



Named Method Lists for AAA Authorization and Accounting

Feature Summary

In earlier Cisco IOS releases, only named authentication method lists were supported under Cisco's Authentication, Authorization, and Accounting (AAA) network security services. With Cisco IOS Release 11.3(3)T, AAA has been extended to support both authorization and accounting named method lists. Named method lists for authorization and accounting function the same way as those for authentication.

Benefits

Named method lists for AAA authorization and accounting allow you to define different methods for authorization and accounting and apply those methods on a per-interface or per-line basis.

List of Terms

Authentication, Authorization, and Accounting (AAA)—Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

Network access server (NAS)—A Cisco access server or any other Cisco device that is acting as a client to the AAA server.

Platforms

This feature is supported on all Cisco IOS platforms.

Prerequisites

Before configuring authorization or accounting using named method lists, you must first perform the following tasks:

- Enable AAA on your network access server. For more information about enabling AAA on your Cisco router or access server, refer to the “AAA Overview” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- Configure AAA authentication. Authorization generally takes place after authentication and relies on authentication to work properly. For more information about AAA authentication, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- Define the characteristics of your RADIUS or TACACS+ security server if you are issuing RADIUS or TACACS+ authorization. For more information about configuring your Cisco network access server to communicate with your RADIUS security server, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*. For more information about configuring your Cisco network access server to communicate with your TACACS+ security server, refer to the “Configuring TACACS+” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- Define the rights associated with specific users by using the **username** command if you are issuing local authorization. For more information about the **username** command, refer to the Cisco IOS Release 11.3 *Security Command Reference*.
- Create the administrative instances of users in the Kerberos key distribution center by issuing the **kerberos instance map** command if you are using Kerberos. For more information about Kerberos, refer to the “Configuring Kerberos” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Supported MIBs and RFCs

No RFCs or MIBs are supported by this feature.

Functional Description

This section explains the details of named authorization and accounting method lists.

Named Method Lists for Authorization

Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

Cisco IOS software supports the following six methods for authorization:

- **TACACS+**—The NAS exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- **If-Authenticated**—The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None**—The NAS does not request authorization information; authorization is not performed over this line/interface.
- **Local**—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.
- **RADIUS**—The NAS requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- **Kerberos Instance Map**—The NAS uses the instance defined by the **kerberos instance map** command for authorization.

Method lists are specific to the type of authorization being requested. AAA supports four different types of authorization:

- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Reverse Access**—Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed. The only exception is the default method list (which is named “default”). If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Named Method Lists for Accounting

Like authentication and authorization method lists, method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for accounting services.

Cisco IOS software supports the following two methods for accounting:

- **TACACS+**—The NAS reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **RADIUS**—The NAS reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Accounting method lists are specific to the type of accounting being requested. AAA supports five different types of accounting:

- **Network**—Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
- **EXEC**—Provides information about user EXEC terminal sessions of the network access server.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Connection**—Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler-disassembler (PAD), and rlogin.
- **System**—Provides information about system-level events.

Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

Once again, when you create a named method list, you are defining a particular list of accounting methods for the indicated accounting type.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods will be performed. The only exception is the default method list (which is named “default”). If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Configuration Tasks

The following sections describe how to define and apply named method lists:

- Configure AAA Authorization Using Named Method Lists
- Configure AAA Accounting Using Named Method Lists

Configure AAA Authorization Using Named Method Lists

To configure AAA authorization using named method lists, perform the following tasks beginning in global configuration mode:

Task	Command
Create an authorization method list for a particular authorization type and enable authorization.	aaa authorization { network exec commands <i>level</i> reverse-access } { default <i>list-name</i> } [<i>method1</i> <i>method2...</i>]
Enter the line configuration mode for the lines to which you want to apply the authorization method list. or Enter the interface configuration mode for the interfaces to which you want to apply the authorization method list.	line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>] interface <i>interface-type interface-number</i>
Apply the authorization list to a line or set of lines. or Apply the authorization list to an interface or set of interfaces.	authorization { arap commands <i>level</i> exec reverse-access } { default <i>list-name</i> } ppp authorization { default <i>list-name</i> }

Authorization Types

Named authorization method lists are specific to the indicated type of authorization. To create a method list to enable authorization for all network-related service requests (including SLIP, PPP, PPP NCPs, and ARA protocols), use the **network** keyword.

