Configuring the Managed IPv6 Layer 2 Tunnel Protocol Network Server

This document describes how to enable the Managed IPv6 Layer 2 Tunnel Protocol Network Server feature.

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 Configuring the Managed IPv6 LNS

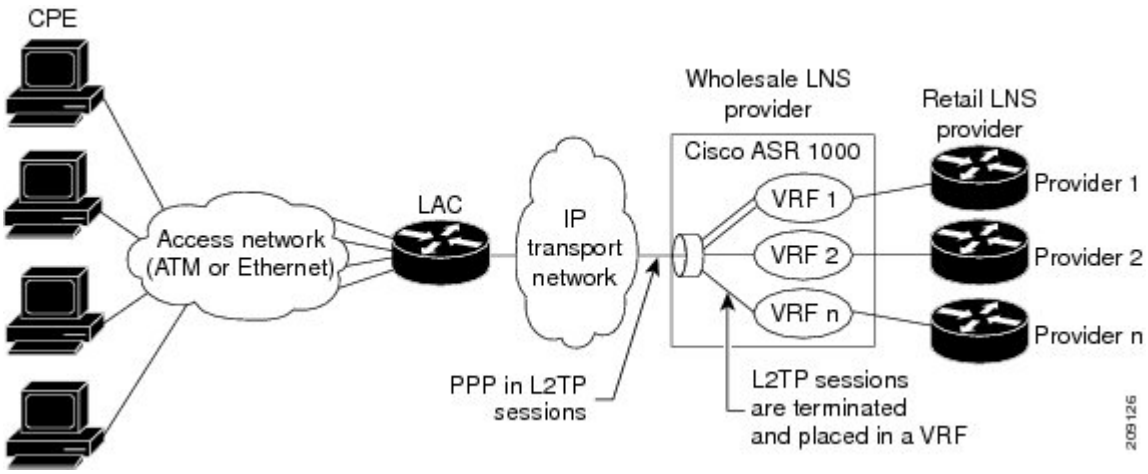
For the router to function as an LNS, you must enable Authentication, Authorization, and Accounting (AAA) on the Layer 2 Tunnel Protocol Network Server (LNS) and the Layer 2 Access Concentrator (LAC), by entering the **aaanew-model** global configuration command. For more information, see the " Authentication, Authorization, and Accounting " chapter in the *Cisco IOS XE Security: Securing User Services Configuration Guide* .

Information About Configuring the Managed IPv6 LNS

L2TP Network Server

The router can function as an LNS. The LNS is a peer to the LAC and sits on one side of an L2TP tunnel. The LNS routes packets to and from the LAC and a destination network. When the router functions as an LNS, you can configure the router to terminate the PPP sessions and route the client IP packets onto the ISP or corporate network toward their final destination (see the figure below). The router can use the Managed IPv6 LNS feature to terminate L2TP sessions from the LAC and place each session into the appropriate IPv6 VRF instance based on the VRF applied to the virtual template interface or alternatively, based on the VRF received for the user through AAA. The router then routes each session within the VRF to the destination network.

Figure 1: Terminating and Forwarding Sessions from the LAC



Tunnel Accounting

The tunnel accounting feature enhances AAA accounting by adding the ability to include tunnel-related statistics in the RADIUS information. Before you can collect tunnel usage information, you must configure the following attributes on the RADIUS server:

- Acct-Tunnel-Connection—Specifies the identifier assigned to the tunnel session. This attribute and the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes provide a way to uniquely identify a tunnel session for auditing purposes.
- Acct-Tunnel-Packets-Lost—Specifies the number of packets lost on a given link.

The table below describes the values for the Acct-Status-Type attribute that support tunnel accounting on the RADIUS server.

Table 1: Acct-Status-Type Values for RADIUS Tunnel Accounting

Acct-Status-Type Values	Value	Description
Tunnel-Link-Reject	14	Marks the rejection of the establishment of a new link in an existing tunnel.
Tunnel-Link-Start	12	Marks the creation of a tunnel link within an L2TP tunnel that carries multiple links.
Tunnel-Link-Stop	13	Marks the destruction of a tunnel link within an L2TP tunnel that carries multiple links.
Tunnel-Reject	11	Marks the rejection of the establishment of a tunnel with another device.
Tunnel-Start	9	Marks the establishment of a tunnel with another device.
Tunnel-Stop	10	Marks the destruction of a tunnel to or from another device.

