Implementing ADSL for IPv6

This module describes the implementation of prefix pools, the authorization, authentication, and accounting (AAA) server, and per-user Remote Access Dial-In User Service (RADIUS) attributes in IPv6. It also describes the deployment of IPv6 in Digital Subscriber Line (DSL) and dial-access environments. Asymmetric Digital Subscriber Line (ADSL) provides the extensions that make large-scale access possible for IPv6 environments, including IPv6 RADIUS attributes, stateless address configuration on Point-to-Point Protocol (PPP) links, per-user static routes, and access control lists (ACLs).

- Finding Feature Information, on page 1
- Restrictions for Implementing ADSL for IPv6, on page 1
- Information About Implementing ADSL for IPv6, on page 2
- How to Configure ADSL in IPv6, on page 9
- Configuration Examples for Implementing ADSL for IPv6, on page 19
- Additional References, on page 21
- Feature Information for Implementing ADSL for IPv6, on page 22

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 Toolland 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.

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.

Restrictions for Implementing ADSL for IPv6

ADSL deployment is available for interfaces with PPP encapsulation enabled, including PPP over ATM (PPPoA), PPP over Ethernet (PPPoE, PPPoEoVLAN, PPPoEoQinQ) and PPPoEoA.

Information About Implementing ADSL for IPv6

Address Assignment for IPv6

A Cisco router configured with IPv6 will advertise its IPv6 prefixes on one or more interfaces, allowing IPv6 clients to automatically configure their addresses. In IPv6, address assignment is performed at the network layer, in contrast to IPv4 where a number of functions are handled in the PPP layer. The only function handled in IPv6 Control Protocol is the negotiation of a unique interface identifier. Everything else, including DNS server discovery, is done within the IPv6 protocol itself.

In IPv6, ISPs assign long-lived prefixes to users, which has some impact on the routing system. In typical IPv4 environments, each network access server (NAS) has a pool of 24-bit addresses and users get addresses from this pool when dialing in. If a user dials another POP or is connected to another NAS at the same POP, a different IPv4 address is assigned.

Addresses for IPv6 are assigned by the following methods.

Stateless Address Autoconfiguration

Assigning addresses using the stateless address autoconfiguration method can be used only to assign 64-bit prefixes. Each user is assigned a 64-bit prefix, which is advertised to the user in a router advertisement (RA). All addresses are automatically configured based on the assigned prefix.

A typical scenario is to assign a separate 64-bit prefix per user; however, users can also be assigned a prefix from a shared pool of addresses. Using the shared pool limits addresses to only one address per user.

This method works best for the cases where the customer provider edge (CPE) router is a single PC or is limited to only one subnet. If the user has multiple subnets, Layer 2 (L2) bridging, multilink subnets or proxy RA can be used. The prefix advertised in the RA can come from an authorization, authentication, and accounting (AAA) server, which also provides the prefix attribute, can be manually configured, or can be allocated from a prefix pool.

The Framed-Interface-Id AAA attribute influences the choice of interface identifier for peers and, in combination with the prefix, the complete IPv6 address can be determined.

Prefix Delegation

An IPv6 prefix delegating device selects IPv6 prefixes to be assigned to a requesting device upon receiving a request from the client. The delegating device might select prefixes for a requesting device in the following ways:

- Dynamic assignment from a pool of available prefixes.
- Dynamic assignment from a pool name obtained from the RADIUS server.
- Assignment of prefix obtained from the RADIUS sever.

Contrary to IPv4 address assignment, an IPv6 user will be assigned a prefix, not a single address. Typically the Internet service provider (ISP) assigns a 64- or 48-bit prefix.

Accounting Start and Stop Messages

PPP calls a registry to allow DHCPv6 to append the delegated prefix information to accounting start and stop messages. When accounting is configured for a DHCPv6 pool, accounting interim packets are sent to broadband sessions after binding is provided from the pool.

Forced Release of a Binding

The DHCPv6 server maintains an automatic binding table in memory to track the assignment of some configuration parameters, such as prefixes between the server and its clients. The automatic bindings can be stored permanently in the database agent, which can be, for example, a remote TFTP server or local NVRAM file system.

