6AOSCG0055-29G
June 2015

ADTRAN

Configuration Guide

Carrier Ethernet Services in AOS

This configuration guide describes the configuration steps for Layer 2 and Layer 3 networking using carrier Ethernet in ADTRAN Operating System (AOS) products. This configuration guide includes an overview of Ethernet in the first mile (EFM) and Metro Ethernet Forum (MEF) terminology and the configuration, application, and troubleshooting steps for using carrier Ethernet technologies on customer-edge equipment.

This guide contains the following sections:

AOS Carrier Ethernet Services Overview

In AOS release R10.10.0, a new line of converged access router products was introduced to provide communication between customer networks (private local area networks (LANs)), and the service provider's Metro Ethernet Network (MEN) using both Layer 2 (the data link layer) and Layer 3 (the networking layer) of the Open Systems Interconnect (OSI) networking model. These products function as remote devices that provide Layer 2 and Layer 3 business services over the MEN, with carrier-grade Ethernet services in addition to Internet Protocol version 4 (IPv4) and IPv6 routing functions, firewall capabilities, and Quality of Service (QoS). These AOS products function as the demarcation point between the service provider's network and the customer network using Ethernet connections in a point-to-point configuration, or an E-Line configuration as defined by the MEF.

The router capable of carrier Ethernet connects to the MEN using the Gigabit Ethernet or EFM group interfaces, functioning as the network-to-network interface (NNI), and forms a demarcation point between the customer LAN and the MEN. The MEN is accessed using one or more Ethernet virtual connections (EVCs), which are associated with EFM group or Gigabit Ethernet interfaces. In addition, EVC maps, policers, and shapers are used to control the flow of traffic. *Figure 1* illustrates the placement of the AOS product within the MEN structure.

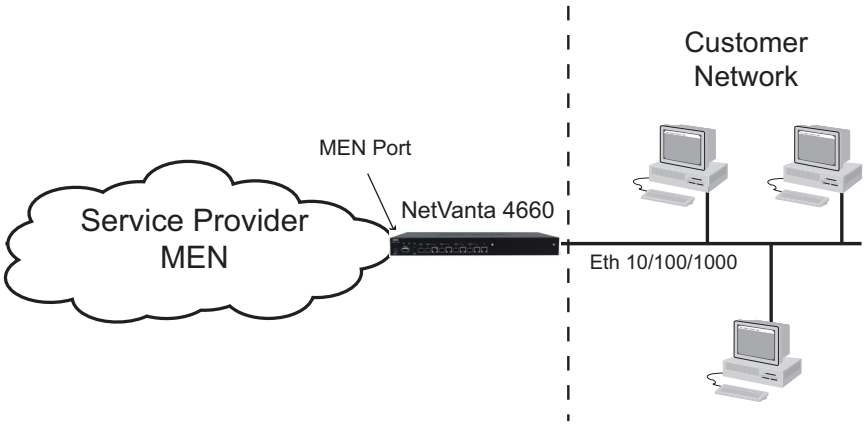

Figure 1. AOS Products and the MEN

MEF Components within the AOS Product

This configuration guide focuses on the configuration of MEN components in customer-side AOS router products. These components include the EFM group or Gigabit Ethernet interface as the MEN port, the EVC, the EVC map, policer, shaper, and interface queues. These components can be used for both Layer 2 and Layer 3 services through the user network interface (UNI) and across the MEN. Details of each of these components, and its function in the AOS product, are described in the following sections.

MEN Port

A MEN port is the interface that is connected to the MEN. This port can be a Gigabit Ethernet interface, or an EFM group. Typically, EFM groups are used when the AOS product is using a module for MEN connection (such as a VDSL or SHDSL module).

The EFM group is a logical Ethernet interface that represents an EFM bonding group. Physical interfaces are connected to the EFM group and provide physical links to carry bonded traffic. These groups are used in Layer 2/Layer 3 connections to the MEN. The EFM group can operate as the MEN port for the AOS product.

Both Gigabit Ethernet and EFM groups can be used for either Layer 2 or Layer 3 connections to the MEN. When configuring Layer 2 parameters, configuration is done in the parent interface. When configuring Layer 3 parameters, configuration is done in the subinterface.

EVC

An EVC connects a local UNI endpoint with a remote NNI endpoint and passes Ethernet service frames through these endpoints. The EVCs prevent data transfer between subscriber sites that are not part of the same EVC, providing data privacy and security similar to a Frame Relay or asynchronous transfer mode (ATM) permanent virtual circuit (PVC). EVCs are configured to connect to the MEN port, whether that port is an EFM group or a Gigabit Ethernet interface.

Each EVC has an associated service tag (s-tag), which is the service provider's VLAN ID and the outer tag in Q-in-Q VLAN tagging, whose VLAN ID is unique among other EVCs in the MEN (and the AOS product). 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 edge (CE) VLAN ID can be preserved on EVC traffic across the MEN, if necessary. The CE VLAN ID is the VLAN ID of the Ethernet frames received on the UNI interface.

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, the EVC must be associated with a UNI for traffic to flow.

System Management EVC

The system management EVC is a specialized EVC that provides an in-band IP network interface for system management and control. It allows local IP address information to be provisioned, and it configures the underlying AOS hardware to forward packets to the CPU for local IP stack processing. By default, the system management EVC resides in a named virtual routing and forwarding (VRF) instance, the system-management VRF, although that can be changed by the user if desired. The system management EVC is the only interface included in this VRF by default. This EVC can be used to access the unit and monitor or troubleshoot any functional issues.

System Control EVC

The system control EVC is a second specialized EVC that can be used for various purposes. It provides a method for separating session control interfaces from other customer services. The system control EVC can use Ethernet or Point-to-Point over Ethernet (PPPoE) encapsulation. Unlike the system management EVC, the system control EVC resides in the default VRF by default, although typically it should be placed in its own unique VRF to isolate its traffic.

Policer

A policer is a bandwidth-limiting profile that limits the amount of inbound traffic into the AOS product from the UNI. This component is commonly used to limit Layer 2 traffic in the UNI-to-MEN direction, but it can also be applied to Layer 3 traffic on Ethernet subinterfaces on both the UNI or MEN ports. The amount of traffic can be limited per EVC, UNI, interface, or EVC map 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 bandwidth usage is too great, and how to mark or drop traffic based on the configured thresholds.

Policers can be applied in one of the following ways:

- Ingress bandwidth policer per ingress UNI
- Ingress bandwidth policer per EVC
- Ingress bandwidth policer per EVC map
- Ingress bandwidth policer per Ethernet subinterface

In typical applications, the bandwidth available on the EVC is less than the bandwidth available at the UNI port. Bandwidth bottleneck is typically in the UNI-to-MEN direction; therefore, all bandwidth policers are applied only for traffic conducted in the UNI-to-MEN direction. Policers are not applied to the traffic conducted in the MEN-to-UNI direction.

The configurable attributes of the EVC policer 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.). Policer configuration is detailed in the *Carrier Ethernet Services QoS* configuration guide, available online at https://supportforums.adtran.com.

EVC Map

An EVC map is a traffic filter that matches traffic based on specific criteria and associates the traffic with a specific EVC. This component is used in Layer 2 configurations only. Each map is associated with a single EVC and UNI, and may include the customer VLAN ID and class of service (CoS) behavior of the traffic. Maps are used to classify traffic from a UNI for forwarding, and provides the mechanism for VLAN tag manipulation and forwarding.

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

Shaper

A traffic shaper is used to rate limit and smooth bursts of traffic traveling between the AOS product and the MEN. Shapers can be used for both Layer 2 and Layer 3 transmissions. When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens, the packet is delayed until there are enough tokens to allow transmission. Shapers do not drop frames with a small burst of traffic, but they can add latency.

The configurable attributes of the shaper include specifying to which interface or queue(s) the shaper is applied and the traffic rate. Shaper configuration is detailed in the *Carrier Ethernet Services QoS* configuration guide, available online at https://supportforums.adtran.com.

Interface Queues

Each interface, whether an EFM group or Gigabit Ethernet interface, provides eight hardware queues for traffic management and congestion avoidance. Queues are used for both Layer 2 and Layer 3 traffic. These queues absorb packets when the ingress rate of traffic exceeds the egress rate, allowing bursts of packets to be transmitted through the system without incurring loss. The individual queues can be used in strict priority or weighted fair queueing (WFQ) configurations to allow the desired traffic prioritization.

Queues must be managed to prevent packet loss and delay along the network. Configurable attributes of the queue include specifying the queue congestion management algorithm, CoS settings, drop probabilities, queue depth, thresholds, and the weight of the queue (when using WFQ) for traffic traversing the MEN port interface.

Queue configuration is detailed in the *Carrier Ethernet Services QoS* configuration guide, available online at https://supportforums.adtran.com.

Component Interaction for Carrier Ethernet Services

Within the AOS product, the multiple components work together to provide traffic flow to the MEN. The following sections describe the interaction between these components and packet flows for both Layer 2 and Layer 3 carrier Ethernet services.

General Layer 2 Packet Flow (UNI-to-MEN, MEN-to-UNI)

Packet flows for services over the MEN travel in both directions: from the UNI to the MEN, and from the MEN to the UNI. *Figure 2 on page 5* illustrates the Layer 2 traffic flow pattern through the AOS product.

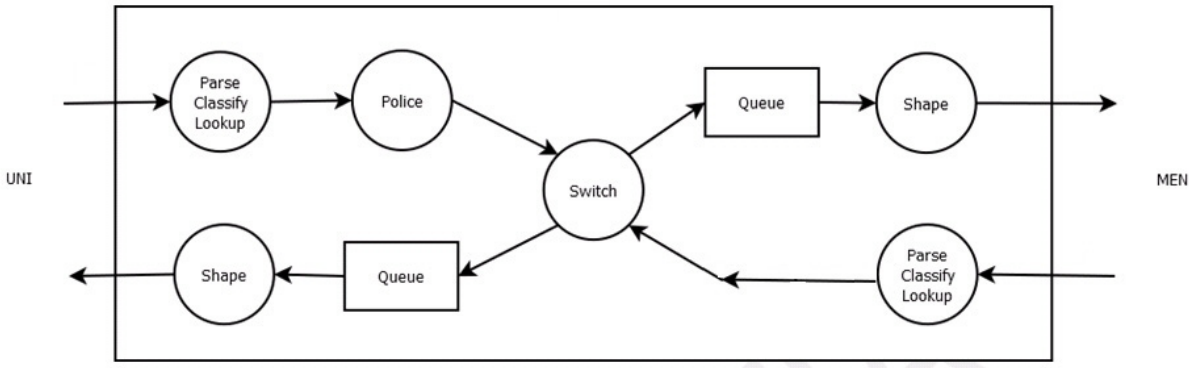

Figure 2. Packet Flow Across the AOS Product

In traffic flowing from the UNI to the MEN, Ethernet frames are either untagged or tagged with a CE VLAN. If the packet matches an EVC map, it is then forwarded though the configured MEN port. If the packet does not match an EVC map, it is discarded. If CE VLAN preservation is enabled, as it is by default, then the s-tag and c-tag (optional) are added to the outgoing Ethernet frame. If CE VLAN preservation is disabled, then the customer CE VLAN tag is stripped and then the s-tag and c-tag (optional) are added to the outgoing Ethernet frame.

