Dynamic Ethernet Service Activation

The Dynamic Ethernet Service Activation (DESA) feature enables the dynamic provisioning of Layer 2 services and transport using dynamic policy. DESA enables increased intelligence in the network control plane, which lowers the cost of network management systems and achieves the following:

- Advanced Ethernet services, with automated subscriber to retail service provider transport mapping and subscriber access service level agreement (SLA) configuration.
- Automated Ethernet services, zero-touch billable Ethernet VPNs and transport services.
- Enhanced retailer network-to-network interface (NNI) that enables enhanced transparency and scalability.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Dynamic Ethernet Service Activation

- Understanding of how to configure the Ethernet virtual connection (EVC), Accounting, Authentication, and Authorization (AAA), and the Intelligent Services Gateway (ISG) control policies.
- Understanding of how to configure xconnect to configure virtual private wire services (VPWS).
- Cisco 7600 routers with ES+ line cards.

Restrictions for Dynamic Ethernet Service Activation

- Static pseudowires cannot be configured from RADIUS.
- A physical interface can support a maximum of 100 Layer 2 contexts.
- A dynamic service instance identifier must begin at 101.
- Security access control lists (ACLs) are not supported. ACL definitions are defined in the user profile.
- Manual or static configuration cannot be applied to a dynamic Ethernet session after the configuration is downloaded.
- The connectivity fault management (CFM) domain cannot be downloaded from an AAA server. CFM domains must be configured on the router prior to EVC download.
- Dynamic creation of a switched virtual interface (SVI) from AAA is not supported
- Dynamic creation of virtual private LAN service (VPLS) virtual forwarding instance (VFI) and SW-based Ethernet over MPLS (EoMPLS) (that is, xconnect under SVI) from AAA is not supported.
- CISCO-EVC-MIB is not supported for the dynamic Ethernet sessions.
- Per-flow (traffic class) Ethernet accounting is not supported.
- VPLS cannot be configured from RADIUS.

Information About Dynamic Ethernet Service Activation

Overview on Dynamic Ethernet Service Activation

Carrier Ethernet enables service providers to offer ubiquitous end-to-end services and transport mechanisms to their customers.

End-to-end services are categorized as follows:

- Layer 2: L2VPN services
- Layer 3: IP (Internet) or Layer 3 (L3) VPN

Transport mechanisms refer to the technology used by the service provider. Some of the transport mechanism are as follows:

- Native Ethernet
- IP/Multi Protocol Label Switching (MPLS)
- SONET, ATM, Frame Relay (FR), and so on

DESA provides network-based service control by integrating the Cisco EVC framework with a dynamic policy.

DESA delivers an intelligent transport-aware service gateway that can be used at various points in a network. Some of the capabilities provided by DESA are as follows:

- Utilizes AAA to dynamically discover and associate a network transport service with a subscriber context, based on subscriber identity.
- Offers subscriber session awareness at Layer 2.
- Utilizes the ability of the ISG to dynamically apply per-subscriber services based on the subscriber identity, service policy, and subscriber profile derived from the service control layer.
- Provides an abstraction for EVC service configuration above the underlying Ethernet technology, alongside ISG policies and services, with these being subject to be applied or modified based on control and policy plane decisions.

In Cisco IOS Release 15.1(2)S, DESA supports two major functions, EVC accounting and Dynamic Ethernet Layer 2 session provisioning.

EVC Accounting

In a service provider network, billing servers receive accounting records from network elements to measure the usage of particular services by specific users. Billing systems use these records to generate per-usage bills for customers. These accounting records carry traffic statistics measured at a point of interest in the network.

The EVC accounting feature exposes native Ethernet traffic to billing systems via accounting interfaces and policies. Through the integration of EVC, ISG, and AAA functions, Ethernet accounting provides a mechanism for service providers to track usage-based services, billing mechanisms for incremental or temporary services, and provide a traceable accountability method for SLA enforcement.

Ethernet flows between subscriber sites across the Carrier Ethernet network are delivered over an EVC architecture construct. EVC denotes an end-to-end connection across the network on which the user can apply a set of services. Ingress Ethernet frames on a port are mapped or classified to an Ethernet service instance based on the information in the Ethernet frame header. The accounting statistics per Ethernet service instance, which represent aggregate counts for an EVC's traffic, are collected. The Ethernet service instance represents only one instance of an EVC per port.

Each accounting record includes the following packet information:

- Input packets
- Output packets
- Input bytes
- Output bytes

Ethernet accounting applies to the following connection topologies:

- Point-to-point (P2P)
- Point-to-multipoint
- Multipoint-to-multipoint

Ethernet accounting applies to the following data-forwarding types:

- EVC switched service (EVC over a bridge domain)
- EVC switched service (local switching)
- EVC tunneled service (EVC over MPLS/IP P2P pseudowire (PW))

Ethernet Accounting Configuration

To configure Ethernet accounting, you must first configure accounting traffic classifiers via a class-map policy and associate it with a control policy. Next, you must configure the control policy at the global level, interface level, and dynamic Ethernet session target level. If control policies are configured at multiple levels, the control policy at the inner level has higher precedence over those at higher levels.

The following session-level traffic classification can be applied through the **encapsulation** command:

- Stacked-VLAN (S-VLAN) range or list
- Customer-VLAN (C-VLAN) range or list
- CoS range or list
- VLAN Ethertype
- Payload type

For service instances configured statically via the command-line interface (CLI), you must use the **ethernet subscriber static** command before enabling EVC accounting on the service instance. Without this configuration, the EVC accounting feature cannot be applied.

Per-Session Accounting

Per-session accounting generates a single accounting record for aggregate traffic. This Ethernet ISG session can be either statically or dynamically instantiated.

You can enable accounting at multiple configuration sources such as a user profile on the AAA server, service profile on the AAA server, or service policy on the ISG device. Usage of the ISG control policy for static Ethernet sessions ensures that the steps for enabling per-session accounting remain the same for both static and dynamic Ethernet sessions.

Per-Session RADIUS Accounting Record Format

DESA provides support for generating RADIUS accounting records on a per-subscriber and on a per-class-per-subscriber basis for static and dynamic Ethernet sessions.