DHCPv6 invokes a routine when the virtual interface used by PPP terminates. This routine automatically releases any delegated prefix bindings associated with the PPP virtual interface that is being terminated.

When a PPP virtual interface terminates, the routine runs through the full table of DHCPv6 bindings checking for the matching interface. Because PPP uses a virtual interface, this subroutine clears any related lease information when the PPP connection terminates.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using the **ipv6 dhcp binding track ppp** command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

DHCP SIP Server Options

Two DHCP for IPv6 Session Initiation Protocol (SIP) server options describe a local outbound SIP proxy: one carries a list of domain names, the other a list of IPv6 addresses. These two options can be configured in a DHCPv6 configuration pool.

AAA over IPv6

Vendor-specific attributes (VSAs) are used to support Authentication, Authorization and Accounting(AAA) over IPv6. Cisco VSAs are inacl, outacl, prefix, and route.

You can configure prefix pools and pool names by using the AAA protocol. Customers can deploy an IPv6 RADIUS server or a TACACS+ server to communicate with Cisco devices.

AAA Support for IPv6 RADIUS Attributes

The following RADIUS attributes, as described in RFC 3162, are supported for IPv6:

- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- Login-IPv6-Host

The following RADIUS attributes are also supported for IPv6:

- Delegated-IPv6-Prefix (RFC 4818)
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route

The attributes listed above can be configured on a RADIUS server and downloaded to access servers, where they can be applied to access connections.

Prerequisites for Using AAA Attributes for IPv6

AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162.

RADIUS Per-User Attributes for Virtual Access in IPv6 Environments

The following IPv6 RADIUS attributes are supported for virtual access and can be used as attribute-value (AV) pairs:

- Delegated-IPv6-Prefix
- Delegated-IPv6-Prefix-Pool
- DNS-Server-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Pool
- Framed-IPv6-Prefix
- Framed-IPv6-Route
- IPv6 ACL
- IPv6_DNS_Servers
- IPv6 Pool
- IPv6 Prefix#
- IPv6 Route
- Login-IPv6-Host

Delegated-IPv6-Prefix

The Delegated-IPv6-Prefix attribute indicates an IPv6 prefix to be delegated to a user for use in a network. This attribute is used during DHCP prefix delegation between a RADIUS server and a delegating device. A Network Access Server (NAS) that hosts a DHCP Version 6 (DHCPv6) server can act as a delegating device.

The following example shows how to use the Delegated-IPv6-Prefix attribute:

```
ipv6:delegated-prefix=2001:DB8::/64
```

Note The Cisco VSA format is not supported for this attribute. If you try to add this attribute in the Cisco VSA format into a user profile, the RADIUS server response fails. Use only the IETF attribute format for this attribute.

Delegated-IPv6-Prefix-Pool

The Delegated-IPv6-Prefix-Pool attribute indicates the name of a prefix pool from which a prefix is selected and delegated to a device.

Prefix delegation is a DHCPv6 option for delegating IPv6 prefixes. Prefix delegation involves a delegating device that selects a prefix and assigns it on a temporary basis to a requesting device. A delegating device uses many strategies to choose a prefix. One method is to choose a prefix from a prefix pool with a name that is defined locally on a device.

The Delegated-IPv6-Prefix-Pool attribute indicates the name of an assigned prefix pool. A RADIUS server uses this attribute to communicate the name of a prefix pool to a NAS hosting a DHCPv6 server and acting as a delegating device.

You may use DHCPv6 prefix delegation along with ICMPv6 stateless address autoconfiguration (SLAAC) on a network. In this case, both the Delegated-IPv6-Prefix-Pool attribute and the Framed-IPv6-Pool attribute may be included within the same packet. To avoid ambiguity, the Delegated-IPv6-Prefix-Pool attribute should be restricted to the authorization and accounting of prefix pools used in DHCPv6 delegation, and the Framed-IPv6-Pool attribute should be used for the authorization and accounting of prefix pools used in SLAAC.

