Cisco ME 3400 Series
Ethernet Access Switches

Technical Overview:
ME 3400-24TS / ME 3400G-12CS / ME 3400G-2CS

Søren Andreasen
System Engineer, Cisco DK
CCIE #3252
Soren@cisco.com
Cisco ME 3400 Series Agenda

1. Cisco Metro Ethernet Access Product Family

2. ME 3400 Series Hardware Feature Overview
   - ME 3400-24TS
   - ME 3400G-12CS
   - ME 3400G-2CS

3. ME 3400 Series Software Feature Overview

4. Metro Specific Software Details:
   - UNI / NNI Port Types
   - Security
   - Flex-Link
   - Per VLAN MAC Learning
   - Cable Diagnostics (TDR)
   - Link State Tracking
   - QoS
   - Ethernet OAM
Cisco Metro Ethernet Access
Product Positioning
DSBU Metro

Our Primary Focus = Metro Ethernet Access (U-PE)

U-PE = User – Provider Edge Device

Metro Ethernet Forum MEF 9 og 14 compliant (Layer 2 og QOS)

Carrier Ethernet Architecture

<table>
<thead>
<tr>
<th>Access</th>
<th>Aggregation</th>
<th>Edge</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>U-PE</td>
<td>PE-AGG</td>
<td>N-PE</td>
<td></td>
</tr>
<tr>
<td>Admission control, Security Policy Enforcement, Classification, Policing and Marking, Queuing and scheduling</td>
<td>Traffic aggregation, Congestion management, L2 wholesale handoff, Service insertion</td>
<td>MPLS, L2TPv3, VPWS, VPLS, L3VPN, Internet Access, Service Gateway, Value Added Services (Security, Voice,…)</td>
<td>Fast Packet Forwarding (IP/MPLS), Sophisticated Traffic Engineering and Congestion management</td>
</tr>
</tbody>
</table>
Cisco Metro Ethernet Access Product Family
(Prior to Introducing the ME 3400 Series)

**Catalyst 2950**
- Basic and L2+ intelligent services
- Target Market:
  - ETTS – residential & SOHO
  - MDU

**Catalyst 3550**
- Enhanced L2/3 services
- Target Market:
  - ETTB – business
  - MTU

**Catalyst 3750 Metro**
- Premium L2/3 services with hierarchical QoS, and MPLS
- Target Market:
  - ETTB – business premium
  - MTU

Metro Access Topology
- Ring
- Hub-and-spoke
New Cisco Metro Access Product Family

ME 3400 series

- Enhanced Layer 2/3 services
  - Target Market
    - ETTH
    - Layer 2 VPN
    - Layer 3 VPN
    - Intelligent Ethernet Demarcation

Catalyst 3750 Metro

- Premium L2/3 services with hierarchical QoS, and MPLS
  - Target Market
    - ETTB – business premium
    - MTU

Metro Access Topology
- Ring
- Hub-and-spoke
Metro Ethernet Access Network
DSBU Metro Product Applications

Customer Premise (U-PE)

Business
- 3750 Metro or ME 3400-24TS
- ME 3400G-2CS
- GE
- ME 3400G-12CS

Residential
- ME 3400-24TS
- ME 3400-24TS
- DSL

Mini-CO / POP

- ME 3400G-12CS
- GE
- 100M or GE
- DSL
- ONT
- PON
- GE
Cisco Metro Ethernet Access Portfolio

Service Offerings

L3 VPN

Service Range
3750M L2/3

L2 VPN

Service Range
ME 3400 L2/3

Residential Services

2004 2005 2006 Calendar Year

3750Metro
IP Services
Metro IP Access
ME 3400 AC/DC
Metro Access
Metro Base
IP Base
Advanced IP

Cisco Metro Ethernet Access Portfolio

Service Offerings

L3 VPN

Service Range
3750M L2/3

L2 VPN

Service Range
ME 3400 L2/3

Residential Services

2004 2005 2006 Calendar Year

3750Metro
IP Services
Metro IP Access
ME 3400 AC/DC
Metro Access
Metro Base
IP Base
Advanced IP
# Cisco Metro Ethernet Access Portfolio

## Business VPN Service Enablers

<table>
<thead>
<tr>
<th>Feature</th>
<th>3750 Metro</th>
<th>ME 3400 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>L2VPN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address Table Size</td>
<td>12k</td>
<td>8k</td>
</tr>
<tr>
<td>Configurable Per VLAN MAC Learning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>802.1Q Trunking (Q-in-Q)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Q-in-Q CoS mapping</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>L2 Protocol Tunneling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN Mapping (1:1, 2:1, 1:2 Translation)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>EoMPLS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>H-VPLS Attachment Circuits</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EoMPLS or 802.1Q</td>
<td></td>
<td>802.1Q</td>
</tr>
<tr>
<td><strong>L3VPN</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-VRF CE</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MPLS VPN</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
# Cisco Metro Ethernet Access Portfolio

## Quality of Service

<table>
<thead>
<tr>
<th>Feature</th>
<th>3750 Metro</th>
<th>ME 3400 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quality of Service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Rate 3 Color Policing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Per port per VLAN Ingress Policing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Number of Ingress Policers per Port</td>
<td>64 non-ES Ports 2,000 ES Ports</td>
<td>48</td>
</tr>
<tr>
<td>Egress Policing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Number of Egress Policiers per Port</td>
<td>8,192</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of Egress Queues</td>
<td>4 non-ES Ports 8,192 ES Ports</td>
<td>4</td>
</tr>
<tr>
<td>Number of Shapers</td>
<td>8,192</td>
<td>1 Port Shaper 4 Queue Shapers</td>
</tr>
<tr>
<td>Hierarchical QoS (HQF)</td>
<td>3 Levels</td>
<td>No</td>
</tr>
<tr>
<td>Strict Priority Queueing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Congestion Avoidance Mechanism</td>
<td>WRED</td>
<td>WTD</td>
</tr>
</tbody>
</table>

Session Number
Presentation_ID
© 2006 Cisco Systems, Inc. All rights reserved.

Cisco Confidential
###Cisco Metro Ethernet Access Portfolio
Subscriber, Switch, and Network Security

<table>
<thead>
<tr>
<th>Feature</th>
<th>3750 Metro</th>
<th>ME 3400 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNI Default no Local Switching</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP Snooping / IP Source Guard</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic ARP Inspection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Private VLAN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Control Plane Security</td>
<td>Future</td>
<td>Yes</td>
</tr>
<tr>
<td>Storm Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Port Security</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UNI Default Port Down</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Access Control Lists (VACL,RACL,PACL)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>802.1x</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Network Availability / Scalability

<table>
<thead>
<tr>
<th>Feature</th>
<th>3750 <strong>Metro</strong></th>
<th>ME 3400 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexlink (Back-up Interface)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UDLD</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>802.1s / 802.1w</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EtherChannel / LACP / PAgP</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CWDM SFPs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DWDM SFPs</td>
<td>Future</td>
<td>Future</td>
</tr>
</tbody>
</table>
# Cisco Metro Ethernet Access Portfolio

## Multicast for Triple Play Services

<table>
<thead>
<tr>
<th>Feature</th>
<th>3750 Metro</th>
<th>ME 3400 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IGMP Filtering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IGMP Throttling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MVR (Multicast VLAN Registration)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MSDP (Multicast Discovery Protocol)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM (SM, DM, SDM)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Cisco ME 3400 Series
Hardware Feature Overview
Cisco ME 3400 series
Ethernet Access Switches

- The first purpose built Ethernet Access Switch optimized for both the ETTH triple play and ETTB VPN services
- Industry leading hardware and software designed to simplify deployment, management, and troubleshooting of Metro networks
- Provides the most complete security solution for Metro Ethernet Access network
ME 3400-24TS Product Overview - Service Provider Hardware Design:

Shipping Since November 2005

<table>
<thead>
<tr>
<th>Hardware Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC and DC Power Supply Options, NEBs and ETSI Certifications</td>
<td>Can be located in either customer premise or service provider environments</td>
</tr>
<tr>
<td>All front cabling</td>
<td>Provides ease of installation and maintenance, including environments were rear access is not permitted</td>
</tr>
<tr>
<td>1RU with Flexible Mounting Options</td>
<td>Includes options for 19”and 23” rack mount as well as wall mount</td>
</tr>
<tr>
<td>9.5 inch depth (same as 2950)</td>
<td>Can be installed in space confined environments including Telco closets and/or wall-mounted enclosures</td>
</tr>
<tr>
<td>Higher temperature range</td>
<td>Operating range from 0 ~ 50c</td>
</tr>
<tr>
<td>24 10/100 + 2 SFP</td>
<td>Supports both 100Mb/s and 1Gb/s SFPs for flexible uplink options from a single platform</td>
</tr>
<tr>
<td>Wide range of SFP support</td>
<td>Includes various reaches, single and multimode fiber, single fiber, and CWDM. SFP patch cable option is also available, providing a cost effective solution for stacking applications</td>
</tr>
</tbody>
</table>
ME 3400-24TS Product Overview-
Hardware Details

AC Power Version, Front View

- 100-240 VAC, 50-60Hz with Power Cable Retaining Clip
- Air Intake
- System Status LED
- Standard Console Port
- Port Status LEDs
- 24 FastEthernet Ports
- 2 Gigabit Ethernet Ports Supports Fiber and Copper SFPs, Including 100FX
- Air Intake
- Optional Chassis Ground Connector

DC Power Version, Front View

- -48 VDC with Separate A and B Inputs

Session Number
Presentation_ID
© 2006 Cisco Systems, Inc. All rights reserved.
Cisco Confidential
Two mounting brackets for 19” racks are part of the default installation kit for the ME 3400. Optional ETSI and 23” rack installation kits are also available.

The ME 3400 can also be wall-mounted using the standard 19” rack mount hardware.

Paint mask and #10 screws provided for optional two-hole chassis ground lug (standard 5/8” hole spacing center to center).

Fan is located on the rear panel of the chassis (air exhaust).
ME 3400G-12CS
Gigabit Access or In-Building Aggregation

Maintains ME 3400-24TS look and feel

ME 3400-24TS (AC Version Shown)

ME 3400G-12CS (AC Version Shown)
ME 3400G-12CS
Product Overview

• 12 Dual Purpose ports + 4 SFP only ports
• Positioned for Gigabit access and in-building aggregation
• Wire-speed switch built with Cisco switching ASIC
• Dual fixed redundant AC or DC Power Supply and Fans
• All-front cabling simplify troubleshooting and installation in the field
• Higher temperature range support: 0 ~ 50C, with temperature sensor device
• Supports both Fast Ethernet and Gigabit Ethernet SFP modules
• Industry standards certification for quality and service support: NEBS 3, MEF 9, MEF 14
• Supports same Metro Software Images / Features as ME 3400-24TS
• Requires 12.2(25)SEG1 or later release **Does not support earlier releases of ME 3400 Series software.**
ME 3400G-12CS Product Overview - Hardware Details

AC Power Version, Front View

- Power Supply Input 1 (PS1)
- Power Supply Input 2 (PS2)
- Air Intake
- Standard Console Port
- System Status LED
- Port Status LEDs are between the SFP and RJ45 jack for each port
- Ports 1-12 Dual-Media Gigabit Ethernet Ports
  - Can use either RJ45 or SFP
- Optional Chassis Ground Connector
- Ports 13-16 Gigabit Ethernet SFP Ports

DC Power Version Not Shown
Note:
Dual fans are provided for redundancy. Like the power supplies, individual fans are not field replaceable.
For each pair of dual purpose ports, either the 10/100/1000 RJ-45 port or the SFP port can be used (but not both simultaneously).

- LEDs indicate which port is active.
- The media type can be configured as:
  - auto-select (default)
  - rj45
  - sfp
- With media type configured for auto-select, the first port in the pair to achieve link is selected.
- If both ports in the pair are connected, the SFP port takes priority. The priority is not configurable.
- Speed and Duplex can not be manually configured without first configuring a media type of rj45 or sfp (Not configurable with auto-select media type).
**ME 3400G-12CS Product Overview - System LEDs**

**LED Definition:**

<table>
<thead>
<tr>
<th>LEDs</th>
<th>LED Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
<td>Off – no power</td>
</tr>
<tr>
<td></td>
<td>Alternating Green/Off – POST in progress</td>
</tr>
<tr>
<td></td>
<td>Solid Green – System Healthy (normal operation)</td>
</tr>
<tr>
<td></td>
<td>Solid Amber – System Faulty</td>
</tr>
<tr>
<td>PS 1 &amp; PS 2</td>
<td>Solid Green – Functional Power Supply or PS Alarm Suppressed</td>
</tr>
<tr>
<td></td>
<td>Solid Amber – Bad/Non-Functional Power Supply or no AC/DC input</td>
</tr>
</tbody>
</table>
ME 3400G-2CS
Product Overview

• 2 Dual Purpose ports + 2 SFP only ports
• Smaller footprint (approximately same as Catalyst 2940)
• Wire-speed switch built with Cisco switching ASIC
• Fixed AC only
• Higher temperature range support: 0 ~ 50c
• Supports both Fast Ethernet and Gigabit Ethernet SFP modules
• Supports same Metro Software Images / Features as ME 3400-24TS and ME 3400G-12CS
• Requires 12.2(35)SE (Fall ’06) or later release. Does not support earlier releases of ME 3400 Series software.
ME 3400G-2CS Product Overview - Hardware Details

Front View

- **Port Status LEDs**: Between the SFP and RJ45 jack for each port.
- **System Status LED**
- **Air Intake**
- **Standard Console Port**
- **Ports 1-2**: Dual-purpose Gigabit Ethernet
- **Ports 3-4**: Gigabit Ethernet SFP Ports

Rear View

- **Single Fan**
- **Power Supply Input (AC Only)**
ME 3400G-2CS
Intelligent Customer Premise Demarcation

- Ability to offer L2 and L3 VPNs in one box
- Redundant uplinks with failover capability using Flexlink
- 802.1ag Ethernet OAM for end-to-end Ethernet “circuit” management
- ELMI for CPE management
- Robust QoS with ingress per VLAN policing and egress shaping
- Support for ring topology
- Etherchannel for multi-GE services
- Platform and feature consistency for multi-tenant buildings (ME3400-24TS or ME3400G-12CS) and single-tenant buildings (ME-3400-2CS)
ME 3400 Series
Hardware - Supported SFPs

<table>
<thead>
<tr>
<th>Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLC-T</td>
<td>1000BASE-T (Copper)</td>
</tr>
<tr>
<td>GLC-SX-MM</td>
<td>1000BASE-SX short wavelength</td>
</tr>
<tr>
<td>GLC-LH-SM</td>
<td>1000BASE-LX/LH long-wavelength/long haul</td>
</tr>
<tr>
<td>GLC-ZX-SM</td>
<td>1000BASE-ZX extended distance</td>
</tr>
<tr>
<td>GLC-BX-D</td>
<td>1000BASE-BX10-D downstream bidirectional single fiber</td>
</tr>
<tr>
<td>GLC-BX-U</td>
<td>1000BASE-BX10-U upstream bidirectional single fiber</td>
</tr>
<tr>
<td>GLC-GE-100FX</td>
<td>100Base-FX (MM Fiber) (Works in “Multi-speed” GE SFP ports of other Cisco platforms like 3560, 3750 (non-Metro), 2970)</td>
</tr>
<tr>
<td>GLC-FE-100FX</td>
<td>100Base-FX (MM Fiber)</td>
</tr>
<tr>
<td>GLC-FE-100LX</td>
<td>100Base-LX (SM Fiber)</td>
</tr>
<tr>
<td>GLC-FE-100BX-D</td>
<td>100BASE-BX-D downstream bidirectional single fiber</td>
</tr>
<tr>
<td>GLC-FE-100BX-U</td>
<td>100BASE-BX-U upstream bidirectional single fiber</td>
</tr>
<tr>
<td>CWDM-SFP-xxxx</td>
<td>CWDM SFP xxxx nm; Gigabit Ethernet (xxxx=1470, 1490, 1510, 1530, 1550, 1570, 1590, 1610)</td>
</tr>
<tr>
<td>DWDM-SFP-xxxx</td>
<td>Available 2HCY06: we will support all 32 wavelengths</td>
</tr>
</tbody>
</table>