Each per-session accounting record can be identified by a unique Acct-Session-ID. The DESA feature introduces two new attributes--stag-vlan-id and ctag-vlan-id. These two new attributes can represent a single or a range of VLAN values.

For detailed steps on configuring Ethernet accounting, see the How to Configure Dynamic Ethernet Service Activation section.

Ethernet Layer 2 Session Provisioning

DESA supports static (preconfigured) and dynamic (dynamic service instances) Ethernet sessions.

Static Ethernet Session Provisioning

Static Ethernet sessions are configured by applying the **ethernet subscriber static** command to Ethernet service instances that are explicitly provisioned using the CLI. DESA supports the application of certain features dynamically to static Ethernet sessions.

Dynamic Ethernet Session Provisioning

Prior to the introduction of DESA, Ethernet service instances had to be configured statically using the CLI. DESA supports creation of dynamic service instances. This dynamic service instance creation is controlled by ISG infrastructure. ISG sessions for Ethernet service instances are referred to as dynamic Ethernet sessions.

DESA provides mechanisms for establishing dynamic Ethernet sessions through an embedded policy plane. The policy plane provides the infrastructure for managing the lifecycle of a session, focusing on authenticating and authorizing sessions.

Dynamic Ethernet sessions are transient in nature, that is, they support start and end events. The start event is marked by the receipt of a frame of interest, which is called the first sign of life (FSoL). The end event is triggered by the expiry of a session idle timer. The FSoL trigger causes a chain of events that starts with subscriber authentication and authorization, followed by service and features determination according to policy rules, thereby leading to dynamic session provisioning and feature or service enablement.

Control Policies

An ISG control policy defines actions that are taken in response to specified events and conditions. Control policies consist of one or more control policy rules. Each control policy rule consists of a condition defined by a control class, session events, and one or more actions. For more information about control policies, refer to the *Cisco IOS Intelligent Services Gateway Configuration Guide* .

You can specify ISG control policies in a hierarchical manner. DESA introduces a new level called the service instance level. For a given session, the policy manager executes the control policy with the highest precedence.

Layer 2 Context

Prior to the introduction of DESA, support for creating service instances was available under Ethernet ports, and you could define only one control policy and one type of session initiator under a single port.

DESA supports the Layer 2 context, a specific Ethernet service instance that classifies FSoL frames and sends them to the device CPU for processing. This processing involves determining whether the FSoL frame should trigger the creation of a dynamic Ethernet session based on AAA authorization.

The Layer 2 context can dynamically trigger multiple service instances based on the configuration within the Layer 2 context. The encapsulation criteria associated with the Layer 2 context must be broad enough to attract desired FSoLs that can trigger dynamic Ethernet sessions.

You can create a new Layer 2 context under an Ethernet port in the following scenarios:

- If there is a requirement to create Ethernet sessions based on multiple different initiators, you can create one Layer 2 context for each type of initiator.
- If there is a requirement to apply different ISG control policies to control sessions under the same Ethernet port.

The number of Layer 2 contexts can be of the same order of magnitude as the number of the ports in the system.

Dynamic Ethernet sessions can be categorized according to the type of the service delimiter that is used to classify (demultiplex) frames into subscriber sessions. In Cisco IOS Release 15.1(2)S, VLAN sessions are the type of dynamic Ethernet sessions supported.

VLAN Sessions

A VLAN session is a dynamic Ethernet session in which the service delimiter is either a VLAN (S-VLAN or C-VLAN), or a VLAN stack; that is, double tagged (S-VLAN + C-VLAN).

Single VLAN

When the service delimiter is a single VLAN, the associated EtherType can be one of the following:

- 0x8100
- 0x9100
- 0x9200
- 0x88a8

You can configure the device with a static Layer 2 context that covers a list or range of single VLANs. There may be multiple Layer 2 contexts per interface (with disjoint VLAN sets). VLAN sessions are logically instantiated over the context with the matching encapsulation. There can be multiple sessions over a single Layer 2 context.

VLAN Stack

When the service delimiter is a VLAN stack, the outermost VLAN can have any of the EtherTypes presented under the single VLAN section, whereas the inner VLAN must have an EtherType of 0x8100. The device can be configured with a static Layer 2 context that matches a unique outermost tag (S-VLAN) and a range of inner tags (C-VLANs).

There can be many static Layer 2 contexts per physical port with nonoverlapping encapsulation. VLAN sessions are logically instantiated over the context with appropriate encapsulation. There can multiple sessions over one Layer 2 context.

There is always a unique session per C-VLAN within a given S-VLAN.

FSoL Detection for AToM VC

DESA enables dynamic EoMPLS virtual circuits (VCs) to be established upon the receipt of FSoL events on the pre-established LDP session, between the aggregation and distribution nodes.

The FSoLs are gleaned for authorization keys that are sent to the ISG policy plane for downloading the provisioned profiles. This results in the ingress VC being accepted and in the creation of the Ethernet session and the egress VC.

FSoL Mechanisms

DESA enables establishing the dynamic Ethernet sessions upon the receipt of FSoL frames from the access or core side of the Layer 2 Ethernet network.

Various mechanisms can be used by a provider device as the FSoL indication of an incoming Ethernet session from a CE node.

Cisco IOS Release 15.1(2)S supports two types of FSoL mechanisms, unclassified service frames and Label Distribution Protocol (LDP) for Any Transport over MPLS (AToM).

Unclassified Service Frames

Unclassified service frames are frames that do not belong to an existing active session but that trigger dynamic Ethernet sessions. Unclassified frames depend on the following characteristics:

- Type of Ethernet session. Cisco IOS Release 15.1(2)S supports VLAN sessions.
- Classifier of the associated Layer 2 context.

If the Layer 2 context classifier matches a range or list of single VLANs, the FSoL for the Layer 2 session is the first Ethernet frame received on a given VLAN within the range or list.

If the Layer 2 context classifier matches a single S-VLAN and range or list of C-VLANs, the FSoL is receipt of a double-tagged Ethernet frame whose C-VLAN does not have an existing session. That is, the FSoL is the first received frame on the C-VLAN for that S-VLAN.

