6AOSCG0012-29C
January 2013

ADTRAN

Configuration Guide

Configuring EFM NIM2s and the MEF Ethernet Interface in AOS

This configuration guide describes the configuration steps for the NetVanta Ethernet in the First Mile (EFM) network interface modules (NIM2s) and the Metro Ethernet Forum (MEF) Ethernet interface in ADTRAN Operating System (AOS) products. This configuration guide includes an overview of EFM and MEF technology, the components of the EFM system in an AOS product, and the configuration, application, and troubleshooting steps for using EFM NIM2s and the MEF Ethernet interface.

This guide contains the following sections:

EFM NIM2 and MEF Technology Overview

EFM NIM2s are used by ADTRAN products to provide EFM capabilities across wide area network (WAN) interfaces. EFM NIM2 modules enable host devices to participate in existing Metro Ethernet networks (MENs) that are deployed using EFM technology. The EFM technology allows multiple single-pair high-speed digital subscriber line (SHDSL) or T1/E1 loops to be bonded together for higher aggregate bandwidth. In essence, the use of EFM NIM2 modules and the MEF Ethernet interface allows the support of carrier Ethernet technologies on what are typically considered enterprise platforms by providing methods for Ethernet traffic to natively ride on other physical transports, such as T1/E1 and SHDSL. In addition, EFM NIM2 modules support the bonding of multiple physical links into EFM bonding groups, Layer 2 traffic policing with multiple queues (using Ethernet virtual connections (EVCs), EVC maps, and MEF policer policies), and operations, administration, and maintenance (OAM) pre-provisioning. EFM NIM2 modules and virtual MEF Ethernet interfaces can also be used in bad splice detection, T-scan operations, and Point-to-Point Protocol over Ethernet (PPPoE) applications.

The ADTRAN products employing EFM NIM2 modules form a demarcation point between the customer local area network (LAN) and the MEN. The MEN is accessed through one or more EVCs, which are associated with an EFM bonding group that functions as a MEN port. *Figure 1 on page 3* illustrates the MEN configuration components and terminology.

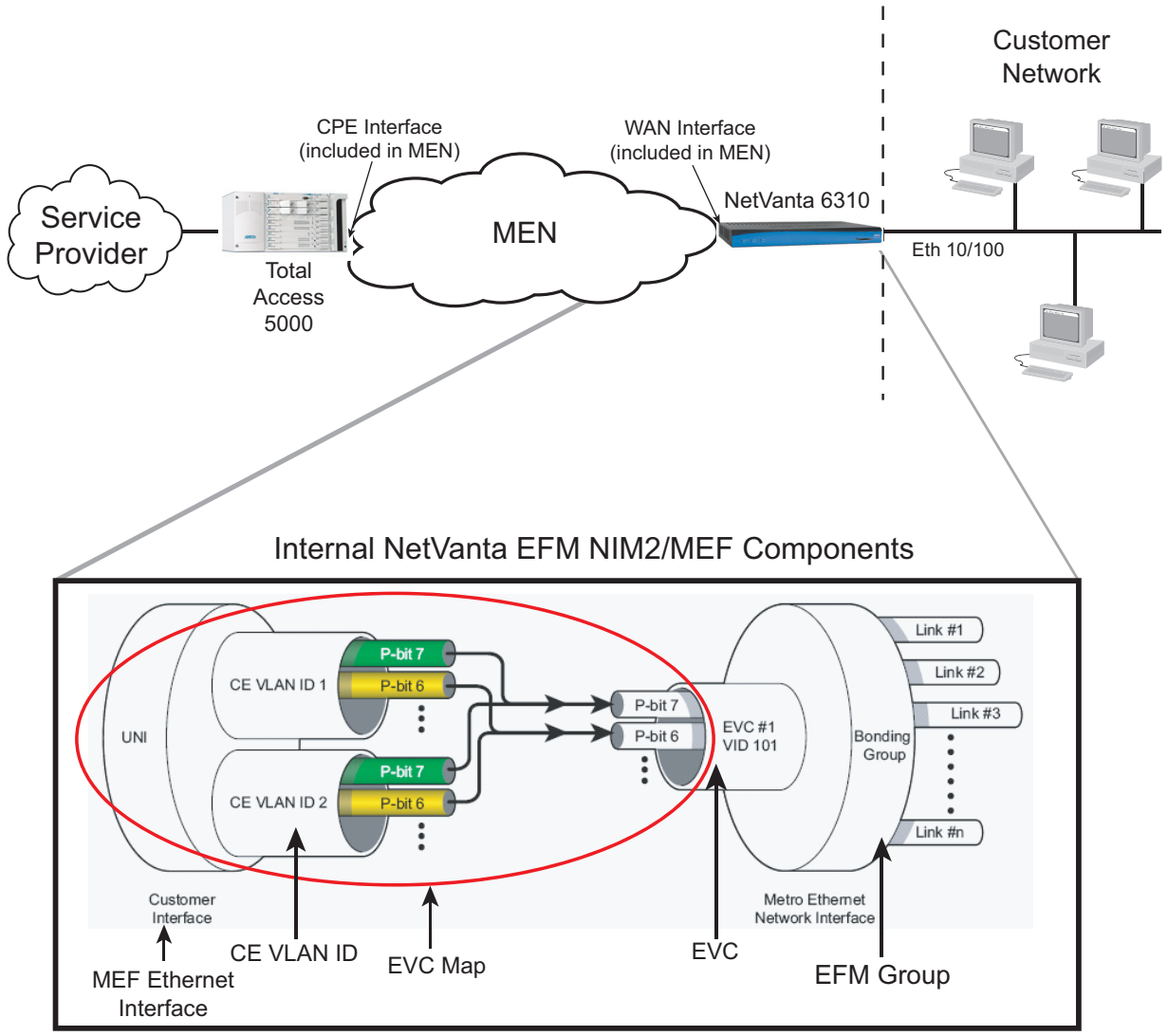

Figure 1. ADTRAN Products in the MEN Topology

EFM NIM2 and MEF Ethernet Interface Components

This configuration guide focuses on the configuration of MEN components in customer-side ADTRAN products. These components include the EVC, the EVC map, the EFM bonding group, the MEF policer profile, and the MEF Ethernet interface quality of service (QoS) settings. The traffic flow between these components is described in the following illustration.

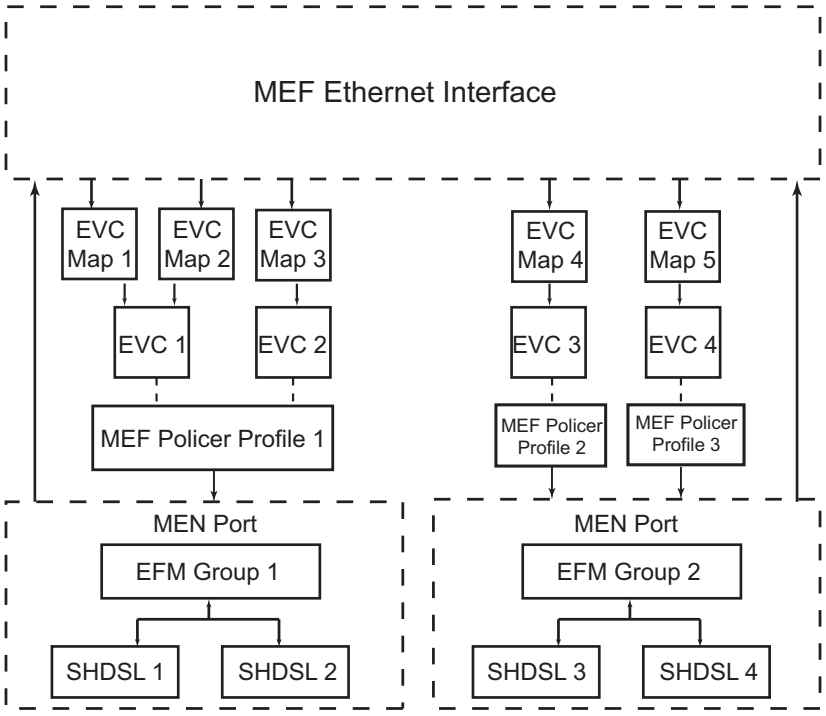

Figure 2. EFM NIM2 Internal Traffic Flow in ADTRAN Products

The EVC

The EVC connects two endpoints (for example, the Total Access 5000 and the customer premise equipment (CPE) device) and passes Ethernet service frames through these endpoints. The EVCs prevent data transfer between subscriber sites that are not part of the same EVC, thus providing data privacy and security similar to a Frame Relay or an asynchronous transfer mode (ATM) permanent virtual circuit (PVC). EVCs are configured to be part of a bonding group (EFM group).

Each EVC has an associated subscriber tag (s-tag), which is the service provider VLAN ID and the outer tag in Q-in-Q VLAN tagging, whose VLAN ID is unique among other EVCs in the MEN. This unique s-tag allows the EVC to be identified and separated from other EVCs within the MEN. The s-tag exists only within the MEN and is not transmitted from or received at the customer LAN. In addition, the customer-side VLAN ID can be preserved on EVC traffic across the MEN if necessary. The customer equipment (CE) VLAN ID is the VLAN ID of the MEF Ethernet subinterface on the AOS unit. This inner tag in Q-in-Q VLAN tagging can be preserved or stripped by the EFM module on both inbound and outbound frames.

The configurable attributes of the EVC include the EVC name, the MEN port to which the EVC is connected, whether the CE VLAN ID is preserved in the EVC traffic, and whether the EVC is enabled. Once these parameters are configured for the EVC, the EVC must be associated with a UNI port for traffic to flow.

The EVC Map

The EVC map is a traffic filter that matches traffic based on specific criteria and associates the traffic with a specific EVC. Each map is associated with a single EVC and UNI, and it includes the customer VLAN ID and class of service (CoS) behavior of the traffic. Maps are used to classify traffic for a specific EVC for forwarding to a UNI, and for use by the MEF Policer Profile for rate limiting.

The configurable attributes of the EVC map include the map name, the UNI associated with the map, the EVC associated with the map, the matching criteria used to match traffic (includes the customer VLAN ID, customer priority bit, differentiated services code point (DSCP) bits, or untagged traffic), and the priority bits and egress queues the EVC uses for matched traffic.

The MEF Policer Profile

The MEF Policer Profile is a bandwidth-limiting profile that limits the amount of outbound traffic from the AOS unit to the MEN. The amount of traffic can be limited on EVCs, UNIs, or EVC maps based on traffic committed burst size (CBS), committed information rate (CIR), excess burst size (EBS), and excess information rate (EIR). These thresholds are used to determine when the EVC bandwidth usage is too great, and the traffic is either queued or dropped based on the configured thresholds.

