXPLICIT_ROUTE
  - RECORD_ROUTE (PATH/RESV)
  - SESSION_ATTRIBUTE (PATH)
- LFIB populated using RSVP labels allocated by RESV messages
Traffic Selection

• Traffic enters tunnel at head end
• Multiple traffic selection options
  – Auto-route (announce / destination)
  – Static routes
  – Policy Based Routing
  – Forward Adjacency
  – Pseudowire Tunnel Selection
  – Policy / Class Based Tunnel Selection
• Tunnel path computation independent of routing decision injecting traffic into tunnel
Point-to-Multipoint (P2MP) TE LSP

- Unidirectional
- Explicitly routed
- One head end, but one or more tail ends (destinations)
- Same characteristics (constraints, protection, etc.) for all destinations
P2MP TE LSP Terminology

- **Head-end/Source**: Node where LSP signaling is initiated
- **Mid-point**: Transit node where LSP signaling is processed (not a head-end, not a tail-end)
- **Tail-end/Leaf/destination**: node where LSP signaling ends
- **Branch point**: Node where packet replication is performed
- **Source-to-leaf (S2L) sub-LSP**: P2MP TE LSP segment that runs from source to one leaf
P2MP TE LSP Path Computation

- Constrained Shortest Path First (CSPF) used to compute an adequate tree
- CSPF executed per destination
- TE topology database and tunnel constraints used as input for path computation
- Path constraints may include loose, included, excluded hops
- Same constraints for all destinations (bandwidth, affinities, priorities, etc.)
- Path computation yields explicit path to each destination
- No changes to OSPF/IS-IS TE extensions
- Static paths possible with offline path computation

Path to R4: (R1, R2, R4)
Path to R5: (R1, R2, R5)
P2MP TE LSP Signaling

- Source sends unique PATH message per destination
- LFIB populated using RSVP labels allocated by RESV messages
- Multicast state built by reusing sub-LSP labels at branch points
Configuring P2MP Tunnel at Head End (Cisco IOS)

```plaintext
mpls traffic-eng destination list name P2MP-LIST-DST1
ip 172.16.255.1 path-option 10 explicit name PATH1
ip 172.16.255.2 path-option 10 dynamic
ip 172.16.255.3 path-option 10 dynamic
ip 172.16.255.4 path-option 10 dynamic

interface Tunnel1
  description FROM-ROUTER-TO-LIST-DST1
  ip unnumbered Loopback0
tunnel mode mpls traffic-eng point-to-multipoint
tunnel destination list mpls traffic-eng name P2MP-LIST-DST1
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 1000
```

Destination list with one path-option per destination

P2MP TE Tunnel

Destination list

Signaled bandwidth and setup / hold priorities
Configuring P2MP Tunnel at Head End (Cisco IOS XR)

```interface tunnel-mte1
  ipv4 unnumbered Loopback0
  destination 172.16.255.129
    path-option 10 explicit name PATH1
    path-option 20 dynamic
  destination 172.16.255.130
    path-option 10 dynamic
  priority 0 0
  signalled-bandwidth 100000
!```

MPLS TE P2MP tunnel
Destination with path-option list
Destination with single path-option
Signaled bandwidth and setup / hold priorities
MPLS TE Use Cases

Point-to-Point SLA

Protection

Bandwidth Optimization

Strategic / Planned

Tactical / Reactive
MPLS TE Integration with Network Services

A TE LSP provides transport for different network services

Low-Latency, BW Protected TE LSP
TE LSP with Reserved BW
L2VPN (Pseudowire)
IP (VPN) Service
TE and QoS
Motivations

- Point-to-point SLAs
- Admission control
- Integration with DiffServ architecture
- Increased routing control to improve network performance
MPLS TE and DiffServ Deployment Models

**MPLS TE and no DiffServ**
- A solution when:
  - No differentiation required
  - Optimization required
- Limit link load to actual link capacity
- No notion of traffic classes

**MPLS TE and DiffServ**
- A solution when:
  - Differentiation required
  - Optimization required
- Limit class capacity to expected class load
- Limit class load to actual class capacity for one class

**DiffServ-Aware TE and DiffServ**
- A solution when:
  - Strong differentiation required
  - Fine optimization required
- Limit class capacity to expected class load
- Limit class load to actual class capacity for at least two classes
DiffServ-Aware Traffic Engineering

- Enables per-class traffic engineering
- IS-IS or OSPF flood link information (as usual)
- Per-class unreserved bandwidth on each link
- New RSVP object (CLASSTYPE)
- Nodes manages link bandwidth using a bandwidth constraint model
- Two models defined
  - Maximum Allocation Model (MAM)
  - Russian Doll Model (RDM)
- Unique class definition and constraint model throughout network
- Two classes (class-types) in current implementations

IP/MPLS

PE1

PE2

PE3

Bandwidth Constraints

Class-type 1 (voice) 20%
Class-type 2 (video) 40%
Maximum Allocation Model (MAM)

• BW pool applies to one class
• Sum of BW pools may exceed MRB
• Sum of total reserved BW may not exceed MRB
• Current implementation supports BC0 and BC1
Russian Dolls Model (RDM)

- BW pool applies to one or more classes
- Global BW pool (BC0) equals MRB
- BC0..BCn used for computing unreserved BW for class n
- Current implementation supports BC0 and BC1
Traffic Protection
Traffic Protection Using MPLS TE Fast Re-Route (FRR)

- Sub-second recovery against node/link failures
- Scalable 1:N protection
- Greater protection granularity
- Cost-effective alternative to 1:1 protection
- Bandwidth protection
- Topology independent

![Diagram showing Primary and Backup TE LSPs in an IP/MPLS network with nodes R1, R2, and R8.]
FRR Link Protection Operation

- Requires **pre-signalled next-hop** (NHOP) backup tunnel
- Point of Local Repair (PLR) swaps label and pushes backup label
- Backup terminates on Merge Point (MP) where traffic re-joins primary
- Restoration time expected under ~50 ms
FRR Node Protection Operation

- Requires pre-signalled next-next-hop (NNHOP) backup tunnel
- Point of Local Repair (PLR) swaps next-hop label and pushes backup label
- Backup terminates on Merge Point (MP) where traffic re-joins primary
- Restoration time depends on failure detection time
Bidirectional Forwarding Detection Trigger for FRR

- FRR relies on quick PLR failure detection
- Some failures may not produce loss of signal or alarms on a link
- BFD provides light-weight neighbor connectivity failure detection
- Preferred over RSVP Hellos
Bandwidth Protection

- Backup tunnel with associated bandwidth capacity
- Backup tunnel may or may not actually signal bandwidth
- PLR will decide best backup to protect primary
  - nhop/nnhop
  - backup-bw
  - class-type
  - node-protection flag
AutoTunnel: Primary Tunnels
What’s the Problem?

• FRR can protect TE Traffic
• No protection mechanism for IP or LDP traffic
• How to leverage FRR for all traffic?
• What if protection desired without traffic engineering?
AutoTunnel: Primary Tunnels

What’s the Solution?

- Create protected one-hop tunnels on all TE links
  - Priority: 7/7
  - Bandwidth: 0
  - Affinity: 0x0/0xFFFF
  - Auto-BW: OFF
  - Auto-Route: ON
  - Fast-Reroute: ON
  - Forwarding-Adj: OFF
  - Load-Sharing: OFF

- Tunnel interfaces not shown on router configuration

- Configure desired backup tunnels (manually or automatically)
Configuring AutoTunnel Primary Tunnels (Cisco IOS)