The following example shows how an address prefix is selected from a pool named pool1. The prefix pool pool1 is downloaded to a delegating device from a RADIUS server by using the Delegated-IPv6-Prefix-Pool attribute. The device then selects the address prefix 2001:DB8::/64 from this prefix pool.

```
Cisco:Cisco-AVpair = "ipv6:delegated-ipv6-pool = pool1"
!
ipv6 dhcp pool pool1
address prefix 2001:DB8::/64
!
```

DNS-Server-IPv6-Address

The DNS-Server-IPv6-Address attribute indicates the IPv6 address of a Domain Name System (DNS) server. A DHCPv6 server can configure a host with the IPv6 address of a DNS server. The IPv6 address of the DNS server can also be conveyed to the host using router advertisement messages from ICMPv6 devices.

A NAS may host a DHCPv6 server to handle DHCPv6 requests from hosts. The NAS may also act as a device that provides router advertisement messages. Therefore, this attribute is used to provide the NAS with the IPv6 address of the DNS server.

If a NAS has to announce more than one recursive DNS server to a host, this attribute can be included multiple times in Access-Accept packets sent from the NAS to the host.

The following example shows how you can define the IPv6 address of a DNS server by using the DNS-Server-IPv6-Address attribute:

```
Cisco:Cisco-AVpair = "ipv6:ipv6-dns-servers-addr=2001:DB8::"
```

Framed-Interface-Id

The Framed-Interface-Id attribute indicates an IPv6 interface identifier to be configured for a user.

This attribute is used during IPv6 Control Protocol (IPv6CP) negotiations of the Interface-Identifier option. If negotiations are successful, the NAS uses this attribute to communicate a preferred IPv6 interface identifier to the RADIUS server by using Access-Request packets. This attribute may also be used in Access-Accept packets.

Framed-IPv6-Pool

The Framed-IPv6-Pool attribute indicates the name of a pool that is used to assign an IPv6 prefix to a user. This pool should be either defined locally on a device or defined on a RADIUS server from where pools can be downloaded.

Framed-IPv6-Prefix

The Framed-IPv6-Prefix attribute indicates an IPv6 prefix (and a corresponding route) to be configured for a user. So this attribute performs the same function as a Cisco VSA and is used for virtual access only. A NAS uses this attribute to communicate a preferred IPv6 prefix to a RADIUS server by using Access-Request packets. This attribute may also be used in Access-Accept packets and can appear multiple times in these packets. The NAS creates a corresponding route for the prefix.

This attribute is used by a user to specify which prefixes to advertise in router advertisement messages of the Neighbor Discovery Protocol.

This attribute can also be used for DHCPv6 prefix delegation, and a separate profile must be created for a user on the RADIUS server. The username associated with this separate profile has the suffix “-dhcpv6”.

The Framed-IPv6-Prefix attribute is treated differently in this separate profile and the regular profile of a user. If a NAS needs to send a prefix through router advertisement messages, the prefix is placed in the Framed-IPv6-Prefix attribute of the regular profile of the user. If a NAS needs to delegate a prefix to the network of a remote user, the prefix is placed in the Framed-IPv6-Prefix attribute of the separate profile of the user.

Note The RADIUS IETF attribute format and the Cisco VSA format are supported for this attribute.

Framed-IPv6-Route

The Framed-IPv6-Route attribute indicates the routing information to be configured for a user on a NAS. This attribute performs the same function as a Cisco VSA. The value of the attribute is a string and is specified by using the **ipv6 route** command.

IPv6 ACL

The IPv6 ACL attribute is used to specify a complete IPv6 access list. The unique name of an access list is generated automatically. An access list is removed when the respective user logs out. The previous access list on the interface is then reapplied.

The inacl and outacl attributes enable you to specify an existing access list configured on a device. The following example shows how to define an access list identified with number 1:

```
cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:outacl#1=deny 2001:DB8::/10",
```

IPv6_DNS_Servers

The IPv6_DNS_Servers attribute is used to send up to two DNS server addresses to the DHCPv6 server. The DNS server addresses are saved in the interface DHCPv6 subblock and override other configurations in the DHCPv6 pool. This attribute is also included in attributes returned for AAA start and stop notifications.