In traffic flowing from the MEN to the UNI, Ethernet frames have an s-tag, but may also have a c-tag and CE VLAN tag. If the packet matches the EVC, then it is forwarded through to the UNI port associated with the EVC maps that connect to the matched EVC. Once the packet has matched an EVC, the s-tag and c-tag (if present) are stripped from the Ethernet frame. If CE VLAN preservation is disabled, then the CE VLAN for the EVC map connected to the matching EVC is added to the packet and the packet is sent out the UNI. If CE VLAN preservation is enabled, as it is by default, then the packet is forwarded out the UNI with no changes.

VRFs and AOS Carrier Ethernet Services

VRF instances are configurable items used to isolate Layer 3 traffic within the AOS product. For carrier Ethernet routers, two pre-configured VRFs exist by default: the unnamed, default VRF (of which every IP interface and service are a part unless otherwise specified in configuration), and the system management VRF, of which the system management EVC is a part. The system control EVC can be placed in its own user-configured VRF to isolate its traffic. For more information about the configuration and use of VRFs, refer to the *Configuring Multi-VRF* configuration guide, available online at https://supportforums.adtran.com.

Hardware and Software Requirements and Limitations

Layer 2 and Layer 3 carrier Ethernet services are only available on AOS platforms running AOS firmware R10.10.0 or later as outlined in the *AOS Product Feature Matrix*, available online at http://supportforums.adtran.com.

As of AOS firmware release R10.11.0, a transparent mode for AOS carrier Ethernet services is available. Refer to *AOS Carrier Ethernet Services in Transparent Mode on page 28* for more information.

As of AOS firmware release R11.1.0, shapers can be configured on a per-queue basis and operations, administration, and management (OAM) pre-provisioning can be configured on Layer 2 interfaces.

As of AOS firmware release R11.4.0, the EFM group can automatically detect if a link is EFM bonded or EFM non-bonded. The AOS device can detect the link type during training with the Digital Subscriber Line Access Multiplexer (DSLAM) and automatically set the bonding mode to match the service offering.

In AOS firmware release R11.5.0, the ETREE, Ethernet local management interface (E-LMI), MAC address filtering, and EtherType filtering features were added.

In AOS firmware release R11.6.0, support for matching multiple VLANs to a single EVC map was added. This feature is available on Gigabit Ethernet ports configured as UNIs on carrier products as outlined in the *AOS Product Feature Matrix*, available online at http://supportforums.adtran.com. E-LMI was also enhanced to reflect applicable Y.1731 defects and configured bandwidth defects. In addition, the ability to change the type of acceptable tag protocol identifiers (TPIDs) for Ethernet frames on the EVC and EVC map was added.

In AOS firmware release R11.7.0, support for specifying the maximum transmission unit (MTU) for the Layer 2 user network interface (UNI) was added. This feature is available only on the Gigabit Ethernet interface.

Rules for Provisioning EVCs, EVC Maps, Policers, Shapers, and Queues

To ensure valid provisioning, the rules below are enforced for EVCs, EVC maps, and policers. In most cases, the value of the status attribute for an entity provides a brief description of the condition.

1. An EVC, EVC map, policer, or shaper is applied only if the respective EVC or interface is running.
2. Two EVC maps are considered to be duplicate if they both have the same UNI port, CE VLAN ID, and overlapping ranges for CE VLAN priority, DSCP value, or untagged/priority-tagged frames.
3. Two EVCs are considered to be duplicate if they both have the same value for the s-tag attribute.
4. Two policers are considered to be duplicate if they both have the same mode, UNI, and EVC attributes.
5. No two EVCs can have the same name.
6. No EVC maps can have the same name.
7. No two policers can have the same name.
8. No two shapers can have the same name.
9. If the network element is managed through a VLAN on a designated EFM group or Ethernet port to which the system management EVC is connected as a MEN port, the following applies:
   - Any EVC connected to the same MEN port with an s-tag VLAN ID (VID) value equal to the management VID value is invalid.
   - If there are no EVCs connected to the MEN port, then any EVC map connected to the same port as a UNI is invalid.
   - If a port is connected to the system management EVC as a UNI, it cannot be used by any EVCs or EVC maps.
10. If the CE VLAN ID preservation attribute of an EVC is disabled, all of the associated EVC maps must have the same CE VLAN ID attribute value.
11. When multiple EVC maps are applied to a common EVC, each EVC map must have the same UNI. Multiple UNIs cannot be mapped to a common EVC.
12. If two EVC maps have the same UNI, only one of the EVC maps can be provisioned to allow untagged and priority tagged frames.
13. No one Ethernet frame can be governed by more than one policer.
14. When two or more EVC maps have overlapping criteria, and an incoming packet matches two or more of the criteria for the EVC maps, the EVC map that has provisioning options of higher precedence is used to forward traffic. EVC map order of precedence is outlined in *Table 1 on page 7*.

Table 1. EVC Map Traffic Forwarding Order of Precedence

Precedence	Provisioning Options
1	Traffic type + Untagged + DSCP + UNI port
2	Traffic type + Untagged + UNI port
3	Traffic type + P-bit + CE VLAN ID + UNI port
4	Traffic type + P-bit + UNI port
5	Traffic type + DSCP + CE VLAN ID + UNI port

Table 1. EVC Map Traffic Forwarding Order of Precedence *(Continued)*

Precedence	Provisioning Options
6	Traffic type + DSCP + UNI port
7	Traffic type + CE VLAN ID + UNI port
8	Traffic type + UNI port
9	EtherType + DSCP + UNI Port
10	Untagged + EtherType + DSCP + UNI port
11	Untagged + EtherType + DSCP + UNI port
12	Untagged + DSCP + UNI port
13	Untagged + UNI port
14	CE VLAN ID + DSCP + UNI port
15	CE VLAN ID + P-bit + UNI port
16	EtherType + DSCP + UNI port
17	CE VLAN ID + EtherType + UNI port
18	CE VLAN ID + UNI port
19	DSCP + UNI port
20	P-bit + UNI port
21	EtherType + UNI port
22	UNI port

Additional Specifications

In addition to the provisioning rules outlined above, the following are a few specifications to keep in mind when configuring the AOS product for Layer 2/Layer 3 carrier Ethernet services:

1. The CE VLAN ID does not support the native VLAN option. Instead, an **untagged** option is supported. When configured, all untagged and priority tagged (VLAN 0) packets are identified with a particular interface.
2. For Layer 3 MEN connections, a new EVC must be created in order to specify which EVC (s-tag) is used by the subinterface. The EVC's connected MEN port must match the parent interface for the Layer 3 interface in order for the interface to become active. The new EVC must be created if the parent interface is an NNI, and each NNI subinterface must use a unique EVC. If the parent interface is a UNI, an EVC is not used.
3. If a subinterface is configured on a UNI port, then it only requires a CE VLAN ID to be specified before it can become active. The port is considered a UNI if it has not been connected to any EVCs. If it is later connected to an EVC, then the EVC must be created for the subinterface to be active.

4. If a subinterface is configured on a NNI port for Layer 3 services, then it must specify either a CE VLAN ID, or the untagged CE VLAN option, and it must be connected to an EVC.
5. Ethernet and EFM group interfaces are permanently in 802.1q encapsulation mode on AOS carrier Ethernet products.

Layer 2/Layer 3 Carrier Ethernet Configuration Overview

To configure Layer 2 and Layer 3 carrier Ethernet services on the AOS product, you will need to complete the following tasks:

1. *Accessing the AOS Product Using the CLI on page 9*.
2. *Configuring Common Carrier Ethernet Components on page 10*.
3. *Configuring Layer 2 Carrier Ethernet Components on page 14*.
4. *Configuring Layer 3 Carrier Ethernet Components on page 23*.

Accessing the AOS Product Using the CLI

To begin configuring the carrier Ethernet services on the AOS product, 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**.

> NOTE *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.

> NOTE *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 carrier Ethernet features.

Configuring Common Carrier Ethernet Components

Carrier Ethernet services in AOS include both Layer 2 and Layer 3 components. Some components are Layer 2 specific, others are Layer 3 specific, and some are common to both Layer 2 and Layer 3 services. The following sections describe the carrier Ethernet components used by both Layer 2 and Layer 3 services, including:

- *Configuring the MEN Port on page 10*
- *Configuring the EVC on page 12*

Configuring the MEN Port

The first step in configuring the carrier Ethernet features on an AOS product is to configure the MEN port. The MEN port is the connection to the MEN, and can be either a Gigabit Ethernet interface or an EFM group. Gigabit Ethernet interfaces are used as the MEN port when no modules are used in the AOS product, and EFM groups are used as the MEN port when modules (such as the VDSL or SHDSL modules) are used. Both can be used simultaneously if desired. When using Layer 2 services, the Gigabit Ethernet interface or the EFM group interface only need to be enabled, and have links added in the case of the EFM group. When using Layer 3 services, the Gigabit Ethernet subinterface or the EFM group subinterface must also be configured with a CE VLAN ID, a connected EVC, and an IP address.

Configuring the Gigabit Ethernet Interface as the MEN Port

To configure the Gigabit Ethernet interface as a MEN port, you must first enable the interface. If you are going to use Layer 3 services through the Gigabit Ethernet interface, you must also configure a Gigabit Ethernet subinterface with a CE VLAN ID, an EVC, and an IP address. To configure the Gigabit Ethernet interface as the MEN port, follow these steps:

1. Create the Gigabit Ethernet interface using the **interface gigabit-ethernet** <*slot/port*> command from the Global Configuration mode. Specify the slot and port for the interface. Enter the command as follows:

   (config)**#interface gigabit-ethernet 0/1**
   (config-giga-eth 0/1)#

2. For Layer 2 MEN traffic, you only need to enable the interface using the **no shutdown** command from the interface's configuration mode as follows:

   (config-giga-eth 0/1)**#no shutdown**
   (config-giga-eth 0/1)#

The Gigabit Ethernet interface is now configured as a MEN port for Layer 2 services (refer to *Configure the Gigabit Ethernet Subinterface for Layer 3 Services (Optional) on page 23* for Layer 3 service configuration). You can choose to optionally configure an EFM group as a MEN port, or continue with the carrier Ethernet services configuration.