```plaintext
mpls traffic-eng tunnels
mpls traffic-eng auto-tunnel primary onehop
mpls traffic-eng auto-tunnel primary tunnel-num min 900 max 999
!
```

Enable auto-tunnel primary

Range for primary tunnel interfaces
**AutoTunnel: Backup Tunnels**

**What’s the Problem?**

- MPLS FRR requires backup tunnels to be preconfigured
- Automation of backup tunnels is desirable
AutoTunnel: Backup Tunnels
What’s the Solution?

Create backup tunnels automatically as needed

- Detect if a primary tunnel requires protection and is not protected
- Verify that a backup tunnel doesn’t already exist
- Compute a backup path to NHOP and NNHOP excluding the protected facility
- Optionally, consider shared risk link groups during backup path computation
- Signal backup tunnels

Primary TE LSP

Backup TE LSP
Configuring AutoTunnel Backup Tunnels (Cisco IOS)

mpls traffic-eng tunnels
mpls traffic-eng auto-tunnel backup nhop-only
mpls traffic-eng auto-tunnel backup tunnel-num min 1900 max 1999
mpls traffic-eng auto-tunnel backup srlg exclude preferred

Enable auto-tunnel backup (NHOP tunnels only)
Range for backup tunnel interfaces
Preferably consider SRLGs
Configuring AutoTunnel Backup Tunnels (Cisco IOS XR)

```plaintext
ipv4 unnumbered mpls traffic-eng Loopback 0
!
mpls traffic-eng
interface GigabitEthernet0/0/0/0
auto-tunnel backup
  exclude srlg preferred
  nhop-only
!
auto-tunnel backup
tunnel-id min min 1900 max 1999
!
```

- **Source interface for backup tunnels**
- **Protect interface with dynamically created (next-hop only) backup tunnels. Preferably consider SRLGs.**
- **Range for backup tunnel interfaces**
Shared Risk Link Group (SRLG)

- Some links may share same physical resource (e.g. fiber, conduit)
- AutoTunnel Backup can force or prefer exclusion of SRLG to guarantee diversely routed backup tunnels
- IS-IS and OSPF flood SRLG membership as an additional link attribute
What About Path Protection?

- Primary and standby share head and tail, but expected to be diversely routed
- Generally higher restoration times compared to local protection
- Doubles number of TE LSPs (1:1 protection)
- May be an acceptable solution for restricted topologies (e.g. rings)
- Cisco IOS
  - Separate path option sequences for primary and standby
    - Explicit paths only
    - No path diversity
- Cisco IOS XR
  - Single or separate path-option sequence for primary and standby
    - Explicit and dynamic paths
    - Automatic path diversity (node-link, node, link) when using single path-option sequence
    - BFD may be used for end-to-end fault detection
P2MP TE LSP Traffic Protection

- No new protocol extensions to support FRR
- Protection requirement applies to all destinations
- P2P LSP as backup tunnel for a sub-LSP
- No changes to label stacking procedure
- Only link protection supported
- Head-end protection requires path redundancy (live-standby / live-live)
Head End Resiliency Models for P2MP TE

**Live-Standby**

- Redundant TE LSPs with **different ingress** PEs
- LSPs may or may not be disjoint
- Link failures generally protected via FRR
- Several **bandwidth options** for Standby TE LSP
  - Same bandwidth reservation as Live path
  - No bandwidth reservation
  - Adaptive bandwidth reservation (auto-bandwidth)

**Live-Live**

- Redundant P2MP LSPs with **different ingress and egress** PEs
- LSPs are generally disjoint
- Receiver or near-receiver stream selection and switchover
- FRR generally not a requirement
- Same bandwidth reservation on both TE LSPs
Bandwidth optimization
Strategic / Planned Bandwidth Optimization

- Tries to optimize underlying physical topology based on traffic matrix
- Key goal is to avoid link over/under utilization
- On-line (CSPF) or off-line path computation
- May result in a significant number of tunnels
- Should not increase your routing adjacencies
Traffic Matrix Measurement

- Interface counters on unconstrained tunnels
- Interface MIB
- MPLS LSR MIB
- NetFlow
  - NetFlow BGP Next Hop
  - MPLS-Aware NetFlow
  - Egress/Output NetFlow
- BGP policy accounting
  - Communities
  - AS path
  - IP prefix
AutoTunnel Mesh

• Mesh group: LSRs to mesh automatically

• Membership identified by
  – Matching TE Router ID against ACL (Cisco IOS and IOS XR)
  – IGP mesh-group advertisement (Cisco IOS)

• Each member automatically creates tunnel upon detection of a member

• Tunnels instantiated from template

• Individual tunnels not displayed in router configuration
Auto Bandwidth

- Dynamically adjust bandwidth reservation based on measured traffic
- Optional minimum and maximum limits
- Sampling and resizing timers
- Tunnel resized to largest sample since last adjustment
- Actual resizing can be subject to adjustment threshold and overflow/underflow detection
Configuring AutoTunnel Mesh (Cisco IOS)

```
mpls traffic-eng tunnels
mpls traffic-eng auto-tunnel mesh
!
interface Auto-Template1
  ip unnumbered Loopback0
tunnel destination mesh-group 10
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng auto-bw frequency 3600
!
router ospf 16
  log-adjacency-changes
  mpls traffic-eng router-id Loopback0
  mpls traffic-eng area 0
mpls traffic-eng mesh-group 10 Loopback0 area 0
  passive-interface Loopback0
  network 172.16.0.0 0.0.255.255 area 0
!
```

Enable Auto-tunnel Mesh

Tunnel template

Template instanciated for each member of mesh group 10

Dynamic (CSPF) path and dynamic bandwidth adjustment for all mesh tunnels

Advertise mesh group 10 membership in area 0
Configuring AutoTunnel Mesh (Cisco IOS XR)

```
ipv4 unnumbered mpls traffic-eng Loopback 0
!
mpls traffic-eng
  auto-tunnel mesh
  group 10
  attribute-set 10
  destination-list DST-RID-ACL
  !
  tunnel-id min 1000 max 2000
  !
  attribute-set auto-mesh 10
  autoroute announce
  path-selection metric te
  !
!
```

- **Source interface for backup tunnels**
- **Mesh group 10 identified by ACL DST-RID-ACL**
- **Range for mesh tunnel interfaces**
- **Attribute set for tunnels in mesh group 10**
Tactical / Reactive Bandwidth Optimization

- Selective deployment of tunnels when highly-utilized links are identified
- Generally, deployed until next upgrade cycle alleviates congested links
Centralized Tunnel Creation and Control
### Cisco PCE Models (Cisco IOS XR)

#### Inter-Area MPLS TE

- **ABRs act as stateless PCEs**
- **ABRs implement backward recursive PCE-Based Computation**
- **Introduced in IOS XR 3.5.2**
- **IOS XR 5.1.1 introduces PCEP RFC-compliance**

- **Out-of-network, stateless PCE server**
- **PCC initiates LSPs**
- **Introduced in IOS XR 3.5.2**
- **IOS XR 5.1.1 introduces PCEP RFC-compliance**

---

### SDNWAN Orchestration

- **Out-of-network, stateful PCE server**
- **PCE always initiates LSPs**
- **Introduced in IOS XR 5.1.1**
Active Stateful PCE

- Introduces PCEP extensions for
  - LSP state synchronization between PCCs and PCEs
  - PCC delegation of LSP control to PCE

- Active stateful PCE
  - PCC maintains state synchronization with PCE
  - PCC may delegate LSP control to PCE

- PCC always owns LSP state

- Cisco WAN orchestration solution relies on an active stateful PCE that initiates LSP setup
PCE-Initiated Tunnels in Cisco IOS XR

- Treated as dynamically created tunnels (auto-tunnel)
- Tunnel number allocated from user defined range
- Router does NOT verify or compute path that PCE provides (treated as verbatim path)
- Router does not attempt local LSP re-optimization
- PCE responsible for LSP re-optimization
- PCE sends an PCEP Update when a better path exists
- Tunnels may be inter-area
- Only PCE-initiated LSPs can be delegated
### PCE-Initiated LSP

#### Session Establishment
- **PCC** open
- **Stateful (U, I flag)**
- **LSP Cleanup Timer**

#### State Synchronization
- **PCC** open
- **Stateful (U, I flag)**
- **LSP Cleanup Timer**
- **Keepalive**
- **Keepalive**

- PCE / PCC advertise stateful capability
- Session support LSP updates (U flag)
- Session supports LSP creation/initiation (I flag)
- Cleanup timer for PCE LSPs
- Session established when both peers receive keepalive

#### LSP Creation / Initiation
- **PCC** opens
- **Stateful (U, I flag)**
- **LSP Cleanup Timer**
- **LSP id=X**
- **(S flag)**
- **Report**
- **Name=“MyLSP”**
- **Attribute list**
- **PCE**

#### LSP Update
- **PCC** updates LSP state and/or attributes
- **Report**
- **Status=“Up”**
- **(D flag)**

#### LSP Reporting
- **PCC** reports LSP state as part of
  - Initial state synchronization
  - Control delegation
  - Control revoking
  - Deletion
  - Signaling error
  - State change
- **Report**
- **Status=“X”**
- **(D flag)**

- **PCE** request LSP creation / initiation with attribute list
- **PCC** attempts LSP setup and reports back LSP id and state
- **PCC** automatically delegates LSP control (D flag) to PCE
- **PCC** may not revoke delegation
- **PCC** may return delegation

- **PCE** updates LSP state and/or attributes
- **Report with status=“Up” sent to all stateful PCEs**

- **PCC** automatically delegates LSP control (D flag) to PCE
- **PCC** may not revoke delegation
- **PCC** may return delegation

- **PCC** reports LSP state as part of
  - Initial state synchronization
  - Control delegation
  - Control revoking
  - Deletion
  - Signaling error
  - State change
- **Sent to all stateful PCEs**
Configuration for PCE-Initiated Tunnels (Cisco IOS XR)

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mls traffic-eng
pce
peer ipv4 172.16.255.3
  stateful-client
  capabilities instantiation
  capabilities update
!
!
auto-tunnel pce
  tunnel-id min 1000 max 5000
!
!
```