IPv6 Pool

The IPv6 Pool attribute extends the IPv4 address pool attribute to support the IPv6 protocol for RADIUS authentication. This attribute specifies the name of a local pool on a NAS from which a prefix is chosen and used whenever PPP is configured and the protocol is specified as IPv6. The address pool works with local pooling and specifies the name of a local pool that is preconfigured on the NAS.

IPv6 Prefix#

The IPv6 Prefix# attribute indicates which prefixes to advertise in router advertisement messages of the Neighbor Discovery Protocol. When this attribute is used, a corresponding route (marked as a per-user static route) is installed in the routing information base (RIB) tables for a given prefix.

The following example shows how to specify which prefixes to advertise:

```
cisco-avpair = "ipv6:prefix#1=2001:DB8::/64",
cisco-avpair = "ipv6:prefix#2=2001:DB8::/64",
```

IPv6 Route

The IPv6 Route attribute is used to specify a static route for a user. A static route is appropriate when Cisco software cannot dynamically build a route to the destination. See the **ipv6 route** command for more information about building static routes.

The following example shows how to use the IPv6 Route attribute to define a static route:

```
cisco-avpair = "ipv6:route#1=2001:DB8:cc00:1::/48",
cisco-avpair = "ipv6:route#2=2001:DB8:cc00:2::/48",
```

Login-IPv6-Host

The Login-IPv6-Host attribute indicates IPv6 addresses of hosts with which to connect a user when the Login-Service attribute is included. A NAS uses the Login-IPv6-Host attribute in Access-Request packets to communicate to a RADIUS server that it prefers to use certain hosts.

PPP IPv6 Accounting Delay Enhancements

This feature enhances accounting records for dual-stack networks. It ensures that a unique IPv6 address is assigned to PPP IPv6 and IPv4 sessions for IP addresses that are received from RADIUS.

When this feature is enabled, it automatically creates a database to hold new incoming access-accept responses from RADIUS. The access-accept responses in this database are then checked for duplicates of a specific set of attributes. If the attributes are already present in the database, then the RADIUS server has already offered them to an existing session; therefore, the new session is immediately removed and a stop-record message sent. If none of the specific set of attributes are in the database, they are immediately added to the database, and the session proceeds normally. When the session is removed, the entries in the database are also removed.

The following RADIUS attributes are tracked in the database and checked at access-accept time:

- Framed-IPv6-Prefix
- Delegated-IPv6-Prefix

The attributes are available as standard RFC-defined binary format, or as Cisco VSAs. (The Delegated-IPv6-Prefix attribute currently does not have a VSA definition in AAA.)

TACACS+ Over an IPv6 Transport

An IPv6 server can be configured to use TACACS+. Both IPv6 and IPv4 servers can be configured to use TACACS+ using a name instead of an IPv4 or IPv6 address.

IPv6 Prefix Pools

The function of prefix pools in IPv6 is similar to that of address pools in IPv4. The main difference is that IPv6 assigns prefixes rather than single addresses.

As in IPv4, a pool or a pool definition in IPv6 can be configured locally or it can be retrieved from an AAA server. Overlapping membership between pools is not permitted.

Once a pool is configured, it cannot be changed. If you change the configuration, the pool will be removed and re-created. All prefixes previously allocated will be freed.

Prefix pools can be defined so that each user is allocated a 64-bit prefix or so that a single prefix is shared among several users. In a shared prefix pool, each user may receive only one address from the pool.

Broadband IPv6 Counter Support at LNS

This feature provides support for broadband PPP IPv6 sessions at the layer 2 tunneling protocol (L2TP) network server (LNS). The sessions are forwarded by L2TP access concentrator (LAC) using layer 2 tunneling protocol L2TP over IPv6.

This feature is enabled automatically when the user configures LNS and enables IPv6.

How to Configure ADSL in IPv6

Configuring the NAS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. **aaa new-model**
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authorization configuration default** {**radius** | **tacacs+**
7. **show ipv6 route** [*ipv6-address* | *ipv6-prefix / prefix-length* | *protocol* | *interface-type interface-number*
8. **virtual-profile virtual-template** *number*
9. **interface serial** *controller-number* **:** *timeslot*
10. **encapsulation** *encapsulation-type*
11. **exit**
12. **dialer-group** *group-number*
13. **ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]
14. **interface virtual-template** *number*
15. **ipv6 enable**
16. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
17. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*

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	**hostname** *name* **Example:**	Specifies the hostname for the network server.