The configurable attributes of the MEF Policer Profile include the profile name, the CBS, CIR, EBS, and EIR thresholds, whether the profile is enabled, and the components to which the policer profile is applied (EVCs, UNIs, EVC maps, etc.).

MEF Ethernet Interface

The MEF Ethernet interface is a virtual Ethernet interface used as the UNI in an AOS product with an EFM NIM2, providing a connection between the NIM2 and the AOS product. In addition, the MEF Ethernet interface is used as the Layer 2 and 3 WAN interface and is configured with normal WAN interface, primary media gateway, and QoS configurations.

There are a couple of items to note in the MEF Ethernet interface configuration. If you are using 802.1q encapsulation, you must have a native VLAN MEF Ethernet subinterface configured for the EFM NIM2 to communicate with the AOS unit. In addition, to use low latency queuing (LLQ), you must apply a MEF QoS map to the interface. The MEF Ethernet interface is dynamically aware of the available bandwidth, so there is no need to use traffic shaping, unless you are performing PPPoE over the MEF Ethernet interface (refer to *Using the EFM NIM2 for PPPoE Applications on page 23*).

The EFM Group

The EFM group is a logical interface that represents the EFM bonding group as the MEN port. Each NIM2 has four SHDSL interfaces, or four T1/E1 interfaces, which allow two EFM groups for each pair of interfaces or a single EFM group for up to all four interfaces. The EFM groups allow EVCs to be associated logically as a MEN port and to use the same interfaces for connection with the MEN.

The configurable attributes of the EFM group include the group identifier, the physical interfaces used by the group, the excessive code violation threshold for the interface's link in the EFM group, and whether the EFM group is enabled.

MEF Ethernet QoS

MEF Ethernet QoS can be configured to specify that MEF traffic is sent to a specified hardware queue, or to specify a MEN priority is associated with untagged traffic from the customer side of the network. By default, CoS maps are used to specify hardware queues for MEF traffic. CoS values (0 to 7) are associated with up to 8 hardware queues (1 to 8), and traffic is sent to a specific queue based on the CoS value and queue association formed in the MEF QoS configuration. The MEN priority for MEF Ethernet traffic is specified by assigning a priority bit (0 to 7) to MEF Ethernet traffic in the MEF QoS configuration. The global MEF Ethernet QoS settings can also be used by the EVC map as traffic mapping directions.

Hardware and Software Requirements and Limitations

EFM NIM2s are supported on ADTRAN products as outlined in the *AOS Product Feature Matrix*, available online at https://supportforums.adtran.com.

The EFM NIM2s require the NetVanta 6310 or 6330 Series products to be running AOS firmware release A3.01 or later. If the NetVanta unit is being used in conjunction with a Total Access 5000 platform, the Total Access 5000 must be running SR 4.1.1 or SR 5.x. You can find the latest available code online at www.adtran.com.

When using the EFM NIM2, the firmware on both the NIM2 and AOS unit should match what was provided in the firmware bundle. If you must upgrade your firmware, upgrade it on the NIM2 first, and then the AOS product. If you require assistance to upgrade your firmware, refer to the ADTRAN Knowledge Base article, *Upgrading AOS Firmware*, available online at https://supportforums.adtran.com. In addition, technical support can provide both the AOS unit and NIM2 firmware, as well as instructions on performing firmware upgrades.

The bad splice detection and T-scan features are only available on SHDSL EFM NIM2s running AOS firmware release A4.05.00 or later.

PPPoE over the MEF Ethernet interface is only available on EFM NIM2s running AOS firmware release R10.6.00 or later.

EVCs must be associated with a MEN port (EFM group) for traffic to flow. EVC maps must be associated with both a UNI port and an EVC for traffic to be properly mapped.

EFM NIM2s and the MEF Ethernet interfaces are configured using the command line interface (CLI).

If you are using 802.1q encapsulation, you must have a native VLAN MEF Ethernet subinterface configured for the EFM NIM2 to communicate with the AOS unit.

Bridging, bonding across multiple modules, and medium access control (MAC) switched EVCs are not supported on EFM NIM2 or MEF Ethernet interfaces.

You must be running AOS firmware release A5.02 or later on the NetVanta unit to support operation with Total Access 3000 EFM modules. For Total Access 3000 EFM modules to work properly with the NetVanta EFM NIM2s, ***no loopback detection*** *must be configured on the EFM group on the NetVanta device.*

EFM NIM2 and MEF Ethernet Configuration Overview

To configure the EFM NIM2 and the MEF Ethernet interface on the AOS product, you will need to complete the following tasks:

1. Access the AOS unit using the CLI.
2. Configure the EFM group.
3. Configure whether to use any received OAM EVC pre-provisioning (optional). This option is available if your NetVanta product receives its configuration information from a Total Access 5000.
4. Configure the MEF Ethernet interface.
5. Configure the EVC.
6. Configure the EVC map.
7. Configure the MEF Policer Profile (optional).
8. Configure MEF QoS (optional).

Accessing the AOS Unit Using the CLI

To begin configuring the EFM NIM2 or the MEF Ethernet interface, you will need to access the CLI following these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>). For example, **telnet 10.10.10.1**.

*If during the unit's setup process you have changed the default IP address (**10.10.10.1**), use the configured IP address.*

3. Enter your user name and password at the prompt.

*The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enter Enable mode on your unit by entering **enable** at the prompt as follows:

   >enable

5. Enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

   #configure terminal
   (config)#

You can now begin configuring the EFM NIM2 and the MEF Ethernet features.

Configuring the EFM Group

The first step in configuring the EFM NIM2 and the MEF Ethernet features on an AOS product is to configure the EFM group. The EFM group is a logical interface that represents the EFM bonding group. The interfaces that are connected to the EFM group provide physical links that act as the MEN port and carry bonded traffic.

Creating the EFM Group and Associating Interfaces

EFM groups are created using the **interface efm-group** <*group id*> command from the Global Configuration mode. The <*group id*> parameter is the unique numerical identifier for the EFM group. Valid ID range is **1** to **1024**. For example, to create EFM group **1**, enter the command as follows:

(config)**#interface efm-group 1**
(config-efm-group 1)#

Once the EFM group is created, you enter the EFM Group Configuration mode. In this mode, interfaces are associated with the group using the **connect** <*interface*> command. Specify an interface in the format <*interface type [slot/port]*>. For example, for a SHDSL interface, use **shdsl 1/1**. Available interfaces for the EFM group include SHDSL interfaces, T1 interfaces, and E1 interfaces. The following example connects the SHDSL interface **shdsl 1/1** to EFM group **1**:

(config)**#interface efm-group 1**
(config-efm-group 1)**#connect shdsl 1/1**

Use the **connect** command to associate each interface that you need to the appropriate EFM group. Each EFM NIM2 supports up to two EFM groups, and each EFM group supports one to four interfaces (four interfaces total per NIM2).

You cannot mix interfaces from different NIM modules in the EFM groups. For example, interfaces from a NIM in slot 1 cannot be mixed with interfaces from a NIM in slot 2.

Specifying EFM Group XCV Thresholds and Interface Link Removal (Optional)

Once you have created the appropriate number of EFM groups and associated the appropriate interfaces with the group, you can optionally specify the excessive code violation threshold for the interface's link in the EFM group, and that the link is removed if the threshold is exceeded. This is a two-step configuration that occurs in the EFM Group Configuration. First, you must specify the excessive code violation threshold for the group, and second you must specify that links exceeding this threshold are removed.

To specify the excessive code violation threshold for the links in the EFM group, use the **thresholds xcv [1e-5 | 1e-6 | 1e-7]** command from the EFM Group Configuration mode. The **1e-5**, **1e-6**, and **1e-7** parameters specify the threshold bit error rate. Using the **no** form of this command returns the value to the default. By default, the threshold is set to **1e-7**. To specify an excessive code violation threshold for the EFM group, enter the command from the EFM Group Configuration mode as follows:

```
(config-efm-group 1)#thresholds xcv 1e-6
```

For thresholds to be enforced, you must enable link removal in the EFM group configuration using the **xcv-link-removal** command. This command specifies that an interface's link to the EFM group is removed if the excessive code violation threshold is exceeded. Using the **no** form of this command disables the link removal. By default, link removal is enabled. To enable interface link removal for excessive code violations, enter the command as follows:

```
(config-efm-group 1)#xcv-link-removal
```

Enabling the EFM Group

As with any other interface, the EFM group must be enabled. To enable the EFM group, enter the **no shutdown** command from the group's configuration mode as follows:

```
(config-efm-group 1)#no shutdown
```

Once you have created the EFM group, associated interfaces with the group, optionally specified excessive code violation thresholds for the group, and enabled the group, you have successfully configured the EFM group. This also means you have created the MEN port necessary for MEF Ethernet features to function. The next step in the EFM NIM2/MEF Ethernet configuration is to either configure OAM EVC pre-provisioning (optional if your NetVanta product receives its configuration information from a Total Access 5000) or begin configuring MEF Ethernet interface.

Configuring OAM EVC Pre-Provisioning (Optional)

In some network configurations, OAM EVC IP information can be pre-provisioned in a Total Access 5000 and pushed to the NetVanta product as soon as an active link is added to the EFM group. This configuration can include an IP address and subnet mask, the default gateway, and the host name. If your network employs a Total Access 5000, and you are only using a single EVC for all traffic, the entirety of the EFM NIM2/MEF Ethernet interface configuration can be done on the Total Access rather than on the NetVanta product.

If you are not using EVC pre-provisioning, you should disable subtended host mode on the MEF Ethernet interface. In some Total Access 5000 system releases, if subtended host provisioning is not configured, invalid provisioning can be sent. To disable subtended host mode, enter the **subtended-host mode disabled** command from the MEF Ethernet Interface Configuration mode prompt. For example, enter the command as follows:

```
(config)#interface mef-ethernet 1/1
(config-mef-ethernet 1/1)#subtended-host mode disabled
```

For more information about configuring the Total Access 5000 for EFM NIM2s in a NetVanta product, refer to the configuration example, *Single EVC Configuration Using a NetVanta 6310 and Total Access 5000 with Pre-Provisioning on page 16*.

Configuring the MEF Ethernet Interface

After configuring the EFM group, the next step in EFM NIM2 configuration is to configure the MEF Ethernet interface. The MEF Ethernet interface is configured in the same manner as other Ethernet interfaces. The MEF Ethernet interface is a virtual interface, and it provides the connection between the EFM NIM2 and the NetVanta unit. The configurable parameters of the MEF Ethernet interface include access policies, aliases, IP addresses and subnet masks, QoS policies, and more.

To enter the MEF Ethernet Interface Configuration mode, enter the **interface mef-ethernet [**<*slot/port*> | <*slot/port.subinterface*>**]** command from the Global Configuration mode prompt. For example, to enter the configuration of MEF Ethernet interface in slot **1** port **1**, enter the command as follows:

```
(config)#interface mef-ethernet 1/1
(config-mef-ethernet 1/1)#
```

From the MEF Ethernet Configuration mode prompt, enter **?** to view the various features configurable on the interface.