DOM (Digital Optical Monitoring) is under consideration for a future release

Cisco External Site for SFP Datasheets
ME 3400 Series
Hardware - Supported SFPs

• Gigabit SFP “patch cables” are supported.
• These patch cables allow a full-duplex gigabit connection between two switches, and are appropriate for customers who require multi-switch port density with a single uplink port.
• Cost effective option for stacking applications
• Cisco “StackWise” technology is not supported on the Cisco 3750ME or ME3400 Series

Part #: CAB-SFP-50CM
# ME 3400 Series- Hardware Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>ME 3400-24TS</th>
<th>ME 3400G-12CS</th>
<th>ME 3400G-2CS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Specifications</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet Ports</td>
<td>24 x 10/100 copper + 2 SFP Only</td>
<td>12 x Dual Purpose + 4 SFP Only</td>
<td>2 x Dual Purpose + 2 SFP Only</td>
</tr>
<tr>
<td>Chassis H x W x D</td>
<td>1.72&quot;H x 17.5&quot;W x 9.5&quot;D (4.45 x 44.5 x 24.18 cm)</td>
<td>1.72&quot; H x 17.5&quot; W x 11&quot;D (4.45 x 44.5 x 27.94 cm)</td>
<td>1.72&quot;H x 10.6&quot; W x 7.1&quot; D (4.45 x 26.9 x 18.2 cm)</td>
</tr>
<tr>
<td>Weight</td>
<td>8.2 lb (3.72 kg)</td>
<td>AC Version = 9.3 lb (4.2 kg)</td>
<td>3.5 lb (1.6 kg)</td>
</tr>
<tr>
<td>Available Rack Mount Accessories</td>
<td>19&quot;, ETSI, 23&quot; Racks</td>
<td>19&quot;, ETSI, 23&quot; Racks</td>
<td>19&quot;, 23&quot; (no ETSI)</td>
</tr>
<tr>
<td>Wall Mount Option</td>
<td>Yes, Using 19&quot; Brackets shipped with Unit</td>
<td>Yes, Using 19&quot; Brackets shipped with Unit</td>
<td>Yes, Using 19&quot; Brackets shipped with Unit</td>
</tr>
<tr>
<td>Cabling</td>
<td>All Front Access</td>
<td>All Front Access</td>
<td>All Front Access except power and ground</td>
</tr>
<tr>
<td><strong>Power Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Power Input</td>
<td>100 to 240 VAC, 1 to 0.5A, 50-60 Hz</td>
<td>100 to 240 VAC, 1.6 to 0.8A, 50-60 Hz</td>
<td>100 to 240 VAC, 0.5-0.25A, 50-60Hz</td>
</tr>
<tr>
<td>DC Power Input</td>
<td>-36 to -72 VDC, 2 to 1A</td>
<td>-36 to -72 VDC, 4.5 to 2A</td>
<td>Not Available</td>
</tr>
<tr>
<td>Dual Power Supplies</td>
<td>Not Available</td>
<td>Yes, Fixed AC or DC</td>
<td>Not Available</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>25W (typical) 30W (maximum) 102 BTUs per hour</td>
<td>55W (typical) 70W (maximum) 327 BTUs per hour</td>
<td>15W (typical) 20W (maximum) 68 BTUs per hour</td>
</tr>
<tr>
<td>Specification</td>
<td>ME 3400-24TS</td>
<td>ME 3400G-12CS</td>
<td>ME 3400G-2CS</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>Environmental</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan and Cooling</td>
<td>1 Fan, Front to Rear</td>
<td>2 Fans, Front to Rear</td>
<td>1 Fan, Front to Rear</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>32 to 113F (0 to 50C)</td>
<td>32 to 113F (0 to 50C)</td>
<td>32 to 113F (0 to 50C)</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-13 to 158F (-25 to 70C)</td>
<td>-13 to 158F (-25 to 70C)</td>
<td>-13 to 158F (-25 to 70C)</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>10 to 85% (noncondensing)</td>
<td>10 to 85% (noncondensing)</td>
<td>10 to 85% (noncondensing)</td>
</tr>
<tr>
<td>Operating Altitude</td>
<td>Up to 10,000 ft (3049 m)</td>
<td>Up to 10,000 ft (3049 m)</td>
<td>Up to 10,000 ft (3049 m)</td>
</tr>
<tr>
<td>Storage Altitude</td>
<td>Up to 15,000 ft (4573 m)</td>
<td>Up to 15,000 ft (4573 m)</td>
<td>Up to 15,000 ft (4573 m)</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Predicted MTBF</td>
<td>AC Version= 391,823 hrs DC Version= 492,603 hrs</td>
<td>AC Version= 247,563 hrs DC Version= 297,688 hrs</td>
<td>AC Version= 486,352 DC Version= N/A</td>
</tr>
</tbody>
</table>
## ME 3400 Series Specifications

### Electromagnetic and Safety Compliance

| Electromagnetic Emissions Compliance (EMC) | FCC Part 15 Class A  
|                                           | EN 55022B Class A (CISPR22 Class A)  
|                                           | EN 55024  
|                                           | EN 300 368  
|                                           | GR-1089 CORE Class A  
|                                           | VCCI Class I  
|                                           | AS/NZS 3548 Class A or AS/NZS CISPR22 Class A  
|                                           | MIC  
|                                           | CE Marking  
|                                           | China (EMC requirements)  
| Safety                                    | UL 60950-1 1st Edition  
|                                           | UL to CAN/CSA 22.2 No. 60950-1-03 (1st Edition)  
|                                           | TUV/GS to EN60950-1 1st Edition  
|                                           | CB to IEC60950-1 1st Edition, with all country deviations  
|                                           | AS/NZS 3260, TS001  
|                                           | CE Marking  
|                                           | NOM to NOM-019-SCFI  
|                                           | CLEI Coding  

# ME 3400 Series Specifications

## NEBS and ETSI Compliance

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NEBS</strong></td>
<td>GR-63-CORE, GR-1089-CORE-Level 3, Type 2</td>
</tr>
<tr>
<td><strong>ETSI</strong></td>
<td>EN 300 019 – Storage: Class 1.2, Transportation: Class 2.3, In-Use: Class 3.2</td>
</tr>
</tbody>
</table>
| **Noise Specifications** | Cisco Office Product Spec: 48dBA (Sound Pressure), 4.8 Bel (Sound Power)  
EN 300 753 |
Cisco ME 3400 Series
Software Feature Overview
ME 3400 Series Product Overview-
Three Service Provider Offerings-One Platform

Service Offerings

L3 VPN

L2 VPN

Residential Services

Three SW images

Metro IP Access

Metro Access

Metro Base

One Hardware Platform:
ME 3400

Metro Ethernet
ME 3400 Series Software Feature Overview - Feature Summary by Image

12.2(25)EX if not Otherwise Noted*

<table>
<thead>
<tr>
<th>Metro Base Image Includes:</th>
<th>Metro Access Image Includes:</th>
<th>Metro IP Access Image Includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metro Base Features Plus:</td>
<td>Metro Access Features Plus:</td>
<td>Metro IP Access Features Plus:</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>802.1s/w</td>
<td>L2PT (L2PT on trunk 12.2(25)SEG)</td>
<td>VRF-Lite</td>
</tr>
<tr>
<td>802.1d</td>
<td>Per-port VLAN policing 12.2(25)SEG</td>
<td>Advanced IP Routing</td>
</tr>
<tr>
<td>802.1q</td>
<td>DAI / IPSG</td>
<td>BGP</td>
</tr>
<tr>
<td>802.1p</td>
<td>802.1q tunneling</td>
<td>OSPF</td>
</tr>
<tr>
<td>802.1x</td>
<td>Flex-Link (MMN and Preemption 12.2(25)SEG)</td>
<td>IS-IS 12.2(25)SEG</td>
</tr>
<tr>
<td>UNI/NNI (4 NNIs Max)</td>
<td>Configurable Per VLAN MAC Learning</td>
<td>RIPv1, RIPv2, Static Routing</td>
</tr>
<tr>
<td>IGMP and MVR</td>
<td>Ethernet OAM-802.1ag 12.2(25)SEG</td>
<td>EIGRP</td>
</tr>
<tr>
<td>Control Plane Security</td>
<td>Ethernet OAM-ELMI 12.2(25)SEG</td>
<td>Multicast (PIM Dense Mode, Sparse Mode, Sparse-Dense Mode, MSDP)</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>Link State Tracking 12.2(25)SEG</td>
<td>NNI on all ports 12.2(25)SEG</td>
</tr>
<tr>
<td>MQC QoS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVLAN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


