What You Make Possible
Designing Access Network With the ME3600X and ME3800X

Nicolas Breton
Product Manager Cisco

Waris Sagheer
TME Architect Cisco
Agenda

- Platform introduction
- Design with Ethernet Virtual Circuit (EVC)
- Quality of Services with ME3600X and ME3800X
- Design with MPLS
- Design with OAM
- Platform Security
- Scale Profiles
- Case Studies
Platform Introduction
What is the Access?

Unified Access

ME36/3800 Roles in the Network
- CPE
- UPE
- Pre-Aggregation

Applications
- Service Provider Wireline
- Service Provider Mobile
- Carrier Ethernet
- Enterprise Edge
What is the Access?

Residential Services
- High Speed Internet
- VOIP
- IPTV, VoD

Business L2 Services
- E-LINE
- E-LAN
- E-TREE

Mobile Backhaul

Business L3 Services
- L3VPN
Introducing ME3800 / 3600X
Flexible Service Delivery at 10G

Carrier Ethernet Switch Routers:
- Cisco ME 3800X

Cisco ME 3600X (Copper & Fiber)

Cisco ME 3600X 24CX

ME3600X 24FS/24TS, ME3800X

<table>
<thead>
<tr>
<th>Small Form Factor</th>
<th>1RU, 20” depth</th>
<th>2RU, 15.5” depth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>24 GE 2 10GE SFP+</td>
<td>24 GE 4 10GE XFP 16 T1/E2, 4 OC3</td>
</tr>
<tr>
<td>Power Option</td>
<td>AC or DC modular includes +24VDC option</td>
<td></td>
</tr>
</tbody>
</table>

- Key Highlights
  - MPLS on all ports
  - H-QoS with Deep Buffers
  - Timing: SynchE, BITS
  - EVC
  - Ethernet OAM
ME 3600X Build for the Access

- Service Termination
  - Ethernet Virtual Circuit
  - QoS Policies
  - Security
- OAM
  - Fault Monitoring
  - Performance Monitoring

<table>
<thead>
<tr>
<th>Feature</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC addresses</td>
<td>16,000</td>
</tr>
<tr>
<td>EFP</td>
<td>4,000</td>
</tr>
<tr>
<td>Bridge Domains</td>
<td>4,000</td>
</tr>
<tr>
<td>IPv4</td>
<td>24,000 IPv4 routes</td>
</tr>
<tr>
<td>MPLS</td>
<td>512 PW</td>
</tr>
<tr>
<td></td>
<td>128 MPLS VPNs</td>
</tr>
<tr>
<td>QoS</td>
<td>4,000 queues</td>
</tr>
<tr>
<td></td>
<td>2,000 ingress policers</td>
</tr>
<tr>
<td></td>
<td>4,000 egress shapers</td>
</tr>
<tr>
<td>Multicast groups</td>
<td>1,000</td>
</tr>
</tbody>
</table>
ME 3800X in the aggregation

- Aggregation
- EVC
- QoS Policies
- Multicast
- Resiliency

Scale for the Aggregation

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC addresses</td>
<td>256,000</td>
</tr>
<tr>
<td>EFP</td>
<td>16,000</td>
</tr>
<tr>
<td>Bridge Domains</td>
<td>8,000</td>
</tr>
<tr>
<td>IPv4</td>
<td>80,000 IP v4 routes</td>
</tr>
<tr>
<td>MPLS</td>
<td>16,000 PW 2,000 MPLS VPN</td>
</tr>
<tr>
<td>Qos</td>
<td>32,000 queues 16,000 ingress policers 32,000 egress shapers</td>
</tr>
<tr>
<td>Multicast groups</td>
<td>4,000</td>
</tr>
</tbody>
</table>
# Comparing ME3600X Series and ME3800X Series

<table>
<thead>
<tr>
<th></th>
<th>ME 3600X</th>
<th>ME 3800X</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Ethernet Access Switch</td>
<td>Carrier Ethernet Switch Router</td>
</tr>
<tr>
<td><strong>Deployment</strong></td>
<td>Access</td>
<td>Aggregation</td>
</tr>
<tr>
<td><strong>SKU</strong></td>
<td>ME3600X-24TS (Copper)</td>
<td>ME3800X-24FS (Fiber)</td>
</tr>
<tr>
<td><strong>10Gig SFP +</strong></td>
<td>10Gig License Required</td>
<td>No 10Gig License Required</td>
</tr>
<tr>
<td></td>
<td>(SFP+ slots can be used for 1Gig SFP without any additional license)</td>
<td>(SFP+ slots can be used for 1Gig SFP without any additional license)</td>
</tr>
<tr>
<td><strong>Features</strong></td>
<td>Same Features MPLS/L3VPN/L2VPN/BGP/IGP</td>
<td></td>
</tr>
<tr>
<td><strong>Buffers</strong></td>
<td>44 MBytes</td>
<td>352 MBytes</td>
</tr>
<tr>
<td><strong>VPLS</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Medium</td>
<td>Large</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td>Two Licenses</td>
<td>Six Licenses</td>
</tr>
<tr>
<td></td>
<td>Metro IP Access (IPv4 &amp; Layer2)</td>
<td>Metro Ethernet Services (Layer2 Only)</td>
</tr>
<tr>
<td></td>
<td>Advanced Metro IP Access (MPLS, IP &amp; Layer2)</td>
<td>Metro IP Services (IP and Layer2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Metro Aggregation Services (MPLS, IP and Layer 2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Scaled Metro Ethernet, Metro IP and Metro Aggregation</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Line rate performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Throughput: 44Gbps Full Duplex</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forwarding Capacity: 65Mpps</td>
<td></td>
</tr>
</tbody>
</table>
Innovation
Cisco Carrier Ethernet ASICs

- Most comprehensive CE feature set in an ASIC
- Builds on Cisco’s expertise working with service providers worldwide
- Purposely build for the Carrier Ethernet and MPLS Access and pre-aggregation
**ME3800X/3600X Architecture Overview**

**Cisco Carrier Ethernet ASIC**

1. **Ingress Packet processing**
   - Parsing packets
   - Access Control List
   - QoS Classification
   - QoS Policing
   - Lookup operations
   - L2/L3/MPLS forwarding

2. **Buffering**

   2.1. **Multicast Replication**

3. **Traffic management**
   - Queuing
   - Scheduling

4. **Egress Packet processing**
   - Packets Rewrite

**Unicast Life of a packet**

**Multicast Life of a packet**

**Performance with all Service enabled**
- 24Gbps
- 36 Mpps
- Low latency/Jitter (<20us)
Network Design with Ethernet Virtual Circuit (EVC)
Cisco Ethernet Virtual Circuit (EVC) Framework

Enables Service

- Service Identification
- Service Transport
- Service Policies

Frame classification
VLAN tag manipulation

→ Many Services on same port

Service Instance associates:
- Encapsulation
- VLAN rewrite
- Bridge Domain

EFP (Ethernet Flow Point) or sub-interface
Flexible VLAN tag classification
Flexible VLAN tag rewrite
Flexible Ethertype (.1Q, QinQ)
Cisco Ethernet Virtual Circuit (EVC) Framework

Enables Service

- Service Identification
- Service Transport
- Service Policies

Bridge Domain
Ethernet over MPLS (VPWS)
Virtual Private Lan Services (VPLS)

→ Many Transport Options

Routing
→ L2 to L3 Option

Service Instance associates:
- Encapsulation
- VLAN rewrite
- Bridge Domain

EFP (Ethernet Flow Point) or sub-interface
Flexible VLAN tag classification
Flexible VLAN tag rewrite
Flexible Ethertype (.1Q, QinQ)

EoMPLS PW
EoMPLS PW
EoMPLS PW

Bridging
VPLS
IP/MPLS
MPLS VPN
Virtual Routing
Routing
Cisco Ethernet Virtual Circuit (EVC) Framework

Enables Service

- Service Identification
- Service Transport
- Service Policies

Security
- ACL on EVC

QoS
- Service Policies on EFP

OAM
- OAM Maintenance Point on EFP
- Fault Monitoring (802.1ag)
- Performance Monitoring (Y.1731 2 Way Delay)
- E-LMI

Service Instance associates:
- Encapsulation
- VLAN rewrite
- Bridge Domain

EFP (Ethernet Flow Point) or sub-interface

Flexible VLAN tag classification

Flexible VLAN tag rewrite

Flexible Ethertype (.1Q, QinQ)