	Command or Action	Purpose
	`Router(config)# hostname cust1-53a`	
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA server.
Step 5	**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Router(config)# aaa authentication ppp default if-needed group radius`	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
Step 6	**aaa authorization configuration default** {**radius** | **tacacs+** **Example:** `Router(config)# aaa authorization configuration default radius`	Downloads configuration information from the AAA server.
Step 7	**show ipv6 route** [*ipv6-address* | *ipv6-prefix* / *prefix-length* | *protocol* | *interface-type interface-number* **Example:** `Router(config)# show ipv6 route`	Shows the routes installed by the previous commands.
Step 8	**virtual-profile virtual-template** *number* **Example:** `Router(config)# virtual-profile virtual-template 1`	Enables virtual profiles by virtual interface template.
Step 9	**interface serial** *controller-number* **:** *timeslot* **Example:** `Router(config)# interface serial 0:15`	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, channel-associated signaling, or robbed-bit signaling). This command also puts the router into interface configuration mode.
Step 10	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation ppp`	Sets the encapsulation method used by the interface.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 12	**dialer-group** *group-number* **Example:** `Router(config)# dialer-group 1`	Controls access by configuring an interface to belong to a specific dialing group.
Step 13	**ppp authentication** *protocol1* [*protocol2...*] [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**] **Example:** `Router(config)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
Step 14	**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 virtual access interfaces.
Step 15	**ipv6 enable** **Example:** `Router(config)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 16	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*} **Example:** `Router(config)# dialer-list 1 protocol ipv6 permit`	Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list.
Step 17	**radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds* **Example:** `Router(config)# radius-server host 172.17.250.8 auth-port 1812 acct-port 1813 key testing123`	Specifies a RADIUS server host.

Enabling the Sending of Accounting Start and Stop Messages

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **accounting** *mlist*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.
Step 4	**accounting** *mlist* **Example:** `Device(config-dhcp)# accounting list1`	Enables accounting start and stop messages to be sent.

Removing Delegated Prefix Bindings

Perform this task to release any delegated prefix bindings associated with the PPP virtual interface that is being terminated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp bindings track ppp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface VirtualAccess2.2`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 dhcp bindings track ppp** **Example:** `Device(config-if)# ipv6 dhcp bindings track ppp`	Releases any delegated prefix leases associated with the PPP virtual interface that is being terminated.

Configuring DHCPv6 AAA Options

Perform the following task to configure the option of acquiring prefixes from the AAA server:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *pool-name*
4. **prefix-delegation aaa** [**method-list** *method-list*] [*lifetime*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *pool-name* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters IPv6 DHCP pool configuration mode.
Step 4	**prefix-delegation aaa** [**method-list** *method-list*] [*lifetime*] **Example:** `Device(config-dhcpv6)# prefix-delegation aaa method-list list1`	Specifies that prefixes are to be acquired from AAA servers.
Step 5	**end** **Example:** `Device(config-dhcpv6)# end`	Exits IPv6 DHCP pool configuration mode and returns to privileged EXEC mode.

Configuring PPP IPv6 Accounting Delay Enhancements

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ppp unique address access-accept**

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	**ppp unique address access-accept** **Example:** `Router(config)# ppp unique address access-accept`	Tracks duplicate addresses received from RADIUS and creates a standalone database.