ME 3400G-12CS will require 12.2(25)SEG1 or later. ME 3400G-2CS will require 12.2(35)SE or later
### ME 3400 Series Software Feature Overview - SDM Template Performances

<table>
<thead>
<tr>
<th>Feature</th>
<th>Metro Base and Metro Access Template</th>
<th>Metro IP Access Template (routing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 unicast MAC addresses</td>
<td>8k</td>
<td>1k</td>
</tr>
<tr>
<td>L2 VLANs (simultaneously active)</td>
<td>1005</td>
<td>1005</td>
</tr>
<tr>
<td>VLAN IDs (Maximum)</td>
<td>4094</td>
<td>4094</td>
</tr>
<tr>
<td>IPv4 IGMP groups</td>
<td>1k</td>
<td>*1k</td>
</tr>
<tr>
<td>IPv4 multicast routes</td>
<td>N/A</td>
<td>*1k</td>
</tr>
<tr>
<td>IPv4 unicast routes</td>
<td>N/A</td>
<td>5K</td>
</tr>
<tr>
<td>Number of VRFs</td>
<td>N/A</td>
<td>26</td>
</tr>
<tr>
<td>Directly-connected IPv4 hosts</td>
<td>N/A</td>
<td>1k</td>
</tr>
<tr>
<td>L3 indirectly connected unicast routes</td>
<td>N/A</td>
<td>4k</td>
</tr>
<tr>
<td>IPv4 Policy Based Routing ACEs</td>
<td>N/A</td>
<td>512</td>
</tr>
<tr>
<td>IPv4 QoS ACEs</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>MAC security ACEs (shared among VACL, PACL and RACL for input and output)</td>
<td>1k</td>
<td>1k</td>
</tr>
</tbody>
</table>

* In the Metro IP Access template, a total of 1K is available for IGMP groups + multicast routes
# ME 3400 Series
## Product List Pricing

<table>
<thead>
<tr>
<th>Product</th>
<th>Product Description</th>
<th>List Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>ME 3400-24TS-A</td>
<td>24 10/100 + 2 SFP, AC Power</td>
<td>$1,995</td>
</tr>
<tr>
<td>ME 3400-24TS-D</td>
<td>24 10/100 + 2 SFP, DC Power</td>
<td>$2,495</td>
</tr>
<tr>
<td>ME 3400G-12CS-A</td>
<td>12 dual-purpose + 4 SFP, Dual AC Power</td>
<td>$6,995</td>
</tr>
<tr>
<td>ME 3400G-12CS-D</td>
<td>12 dual-purpose + 4 SFP, Dual DC Power</td>
<td>$7,995</td>
</tr>
<tr>
<td>ME 3400G-2CS-A</td>
<td>2 dual-purpose + 2 SFP, AC Power</td>
<td>$1,695</td>
</tr>
</tbody>
</table>

**Software**

<table>
<thead>
<tr>
<th>Software Description</th>
<th>List Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metro Base SW Feature Image</td>
<td>$0</td>
</tr>
<tr>
<td>Metro Access SW Feature Image</td>
<td>$1,000</td>
</tr>
<tr>
<td>Metro IP Access SW Feature Image</td>
<td>$2,995</td>
</tr>
</tbody>
</table>

**Software Upgrade**

<table>
<thead>
<tr>
<th>Software Upgrade Description</th>
<th>List Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD kit for METROACCESS Upgrade from METROBASE</td>
<td>$1,000</td>
</tr>
<tr>
<td>CD kit for METROIPACCESS Upgrade from METROBASE</td>
<td>$2,995</td>
</tr>
<tr>
<td>CD kit for METROIPACCESS Upgrade from METROACCESS</td>
<td>$1,995</td>
</tr>
</tbody>
</table>
ME 3400G-12CS and ME 3400G-2CS
Software Differences

- For ease of deployment and operational efficiency, all ME 3400 Series products support the same software images and features.
- There are a few minor CLI exceptions due to differences in the hardware options:

### ME 3400G-12CS and ME 3400G-2CS Differences:

- Both platforms support the configuration of media type for the Dual Purpose ports:
  
  **Example:**
  
  3400G(config)# interface gi0/1
  3400G(config-if)# media-type rj45

  **Available options for media type are:**
  
  - auto-select (either rj45 port or sfp port may become active)
  - rj45 (force use of rj45 port)
  - sfp (force use of SFP port)

- Interface attributes that are media type dependent (speed, duplex, etc.) are NOT configurable when the media type is set to ‘auto-select’. When the media type is set to rj45 or sfp, only configuration options that are appropriate for the specified media type will be available on the command line.

- Uses the ‘system mtu jumbo’ command for L2 MTU settings for all ports and all port speeds. ME 3400-24TS uses the ‘system mtu’ command for 10/100 ports.
ME 3400G-12CS Differences:

- Power supply failure will be indicated with CLI messages, system LED state, MIB state and MIB traps. Not connecting a power supply input is considered a power supply failure. In applications where only a single power supply will be connected, the power supply failure alarms may be suppressed with the command `no power-supply dual`.

- ‘show environment’ commands now display information for dual power supplies, dual fans, and temperature monitor settings.

Example:

3400G#show env all
FAN 1 is OK
FAN 2 is OK
TEMPERATURE is OK
Temperature Value: 31 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 56 Degree Celsius
Red Threshold : 66 Degree Celsius
POWER SUPPLY 1 is OK
POWER SUPPLY 2 is OK - Alarm disabled
The ME 3400 Series provides three different types of MTU settings:

- `system mtu` is used for Ethernet 10/100M Ports
- `system mtu jumbo` is used for Gigabit Ethernet Ports (fixed or SFP)
- `system mtu routing` is used for layer 3 Ports

ME 3400-24TS uses the “`system mtu`” command for 10/100 ports and the “`system mtu jumbo`” command for SFP ports.

Since all ports on the ME 3400G-12CS and ME 3400G-2CS run Gigabit Ethernet speeds, it uses the “`system mtu jumbo`” command for L2 MTU settings for all ports and all port speeds.

For 12.2(25)SEG and later releases, the following apply:

- The maximum value for the jumbo MTU is 9000 bytes
- The maximum value for the system MTU is 1998 bytes
- The maximum value for the routing MTU is 1998 bytes
- The default value for all MTU types is 1500 bytes

Note: Prior to release 12.2(25)SEG, the system MTU range was 1500-1546 and the `system mtu routing` command did not exist.
ME 3400 Series
Keepalives

• Keepalive behavior is consistent across ME3400 platforms (ME3400-24CS, ME3400-12CS)
• Keepalives are OFF for NNI Ports by default
• Keepalives are ON for UNI Ports by default
• Changing an interface from UNI to NNI or from NNI to UNI (using the “port-type” interface-level command) has no effect on the keepalive state
• Customers can use the CLI “[no] keepalives” on the interface to control the keepalive behavior
• Other DSBU platforms will have keepalives OFF by default for any SFP port
Cisco ME 3400 Series
Metro Specific Software Details
ME 3400 Series
UNI / NNI Port Types
Feature Introduction:

- “UNI” and “NNI” are well known terms for describing access and network ports in the service provider environment:
  - UNI ports are customer facing: A UNI port may be connected to a Home Access Gateway or a host providing connectivity for Voice, IPTV and Data services for example
  - NNI ports are for network connectivity: Uplink or Downlink
- All ports have a default port type assigned (either UNI or NNI)
- Port types are configurable through CLI
- All ports have a port type
ME 3400 Series Provisioning Features - UNI/NNI Port Types (ME 3400-24TS-A Shown)