*If you are using 802.1q encapsulation, you **MUST** have a native VLAN mef-ethernet subinterface configured for the EFM NIM2 to communicate with the NetVanta unit.*

If you want to use LLQ on the MEF Ethernet interface, you must apply a QoS map to the interface. You do not, however, need to configure the traffic shape rate because the interface is aware of the available bandwidth.

Configuring the EVC

After configuring the EFM group and MEF Ethernet interface, the next step in EFM NIM2 configuration is to configure the EVC. Configuring the EVC includes naming the EVC, associating the EVC with a specific MEN port (the EFM group in the NetVanta unit), specifying whether the CE VLAN ID is preserved in outbound traffic from the NetVanta unit, specifying the s-tag and enabling the EVC. To configure the EVC, follow these steps:

1. To create the EVC, enter the name for the EVC, and enter the EVC's configuration mode using the **mef evc** <*name*> command from the Global Configuration mode. Use the **no** form of this command to remove the EVC from the NetVanta unit's configuration. For example, to create an EVC named **DATA**, enter the command as follows:

   ```
   (config)#mef evc DATA
   (config-evc-DATA)#
   ```

2. You must specify the VLAN ID used by the service provider for the EVC. This VLAN ID, the s-tag, is used by the carrier to mark traffic from this EVC in the MEN. Specify the service provider VLAN ID in traffic outbound from this EVC by entering the **s-tag** <*vlan id*> command from the MEF EVC Configuration mode. The <*vlan id*> parameter is the ID of the service provider VLAN. Valid range is **1** to **4094**. By default, the s-tag VLAN ID associated with traffic outbound on the EVC is **0**, which indicates that the traffic on the EVC is untagged. Using the **no** form of this command returns the s-tag VLAN ID value to the default. To set the s-tag on traffic flowing through this EVC, enter the command as follows:


```
(config-evc-DATA)#s-tag 400
(config-evc-DATA)#
```

3. Specify whether the CE VLAN ID is preserved in outbound traffic using the **preserve-ce-vlan** command from the MEF EVC Configuration mode. The CE VLAN ID is the ID of the VLAN on the MEF Ethernet subinterface. A VLAN on the MEF Ethernet subinterface must be configured to preserve the CE VLAN ID. Preserving the CE VLAN ID is enabled by default, and the preserved CE VLAN ID can be used for matching traffic in EVC maps. Use the **no** form of this command to disable CE VLAN ID preservation in traffic outbound through the EVC. For most applications, you will not need to preserve the CE VLAN ID. To disable CE VLAN ID preservation, enter the command as follows:

   ```
   (config-evc-DATA)#no preserve-ce-vlan
   (config-evc-DATA)#
   ```

4. By default, the EVC is enabled once it is configured. However, if you need to disable the EVC or reenable it, enter the **shutdown** command from the MEF EVC Configuration mode. Using the **no** form of this command enables the EVC. For example, to enable the EVC after it has been disabled, enter the command as follows:

   ```
   (config-evc-DATA)#no shutdown
   (config-evc-DATA)#
   ```

5. Once the EVC is configured, it must be associated with a MEN port for traffic to flow. Associate the EVC with a specific MEN port (EFM group) using the **connect men-port efm-group** <*group id*> from the MEF EVC Configuration mode. The <*group id*> parameter is the ID of the EFM group to which you want to associate this EVC. Valid EFM group ID range is **1** to **1024**. Use the **no** form of this command to remove the association between this EVC and the specified EFM group. Multiple EVCs can be associated with a single EFM group. The EFM group must be created before associating the EVC and the group. For example, to associate EVC **DATA** with the EFM group (MEN port) **1**, enter the command as follows:

   ```
   (config-evc-DATA)#connect men-port efm-group 1
   (config-evc-DATA)#
   ```

The EVC is now configured.

Configuring the EVC Map

After the EVC is configured, you need to configure an EVC map which matches traffic to a specified EVC using matching criteria similar to that of QoS matching. Each EVC map is associated with a single EVC, and can match traffic to an EVC based on the traffic's CE VLAN ID, the CE VLAN priority (PRI) value, the DSCP value, or if the traffic has no CE VLAN ID (untagged). When determining traffic match criteria, keep in mind you can specify multiple criteria for a single map. Multiple match statements function as a logical AND.

Once you have specified the match criteria for the EVC map to map matching traffic to an EVC, you must associate the EVC map with both an EVC and a UNI. The UNI in this case is the MEF Ethernet interface to which you want to map the traffic. Even if you are using 802.1q encapsulation, the main interface will be used as the UNI. EVC maps will always have two connection statements: one to an EVC and one to a UNI, unless the traffic matching the EVC map is to be discarded.

After configuring the EVC map and associating it with an EVC, you can also optionally specify 802.1p values for the s-tag of the traffic and the queue used when the traffic is sent to the MEN.

To configure the EVC map, follow these steps:

1. Specify a name for the EVC map and enter the map's configuration mode using the **mef evc-map** <*name*> command from the Global Configuration mode prompt. The <*name*> parameter is the name of the EVC map. Using the **no** form of this command removes the EVC map from the NetVanta unit's configuration. For example, to create an EVC map called **Map1** and enter the MEF EVC Map Configuration mode, enter the command as follows:

   ```
   (config)#mef evc-map Map1
   (config-evc-map-MAP1)#
   ```

2. Specify the traffic matching criteria for the map to send traffic to the associated EVC using the following command **match [ce-vlan-id** <*vlan id*> **| ce-vlan-pri** <*value*> **| dscp** <*value*> **| untagged]** from the MEF EVC Map Configuration mode. The **ce-vlan-id** <*vlan id*> parameter specifies that traffic with a CE VLAN ID that matches the specified ID is mapped to the specified EVC.

   > NOTE *The CE VLAN ID maps to the VLAN ID configured on the MEF Ethernet subinterface.*

   The valid VLAN ID range is **1** to **4095**. The **ce-vlan-pri** <*value*> parameter specifies that traffic with a CE VLAN PRI value that matches the specified value is mapped to the specified EVC. The <*value*> parameter is the priority bit associated with the CE VLAN PRI, or the CE VLAN 802.1p value. Valid value range is **0** to **7**. The **dscp** <*value*> parameter specifies that traffic matching the specified DSCP value is mapped to the specified EVC. Valid range is **0** to **63**. The **untagged** parameter specifies that untagged traffic is mapped to the specified EVC. By default, no matching criteria is specified. Using the **no** form of this command removes the matching criteria from the EVC map. As with other QoS or traffic matching features, each traffic flow is compared to the first criteria entered in the map's configuration. Subsequent criteria are then compared to the traffic in the order the criteria were entered. If multiple criteria are entered in the map, the traffic must match all criteria to be mapped to the EVC.

   For example, to configure an EVC map to send all traffic with a CE VLAN ID of **5** *and* a DSCP value of **10** to a specific EVC, enter the **match** command as follows:

   ```
   (config-evc-map-MAP1)#match ce-vlan-id 5
   (config-evc-map-MAP1)#match dscp 10
   (config-evc-map-MAP1)#
   ```

3. After you have configured the EVC map to determine which traffic is mapped, you must specify what is to be done with the matching traffic. EVC maps are associated with both an EVC and a UNI (MEF Ethernet interface) to specify where the traffic comes from as it is evaluated (UNI) and where it is mapped to if it matches the criteria (EVC). EVC maps are associated with a UNI and an EVC using the **connect [evc** <*name*> **| uni mef-ethernet** <*slot/port*>**]** command. Both parameters must be entered as separate commands for the EVC map to function properly. The **evc** <*name*> parameter specifies the EVC to which the matching traffic is mapped, and the **uni mef-ethernet** <*slot/port*> parameter specifies the UNI from which the traffic is evaluated. Using the **no** form of this command removes the association between the EVC map and the EVC or the UNI. For example, to specify that EVC map **MAP1** is associated with MEF Ethernet interface **1/1** and with EVC **DATA**, enter the command from the MEF EVC Map Configuration mode as follows:


```
(config-evc-map-MAP1)#connect uni mef-ethernet 1/1
(config-evc-map-MAP1)#connect evc DATA
(config-evc-map-MAP1)#
```

Alternatively, you can also use the **connect discard** command to specify that traffic matching the EVC map criteria is discarded. Using the **no** form of this command disables traffic discard. For example, to specify that traffic matching the criteria outlined in EVC map **MAP1** is discarded, enter the command from the MEF EVC Map Configuration mode as follows:

```
(config-evc-map-MAP1)#connect discard
(config-evc-map-MAP1)#
```

Specifying the MEN Values for Traffic That Matches the EVC Map Criteria (Optional)

After you have configured the matching criteria used by the EVC map and associated the EVC map with both a UNI and an EVC, you can optionally define the MEN values applied to the traffic matching the EVC map. The configurable MEN values for traffic matching the EVC map include the MEN priority bit (802.1p value) and specifying the queue to which the traffic is sent. To configure the MEN values for the matched traffic, follow these steps:

1. Optionally specify the priority that the EVC will use for traffic matching the specific EVC map by entering the **men-pri [inherit |** <*value*>**]** command from the MEF EVC Map Configuration mode prompt. The **inherit** parameter specifies that the MEN priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. By default, matched traffic has an inherited priority. The <*value*> parameter specifies a specific priority value is given to the matched traffic in the EVC. Valid range is **0** to **7**. Using the **no** form of this command returns the MEN priority to the default value.

   For example, to specify that traffic matching EVC map **MAP1** is given a priority of **5** in the associated EVC, enter the command as follows:

   ```
   (config-evc-map-MAP1)#men-pri 5
   (config-evc-map-MAP1)#
   ```

2. You can also optionally specify the output queue used by the EVC for traffic that matches the particular EVC map using the **men-queue [inherit |** <*value*>**]** command from the MEF EVC Map Configuration mode. The **inherit** parameter specifies that the queue used by the EVC for the matched traffic is based on the MEN priority setting (specified with the **men-pri** command). By default, matched traffic inherits the queue information. The <*value*> parameter specifies a queue to which the matched traffic is mapped by the EVC. Valid queue range is **1** to **8**. Using the **no** form of this command returns the MEN queue to the default. For example, to specify that traffic matching EVC map **MAP1** is queued in output queue **4**, enter the command as follows:

   ```
   (config-evc-map-MAP1)#men-queue 4
   (config-evc-map-MAP1)#
   ```

The EVC map is now configured and you can configure the MEF policer policy.