For more information about the RADIUS tunnel accounting attributes or the Acct-Status-Type values that support RADIUS tunnel accounting, see RFC 2867, RADIUS Accounting Modifications for Tunnel Protocol Support.

For information about RADIUS accounting attributes supported on the Cisco ASR 1000 Series Aggregation Services Routers, see the “RADIUS Attributes” chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.

For more information on configuring RADIUS, see your RADIUS user documentation.

How to Configure the Managed LNS

Configuring a VRF on the LNS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** {**ipv4**|**ipv6**}
6. **route-target** {*import*|*export*|*both*} *route-target-ext-community*
7. **exit-address-family**
8. **address-family** {**ipv4**|**ipv6**}
9. **route-target** {*import*|*export*|*both*} *route-target-ext-community*
10. **end**
11. **show ipv6 route vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Router(config)# vrf definition vrf1`	Configures a VRF routing table and enters VRF configuration mode. • The *vrf-name*argument is the name of the VRF.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF. • The *route-distinguisher* argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher in either of these formats:

	Command or Action	Purpose
		• 16-bit autonomous system number (ASN): your 32-bit number For example, 101:3. • 32-bit IP address: your 16-bit number For example, 192.168.122.15:1.
Step 5	**address-family** {**ipv4**|**ipv6**} **Example:** `Router(config-vrf) address-family ipv6`	Enters VRF address family configuration mode to specify an address family for a VRF. • The **ipv4** keyword specifies an IPv4 address family for a VRF. • The **ipv6** keyword specifies an IPv6 address family for a VRF.
Step 6	**route-target** {*import*|*export*|*both*} *route-target-ext-community* **Example:** `Router(config-vrf-af) route-target both 100:2`	Creates a route-target extended community for a VRF. • The **import** keyword imports routing information from the target VPN extended community. • The **export** keyword exports routing information to the target VPN extended community. • The **both** keyword imports both import and export routing information to the target VPN extended community. • The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities.
Step 7	**exit-address-family** **Example:** `Router(config-vrf-af)# exit-address-family`	Exits VRF address family configuration mode and enters VRF configuration mode.
Step 8	**address-family** {**ipv4**|**ipv6**} **Example:** `Router(config-vrf) address-family ipv6`	Enters VRF address family configuration mode to specify an address family for a VRF. • The **ipv4** keyword specifies an IPv4 address family for a VRF. • The **ipv6** keyword specifies an IPv6 address family for a VRF.
Step 9	**route-target** {*import*|*export*|*both*} *route-target-ext-community* **Example:** `Router(config-vrf-af)# route-target both 100:3`	Creates a route-target extended community for a VRF. • The **import** keyword specifies to import routing information from the target VPN extended community. • The **export** keyword specifies to export routing information to the target VPN extended community. • The **both** keyword specifies to import both import and export routing information to the target VPN extended community.

	Command or Action	Purpose
		• The *route-target-ext-community* argument adds the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities. • Enter the **route-target** command one time for each target community.
Step 10	**end** **Example:** `Router(config-vrf-af)# end`	Exits VRF address family configuration mode and returns to privileged EXEC mode.
Step 11	**show ipv6 route vrf** *vrf-name* **Example:** `Router# show ipv6 route vrf vrf1`	Displays the IPv6 routing table associated with a VRF.