- For ME 3400-24TS, By default, all 24 10/100 ports are UNI port-type
- For ME 3400G-12CS and ME 3400G-2CS, By default all dual purpose ports are UNI port-type
- UNI ports are shut down by default
- UNI ports will not do local switching by default
- For customers using multiple UNI ports on the same ME 3400, up to 8 UNI ports can be configured to do local switching
- UNI ports have Control Plane Security enabled by default - control protocols can only be dropped or tunneled (i.e. VTP, CDP, BPDU, LACP, PAgP, DTP) – this offers protection against DoS attacks
- UNI ports have the option to process 802.1x, UDLD and IGMP packets

- For ME 3400-24TS, By default, the 2 SFP ports are NNI port-type
- For ME 3400G-12CS and ME 3400G-2CS, By default, the SFP-only ports are NNI port-type
- There can be maximum of 4 ports defined as NNI ports (Applicable to ME 3400-24TS and ME 3400G-12CS, all 4 ports can be configured as NNI on ME 3400G-2CS)

NOTE: In 12.2(25)SEG and later releases - Metro IP Access Image, all ports can be optionally configured as NNI (not limited to 4)

- NNI ports are up by default
ME 3400 Series Provisioning Features - Benefits of UNI/NNI Port Types

Enhanced security

– **UNI Ports default down**: Prevents subscribers from gaining unauthorized access to other ports or services while initial configuration of the switch is in progress

– **No Local Switching by Default**: Provides Circuit-like behavior to separate and protect customer traffic

– **Protection from DoS**: Provides protection from denial-of-service (DoS) attacks related to control protocols which should not appear at UNI ingress ports.

Simpler Management

– **Metro Specific default behaviors**

– **Global configuration, easier to identify and manage like ports**

– **Prevents misconfiguration**: ME 3400 software will not allow the configuration of features that are not intended for the configured port type
ME 3400 Series Provisioning Features-
UNI VLAN types

• Configurable **UNI Community** and **UNI Isolated VLAN Types**

• Traffic is not switched between UNI Ports on UNI Isolated VLANs ("protected port")

• Traffic is switched between UNI ports on UNI Community VLANs (Allowed for Trunk UNI ports in 12.2(25)SEG1 and later releases. Allowed for access ports only in 12.2(25)EX and 12.2(25)SEG)

• Limit of eight UNI Ports in a UNI Community

• **Default** VLAN type is Isolated VLAN
ME 3400 Series
Security
To address potential security threats in the Metro Access Network, a comprehensive set of security mechanisms are required.

These can be divided into three (3) main categories:

<table>
<thead>
<tr>
<th>Subscriber Security</th>
<th>Switch Security</th>
<th>Network Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNI Default No Local Switching</td>
<td>Control Plane Security</td>
<td>UNI Default Port Down</td>
</tr>
<tr>
<td>DHCP Snooping</td>
<td>Port Security</td>
<td>Access Control List</td>
</tr>
<tr>
<td>IP Source Guard</td>
<td>Configurable Per VLAN MAC Learning</td>
<td>IEEE 802.1x</td>
</tr>
<tr>
<td>Dynamic ARP Inspection</td>
<td>Storm Control</td>
<td></td>
</tr>
<tr>
<td>Private VLAN</td>
<td>QoS: Rate Limiting / Priority Policing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure Shell</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration File Security</td>
<td></td>
</tr>
</tbody>
</table>
Subscriber Security –
**UNI Default No Local Switching**

Show command: show vlan uni-vlan <type>

Switch#sh vlan uni-vlan type

Vlan  Type
---- ---------------
10    UNI isolated
20    UNI community

Configuration example:

```
(config) vlan 10
(config-vlan) uni-vlan isolated
(config-vlan) vlan 20
(config-vlan) uni-vlan community
```

**What It Does:**
- Traffic is not switched between UNI ports (even if in the same VLAN) unless specifically permitted

**Benefit:**
Provides subscriber isolation, with circuit-like behavior

*Note: Feature may also be known as “Private VLAN Edge” or “Protected Port” on Cisco Switches, may not be implemented as a default behavior on other platforms.*
**Subscriber Security - DHCP Snooping**

**What It Does:**
- Switch forwards only DHCP requests from untrusted access ports, drops all other types of DHCP traffic
- Allows only designated DHCP ports or uplink ports trusted to relay DHCP Messages
- Builds a DHCP binding table containing client IP address, client MAC address, port, VLAN

**Benefit:**
Eliminates rogue devices from behaving as the DHCP server
Subscriber Security - *IP Source Guard*

**What It Does:**
- If a subscriber is assigned an IP address via DHCP, the switch can enforce that assignment by blocking any packets sent from the client's port claiming to be from a different IP addresses.
- This is accomplished **by enabling DHCP snooping and IP source guard.**
- Prevents a subscriber (or malicious user) from using an IP Address not assigned to them.

**Benefit:**
IP address “spoofing” is prevented

Binds client IP address, client MAC address, port, VLAN number

“I’m assigned IP address 10.2.2.15”

“I’m going to steal address 10.2.2.15”

No, you’re not!
Subscriber Security -
*Dynamic Arp Inspection*

**What It Does:**
- Discards ARP packets with invalid IP-to-MAC address bindings
- This uses the DHCP binding table that was dynamically populated by DCHP Snooping

**Benefit:**
Effectively stops “man-in-the-middle” attacks and “ARP Spoofing”
Subscriber Security -
*Private VLAN*

**What It Does:**
- Private VLANs partition a regular VLAN domain into subdomains, consisting of a pair of VLANs: a primary VLAN and a secondary VLAN
- Two types of Secondary VLANs:
  - Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level
  - Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level

**Benefit:**
In addition to addressing service provider VLAN ID scalability and IP address management issues, the Private VLAN feature offers Layer 2 separation across switches
Switch Security - 
**Control Plane Security**

**What It Does:**

- **By default**, control protocols such as STP, VTP, CDP, DTP, PAgP and LACP are dropped at the UNI.
- Under certain other conditions, traffic may be tunneled and/or rate limited

**Benefit:**

- Provides protection from accidental or malicious L2 PDU DoS attacks which could overload the CPU and degrade system performance and throughput

---

(See Table on Next Slide for More Detail)
### Switch Security - Control Plane Security

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Default Configuration</th>
<th>When Feature is Enabled on UNI Port</th>
<th>L2PT Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>RSVD_STP</td>
<td>Dropped</td>
<td>ELMI Rate Limited</td>
<td>N/A</td>
</tr>
<tr>
<td>PVST+</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>LACP</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>PAgP</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>802.1X</td>
<td>Dropped</td>
<td>Rate Limited</td>
<td>N/A</td>
</tr>
<tr>
<td>CDP</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>DTP</td>
<td>Dropped</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>UDLD</td>
<td>Dropped</td>
<td>Rate Limited</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>VTP</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>CISCO_L2</td>
<td>Dropped</td>
<td>N/A</td>
<td>Rate Limited</td>
</tr>
<tr>
<td>KEEPALIVE</td>
<td>Rate Limited</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CFM</td>
<td>NULL</td>
<td>Rate Limited</td>
<td>N/A</td>
</tr>
<tr>
<td>SWITCH_MAC</td>
<td>Dropped</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SWITCH_ROUTER_MAC</td>
<td>Dropped</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SWITCH_IGMP</td>
<td>Rate Limited</td>
<td>Forwarded</td>
<td>N/A</td>
</tr>
<tr>
<td>SWITCH_L2PT</td>
<td>Dropped</td>
<td>Rate Limited</td>
<td>Rate Limited</td>
</tr>
</tbody>
</table>

**CPS=Control Plane Security**
Switch Security -
*Control Plane Security*

Display the default policer assignment for interface fa0/1:

```bash
switch#show platform policer cpu interface fa0/1
```