LDP for AToM

In an MPLS aggregation network, when a service needs to be established based on the dynamic indication coming in from the MPLS core, the MPLS provider edge (PE) device treats AToM LDP VC label advertisements as FSoL. DESA supports an equivalent of Layer 2 context to provide granular control over the LDP FSoL.

The LDP FSoL contexts serve the following two purposes:

- To identify a range of LDP VC label advertisements to initiate or accept dynamic session creation.
- To specify the control policy to be applied for sessions initiated in the context.

Any network element that should accept LDP VC label advertisements as FSoL indications should have already established targeted LDP sessions over which the label advertisements are to be processed. You can set up this targeted LDP session via static configuration.

If a VPWS PE receives the AToM LDP FSoL, a PW is established toward the MPLS aggregation network (using the VC ID and target peer IP address that are gleaned from the FSoL). This PW is associated with a native Ethernet attachment circuit (AC) specified in the RADIUS authorization response. The AC is effectively a dynamic Ethernet session whose attributes are supplied via RADIUS.

When an xconnect is not configured and an LDP VC label advertisement message arrives, based on the host address, the network address, and the VC ID of the peer, an attempt is made to identify a service authorization

group. The message is treated as a FSoL only when a match is found for the message, and a request is sent to the policy plane for subscriber authorization. However, if a match is not found, subscriber authorization is not attempted.

When a label withdraw message is received, the system checks for a corresponding xconnect. If the xconnect is found, it is removed. Xconnect is not destroyed in response to a pseudowire status message.

Dynamic Transport Provisioning

Dynamic Ethernet sessions are established when the FSoL events are triggered. The information or metadata provided by the FSoL is used as the authorization keys to download RADIUS profiles for Layer 2 transport or PW session attributes.

Single-Sided Model

DESA supports the single-sided model for Layer 2 VPN (L2VPN) provisioning. In the single-sided model, L2VPN is provisioned on the PE only when deemed necessary. The initiator PE detects and instigates the PWs, while the peer PE authorizes and accepts it. This assumes that a target LDP session has already been established between the two PEs.

Automated Transport Setup VPWS

Upon the creation of dynamic Ethernet sessions on the ingress side, the authorized profile also configures the AToM VPWS as the transport service, which in turn configures the Layer 2 tunnel. All the relevant configuration elements must be present in the authorized profiles.

Dynamic Forwarding Services

Dynamic Ethernet sessions must be associated with a forwarding service in order to complete the service transport setup.

DESA supports the following forwarding services:

- Bridge domain service (native Ethernet multipoint bridging)
- Local connect service (P2P stitched services)
- EoMPLS service (P2P tunneled services)

The forwarding services may or may not be preprovisioned on the device. Either way, the forwarding service is associated with the Ethernet sessions dynamically based on the policy determination. If the forwarding service is not preprovisioned, then it is constructed on the go and bound to the session.

Bridge Domain Service

The bridge domain service is a Layer 2 Ethernet multipoint bridging service. DESA supports the association of a dynamic Ethernet session with a Layer 2 bridge domain. The bridge domain may be preconfigured on the device, or dynamically created based on AAA profiles.

Multiple dynamic Ethernet sessions can share the same bridge domain, or they can each have dedicated bridge domains depending on the AAA profiles.

Local Connect Service

The local connect forwarding service is a P2P service. DESA supports the establishment of a local connect service between two dynamic Ethernet sessions.

Note You cannot set up a local connect service between a dynamic Ethernet session and a static session (or a CLI-configured service instance)

EoMPLS Forwarding Service

The EoMPLS forwarding service enables next-generation wholesale models for service providers, where PWs are used to backhaul services from the subscriber edge to the retailer edge.

EoMPLS does not have the mechanisms for signaling tunnels and sessions within tunnels independently. Instead, the signaling involves the establishment of the PW that traditionally has a one-to-one mapping to a service. That is, each service has a dedicated PW.

However, in EoMPLS, the PW is used to multiplex and backhaul the traffic of several subscribers from the subscriber edge to the retailer edge. It is possible to have a single PW per retailer, or a single PW per access node per retailer.

The provisioning of these PWs can follow one of the following two models:

- Single-sided provisioning
- Double-sided provisioning

In the single-sided provisioning model, the FSoL arrives on the attachment circuit of only one MPLS PE device. LDP is used as the FSoL to trigger the PW setup on the far-end PE over the MPLS core.

In the double-sided provisioning model, the FSoL arrives on the attachment circuits of both MPLS PE devices. LDP is not used as the FSoL to trigger the PW setup over the MPLS core.

Dynamic Ethernet Session Mapping to IP L3VPN

For Ethernet transport of business L3VPN services and for residential 3-play services, support for termination of dynamic Ethernet sessions into IP/L3VPN is required.

Dynamic Ethernet sessions are created on the Ethernet interface and associated with bridge domains. An SVI (interface VLAN) is statically preconfigured with the same identifier as that of the bridge domain, and this SVI is configured with an IP address and optionally a virtual routing and forwarding (VRF) instance. This SVI can then be used to offer Layer 3 termination; for example, business L3VPN services or residential IPTV or video on demand (VoD).

Dynamic Ethernet Session Attributes Features and Control Protocols

After a dynamic Ethernet session is created, you can associate attributes, features, and protocols to the session. This can be done either during the initial session setup phase, or later on in the lifetime of the session via a RADIUS CoA.

DESA Attributes Supported During the Initial Setup Phase and via RADIUS CoA

Quality of Service

The dynamic Ethernet sessions support the dynamic configuration of Modular QoS CLI (MQC) Quality of Service (QoS).

MQC is a CLI structure that allows users to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to select traffic, while the QoS features in the traffic policy determine how to treat the classified traffic. The QoS policies define the corresponding EVC bandwidth profile and guarantees the negotiated customer SLAs. For more information about MQC QoS, see Applying QoS Features Using the MQC .

Accounting

DESA supports session accounting. Session accounting is used to report information about a session's state.

For more information about session accounting and class-based accounting, see theISG RADIUS Interface chapter of the *Cisco IOS ISG RADIUS CoA Interface Guide* .