- **Source interface for tunnels**
- **PCE server**
- **Allow PCE-initiated LSP**
- **Range of tunnel-te interfaces for PCE initiated LSPs**
PCE-Initiated LSP (Multiple PCEs)

- PCC synchronizes LSP state over all open stateful PCEP sessions
- When a PCE creates / initiates an LSP
  - PCC will report LSP state to all stateful PCEs
  - PCC will only delegate LSP to originating PCE
- LSP may be re-delegated if originating PCE disconnects or renounces delegation
- LSPs may be re-delegated to a stateful PCE sending a matching LSP creation / initiation before LSP cleanup timeout
Traffic Steering into PCE-Initiated Tunnels

• Two approaches
  – Autoroute announce
  – Policy-based tunnel selection (forwarding class id)

• PCE can specify autoroute announce and forwarding class id during LSP creation / instantiation or update

• Attributes encoded as vendor specific TLVs (same approach used to specify load-share)
 Autoroute Announce

- Prefixes installed in RIB with tunnel as output interface if tunnel destination along shortest path.
- Operates on prefixes at tunnel destination and downstream.
- Prefixes installed with IGP shortest path metric.
- Supported for IS-IS and OSPF.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Next Hop</th>
<th>Metric</th>
<th>Out Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>B</td>
<td>30</td>
<td>Tunnel</td>
</tr>
<tr>
<td>C</td>
<td>B</td>
<td>40</td>
<td>Tunnel</td>
</tr>
<tr>
<td>D</td>
<td>B</td>
<td>40</td>
<td>Tunnel</td>
</tr>
<tr>
<td>Z</td>
<td>Y</td>
<td>20</td>
<td>Ethernet0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>:</td>
<td></td>
</tr>
</tbody>
</table>
Policy Based Tunnel Selection

- Local mechanism at head-end
- PBR policy sets forwarding class for incoming traffic
- Traffic switched to tunnel with matching forwarding class
- Seven forwarding classes supported (1-7)
- One forwarding class reserved as default (0)
General Deployment Considerations
Should RSVP-TE and LDP be Used Simultaneously?

- Guarantees forwarding of VPN traffic if a TE LSP fails
- May be required if full mesh of TE LSPs not in use
- Increased complexity
How Far should Tunnels Span?

- **PE-to-PE Tunnels**
  - More granular control on traffic forwarding
  - Larger number of TE LSPs

- **P-to-P Tunnels**
  - Requires IP tunnels or LDP over TE tunnels to carry VPN traffic (deeper label stack)
  - Fewer TE LSPs
  - May be extended with PE-P tunnels
MPLS TE on Link Bundles

- Different platforms support different link bundles
  - Ethernet
  - POS
  - Multilink PPP
- Bundles appear as single link in topology database
- Same rules for link state flooding
- LSP preemption if bundle bandwidth becomes insufficient
- Configurable minimum number of links to maintain bundle active
- Bundle failure can act as trigger for FRR
Per-Service Tunnel Selection

- Services (L2VPN / L3VPN) generally receive a path automatically
  - Recursive resolution of BGP next hops
  - Recursive resolution of LDP peers
- L2VPN provides granular per-tunnel control using pseudowire tunnel selection
- When using BGP (L2VPN, L3VPN, IP):
  - On tail end, add loopback at destination for each service that needs separate forwarding
  - On tail end, add policy to modify next-hop on BGP updates
  - On head end, add static route to force BGP next hops down specific paths
Summary

• Technology Overview
  – Explicit and constrained-based routing
  – TE protocol extensions (OSPF, ISIS and RSVP)
  – P2P and P2MP TE LSP

• TE and QoS
  – DS-TE (MAM, RDM)
  – PBTS / CBTS

• Traffic Protection
  – Link/node protection (auto-tunnel)
  – Bandwidth protection
  – Path protection

• Bandwidth optimization
  – Strategic / planned (full mesh, auto-tunnel)
  – Tactical / reactive

• Centralized Tunnel Creation and Control
  – Centralized SDN model
  – PCE-initiated tunnels

• General Deployment Considerations
  – MPLS TE and LDP
  – PE-to-PE vs. P-to-P tunnels
  – TE over Bundles
  – Per-Service Tunnel Selection
Recommended Reading
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could be a Winner

• Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

• Send a tweet and include
  – Your favorite speaker’s Twitter handle @111pontes
  – Two hashtags: #CLUS #MyFavoriteSpeaker

• You can submit an entry for more than one of your “favorite” speakers

• Don’t forget to follow @CiscoLive and @CiscoPress

• View the official rules at http://bit.ly/CLUSwin
Complete Your Online Session Evaluation

• Give us your feedback and you could win fabulous prizes. Winners announced daily.

• Complete your session evaluation through the Cisco Live mobile app or visit one of the interactive kiosks located throughout the convention center.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
Configuring MPLS TE and Link Information Distribution Using IS-IS (Cisco IOS)

```
mpls traffic-eng tunnels
interface TenGigabitEthernet0/1/0
  ip address 172.16.0.0 255.255.255.254
  ip router isis

mpls traffic-eng tunnels
mpls traffic-eng attribute-flags 0xF
mpls traffic-eng administrative-weight 20
  ip rsvp bandwidth 100000

router isis
  net 49.0001.1720.1625.5001.00
  is-type level-2-only
metric-style wide
mpls traffic-eng router-id Loopback0
mpls traffic-eng level-2
  passive-interface Loopback0
```

- Enable MPLS TE on this node
- Enable MPLS TE on this interface, specify attribute flags (colors), TE metric and maximum reservable bandwidth
- Enable wide metric format and TE extensions (TE Id, router level)
Configuring MPLS TE and Link Information Distribution Using OSPF (Cisco IOS XR)

```
router ospf DEFAULT
  area 0
    mpls traffic-eng
    interface Loopback0
      passive
    !
    interface TenGigE0/0/0/0
    !
    mpls traffic-eng router-id Loopback0
rsvp
  interface TenGigE0/0/0/0
    bandwidth 100000
  !
  !
  mpls traffic-eng
  interface TenGigE0/0/0/0
    admin-weight 5
    attribute-flags 0x8
  !
```