Configuring a Virtual Template Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **vrf forwarding** *name*
5. **ppp authentication chap**
6. **end**
7. **show interfaces virtual-access** *number* **[configuration]**
8. **debug ppp chap**
9. **debug ppp negotiation**
10. **debug ppp negotiation chap**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface and enters interface configuration mode.
Step 4	**vrf forwarding** *name* **Example:** `Router(config-if)# vrf forwarding vpn-1`	(Optional) Maps the virtual template interface to a VRF routing table. **Note** If the VRF assignment is received via the RADIUS server, then this step is not required.
Step 5	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables CHAP authentication on the virtual template interface, which is applied to virtual access interfaces (VAI).
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show interfaces virtual-access** *number* **[configuration]** **Example:** `Router# show interfaces virtual-access number [configuration]`	Displays status, traffic data, and configuration information about the VAI you specify.
Step 8	**debug ppp chap** **Example:** `Router# debug ppp chap`	Displays authentication protocol messages for Challenge Authentication Protocol (CHAP) packet exchanges. • This command is useful when a CHAP authentication failure occurs due to a configuration mismatch between devices. Verifying and correcting any username and password mismatch resolves the problem.

	Command or Action	Purpose
Step 9	**debug ppp negotiation** **Example:** `Router# debug ppp negotiation`	Displays information on traffic and exchanges in an internetwork implementing PPP.
Step 10	**debug ppp negotiation chap** **Example:** `Router# debug ppp negotiation chap`	Deciphers a CHAP negotiation problem due to a connectivity problem between a Cisco and non-Cisco device.

Assigning a VRF via the RADIUS Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization configuration** *method-name* **group** *group-name*
4. **ipv6 dhcp pool** *pool-name*
5. **prefix-delegation aaa** [**method-list***method-list*]
6. **dns-server** *ipv6-address*
7. **exit**
8. **interface virtual-template** *number*
9. **ipv6 nd prefix framed-ipv6-prefix**
10. **ipv6 dhcp server** *pool-name* **rapid-commit**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization configuration** *method-name* **group** *group-name* **Example:** `Router(config)# aaa authorization configuration DHCPv6-PD group DHCPv6-PD-RADIUS`	Downloads configuration information from the AAA server using RADIUS.
Step 4	**ipv6 dhcp pool** *pool-name* **Example:** `Router(config)# ipv6 dhcp pool DHCPv6-PD`	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
Step 5	**prefix-delegation aaa** [**method-list***method-list*] **Example:** `Router(config-dhcpv6)# prefix-delegation aaa method-list DHCPv6-PD`	Specifies that prefixes are to be acquired from AAA servers.
Step 6	**dns-server** *ipv6-address* **Example:** `Router(config-dhcpv6)# dns-server 2001:0DB8:3000:3000::42`	Specifies the Domain Name System (DNS) IPv6 servers available to a DHCP for IPv6 client.
Step 7	**exit** **Example:** `Router(config-dhcpv6)# exit`	Exits DHCP for IPv6 pool configuration mode and enters global configuration mode.
Step 8	**interface virtual-template** *number* **Example:** `Router(config)# interface virtual-template 1`	Creates a virtual template interface that can be configured and applied dynamically in creating VAIs, and enters interface configuration mode.
Step 9	**ipv6 nd prefix framed-ipv6-prefix** **Example:** `Router(config-if)# ipv6 nd prefix framed-ipv6-prefix`	Adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue.

	Command or Action	Purpose
Step 10	**ipv6 dhcp server** *pool-name* **rapid-commit** **Example:** `Router(config-if)# ipv6 dhcp server DHCPv6-PD rapid-commit`	Enables DHCPv6 on an interface.
Step 11	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the LNS to Initiate and Receive L2TP Traffic

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn enable**
4. **vpdn-group** *group-name*
5. **accept-dialin**
6. **protocol l2tp**
7. **virtual-template** *template-number*
8. **exit**
9. **terminate-from hostname** *hostname*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**vpdn enable** **Example:** `Router(config)# vpdn enable`	Enables VPDN networking on the router and informs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway) if one is present.
Step 4	**vpdn-group** *group-name* **Example:** `Router(config)# vpdn-group group1`	Defines a local group name for which you can assign other VPDN variables. • Enters VPDN group configuration mode.
Step 5	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from the LAC and creates an accept-dialin VPDN subgroup. • Enters accept dial-in VPDN subgroup configuration mode.
Step 6	**protocol 12tp** **Example:** `Router(config-vpdn-acc-in)# protocol 12tp`	Specifies the Layer 2 Tunnel Protocol.
Step 7	**virtual-template** *template-number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1`	Specifies the virtual template to be used to clone VAIs.
Step 8	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Returns to VPDN group configuration mode.
Step 9	**terminate-from hostname** *hostname* **Example:** `Router(config-vpdn)# terminate-from hostname lac1-vpn1`	Specifies the hostname of the remote LAC that is required when accepting a VPDN tunnel.
Step 10	**end** **Example:** `Router(config-vpdn)# end`	Exits VPDN configuration mode and returns to privileged EXEC mode.