Idle Timeout and Session Timeout

The idle timeout feature allows the automatic termination of a dynamic Ethernet session after a period of inactivity. The device monitors the traffic transmission activity of the session, and if a user-specified period of time elapses before any new packets are received or transmitted for a given dynamic Ethernet session, then that session is torn down and its associated resources are freed. This feature allows network operators to protect the device from resource depletion when the sessions are short-lived or transient in nature. The idle timeout period is configured via AAA attributes.

ACLs

Dynamic Ethernet sessions support configuration of Layer 2 and Layer 3 ACLs. Because ACLs can be highly tailored to the services offered, dynamic Ethernet sessions support building the ACL definition dynamically. That is, the global ACL definition can be preconfigured statically on the device or can be downloaded via RADIUS.

DESA Attributes Supported During the Initial Setup Phase

EVC and EVC Per UNI Attributes

The following session attributes are provisioned dynamically upon the initial authorization:

- EVC name
- Encapsulation
- Rewrite (that is, VLAN translations)
- User Network Interface (UNI) count and service type (point-to-point or multipoint)

- CE-VLAN to EVC map
- Layer 2 Control Protocol (L2CP) handling

DHCP Snooping

Dynamic Ethernet sessions support configuration of DHCP snooping on bridge domains. DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages. DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You can use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

The function of DHCP snooping is to watch for DHCP request and response packets. By gleaning data from these packets, a table of MAC interface bindings, also called as DHCP snooping table, is built. These bindings can then be used to validate transactions from other services. For example, IP source guard uses the DHCP snooping bindings to prevent IP address spoofing.

DHCP Snooping Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP snooping option-82 feature is enabled on the router, a subscriber device is identified by the router port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access router and are uniquely identified.

Dynamic Ethernet sessions provide the capability to dynamically configure the DHCP Option 82 subscriber ID on a per Ethernet session basis.

IP Source Guard

IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

The dynamic Ethernet sessions support dynamic configuration of IP source guard. When the IP source guard feature is enabled, it blocks all IP traffic on the session except for DHCP packets, which are captured by DHCP snooping. When a CE receives a valid IP address from the DHCP server, an automatic ACL is installed on the session that permits the traffic from that IP address only. Optionally, this ACL may also permit only traffic from the source MAC address gleaned from the DHCP request. All other traffic ingressed on the session, which does not have the matching source IP address, and optionally source MAC address, is blocked. In addition to DHCP snooping binding, IP source guard also filters IP traffic, based on static IP bindings. This allows the feature to operate on sessions where the clients have statically assigned IP addresses.

Dynamic configuration of IP source guard is supported on per-dynamic Ethernet session basis.

MAC Security

You can use MAC security with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside

the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

Dynamic Ethernet sessions support dynamic configuration of the EVC MAC security. MAC security has configuration knobs that apply both per dynamic Ethernet session and per bridge domain, and both can be configured dynamically.

Connectivity Fault Management

Carrier Ethernet networks are operated by multiple independent organizations, with restricted management access to each other's equipment. This imposes a new set of Operations, Administration, and Maintenance (OAM) requirements across Carrier Ethernet networks. Ethernet OAM provides tools for monitoring and troubleshooting end-to-end Ethernet services by providing capabilities for detecting, verifying, and isolating connectivity failures in the network.

Connectivity Fault Management (CFM, IEEE 802.1ag) is a service-level OAM protocol that provides tools for monitoring and troubleshooting end-to-end Ethernet services. Cisco IOS E-OAM implementation relies on CFM for end-to-end status of the Ethernet Service across PE devices in the Carrier Ethernet network and updates the CE device via the Ethernet Local Management Interface (E-LMI). The end-to-end connection can from a PE to PE or from a CE to CE. A service can be identified as an S-VLAN or an EVC service.

Dynamic Ethernet sessions support CFM. Activating CFM involves tasks that are performed once at network provisioning time, such as setting up maintenance domains, in addition to tasks that are completed as part of service provisioning.

For both static and dynamic Ethernet sessions, RADIUS-based dynamic provisioning of per-service CFM attributes is supported. These include the following:

- Creating up and down maintenance endpoints (MEPs) (specifying the domain, maintenance point ID (MPID), CoS, alarm delay, reset interval, and notification options)
- Creating maintenance intermediate points (MIPs) (specifying level) or per MA,MIP autocreate option (the global and per-domain MIP autocreate options are specified as part of network provisioning)
- Defining static remote MEP lists, and enabling/disabling remote MEP check
- Defining short MA names
- Defining CFM sender ID
- Specifying maximum number of MEPs per MA
- Enabling/disabling CCM transmission, and defining continuity check interval and loss threshold
- Enabling Alarm Indication Signal (AIS) and specifying AIS options (period, expiry threshold, alarm suppression, and level)
- Enabling LCK and specifying LCK options (period, expiry threshold and level)
- Specifying CFM encapsulation on dynamic Ethernet sessions with ambiguous classifiers
- OAM Interworking options (CFM to E-LMI, 802.3ah to CFM)

For static Ethernet sessions, the keys used as part of the authorization request to obtain the configuration profile hosting the CFM attributes are as follows:

- EVC ID
- Host name or router ID

- Port ID

For dynamic Ethernet sessions, the keys vary depending on the type of FSoL and will in general be equal to or a subset of the keys required for initial session authorization.

E-LMI

E-LMI is an Ethernet OAM protocol. It provides information that enables autoconfiguration of CE devices and provides the status of EVCs for large Ethernet metropolitan-area networks (MANs) and WANs. Specifically, E-LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. E-LMI also communicates the attributes of an EVC and a UNI to a CE device.

E-LMI has significance at the UNI between the metro Ethernet network (MEN) and the CE. The protocol serves two functions:

- Provides fault notification from PE to CE (EVC and remote UNI status).
- Provides message formats to allow the automated configuration of the CE remotely from the PE.

DESA supports the dynamic provisioning of the following E-LMI attributes for the purpose of communicating them to the CE:

- EVC ID
- EVC type (P2P or multipoint)
- CE-VLAN/EVC map

AAA Schema for EVC

The AAA schema for EVC ensures that the off-box configuration and accounting of Ethernet services (via RADIUS) is supported for native Ethernet bridged services.