Configuring the MEF Policer Policy

The MEF policer policy limits the amount of traffic outbound from the NetVanta unit to the MEN. Traffic can be limited based on CIR, CBS, EBS, and EIR thresholds. The CBS and CIR thresholds specify the committed burst sizes and transmission rates of traffic. When these thresholds are exceeded, traffic may be dropped. The EBS and EIR thresholds specify the excess burst sizes or transmission rates (over and above

the committed sizes or rates), basically specifying the maximum burst size or rate allowable before the traffic is dropped. In this way, the MEF policer policy functions similarly to Frame Relay policing. Properly configuring the MEF policer policy relies on specifying the name and the thresholds for the policy, and applying the policy to an EVC component (UNI, EVC, or EVC map). To configure the MEF policer policy, follow these steps:

1. Create and name the policy by entering the **mef policer** <*name*> command from the Global Configuration mode prompt. The <*name*> parameter is the name given to this policy. For example, to create the MEF policer policy **Policy1** and enter the policy's configuration mode, enter the command as follows:

   (config)**#mef policer Policy1**
   (config-policer-POLICY1)#

2. Once you have entered the MEF Policer Policy Configuration mode, you can specify the CBS, CIR, EBS, and EIR thresholds. To set the CIR threshold, enter the **cir** <*number*> command from the MEF Policer Policy Configuration mode. The <*number*> parameter is the average maximum transmission rate of traffic in kilobits per second (kbps) allowed before the traffic may be dropped. Valid range is **250** to **600000** kbps. By default, the CIR threshold is **600000** kbps. Using the **no** form of this command returns the CIR threshold to the default value. For example, to change the CIR threshold for the MEF policer policy, enter the command as follows:

   (config-policer-POLICY1)**#cir 5000**

   To set the CBS threshold, enter the **cbs** <*number*> command. The CBS threshold, or the maximum number of bytes transmitted as a burst before the policer policy may begin to drop traffic. Valid range is **0** to **2147483647** bytes. By default, the CBS threshold is **0** bytes. Using the **no** form of this command returns the CBS threshold to the default value. To change the CBS threshold for the MEF policer policy, enter the command as follows:

   (config-policer-POLICY1)**#cbs 6500**

   To set the EIR threshold, enter the **eir** <*number*> command from the MEF Policer Policy Configuration mode. The <*number*> parameter is the allowed maximum rate in kbps, at which traffic will be transmitted before the policer policy drops the traffic. This is the maximum above the CIR value. The EIR must be greater or equal to the CIR. Valid range is **250** to **600000** kbps. By default, the EIR threshold is **600000** kbps. Using the **no** form of this command returns the EIR threshold to the default value. To change the EIR threshold for the MEF policer policy, enter the command as follows:

   (config-policer-POLICY1)**#eir 6000**

   To set the EBS threshold, enter the **ebs** <*number*> command from the MEF Policer Policy Configuration mode. The <*number*> parameter is the allowed maximum number of bytes transmitted as a burst of data, over and above the CBS threshold, before the policer drops the traffic. Valid range is **0** to **2147483647** bytes, with a default value of **0** bytes. Using the **no** form of this command returns the threshold to the default value. To change the EBS threshold for the MEF policer policy, enter the command as follows:

   (config-policer-POLICY1)**#ebs 1000**

3. After configuring the thresholds for queuing or dropping traffic, you must apply the MEF policer policy to an EVC component. EVC components include EVCs, EVC maps, and UNIs. MEF policer policies are applied to EVC components using the **per [custom [add-map** <*name*> **| remove-map** <*name*>**] | evc** <*name*> **| uni mef-ethernet** <*slot/port*>**]** command from the MEF Policer Policy Configuration mode. The **custom** parameter allows you to apply the MEF policer policy to one or more EVC maps.

The additional **add-map** and **remove-map** parameters add or remove the policer from the EVC map, and the <*name*> parameter specifies to which EVC map the policer policy is added or removed. The **evc** parameter allows you to apply the MEF policer policy to an EVC, and the <*name*> parameter specifies to which EVC the map is applied. When policies are applied to an EVC, they are applied to egress traffic on the EVC. The **uni mef-ethernet** <*slot/port*> parameter allows you to apply the MEF policer policy to egress traffic on the specified MEF Ethernet interface (the UNI) for all connected EVCs. You must specify the slot and port of the MEF Ethernet interface to apply the policer policy. For example, to apply MEF policer policy **POLICY1** to EVC map **MAP1**, enter the command as follows:

```
(config-policer-POLICY1)#per custom add-map MAP1
(config-policer-POLICY1)#
```

Using the **no** form of this command removes the policer policy from the EVC component.

The MEF policer policy configuration is completed once the policy is applied to an EVC component.

Configuring MEF Ethernet QoS (Optional)

You can optionally configure, on a global level, the MEF Ethernet QoS parameters. These parameters specify the hardware queues used by the EVC when traffic matching an EVC map is discovered, as well as the MEN priority given to untagged traffic. These values are inherited by the EVC map for traffic that matches the map criteria when MEN queue parameters are configured (refer to *Specifying the MEN Values for Traffic That Matches the EVC Map Criteria (Optional) on page 13*). To configure the MEF Ethernet QoS parameters, follow these steps:

1. You can specify the queue used by traffic using the **mef qos cos-map** <*number*> <*value*> from the Global Configuration mode. The <*number*> parameter is the queue to which the traffic should be sent, and the <*value*> parameter is the CoS value mapped to the queue. Valid <*number*> range is **1** to **8**, and valid <*value*> range is **0** to **7**. These values are then used by the EVC map when **men-queue** is set to **inherit**. Using the **no** form of this command returns the queue priorities to the default values. The default values are outlined in *Table 1*.

Table 1. Default MEF QoS Queue Assignments

Queue and Assigned CoS Values	One CoS Value is Assigned to Each Queue by Default
(config)**#mef qos cos-map 1 1**	CoS value 1 is assigned to queue 1 by default.
(config)**#mef qos cos-map 2 0**	CoS value 0 is assigned to queue 2 by default.
(config)**#mef qos cos-map 3 2**	CoS value 2 is assigned to queue 3 by default.
(config)**#mef qos cos-map 4 3**	CoS value 3 is assigned to queue 4 by default.
(config)**#mef qos cos-map 5 4**	CoS value 4 is assigned to queue 5 by default.
(config)**#mef qos cos-map 6 5**	CoS value 5 is assigned to queue 6 by default.
(config)**#mef qos cos-map 7 6**	CoS value 6 is assigned to queue 7 by default.
(config)**#mef qos cos-map 8 7**	CoS value 7 is assigned to queue 8 by default.

For example, to specify that CoS values of **3** and **4** are mapped to queue **1**, enter the command as follows:

(config)**#mef qos cos-map 1 3 4**
(config)#

2. You can also specify the MEN priority for untagged traffic on the EVC. To specify the MEN priority for untagged traffic from the MEF Ethernet interface, enter the **mef qos untagged** <*value*> command from the Global Configuration mode prompt. The <*value*> parameter is the MEN priority. Valid range is **0** to **7**. By default, no MEN priority is assigned to untagged traffic. Using the **no** form of this command removes the priority from untagged traffic. To specify the MEN priority for untagged traffic, enter the command as follows:

   (config)**#mef qos untagged 5**

EFM NIM2 and MEF Ethernet Interface Configuration Examples

The following sections describe typical EFM NIM2 and MEF Ethernet interface configurations. All of the following examples were configured using the CLI. The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide you with a method of copying and pasting directly from this guide into the CLI. You should make the necessary adjustments to these configurations before adding them to your configuration to ensure they will function properly in your network.

Single EVC Configuration Using a NetVanta 6310 and Total Access 5000 with Pre-Provisioning

In the following configuration example, a NetVanta 6310/6330 Series product with an EFM NIM2 is configured with an EFM group, and receives all other configuration information from a Total Access 5000. The Total Access 5000 is configured with an EFM group and an EVC. All Total Access 5000 configuration information is based on a Total Access 5000 running SR 5.5.x connected via a SHDSL EFM NIM2 to a NetVanta 6310 running A4.05. In this example, the NetVanta 6310 receives its EFM NIM2 configuration from a Total Access 5000 unit through pre-provisioned IP information. The IP address and subnet mask, default gateway, host name, default EVC, default EVC map, and default route are all provided by the Total Access 5000 to the NetVanta 6310 as soon as an active link is added to the EFM group in the NetVanta 6310.

NetVanta 6310 Configuration

```
interface efm-group 1
    connect shdsl 1/1
    connect shdsl 1/2
    connect shdsl 1/3
    connect shdsl 1/4
    no shutdown
```

Total Access 5000 Configuration

```
interface efm-group 1/1/1
    alias “LAB_NV_6310_SHDSL_EFM”
    subtended-host snmp-server chassis-id “Lab_NV6310_SHDSL_EFM”
```



```
    subtended-host ip address 10.42.22.10 255.255.255.252
    subtended-host ip default-gateway 10.42.220.9
    link 1/9-12
    subtended-host s-tag 3320
!
evc “Lab_NV6310_SHDSL_EFM”
    s-tag 3320
    connect men-port default-ethernet
    connect men-port efm-group 1/1/1
    no shutdown
!
!
interface shdsl 1/1/9
    no shutdown
    description “Lab_NV6310_SHDSL_EFM”
!
interface shdsl 1/1/10
    no shutdown
    description “Lab_NV6310_SHDSL_EFM”
!
interface shdsl 1/1/11
    no shutdown
    description “Lab_NV6310_SHDSL_EFM”
!
interface shdsl 1/1/12
    no shutdown
    description “Lab_NV6310_SHDSL_EFM”
!
```

EVC Management Information Received by NetVanta 6310

```
2010.12.06 12:26:14 EFM slot 1: Add link 1 to EFM group comm ID 1
2010.12.06 12:26:14 EFM Provisioning: Slot 1 Received MEN sTag for EVC, sTag: 3220, MenPort:
    efm-group 1
2010.12.06 12:26:14 EFM Provisioning: Slot 1 Received MEN sTag for EVC, sTag: 3320, MenPort:
    efm-group 1
2010.12.06 12:26:14 EFM.OAM Provisioning: Slot 1 Received MEN sTag provisioning OAM
2010.12.06 12:26:14 INTERFACE_STATUS.mef-ethernet 1/1 changed state to up
2010.12.06 12:26:14 EFM Provisioning: Slot 1 Received IP: 10.42.220.10 NM: 255.255.255.252 DefGW:
    10.42.220.9
2010.12.06 12:26:15 EFM Provisioning: Slot 1 Received Hostname: Lab_NV6310_SHDSL_EFM
2010.12.06 12:26:15 EFM MEF EVC Map DEFAULT: Connect UNI mef-ethernet 1/1
2010.12.06 12:26:15 EFM MEF EVC Map DEFAULT: Connect EVC DEFAULT
2010.12.06 12:26:15 MEF Slot 1: connect Map DEFAULT EVC DEFAULT MEN port efm-group 1
        Match any S-tag 3320 Preserve ce-vlan-id MEN Pri 999 MEN Q 999
2010.12.06 12:26:15 EFM Provisioning: Slot 1 Received DEFAULT Evc-Map, Uni: mef-ethernet 1/1,
        Evc: DEFAULT
2010.12.06 12:26:15 EFM Provisioning: Slot 1 Received DEFAULT Evc, sTag: 3320,
        MenPort: efm-group 1
```