Configuring the EFM Group as a MEN Port

An EFM group can also be configured to the be the MEN port. 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.

Create the EFM Group and Associate Interfaces

EFM groups are created using the **interface efm-group** <*slot/group*> command from the Global Configuration mode. The <*slot/group*> parameter is the unique numerical identifier for the EFM group and its slot. The slot parameter is the slot in which the bonded interface resides. Valid group range is **1** to **1024**. For example, to create EFM group **1/1**, enter the command as follows:

```
(config)#interface efm-group 1/1
(config-efm-group 1/1)#
```

Once the EFM group is created, you enter the EFM group's configuration mode. In this mode, interfaces are associated with the EFM group using the **link** <*slot/port*> command. Specify an interface in the format <*slot/port*>. Available interfaces for the EFM group include SHDSL, VDSL, T1, and E1 interfaces. The following example connects the SHDSL interface **1/1** to EFM group **1/1**:

```
(config)#interface efm-group 1/1
(config-efm-group 1/1)#link 1/1
```

Use the **link** command to associate the interfaces you require to the appropriate EFM group.

> *Interfaces that will be connected to the EFM group must be enabled. Enable the interface by entering the **no shutdown** command from the interface's configuration mode.*

Specify the EFM Group Bonding Mode (Optional)

Once the EFM group is created, you can optionally specify the bonding mode used by the group. The EFM group bonding mode can be set to automatically detect the advertised mode received from the DSLAM during the initial handshake, in which case the AOS device automatically detects if the link is bonded or non-bonded, and the EFM group's bonding mode is automatically set to match the service offering. Alternatively, the EFM bonding mode can be set to use only bonded links for passing traffic. This is the default behavior.

When EFM bonding is set to auto detect, the link type of the first link to train is used and its service type determines the service mode used for the EFM group. The service can be either bonded or non-bonded, depending on the type of link that connected first. Once a link is connected, the service mode is set, and the EFM group must be toggled between the UP and DOWN states to switch between service modes. Only one non-bonded link is supported at a time. If a second non-bonded link is connected, it is not used for passing traffic even though it is physically UP. If a bonded link connects first, any other bonded link from the candidate list is added to bonded service and also forwards traffic.

Use the **bonding [auto-detect | forced-on]** command to specify the service mode (bonded or automatically detected) used by the EFM group. By default, the EFM group uses bonded service only (**forced-on**). The **auto-detect** parameter specifies that the EFM group automatically matches the service type of the first connected link, whether bonded or non-bonded. Use the **no** form of this command to return the bonding type to the default value. To change the EFM group bonding type, enter the command from the EFM group interface as follows:

```
(config)#interface efm-group 1/1
(config-efm-group 1/1)#bonding auto-detect
```


Enable 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 1/1)#no shutdown
```

Specify the EFM Group XCV Thresholds and Interface Link Removal (Optional)

Once you have created the EFM group and associated the appropriate interfaces with it, you can optionally specify the excessive code violation (XCV) 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's configuration mode. 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's 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's configuration mode as follows:

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

For thresholds to be enforced, you must enable link removal in the EFM group's 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 1/1)#xcv-link-removal
```

After configuring the Gigabit Ethernet interface and the EFM group, you have created the MEN port and can begin configuring the other carrier Ethernet services.

Configuring the EVC

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

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

   ```
   (config)#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 EVC's configuration mode. The <*vlan id*> parameter is the ID of the service provider's VLAN. Valid range is

2 to **4094**. By default, no s-tag is configured. 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 EVC's configuration mode. The CE VLAN ID is the VLAN ID on the UNI interface. Preserving the CE VLAN ID is enabled by default. Use the **no** form of this command to disable CE VLAN ID preservation in traffic through the EVC. 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 disabled once it is configured. To enable the EVC, enter the **no shutdown** command from the EVC's configuration mode. For example, to enable the EVC, 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 using the **connect men-port [efm-group** <*slot/group*> | **gigabit-ethernet** <*slot/port*>**]** from the EVC's configuration mode. The <*slot/group*> parameter is the ID of the EFM group to which you want to associate this EVC. Enter the slot and group number. You can alternatively associate the Gigabit Ethernet interface with this EVC by entering the slot and port of the Gigabit Ethernet interface. Use the **no** form of this command to remove the association between this EVC and the specified interface. Multiple EVCs can be associated with a single interface. The EFM group must be created before associating the EVC to an EFM group. For example, to associate EVC **DATA** with the EFM group **1/1**, enter the command as follows:

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

The EVC is now configured. You can configure the parameters of the system control and system management EVCs in the same manner, although there are additional commands for IP and MEN priority settings for these EVCs. The system control EVC also has additional commands for encapsulation and PPPoE. Access the system control EVC by entering the **system-control-evc** command at the Global Configuration mode prompt as follows:

```
(config)#system-control-evc
(config-sys-ctrl-evc)#
```

Access the system management EVC by entering the **system-management-evc** command from the Global Configuration mode prompt as follows:

```
(config)#system-management-evc
(config-sys-mgmt-evc)#
```

The available configuration commands for the system management and system control EVCs are outlined in the *AOS Command Reference Guide*, available online at https://supportforums.adtran.com.

Configuring Layer 2 Carrier Ethernet Components

Carrier Ethernet services in AOS include both Layer 2 and Layer 3 components. Some components are Layer 2 specific, others are Layer 3 specific, and some are common to both Layer 2 and Layer 3 features. The following sections describe the carrier Ethernet components used only by Layer 2 services, including:

Configuring the EVC Map

For Layer 2 carrier Ethernet services, you can configure an EVC map that will match traffic to a specified EVC. Each EVC map is associated with a single EVC, and can match traffic to an EVC based on the traffic's category of destination MAC address (for example, broadcast, multicast, unicast, or L2CP), 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 interface from which you want to map the traffic. 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, in which case you need a connection to a UNI and a connection to the discard target.

After configuring the EVC map and associating it with an EVC, you can optionally specify 802.1p values for the s-tag and c-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 **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 AOS product's configuration. For example, to create an EVC map called **MAP1** and enter the EVC map's configuration mode, enter the command as follows:

   ```
   (config)#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 [broadcast | ce-vlan-id** <*vlan id*> **| ce-vlan-pri** <*value*> **| dscp** <*value*> **| l2cp| multicast | unicast | untagged]** from the EVC map's configuration mode. The **l2cp**, **broadcast**, **multicast**, and **unicast** parameters specify the type of destination MAC address to be mapped to the associated EVC. The **ce-vlan-id** <*vlan id*> parameter specifies that traffic with a matching CE VLAN ID is mapped to the EVC. VLAN IDs can be a single ID, multiple IDs, or a range of IDs. Multiple

VLAN IDs should be separated with a comma (**600,200,800**). A range can be specified with a hyphen (**400-500**). The valid VLAN ID range is **1** to **4094**.

> NOTE *Identical VLAN bundles (a set of multiple VLAN IDs) can exist on two or more EVC maps, provided there is at least one additional match criteria that allows the EVC maps to become active. Different VLAN bundles that overlap on two EVC maps on the same UNI are not allowed and will prevent both EVC maps from becoming active. For example, one EVC map with VLAN IDs 201-400 conflicts with another EVC map with VLAN IDs 301-500 if they are on the same UNI since VLAN IDs 301-400 are overlapping in both VLAN bundles.*

The **ce-vlan-pri** <*value*> parameter specifies that traffic with a matching CE VLAN PRI value is mapped to the 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 IPv4 and IPv6 traffic matching the specified DSCP value is mapped to the EVC. Valid 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. 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)#
```

> NOTE *A common misconfiguration is to forget that Address Resolution Protocol (ARP) is not IPv4 traffic and thus create an EVC map to match IPv4 traffic with a certain DSCP value to send over an EVC without also adding a map that sends ARP over the same EVC. Without ARP to resolve the initial MAC address to IPv4 address binding, no IPv4 traffic can be sent.*

You can also specify an EtherType filter to use as matching criteria on the EVC map. EtherType filters allow you to specify a certain EtherType (such as Address Resolution Protocol (ARP) or Internet Protocol version 6 (IPv6)) as EVC map matching criteria for allowed traffic into the UNI interface. This feature can also be configured to drop certain EtherTypes by associating an EVC map with a discard type, rather than a valid EVC. To specify EtherType matching on the EVC map, enter the **match ethertype** <*value*> command from the EVC map's configuration mode. The <*value*> parameter is the hexadecimal value to use as an additional match criteria for the EVC map. Enter the command as follows:

```
(config-evc-map MAP1)#match ethertype 0x0806
(config-evc-map MAP1)#
```

You can also specify a MAC address to use as matching criteria on the EVC map. To specify destination MAC address matching on the EVC map, enter the **match destination mac address** <*mac address*> command from the EVC map's configuration mode. The <*mac address*> parameter is the MAC address to match. Express MAC addresses in the HH:HH:HH:HH:HH:HH (for example, **08:00:69:02:06:CB**). Enter the command as follows:


```
(config-evc-map MAP1)#match destination mac address 00:A0:C8:00:00:01
(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 (Gigabit Ethernet interface or EFM group) to specify the traffic source from which it is evaluated (UNI) and where it is to be mapped if it matches the criteria (EVC). EVC maps are associated with a UNI and an EVC using the **connect [evc** <*name*> **| uni gigabit-ethernet** <*slot/port*> **| uni efm-group** <*slot/group*>**]** command. Both an EVC and a UNI 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 gigabit-ethernet** <*slot/port*> and **uni efm-group** <*slot/group*> parameters specify 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 UNI Gigabit Ethernet interface **0/1** and with EVC **DATA**, enter the command from the EVC map's configuration mode as follows:

   ```
   (config-evc-map MAP1)#connect uni gigabit-ethernet 0/1
   (config-evc-map MAP1)#connect evc DATA
   (config-evc-map MAP1)#
   ```

   Alternatively, you can use the **connect discard** command instead of the **connect evc** 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 EVC map's configuration mode as follows:

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

4. To enable the EVC map, enter the **no shutdown** command from the EVC map's configuration mode as follows:

   ```
   (config-evc-map MAP1)#no shutdown
   (config-evc-map MAP1)#
   ```

Specify 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 s-tag priority bit (802.1p value), specifying the queue to which the traffic is sent, specifying a c-tag, and specifying the c-tag priority. To configure the MEN values for the matched traffic, follow these steps:

1. You can optionally specify the s-tag priority bits (802.1p value) that the EVC will use for traffic matching the specific EVC map by entering the **men-pri [inherit |** <*value*>**]** command from the EVC map's configuration mode prompt. The **inherit** parameter specifies that the 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 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 an s-tag 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 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 EVC map's configuration mode. The **inherit** parameter specifies that the queue used by the EVC for the matched traffic is based on the default global p-bit-to-queue mapping (based on the priority bits (802.1p) of the s-tag). 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 **0** to **7**. 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)#
   ```

3. You can optionally specify the c-tag to be inserted and that will be used to identify traffic on the EVC for a specific customer using the **men-c-tag** <*value*> command from the EVC map's configuration mode. When traffic matches the EVC map, it will be tagged with this c-tag value. The <*value*> parameter is the c-tag value. Valid range is **2** to **4094**. By default, the c-tag is not specified. Using the **no** form of this command removes the c-tag value.
   For example, to specify that traffic matching EVC map **MAP1** is tagged with a c-tag value of **20**, enter the command as follows:

   ```
   (config-evc-map MAP1)#men-c-tag 20
   (config-evc-map MAP1)#
   ```

4. You can optionally specify the c-tag priority bits that the EVC will use on the c-tag using the **men-c-tag-pri [inherit |** <*value*>**]** command from the EVC map's configuration mode. The **inherit** parameter specifies that the c-tag 802.1p value for the matched traffic is inherited from the 802.1p value of the s-tag. By default, matched traffic has an inherited priority. The <*value*> parameter specifies the priority value given to the matched traffic in the EVC. Valid range is **0** to **7**. Using the **no** form of this command returns the MEN c-tag priority to the default value. For example, to specify the c-tag priority as **6** for traffic matching EVC map **MAP1**, enter the command as follows:

   ```
   (config-evc-map MAP1)#men-c-tag-pri 6
   (config-evc-map MAP1)#
   ```

Specifying Accepted TPIDs for Ethernet Frames Received on the UNI (Optional)

In AOS firmware release R11.6.0, the capability to define accepted tag protocol identifiers (TPIDs) for Ethernet frames received on a UNI was added to the EVC map. This feature allows you to specify that TPIDs other than 0x8100, are accepted on the UNI interface that is matching on VLAN ID or priority. For example, you can now specify that frames with a TIPID of 0x88a8 are accepted. To configure the accepted TPID, you can set the value globally, using the **ethernet ce-vlan-tpid** <*value*> command from the Global Configuration mode. You can override the global setting to return to the default value of 0x8100 on a per-map basis using the **no ce-vlan-tpid** command from the EVC map's configuration mode.

If the TPID is configured using the global command, all EVC maps will default to the globally-specified TPID for CE VLAN ID matching. All EVC maps will also default to using the specified TPID for adding CE VLAN IDs to traffic flowing in the MEN to UNI direction when the CE VLAN ID is not preserved as well as using the specified TPID for adding c-tags to traffic flowing in the UNI to MEN direction. By default, no special global handling of TPIDs is configured, and EVC maps accept and process packets with a CE VLAN TIPID of 0x8100. Using the **ethernet ce-vlan-tpid** <*value*> command allows you to specify

that other TPIDs, such as 0x88a8 or 0x9100 are accepted. The <*value*> parameter of this command specifies the hexadecimal value of the TPID to accept, for example, **0x88a8**. Using the **no** form of this command returns the accepted TPID to 0x8100. To configure the accepted CE VLAN TPID globally, enter the command as follows:

```
(config)#ethernet ce-vlan-tpid 0x88a8
```

When the global TPID is configured, all EVC maps automatically use the global setting for matching packets based on CE VLAN ID. You can use the **no ce-vlan-tpid** command from the EVC map's configuration mode to specify that the particular EVC map does not use the global setting, but instead uses TPID 0x8100 for the TPID or added c-tag. Entering the command as **ce-vlan-tpid** from the EVC map's configuration mode specifies that the map uses the global TPID setting, and is the default behavior.

To specify the EVC map does not use the globally accepted TPID, enter the command as follows:

```
(config)#evc-map MAP1
(config-evc-map MAP1)#no ce-vlan-tpid
```

The configuration of the accepted TPIDs can impact traffic flowing from both the UNI to the MEN or the MEN to the UNI. Traffic flowing from the UNI to the MEN can be impacted if one or more of the following statements is in the EVC map: **match ce-vlan-id** or **match ce-vlan-pri**. In addition, if the **no preserve ce-vlan-id** is configured on the EVC, MEN to UNI traffic can be impacted. Traffic flowing from the MEN to the UNI can also be impacted if the **men-c-tag** <*value*> command has been issued in the EVC map.

*Adding EVC maps with different TPID configurations to an EVC can cause the maps to not function if the **men-c-tag** <value> command has been configured.*

Enable ETREE on the EVC Map (Optional)

ETREE is a rooted multipoint EVC network configuration that provides traffic separation between users of UNI interfaces. In this configuration, each UNI is either a root or leaf, and traffic can flow from root to leaf, leaf to root, or root to root, but not between leaves. To achieve this type of traffic separation, ingressing UNI traffic is blocked on the EVC map that connects the UNI to a leaf UNI using the **block uni ingress-only** command in the EVC map's configuration. By default, this feature is disabled. Using the **no** form of this command disables the feature. To enable ETREE on the EVC map, enter the command as follows:

```
(config-evc-map MAP1)#block uni ingress-only
(config-evc-map MAP1)#
```

The EVC map is now configured.

Configuring OAM Pre-Provisioning

In some network configurations, system-management EVC s-tag and IP information can be pre-provisioned in another ADTRAN product and pushed to the current unit using link OAM as soon as an active link is added to the EFM group or Gigabit Ethernet interface. This configuration can include the s-tag, IP address and subnet mask, and the default route.

To enable subtended host listener mode, enter the **subtended-host mode listener** command from the EFM group or Gigabit Ethernet Interface Configuration mode prompt. For example, enter the command as follows:

```
(config)#interface gigabit-ethernet 0/1
(config-giga-eth 0/1)#subtended-host mode listener
```

By default, the Gigabit Ethernet 0/1 and EFM group 1/1 interfaces have pre-provisioning listening enabled. All other interfaces have pre-provisioning disabled.

If you are not using OAM pre-provisioning, you should disable subtended host mode on the EFM group or Gigabit Ethernet interface. In some ADTRAN product system releases, if subtended host provisioning is not configured, invalid provisioning information can be sent. To disable subtended host mode, enter the **subtended-host mode disabled** command from the EFM group or Gigabit Ethernet Interface Configuration mode prompt.

For example, enter the command as follows:

```
(config)#interface gigabit-ethernet 0/1
(config-giga-eth 0/1)#subtended-host mode disabled
```

Configuring E-LMI

Ethernet local management interface (E-LMI) is a feature used by AOS to provide UNI and EVC status information to the CE device. Status information gathered from the AOS device is exchanged with the CE device using E-LMI messages. E-LMI is used to report the status of one or more EVCs on the UNI. Each EVC can be in one and only one of the following states:

- NOT ACTIVE, indicating that the EVC cannot transfer traffic on any of the UNIs in the EVC. The EVC might be administratively down, a Y.1731 defect might be present, or a configured bandwidth requirement might not be satisfied.
- ACTIVE, indicating that the EVC is capable of passing traffic on all UNIs in the EVC.
- PARTIALLY ACTIVE, indicating that the EVC cannot pass traffic on some of the UNIs in the EVC. This status is only relevant in E-LAN or E-TREE mode.

Additionally, the EVC might be reported as NEW when it has been configured for the first time. Status information can be viewed using the **show** and **debug** commands associated with the E-LMI feature (refer to *Troubleshooting Commands for E-LMI on page 43*).

E-LMI and Y.1731

In AOS firmware release R11.6.0, E-LMI was enhanced to reflect applicable Y.1731 defects and configured bandwidth defects. When reporting UNI and EVC status information, E-LMI takes into account Y.1731 alarms and conditions such as loss of continuity (LOC) and remote defect indication (RDI) conditions. LOC occurs when a MEP stops receiving continuity check messages (CCMs) from a remote MEP, and the remote MEP is considered DOWN. Once a MEP detects a LOC condition, it transmits RDI upstream to indicate that a line failure exists downstream. In Y.1731, maintenance entity groups (MEGs) are represented by a service tag (s-tag), which corresponds to an EVC. The MEPs can be attached to the MEN or UNI interface, and correspond to that EVC. If Y.1731 indicates no LOC or RDI conditions exist on all MEPs, the MEG/EVC status is ACTIVE, and if the MEG/EVC shows RDI or LOC conditions on all MEPs, the MEG/EVC status is NOT ACTIVE.

E-LMI and Bandwidth Monitoring

An interface bandwidth threshold can be specified as a criteria for EVC status, as well. If the interface's bandwidth drops below the specified threshold, E-LMI will indicate a change in the status of the EVC. E-LMI will indicate that the EVC is NOT ACTIVE if the bandwidth threshold for the specified interface does not meet the configured bandwidth threshold. For example, if a MEN has a bandwidth threshold of 8 kbps and the bandwidth on the interface drops to 5 kbps, E-LMI will indicate that the EVC is NOT ACTIVE.

To configure E-LMI functionality on the AOS device, follow these steps:

1. Enable the E-LMI feature on the UNI interface using the **ethernet lmi** command from the interface's configuration mode. By default, this feature is disabled. When enabled, the feature is in PE mode by default. Using the **no** form of this command disables the E-LMI feature. To enable E-LMI, enter the command as follows:

   (config)**#interface gigabit-ethernet 0/2**
   (config-giga-eth 0/2)**#ethernet lmi**

2. Configure the E-LMI polling timer using the **ethernet lmi t392 [**<*value*> **| 0]** command from the Global Configuration mode. When enabled, the AOS device expects a STATUS ENQUIRY message to be received with in the interval specified by t392. If it is not received from the CE within the interval specified, a status inquiry time out error will be logged. The <*value*> parameter is the time, in seconds, for the polling verification timer. Valid range is **5** to **30** seconds, and by default is set to **15** seconds. Entering **0** disables the polling timer. Using the **no** form of this command returns the polling timer to the default value. To configure the E-LMI polling timer, enter the command as follows:

   (config)**#ethernet lmi t392 20**

3. Configure the E-LMI operational polling status counter using the **ethernet lmi n393** <*value*> command from the Global Configuration mode. The n393 counter is used to determine if E-LMI is operational or not. The unit is deemed not operational if n393 polling verification time outs occur. It will not be deemed operational again until n393 valid status inquiries are received within the polling time. Valid range is **2** to **10**, with a default value of **4**. Using the **no** form of this command returns the counter to the default value. Enter the command as follows:

   (config)**#ethernet lmi n393 7**

4. Configure E-LMI to monitor the bandwidth of a MEN interface to determine the status of the EVC using the **ethernet lmi interface** <*interface*> **bandwidth-threshold [downspeed** <*value*> **| upspeed** <*value*>**]** command from the interface's configuration mode. If the bandwidth of the interface drops below the specified amount, E-LMI will indicate that the EVC status is NOT ACTIVE. The <*interface*> parameter specifies the interface to monitor. Specify an interface in the format **interface type** <*slot/port*>. The **downspeed** <*value*> parameter specifies the bandwidth threshold for traffic moving from the MEN to the UNI. The **upspeed** <*value*> parameter specifies the bandwidth threshold for traffic moving from the UNI to the MEN. Valid range is **0** to **4294967295** kbps for both **downspeed** and **upspeed** parameters. Use the **no** form of this command to disable the feature. Enter the command as follows:

   (config)**#interface eth 0/2**
   (config-eth 0/2)**#ethernet lmi interface efm-group 1/1 bandwidth-threshold downspeed 128**

Configuring MAC Address Filtering

Media access control (MAC) address filtering can be used on a UNI interface when a known hardware address or range of addresses is expected from a UNI port and any other addresses not allowed should be dropped. MAC address filtering uses a MAC hardware access control list (ACL) to specify the allowed MAC addresses. In addition to MAC ACLs, a MAC address learn limit can be used as a rudimentary security measure for UNI ports which are expected to only ever learn a certain number of known MAC addresses. Both MAC filtering abilities prevent additional, potentially rogue, addresses from being forwarded from the interface. MAC hardware ACLs and MAC address limits are both applied to a physical port and can be used simultaneously.

Configuring MAC Hardware ACLs

MAC hardware ACLs are configured using the **mac hw-access-list standard** <*name*>command from the Global Configuration mode. The <*name*> parameter is the name of the MAC ACL. By default, no MAC ACLs exist. Use the **no** form of this command to remove the MAC ACL from the unit's configuration. This command creates the MAC ACL and enters the ACL's configuration mode. Enter the command as follows:

```
(config)#mac hw-access-list standard ALLOWADTRAN
(config-std-mac-acl)#
```

Once you have entered the Standard MAC ACL Configuration mode, you can specify the MAC addresses to be allowed or denied on the interface. To allow a MAC address, use the **permit mac** <*source*> command. To deny a MAC address, use the **deny mac** <*source*> command. The <*source*> parameter specifies the source used for frame matching. Sources can be expressed in one of three ways:

- Using the keyword **any** to match any MAC address.
- Using **address** <*mac address*> to specify a single host address. MAC addresses should be expressed in the format HH:HH:HH:HH:HH:HH (for example, **08:00:69:02:06:CB**).
- Using the <*mac address*> <*wildcard mask*> format to match all MAC addresses in a range. The wildcard mask corresponds to a range of MAC addresses or a specific host. Wildcard masks are expressed in the format HH:HH:HH:HH:HH:HH (for example, **00:00:00:FF:FF:FF**)

Multiple addresses can be permitted or denied in the ACL. To remove an address, use the **no** form of the appropriate command. To allow a MAC address, enter the command from the ACL's configuration mode as follows:

```
(config-std-mac-acl)# permit mac 00:A0:C8:00:00:01
(config-std-mac-acl)#
```

To allow a MAC address using wildcards, enter the command as follows:

```
(config-std-mac-acl)#permit mac 00:A0:C8:00:00:01 00:00:00:FF:FF:FF
(config-std-mac-acl)#
```

To deny a MAC address, enter the command as follows:

```
(config-std-mac-acl)#deny mac 00:A0:C8:00:00:01
(config-std-mac-acl)#
```

To deny a MAC address using wildcards, enter the command as follows:

```
(config-std-mac-acl)#deny mac 00:A0:C8:00:00:01 00:00:00:FF:FF:FF
(config-std-mac-acl)#
```


Once the MAC ACL has been created, apply it to the UNI interface using the **mac access-group** <*mac acl name*> command from the interface's configuration mode. Use the **no** form of this command to remove the ACL from the interface. When applied, these ACLs provide source MAC address filtering on the interface. To apply a MAC ACL to a UNI interface, enter the command as follows:

```
(config)#interface gigabit-ethernet 0/2
(config-giga-eth 0/2)#mac access-group ALLOWADTRAN
```

Configuring MAC Address Limits

MAC address limits specify the maximum number of MAC addresses to be learned on the interface. This limit pulls from a global pool of 1024 learnable MAC addresses. In addition, when MAC limits are enabled on an interface with a MAC ACL applied, addresses are learned that match the ACL up to the specified limit. The maximum number of MAC addresses allowed is **1024**. MAC address limits are specified on the interface using the **mac limit** <*value*> command. Value range is **1** to **1024**. By default, no MAC address limit is specified. Use the **no** form of this command to disable MAC address limits. Enter the command from the interface's configuration mode as follows:

```
(config)#interface gigabit-ethernet 0/2
(config-giga-eth 0/2)#mac limit 800
```

Configuring MAC Address Aging Time

The MAC address aging time specifies the time, in seconds, that a MAC address is considered valid. The MAC address aging time is specified using the **mac aging-time** <*value*> command from the interface's configuration mode. The <*value*> parameter is the aging time in seconds. Valid range is **0** to **3600** seconds. By default, the MAC address aging time is set to **300** seconds. A value of **0** forces learn and lock behavior. Use the **no** form of this command to return to the default value. To change the MAC address aging time, enter the command as follows from the interface's configuration mode:

```
(config)#interface gigabit-ethernet 0/2
(config-giga-eth 0/2)#mac aging-time 600
```

Specifying the MTU for Layer 2 UNI (Optional)

You can optionally specify the MTU for the Layer 2 UNI using the **mtu** <*size*> **include-l2-header** command from the Gigabit Ethernet interface configuration mode. This MTU size includes the Layer 2 header, any associated tags, and the Layer 2 payload, but not the frame check sequence (FCS). Valid <*size*> range is **60** to **9242** bytes, and by default is configured to be **9242** bytes. Use the **no** form of this command to return to the default value. To change the MTU on the Layer 2 interface, enter the command as follows from the interface's configuration mode:

```
(config)#interface gigabit-ethernet 0/2
(config-giga-eth 0/2)#mtu 4400 include-l2-header
```

This command specifies the MTU for Layer 2 interfaces only. If the Layer 2 MTU is configured to be below the MTU for the Layer 3 interface, a misconfiguration occurs and as a result, traffic can be lost. To avoid a misconfiguration, a warning is displayed whenever the Layer 2 MTU is configured below 1526 bytes.

Configuring Layer 3 Carrier Ethernet Components

Carrier Ethernet services in AOS include both Layer 2 and Layer 3 components. Some components are Layer 2 specific, others are Layer 3 specific, and some are common to both Layer 2 and Layer 3 features. The following sections describe the carrier Ethernet components used only by Layer 3 services, including:

Configure the Gigabit Ethernet Subinterface for Layer 3 Services (Optional)

The following steps configure the Gigabit Ethernet subinterface for Layer 3 services.

1. Configure a Gigabit Ethernet subinterface using the **interface gigabit-ethernet** <*slot/port.subinterface id*> command from the Global Configuration mode. Enter the command as follows:

   (config)**#interface gigabit-ethernet 0/1.123**
   (config-giga-eth 0/1.123)#

2. Specify the CE VLAN ID as **untagged** for the Gigabit Ethernet subinterface using the **ce-vlan-id untagged** command from the subinterface's configuration mode. If you want there to be a CE VLAN tag, you can specify that value instead. Enter the command as follows:

   (config-giga-eth 0/1.123)**#ce-vlan-id untagged**
   (config-giga-eth 0/1.123)#

3. Specify the EVC that is connected to the Gigabit Ethernet subinterface using the **connect evc** <*name*> command from the subinterface's configuration mode. The <*name*> parameter is the name of the EVC that will be connected to the Gigabit Ethernet subinterface. Enter the command as follows:

   (config-giga-eth 0/1.123)**#connect evc EVC1**
   (config-giga-eth 0/1.123)#

4. Specify the IP address of the Gigabit Ethernet subinterface using the **ip address** <*ip address*> <*subnet mask*> command. Enter IP addresses in dotted decimal notation, for example, **10.10.10.1**. To specify the IP address of the Gigabit Ethernet subinterface, enter the command as follows:

   (config-giga-eth 0/1.123)**#ip address 198.51.100.2 255.255.255.252**
   (config-giga-eth 0/1.123)#

   

   *You can optionally specify an IPv6 address for the Gigabit Ethernet subinterface using the **ipv6 address** command.*

5. Enable the Gigabit Ethernet subinterface using the **no shutdown** command from the subinterface's configuration mode as follows:

   (config-giga-eth 0/1.123)**#no shutdown**
   (config-giga-eth 0/1.123)#

Configure the EFM Group Subinterface for Layer 3 Services (Optional)

Just as the Gigabit Ethernet subinterface must be configured for Layer 3 services across the MEN, the EFM group subinterface must be configured in the same manner. The subinterface must be created, assigned a CE VLAN ID, connected with an EVC, and given an IP address. This configuration uses the same commands as the Gigabit Ethernet subinterface, but are executed from the EFM group subinterface's configuration mode.

The example below creates the EFM group subinterface and applies the minimal configuration for Layer 3 services across the MEN:

(config)**#interface efm-group 1/1.123**
(config-efm-group 1/1.123)**#ce-vlan-id untagged**
(config-efm-group 1/1.123)**#connect evc EVC2**
(config-efm-group 1/1.123)**#ip address 198.51.100.5 255.255.255.252**
(config-efm-group 1/1.123)**#no shutdown**

Configure Additional Subinterface Settings (Optional)

The following commands can be used to configure additional settings on the Layer 3 subinterface.

1. Use the **egress-queue [inherit |** <*value*>**]** command to specify the queue for traffic egressing the subinterface. The **inherit** parameter specifies that the PCP of the traffic's outer tag is used to automatically map traffic to the egress queue on a per-packet basis using the QoS CoS map settings. The <*value*> parameter specifies an egress queue for the subinterface. Valid range is **0** to **7**. By default, egress queue mapping is set to **inherit**. Using the **no** form of this command returns the egress queue to the default value. To change the egress queue for the subinterface, enter the command from the subinterface's configuration mode as follows:

   (config)**#interface gigabit-ethernet 0/1.123**
   (config-giga-eth 0/1.123)**#egress-queue 5**

2. Use the **men-pri [inherit |** <*value*>**]** command to specify the s-tag priority bits (802.1p value) for traffic egressing the subinterface. The **inherit** parameter specifies that the priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. The <*value*> parameter specifies an s-tag priority value. Valid range is **0** to **7**. By default, the s-tag priority value is set to **inherit**. Using the **no** form of this command returns the s-tag priority value to the default setting. To change the s-tag priority on the subinterface, enter the command from the subinterface's configuration mode as follows:

   (config-giga-eth 0/1.123)**#men-pri 5**

3. Use the **men-c-tag** <*value*> parameter to specify the c-tag to be inserted into subinterface traffic. Valid c-tag <*value*> range is **2** to **4094**. By default, c-tags are not inserted into subinterface traffic. Using the **no** form of this command returns to the default setting. To specify a c-tag for the subinterface, enter the command from the subinterface's configuration mode as follows:

   (config-giga-eth 0/1.123)**#men-c-tag 20**

4. Use the **men-c-tag-pri [inherit |** <*value*>**]** command to specify the c-tag priority bits (802.1p value) for matching traffic on the subinterface. The **inherit** parameter specifies that the c-tag priority is inherited from the 802.1p value of the s-tag. The <*value*> parameter specifies a c-tag priority value. Valid range is **0** to **7**. By default, the c-tag priority value is set to **inherit**. Using the **no** form of this

command returns the c-tag priority value to the default setting. To change the c-tag priority on the subinterface, enter the command from the subinterface's configuration mode as follows:

(config-giga-eth 0/1.123)**#men-c-tag-pri 6**

AOS Carrier Ethernet Services Configuration Examples

The following sections describe typical Layer 2 and Layer 3 carrier Ethernet services configurations on the AOS product. The first example is a configuration for Layer 2 services across the MEN, and the second example is a configuration for Layer 3 services across the MEN. Both Layer 2 and Layer 3 services can be simultaneously configured on the same AOS product, as shown in *Example 3: Combined Layer 2 and Layer 3 Carrier Ethernet Configuration on page 26*.

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.

Example 1: Layer 2 Carrier Ethernet Configuration

The following configuration provides Layer 2 services across the MEN. In this configuration example, two Gigabit Ethernet interfaces are configured: one as the MEN port (Gigabit Ethernet **0/1**) and one as the UNI (Gigabit Ethernet **0/2**). An EVC is created (**L2_DATA**) which is connected to the MEN port, with an attached EVC map.

