



Multicast User Authentication and Profile Support

- [Restrictions for Multicast User Authentication and Profile Support, on page 1](#)
- [Information About Multicast User Authentication and Profile Support, on page 1](#)
- [How to Configure Multicast User Authentication and Profile Support, on page 2](#)
- [Configuration Examples for Multicast User Authentication and Profile Support, on page 4](#)
- [Additional References for IPv6 Services: AAAA DNS Lookups, on page 4](#)
- [Feature Information for Multicast User Authentication and Profile Support, on page 5](#)

Restrictions for Multicast User Authentication and Profile Support

The port, interface, VC, or VLAN ID is the user or subscriber identity. User identity by hostname, user ID, or password is not supported.

Information About Multicast User Authentication and Profile Support

IPv6 Multicast User Authentication and Profile Support

IPv6 multicast by design allows any host in the network to become a receiver or a source for a multicast group. Therefore, multicast access control is needed to control multicast traffic in the network. Access control functionality consists mainly of source access control and accounting, receiver access control and accounting, and provisioning of this access control mechanism.

Multicast access control provides an interface between multicast and authentication, authorization, and accounting (AAA) for provisioning, authorizing, and accounting at the last-hop device, receiver access control functions in multicast, and group or channel disabling capability in multicast.

When you deploy a new multicast service environment, it is necessary to add user authentication and provide a user profile download on a per-interface basis. The use of AAA and IPv6 multicast supports user authentication and downloading of the user profile in a multicast environment.

The event that triggers the download of a multicast access-control profile from the RADIUS server to the access device is arrival of an MLD join on the access device. When this event occurs, a user can cause the authorization cache to time out and request download periodically or use an appropriate multicast clear command to trigger a new download in case of profile changes.

Accounting occurs via RADIUS accounting. Start and stop accounting records are sent to the RADIUS server from the access device. In order for you to track resource consumption on a per-stream basis, these accounting records provide information about the multicast source and group. The start record is sent when the last-hop device receives a new MLD report, and the stop record is sent upon MLD leave or if the group or channel is deleted for any reason.

How to Configure Multicast User Authentication and Profile Support

Enabling AAA Access Control for IPv6 Multicast

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa new-model`

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa new-model Example: Device(config)# aaa new-model | Enables the AAA access control system. |

Specifying Method Lists and Enabling Multicast Accounting

SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **aaa authorization multicast default** [*method3* | *method4*]
4. **aaa accounting multicast default** [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*]
5. **interface** *type number*
6. **ipv6 multicast aaa account receive** *access-list-name* [**throttle** *throttle-number*]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | aaa authorization multicast default [<i>method3</i> <i>method4</i>] Example: Device(config)# aaa authorization multicast default | Enables AAA authorization and sets parameters that restrict user access to an IPv6 multicast network. |
| Step 4 | aaa accounting multicast default [start-stop stop-only] [broadcast] [<i>method1</i>] [<i>method2</i>] [<i>method3</i>] [<i>method4</i>] Example: Device(config)# aaa accounting multicast default | Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS. |
| Step 5 | interface <i>type number</i> Example: Device(config)# interface FastEthernet 1/0 | Specifies an interface type and number, and places the device in interface configuration mode. |
| Step 6 | ipv6 multicast aaa account receive <i>access-list-name</i> [throttle <i>throttle-number</i>] Example: Device(config-if)# ipv6 multicast aaa account receive list1 | Enables AAA accounting on specified groups or channels. |

Disabling the Device from Receiving Unauthenticated Multicast Traffic

In some situations, access control may be needed to prevent multicast traffic from being received unless the subscriber is authenticated and the channels are authorized as per access control profiles. That is, there should be no traffic at all unless specified otherwise by access control profiles.

SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 multicast group-range [access-list-name]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ipv6 multicast group-range [access-list-name] Example: Device(config)# ipv6 multicast group-range | Disables multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a device. |

Configuration Examples for Multicast User Authentication and Profile Support

Example: Enabling AAA Access Control, Specifying Method Lists, and Enabling Multicast Accounting for IPv6

```

Device(config)# aaa new-model
Device(config)# aaa authorization multicast default
Device(config)# aaa accounting multicast default
Device(config)# interface FastEthernet 1/0
Device(config-if)# ipv6 multicast aaa account receive list1

```

Additional References for IPv6 Services: AAAA DNS Lookups

Related Documents

| Related Topic | Document Title |
|----------------------------------|---------------------------------|
| IPv6 addressing and connectivity | <i>IPv6 Configuration Guide</i> |

| Related Topic | Document Title |
|-----------------------------|--|
| IPv4 services configuration | <i>IP Application Services Configuration Guide</i> |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| IPv6 commands | <i>Cisco IOS IPv6 Command Reference</i> |
| Cisco IOS IPv6 features | Cisco IOS IPv6 Feature Mapping |

Standards and RFCs

| Standard/RFC | Title |
|---------------|------------------|
| RFCs for IPv6 | <i>IPv6 RFCs</i> |

MIBs

| MIB | MIBs Link |
|-------|--|
| None. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

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 Multicast User Authentication and Profile Support

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.