NetVanta 6310 EFM NIM2 Configuration After Pre-Provisioning

```
interface mef-ethernet 1/1
    encapsulation 802.1q
    no shutdown
!
interface mef-ethernet 1/1.1
    vlan-id 1 native
    ip address 10.42.220.10 255.255.255.252
    no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.42.220.9
!
mef evc DEFAULT
    s-tag 3320
    connect men-port efm-group 1
    no shutdown
!
mef evc-map DEFAULT
    connect uni mef-ethernet 1/1
    connect evc DEFAULT
    no shutdown
!
```

Multiple EVCs with QoS Configuration Using a NetVanta 6310

The following example is the configuration of two EVCs (DATA and DEFAULT), four EVC maps, three of which are applied to the EVC DEFAULT and one applied to the EVC DATA, one EFM group, one MEF Ethernet interface, and two MEF Ethernet subinterfaces on a NetVanta 6310. The QoS portion of this configuration relies on the QoS policy applied to the MEF Ethernet interface (VoIP_Out_Untagged). Each EVC has a different s-tag, but both are configured without the preservation of the CE VLAN ID. In addition, because 802.1q encapsulation is used on the MEF Ethernet interface, the native VLAN is specified on the MEF Ethernet subinterface **1/1.1**. EVC **DEFAULT** is used for voice traffic and EVC **DATA** is used for customer data in this configuration example.

```
interface mef-ethernet 1/1
    subtended-host mode disabled
    encapsulation 802.1q
    qos-policy out VoIP_Out
    no shutdown
!
interface mef-ethernet 1/1.1
    vlan-id 1 native
    ip address 10.42.220.10 255.255.255.252
    media-gateway ip primary
    no shutdown
!
```



```
interface mef-ethernet 1/1.3220
    vlan-id 3220
    ip vrf forwarding Data
    ip address 10.42.220.2 255.255.255.248
    no shutdown
!
interface efm-group 1
    connect shdsl 1/1
    connect shdsl 1/2
    connect shdsl 1/3
    connect shdsl 1/4
    no shutdown
!
mef evc DATA
    s-tag 3220
    no preserve-ce-vlan
    connect men-port efm-group 1
    no shutdown
!
mef evc DEFAULT
    s-tag 3320
    no preserve-ce-vlan
    connect men-port efm-group 1
    no shutdown
!
mef evc-map DATA
    match ce-vlan-id 3220
    connect uni mef-ethernet 1/1
    connect evc DATA
    no shutdown
!
mef evc-map DEFAULT
    match untagged
    connect uni mef-ethernet 1/1
    connect evc DEFAULT
    no shutdown
!
mef evc-map DEFAULT_VOICE_RTP
    match untagged
    match dscp 46
    men-pri 5
    connect uni mef-ethernet 1/1
    connect evc DEFAULT
    no shutdown
!
```



```
mef evc-map DEFAULT_VOICE_SIGNALING
    match untagged
    match dscp 26
    men-pri 3
    connect uni mef-ethernet 1/1
    connect evc DEFAULT
    no shutdown
!
```

Using the EFM NIM2 for T-scan and Bad Splice Detection

The EFM NIM2, when used with SHDSL interfaces, can provide T-scan and bad splice detection methods of testing lines for faults. Both test types can provide an estimate of the distance to the fault, and T-scan can provide information as to the type of fault. Both test types, and their configuration, are described in the following sections.

A4.05 application code and A4.05 NIM2 code are required for the use of both T-scan and bad splice detection features.

T-scan Line Test

The T-scan line test is a testing feature that allows users to isolate faults in lines by estimating the distance to the fault and determining the type of fault, whether a short or an open connection. T-scan is an intrusive test, which causes trained SHDSL loops to go down, but it is useful as a method for finding faults in loops that will not train, rather than as a performance metric for operational loops.

T-scan can be started on any port that is enabled from the SHDSL interface in the CLI. T-scan tests typically take from 20 seconds to one minute to complete, and timeout after 90 seconds to restore control to the CLI. When the test is complete, results are displayed in the CLI or can be viewed at a later time using the **test tscan display-results** command. Displayed results include the date and time of the test, the status of the test, the line rate used while T-scan operates (typically 16 or 32 DSOs), the distance to the fault if one is detected (displayed in feet), and the fault type that is found. The minimum distance for the T-scan test is **0** feet and the maximum T-scan test distance is **12000** feet. Faults detected by the T-scan test include the following:

- OK (no faults found)
- Open (an open loop is detected)
- Short (a short detected in the loop)
- Unknown (unable to determine fault type)
- GFI (a ground fault is detected)
- Single Open (a single open fault is detected)

To initiate a T-scan test, enter the **test tscan** command from the SHDSL Interface Configuration mode. You should enter this command for the interface you want to test. For example, to begin a T-scan test on the SHDSL interface **1/1**, enter the command as follows:

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#test tscan
Accumulating Data.....
```

The series of dots will continue to be displayed until the T-scan test is completed. Once the test is complete, the results are displayed in the CLI.

To view T-scan test results after the initial results are displayed, enter the **test tscan display-results** from the SHDSL interface on which the test was run. For example, to display the last T-scan test results for SHDSL interface **1/1**, enter the command as follows:

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#test tscan display-results
shdsl 1/1 TSCAN Results
Date/Time   : Thu, October 28, 2010 04:30:59 PM, CDT
Status      : Done
Rate        : 32 DSOs
Distance    : 1100 ft
Fault       : Open
```

To clear the results of previously completed T-scan tests, enter the **test tscan clear-results** command from the SHDSL Interface Configuration mode.

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#test tscan clear-results
```

When results are cleared, the test result fields return to their default state as shown below.

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#test tscan display-results
shdsl 1/1 TSCAN Results
Date/Time   : Not Run
Status      : Idle
Rate        : 32 DSOs
Distance    : N/A
Fault       : Unknown
```

Bad Splice Detection Test

The bad splice detection test is a line testing feature that allows users to locate intermittent faults in lines by estimating the distance to the fault. Splice detection is always enabled on the SHDSL EFM NIM2 module and it continually monitors the signal-to-noise ratio (SNR) of the connection. When a negative change in the SNR is detected, a measurement is taken to determine the distance to where the issue is possibly occurring on the line.

Unlike T-scan testing, bad splice detection testing continually runs while the SHDSL loop is trained and it does not interfere with normal operation. Therefore, T-scan is helpful when the loop will not train, while bad splice detection is used to monitor the loop for possible weaknesses and intermittent faults.

Bad splice detection results are compiled for 24-hour periods. A history of the test results is kept for the past seven days and can be displayed in the CLI using the **show interface shdsl** <*slot/port*> **splice-detect 24-hour [**<*interval*>**]** command from the Enable mode. Results for the bad splice detection test include the test interval (whether the current 24-hour period or a previous 24-hour interval), a summary of issues found during the period (bad splice, loss of signal, or no trouble found), and the distance to the fault and the number of times a fault detection has been made at that distance. The following are the results that can be displayed:

- Current Splice Detect Data (indicates this is the splice detection data for the current 24-hour period)
- Interval <*N*> Splice Detect Data (indicates a previous period of data is displayed, where <*N*> can range from 1 to 7)
- Summary: No Trouble Found (indicates the port is UP and no faults were found)
- Summary: Bad splice detected (indicates a bad splice has been detected)
- Summary: Loss of Signal (indicates the port is not currently in the UP state)
- Distance (indicates the estimated distance in either meters or feet to the fault)
- Count (indicates the number of times a problem has been detected at the specified distance)

Bad splices are declared by the test when at least five fault detections have been made at a single distance. If one of the previous periods of testing resulted in at least five detections at a single distance, it will also display in the Summary portion of the test results. If there are multiple bad splices across one or more testing intervals, the displayed bad splice is the one that has occurred the most times for the currently displayed interval results and the one with the highest line rate.

Because bad splice detection is always enabled and cannot be disabled, there is very little configuration necessary. Tests cannot be run on demand, but you can select when to display the results. In addition, the distance measurement to the fault can be displayed in either feet or meters. To change the distance measurement for the bad splice test, enter the **test splice-detect distance-type [feet | meters]** command from the SHDSL Interface Configuration mode. By default, results are displayed in feet. Using the **no** form of this command returns measurements to the default unit of measurement. For example, to change the distance measurement to meters, enter the command as follows:

```
(config)#interface shdsl 1/1
(config-shdsl 1/1)#test splice-detect distance-type meters
```

To display the bad splice detection test results, enter the **show interface shdsl** <*slot/port*> **splice-detect 24-hour [**<*interval*>**]** command from the Enable mode. The optional <*interval*> parameter allows you to specify that results from one or more of the previous 24-hour intervals are displayed. Valid interval range is **1** to **7**. You can enter a single interval, or range of intervals when separated by a dash (for example, **1-3**). If you do not specify an interval, the results from the current interval are displayed. To display bad splice detection test results, enter the command as follows:

#show interface shdsl 1/1 splice-detect 24-hour
Current Splice Detect Data
Summary: No Trouble Found

Distance (ft)	Count
0	0
200	0
400	0
600	0
800	0
1000	0
1200	0

You can clear the data for all intervals by issuing the **clear counters shdsl** <*slot/port*> **splice-detect** command from the Enable mode prompt. For example, to clear all gathered data for bad splice detection tests on SHDSL interface **1/1**, enter the command as follows:

#clear counters shdsl 1/1 splice-detect

Using the EFM NIM2 for PPPoE Applications

In AOS firmware release R10.6.0, the ability to cross-connect a MEF Ethernet subinterface with a Point-to-Point Protocol (PPP) interface was introduced. To use this feature, 802.1q encapsulation is enabled on the MEF Ethernet interface, and a subinterface is created to be connected to the PPP interface. Subinterfaces are identified in the following format: **interface type** <*slot/port.subinterface id*>, for example **interface mef-ethernet 1/1.21**.

When using PPPoE over the MEF Ethernet subinterface, the PPPoE traffic uses the IP address of the PPP interface, but non-PPPoE traffic is also allowed. IP addresses can be on the MEF Ethernet interface when PPPoE is used on the full interface, but not when PPPoE is used on a subinterface. An IP address cannot be configured on the main MEF Ethernet interface after 802.1q encapsulation has been enabled.