Bridge Domain

SI

Bridging

VPLS

EoMPLS PW

VPWS

EoMPLS PW

Flexible VLAN tag classification

Flexible VLAN tag rewrite

Flexible Ethertype (.1Q, QinQ)
### EVC Implementation on ME3800X/3600X

#### Encapsulation
- Untagged
- Single tagged
- Double tagged
- Default
- Priority tag CoS
- Ethertype

#### Rewrite
- Pop 1
- Pop 2
- None
- Push
- Translate

#### Bridge Domains
- Up to 8,000 BD*
- * With QoS, 4000 only

#### Protocol Tunneling
- Per EFP
- cdp, dtp, lacp, pagp, stp, vtp, udld, lldp
- Peer
- Tunnel
- Forward

---

**interface GigabitEthernet0/2**

```
service instance 10 ethernet encapsulation dot1q 11 rewrite ingress tag pop 1 symmetric bridge-domain 12
```

---

**Encapsulation DOT1Q 100 Second-DOT1Q 1000,1001,1002**

**Priority Tagged with CoS list**

**Encapsulation Priority-Tagged COS 0-3**

**Ethertype IPv6**

**Encapsulation DOT1Q 10 ETYPe IPv6**
IPv6 Ethertype

Router Configuration W2-2

```plaintext
interface GigabitEthernet0/4
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
  encapsulation dot1q 10 etype ipv6
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2000
end

interface Vlan2000
  no ip address
  xconnect 200.1.1.12 100 encapsulation mpls
end
```

Traffic Capture

![Traffic Capture Diagram](image)

Topology

![Topology Diagram](image)
QinQ Configuration Example

EFP to Switchport

INGRESS UNI
interface GigabitEthernet0/1
switchport trunk allowed vlan none
switchport mode trunk
service instance 10 ethernet
encapsulation dot1q 10
bridge-domain 100

EGRESS NNI
interface GigabitEthernet0/2
switchport mode trunk

VLAN 10 (C-TAG) VLAN 100 (S-TAG)

Switchport: Implicit push on egress & implicit pop on ingress
QinQ Configuration

interface GigabitEthernet0/1
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
  encapsulation dot1q 10
  bridge-domain 1200

interface GigabitEthernet0/2
  switchport mode trunk

Topology

IXIA Interface Configuration

<table>
<thead>
<tr>
<th>Port Description</th>
<th>Port Link</th>
<th>Interface Description</th>
<th>IPv4 Address (10.0.x.x - Reserved IP)</th>
<th>IPv4 Mask Width</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.27.153.151:01:00-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>2</td>
<td>172.27.153.151:01:01-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>3</td>
<td>172.27.153.151:01:02-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>4</td>
<td>172.27.153.151:01:03-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>5</td>
<td>172.27.153.151:01:04-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>6</td>
<td>172.27.153.151:01:05-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>7</td>
<td>172.27.153.151:01:06-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
<tr>
<td>8</td>
<td>172.27.153.151:01:07-Ether1</td>
<td>Connected - ProtocolInt</td>
<td>7.1.1.1</td>
<td>24</td>
<td>7.1.1.2</td>
</tr>
</tbody>
</table>

Connected Int... Unconnected Int... ORE Tunnels Discovered Int... Interface Addr... DHCPv4 Disc... DHCPv6 Disc...
IPv4 Double Tagged Packet Capture
Selective QinQ
Ingress EFP to Egress Switchport

**INGRESS UNI**
- interface GigabitEthernet0/1
- switchport trunk allowed vlan none
- switchport mode trunk
- service instance 10 ethernet
  - encapsulation dot1q 10-20
  - bridge-domain 100
- service instance 20 ethernet
  - encapsulation dot1q 20-30
  - bridge-domain 200

**EGRESS NNI**
- interface GigabitEthernet0/2
- switchport mode trunk

---

Traffic Direction

**Switchport: Implicit push on egress & implicit pop on ingress**
QinQ Configuration
Ingress EFP to Egress EFP

INGRESS UNI
interface GigabitEthernet0/1
switchport trunk allowed vlan none
switchport mode trunk
service instance 10 ethernet
encapsulation dot1q 1-50
bridge-domain 5000

EGRESS UNI
interface GigabitEthernet0/2
switchport trunk allowed vlan none
switchport mode trunk
service instance 10 ethernet
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
bridge-domain 5000

VLAN 1-50 (C-TAG)
VLAN 100 (S-TAG)
VLAN 1-50 (C-TAG)

ME3800X/ME3600X SWITCH
Traffic Direction
## VLAN Translation

**Summary table**

<table>
<thead>
<tr>
<th>VLAN Translation</th>
<th>Ingress Interface</th>
<th>Egress Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>Rewrite pop 1</td>
<td>Rewrite pop 1</td>
</tr>
<tr>
<td>1:2</td>
<td>Rewrite pop 1</td>
<td>Rewrite pop 2</td>
</tr>
<tr>
<td>2:1</td>
<td>Rewrite pop 2</td>
<td>Rewrite pop 1</td>
</tr>
<tr>
<td>2:2</td>
<td>Rewrite pop 2</td>
<td>Rewrite pop 2</td>
</tr>
</tbody>
</table>
UNI with 1:1 Translation

Ingress EFP to Egress EFP

**INGRESS UNI**

Interface GigabitEthernet0/1
switchport trunk allowed vlan none
switchport mode trunk
service instance 10 ethernet
encapsulation dot1q 10
rewrite ingress tag pop 1 symmetric
bridge-domain 10

**EGRESS UNI**

Interface GigabitEthernet0/2
switchport trunk allowed vlan none
switchport mode trunk
service instance 10 ethernet
encapsulation dot1q 20
rewrite ingress tag pop 1 symmetric
bridge-domain 10

Traffic Direction

- VLAN 10
- INGRESS EFP
- Gig 0/1
- UNTAG
- VLAN 20
- EGRESS EFP
- Gig 0/2
- ME3800X/ME3600X
- Push
- Pop
- Traffic Direction
L2 Protocol Tunneling

Tunnel Option

- To enable L2PT, the command to do this is: “l2protocol tunnel “

  interface GigabitEthernet0/4
  service instance 20 ethernet
  encapsulation untagged, dot1q 200 second-dot1q 300
  l2protocol tunnel cdp stp vtp dtp pagp lacp udld lldp
  bridge-domain 10

- Protocols supported: cdp, dtp, lacp, pagp, stp, vtp udld lldp
- If a protocol is not supported by L2PT, then it is dropped at the interface
L2 Protocol Tunneling

Why L2PT Forward?

• Interop with Cisco devices which do not support L2PT tunnel (e.g. Cisco 7600)
• Interop with Non Cisco devices to tunnel BPDUs

L2PT Forward Configuration

```
interface GigabitEthernet0/1
switchport trunk allowed vlan none
switchport mode trunk
service instance 10 ethernet
encapsulation dot1q 10 second-dot1q 20
rewrite ingress tag pop 2 symmetric
l2protocol forward cdp stp
xconnect 5.5.5.5 1000 encapsulation mpls
mtu 1500
```
# L2PT Summary

<table>
<thead>
<tr>
<th></th>
<th>EFP with BD</th>
<th>EFP with SVI (Xconnect)</th>
<th>EFP with Xconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>Drop all BPDU</td>
<td>Drop all BPDU</td>
<td>Drop all BPDU</td>
</tr>
<tr>
<td><strong>L2PT Forward</strong></td>
<td>Forward All*:</td>
<td>Forward All*:</td>
<td>Forward All*:</td>
</tr>
<tr>
<td></td>
<td><code>l2protocol forward</code></td>
<td><code>l2protocol forward</code></td>
<td><code>l2protocol forward</code></td>
</tr>
<tr>
<td></td>
<td>Selective:</td>
<td>Selective:</td>
<td>Selective:</td>
</tr>
<tr>
<td></td>
<td><code>l2protocol forward cdp stp</code></td>
<td><code>l2protocol forward cdp stp</code></td>
<td><code>l2protocol forward cdp stp</code></td>
</tr>
<tr>
<td><strong>Hop by Hop need to enable on every hop</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>L2PT Tunnel</strong></td>
<td>Forward All*:</td>
<td>Forward All*:</td>
<td>Forward All*:</td>
</tr>
<tr>
<td></td>
<td><code>l2protocol tunnel</code></td>
<td><code>l2protocol tunnel</code></td>
<td><code>l2protocol tunnel</code></td>
</tr>
<tr>
<td></td>
<td>Selective:</td>
<td>Selective:</td>
<td>Selective:</td>
</tr>
<tr>
<td></td>
<td><code>l2protocol tunnel cdp stp</code></td>
<td><code>l2protocol tunnel cdp stp</code></td>
<td><code>l2protocol tunnel cdp stp</code></td>
</tr>
<tr>
<td><em><em>All</em>: Local Switching is supported with tunnel and forward</em>*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*cdp* Cisco Discovery Protocol  
*dtp* Dynamic Trunking Protocol  
*lacp* LACP Protocol  
*lldp* Link Layer Discovery Protocol  
*pagg* PortAggregation Protocol  
*stp* Spanning Tree Protocol  
*udld* UDLD Protocol  
*vtp* Vlan Trunking Protocol
Quality of Service
QoS