Dynamic Service Activation and Deactivation Using COA

The DESA feature allows administrators to dynamically apply and remove services on existing Ethernet sessions from an external server using a change of authorization (CoA) extension. A service consisting of individual features must be atomic; if any of the constituent features fail, the entire service is removed, leaving the session in the original state.

The following table provides CoA capabilities that are supported by DESA:

Table 1: CoA Capabilities Supported for PEI

CoA Capabilities	Description
Service Activate	Applies a service (a named collection of EVC and ISG features) on an existing session.
Service Deactivate	Removes a service from an existing session.
Session Query	Queries details related to a session from RADIUS.

CoA Capabilities	Description
Session Query for Service Status	Queries the status of a service.

How to Configure Dynamic Ethernet Service Activation

Configuring AAA for Enabling Accounting

Cisco IOS AAA supports six different types of accounting (network, exec, commands, connection, system, and resource), two accounting record types (stop-only, start-stop), and two accounting methods (TACACS+, RADIUS). You can specify these options by defining an AAA method list by using the **aaa accounting** command. For more information, see the Cisco IOS Security Command Reference and the Configuring Accounting chapter of the *Security Configuration Guide: Securing User Services*.

After defining the AAA method list, you can use it to configure accounting by referring to the named method list from different configuration sources such as the RADIUS user profile, RADIUS service profile, and on-router service policy map.

You can define a default method list (a method list with the name “default”). This default method list is automatically applied to all sessions except those that have a named method list explicitly configured.

Configuring AAA Enabling Interim Accounting Update

You can periodically generate accounting records. Two types of interim accounting are supported, accounting updates for new information and periodic accounting.

Accounting updates for new information can be enabled or disabled globally by issuing the **aaa accounting update** command on a router. However, interval for periodic accounting can be configured at three configuration sources--on the router, in the user profile on the AAA server, and in the service profile on the AAA server. For more information, see the Cisco IOS Security Command Reference and the http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_accountg.html“Configuring Accounting” chapter of the *Security Configuration Guide: Securing User Services*.

Configuring ISG Control Policy to Apply ISG Services

To define a control policy, you must first define a control class map to identify events and conditions and then define a control policy map to bind the control class map to different actions. Control polices can be defined in multiple levels such as global, interface, subinterface, virtual-template, VC, and private virtual circuit (PVC).

The policy manager executes the rules in the control policy only after the session comes into existence. For information about configuring control policies, see Configuring ISG Control Policies .

Configuring Per-Session Accounting

Perform the following task to configure per-session accounting for an Ethernet session.

Before You Begin

- Accounting traffic classifiers must be configured via class-map policies and associated with a control policy. For more information about configuring traffic classifiers, see Configuring ISG Control Policies.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet** [*evc-name*]
5. **encapsulation dot1q**
6. **service-policy type control** *policy-map-name*
7. **ethernet subscriber static**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface type and number, and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet test`	Configures an Ethernet service instance on an interface, and to enters service instance configuration mode

	Command or Action	Purpose
Step 5	**encapsulation dot1q** **Example:** `Router(config-if-srv)# encapsulation dot1q`	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.
Step 6	**service-policy type control** *policy-map-name* **Example:** `Router(config-if-srv)# service-policy type control policy1`	Applies a control policy to a context.
Step 7	**ethernet subscriber static** **Example:** `Router(config-if-srv)# ethernet subscriber static`	Creates static sessions for configuring EVC accounting.
Step 8	**end** **Example:** `Router(config-if-srv)# end`	Exits service instance configuration mode and enters privileged EXEC mode.

Disabling Per-Session Accounting Configuration

Tasks for disabling per-session accounting depends on the methodology that was used to configure the per-session accounting feature.

Disabling a per-flow accounting configuration when the feature was installed through a per-user profile

SUMMARY STEPS

1. Modify the user profile associated with the target session to remove the Cisco Attribute Value (AV) pair "accounting-list=method_list_name"
2. Clear the target session by using the CLI command or packet of disconnect (PoD) from the AAA server.

DETAILED STEPS

Step 1 Modify the user profile associated with the target session to remove the Cisco Attribute Value (AV) pair "accounting-list=method_list_name"

Step 2 Clear the target session by using the CLI command or packet of disconnect (PoD) from the AAA server.

Disabling a per-flow accounting configuration when the feature was installed through a service profile

Perform this task to disable a per-flow accounting configuration, if the feature was installed through a service profile on an AAA server or a service-policy on the router.

SUMMARY STEPS

1. Identify the Acct-Session-ID (the RADIUS attribute 44) associated with the target session.
2. Identify the service name (that is, the service-profile name on AAA server or the service-policy name on the router) that contains the feature that must be uninstalled.
3. Apply the Acct-Session-ID and service name with the ISG service deactivate mechanism to remove the service from the target session. This mechanism makes use of the RADIUS CoA feature. For more information, see the *Cisco ISG RADIUS Interface Guide* .

DETAILED STEPS

Step 1 Identify the Acct-Session-ID (the RADIUS attribute 44) associated with the target session.

Step 2 Identify the service name (that is, the service-profile name on AAA server or the service-policy name on the router) that contains the feature that must be uninstalled.

Step 3 Apply the Acct-Session-ID and service name with the ISG service deactivate mechanism to remove the service from the target session. This mechanism makes use of the RADIUS CoA feature. For more information, see the *Cisco ISG RADIUS Interface Guide* .

Note Deactivating a service on a session removes all the features applied through the service.

Modifying Per-Session Accounting Configuration

In an ISG framework, you can activate a feature by configuring it inside a user profile or bundling it inside an off-box service-profile or on-box service-policy.

You can modify a per-session accounting configuration by first deactivating a service, and then reactivating a new service. Alternatively, you can modify the service definition and clear all the sessions using the service to force them to reauthorize.

Configuring a Layer 2 Context

Perform this task to configure a Layer 2 context.