- **Enable MPLS TE extensions on this area**
- **MPLS TE router id**
- **Configuration mode for RSVP global and interface (e.g. maximum reservable bandwidth) commands**
- **Configuration mode for MPLS TE global and interface (e.g. TE metric, attribute flags) commands**
Configuring MPLS TE and Link Information Distribution Using IS-IS (Cisco NX-OS)

feature isis
feature mpls traffic-eng

interface Ethernet1/1
  mpls traffic-eng tunnels
  mpls traffic-eng administrative-weight 20
  mpls traffic-eng attribute-flags 0xf
  mpls traffic-eng bandwidth 10000000
  no switchport
  ip address 172.16.0.14/31
  ip router isis DEFAULT
  no shutdown

router isis DEFAULT
  mpls traffic-eng level-2
  mpls traffic-eng router-id loopback0
  net 49.0001.1720.1625.5202.00
  is-type level-2

Enable MPLS TE on this device
Enable MPLS TE on this interface, specify attribute flags (colors), TE metric and maximum reservable bandwidth
Enable TE extensions (TE Id, router level)
Configuring Tunnel at Head End (Cisco IOS)

interface Tunnel1
  description FROM-ROUTER-TO-DST1
  ip unnumbered Loopback0
  tunnel destination 172.16.255.3
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng priority 5 5
  tunnel mpls traffic-eng bandwidth 10000
  tunnel mpls traffic-eng affinity 0x0 mask 0xF
  tunnel mpls traffic-eng path-option 5 explicit name PATH1
  tunnel mpls traffic-eng path-option 10 dynamic

  ip explicit-path name PATH1 enable
  next-address 172.16.0.1
  next-address 172.16.8.0

Configuring Tunnel at Head End (Cisco IOS XR)

explicit-path name PATH1
index 1 next-address ipv4 unicast 172.16.0.4
index 2 next-address ipv4 unicast 172.16.0.7
index 3 next-address ipv4 unicast 172.16.4.2
!

interface tunnel-te1
description FROM-ROUTER-TO-DST1
ipv4 unnumbered Loopback0
priority 5 5
signalled-bandwidth 100000
destination 172.16.255.2
path-option 10 explicit name PATH1
path-option 20 dynamic
affinity f mask f
!

Explicit path definition
MPLS TE point-to-point tunnel
Signaled bandwidth and priority
Tunnel destination
Tunnel path options (explicit, otherwise, dynamic)
Consider links with 0xF/0xF as attribute flags (colors)
Configuring Tunnel at Head End (Cisco NX-OS)

```
mpls traffic-eng
  explicit-path name PATH1
    index 10 next-address 172.16.0.15
    index 20 next-address 172.16.0.13

interface tunnel-te1
  description FROM-ROUTER-TO-DST1
  ip unnumbered loopback0
  no shutdown
  destination 172.16.255.5
  affinity 0xf mask 0xf
  bandwidth 10000
  path-option 10 explicit name PATH1
  path-option 20 dynamic
  priority 5 5
```

- **Explicit path definition**
- **MPLS TE point-to-point tunnel**
- **Tunnel destination**
  - **Consider links with 0xF/0xF as attribute flags (colors)**
  - **Signaled bandwidth**
  - **Tunnel path options (explicit, otherwise, dynamic)**
  - **Signaled priority**
P2MP TE LSP Traffic Selection
IP Multicast

- One or more IP multicast groups mapped to a Tunnel
- Groups mapped via static IGMP join
- PIM outside of MPLS network
- Modified egress RPF check against TE LSP and tunnel head end (source address)
- Egress node may abstract TE LSP as a virtual interface (LSPVIF) for RPF purposes

<table>
<thead>
<tr>
<th>P2MP Tunnel</th>
<th>Multicast Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>(192.168.5.1, 232.0.0.1)</td>
</tr>
<tr>
<td></td>
<td>(192.168.5.1, 232.0.0.2)</td>
</tr>
<tr>
<td>Tunnel2</td>
<td>(192.168.5.1, 232.0.0.3)</td>
</tr>
</tbody>
</table>
Statically Mapping Multicast Groups to a P2MP Tunnel (Cisco IOS)

```bash
mpls traffic-eng destination list name P2MP-LIST-DST1
  ip 172.16.255.1 path-option 10 explicit name PATH1
  ip 172.16.255.2 path-option 10 dynamic
  ip 172.16.255.3 path-option 10 dynamic
  ip 172.16.255.4 path-option 10 dynamic

interface Tunnel1
  description FROM-ROUTER-TO-LIST-DST1
  ip unnumbered Loopback0

  ip pim passive
  ip igmp static-group 232.0.0.1 source 192.168.5.1
  ip igmp static-group 232.0.0.2 source 192.168.5.1

  tunnel mode mpls traffic-eng point-to-multipoint
  tunnel destination list mpls traffic-eng name P2MP-LIST-DST1
  tunnel mpls traffic-eng priority 7 7
  tunnel mpls traffic-eng bandwidth 1000
```

- Destination list with one path-option per destination
- Multipicast groups mapped to tunnel
- P2MP TE Tunnel
- Destination list
- Signaled bandwidth and setup / hold priorities
Configuring RPF Check at P2MP Tunnel Tail End (Cisco IOS)

```
ip multicast mpls traffic-eng
ip mroute 192.168.5.1 255.255.255.255 172.16.255.5
!
```

Enable IPv4 multicast over P2MP TE LSP

Tunnel source (172.16.255.5) as next-hop for IP Multicast source (192.168.5.1) RPF check
Statically Mapping Multicast Groups to a P2MP Tunnel (Cisco IOS XR)

```interface tunnel-mte1
ipv4 unnumbered Loopback0
destination 172.16.255.129
  path-option 10 explicit name PATH1
  path-option 20 dynamic

destination 172.16.255.130
  path-option 10 dynamic

priority 0 0
  signalled-bandwidth 100000

node-capability label-switched-multicast
  multicast-routing
  address-family ipv4

interface tunnel-mte1
  enable

interface all enable

router igmp
  vrf default

interface tunnel-mte1
  static-group 232.0.0.1 192.168.5.1
  static-group 232.0.0.2 192.168.5.1
```

- **MPLS TE P2MP tunnel**
- **Destination with path-option list**
- **Destination with single path-option**
- **Signaled bandwidth and setup / hold priorities**
- **Enable MPLS multicast**
- **Enable multicast forwarding over tunnel-mte1**
- **Multicast groups mapped to tunnel-mte1**
Configuring RPF Check at P2MP Tunnel Tail End (Cisco IOS XR)

```
multicast-routing
  address-family ipv4
    core-tree-protocol rsvp-te
    static-rpf 192.168.5.1 32 mpls 172.16.255.3
    interface all enable

!    
```
Configuring MPLS TE and Link Information Distribution Using OSPF (Cisco IOS)

```plaintext
! mpls traffic-eng tunnels
! interface TenGigabitEthernet0/1/0
   ip address 172.16.0.0 255.255.255.254

! mpls traffic-eng tunnels
   mpls traffic-eng attribute-flags 0xF
   mpls traffic-eng administrative-weight 20
   ip rsvp bandwidth 100000

! router ospf 100
   log-adjacency-changes
   passive-interface Loopback0
   network 172.16.0.0 0.0.255.255 area 0

! mpls traffic-eng router-id Loopback0
! mpls traffic-eng area 0
```

- Enable MPLS TE on this node
- Enable MPLS TE on this interface
- Attribute flags
- TE metric
- Maximum reservable bandwidth
- Enable TE extensions (TE router id and area)
Configuring MPLS TE and Link Information Distribution Using IS-IS (Cisco IOS XR)

```
router isis DEFAULT
  is-type level-2-only
  net 49.0001.1720.1625.5129.00
  address-family ipv4 unicast
    metric-style wide
    mpls traffic-eng level 2
    mpls traffic-eng router-id Loopback0

  ! interface Loopback0
  passive
  address-family ipv4 unicast
  ! interface TenGigE0/0/0/0
  address-family ipv4 unicast
  !

rsvp
  interface TenGigE0/0/0/0
  bandwidth 100000
  !

mpls traffic-eng
  interface TenGigE0/0/0/0
  admin-weight 5
  attribute-flags 0x8
```
P2MP TE LSP Traffic Selection
Static P2MP Pseudowires