<table>
<thead>
<tr>
<th>Feature</th>
<th>Policer Index</th>
<th>Physical Policer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/1</td>
<td></td>
<td>26</td>
</tr>
<tr>
<td>STP</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td>LACP</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>8021X</td>
<td>3</td>
<td>26</td>
</tr>
<tr>
<td>RSVD_STP</td>
<td>4</td>
<td>26</td>
</tr>
<tr>
<td>PVST_PLUS</td>
<td>5</td>
<td>26</td>
</tr>
<tr>
<td>CDP</td>
<td>6</td>
<td>26</td>
</tr>
<tr>
<td>DTP</td>
<td>7</td>
<td>26</td>
</tr>
<tr>
<td>UDLD</td>
<td>8</td>
<td>26</td>
</tr>
<tr>
<td>PAGP</td>
<td>9</td>
<td>26</td>
</tr>
<tr>
<td>VTP</td>
<td>10</td>
<td>26</td>
</tr>
<tr>
<td>CISCO_L2</td>
<td>11</td>
<td>26</td>
</tr>
<tr>
<td>KEEPALIVE</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>SWITCH_MAC</td>
<td>13</td>
<td>26</td>
</tr>
<tr>
<td>SWITCH_ROUTER_MAC</td>
<td>14</td>
<td>26</td>
</tr>
<tr>
<td>SWITCH_IGMP</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>SWITCH_L2PT</td>
<td>16</td>
<td>26</td>
</tr>
</tbody>
</table>

"26" is the Default "Drop All Policer"

"0" is the Default "Rate-Limiting Policer" for Interface FA 0/1
Switch Security -

*Port Security*

**What It Does:**
- Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch

**Benefit:**
- Protection against malicious MAC Flooding attacks
- Ensures only approved users can log on to the network (secure MAC entries)
- The service provider can use this feature to limit the number of MAC addresses per subscriber UNI (can be included as part of the SLA)
Switch Security -
Port Security

Security Violation Mode Actions:

<table>
<thead>
<tr>
<th>Violation Mode</th>
<th>Traffic is forwarded(^1)</th>
<th>Sends SNMP trap</th>
<th>Sends syslog message</th>
<th>Displays error message(^2)</th>
<th>Violation counter increments</th>
<th>Shuts down port</th>
</tr>
</thead>
<tbody>
<tr>
<td>protect</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>restrict</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>shutdown</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Notes:

1. Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
2. The switch returns an error message if you manually configure an address that would cause a security violation.
3. Can Optionally set Per VLAN Limits.

Only 3 MAC Addresses Allowed on the Port: Take Action
Switch Security -
**Configurable Per VLAN MAC Learning**

**What It Does:**
- Provides a configurable mechanism to control how MAC addresses are learned on a per VLAN basis

**Benefit:**
- VLANs with only two ports (for example an EVPL service) can have MAC learning disabled, avoiding unnecessary depletion of the CAM table space
- Protection against malicious MAC flooding attacks on that VLAN

**To Disable MAC learning for VLAN 10:**
```plaintext
switch(config)# no mac address-table learning vlan 10
```
Switch Security - 
*Storm Control*

**What It Does:**
- Limits the volume of broadcast, multicast and/or unicast traffic
- Ports can be disabled or can send traps if configuration limits are exceeded
- Also sometimes known as Broadcast suppression

**Benefit:**
- Protects the network from intentional and unintentional flood attacks i.e. STP loops
- Limits the combined rate of broadcast and multicast traffic to normal peak loads
Switch Security - *Rate Limiting*

**What It Does:**
- Rate limiters can limit traffic per VLAN, port or user to mitigate the impact of packet-blasting worms and limit the amount of traffic a user can send onto the network.
- Can rate limit using either traffic policing or shaping functions.

**Benefit:**
- Prevents a malicious user from flooding the network with traffic, affecting other users and the management of the network itself.

What It Does:
- Rate limiters can limit traffic per VLAN, port or user to mitigate the impact of packet-blasting worms and limit the amount of traffic a user can send onto the network.
- Can rate limit using either traffic policing or shaping functions.

Benefit:
- Prevents a malicious user from flooding the network with traffic, affecting other users and the management of the network itself.
Switch Security -
**Priority Policing**

**What It Does:**
- A strict priority queue can consume all available bandwidth and starve all other queues
- Priority Policing limits the amount of traffic that can be scheduled by the priority queue

**Benefit:**
- Prevents a malicious user from flooding the network traffic marked as priority, starving other classes
- Allows the Service Provider to "trust" the customer QoS markings (DSCP, IPP, CoS) without being concerned with complete starvation of lower class queues

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 200000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth 500000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth 200000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```
Switch Security -
Secure Shell (SSH)

What It Does:
• SSH is a protocol that can provide a secure connections to a remote device for management
• Data is sent through an encrypted tunnel (DES or 3DES) to secure transmission and integrity of data.
• Authenticates users and ensures secure file transfer and copying
• To use this feature, you must install the cryptographic (encrypted) software image on your switch

Benefit:
• Both sides of tunnel are authenticated so that man-in-the-middle attacks are prevented and critical management information is not compromised
• Provides improved security as compared to Telnet sessions by providing strong encryption when a device is authenticated
• Protects passwords and configuration information
Switch Security -
*Configuration File Security*

**What It Does:**
- The default configuration for the switch allows an end user to recover from a lost password by interrupting the boot process during power-on and by entering a new password.

- However, a system administrator can disable some of the functionality of password recovery by allowing an end user to *reset a password only by agreeing to return to the default configuration*.

- In this case, the switch *will erase the configuration file* if forced into the password recovery process.

**Benefit:**
- Prevents malicious users from *accessing critical information contained in the configuration file* by using the password recovery process.
Network Security -
**UNI Default Port Down**

**What It Does:**
- Unlike ports on traditional Enterprise LAN switching products, the UNI ports are Shut Down by default.
  - NNI ports are enabled (no shut) by default to allow for remote connectivity by the Network Admin.

**Benefit:**
- Prevents unauthorized access to network services while a switch is being installed and initially configured.
- **Default behavior for UNI / NNI port types**

```plaintext
switch(config)#int fa0/1
switch(config-if)#no shut
switch(config-if)#exit
```
Network Security -
Access Control Lists (ACLs)

What It Does:
• ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or VLANs

• An ACL is a sequential collection of permit and deny conditions (ACEs) that apply to packets.

• IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP)

• Ethernet (MAC) ACLs are used to filter non-IP traffic.

• Port, VLAN and Router ACLs are supported

Benefit:
• Restrict network use by certain users or devices

• Administrators can selectively apply extended ACLs based on the time of day and week for added flexibility and/or automation
Network Security -
Access Control Lists (ACLs)

Three Types of ACLs:

• **Port ACLs** - Control traffic entering a Layer 2 interface (inbound)

• **Router ACLs** - Control routed traffic between VLANs, applied to Layer 3 interfaces (inbound or outbound).

• **VLAN ACLs** or VLAN maps - Control all packets (forwarded and routed).
  - VLAN maps can be used to filter traffic between devices in the same VLAN
  - Control based on Layer 3 addresses for IPv4
  - Unsupported protocols are controlled through MAC addresses using Ethernet ACEs.