General Information

- All QoS configuration on the ME 3800X and 3600X switches is Modular QoS CLI (MQC) compliant
  - QoS is always enabled. No concept of “mls qos”
- Quality of service (QoS) on the ME 3800X and ME 3600X switches includes
  - Traffic classification
  - Marking
  - Policing
  - Queuing, and Scheduling
- Ingress & Egress Policies are applied on packet on the wire
  - Ingress policy is applied on the packets **BEFORE** any rewrite
  - Egress policy is applied on the packets **AFTER** any rewrite
QoS Overview

- **General Information**
  
  - Traffic Classification, Marking and Policing can be configured in ingress service policy *(No Support for Ingress Queuing)*
  
  - Traffic Classification, Marking, Policing on the Priority Queuing, and Scheduling can be configured in egress service policy
Hierarchical QoS
General Information

- ME 3800X and ME 3600X Switches support up to 3-Level H-QoS

- These three QoS levels are designated:
  - Class level: Supports matching CoS, DSCP, IP Precedence, or MPLS EXP. Use the class-map “match {cos [inner] cos-list | dscp dscp-list | ip precedence ip-precedence-list | mpls experimental exp-list}” command.
  - VLAN level: Includes per-VLAN QoS. Use the class-map “match vlan vlan-id” or “match vlan inner vlan-id” command.
  - Physical level: Shaping or policing supported only on the class-default class. Use the shape, police cir, or police cir percent policy-map class configuration command.
Switchport 3-Level H-QOS Policy

Channel, Subchannel, Queues

- In the Policy-B mentioned above, class class-default in Policy-B will correspond to channels in the ASIC,
- Classes inside ‘policy-map vlan’ will correspond to subchannels in the ASIC
- Classes inside ‘policy-map phb’ will correspond to queues in the ASIC.

```
policy-map Policy-B >>>> Port Level (3-Level)
class class-default
  shape average 10M
  service-policy vlan

policy-map vlan >>>> Vlan Level
class vlan1
  shape average 5M
  service-policy phb
class phb2
  shape average 6M
  service-policy phb

policy-map phb >>>> Class Level
class phb1
  shape average 1M
class phb2
  shape average 2M
```
EFP 2-level H-QOS Policy

- In Policy-A, class class-default in Policy-A will correspond to subchannel in the ASIC
- Classes inside ‘policy-map phb’ will correspond to queues in the ASIC
- When scheduler action commands are given for a class
  - A profile will be allocated from the respective profile tables
  - The new profile will be attached to the corresponding ASIC entities, such as queues and subchannel.
- A policy in a EFP will correspond to separate queue-subchannel hierarchy.

3-Level Policy supported since 15.1(2)EY using Port shaper

```
policy-map Policy-A >>> EFP Level without match vlan
class class-default
  shape average 10M
  service-policy phb

policy-map phb >>> Class Level
class phb1
  shape average 1M
class phb2
  shape average 2M
```
Hierarchical QoS

- Hierarchical order: Physical, VLAN, and Class Level
  - Attach a class-level policy map to a VLAN-level policy map
  - Attach the VLAN-level policy map to a physical-level policy map
  - Attach the physical-level policy map to a port (switchport) or EFP

- Levels may be omitted, but the order of the levels (class level, VLAN level, physical level) must be preserved.
High-Level QoS Support

- 3 level hierarchy
- QoS Available on all ports: Switchport, EVC, routed Ports
- Deep buffers:
  - 44MB on ME3600X
  - 352MB on ME3800X
- Large number of queues
- Cisco standard MQC CLI
- QoS for Ethernet, IP and MPLS

- Classification
- Policing
- Marking
- Classification
- Policing
- Marking

Replication

Egress Queue/Schedule Congestion Control

QoS Actions at Ingress

QoS Actions at Egress
Classification Security Model

- **Scenario 1:** If the PHB match on a class-map of an input policy-map is 'dscp af'
  - Traffic can match on the egress ONLY based on 'dscp af'

- **Scenario 2:** If the PHB match on a class-map of an input policy-map is 'cos 2' and it is remarking the “cos 2” to 'cos 3'
  - We can classify the traffic on the Egress ONLY based on 'cos 3'

- **Scenario 3:** If the class-map of an input policy-map is based on any flow criteria like MAC/IP ACL
  - Traffic is NOT eligible for Egress classification
Classification Security Model contd..

- **Scenario 4:** If the traffic does NOT hit any input policy-maps
  - Egress classification can take place on ANY criteria given in the egress policy-map.

- **Scenario 5:** If the traffic hits the default class of the input policy-map
  - Traffic is NOT eligible for Egress classification.
QoS Policy on Etherchannel

- You cannot attach a service policy to an EtherChannel.
- You can only attach service policies to individual ports in the port channel.
- You cannot attach a service policy to an EFP that belongs to a port channel interface.
- When a configured policer rate, policer burst-size, queue-rate, or queue-size cannot be achieved in hardware within 1 percent, the configuration is rejected.
Ingress QoS

interface GigabitEthernet0/3
service instance 1 ethernet
encapsulation dot1q 200
rewrite ingress tag pop 1 symmetric
service-policy input vlan

2nd level
policy-map vlan
class vlan
service-policy phb

3rd level
policy-map phb
class phb
police cir 100000000
conform-action set-mpls-exp-imposition-transmit 5
conform-action set-qos-transmit 5

Marking at any one level
Default Propagation

- Default COS propagation from Inner to Outer COS (Egress PUSH 1 & Egress PUSH 2)
- No COS propagation from Outer COS to Inner COS in case of Disposition
# Default COS Preservation with VLAN Translation

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Translation 1:1</td>
<td>“P” bit Ingress = 4 and Egress = 4</td>
</tr>
<tr>
<td>VLAN Translation 1:2</td>
<td>“P” bit Ingress = 4 and Egress = 4(S-VLAN), 4 (C-VLAN)</td>
</tr>
<tr>
<td>VLAN Translation 1:2 (EFP only)</td>
<td>“P” bit Ingress = 4 and Egress = 4(S-VLAN), 4 (C-VLAN)</td>
</tr>
<tr>
<td>VLAN Translation 2:1</td>
<td>“P” bit Ingress = 4(S-VLAN), 6 (C-VLAN) and Egress = 4</td>
</tr>
<tr>
<td>VLAN Translation 2:2</td>
<td>“P” bit Ingress = 4(S-VLAN), 6 (C-VLAN) and Egress = 4(S-VLAN), 4 (C-VLAN)</td>
</tr>
</tbody>
</table>
MPLS QOS

- The EXP Marking actions ("set mpls exp topmost", "set mpls exp imposition") modifies the EXP of the MPLS packet for only routed/MPLS-routed traffic.
- The exp-value of the topmost outgoing label after these operations is available for egress classification.
- Long pipe, Short pipe, Pipe & Uniform modes are supported
- Default behavior Short-Pipe mode.
- Pipe mode need to be configured explicitly using IOS MQC CLI (QOS Group & Discard Class)
MPLS/VPN QOS

- Ingress & Egress QOS Policies on MPLS/VPN
- Default Behavior: Prec & DSCP values are automatically copied to the EXP bit
- Default behavior can be changed by using "set mpls experimental imposition <imposed-exp-value>" at ingress
- DSCP values are NOT automatically copied to COS bits
EoMPLS QOS

- The default behavior for the EoMPLS is to use a value of “0” in the EXP bits of the VC and tunnel labels.
- Ingress packet classification can be COS or DSCP/Prec
- Default behavior can be changed by using “set mpls experimental imposition <imposed-exp-value>” at ingress
- EXP values are NOT automatically copied to COS bits
## QoS treatment for CPU generated traffic

**Egress**

- CPU generated traffic **automatically** classified as follow:

<table>
<thead>
<tr>
<th>Classified As</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest Priority</td>
<td>EIGRP, HSRP, GRE, LDP, OSPF, RIP, WCCP, BFD, CFM, SAA, CDP, ISIS, DTP, IGRP, Ether OAM, LACP, LLDP, UDLD, PAGP, STP, IKE, IKEv2, ICMP, BOOTP, RARP, IGMP, MSDP, PIM, Telnet, SSH, RSVP, LSP ping, WCCP, GLBP, RGMP, HSRP, VRRP, BFD, BGP, RIP, EIGRP</td>
</tr>
<tr>
<td>Normal Priority</td>
<td>All other protocols.</td>
</tr>
</tbody>
</table>

- No Qos policy required for that classification to take place
## QoS treatment for CPU generated traffic