- Provides a layer-2 multicast service with segmentation
- Multicast forwarding plane from root to leaves (all traffic types: multicast, broadcast, unicast)
- Unicast forwarding plane from leaves to root
- Initial implementation supporting only static pseudowire
- Label bindings defined statically on root and leaves
- No control plane (targeted LDP)
- No context-specific label space on leaves
A solution when:
- No differentiation required
- Optimization required
- Full mesh or selective deployment to avoid over-subscription
- Increased network utilization
- Adjust link load to actual link capacity
- No notion of traffic classes
Network with MPLS DiffServ and MPLS TE

• A solution when:
  Differentiation required
  Optimization required

• Adjust **class** capacity to expected **class** load

• Adjust **class** load to actual **class** capacity for one **class**

• Alternatively, adjust **link** load to actual **link** capacity
Network with MPLS DiffServ and MPLS DS-TE

- A solution when:
  - Strong differentiation required
  - Fine optimization required
- Control both load and capacity per class
- Adjust class capacity to expected class load
- Adjust class load to actual class capacity
Pre-standard DS-TE Implementation

• Only supports Russian Dolls Model (RDM) for bandwidth constraints

• No changes to RSVP-TE specs to signal desired pool (leverages ADSPEC object in PATH messages)
  Sub-pool TE LSPs signaled as guaranteed service
  Global pool TE LSPs signaled as controlled-load service

• Modified OSPF-TE and ISIS-TE advertisements to include two pools at 8 priority levels each (16 entries per link total)

• Available on IOS and IOS XR
What Is New in IETF DS-TE Implementation?

• Supports both RDM and MAM (Maximum Allocation Model) for bandwidth constraints

• New CLASSTYPE object in RSVP-TE to signal desired class-type (unused by “class-type 0” for backward compatibility with non-DS-TE)

• Minor Changes to OSPF-TE and ISIS-TE bandwidth advertisements
  - Same “unreserved bandwidth” sub-TLV (8 entries) as non-DS-TE interpreted according to local definition of TE-Class (class-type/preemption priority)
  - New BC sub-TLV

• Operates in migration or IETF mode in Cisco IOS

• Developed simultaneously for IOS and IOS XR
# TE-Class Definition Examples

**TE-Class definition ****MUST** be consistent throughout the network

## Default TE-Class definition

<table>
<thead>
<tr>
<th></th>
<th>Priority 0</th>
<th>Priority 1</th>
<th>Priority 2</th>
<th>Priority 3</th>
<th>Priority 4</th>
<th>Priority 5</th>
<th>Priority 6</th>
<th>Priority 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT0 (Global)</td>
<td>TE-Class4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TE-Class0</td>
</tr>
<tr>
<td>CT1 (Sub)</td>
<td>TE-Class5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TE-Class1</td>
</tr>
</tbody>
</table>

## TE-Class definition compatible with non-DS-TE

<table>
<thead>
<tr>
<th></th>
<th>Priority 0</th>
<th>Priority 1</th>
<th>Priority 2</th>
<th>Priority 3</th>
<th>Priority 4</th>
<th>Priority 5</th>
<th>Priority 6</th>
<th>Priority 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT0 (Global)</td>
<td>TE-Class0</td>
<td>TE-Class1</td>
<td>TE-Class2</td>
<td>TE-Class3</td>
<td>TE-Class4</td>
<td>TE-Class5</td>
<td>TE-Class5</td>
<td>TE-Class7</td>
</tr>
<tr>
<td>CT1 (Sub)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## User-defined TE-Cla**s with no preemption between class-types

<table>
<thead>
<tr>
<th></th>
<th>Priority 0</th>
<th>Priority 1</th>
<th>Priority 2</th>
<th>Priority 3</th>
<th>Priority 4</th>
<th>Priority 5</th>
<th>Priority 6</th>
<th>Priority 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT0 (Global)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TE-Class4</td>
<td>TE-Class5</td>
<td>TE-Class6</td>
<td>TE-Class7</td>
</tr>
<tr>
<td>CT1 (Sub)</td>
<td>TE-Class0</td>
<td>TE-Class1</td>
<td>TE-Class2</td>
<td>TE-Class3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## User-defined TE-Cla**s with preemption between/within class-types

<table>
<thead>
<tr>
<th></th>
<th>Priority 0</th>
<th>Priority 1</th>
<th>Priority 2</th>
<th>Priority 3</th>
<th>Priority 4</th>
<th>Priority 5</th>
<th>Priority 6</th>
<th>Priority 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>CT0 (Global)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TE-Class7</td>
</tr>
<tr>
<td>CT1 (Sub)</td>
<td>TE-Class0</td>
<td>TE-Class1</td>
<td>TE-Class2</td>
<td>TE-Class3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

User-defined TE-Cla**ses with no preemption between class-types

User-defined TE-Cla**ses with preemption between/within class-types

**Default TE-Class definition**

**TE-Class definition compatible with non-DS-TE**

**User-defined TE-Class with no preemption between class-types**

**User-defined TE-Class with preemption between/within class-types**
## MAM vs. RDM

<table>
<thead>
<tr>
<th>MAM</th>
<th>RDM</th>
</tr>
</thead>
<tbody>
<tr>
<td>One BC per CT</td>
<td>One or more CTs per BC</td>
</tr>
<tr>
<td>Sum of all BCs may exceed maximum reservable bandwidth</td>
<td>BC0 always equals to maximum reservable bandwidth</td>
</tr>
<tr>
<td>Preemption not required to provide bandwidth guarantees per CT</td>
<td>Preemption required to provide bandwidth guarantees per CT</td>
</tr>
<tr>
<td>Bandwidth efficiency and protection against QoS degradation are mutually exclusive</td>
<td>Provides bandwidth efficiency and protection against QoS degradation simultaneously</td>
</tr>
</tbody>
</table>
Configuring DS-TE Classes and Bandwidth Constraints (Cisco IOS)

RDM

```plaintext
mpls traffic-eng tunnels
mpls traffic-eng ds-te mode ietf
mpls traffic-eng ds-te te-classes
te-class 0 class-type 1 priority 0
te-class 1 class-type 1 priority 1
te-class 2 class-type 1 priority 2
te-class 3 class-type 1 priority 3
te-class 4 class-type 0 priority 4
te-class 5 class-type 0 priority 5
te-class 6 class-type 0 priority 6
te-class 7 class-type 0 priority 7
!
interface TenGigabitEthernet0/1/0
  ip address 172.16.0.0 255.255.255.254
  mpls traffic-eng tunnels
  ip rsvp bandwidth rdm bc0 155000 bc1 55000
```

Enable IETF DS-TE
Explicit TE-Class definition
RDM bandwidth constraints

MAM

```plaintext
mpls traffic-eng tunnels
mpls traffic-eng ds-te mode ietf
mpl traffic-eng ds-te bc-model mam
!
interface TenGigabitEthernet0/1/0
  ip address 172.16.0.0 255.255.255.254
  mpls traffic-eng tunnels
  ip rsvp bandwidth mam max-reservable-bw 155000 bc0 100000 bc1 55000
```

Enable IETF DS-TE and use default TE-Class definition
Enable MAM
MAM bandwidth constraints
Configuring DS-TE Tunnel (Cisco IOS)

interface Tunnel1
description FROM-ROUTER-TO-DST1-CT0
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 172.16.255.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 5 5
tunnel mpls traffic-eng bandwidth 100000 class-type 0
tunnel mpls traffic-eng path-option 10 dynamic

Signal Tunnel1
with CT0 (priority and CT must match valid TE-Class)

interface Tunnel2
description FROM-ROUTER-TO-DST1-CT1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 172.16.255.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 0 0
tunnel mpls traffic-eng bandwidth 50000 class-type 1
tunnel mpls traffic-eng path-option 10 dynamic

Signal Tunnel2
with CT1 (priority and CT must match valid TE-Class)
Configuring DS-TE Classes and Bandwidth Constraints (Cisco IOS XR)