To create a method list to enable authorization to determine if a user is allowed to run an EXEC shell, use the **exec** keyword.

To create a method list to enable authorization for specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword. (This allows you to authorize all commands associated with a specified command level from 0 to 15.)

To create a method list to enable authorization for reverse Telnet functions, use the **reverse-access** keyword.

For information about the four types of authorization supported by the Cisco IOS software, refer to the “Configuring Authorization” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Authorization Methods

To have the network access server request authorization information via a TACACS+ security server, use the **aaa authorization** command with the **tacacs+** *method* keyword. For more specific information about configuring authorization using a TACACS+ security server, refer to the “Configuring TACACS+” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

To allow users to have access to the functions they request as long as they have been authenticated, use the **aaa authorization {type}** command with the **if-authenticated** *method* keyword. If you select this method, all requested functions are automatically granted to authenticated users.

There may be times when you do not want to run authorization from a particular interface or line. To stop authorization activities on designated lines or interfaces, use the **none** *method* keyword.

To select local authorization, which means that the router or access server consults its local user database to determine the functions a user is permitted, use the **local method** keyword. The functions associated with local authorization are defined by using the **username** global configuration command. For a list of permitted functions, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

To have the NAS request authorization via a RADIUS security server, use the **radius method** keyword. For more specific information about configuring authorization using a RADIUS security server, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

To run authorization to determine if a user is allowed to run an EXEC shell at a specific privilege level based on a mapped Kerberos instance, use the **krb5-instance method** keyword. For more information, refer to the “Enable Kerberos Instance Mapping” section of the “Configuring Kerberos” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Note Authorization method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for authorization applies.

Configure AAA Accounting Using Named Method Lists

To configure AAA accounting using named method lists, perform the following tasks beginning in global configuration mode:

Task	Command
Create an accounting method list and enable accounting.	aaa accounting {system network exec connection commands <i>level</i> } {default list-name} {start-stop wait-start stop-only none} [<i>method1</i> [<i>method2...</i>]]
Enter the line configuration mode for the lines to which you want to apply the accounting method list.	line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>]
or	
Enter the interface configuration mode for the interfaces to which you want to apply the accounting method list.	interface <i>interface-type interface-number</i>
Apply the accounting method list to a line or set of lines.	accounting {arap exec connection commands <i>level</i> } {default list-name}
or	
Apply the accounting method list to an interface or set of interfaces.	ppp accounting {default list-name}

Note System accounting does not use named method lists. For system accounting, you can only define the default method list.

Accounting Types

Named accounting method lists are specific to the indicated type of accounting. To create a method list to provide accounting information for ARAP (network) sessions, use the **arap** keyword.

To create a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, start and stop times, use the **exec** keyword.

To create a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword.

To create a method list to provide accounting information about all outbound connections made from the network access server, use the **connection** keyword.

System accounting does not support named method lists.

For minimal accounting, use the **stop-only** keyword, which instructs the specified method (RADIUS or TACACS+) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the **start-stop** keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. You can further control access and accounting by using the **wait-start** keyword, which ensures that the RADIUS or TACACS+ security server acknowledges the start notice before granting the user's process request. To stop all accounting activities on this line or interface, use the **none** keyword.

For more information, refer to the "Configuring Accounting" chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Accounting Methods

To have the NAS send accounting information from a TACACS+ security server, use the **tacacs+ method** keyword. For more specific information about configuring TACACS+ for accounting services, refer to the "Configuring TACACS+" chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

To have the NAS send accounting information from a RADIUS security server, use the **radius method** keyword. For more specific information about configuring RADIUS for accounting services, refer to the "Configuring RADIUS" chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Note Accounting method lists for SLIP follow whatever is configured for PPP on the relevant interface. If no lists are defined and applied to a particular interface (or no PPP settings are configured), the default setting for accounting applies.