### Egress

<table>
<thead>
<tr>
<th></th>
<th>High Priority</th>
<th>Normal Priority</th>
<th>Configuration required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classification</strong></td>
<td>Automatic</td>
<td>Automatic</td>
<td>No</td>
</tr>
<tr>
<td><strong>Egress policing</strong></td>
<td>No policer is applied to CPU generated traffic</td>
<td>No policer is applied to CPU generated traffic</td>
<td>No</td>
</tr>
<tr>
<td><strong>Marking</strong></td>
<td>Takes place at the CPU and is specific to each protocol</td>
<td>Takes place at the CPU and is specific to each protocol</td>
<td>No</td>
</tr>
<tr>
<td><strong>Queueing</strong></td>
<td>One Separate queue per interface</td>
<td>One separate queue per interface</td>
<td>No</td>
</tr>
<tr>
<td>Queue limit</td>
<td>Queue limit is 100us</td>
<td>Queue limit is 100us</td>
<td></td>
</tr>
<tr>
<td><strong>Scheduling</strong></td>
<td>absolute priority</td>
<td>Normal Priority</td>
<td>No</td>
</tr>
</tbody>
</table>
### 3 Level Hierarchy QoS Scalability

<table>
<thead>
<tr>
<th></th>
<th>ME3600X</th>
<th>ME3800X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffers</td>
<td>44MB</td>
<td>344MB</td>
</tr>
<tr>
<td>Queues*</td>
<td>4,000</td>
<td>32,000</td>
</tr>
<tr>
<td>Classifications*</td>
<td>4,000</td>
<td>24,000</td>
</tr>
<tr>
<td>Policers*</td>
<td>2,000</td>
<td>16,000</td>
</tr>
</tbody>
</table>

* Per system. Per ASIC is half these values

---

**ME3600X#sh policy-map interface gigabitEthernet 0/1**

**Service-policy input: ingress-stats-policer**

**Class-map: cos-0 (match-all)**

- 0 packets
- Match: cos 0
- police cir 1000000000 bc 1000000
- conform-action transmit
- exceed-action transmit
- conform: 4572455 (packets) 1152258660 (bytes)
- exceed: 0 (packets) 0 (bytes)
- conform: 83823667 bps, exceed: 0 bps

**Class-map: class-default (match-any)**

- 0 packets, 0 bytes
- 5 minute offered rate 0 bps, drop rate 0 bps
- Match: any

---

**Egress QoS Parameter**

<table>
<thead>
<tr>
<th>Egress QoS Parameter</th>
<th>Maximum Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit and Drop Statistics: Packets, Bytes and Rates</td>
<td>Per-queue, per-threshold</td>
</tr>
<tr>
<td>Queues per Subscriber or Service</td>
<td>8</td>
</tr>
<tr>
<td>Shapers</td>
<td>No limitation</td>
</tr>
<tr>
<td>WRED Thresholds per-Queue</td>
<td>3</td>
</tr>
</tbody>
</table>
Network Design With IP/MPLS
Salient MPLS Features

Summary for MPLS capabilities

- MPLS is enabled on all ports
- Role in the MPLS network
  - Label Edge Router
  - Label Switch Router
- Performance
  - TCAM Based Hardware Forwarding
  - Support of “5” MPLS Labels Push & “3” MPLS Labels Pop
    - NO performance degradation upon enabling multiple features at the same time
  - Support to enable Advanced MPLS features at the same time – L3VPN, L2VPN, RFC 3107 & TE/FRR
    - NO performance degradation upon MPLS labels push or pop operation
- Scale
  - Separate TCAM region for IPv4, IPv6, EVC & Multicast
  - Advertised scale numbers are multidimensional
**MPLS Best Practices**

Router ID, LDP Session Initialization, Label Filtering

1. Configure dedicated Router ID

2. Optimize the LDP session initialization

3. Enable Label Filtering
   - Apply the Local Label Allocation Filtering

```
! IOS - prefix list
ip prefix-list List3 permit 192.168.0.0/16 ge 18
!
mpls ldp label
  allocate global prefix-list List3
  exit
!

! IOS - host routes
mpls ldp label
  allocate global host-routes
  exit
```
MPLS Best Practices
Inbound and Outbound Label filtering

4. Apply the Output Label Filtering if LLAF not available

   no mpls ldp advertise-labels
   mpls ldp advertise-labels for 22
   access-list 22 permit 172.16.0.0 0.0.3.255

5. Apply the Inbound Label Filtering (optional)

   access-list 1 permit 172.16.0.0 0.0.3.255
   mpls ldp neighbor 172.16.0.1 labels accept 1
MPLS Best Practices

Default Route, Authentication, Purge, Dampening and Carrier Delay

6. Enable mpls on the default route using the following global command " mpls ip default-route"

7. Configure MD5 Authentication
   – OSPF
   – BGP
   – ISIS
   – LDP

8. Enable "ip routing protocol purge interface" globally

9. Enable "dampening" & "carrier-delay msec 1" on the interface
MPLS Best Practices

Convergence

10. Improve IGP (OSPF/IS-IS) convergence
   - tuning IS-IS/OSPF SPF timers and other mechanisms.
   - Loopbacks used as BGP next-hops need to be prioritized

```
router ospf 1
ispf
log-adjacency-changes
timers throttle lsa all 10 20 5000
timers throttle spf 50 50 5000
timers lsa arrival 10
timers pacing flood 5
```
MPLS Best Practices

Fast Failure Detection and BFD

11. Enable BFD for fast failure detection in case of Loss of Light cannot be detected
   - BFD is supported for the following interfaces
     - Port Mode
     - Switched Virtual Interface (SVI) - Requires global configuration "platform bfd allow-svi"
     - Port-Channel
     - Static
     - Per VRF
   - BFD Numbers
     - 50 msec, 50 sessions supported
     - 150 msec, 150 sessions supported
     - 300 msec, 200 sessions supported
MPLS Best Practices

LDP Sessions

12. Use session protection for LDP and Targeted LDP (when reducing IGP timers.)
   • `Router(config)# mpls ldp session protection`
     - `mpls ldp session protection [vrf vpn-name] [for acl] [duration seconds]`

13. Use LDP/IGP sync and reduce “holddown” timer
   • `router ospf <num> / router isis <tag>
   • `mpls ldp sync`
     - Recommended to reduce the IGP sync holddown timer to a non-infinite time (a few minutes or so) to avoid device isolation
     • `mpls ldp igp sync holddown 600000`
     • `mpls ldp igp sync delay 10`
MPLS Best Practices
BGP Sessions and Protection

14. Enable Path MTU Discovery on all BGP speakers.
   "3800-H-2(config)#ip tcp path-mtu-discovery"

15. Use BGP next-hop tracking (NHT)
    avoid BGP scan-time delay
    when BGP next-hop changes

16. Adjust MinAdvertisementInterval (MAI) on eBGP and iBGP/vpnv4 sessions
    speed up route advertisements.

17. Evaluate Importing Multiple Paths to Protect Against RR Failures - BGP Add Path [Roadmap]

18. “Use” BGP Prefix Independent Convergence (BGP PIC Core & Edge)
    infrastructure – BGP FRR [Roadmap]
MPLS Best Practices

MPLS VPN

19. Use a unique RD per VRF per PE router

20. Define an upper limit at the PE on the number of prefixes received from the CE for each VRF or neighbor.
   1. ‘maximum routes within the VRF configuration in IOS
   2. ‘maximum-prefix’ per neighbor within the BGP VRF af (if BGP on the PE-CE)

21. Configure ‘no bgp default ipv4-unicast’

22. Use dedicated route reflector pairs

23. Use unique Cluster-IDs on RRs (i.e. no need manual configuration)
MPLS Best Practices

HA in helper mode

- Enable HA in helper mode
  - OSPF GR
  - LDP GR
  - BGP GR
  - ISIS GR
Subinterface Simulation on ME3800X/ME3600X

Recommendations

- Subinterface is not supported on ME3800X/ME3600X, Cisco PABU is recommending following to simulate subinterfaces behavior on ME3800X/ME3600X platforms.