Limiting the Number of Sessions per Tunnel

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *group-name*
4. **accept-dialin**
5. **protocol 12tp**
6. **virtual-template** *template-number*
7. **exit**
8. **terminate-from hostname** *host-name*
9. **session-limit** *limit-number*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vpdn-group** *group-name* **Example:** `Router(config)# vpdn-group group1`	Defines a local group name for which you can assign other VPDN variables. • Enters VPDN group configuration mode.
Step 4	**accept-dialin** **Example:** `Router(config-vpdn)# accept-dialin`	Configures the LNS to accept tunneled PPP connections from the LAC and creates an accept-dialin VPDN subgroup. • Enters accept dial-in VPDN subgroup configuration mode.
Step 5	**protocol 12tp** **Example:** `Router(config-vpdn-acc-in)# protocol 12tp`	Specifies the Layer 2 Tunnel Protocol.

	Command or Action	Purpose
Step 6	**virtual-template** *template-number* **Example:** `Router(config-vpdn-acc-in)# virtual-template 1`	Specifies the virtual template to be used to clone VAIs.
Step 7	**exit** **Example:** `Router(config-vpdn-acc-in)# exit`	Returns to VPDN group configuration mode.
Step 8	**terminate-from hostname** *host-name* **Example:** `Router(config-vpdn)# terminate-from hostname test_LAC`	Specifies the hostname of the remote LAC that is required when accepting a VPDN tunnel.
Step 9	**session-limit** *limit-number* **Example:** `Router(config-vpdn)# session-limit 100`	Specifies the maximum number of sessions per tunnel.
Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN configuration mode and returns to privileged EXEC mode.

Configuring RADIUS Attribute Accept or Reject Lists

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp default group** *group-name*
4. **aaa authorization network group group** *group-name*
5. **aaa group server radius** *group-name*
6. **server-private** *ip-address* [**acct-port***port-number*][**timeout***seconds*] [**retransmit***retries*] [**key***string*]
7. **authorization** [**accept**|**reject**] *list-name*
8. **exit**
9. **radius-server attribute list** *listname*
10. **attribute** *value1* [*value2* [*value3...*]]
11. **end**
12. **show accounting**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication ppp default group** *group-name* **Example:** `Router(config)# aaa authentication ppp default group radius_authen1`	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	**aaa authorization network group group** *group-name* **Example:** `Router(config)# aaa authorization network group group radius_authen1`	Sets the parameters that restrict network access to the user.

	Command or Action	Purpose
Step 5	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius VPDN-Group`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server group RADIUS configuration mode.
Step 6	**server-private** *ip-address* [**acct-port***port-number*][**timeout***seconds*] [**retransmit***retries*] [**key***string*] **Example:** `Router(config-sg-radius)# server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1`	Configures the IP address of the private RADIUS server for the group server. • The *ip-address*argument specifies the IP address of the private RADIUS server host. • (Optional) The *port-number*argument specifies the UDP destination port for accounting requests. • (Optional) The *seconds* argument specifies the timeout value (1 to 1000). • (Optional) The *retries*argument specifies the number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. • The *string* argument specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server.
Step 7	**authorization** [**accept**|**reject**] *list-name* **Example:** `Router(config-sg-radius)# authorization accept vpn1-autho-list`	Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server. • The **accept** keyword indicates that all attributes will be rejected except the attributes specified in the *listname* argument. • The **reject** keyword indicates that all attributes will be accepted except for the attributes specified in the *listname* argument and all standard attributes.
Step 8	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server group RADIUS configuration mode and enters global configuration mode.
Step 9	**radius-server attribute list** *listname* **Example:** `Router(config)# radius-server attribute list vpn1-autho-list`	Defines the list name given to the set of attributes defined using the **attribute** command and enters RADIUS attribute list configuration mode. • Define the *listname* argument to be the same as you defined it in step 7.
Step 10	**attribute** *value1* [*value2* [*value3...*]]	Adds attributes to the configured accept or reject list.