Note

- Only one initiator is allowed in each Layer 2 context.
- Modification of the **encapsulation** command associated with a Layer 2 context causes all the associated dynamic Ethernet sessions to be disconnected.
- You cannot specify an IP subscriber initiator in Layer 2 contexts.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet** [*evc-name*]
5. **encapsulation** {{**dot1ad**| **dot1q**}[*vlan-id*| **any**] {**cos** *cos-value* | **etype** *type*| **exact** | **second-dot1q**| **vlan-type**} | **priority-tagged** [**cos** *cos-value*] [**etype** *type*] | **untagged**[**etype** *type*]}
6. **ethernet subscriber**
7. **initiator unclassified vlan**
8. **service-policy type control** *policy-map-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface type and number, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**service instance** *id* **ethernet** [*evc-name*] **Example:** `Router(config-if)# service instance 1 ethernet test`	Configures an Ethernet service instance on an interface, and to enters service instance configuration mode
Step 5	**encapsulation** {{**dot1ad**| **dot1q**}[*vlan-id*| **any**] {**cos** *cos-value* | **etype** *type*| **exact** | **second-dot1q**| **vlan-type**} | **priority-tagged** [**cos** *cos-value*] [**etype** *type*] | **untagged**[**etype** *type*]} **Example:** `Router(config-if-srv)# encapsulation dot1q`	Specifies the classifier to identify the subset of traffic associated with a port.
Step 6	**ethernet subscriber** **Example:** `Router(config-if-srv)# ethernet subscriber`	Enables the Ethernet Layer 2 context. • This context is used for creating dynamic Ethernet sessions. • To disconnect the existing sessions from the Layer 2 context, use the **no ethernet subscriber** command.
Step 7	**initiator unclassified vlan** **Example:** `Router(config-if-srv)# initiator unclassified vlan`	Enables an initiator for detecting the FSoL under Ethernet Layer 2 context. • You must remove the existing initiators before configuring new ones. • To remove an existing initiator, use the **no initiator unclassified vlan** command.
Step 8	**service-policy type control** *policy-map-name* **Example:** `Router(config-if-srv)# service-policy type control policy1`	(Optional) Applies a control policy to a context. • If a control policy is not specified, then the policy manager attempts to find one defined in the hierarchy. • To remove an existing control policy, use the **no service-policy type control** command.
Step 9	**end** **Example:** `Router(config-if-srv)# end`	Exits service instance configuration mode and enters privileged EXEC mode.

Enabling Dynamic Ethernet Sessions

Perform the following task to enable dynamic Ethernet sessions:

SUMMARY STEPS

1. Configure an Layer 2 context on the router. For more information about configuring an Layer 2 context, see the Configuring a Layer 2 Context, on page 18.
2. Configure session keys using a control policy on the router. For more information on configuring session keys by using control policies, see Configuring ISG Control Policies .
3. Configure a per-user profile for dynamic Ethernet sessions on the AAA server. Every dynamically instantiated Ethernet session must have a unique per-user profile on the AAA server. A per-user profile on the AAA server is essentially a set of AAA attributes identified by a username. In case of DESA, the username for the per-user profile is constructed from the session keys.
4. Configure a service profile for the required forwarding services. Cisco recommends that you define a different profile for the forwarding service and use the forwarding service AAA attribute to tie both the profiles.
5. Configure a service profile for the desired EVC and ISG services.

DETAILED STEPS

Step 1 Configure an Layer 2 context on the router. For more information about configuring an Layer 2 context, see the Configuring a Layer 2 Context, on page 18.

Step 2 Configure session keys using a control policy on the router. For more information on configuring session keys by using control policies, see Configuring ISG Control Policies .

Step 3 Configure a per-user profile for dynamic Ethernet sessions on the AAA server. Every dynamically instantiated Ethernet session must have a unique per-user profile on the AAA server. A per-user profile on the AAA server is essentially a set of AAA attributes identified by a username. In case of DESA, the username for the per-user profile is constructed from the session keys.

Step 4 Configure a service profile for the required forwarding services. Cisco recommends that you define a different profile for the forwarding service and use the forwarding service AAA attribute to tie both the profiles.

Step 5 Configure a service profile for the desired EVC and ISG services.

Configuring AToM Subscribers

Perform the following task to configure AToM subscribers:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 subscriber authorization group** *group-name*
4. **peer** {**host** *destination-host-address*| **network** *destination-network-address destination-network-mask*} *vc-id*[*vc-id-range*]
5. **service-policy type control** *policy-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**l2 subscriber authorization group** *group-name* **Example:** `Router(config)# l2 subscriber authorization group group1`	Creates a Layer 2 subscriber authorization group, and enters Layer 2 subscriber group mode. • You must define mutually exclusive service authorization groups.
Step 4	**peer** {**host** *destination-host-address*| **network** *destination-network-address destination-network-mask*} *vc-id*[*vc-id-range*] **Example:** `Router(config-l2-sub-gr)# peer host 10.10.1.1 23 54`	Defines the target LDP peer PE information. • Within a router, the *destination-host-address* and *vc-id-range* combination must be unique to identify a unique service authorization group.
Step 5	**service-policy type control** *policy-map-name* **Example:** `Router(config-if-srv)# service-policy type control policy1`	(Optional) Applies a control policy to a context.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if-srv)# end`	Exits service instance configuration mode and enters privileged EXEC mode.

Verifying Per-Session Accounting and Layer 2 Context

Perform the following task to verify the per-session accounting configuration:

SUMMARY STEPS

1. Enter the **show subscriber session** command to display information about subscriber sessions on the ISG.
2. Enter the **show aaa sessions** command to display AAA subscriber information, including the unique ID.
3. Enter the **show aaa user** command to display attributes related to the AAA session.
4. Enter the **show ethernet service instance detail** command to display information about Ethernet service instances.
5. Enter the **show mpls l2transport vc detail** command to display information about AToM VCs and static PWs that have been enabled to route Layer 2 packets on a router.
6. Enter the **show xconnect all detail** command to display information about xconnect ACs and pseudowires.

DETAILED STEPS

Step 1 Enter the **show subscriber session** command to display information about subscriber sessions on the ISG.