- Unique SVIs on each switchport Trunk using “switchport trunk allowed vlan X”

- To tag the native VLAN egress traffic and drop all untagged ingress traffic, enter the global “vlan dot1q tag native” command

- Remove MST
  - no spanning-tree mst configuration
  - no spanning-tree mode mst
  - no spanning-tree vlan 1-4094

- Disable MAC learning
  - no mac address-table learning vlan X
## Virtual Private Wire Service (VPWS)
Currently available

### Supported Features in FCS:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based EoMPLS</td>
<td>A P2P VC service. Looks like leased line service to the customers.</td>
</tr>
<tr>
<td>U-PE in H-VPLS</td>
<td>A MP2MP L2 bridging service. Provides broadcast domain for the customer networks across the provider's core network. But it supports only one PW from U-PE to N-PE. The PW supports MAC learning.</td>
</tr>
<tr>
<td>VPWS tunnel selection</td>
<td>Allows PW to be transported over a given path. Helpful in selecting MPLS-TE tunnels through the provider core network to get better guarantees of SLAs to the customers.</td>
</tr>
<tr>
<td>PW over FRR</td>
<td>Allows PW to be transported over FRR paths for failover protections due to failure in the provider core network.</td>
</tr>
<tr>
<td>MPLS OAM for PW</td>
<td>Debug and monitor end-to-end status of PW.</td>
</tr>
<tr>
<td>PW redundancy</td>
<td>The backup PW path will be programmed by the control plane once the active PW goes down. Allows disparate Ethernet network across the provider's core network to be connected using PW.</td>
</tr>
<tr>
<td>Auto-Sense Signaling</td>
<td>This feature allows to remote PEs to negotiate VC type signaling.</td>
</tr>
</tbody>
</table>
**VPWS**

**Configuration Example**

**Router Configuration W2-2**

```plaintext
interface GigabitEthernet0/4
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  xconnect 200.1.1.12 100 encapsulation mpls
```

**Router Configuration ME3800-H-2**

```plaintext
interface GigabitEthernet0/14
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  xconnect 200.1.1.11 100 encapsulation mpls
```

**Traffic Capture**

```
  Traffic Item   Tx Frames Rx Frames Frames Delta Loss (%)  Inc Frame Rate Rx Frame Rate Rx Rate (Mb/s) Rx Rate (Mb/s)
  1 UPLAQ Traffic 0    0      0     0      0.000   0.000   0.000   0.000
  2 VPWS Traffic 0    0      0     0      0.000   0.000   0.000   0.000
  3 Traffic Item  11,337 11,337 0     0.000  1,000.000 1,000.000 11.200 11.200
```
VPWS
Push the S-TAG

PACKET CAPTURE
Frame 18130: 1418 bytes on wire (11344 bits), 1418 bytes captured (11344 bits)
MultiProtocol Label Switching Header, Label: 25, Exp: 0, S: 0, TTL: 255
MultiProtocol Label Switching Header, Label: 34, Exp: 0, S: 1, TTL: 255
Ethernet II, Src: 00:00:00:00:00:14 (00:00:00:00:00:14), Dst: 00:00:00:00:00:02 (00:00:00:00:00:02)
802.1Q Virtual LAN, PRI: 5, CFI: 0, ID: 1200
802.1Q Virtual LAN, PRI: 4, CFI: 0, ID: 100

switchport trunk allowed vlan none
switchport mode trunk
service instance 1 ethernet
encapsulation dot1q 3200 second-dot1q 100
rewrite ingress tag pop 1 symmetric
bridge-domain 1200

interface Vlan1200
no ip address
platform rewrite imposition tag push 1 symmetric
xconnect 200.1.1.11 100 encapsulation mpls
Routed PW

- Port based Routed PW
- SVI based Routed PW
- Routed VPLS
- Routed PW over FRR
- L2 Multicast over Routed PW/VPLS
- BFD over SVI is supported with Routed PW configuration
- HSRP/VRRP is supported over Routed PW
- IP Multicast over Routed PW is not supported in this release
Multicast VPN

Introduction

- Based on multicast domains in draft-rosen-vpn-mcast-08.txt
  - Provider builds independent multicast network in the core
  - All arriving customer multicast traffic is encapsulated and multicast across Provider Network
  - A separate multicast Group is used inside of Provider Network for each customer VPN
    - Provider’s multicast address space is independent of all customer address spaces
    - Avoids VPN overlap of customers’ multicast addresses
Multicast VPN

Multicast Domain for VPN_A

Multicast Domain for VPN_B

MDT For VPN_A

MDT For VPN_B

One MVRF For VPN_A

One MVRF For VPN_B
MVPN

Limitations and Scale

- Following type of core interfaces are supported
  - Routed Port and
  - Switch-port trunk SVIs with only 1 port
- Only PIM SSM is supported for Data MDT
- No support for fragmentation
- Maximum of 62 OIFs
- No MTU/ACL support MDT OIFs (towards core)
- No Bidir support.
IP Fast Reroute Overview

- IP Fast Reroute is an **IP based mechanism** that reduces traffic disruption to 10s of milliseconds in event of link or node failure.

- LFA
  - Stands for Loop Free **Alternate**
  - A node other than the primary next hop
  - Provides local protection for unicast traffic in pure IP (and MPLS/LDP) networks in event of a single failure, whether link, node, or shared risk link group (SRLG)

Currently on the Roadmap for release 15.2(4)S
# LFA and MPLS TE FRR

## Comparing the two

<table>
<thead>
<tr>
<th>Feature</th>
<th>LFA FRR</th>
<th>MPLS TE FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repair Path</td>
<td>Least cost</td>
<td>Constraints based with BW guarantee and path control</td>
</tr>
<tr>
<td>Shared Risk Link Group (SRLG)</td>
<td>Capable</td>
<td>Capable</td>
</tr>
<tr>
<td>Link Protection</td>
<td>Capable</td>
<td>Capable</td>
</tr>
<tr>
<td>Node Protection</td>
<td>Capable</td>
<td>Capable</td>
</tr>
<tr>
<td>Path Protection</td>
<td>Not Capable</td>
<td>Capable</td>
</tr>
<tr>
<td>Control Plane Requirement</td>
<td>None with Loop Free Alternate</td>
<td>Required (or Capable?)</td>
</tr>
<tr>
<td>Load Distribution Over Multiple Repair Paths</td>
<td>Capable</td>
<td>Not Capable</td>
</tr>
<tr>
<td>Provisioning Complexity</td>
<td>Minimal</td>
<td>Significant</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Effective with mesh and small rings</td>
<td>No dependency. Works on any survivable network.</td>
</tr>
</tbody>
</table>
**IP FRR**

**Benefits**

- Sub 50 msec convergence without using RSVP-TE.
- Simple operation with minimal configuration;
- Superior LFA scaling without tunnel requirement.
- Incremental deployment with no inter-operability req.
  - There is no change to the standard based IGP protocols
  - IP FRR capability is internal to a box.
- Applicable to pure IP (IP FRR) and MPLS (LDP FRR) networks

---

### MPLS Network vs IP Network

<table>
<thead>
<tr>
<th>Configuration</th>
<th>IP/LDP FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple CLI</td>
<td>Simple CLI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Plane</th>
<th>LDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF/ISIS</td>
<td>OSPF/ISIS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MPLS Network</th>
<th>IP Network</th>
</tr>
</thead>
</table>
## IP FRR

### Protection mechanisms

<table>
<thead>
<tr>
<th>Protection</th>
<th>Description</th>
<th>Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Per-Link</strong></td>
<td>• Goal is to bypass failed link and reach primary node via alternative way</td>
<td>• Protection not possible for some topologies</td>
</tr>
<tr>
<td></td>
<td>• Bad for capacity planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cannot guarantee node protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Repair path may be sub-optimal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 SPF per protected link</td>
<td></td>
</tr>
<tr>
<td><strong>Per-Prefix</strong></td>
<td>• Goal is to find alternative path to destination prefixes</td>
<td>• In same topology, may find some prefixes though not for all.</td>
</tr>
<tr>
<td></td>
<td>• 1 SPF per neighbor</td>
<td></td>
</tr>
</tbody>
</table>

Note: SPF calculations for LFAs are performed in background and preempted in case of convergence event.
What kinds of LFA do we have?

- Directly Connected
- Remote LFA (Ring Topology)
  - Need to tunnel the packet to the LFA
  - Need a “smart” tunnel
- Objective:
  - We want to protect against the loss of the primary next-hop by redirecting traffic to the pre-calculated LFA(s)
Remote LFA

Description

- In previous example, we just do not have neighbor that is also an LFA
- Common with ring topology
- Router B will loop back traffic destined to P/p
  - No LFA for node C
- Solution
  - Use remote LFA
  - Accomplished by tunneling traffic to D to deliver to P/p
Unified MPLS
What is Unified MPLS?
Classical MPLS network with few additions

- Common MPLS technology from Core, Aggregation, Pre-agg and Access
- Scaling enhancement via hierarchy
- Order of 50ms convergence with minimal or no configuration regardless of size of network
- Flexible and adaptive routing control
- Comprehensive architecture covering L2, L3 and transport with seamless LSP integration
- Technology that allows mix and match of devices that may traditionally not support full IP/MPLS capabilities
Unified MPLS for Mobile Transport

- End to End Label Switched Path
- RFC 3107 label allocation to introduce hierarchy for scale
- Loop Free Alternates FRR for 50 msec convergence with no configuration required (LFA FRR now with Remote LFA FRR in future) or RSVP-TE for bandwidth management in the access
- BGP Prefix Independent Convergence to make the 3107 hierarchy converge quickly regardless the size of network
- BGP Route filtering for controlling scale according to the service needs
- MPLS-TP option for access networks, integrated at service or transport level
- LDP Downstream On Demand For Access Networks that don’t support RFC-3107
MPLS TP

Why TP?