	Command or Action	Purpose
	Example: `Router(config-radius-attrl)# attribute 26,200`	• You can use this command multiple times to add attributes to an accept or reject list.
Step 11	**end** **Example:** `Router(config-radius-attrl)# end`	Exits RADIUS attribute list configuration mode and returns to privileged EXEC mode.
Step 12	**show accounting** **Example:** `Router# show accounting`	Displays accounting records for users currently logged in. • Displays active accountable events on the network and helps collect information in the event of a data loss on the accounting server.

Configuring AAA Accounting Using Named Method Lists

Note System accounting does not use named method lists. For system accounting you can define only the default method list. For more information, see the "Configuring Accounting" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa accounting network** *list-name* **start-stop group radius**
4. **line** [**aux** | **console**| **vty**] [*line-number*]
5. **accounting** {**arap**|**commands***level*|**connection**|**exec**|**resource**} [**default** | *list-name*]
6. **end**
7. **debug aaa accounting**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa accounting network** *list-name* **start-stop group radius** **Example:** `Router(config)# aaa accounting network methodlist start-stop group radius`	Creates an accounting method list and enables accounting.
Step 4	**line** [**aux** | **console**| **vty**] [*line-number*] **Example:** `Router(config)# line console 0`	Enters line configuration mode for the line to which you want to apply the accounting method list.
Step 5	**accounting** {**arap**|**commands***level*|**connection**|**exec**|**resource**} [**default** | *list-name*] **Example:** `Router(config-line)# accounting commands 15 list1`	Applies the accounting method list to a line or a set of lines.
Step 6	**end** **Example:** `Router(config-line)# end`	Exits line configuration mode and returns to privileged EXEC mode.
Step 7	**debug aaa accounting** **Example:** `Router# debug aaa accounting`	Displays information on accountable events as they occur.

Configuring RADIUS Tunnel Authentication Method Lists on the LNS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network** *list-name method1* [*method2...*]
4. **vpdn tunnel authorization network** *lmethod-ist-name method1* [*method2...*]
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *dummy-password*
7. **debug aaa authorization**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization network** *list-name method1* [*method2...*] **Example:** `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	Sets parameters that restrict user access to a network. • The *list-name* argument is a character string used to name the list of authentication methods tried when a user logs in. • **group radius**: Uses the list of all RADIUS servers for authentication. • **group** *group-name*: Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. • **if-authenticated**: Succeeds if user has been successfully authenticated. • **local**: Uses the local username database for authentication. • **none**: Uses no authentication. **Note** The method list is only for VPDN tunnel authorization and termination, not for domain and Digital Number Identification Service (DNIS) authorization. Therefore, the method list applies only on the tunnel terminator device - the LAC for dialout sessions and the LNS for dialin sessions.

	Command or Action	Purpose
Step 4	**vpdn tunnel authorization network** *lmethod-ist-name method1* [*method2...*] **Example:** `Router(config)# vpdn tunnel authorization network mymethodlist`	Specifies the AAA method list to use for VPDN remote tunnel hostname-based authorization. • If you do not specify a method list (including a default method list) by using the **vpdn tunnel authorization network** command, local authorization occurs by using the local VPDN group configuration.
Step 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* **Example:** `Router(config)# vpdn tunnel authorization virtual-template 10`	Specifies the default virtual template interface used to clone a VAI. • If you do not specify a virtual template interface in the local VPDN group configuration or in a remote RADIUS configuration, then the default virtual template interface is used.
Step 6	**vpdn tunnel authorization password** *dummy-password* **Example:** `Router(config)# vpdn tunnel authorization password mypassword`	Specifies the password to use for the RADIUS authorization request to retrieve the tunnel configuration based on the remote tunnel hostname.
Step 7	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays information on AAA authorization.