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
  10 deny 171.69.198.102
  20 permit any
```
Network Security -
*IEEE 802.1x*

**What It Does:**

- Client-server-based access control and authentication protocol
- The Metro Access switch **controls the physical access to the network** based on the authentication status of the customer client device
- The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client
- The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server

**Benefit:**

- Prevents unauthorized users from connecting to the network through a UNI port unless they are properly authenticated
- The RADIUS server database maintains "**username-to-VLAN mappings**", assigning the VLAN based on the username of the client connected to the Metro access switch port. You can use this feature to assign network access (VLAN) for client devices.
802.1x message exchange required for Port Authorization:

- **EAPOL-Start**
- **EAP-Request/Identity**
- **EAP-Response/Identity** → **RADIUS Access-Request**
- **EAP-Request/OTP** → **RADIUS Access-Challenge**
- **EAP-Response/OTP** → **RADIUS Access-Request**
- **EAP-Success** ← **RADIUS Access-Accept**
- **EAPOL-Logoff**

**Port Authorized**

**Port Unauthorized**
ME 3400 Series

Flex-Link
ME 3400 Series Link Redundancy - Flex-Link Overview

- Flex-Link operates as a pair of Layer 2 interfaces, where one interface is configured to act as a backup to the other active interface.
- The feature provides a redundant data path as an alternative solution to the Spanning Tree Protocol (STP), allowing users to turn off STP and still provide link redundancy.
- Interoperate with UDLD to provide heart beat exchange in networks with repeaters.
Flex-Link Operation with Repeaters:

The presence of a repeater can cause the flex-Link feature to fail to operate correctly.

To prevent this, use UDLD in aggressive mode together with Flex-Link.

With the UDLD enabled on both of the “end switches”, a heartbeat message is transmitted at regular intervals between connected switches running the protocol.

The primary link will be shut down if any of the following conditions occur:

- One of the interfaces cannot send or receive traffic
- One of the interfaces is down and the other is up
- A fiber (transmit or receive) connection is lost

Under these conditions, aggressive UDLD will allow Flex-Link to correctly activate the backup link

Note 1:
A SONET/SDH or DWDM Transport network could be providing the “repeater” function in this example.
• This is an enhancement to Flex-Link added to ME 3400 in 12.2(25)SEG

• Significantly improves downtime for the downstream traffic too, upon Flex-Link switchover.

• Lightweight protocol: Send a MMN packet to [(Vlan1, Mac1, Mac2..) (Vlan2, Mac1, Mac2..) ..] distribution network.

• Receiver parses the MMN packet and learns or moves the contained mac-addresses. Alternatively, it can flush the mac-address table for the vlans.

• Receiver forwards packet to other switches.
ME 3400 Series Link Redundancy – Flex-Link Preemption Overview

- This is an enhancement to Flex-Link added to ME 3400 in 12.2(25)SEG

- **With the previous implementation:** When old FWD link comes up it goes into standby state → **NO PREEMPTION OCCURS**

- The Preemption enhancements to Flex-Link provide:
  
  Flexibility in choosing FWD link
  Optimization of available bandwidth utilization

**User can configure Flex-Link pair such that when previous FWD link comes back up:**

- Current FWD link continues
  - Preemption mode **Off**

- Previous FWD link preempts the current and begins FWD instead
  - Preemption mode **Forced (with configurable timer)**

- Higher bandwidth interface preempts the other and goes FWD
  - Preemption mode **Bandwidth**

  **By default, flex-Link preemption mode is OFF**
ME 3400 Series Link Redundancy - Flex-Link Features and Benefits

• Ease of use – Avoids the complexity that can be associated with configuring and running the STP protocol

• Fast link fail over – SONET caliber resiliency at a fraction of the cost. Flex-Link failover is handled entirely within interrupt context while STP is handled at process level

• Scalability – fast convergence time regardless of the number of VLANs and MAC addresses

Feature supported in the ME 3400 Metro Access and Metro IP Access images ONLY (NOT supported in the Metro Base image)
ME 3400 Series
Per VLAN MAC Learning
As a Service Provider’s L2VPN network grows, the MAC address forwarding table in the user-facing provider edge (UPE) switch can easily reach maximum capacity.

When new MAC addresses cannot be learned because the forwarding table capacity limit is exceeded, packet flooding will occur.

On the ME 3400, a configurable mechanism is used to allow the service provider to dynamically control how MAC addresses are learned on a per VLAN basis.

Feature supported in ME 3400 Metro Access and Metro IP Access Images ONLY (Not supported in the ME 3400 Metro Base Image)
ME 3400 Series Scalability Features - Port Security + Configurable Per VLAN MAC Learning

Optional: For each EVPL service, disable MAC Learning on the U-PE pass-thru nodes:
no mac address-table learning vlan vlan-id

Optional: For each EVPL service, on N-PE limit the number of MAC addresses based on the Service Definition:
mac address-table limit vlan vlan-id

For each EVPL service, use Port Security on U-PE to limit the number of Secure MAC addresses based on the Service Definition:
switchport port-security maximum value
ME 3400 Series
Cable Diagnostics
The ME 3400-24TS will test both the transmit and receive pairs on FastEthernet 10/100 ports by transmitting on both pairs.

TDR is also supported on the RJ-45 10/100/1000 ports for ME 3400G-12CS and ME 3400G-2CS.

The TDR function is not supported on SFP ports for any of the ME 3400 Series platforms.

```
3400# test cable-diagnostics tdr int fa0/24
3400# show cable-diagnostics tdr int fa0/24
```

Note that accuracy is +/- 15 meters for ME 3400-24TS or +/- 5 meters for ME 3400G-12CS / ME 3400G-2CS when testing cable length to another Ethernet interface connected at the “far-end” of the cable, and +/- 1 meter for all ME 3400 Series platforms when testing to an open or short at the far-end.
The TDR feature in the ME 3400 can detect crossover cables in the signal path, but with reduced cable length accuracy. A crossover cable may be in the path either intentionally or unintentionally. An Ethernet transceiver must be connected at the “far-end” to detect a crossover cable in the signal path.

```
3400# test cable-diagnostics tdr int fa0/24
3400# show cable-diagnostics tdr int fa0/24