- Transport networks still based on circuit switching (SONET/SDH, OTN)
- Packet-based growing fast and dominating traffic mix (driven by Video, Mobile, Cloud, application migration to IP)
- Increased changes in traffic patterns (mobility, cloud)
- Transport networks migrating to packet switching for
  - Bandwidth efficiency (statistical multiplexing)
  - Bandwidth flexibility (bandwidth granularity, signaling)
Label Switched Paths

Description

- Static
- Bidirectional
- Co-routed (same forward and reverse paths)
- In-band Generic Associated Channel (G-ACh)
- Ultimate hop popping (no explicit/implicit null)
- No ECMP
- Contained within a tunnel
Enabling an MPLS TP network
No IP routing required in control and forwarding planes

- Node will still source/terminate IP packets (e.g. SNMP, NTP)
- Link numbers required on each MPLS-TP interface
- Two interface configuration models
  - IP-enabled (uses ARP)
  - IP-less (no ARP)
- IP-enabled requires interface configuration for
  - Local IPv4 address
  - Remote IPv4 (next-hop) address
- IP-less requires configuration of
  - Destination MAC address
- Same OAM messages for IP-enabled and IP-less interface configurations
Network Design with OAM
OAM - Continuity Fault Management (CFM)

- Fault Management Protocols
  - Continuity Check Messages (CCM)
  - Linktrace (Ethernet `tracetoute`)
  - Loopback (Ethernet `Ping`)
  - Alarm Indication signal (ETH AIS)
  - Remote Defect Indicator (ETH RDI)

ME3600X/ME3800X supports all of the above

Maintenance Domain (MD)
Maintenance Associations (MA)
Maintenance End Point (MEP)
Maintenance Intermediate Point (MIP)
OAM - Continuity Fault Management (CFM)
BD or xconnect

Continuity Check
Layer 2 Interface
VLAN 20
Layer 2 Interface

interface gig 0/1
service instance 2 ethernet e2
encapsulation dot1q 2
bridge-domain 2
cfm mep domain L5 mpid 511

interface Port-channel2
service instance 2 ethernet e2
encapsulation dot1q 2
bridge-domain 2
cfm mep domain L5 mpid 512

ethernet evc e2
ethernet cfm domain L5 level 5
service ma1 evc e2 vlan 2
continuity-check
continuity-check interval 100ms

CE 1  UPE A  NPE A  NPE B  UPE B  CE 2

interface ten 0/1
switchport mode trunk
Switchport trunk allowed vlan 2

CFM on BD

VLAN 20
MEP 511 MEP 512
OAM - Continuity Fault Management (CFM)  
BD or xconnect

Continuity Check

Interface gig 0/1  
- service instance 2 ethernet e2  
- encapsulation dot1q 2  
- cfm mep domain L5 mpid 511  
- xconnect 3.3.3.3 2 encapsulation mpls

Interface Port-channel  
- service instance 2 ethernet e2  
- encapsulation dot1q 2  
- cfm mep domain L5 mpid 512  
- xconnect 3.3.3.3 2 encapsulation mpls

PW  
- MEP 511  
- MEP 512

Showing EVC xonnect  
SVI xconnect also supported

ethernet evc e2

ethernet cfm domain L5 level 5  
service ma1 evc e2 vlan 2  
continuity-check  
continuity-check interval 100ms
OAM - Continuity Fault Management

More Configuration

- **UP MEP**
- **DOWN MEP**
- **7 MD levels**
- **CCM frequency**
  - 100ms, 1s or 10s

- Ethernet EV CFC Domain L7 level 7
- Service ma1 evc e2 vlan 2 direction down
- Continuity-check
- Continuity-check interval 10s

- Ethernet EVC Domain L5 level 5
- Service ma1 evc e2 vlan 2
- Continuity-check
- Continuity-check interval 100ms

- Interface Port-channel 2
  - Switchport mode trunk
  - Ethernet CFM MEP Domain L7 mpid 712
  - Vlan 2

- Interface Port-channel 1
  - Switchport mode trunk
  - Ethernet CFM MEP Domain L7 mpid 711
  - Vlan 2
**Ethernet Local Management Interface (E-LMI)**

- Between UNI-C to UNI-N
- Communicates
  - EVC status
  - EVC attributes
  - CE autoconfiguration
  - Remote UNI status
- Standard: defined in MEF16

---

**Interworking**

<table>
<thead>
<tr>
<th>Link</th>
<th>CE</th>
<th>UPE</th>
<th>SP Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-LMI to CFM BD</td>
<td></td>
<td></td>
<td>ELMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CFM &amp; BD</td>
</tr>
<tr>
<td>E-LMI to CFM Xconnect</td>
<td></td>
<td></td>
<td>ELMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CFM EVC xconnect *</td>
</tr>
<tr>
<td>E-LMI to PW OAM</td>
<td></td>
<td></td>
<td>ELMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EVC xconnect with MPLS OAM</td>
</tr>
</tbody>
</table>

*CFM SVI xconnect not supported*
Performance Monitoring

1731 PM

- Supported on
  - Down MEP
  - UP MEP

- Supported with
  - EVC xconnect
  - EVC BD
  - EVC xconnect on Port Channel
  - EVC BD on Port Channel

Performance Monitoring

<table>
<thead>
<tr>
<th></th>
<th>Link CE - UPE</th>
<th>SP Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay/Jitter</td>
<td>ETH DM</td>
<td>DMM/DMR</td>
</tr>
<tr>
<td>Loss</td>
<td>ETH SLM</td>
<td>SLM/SLR</td>
</tr>
<tr>
<td>E-LMI to PW OAM</td>
<td>ELMi</td>
<td>EVC xconnect with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MPLS OAM</td>
</tr>
</tbody>
</table>

*CFM SVI xconnect not supported

ME3600X 24/24TS | ME3600X 24CX
Two way          | One Way, Two Way
Performance Monitoring
1731 PM Scale

Profile 1: 10sec CCM and 1sec DMM

<table>
<thead>
<tr>
<th></th>
<th># of local MEP</th>
<th># of remote MEP</th>
<th># of active DMM</th>
<th>CPU Utilization</th>
<th>Max recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE1</td>
<td>1000</td>
<td>1000</td>
<td>500</td>
<td>7/22%</td>
<td>500 sessions</td>
</tr>
<tr>
<td>PE1</td>
<td>1000</td>
<td>1000</td>
<td>500</td>
<td>12/25%</td>
<td>500 sessions</td>
</tr>
</tbody>
</table>

Profile 2: 1sec CCM and 1sec DMM

<table>
<thead>
<tr>
<th></th>
<th># of local MEP</th>
<th># of remote MEP</th>
<th># of active DMM</th>
<th>CPU Utilization</th>
<th>Max recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE1</td>
<td>500</td>
<td>450</td>
<td>300</td>
<td>9/28%</td>
<td>300 sessions</td>
</tr>
<tr>
<td>PE1</td>
<td>500</td>
<td>450</td>
<td>300</td>
<td>32/52%</td>
<td>57 sessions</td>
</tr>
</tbody>
</table>

Profile 3: 1sec CCM and 1sec DMM

<table>
<thead>
<tr>
<th></th>
<th># of local MEP</th>
<th># of remote MEP</th>
<th># of active DMM</th>
<th>CPU Utilization</th>
<th>Max recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE1</td>
<td>300</td>
<td>300</td>
<td>300</td>
<td>15/20%</td>
<td>300 sessions</td>
</tr>
<tr>
<td>PE1</td>
<td>300</td>
<td>300</td>
<td>277</td>
<td>25/45%</td>
<td>250 sessions</td>
</tr>
</tbody>
</table>
Service Activation - Ethernet Loopback

Ethernet Loopback

- Facility Loopback
- Terminal Loopback
- Mac Swap Option
- Port level
  - Intrusive
  - Mac Swap
- VLAN level
  - Non intrusive
  - Mac Swap
- Per Mac Address loopback

<table>
<thead>
<tr>
<th></th>
<th>Facility</th>
<th>Terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Level</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>VLAN level</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Ingress QoS</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Egress QoS</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Access Control List

<table>
<thead>
<tr>
<th>ACL Type</th>
<th>Take Precedence</th>
<th>Applied to</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ACL</td>
<td>Yes</td>
<td>Layer 2 interface</td>
<td>Ingress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EC not supported</td>
<td></td>
</tr>
<tr>
<td>Router ACL</td>
<td>No</td>
<td>L3 interface Physical, SVI, Port channel</td>
<td>Ingress and Egress</td>
</tr>
<tr>
<td>EVC ACL</td>
<td>Yes</td>
<td>EVC interface</td>
<td>Ingress</td>
</tr>
</tbody>
</table>