Configuration Example

The following example configures a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database will be queried for authentication and authorization information, and accounting services will be handled by a TACACS+ server.

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins radius local
aaa authorization network scoobee radius local
aaa accounting network charley start-stop radius

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication chap dialins
  ppp authorization scoobee
  ppp accounting charley

line 1 16
  autoselect ppp
  autoselect during-login
  login authentication admins
  modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines a method list, admins, for login authentication.
- The **aaa authentication ppp dialins radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network scoobee radius local** command defines the network authorization method list named scoobee, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization will be performed.
- The **aaa accounting network charley start-stop radius** command defines the network accounting method list named charley, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) will be used on serial lines using PPP.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.

- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication chap dialins** command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.
- The **ppp authorization scoobee** command applies the scoobee network authorization method list to the specified interfaces.
- The **ppp accounting charley** command applies the charley network accounting method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the admins method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

Command Reference

This section documents the following new and modified commands:

- **aaa accounting**
- **aaa authorization**
- **accounting**
- **authorization**
- **ppp accounting**
- **ppp authorization**

All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

aaa accounting

To enable AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** global configuration command. Use the **no** form of this command to disable accounting.

```
aaa accounting {system | network | exec | connection | commands level} {default | list-name}
  {start-stop | wait-start | stop-only | none} [method1 [method2...]]
no aaa accounting {system | network | exec | commands level}
```

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.
exec	Runs accounting for EXEC session (user shells). This keyword might return user profile information such as autocommand information.
connection	Provides information about all outbound connections made from the NAS, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
commands	Runs accounting for all commands at the specified privilege level.
<i>level</i>	Specific command level to track for accounting. Valid entries are 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the following list of accounting methods.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.
wait-start	As in start-stop , sends both a start and a stop accounting notice to the accounting server. However, if you use the wait-start keyword, the requested user service does not begin until the start accounting notice is acknowledged. A stop accounting notice is also sent.
stop-only	Sends a stop accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
<i>method</i>	At least one of the keywords described in Table 1.

Default

AAA accounting is disabled. If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis. Method keywords are described in Table 1.

Table 1 AAA Accounting Methods

Keyword	Description
radius	Uses RADIUS to provide accounting service.
tacacs+	Uses TACACS+ to provide accounting services.

Cisco IOS software supports the following two methods for accounting:

- **TACACS+**—The NAS reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **RADIUS**—The NAS reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the method(s) tried in the given sequence.

Named accounting method lists are specific to the indicated type of accounting. To create a method list to provide accounting information for ARAP (network) sessions, use the **arap** keyword. To create a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, start and stop times, use the **exec** keyword. To create a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level, use the **commands** keyword. To create a method list to provide accounting information about all outbound connections made from the network access server, use the **connection** keyword.

Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting notice at the end of the process. For even more accounting control, you can include the **wait-start** keyword, which ensures that the start notice is received by the RADIUS or TACACS+ server before granting the user's process request. Accounting is done only to the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

When **aaa accounting** is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the "RADIUS Attributes" appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the "TACACS+ AV Pairs" appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Note This command cannot be used with TACACS or Extended TACACS.

Example

In the following example, a default commands accounting method list is defined, where commands accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only tacacs+
```

Related Commands

aaa authentication
aaa authorization
aaa new-model

aaa authorization

Use the **aaa authorization** global configuration command to set parameters that restrict a user's network access. Use the **no** form of this command to disable authorization for a function.