The most complex part of this feature is understanding the new combinations of QoS, CoS, and traffic shaping that are available on the various network layers. By introducing PPPoE on an MEF Ethernet subinterface, there can be multiple PPP or IP subinterfaces connected to a single physical interface through multiple VLANs. When using QoS in this application, the QoS map must be applied to the MEF Ethernet interface because in order to operate correctly, it must be applied on the lowest common interface for all the traffic. When using PPPoE over a subinterface, the two most important considerations are combining multiple traffic flows and reprioritizing traffic.

Combining Multiple Traffic Flows

With the support of PPPoE over the MEF Ethernet subinterface, multiple traffic flows are combined on the MEF Ethernet interface. In general, it is not a good idea to drastically oversubscribe the bandwidth of the interface by adding more PPP traffic than can be handled. Also, each PPP interface reports it has the full bandwidth of the lower layer interface because that is the theoretical maximum. This means that if multiple PPP interfaces are sharing a single MEF Ethernet interface, it will essentially be oversubscribed. This

traffic can be managed, however, using Weighted Fair Queueing from a QoS map applied to the interface that matches traffic based on the VLAN of each subinterface. When using PPPoE, the PPP queue must always be first-in first-out (FIFO), and when using 802.1q encapsulation, the QoS map must always be on the main interface.

Reprioritizing Traffic

When using an EFM NIM2, traffic can be prioritized at Layer 3 by applying a QoS map to the MEF interface, and at Layer 2 with P-bits on the EVC map and with MEF policers. *Figure 3* illustrates Layer 2 and Layer 3 traffic prioritization.

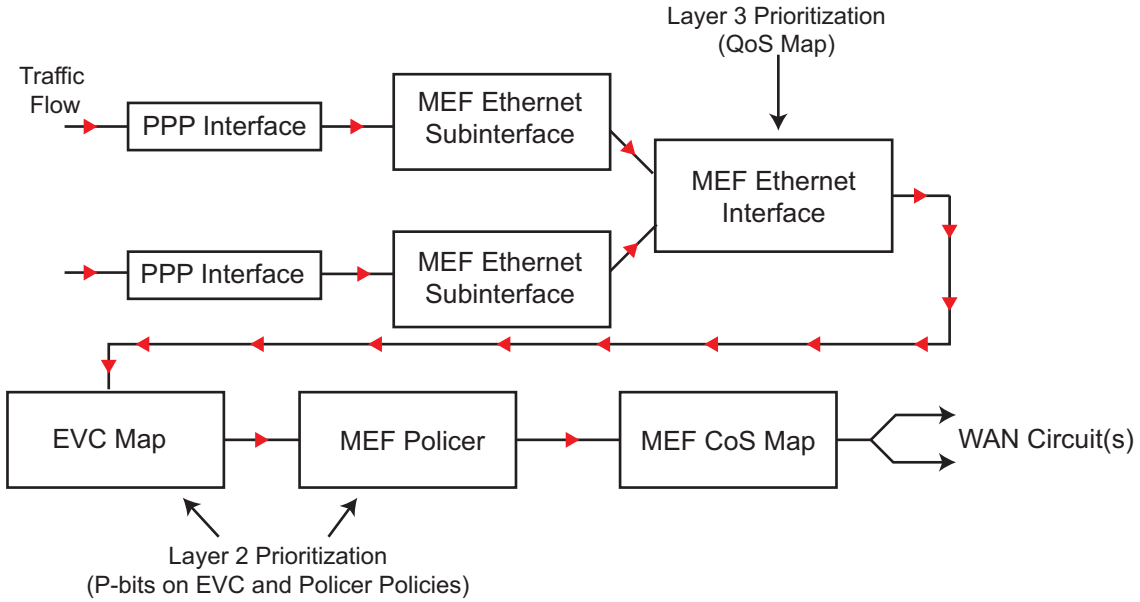

Figure 3. Reprioritizing PPPoE Traffic in Layer 2 and Layer 3

Unexpected results can occur if traffic is prioritized on one layer but not on the other. When using PPPoE with QoS on an EFM NIM2, there are several recommendations:

- Use a QoS map to perform normal Layer 3 QoS functions (such as, priority queueing, bandwidth reservation, etc.).
- In the QoS map configuration, use the VLAN ID applied to each MEF Ethernet subinterface as the traffic matching criteria when traffic from a specific interface needs to be selected and prioritized.
- Traffic shaping on the MEF Ethernet interface, or shaping on the QoS map, must be configured to use QoS on a MEF Ethernet interface so the map knows the maximum amount of bandwidth it can use.
- The QoS map must be applied to the main MEF Ethernet interface, not a subinterface.
- Use the **men-pri** commands on the EVC map(s) to set the P-bits on the S-tag (refer to *Specifying the MEN Values for Traffic That Matches the EVC Map Criteria (Optional) on page 13*).

EFM NIM2 PPPoE Configuration Considerations

When using PPPoE over an EFM NIM2 module, remember the following:

- A traffic shaper must be applied to the MEF interface in order for QoS to function properly.
- Matching DSCP values in an EVC map does not affect packets that are not IP packets. If IP packets are encapsulated in PPP, they cannot be matched even if the IP packet has a matching DSCP value. However, this match can be performed on a QoS map on the MEF Ethernet interface since the map can look at the IP header of the packet and match the DSCP value.

MEF Ethernet and PPPoE Configuration Example One

In this example, two PPP interfaces have been configured to communicate over a MEF Ethernet interface using four SHDSL links and two MEF Ethernet subinterfaces. The two subinterfaces use VLAN IDs 21 and 22. The MEF Ethernet interface is configured with 802.1q encapsulation. Configuration for this example includes:

- Configuring one subinterface with the native VLAN (for control protocol traffic)
- Configuring the VLANs for two additional subinterfaces
- Creating an EFM group with all four SHDSL interfaces
- Adding an S-tag and connecting the EVC to the EFM group
- Connecting the MEF Ethernet interface and the EVC through the EVC map
- Configuring the PPP interfaces to use FIFO queueing and to connect to the MEF subinterfaces

In this configuration, the PPP client receives Ethernet traffic on one side of the network, and sends it over PPP back to a Total Access 5000. *Figure 4* illustrates the network topology for this type of scenario.

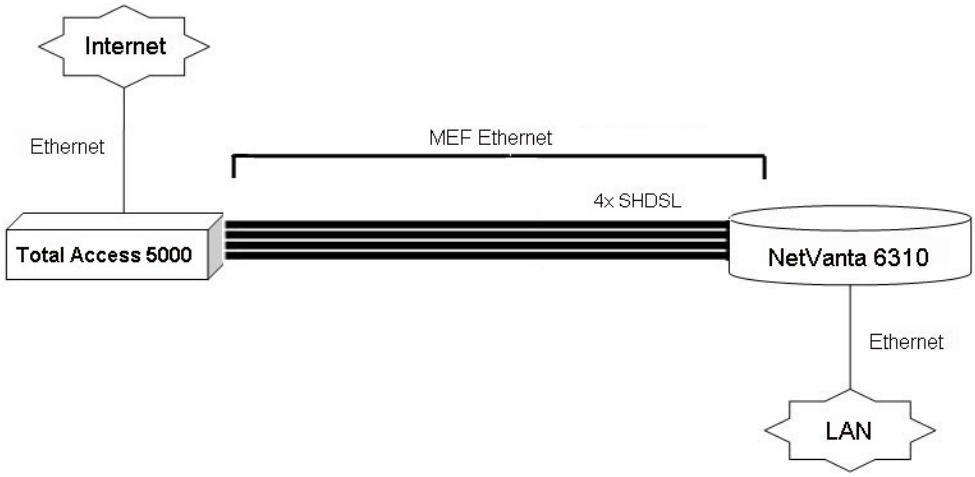

Figure 4. MEF Ethernet and PPPoE

The configuration of the MEF Ethernet interface, its subinterfaces, and the PPP interfaces are as follows:

```
interface mef-ethernet 1/1
    subtended-host mode disabled
    encapsulation 802.1q
    no shutdown
```



```
!
interface mef-ethernet 1/1.1
     vlan-id 1 native
     no ip address
     no shutdown
!
interface mef-ethernet 1/1.21
     vlan-id 21
     no ip address
     no shutdown
!
interface mef-ethernet 1/1.22
     vlan-id 22
     no ip address
     no shutdown
!
interface shdsl 1/1
     no shutdown
!
interface shdsl 1/2
     no shutdown
!
interface shdsl 1/3
     no shutdown
!
interface shdsl 1/4
     no shutdown
!
interface efm-group 1
     connect shdsl 1/1
     connect shdsl 1/2
     connect shdsl 1/3
     connect shdsl 1/4
     no shutdown
!
mef evc DATA
     s-tag 100
     connect men-port efm-group 1
     no shutdown
!
mef evc-map DATA
     connect uni mef-ethernet 1/1
     connect evc DATA
     no shutdown
!
```



```
interface ppp 1
    ip address negotiated
    no fair-queue
    no shutdown
    cross-connect 1 mef-ethernet 1/1.21 ppp 1
!
interface ppp 2
    ip address negotiated
    no fair-queue
    no shutdown
    cross-connect 2 mef-ethernet 1/1.22 ppp 2
!
```

MEF Ethernet and PPPoE Configuration Example Two

This example describes one method for applying QoS in configurations that use PPPoE over an 802.1q encapsulated subinterface on the EFM NIM2 module. This example describes a simple QoS configuration that applies queueing to the MEF Ethernet interface to which a PPP interface is connected through a MEF Ethernet subinterface. The configuration dedicates 90 percent of the available bandwidth on the MEF Ethernet interface to the PPP traffic. The steps for this configuration include:

- Configuring QoS maps for PPP traffic based on VLANs
- Configuring the MEF Ethernet interface with a specified traffic shape rate and maximum reserved bandwidth, and applying the QoS policy
- Configuring the MEF Ethernet subinterface
- Configuring the PPP interface to cross-connect with the MEF Ethernet subinterface

The configuration of the MEF Ethernet interface, its subinterfaces, and the PPP interfaces are as follows:

```
!
qos map MAP 10
    match vlan 21
    bandwidth percent 90
!
interface mef-ethernet 1/1
    subtended-host mode disabled
    encapsulation 802.1q
    traffic-shape rate 10822000
    max-reserved-bandwidth 95
    qos-policy out MAP
    no shutdown
!
interface mef-ethernet 1/1.21
    vlan-id 21
    no ip address
    no shutdown
!
```



```
interface ppp 1
    ip address negotiated
    no fair-queue
    no shutdown
    cross-connect 1 mef-ethernet 1/1.21 ppp 1
!
```

MEF Ethernet and PPPoE Configuration Example Three

This example describes how QoS on the MEF Ethernet interface and CoS on the EVC map are configured. Traffic shaping, which cannot occur on the EVC map and must be configured on the MEF Ethernet interface, is one reason QoS and CoS might be needed on both network layers. In addition, CoS sets the P-bits that assigns traffic to one of the egress queues on the EFM NIM2 module, so you must carefully review your configuration to make sure that traffic is not unintentionally reprioritized on the lower layer.