RDM

```conf
rsvp
interface TenGigE0/0/0/0
bandwidth rdm bc0 155000 bc1 55000
!
! mpls traffic-eng
interface TenGigE0/0/0/0
! ds-te mode intf
ds-te te-classes
te-class 0 class-type 1 priority 0
te-class 1 class-type 1 priority 1
te-class 2 class-type 1 priority 2
te-class 3 class-type 1 priority 3
te-class 4 class-type 0 priority 4
te-class 5 class-type 0 priority 5
te-class 6 class-type 0 priority 6
te-class 7 class-type 0 priority 7
!
! rsvp
interface TenGigE0/0/0/0
bandwidth mam max-reservable-bw 155000 bc0 100000 bc1 55000
!
! mpls traffic-eng
interface TenGigE0/0/0/0
! ds-te mode intf
ds-te bc-model mam
!
```

Enable IETF DS-TE
Explicit TE-Class definition
RDM bandwidth constraints

MAM

```conf
rsvp
interface TenGigE0/0/0/0
bandwidth mam max-reservable-bw 155000 bc0 100000 bc1 55000
!
! mpls traffic-eng
interface TenGigE0/0/0/0
! ds-te mode intf
ds-te bc-model mam
!
```

Enable IETF DS-TE and use default TE-Class definition
MAM bandwidth constraints
Enable MAM
Configuring DS-TE Tunnels (Cisco IOS XR)

interface tunnel-te1
description FROM-ROUTER-TO-DST1-CT0
ipv4 unnumbered Loopback0
priority 5 5
signalled-bandwidth 100000 class-type 0
destination 172.16.255.2
path-option 10 dynamic
!
interface tunnel-te2
description FROM-ROUTER-TO-DST1-CT1
ipv4 unnumbered Loopback0
priority 0 0
signalled-bandwidth 50000 class-type 1
destination 172.16.255.2
path-option 10 dynamic
!

Signal tunnel-te1 with CT0 (priority and CT must match valid TE-Class)

Signal tunnel-te2 with CT1 (priority and CT must match valid TE-Class)
Policy-based Tunnel Selection: PBTS

- EXP-based selection between multiple tunnels to same destination
- Local mechanism at head-end
- Tunnels configured via policy-class or forwarding-class with EXP values to carry
- No IGP extensions
- Supports VRF traffic, IP-to-MPLS and MPLS-to-MPLS switching

<table>
<thead>
<tr>
<th>Prefix</th>
<th>EXP</th>
<th>Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix1, exp 5</td>
<td></td>
<td>tunnel-te1</td>
</tr>
<tr>
<td>Prefix1, *</td>
<td></td>
<td>tunnel-te2</td>
</tr>
<tr>
<td>Prefix2, exp 5</td>
<td></td>
<td>tunnel-te3</td>
</tr>
<tr>
<td>Prefix2, exp 2</td>
<td></td>
<td>tunnel-te4</td>
</tr>
<tr>
<td>Prefix2, *</td>
<td></td>
<td>tunnel-te5</td>
</tr>
<tr>
<td>Prefix3, exp 5</td>
<td></td>
<td>tunnel-te6</td>
</tr>
<tr>
<td>Prefix3, *</td>
<td></td>
<td>tunnel-te7</td>
</tr>
</tbody>
</table>
Class-Based Tunnel Selection: CBTS

- EXP-based selection between **multiple tunnels** to **same destination**
- Local mechanism at head-end (no IGP extensions)
- Tunnel master bundles tunnel members
- Tunnel selection configured on tunnel master (auto-route, etc.)
- Bundle members configured with EXP values to carry
- Bundle members may be configured as default
- Supports VRF traffic, IP-to-MPLS and MPLS-to-MPLS switching paths
Configuring CBTS (Cisco IOS)

```cisco
interface Tunnel1
  ip unnumbered Loopback0
  tunnel destination 172.16.255.2
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng bandwidth 50000 class-type 1
  tunnel mpls traffic-eng path-option 10 dynamic

  tunnel mpls traffic-eng exp 5

! interface Tunnel2
  ip unnumbered Loopback0
  tunnel destination 172.16.255.2
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng bandwidth 100000 class-type 0
  tunnel mpls traffic-eng path-option 10 dynamic

  tunnel mpls traffic-eng exp default

! interface Tunnel10
  ip unnumbered Loopback0
  tunnel destination 172.16.255.2
  tunnel mode mpls traffic-eng

  tunnel mpls traffic-eng exp-bundle master
  tunnel mpls traffic-eng exp-bundle member Tunnel1
  tunnel mpls traffic-eng exp-bundle member Tunnel2

  ip route 192.168.0.0 255.255.255.0 Tunnel10
```

- **Tunnel1** will carry packets with MPLS EXP 5
- **Tunnel2** will carry packets with MPLS EXP other than 5
- **Tunnel10** defined as bundle master with **Tunnel2** and **Tunnel1** as members
- CBTS performed on prefix 192.168.0.0/24 using Tunnel10
Configuring PBTS (Cisco IOS XR)

interface tunnel-te1
  ipv4 unnumbered Loopback0
  autoroute announce
  signalled-bandwidth 10000
  destination 172.16.255.2
  policy-class 5
    path-option 10 explicit name PATH1
    path-option 20 dynamic
  
interface tunnel-te2
  ipv4 unnumbered Loopback0
  autoroute announce
  signalled-bandwidth 50000
  destination 172.16.255.2
  path-option 10 explicit name PATH2
  path-option 20 dynamic

**Why this configuration?**
- **tunnel-te1** will carry packets with MPLS EXP 5
- **tunnel-te2** will carry packets with MPLS EXP other than 5 (default tunnel)
Tunnel-based Admission Control

- Tunnel aggregates RSVP (IPv4) flows
- No per-flow state in forwarding plane (only DiffServ)
- No per-flow state in control plane within MPLS TE network
- RSVP enhancements enable end-to-end admission control solution (Receiver Proxy, Sender Notification, Fast Local Repair)
Configuring Tunnel-based Admission Control (Cisco IOS)

interface Tunnel1
  ip unnumbered Loopback0
  tunnel destination 172.16.255.2
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng priority 7 7
  tunnel mpls traffic-eng bandwidth 100000
  tunnel mpls traffic-eng path-option 10 dynamic

ip rsvp policy local default
  maximum senders 200
  maximum bandwidth single 1000
  forward all
  ip rsvp bandwidth 100000

interface GigabitEthernet3/3/0
  ip address 192.168.0.1 255.255.255.254
  service-policy output OUT-POLICY
  ip rsvp bandwidth percent 10
  ip rsvp listener outbound reply
  ip rsvp data-packet classification none
  ip rsvp resource-provider none
  ip rsvp qos

Signed bandwidth
RSVP local policy (200 flows max, 1Mbps per flow max)
Maximum reservable bandwidth
Interface QoS policy (DiffServ)
Maximum reservable bandwidth
Act as RSVP receiver proxy on this interface
No RSVP flow classification
No RSVP flow queuing
Enable per-flow RSVP
Configuring FRR (Cisco IOS)

**Primary Tunnel**

```
interface Tunnel1
    description FROM-ROUTER-TO-DST1-FRR
    ip unnumbered Loopback0
    tunnel destination 172.16.255.2
    tunnel mode mpls traffic-eng
    tunnel mpls traffic-eng bandwidth 20000
    tunnel mpls traffic-eng path-option 10 dynamic
    tunnel mpls traffic-eng fast-reroute
```

**Backup Tunnel**

```
interface Tunnel1
    description NNHOP-BACKUP
    ip unnumbered Loopback0
    tunnel destination 172.16.255.2
    tunnel mode mpls traffic-eng
    tunnel mpls traffic-eng path-option 10 explicit name PATH1

    !
    interface TenGigabitEthernet1/0/0
    ip address 172.16.192.5 255.255.255.254
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
    !
```

- Indicate the desire for local protection during signaling
- Explicitly routed backup to 172.16.255.2 with zero bandwidth
- Use Tunnel1 as backup for protected LSPs through TenGigabitEthernet1/0/0
Configuring FRR (Cisco IOS XR)

### Primary Tunnel

```conf
interface tunnel-te1
description FROM-ROUTER-TO-DST1-FRR
ipv4 unnumbered Loopback0
signalled-bandwidth 30000
destination 172.16.255.2
    fast-reroute
    path-option 10 dynamic
```

- Indicate the desire for local protection during signaling.