Configuring the LNS for RADIUS Tunnel Authentication

Perform the following tasks to configure LNS for RADIUS Tunnel Authentication:

Note Cisco ASR 1000 Series Aggregation Services Routers supports L2TP tunnel authorization. However, RADIUS does not provide attributes for such parameter values as L2TP tunnel timeouts, L2TP tunnel hello intervals, and L2TP tunnel receive window size. When the Cisco ASR 1000 Series Aggregation Services Router does not receive a RADIUS attribute for a parameter, the router uses the default value.

Configuring RADIUS Tunnel Authentication Method Lists on the LNS

To configure method lists on the LNS for RADIUS tunnel authentication, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network** *list-name method1* [*method2...*]
4. **vpdn tunnel authorization network** *method- list-name*
5. **vpdn tunnel authorization virtual-template** *vtemplate-number*
6. **vpdn tunnel authorization password** *dummy-password*
7. **end**
8. **debug aaa authorization**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization network** *list-name method1* [*method2...*] **Example:** `Router(config)# aaa authorization network mymethodlist group VPDN-Group`	Sets parameters that restrict user access to a network • The*list-name*argument is a character string used to name the list of authentication methods tried when a user logs in. • **groupradius—**Uses the list of all RADIUS servers for authentication. • **group***group-name***—**Uses a subset of RADIUS servers for authentication as defined by the **aaagroupserverradius** command. • **if-authenticated—**Succeeds if user has been successfully authenticated. • **local—**Uses the local username database for authentication. • **none—**Uses no authentication. **Note** The method list is only for VPDN tunnel authorization and termination, not for domain and Digital Number Identification Service (DNIS) authorization. Therefore, the method list applies only on the tunnel terminator device—the LAC for dialout sessions and the LNS for dialin sessions.

	Command or Action	Purpose
Step 4	**vpdn tunnel authorization network** *method- list-name* **Example:** `Router(config)# vpdn tunnel authorization network mymethodlist`	Specifies the AAA method list to use for VPDN remote tunnel hostname-based authorization. • If you do not specify a method list (including a default method list) by using the **vpdntunnelauthorizationnetwork** command, local authorization occurs by using the local VPDN group configuration.
Step 5	**vpdn tunnel authorization virtual-template** *vtemplate-number* **Example:** `Router(config)# vpdn tunnel authorization virtual-template 10`	Specifies the default virtual template interface used to clone a VAI. • If you do not specify a virtual template interface in the local VPDN group configuration or in a remote RADIUS configuration, then the default virtual template interface is used. **Note** The **vpdntunnelauthorizationvirtual-template** command is applicable only on the LNS.
Step 6	**vpdn tunnel authorization password** *dummy-password* **Example:** `Router(config)# vpdn tunnel authorization password mypassword`	Specifies the password to use for the RADIUS authorization request to retrieve the tunnel configuration based on the remote tunnel hostname. • By default, the password is cisco, but you can configure a different password. **Note** The **vpdntunnelauthorizationpassword** command is applicable on both the LAC and LNS.
Step 7	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays information on AAA authorization.

Configuring AAA Authentication Methods

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. Configure RADIUS security protocol parameters. For more information about RADIUS, see the "Configuring RADIUS" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services .
5. **aaa authentication**
6. Apply the authentication method lists to an interface, a line, or a set of lines as required. For more information about authentication method lists, see the "Configuring Authentication" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services .
7. **end**

DETAILED STEPS

Step 1 **enable**

Step 2 **configure terminal**

Step 3 **aaa new-model**
Enter this command in global configuration mode to enable AAA.

Step 4 Configure RADIUS security protocol parameters. For more information about RADIUS, see the "Configuring RADIUS" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services .

Step 5 **aaa authentication**
Enter this command to define the authentication method lists.

Step 6 Apply the authentication method lists to an interface, a line, or a set of lines as required. For more information about authentication method lists, see the "Configuring Authentication" chapter in the Cisco IOS XE Security Configuration Guide: Securing User Services .