In this example, one PPP interface is used to handle customer traffic, and one IP interface is used to handle management traffic. The PPP interface receives 90 percent of the bandwidth, and the IP interface receives the other 5 percent. The IP traffic is configured with P-bits value of **6** (internetwork control) on the management VLAN. The S-tag P-bits value is set by inheriting the P-bits value that was previously set in the packet's CE VLAN tag. In this case, all previously set P-bits are **0** (best effort), which is the default value.

The steps necessary for this configuration include:

- Creating a QoS map (**MAP**)
- Configuring the map to match all PPP traffic with 90 percent of the bandwidth and IP traffic with 5 percent of the bandwidth
- Applying the map to the MEF Ethernet interface
- Configuring the EVC map to set the IP traffic's P-bits to **6** by matching traffic on VLAN 22

The configuration of the MEF Ethernet interface, its subinterfaces, and the PPP interfaces are as follows:

```
!
qos map MAP 10
    match vlan 21
    bandwidth percent 90
!
qos map MAP 11
    match vlan 22
    bandwidth percent 5
!
interface mef-ethernet 1/1
    subtended-host mode disabled
    encapsulation 802.1q
    traffic-shape rate 10822000
    max-reserved-bandwidth 95
    qos-policy out MAP
    no shutdown
!
```



```
interface mef-ethernet 1/1.1
    vlan-id 1 native
    no ip address
    no shutdown
!
interface mef-ethernet 1/1.21
    vlan-id 21
    no ip address
    no shutdown
!
interface mef-ethernet 1/1.22
    vlan-id 22
    ip address 10.10.22.2 255.255.255.0
    no shutdown
!
interface shdsl 1/1
    no shutdown
!
interface shdsl 1/2
    no shutdown
!
interface shdsl 1/3
    no shutdown
!
interface shdsl 1/4
    no shutdown
!
interface efm-group 1
    connect shdsl 1/1
    connect shdsl 1/2
    connect shdsl 1/3
    connect shdsl 1/4
    no shutdown
!
mef evc DATA
    s-tag 101
    connect men-port efm-group 1
    no shutdown
!
mef evc-map DATA-IP
    match ce-vlan-id 22
    men-pri 6
    connect uni mef-ethernet 1/1
    connect evc DATA
    no shutdown
!
```



```
mef evc-map DATA-PPP
    match ce-vlan-id 21
    connect uni mef-ethernet 1/1
    connect evc DATA
    men-pri inherit
    no shutdown
!
interface ppp 1
    ip address negotiated
    no fair-queue
    no shutdown
    cross-connect 1 mef-ethernet 1/1.21 ppp 1
!
```

EFM NIM2/MEF Ethernet Configuration Command Summary

The following tables summarize the commands associated with configuring and using the EFM NIM2 and the MEF Ethernet interface.

Table 2. EFM Group Configuration Commands

Prompt	Command	Description
(config)#	**[no] interface efm-group** *<group id>*	Creates an EFM group and enters the group's configuration mode. Valid group ID range is **1** to **1024**. By default, no EFM groups exist. Using the **no** form of this command removes the group from the unit's configuration.
(config-efm-group 1)#	**[no] connect** *<interface>*	Associates an interface with the EFM group. Specify an interface in the format *<interface type [slot/port]>*. Available interfaces for the EFM group include SHDSL, T1, and E1 interfaces. Using the **no** form of this command removes the interface from the group.
(config-efm-group 1)#	**[no] loopback detection**	Enables or disables the sending of Bandwidth Allocation Control Protocol (BACP) frames used for EFM loopback detection. By default, loopback detection is enabled. This feature should be disabled on the EFM group in the AOS device for use with a Total Access 3000 EFM module.

Table 2. EFM Group Configuration Commands *(Continued)*

Prompt	Command	Description
(config-efm-group 1)#	**[no] thresholds xcv [1e-5 | 1e-6 | 1e-7]**	Specifies the excessive code violation threshold for the links in the EFM group. The **1e-5**, **1e-6**, and **1e-7** parameters specify the threshold bit error rate. By default, thresholds are set to **1e-7**. Using the **no** form of this command returns to the default threshold.
(config-efm-group 1)#	**[no] xcv-link-removal**	Specifies that when XCV thresholds are exceeded, links are removed from the EFM group. Using the **no** form of this command disables the link removal. By default, link removal is enabled.
(config-efm-group 1)#	**no shutdown**	Enables the EFM group.

Table 3. MEF Ethernet Interface Configuration Commands

Prompt	Command	Description
(config)#	**[no] interface mef-ethernet [**<*slot/port*> **|** <*slot/port.subinterface*>**]**	Enters the MEF Ethernet Interface Configuration mode. Using the **no** form of this command removes the interface or the 802.1q subinterfaces from the unit's configuration.

Table 4. EVC Configuration Commands

Prompt	Command	Description
(config)#	**[no] mef evc** <*name*>	Creates an EVC and enters the MEF EVC Configuration mode. Using the **no** form of this command removes the EVC from the unit's configuration.
(config-evc-DATA)#	**[no] preserve-ce-vlan**	Specifies that the CE VLAN ID (ID of VLAN on MEF Ethernet subinterface) is preserved in outbound traffic. By default, CE VLAN ID preservation is enabled. Using the **no** form of this command disables CE VLAN ID preservation in outbound EVC traffic.

Table 4. EVC Configuration Commands *(Continued)*

Prompt	Command	Description
(config-evc-DATA)#	**[no] s-tag** <*vlan id*>	Specifies that the service provider VLAN ID is used by the EVC. The <*vlan id*> parameter is the ID of the service provider VLAN. Valid range is **1** to **4094**. By default, the s-tag VLAN ID associated with traffic outbound on the EVC is **0**, which indicates that the traffic is untagged. Using the **no** form of this command returns the s-tag VLAN ID value to the default.
(config-evc-DATA)#	**[no] connect men-port efm-group** <*group id*>	Associates the EVC with a specific MEN port (EFM group) so that traffic can flow to the MEN. The <*group id*> is the EFM group ID to which you want to associate the EVC. Valid EFM group ID range is **1** to **1024**. Using the **no** form of this command removes the association between the EVC and the EFM group. Multiple EVCs can be associated with a single EFM group.
(config-evc-DATA)#	**no shutdown**	Enables the EVC.

Table 5. EVC Map Configuration Commands

Prompt	Command	Description
(config)#	**[no] mef evc-map** <*name*>	Creates and names a MEF EVC map and enters the MEF EVC Map Configuration mode. The <*name*> parameter is the name of the EVC map. Using the **no** form of this command removes the EVC map from the unit's configuration.

Table 5. EVC Map Configuration Commands *(Continued)*

Prompt	Command	Description
(config-evc-map-MAP1)#	**[no] match [ce-vlan-id** <*vlan id*> **| ce-vlan-pri** <*value*> **| dscp** <*value*> **| untagged]**	Specifies the traffic matching criteria used by the EVC map to identify which traffic to send to the associated EVC. The **ce-vlan-id** <*vlan id*> parameter specifies that traffic with a CE VLAN ID that matches the specified ID is mapped to the EVC. Valid VLAN ID range is **1** to **4095**. The **ce-vlan-pri** <*value*> parameter specifies that traffic with a CE VLAN PRI value that matches the specified value is mapped to the EVC. The <*value*> parameter is the priority bit associated with the CE VLAN, or the CE VLAN 802.1p value. Valid range is **0** to **7**. The **dscp** <*value*> parameter specifies that traffic matching the specified DSCP value is mapped to the EVC. Valid DSCP value range is **0** to **63**. The **untagged** parameter specifies that untagged traffic is mapped to the EVC. By default, no matching criteria is specified. Using the **no** form of this command removes the matching criteria from the EVC map. Traffic is compared to the first criteria entered in the map's configuration. Subsequent criteria are then compared to the traffic in the order the criteria are entered. Multiple matches form a logical AND.
(config-evc-map-MAP1)#	**[no] connect [evc** <*name*> **| uni mef-ethernet** <*slot/port*>**]**	Associates the EVC map with an EVC component. EVC maps must be associated with both an EVC and a UNI for the map to function properly. The **evc** <*name*> parameter specifies the EVC to which the matching traffic is mapped, and the **uni mef-ethernet** <*slot/port*> parameter specifies the UNI from which the traffic is evaluated. Using the **no** form of this command removes the association between the EVC map and the EVC or the UNI.
(config-evc-map-MAP1)#	**[no] connect discard**	Specifies that traffic matching the EVC map criteria is discarded. Using the **no** form of this command disables traffic discard. By default, no traffic is discarded.

Table 5. EVC Map Configuration Commands *(Continued)*

Prompt	Command	Description
(config-evc-map-MAP1)#	**[no] men-pri [inherit |** <*value*>**]**	Specifies the priority that the EVC will use for traffic that matches the specified EVC map. The **inherit** parameter specifies that the MEN priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. By default, matched traffic has an inherited priority. The <*value*> parameter specifies the priority value. Valid range is **0** to **7**. Using the **no** form of this command returns the MEN priority to the default value.
(config-evc-map-MAP1)#	**[no] men-queue [inherit |** <*value*>**]**	Specifies the output queue used by the EVC for traffic that matches the EVC map. The **inherit** parameter specifies that the queue used is based on the MEN priority-to-queue mapping (specified with the **mef qos cos-map** command) and the MEF QoS settings applied to MEF traffic. By default, matched traffic inherits the queue information. The <*value*> parameter specifies a queue to which the matched traffic is mapped by the EVC. Valid queue range is **1** to **8**. Using the **no** form of this command returns the MEN queue to the default.

Table 6. MEF Policer Policy Configuration Commands

Prompt	Command	Description
(config)#	**[no] mef policer** <*name*>	Creates and names the MEF policer policy, and enters the policy configuration mode. The <*name*> parameter is the name given to this policy. Using the **no** form of this command removes the policy from the unit's configuration.
(config-policer-POLICY1)#	**[no] cir** <*number*>	Specifies the average maximum transmission rate of traffic in kbps allowed before the traffic may be dropped. Valid <*number*> range is **250** to **600000** kbps. By default, the CIR threshold is **600000** kbps. Using the **no** form of this command returns the CIR threshold to the default value.
(config-policer-POLICY1)#	**[no] cbs** <*number*>	Specifies the maximum allowable number of bytes transmitted as a burst before the policer policy may drop the traffic. Valid range is **0** to **2147483647** bytes. By default, the CBS threshold is **0** bytes. Using the **no** form of this command returns the CBS threshold to the default value.
(config-policer-POLICY1)#	**[no] eir** <*number*>	Specifies the allowed maximum transmission rate of traffic, over and above the CIR threshold, before the policer policy drops the traffic. The <*number*> range is **250** to **600000** kbps. By default, the EIR threshold is **600000** kbps. The EIR value must be greater than or equal to the CIR value. Using the **no** form of this command returns the EIR threshold to the default value.
(config-policer-POLICY1)#	**[no] ebs** <*number*>	Specifies the allowed maximum number of bytes transmitted as a burst of data, over and above the CBS threshold, before the policer policy drops the traffic. Valid <*number*> range is **0** to **2147483647** bytes. By default, the EBS threshold is **0** bytes. Using the **no** form of this command returns the EBS threshold to the default value.