```
!
interface gigabit-ethernet 0/1
    description NNI
    no shutdown
!
interface gigabit-eth 0/2
    description UNI
    no shutdown
!
evc L2_DATA
    s-tag 2256
    connect men-port gigabit-ethernet 0/1
    no shutdown
!
evc-map L2_DATA
    match untagged
    connect uni gigabit-ethernet 0/2
    connect evc L2_DATA
    no shutdown
!
```


Example 2: Layer 3 Carrier Ethernet Configuration

The following configuration provides Layer 3 services across the MEN. In this configuration example, a Gigabit Ethernet interface and subinterface are configured as the MEN port (Gigabit Ethernet **0/1** and Gigabit Ethernet **0/1.2156**), and Gigabit Ethernet interface and subinterface are configured as the UNI (Gigabit Ethernet **0/3** and Gigabit Ethernet **0/3.1**). An EVC is created (**L3_DATA**) which is connected to the MEN port.

```
!
interface gigabit-ethernet 0/1
    description NNI
    no shutdown
!
interface gigabit-ethernet 0/1.2156
    description L3_DATA NNI
    ce-vlan-id untagged
    connect evc L3_DATA
    ip address 198.51.100.1 255.255.255.252
    ipv6
    ipv6 address 2001:DB8:2::1/64
    no shutdown
!
interface gigabit-ethernet 0/3
    description UNI
    no shutdown
!
interface gigabit-ethernet 0/3.1
    description L3_DATA UNI
    ce-vlan-id untagged
    ip address 192.0.2.1 255.255.255.252
    ipv6
    ipv6 address 2001:DB8:1::1/64
    no shutdown
!
evc L3_DATA
    s-tag 2156
    connect men-port gigabit-ethernet 0/1
    no shutdown
```

Example 3: Combined Layer 2 and Layer 3 Carrier Ethernet Configuration

The following configuration provides advanced combined Layer 2 and Layer 3 carrier Ethernet services in the AOS product. Included in the configuration example are the system management EVC and the system control EVC with PPPoE encapsulation.

```
!
qos map L3_DATA 10
    match dscp af31
    set men-pri 3
```



```
    set egress-queue 3
!
interface gigabit-ethernet 0/1
    description NNI
    no shutdown
!
interface gigabit-ethernet 0/1.2156
    description L3_DATA NNI
    ce-vlan-id untagged
    connect evc L3_DATA
    ip address 198.51.100.1 255.255.255.252
    ipv6
    ipv6 address 2001:DB8:2::1/64
    qos-policy out L3_DATA
    no shutdown
!
interface gigabit-eth 0/2
    description UNI
    no shutdown
!
interface gigabit-ethernet 0/2.100
    description L3_DATA UNI
    ce-vlan-id 100
    ip address 192.0.2.1 255.255.255.252
    ipv6
    ipv6 address 2001:DB8:1::1/64
    no shutdown
!
evc L2_DATA
    s-tag 2256
    connect men-port gigabit-ethernet 0/1
    no shutdown
!
evc L3_DATA
    s-tag 2156
    connect men-port gigabit-ethernet 0/1
    no shutdown
!
evc-map L2_DATA
    match ce-vlan-id 200
    connect uni gigabit-ethernet 0/2
    connect evc L2_DATA
    no shutdown
!
system-management-evc
    connect men-port gigabit-ethernet 0/1
    vrf forwarding system-management
```



```
    ip address 203.0.113.2 255.255.255.0
    ipv6
    ipv6 address 2001:DB8:3::2/64
    ipv6 mode host unicast
    s-tag 2056
    no shutdown
!
system-control-evc
    connect men-port gigabit-ethernet 0/1
    encap pppoe
    vrf forwarding system-control
    no ip address
    ipv6
    ipv6 address autoconfig default
    ipv6 mode host unicast
    ppp chap hostname pppoe
    ppp chap password pppoe
    s-tag 3208
    no shutdown
```

AOS Carrier Ethernet Services in Transparent Mode

AOS carrier Ethernet routers support a Layer 2 transparent mode, a configuration in which subscribers can manage their own packet network domain independently of carrier network services. Transparent mode allows carrier services to be configured so that subscriber data frames and data streams are minimally impacted by carrier networks, and so that associated management and control traffic between subscriber routers and switches are not affected by carrier network configurations.

The UNI configured for use with transparent mode accepts any CE VLAN ID, meaning it does not discard any CE VLAN ID. It supports a single point-to-point EVC, and can map all CE VLAN IDs to an EVC or no CE VLAN IDs to an EVC. This feature allows the customer service to be temporarily disconnected without impacting the EVC.

The following Layer 2 protocols are passed to the EVC when in transparent mode:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- All LANs bridge management group block of protocol
- Generic Attribute Registration Protocol (GARP)
- Link Aggregation Control Protocol (LACP)
- Marker protocol
- Authentication (802.1x)

In addition, the transparent mode UNI can discard 802.3x PAUSE frames, can support point-to-point EVCs, CE VLAN ID preservation, CE VLAN CoS preservation, and can unconditionally tunnel unicast, multicast, and broadcast service frames (except 802.3x PAUSE frames).

Configuring Transparent Mode

The following configuration examples accomplish transparent mode forwarding. The first example is the configuration of a MEF UNI Type 1.1 interface, and the second example is the configuration of two UNI ports without the addition of an s-tag.

MEF UNI Type 1.1 Configuration

In this example, a MEF UNI Type 1.1 is configured, where the Gigabit Ethernet 0/1 interface is the MEN port, and Gigabit Ethernet 0/2 is the UNI port. In this example, all traffic except certain Layer 2 protocols that ingress the UNI port are forwarded out the MEN port with the EVC's s-tag added to the Ethernet frame. Traffic matching the EVC's s-tag that ingress the MEN port will have the s-tag stripped off and the resultant Ethernet frame is forwarded out the UNI port. The EVC map forces all matching traffic into the same queue, and therefore the packets arrive at the remote device in the same order that they are received on the UNI port. Although not included in this example, ingress bandwidth profiles can be used with a policer and egress bandwidth profiles can be used with a shaper.

The configuration of a MEF UNI Type 1.1 is as follows:

```
interface gigabit-ethernet 0/1
    no shutdown
!
interface gigabit-ethernet 0/2
    no shutdown
!
evc EVC
    connect men gigabit-ethernet 0/1
    s-tag 100
    no shutdown
!
evc-map MAP
    connect uni gigabit-ethernet 0/2
    connect evc EVC
    men-queue 0
    no shutdown
!
```

UNI to UNI Configuration

This example is the configuration of two UNI ports, which is used in scenarios in which it is not desirable to add an s-tag. In this example, all traffic except certain Layer 2 control protocols that ingress one UNI port are forwarded out the other UNI port. The EVC maps in this example force all matching traffic into the same queue, forcing packets to leave the egress port in the same order that they were received on the ingress UNI port. Although not configured in this example, ingress bandwidth profiles can be implemented with a policer and egress bandwidth profiles can be implemented with a shaper.

The configuration of the two UNIs is as follows:

```
interface gigabit-ethernet 0/1
    no shutdown
!
```



```
interface gigabit-ethernet 0/2
    no shutdown
!
evc EVC
    s-tag 100
    no shutdown
!
evc-map MAP1
    connect uni gigabit-ethernet 0/1
    connect evc EVC
    men-queue 0
    no shutdown
!
evc-map MAP2
    connect uni gigabit-ethernet 0/2
    connect evc EVC
    men-queue 0
    no shutdown
!
```

AOS Carrier Ethernet Service Command Summary

The following tables summarize the commands associated with configuring and using carrier Ethernet Layer 2 and Layer 3 services on the AOS product.

Common Carrier Ethernet Service Components Commands

The following tables summarize the commands common to both Layer 2 and Layer 3 carrier Ethernet configurations.

Table 2. MEN Port Configuration Commands

Prompt	Command	Description
(config)#	**[no] interface [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]**	Creates a MEN port by configuring an EFM group or a Gigabit Ethernet interface and enters the interface's configuration mode. Using the **no** form of this command on an EFM group removes it from the unit's configuration.
(config-giga-eth 0/1)# OR (config-efm-group 1/1)#	**no shutdown**	Enables the interface for processing.

Table 2. MEN Port Configuration Commands *(Continued)*

Prompt	Command	Description
(config-efm-group 1/1)#	**[no] link** <*slot/port*>	Adds a link or range of links to an EFM group. Enter links in the <*slot/port*> or <*slot/<port to port*> format, for example, **1/1** or **1/1-4**. By default, EFM groups do not contain any links. Use the **no** form of this command to remove the link.
(config-efm-group 1/1)#	**[no] bonding [auto-detect | forced-on]**	Specifies whether the EFM group uses bonded links only (**forced-on**) or automatically detects whether the link is bonded or non-bonded and uses that service type (**auto-detect**). By default, the EFM group uses bonded links only. Use the **no** form of this command to return to the default value.
(config-efm-group 1/1)#	**[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 1/1)#	**[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.

Table 3. EVC Configuration Commands

Prompt	Command	Description
(config)#	**[no] evc** <*name*>	Creates an EVC and enters the EVC's configuration mode. Using the **no** form of this command removes the EVC from the unit's configuration.
(config)#	**system-control-evc**	Enters the system control EVC's configuration mode.
(config)#	**system-management-evc**	Enters the system management EVC's configuration mode.

Table 3. EVC Configuration Commands *(Continued)*

Prompt	Command	Description
(config-evc DATA)#	**[no] s-tag** <*vlan id*>	Specifies the service provider's <*vlan id*> used by the EVC. Valid range is **2** to **4094**. By default, the s-tag is unspecified which prevents the EVC from becoming active. Using the **no** form of this command returns the s-tag VLAN ID value to the default.
(config-evc DATA)#	**[no] preserve-ce-vlan**	Specifies that the CE VLAN ID 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.
(config-evc DATA)#	**[no] connect men-port [efm-group** <*slot/group*> | **gigabit-ethernet** <*slot/port*>**]**	Associates the EVC with a specific MEN port so that traffic can flow to the MEN. The <*slot/group*> is the slot number and group ID to which you want to associate the EVC. Using the **no** form of this command removes the association between the EVC and the MEN port interface.
(config-evc DATA)#	**no shutdown**	Enables the EVC.

Layer 2 Carrier Ethernet Component Commands

The following tables summarize commands specific to Layer 2 carrier Ethernet configurations.

Table 4. EVC Map Configuration Commands

Prompt	Command	Description
(config)#	**[no] evc-map** <*name*>	Creates and names a EVC map and enters the EVC map's 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 4. EVC Map Configuration Commands *(Continued)*

Prompt	Command	Description
(config-evc-map MAP1)#	**[no] match [broadcast | ce-vlan-id** <*vlan id*> **| ce-vlan-pri** <*value*> **| dscp** <*value*> **| l2cp | multicast | unicast | untagged]**	Specifies the traffic matching criteria used by the EVC map to identify which traffic to send to the associated EVC. The **L2CP**, **broadcast**, **multicast**, and **unicast** parameters specify that traffic matching the respective type is mapped to the 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. VLAN IDs can be a single ID, multiple IDs, or a range of IDs. Multiple VLAN IDs should be separated with a comma (**600,200,800**). A range can be specified with a hyphen (**400-500**).Valid VLAN ID range is **1** to **4094**. 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 value associated with the CE VLAN, or the CE VLAN 802.1p value. Valid range is **0** to **7**. The **dscp** <*value*> parameter specifies that IPv4 and IPv6 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, all traffic on the connected UNI port is matched. Using the **no** form of this command removes the matching criteria from the EVC map. Multiple matches form a logical AND.
(config-evc-map MAP1)#	**[no] match ethertype** <*value*>	Specifies traffic matching the specific EtherType is forwarded to the associated EVC. The <*value*> parameter is the hexadecimal value of the EtherType (for example, ARP is **0x0806**). EtherType matching is disabled by default. Using the **no** form of this command removes the matching criteria from the EVC map.

Table 4. EVC Map Configuration Commands *(Continued)*

Prompt	Command	Description
(config-evc-map MAP1)#	**[no] match destination mac address** <*mac address*>	Specifies a destination MAC address to use for matching on the EVC map. Express MAC addresses in the format HH:HH:HH:HH:HH:HH (for example, **00:A0:C8:00:00:01**). Use the **no** form of this command to remove the MAC address matching criteria from the EVC map.
(config-evc-map MAP1)#	**[no] connect [evc** <*name*> **| discard]**	Associates the EVC map with an EVC. EVC maps must be associated with both an EVC (or **discard** target) and a UNI for the map to function properly. The **evc** <*name*> parameter specifies the EVC to which the matching traffic is mapped. The **discard** parameter specifies that traffic matching the EVC map criteria is discarded. Using the **no** form of this command removes the association between the EVC map and the EVC or discard target.
(config-evc-map MAP1)#	**[no] connect uni [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]**	Associates the EVC map with an EVC component. EVC maps must be associated with both an EVC (or **discard** target) and a UNI for the map to function properly. The **uni efm-group** <*slot/group*> and **uni gigabit-ethernet** <*slot/port*> parameters specify the UNI from which the traffic is evaluated. Using the **no** form of this command removes the association between the EVC map and the UNI.
(config-evc-map MAP1)#	**[no] men-pri [inherit |** <*value*>**]**	Specifies the 802.1p value to the service VLAN tag (s-tag) that the EVC will use for traffic that matches the specified EVC map. The **inherit** parameter specifies that the s-tag 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.

Table 4. EVC Map Configuration Commands *(Continued)*

Prompt	Command	Description
(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. 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 **0** to **7**. Using the **no** form of this command returns the MEN queue to the default.
(config-evc-map MAP1)#	**[no] men-c-tag** <*value*>	Specifies the c-tag that is inserted on the matching packets as they leave the MEN port and is used to further identify traffic on the EVC. Valid <*value*> range is **2** to **4094**. By default, a c-tag is not specified.
(config-evc-map MAP1)#	**[no] men-c-tag-pri [inherit |** <*value*>**]**	Specifies the 802.1p value in the c-tag. The **inherit** parameter specifies that the c-tag 802.1p value for the matched traffic is inherited from the 802.1p value of the s-tag. The <*value*> parameter assigns a specific priority value to the c-tag. Valid range is **0** to **7**. By default, the c-tag priority is set to **inherit**. This setting has no effect if the **men-c-tag** is not specified.
(config-evc-map MAP1)#	**[no] block uni ingress-only**	Enables ETREE on the EVC map. The **no** form of this command disables the feature. By default, ETREE is disabled.
(config-evc-map MAP1)#	**no shutdown**	Enables the EVC map.

Table 5. Accepted EtherType Configuration Commands

Prompt	Command	Description
(config)#	**[no] ethernet ce-vlan-tpid** <*value*>	Specifies the globally accepted TPID for packets traversing the UNI interface. The <*value*> parameter is a hexadecimal value that defines the accepted TPID, for example, **0x88a8**. By default, no global TPID setting exists and only **0x8100** TPID is accepted. The **no** form of this command returns to the default value. When this command is issued, all EVC maps use this TPID setting.

Table 5. Accepted EtherType Configuration Commands

Prompt	Command	Description
(config-evc-map MAP1)#	**[no] ce-vlan-tpid**	Specifies that the EVC map uses the globally defined CE VLAN TPID value. This behavior is enabled by default. The **no** form of this command specifies that the EVC map does not use the global setting.

Table 6. Layer 2 OAM Pre-Provisioning Configuration Commands

Prompt	Command	Description
(config-giga-eth 0/1)#	**subtended-host mode listener**	Enables OAM pre-provisioning for the interface. By default, the Gigabit Ethernet 0/1 and EFM group 1/1 interfaces have pre-provisioning enabled. This feature can be configured on either EFM group or Gigabit Ethernet interfaces.
(config-giga-eth 0/1)#	**subtended-host mode disabled**	Disables OAM pre-provisioning for the interface.

Table 7. E-LMI Configuration Commands

Prompt	Command	Description
(config-giga-eth 0/2)#	**[no] ethernet lmi**	Enables E-LMI on the interface. Use the **no** form of this command to disable the feature.
(config)#	**[no] ethernet lmi t392 [**<*value*> **| 0]**	Configures the E-LMI polling verification timer. The <*value*> parameter is the timer value in seconds. Valid range is **5** to **30** seconds. By default, the value is **15** seconds. Specifying a timer value of **0** disables the timer. Use the **no** form of this command to return to the default value.
(config)#	**[no] ethernet lmi n393** <*value*>	Configures the E-LMI operational polling status counter. Valid range is **2** to **10**. Default value is **4**. Use the **no** form of this command to return to the default counter value.

Table 7. E-LMI Configuration Commands *(Continued)*

Prompt	Command	Description
(config)#	**[no] ethernet lmi interface** <*interface*> **bandwidth-threshold [downspeed** <*value*> **| upspeed** <*value*>**]**	Configures E-LMI to monitor the bandwidth of an interface to determine the status of the EVC. If the bandwidth of the interface drops below the specified amount, E-LMI will indicate that the EVC status is NOT ACTIVE. The <*interface*> parameter specifies the interface to monitor. The **downspeed** <*value*> parameter specifies the bandwidth threshold for traffic moving from the MEN to the UNI. The **upspeed** <*value*> parameter specifies the bandwidth threshold for traffic moving from the UNI to the MEN. Valid range is **0** to **4294967295** kbps for both **downspeed** and **upspeed** parameters. Use the **no** form of this command to disable the feature.

Table 8. MAC Address Filtering

Prompt	Command	Description
(config)#	**[no] mac hw-access-list standard** <*name*>	Creates a MAC ACL and enters the ACL's configuration mode. Use the **no** form of this command to remove the ACL from the unit's configuration.

Table 8. MAC Address Filtering *(Continued)*

Prompt	Command	Description
(config-std-mac-acl)#	**[no] permit mac** <*source*>	Specifies a MAC address to allow into the interface. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any MAC address. 2. Using **address** <*mac address*> to specify a single host address. MAC addresses should be expressed in the format HH:HH:HH:HH:HH:HH (for example, **08:00:69:02:06:CB**). 3.Using the <*mac address*> <*wildcard mask*> format to match all MAC addresses in a range. The wildcard mask corresponds to a range of MAC addresses or a specific host. Wildcard masks are expressed in the format HH:HH:HH:HH:HH:HH (for example, **00:00:00:FF:FF:FF**). Use the **no** form of this command to remove the address from the ACL.
(config-std-mac-acl)#	**[no] deny mac** <*source*>	Specifies a MAC address to deny access to the interface. Sources can be expressed in one of three ways: 1. Using the keyword **any** to match any MAC address. 2. Using **address** <*mac address*> to specify a single host address. MAC addresses should be expressed in the format HH:HH:HH:HH:HH:HH (for example, **08:00:69:02:06:CB**). 3.Using the <*mac address*> <*wildcard mask*> format to match all MAC addresses in a range. The wildcard mask corresponds to a range of MAC addresses or a specific host. Wildcard masks are expressed in the format HH:HH:HH:HH:HH:HH (for example, **00:00:00:FF:FF:FF**). Use the **no** form of this command to remove the address from the ACL
(config-giga-eth 0/2)#	**[no] mac access-group** <*acl name*>	Associates a MAC ACL with the UNI interface. Use the **no** form of this command to remove the ACL from the interface.

Table 8. MAC Address Filtering *(Continued)*

Prompt	Command	Description
(config-giga-eth 0/2)#	**[no] mac limit** <*value*>	Specifies the maximum number of MAC addresses to learn on the interface. Valid range is **1** to **1024** addresses. Use the **no** form of this command to remove MAC address limits from the interface.
(config-giga-eth 0/1)#	**[no] mac aging-time** <*value*>	Specifies the MAC address aging time in seconds. Valid range is **0** to **3600** seconds. By default, the aging time is set to **300** seconds. Using a value of **0** seconds forces learn and lock behavior. Use the **no** form of this command to return to the default value.

Table 9. Layer 2 UNI MTU Configuration Command

Prompt	Command	Description
(config-giga-eth 0/1)#	**[no] mtu** <*size*> **include-l2-header**	Specifies the MTU size for the Layer 2 UNI. Valid <*size*> range is **60** to **9242** bytes. By default, the Layer 2 MTU is set to **9242** bytes. Use the **no** form of this command to return to the default value.

Layer 3 Ethernet Service Components Commands

The following tables summarize the commands used in Layer 3 configurations of carrier Ethernet services.

Table 10. Layer 3 Subinterface Configuration Commands

Prompt	Command	Description
(config)#	**[no] interface [efm-group** <*slot/group.subinterface id*> **| gigabit-ethernet** <*slot/port.subinterface id*>**]**	Creates a Layer 3 subinterface on the MEN port for Layer 3 services and enters the subinterface's configuration mode. Using the **no** form of this command removes the subinterface from the unit's configuration.
(config-giga-eth 0/1.1)# OR (config-efm-group 1/1.1)#	**[no] connect evc** <*name*>	Associates an EVC with a Gigabit Ethernet subinterface or an EFM group subinterface. Using the **no** form of this command disconnects the EVC from the subinterface.

Table 10. Layer 3 Subinterface Configuration Commands *(Continued)*

Prompt	Command	Description
(config-giga-eth 0/1.1)# OR (config-efm-group 1/1.1)#	**[no] ce-vlan-id untagged**	Specifies that the CE VLAN is untagged on the MEN port. By default, the CE VLAN ID is unspecified, which prevents the subinterface from becoming active. Using the **no** form of this command removes the CE VLAN ID configuration.
(config-giga-eth 0/1.1)# OR (config-efm-group 1/1.1)#	**[no] ip address** <*ip address*> <*subnet mask*>	Specifies an IP address for the MEN port for Layer 3 services. Enter IP addresses in decimal dotted notation, for example, **198.51.100.1**. Using the **no** form of this command removes the IP address from the subinterface.
(config-giga-eth 0/1.1)# OR (config-efm-group 1/1.1)#	**no shutdown**	Enables the subinterface.
(config-giga-eth 0/1.123)#	**[no] egress-queue [inherit |** <*value*>**]**	Specifies the queue for traffic egressing the subinterface. The **inherit** parameter specifies that the PCP of the traffic's outer tag is used to automatically map traffic to the egress queue on a per-packet basis using the QoS CoS map settings. The <*value*> parameter specifies the egress queue for the subinterface; valid range is **0** to **7**. By default, egress queue mapping is set to **inherit**. Using the **no** form of this command returns the egress queue to the default value.
(config-giga-eth 0/1.123)#	**[no] men-pri [inherit |** <*value*>**]**	Specifies the s-tag priority bits (802.1p value) for matching traffic on the subinterface. The **inherit** parameter specifies that the priority value for the matched traffic is inherited from the 802.1q value of the s-tag. The <*value*> parameter specifies an s-tag priority value; valid range is **0** to **7**. By default, the s-tag priority value is set to **inherit**. Using the **no** form of this command returns the s-tag priority value to the default setting.

Table 10. Layer 3 Subinterface Configuration Commands *(Continued)*

Prompt	Command	Description
(config-giga-eth 0/1.123)#	**[no] men-c-tag** <*value*>	Specifies the c-tag to be inserted into subinterface traffic. Valid c-tag <*value*> range is **2** to **4094**. By default, c-tags are not inserted into subinterface traffic. Using the **no** form of this command returns to the default setting.
(config-giga-eth 0/1.123)#	**[no] men-c-tag-pri [inherit |** <*value*>**]**	Specifies the c-tag priority bits (802.1p value) for traffic on the subinterface. The **inherit** parameter specifies that the c-tag priority is inherited from the 802.1p value of the s-tag. The <*value*> parameter specifies a c-tag priority value; valid range is **0** to **7**. By default, the c-tag priority value is set to **inherit**. Using the **no** form of this command returns the c-tag priority to the default setting.

Troubleshooting

Troubleshooting the configuration of the carrier Ethernet services can be done by using various **show** commands from the CLI.

The **show** commands are used to display current configurations and states of the various EVC components, including any configured EVCs and EVC maps. 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 EVC configurations, you can enter the **show evc** command as follows:

```
#show evc
All EVC Tags Available in MEN
EVC evc1
    S-TAG                   :123
    Admin State             : Enabled
    EVC Status              : Running
    MEN-Port                : gigabit-ethernet 0/1
    CE-VLAN Preservation    : Enabled
```


Table 11 describes the **show** commands available for carrier Ethernet components in AOS.

Table 11. Show Commands for Carrier Ethernet Components

Prompt	Command	Description
#	**show evc [**<*name*>**]**	Displays configuration and state information for all configured EVCs. You can optionally display information for a single EVC by entering the EVC name.
#	**show evc-map [**<*name*>**]**	Displays configuration and state information for all configured EVC maps. You can optionally display information for a single EVC map by entering the EVC map name.
#	**show interface [efm-group** <*slot/group*> **| efm-group** <*slot/group.subinterface*> **| gigabit-ethernet** <*slot/port*> **| gigabit-ethernet** <*slot/port.subinterface*>**] [performance-statistics [15-minute [**<*range*>**] | 24-hour [**<*range*>**]]**	Displays the configuration information for the specified interface or subinterface. You can optionally display the performance statistics for the interface by entering the **performance-statistics** parameter. These statistics can be displayed for 15 minute or 24 hour intervals, and can optionally be limited to a specific range of historic intervals using the <*range*> parameter. Valid interval range is **1** to **96** for 15 minute intervals and **0** to **7** for 24 hour intervals.
#	**show system-control-evc [performance-statistics [15-minute [**<*range*>**] | 24-hour [**<*range*>**]]**	Displays the configuration information for the system control EVC. You can optionally the display the performance statistics for the EVC by entering the **performance-statistics** parameter. These statistics can be displayed for 15 minute or 24 hour intervals, and can optionally be limited to a specific range of historical intervals using the <*range*> parameter. Valid interval range is **1** to **96** for 15 minute intervals and **0** to **7** for 24 hour intervals.
#	**show system-management-evc [performance-statistics [15-minute [**<*range*>**] | 24-hour [**<*range*>**]]**	Displays the configuration information for the system management EVC. You can optionally the display the performance statistics for the EVC by entering the **performance-statistics** parameter. These statistics can be displayed for 15 minute or 24 hour intervals, and can optionally be limited to a specific range of historical intervals using the <*range*> parameter. Valid interval range is **1** to **96** for 15 minute intervals and **0** to **7** for 24 hour intervals..

Table 11. Show Commands for Carrier Ethernet Components *(Continued)*

Prompt	Command	Description
#	**show mac address-table [interface** <*interface*>**] [denied]**	Displays the MAC address table entries for the unit. You can optionally specify that only the MAC address table entries for a single interface are displayed. Specify an interface in the format <**interface type** <*slot/port*>>. The optional **denied** parameter displays the denied MAC addresses in addition to the allowed entries.
#	**show mac address-table count**	Displays the allowed, denied, and total MAC addresses in the MAC address table.
#	**show mac limits**	Displays the configured maximum allowed MAC addresses configured on the unit. In addition, the current number of MAC addresses and learned MAC addresses for each interface are displayed.
#	**show mac hw-access-lists**	Displays the configured MAC hardware ACLs configured on the unit.

Troubleshooting Commands for E-LMI

The following **clear**, **show**, and **debug** commands are used with the E-LMI feature to clear timers and counters, show E-LMI status information, and to enable debug messages associated with the feature.

Use the **clear ethernet lmi statistics [interface** <*interface*>**]** command to clear all E-LMI statistics, or E-LMI statistics for a specific interface only. Specify an interface in the format **interface type** <*slot/port*>. Enter the command from the Enable mode as follows:

```
>enable
#clear ethernet lmi statistics
```

Use the **show ethernet lmi statistics** <*interface*> command to display the E-LMI statistics for an interface. Specify an interface in the format <**interface type** <*slot/port*>>. Enter the command from the Enable mode as follows:

```
>enable
#show ethernet lmi statistics gigabit-ethernet 0/2
E-LMI Statistics for giga-eth 0/2
E-LMI Admin Status: Up
E-LMI Operation Status: Up
    UNI ID: giga-eth 0/2
    Reliability Errors:        0
Status Inquiry Timeouts:       0
Invalid Sequence Number:       0
Invalid Status Request:        0
Protocol Errors:               0
Short Message:                 0
```



```
Invalid Version:                0
Invalid Message Type:           0
Invalid Mandatory IE:           0
Mandatory IE Missing:           0
Out of Sequence IE:             0
Duplicated IE:                  0
Mandatory IE Missing:           0
Unexpected Recognized IE: 0

Last Full Status Inquiry Received:          00:50:35
Last Full Status Sent:                      00:50:35
Last Status Check Inquiry Received:         00:00:06
Last Status Check Sent:                     00:00:06
Last clearing of counters:                  never
```

Use the **show ethernet lmi current [**<*interface*>**]** command to display the current status of EVCs that will be sent out with the next E-LMI status message. Use the optional <*interface*> parameter to display the E-LMI status for the specified interface. Specify an interface in the format <**interface** <*slot/port*>>. Enter the command from the Enable mode as follows to display all current EVC statuses:

```
>enable
#show ethernet lmi current
```

Use the **debug ethernet lmi interface** <*interface*> **[event | packet]** command to enable debug messages of E-LMI events (**event** keyword) or E-LMI packets (**packet** keyword). Specify an interface in the format <**interface** <*slot/port*>>. Use the **no** form of this command to disable E-LMI debug messages.

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

To enable debug messages for E-LMI events, enter the command from the Enable mode as follows:

```
>enable
#debug ethernet lmi interface gigabit-ethernet 0/2 event
```