Step 7 **end**

Configuration Examples for the Managed IPv6 Layer 2 Tunnel Protocol Network Server

Example Managed IPv6 LNS Configuration

The following example shows how to configure Managed IPv6 LNS features on the router. In this example, the router terminates the tunnel from the LAC and associates the VRFs with the interfaces and the virtual

template interfaces. This configuration also shows how to configure RADIUS attribute screening and AAA accounting for the VRFs.

```
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition user_vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv6
 exit-address-family
!
logging buffered 10000000
enable password lab
!
aaa new-model
!
!
aaa group server radius radius_authen1
 server-private 10.1.1.2 acct-port 0 timeout 7 retransmit 3 key cisco1
 ip radius source-interface Loopback20000
!
aaa authentication login default none
aaa authentication ppp default group radius_authen1
aaa authorization network default group radius_authen1
aaa authorization configuration DHCPv6-PD group radius_authen1
!
!
!
!
!
aaa session-id common
aaa policy interface-config allow-subinterface
ppp hold-queue 80000
clock timezone EST -5 0
ip source-route
no ip gratuitous-arps
!
!
!
!
!
!
!
no ip domain lookup
ip host mcp-matrix 10.0.0.2
ip host mcp-sun-2 10.0.0.2
!
!
ipv6 unicast-routing
ipv6 dhcp binding track ppp
ipv6 dhcp pool ipv6_dhcp_pool1
 prefix-delegation aaa method-list DHCPv6-PD
!
!
!
!
multilink bundle-name authenticated
vpdn enable
!
vpdn-group VPDN_LNS1
 accept-dialin
```

```
  protocol l2tp
  virtual-template 1
 terminate-from hostname test_LAC1
 source-ip 10.0.0.2
 local name test_LNS1
 l2tp tunnel password 0 tunnel1
 l2tp tunnel receive-window 100
 l2tp tunnel timeout no-session 30
 l2tp tunnel retransmit retries 7
 l2tp tunnel retransmit timeout min 2
!
!
no virtual-template snmp
!
!
!
!
!
!
!
!
!
username asifp1@test1 password 0 hello1
!
redundancy
 notification-timer 30000
 mode none
!
!
!
!
!
ip tftp source-interface GigabitEthernet 0
!
!
!
!
!
!
!
!
interface Loopback1
 no ip address
!
interface Loopback20000
 ip address 209.165.202.131 255.255.255.224
!
interface GigabitEthernet1/1/0
 mac-address 8888.8888.8888
 no ip address
 load-interval 30
 negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/1/0.1
 encapsulation dot1Q 3
 ip address 209.165.202.132 255.255.255.224
!
interface GigabitEthernet1/1/1
 mac-address 4444.4444.4444
 no ip address
 load-interval 30
 no negotiation auto
 hold-queue 4096 in
 hold-queue 4096 out
!
interface GigabitEthernet1/1/1.1
 vrf forwarding user_vrf1
 encapsulation dot1Q 2
 ipv6 address 12::1/72
!
interface GigabitEthernet1/1/2
```

```
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/3
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/4
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/5
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/6
 no ip address
 negotiation auto
!
interface GigabitEthernet1/1/7
 description Connected to RADIUS
 ip address 209.165.201.1 255.255.255.224
 negotiation auto
!
interface GigabitEthernet1/3/0
 no ip address
 media-type sfp
 negotiation auto
!
interface GigabitEthernet1/3/1
 no ip address
 media-type sfp
 negotiation auto
!
interface GigabitEthernet 0
 vrf forwarding Mgmt-intf
 ip address 209.165.201.1 255.255.255.224
 negotiation auto
!
interface Virtual-Template 1
 no ip address
 no logging event link-status
 ipv6 dhcp server ipv6_dhcp_pool1 rapid-commit
 keepalive 30
 ppp mtu adaptive
 ppp authentication pap
!
ip default-gateway 10.1.0.5
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 209.165.201.1 255.255.255.254 172.16.1.1
ip route vrf Mgmt-intf 209.165.201.29 255.255.255.224 172.16.0.1
!
ip radius source-interface GigabitEthernet1/1/7
logging esm config
cdp run
ipv6 route vrf user_vrf1 ::/0 12::2
!
ipv6 neighbor 12::2 GigabitEthernet1/1/1.1 2222.2222.2222
!
!
!
control-plane
!
call admission limit 90
!
!
!
alias exec call show caller summ
alias exec caller show caller summ
alias exec palt show plat
```

```
alias exec plat show platform
alias exec evsi sho plat hard cpp act feat ess stat
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password password1
!
exception data-corruption buffer truncate
end
```