Example:

```
Router# show subscriber session uid 100 detailed
Subscriber session handle: AAAAAAAA, state: connected, service: xxxx
Unique Session ID: 100
... ... ...
Session inbound features:
Feature: Session accounting
Method List: my_aaa_method_list
Outbound direction:
Packets = 1000 Bytes = 40000
Session outbound features:
Feature: Session accounting
Method List: my_aaa_method_list
Outbound direction:
Packets = 1000 Bytes = 4000
... ... ...
```

Step 2 Enter the **show aaa sessions** command to display AAA subscriber information, including the unique ID.

Example:

```
Router# show aaa user all
Unique id 100 is currently in use.
Accounting:
log=xxxx
Events recorded :
... ... ...
Cumulative Byte/Packet Counts :
Bytes In = 40000 Bytes Out = 40000
Paks In = 1000 Paks Out = 1000
... ... ...
StartTime = xxx
AuthenTime = xxx
    Component = IEDGE_ACCOUNTING
```

Step 3 Enter the **show aaa user** command to display attributes related to the AAA session.

Example:

```
Router# show aaa user all
Unique id 100 is currently in use.
Accounting:
log=xxxx
Events recorded :
... ... ...
Cumulative Byte/Packet Counts :
Bytes In = 40000 Bytes Out = 40000
Paks In = 1000 Paks Out = 1000
... ... ...
StartTime = xxx
AuthenTime = xxx
    Component = IEDGE_ACCOUNTING
```

Step 4 Enter the **show ethernet service instance detail** command to display information about Ethernet service instances.

Example:

```
Router# show ethernet service instance detail
Service Instance ID: 1
Service instance type: L2Context
Intiators: unclassified vlan
Control policy: ABC
Associated Interface: Ethernet0/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q 200-300 vlan protocol type 0x8100
Interface Dot1q Tunnel Ethertype: 0x8100
State: Up
EFP Statistics:
   Pkts In   Bytes In   Pkts Out  Bytes Out
         0          0          0          0
```

Step 5 Enter the **show mpls l2transport vc detail** command to display information about AToM VCs and static PWs that have been enabled to route Layer 2 packets on a router.

Example:

```
Router# show mpls l2transport vc detail
Local interface: Et0/0 up, line protocol up, Eth VLAN 22 up
  Destination address: 33.33.33.34, VC ID: 12346, VC status: up
    Output interface: Et4/0, imposed label stack {19 20}
    Preferred path: not configured
```

```
    Default path: active
    Next hop: 11.11.11.12
  Create time: 00:02:23, last status change time: 00:02:23
  Signaling protocol: LDP, peer 33.33.33.34:0 up
    Targeted Hello: 33.33.33.33(LDP Id) -> 33.33.33.34, LDP is UP
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last local SSS circuit status rcvd: No fault
      Last local SSS circuit status sent: No fault
      Last local  LDP TLV    status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 22, remote 20
    PWID: 8199
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

Step 6 Enter the **show xconnect all detail** command to display information about xconnect ACs and pseudowires.

Example:

```
Router# show xconnect all detail
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0:22(Eth VLAN)           UP mpls 33.33.33.34:12346             UP
            Interworking: ethernet               Local  VC label 22
                                                 Remote VC label 20
                                                 pw-class:
```

Configuration Examples for Dynamic Ethernet Service Activation

Example Configuring AAA Accounting

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
```

```
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method

to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to

use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

Examples Configuring ISG Control Policy to Apply ISG Services

The following example shows how to enable an ISG control policy that directly applies to a service policy:

```
policy-map type control SampleControlPolicyMap1
    class type control always event session-start
      1 service-policy type service SampleAccountingPolicy
```

The following example shows how to enable an ISG control policy that gets authorizations from the AAA server:

```
policy-map type control SampleControlPolicyMap2
    class type control always event session-start
      1 authorize identifier stag-vlan-id plus cos-vlan-id
```

Example Configuring Per-Session Accounting

The following example shows how to define a control policy on the router:

```
policy-map type control SampleControlPolicyMap
    class type control always event session-start
      1 service-policy type service SampleAccountingPolicy
```

The following example shows how to define a service policy on the router:

```
class-map type traffic match-any EmptyClassMap
policy-map type service SampleServicePolicyMap
   class type traffic EmptyClassMap
     accounting aaa list my-method-list
```

The following example shows how to create a static Ethernet session and associate it with the previously defined control policy:

```
service instance 10 ethernet
   encapsulation dot1q 100
   service-policy type control SampleServicePolicyMap.
   ethernet subscriber static
```

Examples Configuring Service Instances

The following example shows how to configure a static bridge domain. This is an example of native Ethernet, where there is no requirement of creating ISG sessions:

```
interface ethernet 0/0
  service instance dot1q 1 second-dot1q 1-2000
   bridge-domain 100
```

The following example shows how to configure a static Ethernet session. In this case, one ISG session is created for every service instance. The initiator of the ISG session is statically configured.

```
interface ethernet 0/0
  service instance 1 ethernet
     encapsulation dot1q 1 second-dot1q 1-2000
     ethernet subscribers static
     bridge-domain 100
```

The following example shows how to configure a service instance that is treated as a Layer 2 context:

Note Layer 2 context and static Ethernet sessions are mutually exclusive on the same port.

```
interface ethernet 0/0
  service instance 1 ethernet
   encapsulation dot1q 1 second-dot1q 1-2000
   service-policy type control mypolicy
   ethernet subscribers
     initiator unclassified-vlan
```

Example Configuring Layer 2 Context

The following example shows how to create a Layer 2 context of unclassified VLAN type:

```
!!Layer2 Context 2
interface Ethernet 0/0
  service instance 2 ethernet
   encapsulation dot1q 1 second-dot1q 2001-4094
   ethernet subscriber
     initiator unclassified-vlan
```

Example Configuring AToM Subscribers

The following example shows how to configure an AToM subscriber:

```
l2subscriber authorization group list1
  peer host 10.10.1.1 vc-id 100-200
   service-policy type control ldpFSOL-ctrl-policy-1
l2subscriber authorization group list2
  peer network 10.10.2.1 mask 255.255.255.0 vc-id 100-200
   service-policy type control ldpFSOL-ctrl-policy-2
```

Example Configuring Single-Sided Dynamic L2VPN VPWS

The following example shows how to configure dynamic L2VPN VPWS on the PE router:

```
l2 subscriber authorization group atom_test1
 service-policy type control atom_rule1
 peer network 10.10.1.1 255.255.0.0 1 4294967295
```

The following is sample RADIUS peer profile configuration:

```
RADIUS Profile
Peer IP Profile (Username: peer-ip:102.102.102.102:vc-id:111111)
Cisco-AVPair = l2vpn:vcid=111111
Cisco-AVPair = l2vpn:service-id=vpws_pw_customer1
Cisco-AVPair = subscriber:sss-service=vpws
Cisco-AVPair = l2vpn:redundancy-group=2
Cisco-AVPair = l2vpn:pw-encapsulation=mpls
Cisco-AVPair = l2vpn:peer-ip-address=102.102.102.102
```

The following is sample L2VPN profile configuration:

```
(Username: vpws_pw_customer1)
Cisco-AVPair = l2vpn:member=ethernet-service-instance:Gi2/3 -stag-type:0x8100
-stag-vlan-id:1000
Cisco-AVPair = l2vpn:member=pseudowire:peer-ip:102.102.102.102:vc-id:111111
```

The following is sample RADIUS user profile configuration:

```
RADIUS Profile
User Profile (Username: RouterA:nas-port:2/0/3/0:1000)
Cisco-AVPair = subscriber:sss-service=vpws
Cisco-AVPair = l2vpn:redundancy-group=1
Cisco-AVPair = l2vpn:service-id=vpws_pw_customer1
Cisco-AVPair = ethernet-service-instance:service-instance-description=Dynamic customer 1
Cisco-AVPair = ethernet-service-instance:stag-vlan-id=1000
Cisco-AVPair = ethernet-service-instance:rewrite-ingress=1
Cisco-AVPair = ethernet-service-instance:rewrite-ingress-tag-operation=Pop1
Cisco-AVPair = ethernet-service-instance:rewrite-ingress-symmetric=TRUE
```

You can verify the Layer 2 context configuration on the PE router with the **show interface**command, as follows:

```
Router# show interface gigabit ethernet 2/3
interface GigabitEthernet2/3
 service instance dynamic 90 ethernet
  description L2 context for single-tag FSOL
  encapsulation dot1q 1000-2000
  ethernet subscriber
  initiator unclassified vlan
  service-policy type control DYNAMIC_EVC
```

You can verify the dynamic service instance on the PE router with the **show derived-config** command, as follows:

```
Router# show derived-config interface gigabit ethernet 2/3
interface GigabitEthernet2/3
<Output snipped for clarity>
.
.
 service instance 101 ethernet
  description Dynamic customer 1
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  xconnect 102.102.102.102 111111 encapsulation mpls
```

Example Configuring Double-Sided Dynamic L2VPN VPWS

In the double-sided provisioning model, you must configure both MPLS PE devices.

The following example shows how to configure L2VPN VPWS on the PE1 router:

```
l2 subscriber authorization group atom_test1
 service-policy type control atom_rule1
 peer network 10.10.10.2 255.255.0.0 1 4294967295
```

The following example shows how to configure L2VPN VPWS on the PE2 router:

```
l2 subscriber authorization group atom_test1
 service-policy type control atom_rule1
 peer network 10.10.10.1 255.255.0.0 1 4294967295
```

The following example shows how to verify the Layer 2 context configuration on the PE1 router:

```
Router# show interface gigabit ethernet 2/3
interface GigabitEthernet2/3
 service instance dynamic 90 ethernet
  description L2 context for single-tag FSOL
  encapsulation dot1q 1000-2000
  ethernet subscriber
  initiator unclassified vlan
  service-policy type control DYNAMIC_EVC
```

The following example shows how to verify the Layer 2 context configuration on the PE2 router:

```
Router# show interface gigabit ethernet 2/4
interface GigabitEthernet2/4
 service instance dynamic 90 ethernet
  description L2 context for single-tag FSOL
  encapsulation dot1q 1000-2000
  ethernet subscriber
  initiator unclassified vlan
  service-policy type control DYNAMIC_EVC
```

The following example shows how to verify the dynamic service instance on the PE1 router:

```
Router# show derived-config interface gigabit ethernet 2/3
interface GigabitEthernet2/3
<Output snipped for clarity>
.
.
 service instance 101 ethernet
  description Dynamic customer 1
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  xconnect 10.10.10.2 111111 encapsulation mpls
```

The following example shows how to verify the dynamic service instance on the PE2 router:

```
Router# show derived-config interface gigabit ethernet 2/4
interface GigabitEthernet2/4
<Output snipped for clarity>
.
.
 service instance 102 ethernet
  description Dynamic customer 1
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  xconnect 10.10.10.1 111111 encapsulation mpls
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands: master list of commands with complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Master Commands List, All Releases
Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Carrier Ethernet Command Reference
ISG commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Intelligent Services Gateway Command Reference
AAA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference
Configuring ISG control policies	Configuring ISG Control Policies module
Configuring different types of AAA accounting	Configuring Accounting module

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Dynamic Ethernet Service Activation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Dynamic Ethernet Service Activation

Feature Name	Releases	Feature Information
Dynamic Ethernet Service Activation	15.1(2)S	The DESA feature enables the dynamic provisioning of Layer 2 services and transport using the dynamic policy. The following commands were introduced or modified: **ais**, **authorize identifier**, **continuity-check**, **debug ethernet service**, **debug ethernet service instance dynamic**, **debug idmgr**, **debug mpls l2transport vc subscriber**, **ethernet cfm mip**, **ethernet subscriber**, **ethernet subscriber session**, **ethernet subscriber static**, **initiator unclassified vlan**, **l2 subscriber**, **maximum meps**, **mep mpid**, **mip auto-create**(cfm-srv), **peer**, **pseudowire (**Layer 2**)**, **service evc**, **service_instance_dynamic**, **service-policy type control policy**, **show database data**, **show derived-config**, **show dwnld_mgr**, **show ethernet cfm domain**, **show ethernet cfm maintenance-points local**, **show ethernet service instance**, **show ethernet service dynamic**, **show subscriber session**.