### Backup Tunnel

```conf
interface tunnel-te1
description NHOP-BACKUP
ipv4 unnumbered Loopback0
destination 172.16.255.130
    path-option 10 explicit name PATH1
```

- Explicitly routed backup to 172.16.255.130 with zero bandwidth.

```conf
mpls traffic-eng
interface TenGigE0/0/0/0
    backup-path tunnel-te1
```

- Use tunnel-te1 as backup for protected LSPs through TenGigE0/0/0/0.
AutoTunnel: Primary Tunnels

Why One-Hop Tunnels?

- CSPF and SPF yield same results (absence of tunnel constraints)
- Auto-route forwards all traffic through one-hop tunnel
- Traffic logically mapped to tunnel but no label imposed (imp-null)
- Traffic is forwarded as if no tunnel was in place
AutoTunnel: Backup Tunnels
What’s the Solution? (Cont.)

• Backup tunnels are preconfigured
  Priority  7/7
  Bandwidth 0
  Affinity 0x0/0xFFFF
  Auto-BW OFF
  Auto-Route OFF
  Fast-Reroute OFF
  Forwarding-Adj OFF
  Load-Sharing OFF

• Backup tunnel interfaces and paths not shown on router configuration
Configuring SRLG (Cisco IOS)

```plaintext
mpls traffic-eng tunnels
mpls traffic-eng auto-tunnel backup nhop-only
mpls traffic-eng auto-tunnel backup srlg exclude force
!
interface TenGigabitEthernet0/1/0
  ip address 172.16.0.0 255.255.255.254
mpls traffic-eng tunnels
mpls traffic-eng srlg 15
mpls traffic-eng srlg 25
ip rsvp bandwidth
!
interface TenGigabitEthernet1/0/0
  ip address 172.16.0.2 255.255.255.254
mpls traffic-eng tunnels
mpls traffic-eng srlg 25
ip rsvp bandwidth
!
```

- **Force SRLG exclusion during backup path computation**
- **Interface member of SRLG 15 and 25**
- **Interface member of SRLG 25**
Configuring Path Protection (Cisco IOS)

interface Tunnel1
ip unnumbered Loopback0
tunnel mode mpls traffic-eng
tunnel destination 172.16.255.2
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 explicit name PATH1
tunnel mpls traffic-eng path-option 20 explicit name PATH2

| tunnel mpls traffic-eng path-option protect 10 explicit name PPATH1 |
| tunnel mpls traffic-eng path-option protect 20 explicit name PPATH2 |

Standby path to be used for PATH1
Standby path to be used for PATH2
Configuring Enhanced Path Protection (Cisco IOS)

```conf
mpls traffic-eng path-option list name PATH-LST
    path-option 10 explicit name PE1-P3-P4-PE2
    path-option 20 explicit name PE1-P5-P6-PE2
    path-option 30 explicit name PE1-P7-P8-PE2
!
interface Tunnel1
    ip unnumbered Loopback0
    tunnel mode mpls traffic-eng
    tunnel destination 172.16.255.2
    tunnel mpls traffic-eng autoroute announce
    tunnel mpls traffic-eng path-option 10 explicit name PE1-P1-P2-PE2

    tunnel mpls traffic-eng path-option protect 10 list name PATH-LST
!
```

- **List of standby paths**
- **Use path list to protect primary path**
Configuring Path Protection (Cisco IOS XR)

interface tunnel-te1
description FROM-ROUTER-TO-DST1
ipv4 unnumbered Loopback0
signalled-bandwidth 100000
destination 172.16.255.2
affinity f mask f

**path-protection**
path-option 10 explicit name PATH1
path-option 20 explicit name PATH2
path-option 30 dynamic
!

Signal an acceptable (node-link, node, link diverse) standby TE LSP based on path-option sequence
Inter-Domain TE – TE LSP Reoptimization

- Reoptimization can be timer/event/admin triggered
- Head end sets ‘path re-evaluation request’ flag (SESSION_ATTRIBUTE)
- Head end receives PathErr message notification from boundary router if a preferable path exists
- Make-before-break TE LSP setup can be initiated after PathErr notification
Configuring Inter-Area Tunnels (Cisco IOS)

```plaintext
mpls traffic-eng tunnels
!
interface Tunnel1
  ip unnumbered Loopback0
  no ip directed-broadcast
  tunnel destination 172.16.255.7
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng path-option 10 explicit name LOOSE-PATH
!
ip route 172.16.255.7 255.255.255.255 Tunnel1
!
ip explicit-path name LOOSE-PATH enable
  next-address loose 172.16.255.3
  next-address loose 172.16.255.5
!
```

Loose-hop path
Static route mapping IP traffic to Tunnel1
List of ABRs as loose hops
Configuring Inter-Area Tunnels with Autoroute Destinations (Cisco IOS)

interface Tunnel1
ip unnumbered Loopback0
tunnel mode mpls traffic-eng
tunnel destination 172.16.255.7

**tunnel mpls traffic-eng autoroute destination**
**tunnel mpls traffic-eng path-option 10 explicit name LOOSE-PATH**
!
ip explicit-path name LOOSE-PATH enable

**next-address loose 172.16.255.3**
**next-address loose 172.16.255.5**
!

Create static route to tunnel destination (172.16.255.7)
Loose-hop path
List of **ABRs** as loose hops
Configuring Inter-Area Tunnels (Cisco IOS XR)

```
explicit-path name LOOSE-PATH

  index 1 next-address loose ipv4 unicast 172.16.255.129
  index 2 next-address loose ipv4 unicast 172.16.255.131

!
interface tunnel-te1
description FROM-ROUTER-TO-DST3
ipv4 unnumbered Loopback0
destination 172.16.255.2

  path-option 10 explicit name LOOSE-PATH

!
router static

  address-family ipv4 unicast
    172.16.255.2/32 tunnel-te1

!```

- **List of ABRs as loose hops**
- **Loose-hop path**
- **Static route mapping IP traffic to tunnel-te1**
Configuring Inter-AS Tunnels (Cisco IOS)

```plaintext
mpls traffic-eng tunnels
!
interface Tunnel1
  ip unnumbered Loopback0
  no ip directed-broadcast
  tunnel destination 172.31.255.5
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng priority 7 7
  tunnel mpls traffic-eng bandwidth 1000
  tunnel mpls traffic-eng path-option 10 explicit name LOOSE-PATH
!
ip route 172.31.255.5 255.255.255.255 Tunnel1
!
ip explicit-path name LOOSE-PATH enable
  next-address loose 172.24.255.1
  next-address loose 172.31.255.1
!
```

- **Loose-hop path**
- **Static route mapping IP traffic to Tunnel1**
- **List of ASBRs as loose hops**
Inter-Domain TE – Authentication and Policy Control

- Authentication and policy control desirable for Inter-AS deployments
- ASBR may perform RSVP authentication (MD5/SHA-1)
- ASBR may enforce a local policy for Inter-AS TE LSPs (e.g. limit bandwidth, message types, protection, etc.)
Configuring Inter-AS TE at ASBR (Cisco IOS)