Configuring TACACS+ over IPv6

Configuring the TACACS+ Server over IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tacacs server** *name*
4. **address ipv6** *ipv6-address*
5. **key** [**0** | **7**] *key-string*
6. **port** [*number*
7. **send-nat-address**
8. **single-connection**
9. **timeout** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**tacacs server** *name* **Example:** `Device(config)# tacacs server server1`	Configures the TACACS+ server for IPv6 and enters TACACS+ server configuration mode.
Step 4	**address ipv6** *ipv6-address* **Example:** `Device(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5`	Configures the IPv6 address of the TACACS+ server.
Step 5	**key** [**0** | **7**] *key-string* **Example:** `Device(config-server-tacacs)# key 0 key1`	Configures the per-server encryption key on the TACACS+ server.
Step 6	**port** [*number* **Example:** `Device(config-server-tacacs)# port 12`	Specifies the TCP port to be used for TACACS+ connections.
Step 7	**send-nat-address** **Example:** `Device(config-server-tacacs)# send-nat-address`	Sends a client's post-NAT address to the TACACS+ server.
Step 8	**single-connection** **Example:** `Device(config-server-tacacs)# single-connection`	Enables all TACACS packets to be sent to the same server using a single TCP connection.
Step 9	**timeout** *seconds* **Example:** `Device(config-server-tacacs)# timeout 10`	Configures the time to wait for a reply from the specified TACACS server.

Specifying the Source Address in TACACS+ Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 tacacs source-interface** *type number*

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	**ipv6 tacacs source-interface** *type number* **Example:** `Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0`	Specifies an interface to use for the source address in TACACS+ packets.

Configuring TACACS+ Server Group Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server tacacs+** *group-name*
4. **server name** *server-name*
5. **server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server tacacs+** *group-name* **Example:** `Device(config)# aaa group server tacacs+ group1`	Groups different TACACS+ server hosts into distinct lists and distinct methods.
Step 4	**server name** *server-name* **Example:** `Device(config-sg-tacacs+)# server name server1`	Specifies an IPv6 TACACS+ server.
Step 5	**server-private** {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] **Example:** `Device(config-sg-tacacs+)# server-private 2001:DB8:3333:4::5 port 19 key key1`	Configures the IPv6 address of the private TACACS+ server for the group server.

Verifying Broadband IPv6 Counter Support at the LNS

This feature is enabled automatically when the user configures LNS and enables IPv6. To verify information about this feature, you can use any or all of the following optional commands as needed.

SUMMARY STEPS

1. **enable**
2. **show l2tp session** [**all** | **packets** [**ipv6**] | **sequence** | **state** | [**brief** | **circuit** | **interworking**] [**hostname**]] [**ip-addr** *ip-addr*[**vcid** *vcid*] | **tunnel**{**id** *local-tunnel-id local-session-id*| **remote-name** *remote-tunnel-name local-tunnel-name*}| **username** *username* | **vcid** *vcid*]
3. **show l2tp tunnel** [**all** | **packets** [**ipv6**] | **state** | **summary** | **transport**] [**id** *local-tunnel-id* | **local-name** *local-tunnel-name remote-tunnel-name*| **remote-name** *remote-tunnel-name local-tunnel-name*]
4. **show l2tun session** [**l2tp** | **pptp**] [**all** [*filter*] | **brief** [*filter*] [**hostname**] | **circuit** [*filter*] [**hostname**] | **interworking** [*filter*] [**hostname**] | **packets ipv6**] [*filter*] | **sequence** [*filter*] | **state** [*filter*]]
5. **show vpdn session** [**l2f** | **l2tp** | **pptp**] [**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]]
6. **show vpdn tunnel** [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets ipv6**] [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport**[*filter*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**show l2tp session** [**all** | **packets** [**ipv6**] | **sequence** | **state** | [**brief** | **circuit** | **interworking**] [**hostname**]] [**ip-addr** *ip-addr*[**vcid** *vcid*] | **tunnel**{**id** *local-tunnel-id local-session-id*| **remote-name** *remote-tunnel-name local-tunnel-name*}| **username** *username* | **vcid** *vcid*] **Example:** `Router# show l2tp session packets ipv6`	Displays information about L2TP sessions.
Step 3	**show l2tp tunnel** [**all** | **packets** [**ipv6**] | **state** | **summary** | **transport**] [**id** *local-tunnel-id* | **local-name** *local-tunnel-name remote-tunnel-name*| **remote-name** *remote-tunnel-name local-tunnel-name*] **Example:** `Router# show l2tp tunnel packets ipv6`	Displays details about L2TP tunnels.
Step 4	**show l2tun session** [**l2tp** | **pptp**] [**all** [*filter*] | **brief** [*filter*] [**hostname**] | **circuit** [*filter*] [**hostname**] | **interworking** [*filter*] [**hostname**] | **packets ipv6**] [*filter*] | **sequence** [*filter*] | **state** [*filter*]] **Example:** `Router# show l2tun session packets ipv6`	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
Step 5	**show vpdn session** [**l2f** | **l2tp** | **pptp**] [**all** | **packets** [**ipv6**] | **sequence** | **state** [*filter*]] **Example:** `Router# show vpdn session packets ipv6`	Displays session information about active Layer 2 sessions for a virtual private dialup network (VPDN).
Step 6	**show vpdn tunnel** [**l2f** | **l2tp** | **pptp**] [**all** [*filter*] | **packets ipv6**] [*filter*] | **state** [*filter*] | **summary** [*filter*] | **transport**[*filter*]] **Example:** `Router# show vpdn tunnel packets ipv6`	Displays information about active Layer 2 tunnels for a VPDN.