<table>
<thead>
<tr>
<th>Interface</th>
<th>Speed</th>
<th>Local pair</th>
<th>Pair length</th>
<th>Remote pair</th>
<th>Pair status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/24</td>
<td>100M</td>
<td><strong>Pair A</strong></td>
<td>81 +/- 15 meters</td>
<td><strong>Pair B</strong></td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Pair B</strong></td>
<td>81 +/- 15 meters</td>
<td><strong>Pair A</strong></td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pair C</td>
<td>N/A</td>
<td>Pair D</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pair D</td>
<td>N/A</td>
<td>Pair C</td>
<td>N/A</td>
</tr>
</tbody>
</table>
```
ME 3400 Series
Link-State Tracking
ME 3400 Series Link-State Tracking
Feature Overview

- This is an enhancement added to ME 3400 in 12.2(25)SEG and later releases
- Tracks the link status of the upstream interfaces.
- Binds the link status of the upstream interfaces with that of the downstream interfaces.
- If all the upstream interfaces in a link-state group go down, the downstream interfaces in the group will be linked down (error-disabled).
- If any upstream interface in the group comes up, all the downstream interfaces in the group will be linked up (clear error-disable).
ME 3400 Series

Link state tracking
ME 3400 Link-State Tracking
Application-Redundant Uplinks from Customer CPE

N-PE “A”
N-PE “B”

Service Provider POP
Customer Site

Link-State Group 1

Gi0/1
Fa0/1

Active link
Standby link
Failed link

U-PE “A”
U-PE “B”

Switch upstream ports
Switch downstream ports
Enable Link state tracking:

UPE-A(config)#
UPE-A(config)#link state track 1

UPE-A(config)#inter gi0/1
UPE-A(config-if)#link state group 1 upstream

UPE-A(config)#inter fa0/1
UPE-A(config-if)#link state group 1 downstream

Display:

UPE-A#show link state group detail
Link State Group: 1     Status: Enabled, Up
Upstream Interfaces : Gi0/1(Up)
Downstream Interfaces : Fa0/1(Up)
(Up):Interface up      (Dwn):Interface Down    (Dis):Interface disabled
ME 3400 Series Quality of Service Features - Introduction

- QoS is configured via the Modular QoS CLI (MQC)
- MQC allows us to standardize all metro platforms on a consistent QoS infrastructure
- Basic steps for MQC QoS configuration:

  1. Define a class-map.
     A class-map is used to identify a specific type of traffic.
     This is referred to as “classification”.

  2. Define a policy-map.
     This step creates a QoS “policy” by specifying the type or “class”
     of traffic on which to perform specific QoS functions, and the
     specific functions to perform on the traffic.

  3. Associate a class-map with a policy-map
     One or more class-maps can be associated with a policy-map.

  4. Apply the policy-map to a port.
     Apply the policy map to the appropriate interfaces.
ME 3400 Series Quality of Service Features-Capabilities

- **Input Policies**
  - Single rate, two-color policers (1R2C) per class or aggregate
  - Classify by VLAN, CoS, DSCP, IP precedence, L2 ACL, and IP ACL
  - Mark by CoS, DSCP, IP precedence, and QoS group

- **Output Policies**
  - Classify by CoS, DSCP, IP precedence, and QoS group
  - Weighted tail drop congestion management
  - Class-based and interface-based traffic shaping
  - Class-based, weighted fair queuing (CB-WFQ)
  - Priority queuing (a.k.a. LLQ)
  - Priority policing
Cisco ME 3400 Series Quality of Service Features—Packet Flow Diagram

QoS Actions at Ingress:

Classification

Inspect incoming packets for VLAN ID, CoS, DSCP, IP Prec, & ACL.

Policing

Ensure conformance to a specified rate.

Marking

Act on Policer decision.

WTD for congestion control. (3 thresholds per queue.)

Reclass or drop out-of-profile packets.

QoS Actions at Egress:

Egress Queue/Schedule Congestion Control

WTD for congestion control. (3 thresholds per queue.)

Egress scheduling with shaping, CB-WFQ & LLQ.
ME 3400 Series
Per-Port, Per-VLAN, Ingress QoS

• Function and Purpose

In the 1st ME 3400 Series software release (12.2(25)EX), QoS policies could be applied only to all traffic received on a Port

12.2(25) SEG adds the capability for independent QoS policies to be applied to all traffic received on each VLAN of each multiplexed Port (Port AND VLAN target)

Policy has significance only for the Port and VLAN explicitly specified

Allows provisioning of independent SLAs per-EVC (VLAN on a multiplexed port), likely for EVPL or E-LAN L2VPN services, by using separate classification, metering, policing and marking functions

Note: Feature available only in the metro access and metro ip access images
ME 3400 Series
Per Port Per VLAN Ingress Policing Example

class-map match-any dscp1-data
match ip dscp 1

class-map match-any dscp23-video
match ip dscp 23

class-map match-any dscp63-voice
match ip dscp 63

class-map match-any customer1-vlan
match vlan 100
match vlan 200
match vlan 300

policy-map ingress-policy-1
class dscp63-voice
police cir 10000000 bc 50000
conform-action set-cos-transmit 5
exceed-action drop

class dscp1-data
police cir 20000000 bc 50000
conform-action set-cos-transmit 5
exceed-action set-cos-transmit 0

class dscp23-video
police cir 30000000 bc 50000
conform-action set-cos-transmit 5
exceed-action set-cos-transmit 4

policy-map customer1-ingress
class customer1-vlan

service policy ingress-policy-1
interface fa0/1
switchport mode trunk
service-policy input customer1-ingress
ME 3400 Series
Input Policing

- Single rate, per-class policing or aggregate policing between classes
- Rate granularity is ~8192 bps across the configurable range from 8kbps to 1Gbps
- Burst granularity is 64 bytes across the entire range from 8000 bytes to 1M bytes
- Software will round both the rate and the burst to the nearest granularity step
ME 3400 Series
Weighted Tail Drop

• WTD is a congestion management mechanism where a single queue can have multiple logical drop thresholds
• Packets are classified into both an egress queue and a logical drop threshold
• WTD is better than tail drop since traffic classes can be differentiated within a single queue
• Supports two drop thresholds per queue plus a default drop threshold
ME 3400 Series
Interface Shaping Granularity

• Hardware interface shaping granularity is 1 – 16/N times the line rate where N=16..64K
  Example GigE shape rates: 58.8M, 111.1M, 157.9M, 200.0M, 238.1M, 272.7M, 304.3M, 333.3M, … 999.6M, 999.7M, 999.8M

• In other words, the low end granularity is very coarse but the high end granularity is very fine

• If a shape rate is specified that has more than about 1% error from what the hardware can achieve, then an error message is displayed

• Error message indicates two closest achievable rates to what was specified
ME 3400 Series
Class Shaping Granularity

• Hardware class shaping granularity is 1/N times the line rate where N=1..64K

  GigE shape rates: 64K, 64.001K, 64.002K ... 142.9M, 166.7M, 200M, 250M, 333.3M, 500M, 1000M

• In other words, the low end granularity is very fine but the high end granularity is very coarse

  Note that this granularity is opposite that of the interface shaping granularity

• If a shape rate is specified that has more than about 1% error from what the hardware can achieve, then an error message is displayed

• Error message indicates two closest achievable rates to what was specified
**ME 3400 Series**

**Priority Policing**

- A priority queue can consume all available bandwidth and thus starve all other queues.

- To prevent this, MQC supports two features:
  - **Priority policing** with the `police <rate>` command OR
  - **Conditional policing** with the `priority <rate> <burst>` command

- Unfortunately, the hardware does not support output policing in any way.

- However, if we consider that a shaper with a small queue acts like a policer, then we can mimic priority policing by using a shaper with a small queue.
ME 3400 Series
Priority Policing (cont.)

• Some important caveats to note:

#1) Priority policing granularity is the same as the class shaping granularity, NOT the input policing granularity (fine at the low end, course at the high end)

#2) A small amount of latency is added when the policer hits its limit since the minimum queue size is 16 buffers (up to 328 µsec at 100Mbps)

#3) The difference between the policed rate and the physical rate is available CIR bandwidth so other classes must use the bandwidth command, not the bandwidth remaining command that is normally used in the presence of a priority class
## ME 3400 Series QoS Feature Cheat Sheet

<table>
<thead>
<tr>
<th>Feature</th>
<th>Scale</th>
<th>Range</th>
<th>Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Policing</td>
<td>47 policers per interface</td>
<td>Rate: 8 Kbps – 1 Gbps</td>
<td>Rate: ~8192 Kbps</td>
</tr>
<tr>
<td></td>
<td>240 policers per system</td>
<td>Burst: 8 Kbytes – 1 Mbytes</td>
<td>Burst: 64 bytes</td>
</tr>
<tr>
<td>WTD</td>
<td>3 thresholds per class</td>
<td>16 – 272 buffers (buffer is 256 bytes)</td>
<td>16 buffers (buffer is 256 bytes)</td>
</tr>
<tr>
<td>Interface Shaping</td>
<td>per parent policy</td>
<td>FE: 5.88 Mbps – 100 Mbps</td>
<td>(1 - 16/N) * line rate</td>
</tr>
<tr>
<td></td>
<td>1 parent per output policy</td>
<td>GE: 58.8 Mbps – 1 Gbps</td>
<td>Low rates: Very coarse</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>High rates: Very fine</td>
</tr>
<tr>
<td>Class Shaping</td>
<td>per class</td>
<td>64 Kbps – 1 Gbps</td>
<td>1/N * line rate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Low rates: Very fine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>High rates: Very coarse</td>
</tr>
<tr>
<td>Priority Policing</td>
<td>per priority class</td>
<td>64 Kbps – 1 Gbps</td>
<td>1/N * line rate</td>
</tr>
<tr>
<td></td>
<td>1 priority class per output policy</td>
<td></td>
<td>Low rates: Very fine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>High rates: Very coarse</td>
</tr>
</tbody>
</table>
ME 3400 Series
Ethernet OAM
(IEEE 802.1ag + E-LMI)
• **Continuity Check (Auto and On-demand)**
  Multicast from MEP. Received by MEPs and MIPs. Catalogued by receiving MEPs.

• **Traceroute**
  Next-hop Multicast from MEP to next MEP or MIP along route. Receiver both replies with unicast to original MEP, and sends Traceroute to next MEP/MIP.

• **Loopback (Ping)**
  Unicast from MEP to MIP or MEP, which replies with unicast to originating MEP.
Ethernet OAM – Ethernet Local Management Interface (E-LMI)

1. Auto-configure C-VLAN/EVC Mapping
2. Improve performance by traffic shaping based on bw profiles
3. Reroute if EVC failure

- Requires tight integration and interoperability between devices
- Leverage Frame Relay LMI and provide similar behavior

1. C-VLAN/EVC Mapping
2. Bandwidth profiles: Per Port, Per EVC, Per CoS
3. EVC status
ELMI (Phase 1)

Frame Relay LMI parity
- UNI Status
- EVC Status
- UNI ID
- CE-VLAN ID/EVC information
- EVC mapping to Vlan(s) on port
- Number of UNI’s in EVC (MPtoMP)
- Error messages when CE-VLAN does not match received EVC-VLAN map
- Display of EVC detail, LMI counters,…

Capability to stop CE traffic upon learning an EVC is down (notification to CE of the deletion, addition, and state of EVC)

CFM-ELMI interworking on the U-PE

*FUTURE* (auto-config of UNI id, EVC id, bandwidth profile, MIB)