```cisco
mpls traffic-eng tunnels
!
key chain A-ASBR1-key
key 1
  key-string 7 151F0E180922F222A
!
interface Serial1/0
  ip address 192.168.0.1 255.255.255.252
  mpls traffic-eng tunnels
mpls traffic-eng passive interface nbc te id 172.16.255.4 nbc igp id ospf 172.16.255.4
  ip rsvp bandwidth
  ip rsvp authentication key-chain A-ASBR1-key
  ip rsvp authentication type sha 1
  ip rsvp authentication
!
routing bgp 65024
  no synchronization
  bgp log-neighbor-changes
  neighbor 172.24.255.3 remote-as 65024
  neighbor 172.24.255.3 update-source Loopback0
  neighbor 192.168.0.2 remote-as 65016
  no auto-summary
!
ip rsvp policy local origin-as 65016
  no fast-reroute
  maximum bandwidth single 10000
  forward all
```

- **Authentication key**
- **Add ASBR link to TE topology database**
- **Enable RSVP authentication**
- **Process signaling from AS 65016 if FRR not requested and 10M or less**
Distributed Path Computation with Backward Recursive PCE-based Computation (BRPC)

- Head-end sends request to a path computation element (PCE)
- PCE recursively computes virtual shortest path tree (SPT) to destination
- Head-end receives reply with virtual SPT if a path exists
- Head-end uses topology database and virtual SPT to compute end-to-end path
- Head-end can discover PCEs dynamically or have them configured statically
Configuring MPLS TE and LDP Simultaneously (Cisco IOS)

```
mls label protocol ldp
mls traffic-eng tunnels
!
interface TenGigabitEthernet0/1/0
   ip address 172.16.0.0 255.255.255.254
   mpls traffic-eng tunnels
   mpls ip
   ip rsvp bandwidth 155000
!
```

- Enable LDP
- Enable MPLS TE
- Enable MPLS TE on interface
- Enable MPLS forwarding for IP (LDP)
Configuring MPLS TE and LDP Simultaneously (Cisco IOS XR)

- Configuration mode for RSVP global and interface commands
  ```
  rsvp
  interface TenGigE0/0/0/0
  bandwidth 155000
  !
  !
  ```

- Configuration mode for MPLS TE global and interface commands
  ```
  mpls traffic-eng
  interface TenGigE0/0/0/0
  !
  !
  ```

- Configuration mode for LDP global and interface commands
  ```
  mpls ldp
  interface TenGigE0/0/0/0
  !
  !
  ```
Configuring LDP Over a TE Tunnel (Cisco IOS)

```
mpls label protocol ldp
mpls traffic-eng tunnels
!
interface Tunnel1
ip unnumbered Loopback0
mpls ip
  tunnel destination 172.16.255.3
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng path-option 10 dynamic
!
```

Enable MPLS forwarding for IP (LDP) on Tunnel1

Enable LDP
Enable LDP on tunnel-te1
MPLS TE on Ethernet Bundle (Cisco IOS)

interface Port-channel1
   ip address 172.16.0.0 255.255.255.254

  mpls traffic-eng tunnels
  mpls traffic-eng attribute-flags 0xF
  mpls traffic-eng administrative-weight 20
  ip rsvp bandwidth percent 100

! interface GigabitEthernet2/0/0
   no ip address

channel-protocol lacp
channel-group 1 mode active

! interface GigabitEthernet2/0/1
   no ip address

channel-protocol lacp
channel-group 1 mode active

Enable MPLS TE on this interface
Attribute flags
TE metric
Maximum reservable bandwidth (100% of total bundle bandwidth)
LACP as channel protocol
Associate with Port-channel1 and enable LACP (non-passive)
LACP as channel protocol
Associate with Port-channel1 and enable LACP (non-passive)
MPLS TE on Ethernet Bundle (Cisco IOS XR)

```
interface Bundle-Ether1
  ipv4 address 172.16.0.1 255.255.255.254
!
interface GigabitEthernet0/1/0/0
bundle id 1 mode active
  negotiation auto
!
interface GigabitEthernet0/1/0/1
bundle id 1 mode active
  negotiation auto
  !
  router ospf 172
    area 0
    mpls traffic-eng
  interface Bundle-Ether1
    network point-to-point
    !
    interface Loopback0
    passive enable
    !
    mpls traffic-eng router-id Loopback0
  !
rsvp
  interface Bundle-Ether1
    bandwidth 2000000
    !
    mpls traffic-eng
  interface Bundle-Ether1
```

- Interface for bundle id 1
- Associate with bundle id 1 (Bundle-Ether1) and enable LACP (non-passive)
- Associate with bundle id 1 (Bundle-Ether1) and enable LACP (non-passive)
- Enable OSPF on bundle
- Maximum reservable bandwidth on bundle
- Enable MPLS TE on bundle
Per-VRF Tunnel Selection (Cisco IOS)

```
ip vrf RED  
   rd 65172:2  
   route-target export 65172:2  
   route-target import 65172:2  
   bgp next-hop Loopback1  
!
interface Loopback0  
ip address 172.16.255.1 255.255.255.255  
!
interface Loopback1  
ip address 172.16.255.101 255.255.255.255  
!
interface Tunnel1  
description FROM-ROUTER-VRF-TO-DST1  
ip unnumbered Loopback0  
tunnel destination 172.16.255.2  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng path-option 10 dynamic  
!
ip route 172.16.255.102 255.255.255.255 Tunnel1  
```

Loopback1 advertised as next hop for VRF RED

Remote next hop mapped to Tunnel1
Inter-Domain Traffic Engineering
Inter-Domain Traffic Engineering: Introduction

• Domain defined as an IGP area or autonomous system
• Head end lacks complete network topology to perform path computation in both cases
• Two path computation approaches
  Per-domain (ERO loose-hop expansion)
  Distributed (Path Computation Element)
Per-Domain Path Computation Using ERO Loose-hop Expansion
Distributed Path Computation using Path Computation Element

Backward Recursive PCE-based Computation (BRPC)

Path (cost 500): R3, ABR3, ABR4, R5, R7

R1 Topology database

Path1 (cost 400): ABR1, ABR2, R4, R6 R7
Path2 (cost 300): ABR3, ABR4, R5, R7

Virtual Shortest Path Tree

ABR1 Topology database (area 0)

Path1 (cost 300): ABR2, R4, R6 R7
Path2 (cost 200): ABR4, R5, R7

Virtual Shortest Path Tree

ABR2 Topology database (area 3)
Configuring PCE (Cisco IOS XR)

**Headend**

```plaintext
interface tunnel-te1
description FROM-ROUTER-TO-DST2
ipv4 unnumbered Loopback0
destination 172.16.255.1
  path-option 10 dynamic pce
router static
  address-family ipv4 unicast
    172.16.255.1/32 tunnel-te1
```

**PCE**

```plaintext
mpls traffic-eng
  pce deadtimer 30
  pce address ipv4 172.16.255.129
  pce keepalive 10
```

- Use discovered PCEs for path computation
- Static route mapping IP traffic to tunnel-te1
- Declare peer down if no keepalive in 30s
- Advertise PCE capability with address 172.16.255.129
- Send per keepalive every 10s
Inter-Domain TE – Fast Re-route

• Same configuration as single domain scenario
• Support for node-id sub-object required to implement ABR/ASBR node protection
• Node-id helps point of local repair (PLR) detect a merge point (MP)
Inter-Domain TE
Take into Account before Implementing

• Semantics of link attributes across domain boundaries
• Semantics of TE-Classes across domain boundaries for DS-TE
• Auto-route destinations creates a static route to tunnel destination and facilitates traffic selection
• Auto-route announce not applicable for traffic selection
Scaling Signaling (Refresh Reduction)

- RSVP soft state needs to be refreshed periodically
- Refresh reduction extensions use message Identifier associated with Path/Resv state
- Summary Refresh (SRefresh) message refreshes state using a message_id list
- SRefresh only replaces refresh Path/Resv messages
Configuring Refresh Reduction (Cisco IOS)

```plaintext
mpls traffic-eng tunnels
!
interface TenGigabitEthernet0/1/0
  ip address 172.16.0.0 255.255.255.254
mpls traffic-eng tunnels
ip rsvp bandwidth 100000
!
router ospf 100
  log-adjacency-changes
  passive-interface Loopback0
  network 172.16.0.0 0.0.255.255 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
!
ip rsvp signalling refresh reduction
```

* Enabled by default in Cisco IOS XR
Thank you.