Configuration Examples for Implementing ADSL for IPv6

Example NAS Configuration

This configuration for the ISP NAS shows the configuration that supports access from the remote CE router.

```
hostname hostname1
  aaa new-model
  aaa authentication ppp default if-needed group radius
  aaa authorization network default

  aaa accounting network default start-stop group radius

  aaa accounting send counters ipv6

  interface virtual-template 1

  ip unnumbered loopback interface1

  ipv6 address autoconfig

  no ipv6 nd ra suppress
  ppp authentication chap

  ppp accounting list1

  no snmp trap link-status

  no logging event link-status

  exit

  aaa group service radius group1

  server-private 10.1.1.1 timeout 5 retransmit 3 key xyz

  radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646

  radius-server vsa send accounting

  radius-server vsa send authentication
```

Example RADIUS Configuration

This RADIUS configuration shows the definition of AV pairs to establish the static routes.

```
  campus1 Auth-Type = Local, Password = "mypassword"
```

```
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ipv6:inacl#1=permit dead::/64 any",
cisco-avpair = "ipv6:route=library::/64",
cisco-avpair = "ipv6:route=cafe::/64",
cisco-avpair = "ipv6:prefix=library::/64 0 0 onlink autoconfig",
cisco-avpair = "ipv6:prefix=cafe::/64 0 0 onlink autoconfig",
cisco-avpair = "ip:route=10.0.0.0 255.0.0.0",
```

Examples: Verifying Broadband IPv6 Counter Support at the LNS

Example: show l2tp session Command

The **show l2tp session** command used with the **packets and ipv6**keywords displays information about IPv6 packets and byte counts in an L2TP session.

```
Router# show l2tp session packets ipv6


L2TP Session Information Total tunnels 1 sessions 1


LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out

16791      53352      27723      30301740   30301742   20159754280 20523375360
```

Example: show l2tp tunnel Command

The **show l2tp tunnel** command used with the **packets** and **ipv6** keywords displays information about IPv6 packet statistics and byte counts in L2TP tunnels.

```
Router# show l2tp tunnel packets ipv6
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID   Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
27723      63060379   63060383   39400320490 40157045438
```

Example: show l2tun session Command

The **show l2tun session** command used with the **packets**and **ipv6**keywords displays information about IPv6 packet statistics and byte counts in an L2TUN session.

```
Router# show l2tun session packets ipv6
L2TP Session Information Total tunnels 1 sessions 1
LocID      RemID      TunID      Pkts-In    Pkts-Out   Bytes-In   Bytes-Out
16791      53352      27723      31120707   31120708   21285014938 21658462236
```

Example: show vpdn session Command

The **show vpdn session** command used with the **l2tp**, **packets**, and **ipv6**keywords displays session information about IPv6 packet statistics and byte counts in an active layer 2 session for a VPDN.

```
Router# show vpdn session l2tp packets ipv6
```

```
L2TP Session Information Total tunnels 1 sessions 1
LocID       RemID       TunID       Pkts-In     Pkts-Out    Bytes-In    Bytes-Out
16791       53352       27723       35215536    35215538    22616342688 23038929320
```