Example LNS Tunnel Accounting Configuration

The following example shows how to configure the LNS to send tunnel accounting records to the RADIUS server:

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@example.com password 0 lab
username user2@example.com password 0 lab
spe 1/0 1/7
firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname ISP_LAC
local name ENT_LNS
!
isdn switch-type primary-5ess
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
interface Loopback 0
ip address 172.16.0.101 255.255.255.0
!
interface Loopback 1
ip address 192.168.0.101 255.255.255.0
!
interface Ethernet 0
ip address 10.1.26.71 255.255.255.0
no ip mroute-cache
```

```
no cdp enable
!
interface virtual-template 1
ip unnumbered Loopback 0
peer default ip address pool vpdn-pool1
ppp authentication chap
!
interface virtual-template 2
ip unnumbered Loopback1
peer default ip address pool vpdn-pool2
ppp authentication chap
!
interface fastethernet 0
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
ip local pool vpdn-pool1 172.16.5.1 172.16.128.100
ip local pool vpdn-pool2 10.0.0.1 10.0.0.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 192.168.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
!
dialer-list 1 protocol ip permit
no cdp run
!
!
radius-server host 172.16.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
end
```

Note For additional accounting examples, see the “Configuring Accounting” chapter in the Cisco IOS XE Security: Secure Services Configuration Guide .

Example Verifying the User Profile on the RADIUS Server

The following is an example user profile on the RADIUS server. The Cisco ASR 1000 Series Aggregation Services Routers retrieves the information in the user profile from the RADIUS server.

```
Radius Profile "user1"
Auth-Type = Local, User-Password = "pwd"
User-Service-Type = Framed-User
Framed-Protocol = PPP
cisco-avpair = "lcp:interface-config=vrf forwarding VRF01"
cisco-avpair = "lcp:interface-config=ipv6 unnumbered loopback1"
Framed-IPv6-Prefix = "2001:DB8:4567:1234::/64"
Delegated-IPv6-Prefix = "2001:DB8:AAAA::/48"
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS XE MPLS commands	*Cisco IOS MPLS Command Reference*
Authentication, authorization and accounting	Authentication, Authorization, and Accounting (AAA)
Configuring RADIUS	Configuring RADIUS
Configuring accounting	Configuring Accounting
RADIUS attributes	"RADIUS Attributes Overview and RADIUS IETF Attributes" module in the *Cisco IOS XE Security Configuration Guide: Securing User Services*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support

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 Configuring Managed IPv6 Layer 2 Tunnel Protocol Network Server

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 Managed IPv6 Layer 2 Tunnel Protocol Network Server

Feature Name	Releases	Feature Information
Managed IPv6 Layer 2 Tunnel Protocol Network Server	Cisco IOS XE Release 3.3S	The Managed IPv6 LNS feature allows the service provider to offer a scalable end-to-end VPN of both IPv4 and IPv6 service to remote users. This feature integrates the Multiprotocol Label Switching (MPLS)-enabled backbone with broadband access capabilities. The following commands were introduced or modified: atm pppatm passive, radius-server attribute list, radius-server key, radius-server retransmit, radius-server vsa send.

Feature Name	Releases	Feature Information
Managed IPv6 Layer 2 Tunnel Protocol Network Server - VRF-Lite only	Cisco IOS XE Release 3.3S	The Managed IPv6 LNS feature allows the service provider to offer a scalable end-to-end VPN of both IPv4 and IPv6 service to remote users. This feature integrates the VRF-Lite enabled backbone with broadband access capabilities.
Managed IPv6 Layer 2 Tunnel Protocol Network Server - MPLS VPN	Cisco IOS XE Release 3.7S	The Managed IPv6 LNS feature allows the service provider to offer a scalable end-to-end VPN of both IPv4 and IPv6 service to remote users. This feature integrates the MPLS enabled backbone with broadband access capabilities.