Table 6. MEF Policer Policy Configuration Commands *(Continued)*

Prompt	Command	Description
(config-policer-POLICY1)#	**[no] per [custom [add-map** <*name*> **| remove-map** <*name*>**] | evc** <*name*> **| uni mef-ethernet** <*slot/port*>**]**	Applies the MEF policer policy to an EVC component. The **custom** parameter allows you to apply the MEF policer policy to one or more EVC maps. The additional **add-map** and **remove-map** parameters adds or removes the policy from the EVC map, and the <*name*> parameter specifies to which EVC map the policer policy is added or removed. The **evc** parameter allows you to apply the MEF policer policy to an EVC, and the <*name*> parameter specifies to which EVC the policy is applied. When policies are applied to an EVC, they are applied to egress traffic on the EVC. The **uni mef-ethernet** <*slot/port*> parameter allows you to apply the MEF policer policy to egress traffic on the specified MEF Ethernet interface (the UNI) for all connected EVCs. You must specify the slot and port of the MEF Ethernet interface to apply the policer policy. By default, no policies are applied to any EVC components. Using the **no** form of this command removes the policer policy from the EVC component.

Table 7. MEF Ethernet QoS Configuration Commands

Prompt	Command	Description
(config)#	**[no] mef qos cos-map** <*number*> <*value*>	Configures the default mapping of queues to CoS markings. The <*number*> parameter is the queue to which a CoS value is mapped, and the <*value*> parameter is the CoS value. Valid <*number*> range is **1** to **8**, and valid <*value*> range is **0** to **7**. Default queue and priority assignments are outlined in *Table 1 on page 15*. Using the **no** form of this command returns the queue mappings to the default value. The queue assignments configured here are used by the EVC map when the **men-queue** is set to **inherit**.

Table 7. MEF Ethernet QoS Configuration Commands *(Continued)*

Prompt	Command	Description
(config)#	**[no] mef qos untagged** <*value*>	Specifies the MEN priority for untagged traffic on the EVC. The <*value*> parameter is the MEN priority. Valid range is **0** to **7**. By default, a MEN priority of **0** is assigned to untagged traffic. Using the **no** form of this command returns to the default priority for untagged traffic.

Table 8. T-scan Test Commands

Prompt	Command	Description
(config-shdsl 1/1)#	**test tscan**	Initiates a T-scan test.
(config-shdsl 1/1)#	**test tscan display-results**	Displays the results from a T-scan test.
(config-shdsl 1/1)#	**test tscan clear-results**	Clears the results of a previously completed T-scan test.

Table 9. Bad Splice Detection Commands

Prompt	Command	Description
(config-shdsl 1/1)#	**[no] test splice-detect distance-type [feet | meters]**	Specifies the distance measurement type for bad splice detection tests. By default, the measurement is completed in **feet**. Using the **no** form of this command returns the measurement type to the default value.
#	**show interface shdsl** <*slot/port*> **splice-detect 24-hour [**<*interval*>**]**	Displays the bad splice detection test results. The <*slot/port*> parameter is the slot and port of the SHDSL interface for which you want to see the test results. The optional <*interval*> parameter allows you to specify that results from one or more of the previous 24-hour intervals are displayed. Valid interval range is **1** to **7**. You can enter a single interval or multiple intervals when separated by a dash.
#	**clear counters shdsl** <*slot/port*> **splice-detect**	Clears the data for all bad splice detection test intervals. The <*slot/port*> parameter is the slot and port of the SHDSL interface for which you want to clear the test data.

Troubleshooting

Troubleshooting the configuration of the EFM NIM2 or the MEF Ethernet interface can be done by using various **show** and **debug** commands from the CLI. The **show** commands display information about the configuration and state of the EFM NIM2 and various MEF components, and the **debug** commands display information about the functioning of the EFM NIM2 and various MEF components. Both **show** and **debug** commands are entered from the Enable mode prompt. The following sections describe the **show** and **debug** commands available for troubleshooting EFM NIM2 and MEF Ethernet interface configurations.

Show Commands

The **show** commands are used to display current configurations and states of the EFM NIM2, MEF Ethernet interface, and various MEF components. Reviewing the configuration of these items allows you to verify item configurations, as a first step in troubleshooting functionality issues. The **show** commands are entered from the Enable mode prompt. For example, to display information about MEF configurations, you can enter the **show mef** as follows:

```
#show mef
MEN Configured EVCs for efm-group 1:
    2213 3216

EVC DATA: Admin UP Protocol Connected UP

    Connected to MEN Port       efm-group 1
    Connected to EVC Map        DATA

    Tag                         3216
    Preserve CE VLAN            No

EVC DEFAULT: Admin UP Protocol Connected UP

    Connected to MEN Port       efm-group 1
    Connected to EVC Map        DEFAULT

    Tag                         2213
    Preserve CE VLAN            Yes

EVC Map DATA: Admin UP Protocol Connected UP

    Connected to UNI            mef-ethernet 1/1
    Connected to EVC            DATA

    MEN Priority                Inherit
    MEN Queue                   Inherit
```


EVC Map DEFAULT: Admin UP Protocol Connected UP

Connected to UNI	mef-ethernet 1/1
Connected to EVC	DEFAULT
MEN Priority	Inherit
MEN Queue	Inherit

Connection: EVC Map DATA

UNI	mef-ethernet 1/1
EVC	DATA
MEN Port	efm-group 1
Connection Status	Connected UP

Connection: EVC Map DEFAULT

UNI	mef-ethernet 1/1
EVC	DEFAULT
MEN Port	efm-group 1
Connection Status	Connected UP

Table 10 describes the **show** commands available for EFM NIM2 configuration and MEF components in AOS.

Table 10. Show Commands for EFM NIM2/MEF Ethernet Components

Prompt	Command	Description
#	**show mef**	Displays all configuration and state information for MEF components, including EVCs, EVC maps, MEF policer policies, MEF Ethernet interfaces, and their associations.
#	**show mef connections [discard | evc** <*name*> **| evc-map** <*name*> **| men-port efm-group** <*group id*> **| policer** <*name*> **| uni mef-ethernet** <*slot/port*>**]**	Displays the configured connections for a specified EVC, EVC map, EFM group, MEF policer policy, and MEF Ethernet interface. Specify a MEF Ethernet interface using the slot and port of the interface. The **discard** parameter displays connections that have a discard target.
#	**show mef evc-map [**<*name*>**]**	Displays the MEN priority and MEN queue information for EVC maps. You can optionally specify that the information for a single map is displayed by using the <*name*> parameter. If no map is specified, all configured EVC maps are displayed.

Table 10. Show Commands for EFM NIM2/MEF Ethernet Components *(Continued)*

Prompt	Command	Description
#	**show mef evc [**<*name*>**]**	Displays the configuration information for EVCs. This information includes the status, s-tag, and CE VLAN preservation status for each EVC. The EVC maps to which the EVC is connected are also displayed. You can optionally specify that the information for a single EVC is displayed by using the <*name*> parameter. If no EVC is specified, all configured EVCs are displayed.
#	**show mef policer [**<*name*>**]**	Displays the configuration information for MEF policer policies. This information includes the status of the policy, the EVC component to which the policy is applied, and the CIR, CBS, EIR, and EBS thresholds for the policy. You can optionally specify that the information for a single MEF policer policy is displayed using the <*name*> parameter. If no MEF policer policy is specified, information for all configured MEF policer policies is displayed.
#	**show running-config mef [**<*verbose*>**]**	Displays the configuration information for all configured MEF components. The optional <*verbose*> parameter specifies that more detailed information about each component is displayed.
#	**show running-config interface mef-ethernet [**<*slot/port*> **|** <*slot/port.subinterface*>**] [**<*verbose*>**]**	Displays the configuration information for a specified MEF Ethernet interface or subinterface. The optional <*verbose*> parameter specifies that more detailed information about the interface is displayed.
#	**show running-config interface efm-group** <*group id*> **[**<*verbose*>**]**	Displays the configuration information for a specified EFM group. The optional <*verbose*> parameter specifies that more detailed information about the EFM group is displayed.
#	**show interfaces efm-group all [connections]**	Displays the status information for all EFM groups. The optional **connections** parameter specifies that statistics for interfaces connected to the EFM group are displayed.

Table 10. Show Commands for EFM NIM2/MEF Ethernet Components *(Continued)*

Prompt	Command	Description
#	**show interfaces efm-group** <*group id*> **[connections] [interval [15-minute** <*value*> **| 24-hour** <*value*>**]]**	Displays statistics for a specific EFM group. Valid <*group id*> range is **1** to **1024**. The optional **connections** parameter specifies that statistics for interfaces connected to the EFM group are displayed. The optional **interval** parameter specifies that statistics are displayed for either a 15-minute or 24-hour period (using the appropriate keyword). The <*value*> parameter specifies which 15-minute period in the last 24 hours or which 24-hour period in the last seven days is displayed. Valid range for a 15-minute period is **1** to **96**; valid range for a 24-hour period is **1** to **7**.

Debug Commands

The **debug** commands are used to alert you when changes happen in the configuration of the EFM NIM2, MEF Ethernet interface, or MEF components. The messages generated by the **debug** command can reveal possible problems in configuration and traffic flow between the various MEF components. All **debug** commands are issued from the Enable mode prompt. For example, to enable debug messaging for MEF configuration, enter the **debug mef config** command as follows:

#debug mef config

Turning on a large amount of debug information can adversely affect the performance of your unit.

Table 11 describes the **debug** commands associated with EFM NIM2 and MEF Ethernet interface configurations.

Table 11. Debug Commands EFM NIM2/MEF Ethernet Components

Prompt	Command	Description
#	**debug mef config [detail]**	Enables debug messaging for MEF configurations. The optional **detail** parameters specifies that more detailed information is displayed.
#	**debug efm config**	Enables debug messaging for EFM configuration.
#	**debug interface shdsl**	Enables debug messaging for SHDSL interfaces.
#	**debug efm oam**	Displays subtended host information received from the Total Access 5000 when using pre-provisioning.