Example: show vpdn tunnel Command

The **show vpdn tunnel**command used with the **l2tp**, **packets**, and **ipv6**keywords displays session information about IPv6 packet statistics and byte counts in an active layer 2 tunnel for a VPDN.

```
Device# show vpdn tunnel l2tp packets ipv6
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID    Pkts-In     Pkts-Out    Bytes-In    Bytes-Out
27723       61422447    61422451    37149801922 37886871686
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 supported feature list	" Start Here: Cisco IOS XE Software Release Specifics for IPv6 Features ," *Cisco IOS XE IPv6 Configuration Guide*
IPv6 basic connectivity	" Implementing IPv6 Addressing and Basic Connectivity, " *Cisco IOS XE IPv6 Configuration Guide*
DHCP for IPv6	" Implementing DHCP for IPv6, " *Cisco IOS XE IPv6 Configuration Guide*
IPv6 commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IPv6 Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
None	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

RFCs	Title
RFC 3162	*RADIUS and IPv6*
RFC 3177	*IAB/IESG Recommendations on IPv6 Address*
RFC 3319	*Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiated Protocol (SIP) Servers*

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 Implementing ADSL for IPv6

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 1: Feature Information for Implementing ADSL for IPv6

Feature Name	Releases	Feature Information
Enhanced IPv6 Features for ADSL and Dial Deployment	Cisco IOS XE Release 2.5	Several features were enhanced to enable IPv6 to use ADSL and dial deployment.
AAA Support for Cisco VSA IPv6 Attributes	Cisco IOS XE Release 2.5	Vendor-specific attributes (VSAs) were developed to support AAA for IPv6.
IPv6 Access Services: PPPoE	Cisco IOS XE Release 2.5	ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoE.
AAA Support for RFC 3162 IPv6 RADIUS Attributes	Cisco IOS XE Release 2.5	The AAA attributes for IPv6 are compliant with RFC 3162 and require a RADIUS server capable of supporting RFC 3162. The following commands were modified by this feature: **ipv6 dhcp pool**, prefix-delegation aaa

Feature Name	Releases	Feature Information
DHCP - DHCPv6 Prefix Delegation RADIUS VSA	Cisco IOS XE Release 2.5	When the user requests a prefix from the prefix delegator, typically the NAS, the prefix is allocated using DHCPv6.
PPP Enhancement for Broadband IPv6	Cisco IOS XE Release 2.5	The following sections provide information about this feature.
AAA Improvements for Broadband IPv6	Cisco IOS XE Release 2.5	
DHCP Enhancements to Support IPv6 Broadband Deployments	Cisco IOS XE Release 2.5	
PPPoA	Cisco IOS XE Release 3.3S	ADSL and dial deployment is available for interfaces with PPP encapsulation enabled, including PPPoA.
SSO - PPPoE IPv6	Cisco IOS XE Release 2.5	This feature is supported in Cisco IOS XE Release 2.5.
Broadband IPv6 Counter Support at LNS	Cisco IOS XE Release 2.6	This feature provides support for broadband PPP IPv6 sessions at the L2TP LNS. The sessions are forwarded by LAC using layer 2 tunneling protocol L2TP over IPv4. The following commands were modified by this feature: **show l2tp session**, **show l2tp tunnel**, **show l2tun session**, **show vpdn session**, **show vpdn tunnel**.
PPP IPv6 Accounting Delay Enhancements	Cisco IOS XE Release 3.2S	This feature enhances accounting records for dual-stack networks. It ensures that a unique IPv6 address is assigned to PPP IPv6 and IPv4 sessions for IP addresses that are received from RADIUS. The following command was introduced by this feature: **debug ppp unique address**, **ppp unique address access-accept**
RADIUS over IPv6	Cisco IOS XE Release 3.2S	RADIUS over IPv6 is supported.
TACACS+ over IPv6	Cisco IOS XE Release 3.2S	TACACS+ over IPv6 is supported. The following commands were introduced or modified by this feature: **aaa group server tacacs+**, **address ipv6 (TACACS+)**, **ipv6 tacacs source-interface**, **key (TACACS+)**, **port (TACACS+)**, **send-nat-address**, **server name (IPv6 TACACS+)**, **server-private (TACACS+)**, **single-connection**, **tacacs server**, **timeout (TACACS+)**.