#### EVC interface
- MAC: Yes (Y)
- IPv4: Yes (Y)
- IPv6: Yes (Y)
- Switchport Interface: Y (Y)
- Routed Interface: Y (Y) Y

#### MAC ACL
- Destination MAC addresses
- Source MAC addresses (any bit wise matching on these fields)
- Ethertype, LSAP, COS fields

#### IP ACL
- IPv4 ACL
  - IP source
  - IP destination, DSCP, Upper layer protocol values, TCP and UDP port numbers, TCP flags
- IPv6 ACL
  - IP Source
  - IP Destination (Full range of prefix length): DSCP
  - TCP and UDP port number

#### Logging
- Y (router ACL only)

#### Fragmentation
- Y

#### Number or extended ACL
- Y
Control Plane Policing (COPP)

Control Plane traffic **Ingress**
>> Default 20 CPU queues
>> Default ingress policers
>> Configurable CIR / CB per queue

Control Plane traffic **egress**
>> 20 CPU queues
>> Default egress policers

Configure CIR/BC per queue
```
platform qos policer cpu queue queue-num cir | cb command
```
# Control Plane Policing (COPP)

## List of 20 CPU Queues

<table>
<thead>
<tr>
<th>Queue used for</th>
<th>Queue used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Software forwarding</td>
<td>11 CFM</td>
</tr>
<tr>
<td>2 Routing Protocols</td>
<td>12 Control</td>
</tr>
<tr>
<td>3 ICMP</td>
<td>13 IP options</td>
</tr>
<tr>
<td>4 Host</td>
<td>14 Multicast</td>
</tr>
<tr>
<td>5 ACL logging</td>
<td>15 Multicast Route</td>
</tr>
<tr>
<td>6 STP</td>
<td>16 Multicast mismatch</td>
</tr>
<tr>
<td>7 L2 Protocols</td>
<td>17 RPF Failed</td>
</tr>
<tr>
<td>8 Multicast Control Plane</td>
<td>18 Routing throttle</td>
</tr>
<tr>
<td>9 Broadcast</td>
<td>19 Multicast Queue</td>
</tr>
<tr>
<td>10 REP</td>
<td>20 MPLS OAM</td>
</tr>
<tr>
<td></td>
<td>21 MPLS MTU</td>
</tr>
</tbody>
</table>

![Diagram of Control Plane Traffic Ingress and Egress](image-url)
Configuring Control Plane Policing (COPP)

Configure Control Plane Policing
>> Ingress only
>> Use QoS ACL (MAC, IP)
>> QoS ACL supports:
   - Prec
   - DSCP
   - Access group

>> Use one Protocol per Class-map
>> Always use the police command
>> Class default:
   - No policer applied
   - Use the default queue policers instead
Configure the control plane policer

Switch#configure terminal
Switch(config)#mac access-list extended copp-stp
Switch(config-ext-macl)#permit any 0180.c200.0000 0000.0000.0000
Switch(config-ext-macl)#exit
Switch(config)#class-map copp-stp
Switch(config-cmap)#match access-group name copp-stp
Switch(config)#policy-map copp
Switch(config-pmap)#class copp-stp
Switch(config-pmap-c)#police cir 5m
Switch(config-pmap-c-policy)#end
Switch(config)#control-plane
Switch(config-cp)#service-policy input copp
Switch(config-cp)#end

>> Use one Protocol per Class-map
>> Always use the police command
>> Class default:
   - No policer applied
   - Use the default queue policers instead
Scale Profiles
# L2VPN Scalability Profile

## Features Tested Scale Numbers

<table>
<thead>
<tr>
<th>Features</th>
<th>Tested Scale Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of EFP</td>
<td>4000</td>
</tr>
<tr>
<td>Number of Pseudowires SVIoMPLS EVC-BD based</td>
<td>512</td>
</tr>
<tr>
<td>Number of Pseudowires SVIoMPLS Switchport-BD based</td>
<td>512</td>
</tr>
<tr>
<td>Number of Pseudowires Port-Mode</td>
<td>10</td>
</tr>
<tr>
<td>Number of Mac-Addresses</td>
<td>128K</td>
</tr>
<tr>
<td>Number of Multicast Channels</td>
<td>2000</td>
</tr>
<tr>
<td>Number of TE tunnels</td>
<td>1K</td>
</tr>
</tbody>
</table>

### Diagram

- **Traffic**
- **ASR9000**
- **MST**
- **REP**
- **ME3600X**
- **ME3800X**
- **EoMPLS Pseudowire (SVI xconnect)**
- **Primary tunnel**
- **Backup tunnel**

© 2012 Cisco and/or its affiliates. All rights reserved.
## L3VPN Scalability Profile

<table>
<thead>
<tr>
<th>L3VPN Profile Scale</th>
<th>Tested Scale Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 routes</td>
<td>2K Static Routes/8K DHCP Entries</td>
</tr>
<tr>
<td>BFD Sessions</td>
<td>28 (50ms * 3)</td>
</tr>
<tr>
<td>STP instances</td>
<td>128</td>
</tr>
<tr>
<td>interfaces per Etherchannel</td>
<td>8</td>
</tr>
<tr>
<td>Ether channel groups</td>
<td>26</td>
</tr>
<tr>
<td>eBGP peers</td>
<td>100</td>
</tr>
<tr>
<td>Pseudowires SVI/OMPLS EVC-BD based</td>
<td>512</td>
</tr>
<tr>
<td>TE tunnels</td>
<td>64</td>
</tr>
<tr>
<td>EVCs per BD</td>
<td>100</td>
</tr>
<tr>
<td>Mac-Addresses</td>
<td>2000</td>
</tr>
<tr>
<td>Multicast Channels</td>
<td>2000</td>
</tr>
</tbody>
</table>

**Tested Scale Number**

<table>
<thead>
<tr>
<th></th>
<th>Tested Scale Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total VPNv4 Routes</td>
<td>18K</td>
</tr>
<tr>
<td>Pseudowires SVI/OMPLS</td>
<td>512</td>
</tr>
<tr>
<td>TE tunnels</td>
<td>1000</td>
</tr>
<tr>
<td>Ether channel groups</td>
<td>64</td>
</tr>
<tr>
<td>eBGP peers</td>
<td>128</td>
</tr>
<tr>
<td>Multicast Channels</td>
<td>2000</td>
</tr>
</tbody>
</table>

Diagram:
- ASR9000
- REP
- ME3600X
- ME3800X
- Traffic
- EoMPLS Pseudowire (SVI xconnect)
- Primary tunnel
- Backup tunnel
## Routing Protocol Adjacencies Scale

<table>
<thead>
<tr>
<th>Feature</th>
<th>Scale Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Peers</td>
<td>100</td>
</tr>
<tr>
<td>ISIS Adjacencies</td>
<td>100</td>
</tr>
<tr>
<td>OSPF Adjacencies</td>
<td>100</td>
</tr>
</tbody>
</table>

![Routing Protocol Adjacencies Diagram](image)
Baseline Convergence Numbers
Resiliency for Layer2 VPN Deployment

- EoMPLS from the access
- VPLS in the Core

<table>
<thead>
<tr>
<th>WITH IGP FAST CONVERGENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Failure</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Failure</td>
</tr>
</tbody>
</table>

Fast Convergence Configuration

Global Configuration

```
ip routing protocol purge interface
mpls ldp session protection

router ospf 1
  lispf
timers throttle lsa all 10 20 5000
timers throttle spf 50 50 5000
timers lsa arrival 10
timers pacing flood 5

int Te0/1
carrier-delay msec 0
```

VPLS is in roadmap for 15.1(2)EY

<table>
<thead>
<tr>
<th>Enabled on the U-PE</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Pseudowire</td>
<td>Node</td>
</tr>
<tr>
<td>Primary and backup tunnels</td>
<td>Link</td>
</tr>
<tr>
<td>PW to TE tunnel association</td>
<td>Link</td>
</tr>
</tbody>
</table>
L2 Rings from CPE to PE with the Resilient Ethernet (REP) Protocol

- Double-ring network design.
- Fast L2 convergence using REP protocol in the access rings
- VPLS on 7600 PEs.

