

AAA Support for IPv6

Authentication, authorization, and accounting (AAA) support for IPv6 is in compliance with RFC 3162. This module provides information about how to configure AAA options for IPv6.

- Information About AAA Support for IPv6, on page 1
- How to Configure AAA Support for IPv6, on page 5
- Configuration Examples for AAA Support for IPv6, on page 6
- Additional References, on page 7
- Feature Information for RADIUS over IPv6, on page 8

Information About AAA Support for IPv6

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.

How to Configure AAA Support for IPv6

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

Procedure

	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.

Configuration Examples for AAA Support for IPv6

Example: DHCPv6 AAA Options Configuration

The following example shows how to configure the DHCPv6 option of acquiring prefixes from the AAA server:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
```

```
Device(config-dhcpv6)# prefix-delegation aaa method-list list1
Device(config-dhcpv6)# end
```

Example: RADIUS Configuration

The following sample RADIUS configuration shows the definition of AV pairs to establish static routes:

```
campus1 Auth-Type = Local, Password = "mypassword"
                User-Service-Type = Framed-User,
                Framed-Protocol = PPP,
                cisco-avpair = "ipv6:inacl#1=permit 2001:DB8:1::/64 any",
                cisco-avpair = "ipv6:route=2001:DB8:2::/64",
                cisco-avpair = "ipv6:route=2001:DB8:3::/64",
                cisco-avpair = "ipv6:prefix=2001:DB8:2::/64 0 0 onlink autoconfig",
                cisco-avpair = "ipv6:prefix=2001:DB8:3::/64 0 0 onlink autoconfig",
                cisco-avpair = "ip:route=10.0.0.0 255.0.0.0",
```

Additional References

Related Documents

Related Topic	Document Title
Using the **time-range** command to establish time ranges	The chapter *Performing Basic System Management* in the *Cisco IOS XE Network Management Configuration Guide*
Network management command descriptions	*Cisco IOS Network Management Command Reference*

Standards

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

MIBs

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

RFCs

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

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 RADIUS over 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 RADIUS over IPv6

Feature Name	Releases	Feature Information
RADIUS over IPv6	15.1(1)SY	RADIUS attributes defined in RFC 3162 are supported.