<table>
<thead>
<tr>
<th>Failure</th>
<th>Link Failure TE0/1</th>
<th>Link Failure TE0/2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>5ms</td>
<td>22ms</td>
</tr>
</tbody>
</table>

Enabled on the U-PE and CPE Protection

<table>
<thead>
<tr>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>REP</td>
</tr>
<tr>
<td>Link and Node protection</td>
</tr>
</tbody>
</table>
L3VPN Resiliency with TE/FRR Tunnel

- MPLS L3VPN design using MP-BGP
- MP-BGP between UPE1, UPE2 and PE2
- PE1, PE3 and P act as LSR
- Traffic Flow
  - UPE1 Gi0/1 \( \rightarrow \) PE2 Te2/1 (VRF)
- TE/FRR for link protection

**Fast Convergence Configuration**

**Global Configuration**

- `ip routing protocol purge interface`
- `mpls ldp session protection`
- `router ospf 1`
- `ispf`
- `timers throttle lsa all 10 20 5000`
- `timers throttle spf 50 50 5000`
- `timers lsa arrival 10`
- `timers pacing flood 5`
- `int te0/1`
- `carrier-delay msec 0`
Case Study: Carrier Ethernet Islands Connectivity using BGP with Label Distribution
Carrier Ethernet Services

- Backhauling of Mobile Operator
- Last Mile Ethernet Access for Corporate Layer3 Services
  - MPLS/VPN
  - Corporate Internet
- Layer2 Circuits (P2P only)
- Transport of Residential High Speed Internet (3-Play) services
Carrier Ethernet - Islands
Connectivity Service

Access

Carrier Ethernet Island

Layer 3 Edge

Dotted line means a link to any device within green blocks

DSLAM
VLAN (HSI, VoIP, Video)

ME3400E (Business)

ME3600X (Mobile)

Second Level Aggregation ME3800X

Aggregation ME3800X

Distribution 7609

BRAS
PE (MPLS-VPN)
End-2-End MPLS LSP for L2 transport over MPLS between AS domains

Inter-AS between two independent IGP clouds

AGG1 & AGG2
ME 3800X

Distribution Node
iBGP with labels
(RFC 3107)

Between Dist and Agg

Aggregation to backbone domain
Distribution = Border routers
CSC-PE to CSC-CE protocol eBGP

CSC-CE1 DIST1
CSC-PE1
VPNv4 + label
iBGP IPv4 + label
eBGP IPv4 + label

End-to-End

CSC-PE2
CSC-CE2 DIST2

TARGETED LDP

MPLS Backbone

MPLS backbone
MPLS L3VPN CsC
BGP free CORE

Distribution Node
iBGP with labels
(RFC 3107)

Between Dist and Agg

Aggregation to backbone domain

 CsC Support in (15.1(2)EY)

CSC-CE1 CSC-CE2
AS1 AS2

107
Design Validation

```
AGG1-ME3800X
neighbor <DIST1> remote-as 65100
neighbor <DIST1> update-source Loopback0
neighbor <DIST2> remote-as 65100
neighbor <DIST2> update-source Loopback0

address-family ipv4
network <AGG1-Loopback> mask 255.255.255.255
neighbor <DIST1> activate
neighbor <DIST1> send-community both
neighbor <DIST1> send-label
neighbor <DIST2> activate
neighbor <DIST2> send-community both
neighbor <DIST2> send-label
maximum-paths ibgp 2
```

```
DIST1-7600
interface 1/1
mpls bgp forwarding

router bgp 65100
neighbor <DIST2> remote-as 65100
neighbor <DIST2> update-source Loopback0
neighbor <AGG1> remote-as 65100
neighbor <AGG1> update-source Loopback0
neighbor <PE1> remote-as 100

address-family ipv4
network <DIST1-Loopback> mask 255.255.255.255
neighbor <DIST2> activate
neighbor <DIST2> send-community both
neighbor <DIST2> next-hop-self
neighbor <DIST2> send-label
neighbor <AGG1> activate
neighbor <AGG1> send-community both
neighbor <AGG1> next-hop-self
neighbor <AGG1> send-label
neighbor <PE1> activate
neighbor <PE1> send-community both
neighbor <PE1> send-label
```
Design Validation contd..

**PE1-7600**

- interface GigabitEthernet1/1
- ip address 192.168.11.1 255.255.255.0
- mpls bgp forwarding  !! auto generated
- end

- router bgp 100
- no bgp default ipv4-unicast
- bgp log-neighbor-changes
- neighbor <RR> remote-as 100
- neighbor <RR> update-source Loopback0

- address-family vpnv4
  - neighbor <RR> activate
  - neighbor <RR> send-community both
  - exit-address-family

- address-family ipv4 vrf ISLA-A
  - no synchronization
  - neighbor <DIST1> remote-as 65100
  - neighbor <DIST1> activate
  - neighbor <DIST1> send-community both
  - neighbor <DIST1> as-override
  - neighbor <DIST1> route-map soo in

- neighbor <DIST1> send-label
- exit-address-family

- route-map soo permit 10
- set extcommunity soo 100:1

**RR**

- router bgp 100
- no bgp default ipv4-unicast
- bgp log-neighbor-changes
- neighbor ibgp peer-group
- neighbor ibgp remote-as 100
- neighbor ibgp update-source Loopback0
- neighbor <PE1> peer-group ibgp
- neighbor <PE2> peer-group ibgp
- neighbor <PE4> peer-group ibgp

- address-family vpnv4
  - neighbor ibgp send-community both
  - neighbor ibgp route-reflector-client
  - neighbor <PE1> activate
  - neighbor <PE2> activate
  - neighbor <PE4> activate
  - exit-address-family
Design Validation contd..

**AGG1-ME3800X**
- switchport trunk allowed vlan none
- switchport mode trunk
- **service instance 1 ethernet**
- encapsulation dot1q 11
- bridge-domain 1000
- !
- interface Vlan1000
- no ip address
- **xconnect 5.5.5.5 300 encapsulation mpls**
- **OR**
- interface Vlan1000
- ip vrf forwarding dslam
- ip address 10.1.1.1 255.255.255.0

**AGG2-ME3800X**
- switchport trunk allowed vlan none
- switchport mode trunk
- **service instance 1 ethernet**
- encapsulation dot1q 12
- bridge-domain 1000
- !
- interface Vlan1000
- no ip address
- **xconnect 6.6.6.6 300 encapsulation mpls**
- **OR**
- interface Vlan1000
- ip vrf forwarding dslam
- ip address 20.1.1.1 255.255.255.0
Public Sector MPLS Network Design

- Public Transport - Highways & Railways
  - L3VPN - Data
  - MVPN - Video Surveillance (The feature is in roadmap for 15.2(1)S Q4CY11)
Case Study: Dual-Box Mobile Backhaul
Dual-Box Mobile Backhaul

Requirements
Fast Convergence (<500ms)
QoS (Voice, Marking)

ME3800X/ME3600X As Mid RAN
Dual Box Solution
L3VPN with Unique RD per VRF
Unique RD enables VPN Loadbalancing
BFD over SVI and HSRP
BFD on Backhaul Interfaces
IGP Fast Convergence
H-QOS
IP SLA

Why ME3800X/ME3600X?
Form Factor
H-QoS
MPLS VPN
Low latency
Fast Convergence
Backhaul Failure – Fiber Pull on ME3600-1
Node failure - ME3600-1 reload
Backhaul Failure - shutdown on 7609

### 7609S#sh ip bgp vpnv4 all

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* i90.90.1.0/24</td>
<td>200.200.1.2</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>200.200.1.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>

### Active to Stby [ms] | Stby to Active [ms]

<table>
<thead>
<tr>
<th></th>
<th>NodeB to RNC</th>
<th>RNC to Node B</th>
<th>NodeB to RNC</th>
<th>RNC to NodeB</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeB to RNC</td>
<td>62</td>
<td>67</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>RNC to Node B</td>
<td>74</td>
<td>73</td>
<td>9</td>
<td>15</td>
</tr>
<tr>
<td>NodeB to RNC</td>
<td>20</td>
<td>55</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>RNC to NodeB</td>
<td>64</td>
<td>66</td>
<td>33</td>
<td>17</td>
</tr>
</tbody>
</table>
Case Study 2: Cable Mobile Backhaul
Cable Mobile Backhaul

ME3600X Key Features

- MPLS Backbone
- Dot1q packets from Cell Site to MSO
- End to End PW from ME3600X to ASR9K to carry dot1q packets
- QoS
- Cost Effective
- 1RU Form Factor
- Green
- End to End management

ME3600X

N-PE

Vlan 10,20

Access

Pre-AGG

DS-PE

Vlan 10,20

Distribution

Core

IP/MPLS

MSO

EoMPLS PW

Cos 4 to Exp 4 QoS mapping + Rate Limiting

class-map match-all match-cos4
match cos 4

policy-map mobile-cos
class match-cos4
police cir 50000000
conform-action set-mpls-exp-transmit 4
Designing with ME36/3800X

Summary

ME3600X for the Access
ME3800X for the Aggregation

Diverse Applications
Residential, Business, Mobile, Public sector, Smart grid

Technical Reference
Convergence and Scale Profiles
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.