```
aaa authorization {network | exec | commands level | reverse-access} {default | list-name}
[method1 [method2...]]
no aaa authorization {network | exec | commands level | reverse-access}
```

Syntax Description

network	Runs authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARA protocol.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.
commands	Runs authorization for all commands at the specified privilege level.
<i>level</i>	Specific command level that should be authorized. Valid entries are 0 through 15.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
default	Uses the listed authorization methods that follow this argument as the default list of methods for authorization.
<i>list-name</i>	Character string used to name the following list of authorization methods.
<i>method</i>	One of the keywords listed in Table 2.

Default

Authorization is disabled for all actions (equivalent to the method keyword **none**). If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Note This command cannot be used with TACACS or Extended TACACS.

Use the **aaa authorization** command to enable authorization and to create named methods lists, defining authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

Use the **aaa authorization** command to create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization method(s) tried in the given sequence.

Method keywords are described in Table 2.

Table 2 AAA Authorization Methods

Keyword	Description
tacacs+	Requests authorization information from the TACACS+ server.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.
local	Uses the local database for authorization.
radius	Uses RADIUS to get authorization information.
krb5-instance	Uses the instance defined by the kerberos instance map command.

Cisco IOS software supports the following six methods for authorization:

- **TACACS+**—The NAS exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.
- **If-Authenticated**—The user is allowed to access the requested function provided the user has been authenticated successfully.
- **None**—The NAS does not request authorization information; authorization is not performed over this line/interface.
- **Local**—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled via the local database.

- **RADIUS**—The NAS requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- **Kerberos Instance Map**—The NAS uses the instance defined by the **kerberos instance map** command for authorization.

Method lists are specific to the type of authorization being requested. AAA supports four different types of authorization:

- **Network**—Applies to network connections. This can include a PPP, SLIP, or ARAP connection.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **Reverse Access**—Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods will be performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is
- Make changes to the request
- Refuse the request and refuse authorization

For a list of supported RADIUS attributes, refer to the “RADIUS Attributes” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*. For a list of supported TACACS+ AV pairs, refer to the “TACACS+ AV Pairs” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Note There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example defines the network authorization method list named `scoobee`, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization will be performed

```
aaa authorization network scoobee radius local
```

Related Commands

aaa accounting
aaa authentication
aaa new-model

accounting

To enable AAA accounting services to a specific line or group of lines, use the **accounting** line configuration command. Use the **no** form of this command to disable this feature.

```
accounting {arap | commands level | connection | exec} [default | list-name]  
no accounting {arap | commands level | connection | exec} [default | list-name]
```

Syntax Description

arap	Enables accounting on line(s) configured for Appletalk Remote Access protocol (ARAP).
commands	Enables accounting on the selected line(s) for all commands at the specified privilege level.
<i>level</i>	Specifies the command level to track for accounting. Valid entries are 0 through 15.
connection	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
exec	Enables accounting for all system-level events not associated with users, such as reloads on the selected line(s).
default	The name of the default method list, created with the aaa accounting command.
<i>list-name</i>	(Optional) Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the aaa accounting command.

Default

Accounting is disabled.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3T.

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list) for a particular type of accounting, you must apply the defined lists to the appropriate lines for accounting services to take place. Use the **accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Example

The following example enables command accounting services (for level 15) using the accounting method list named charlie on line 10:

```
line 10
  accounting commands 15 charlie
```

Related Commands

arap authentication

authorization

login authentication

nasi authentication

authorization

To enable AAA authorization to a specific line or group of lines, use the **authorization** line configuration command. Use the **no** form of this command to disable this feature.

```
authorization {arap | commands level | exec | reverse-access} [default | list-name]  
no authorization {arap | commands level | exec | reverse-access} [default | list-name]
```

Syntax Description

arap	Enables authorization for line(s) configured for AppleTalk Remote Access Protocol (ARAP).
commands	Enables authorization on the selected line(s) for all commands at the specified privilege level.
<i>level</i>	Specific command level to be authorized. Valid entries are 0 through 15.
exec	Enables authorization to determine if the user is allowed to run an EXEC shell on the selected line(s).
reverse-access	Enables authorization to determine if the user is allowed reverse access privileges.
default	The name of the default method list, created with the aaa authorization command.
<i>list-name</i>	Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the aaa authorization command.

Default

Authorization is not enabled.

Command Mode

Line configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3T.

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined lists to the appropriate lines for authorization to take place. Use the **authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected line or group of lines.

Example

The following example enables command authorization (for level 15) using the method list named charlie on line 10:

```
line 10
  authorization commands 15 charlie
```

Related Commands

accounting
arap authentication
login authentication
nasi authentication

ppp accounting

To enable AAA accounting services on the selected interface, use the **ppp accounting** interface configuration command. Use the **no** form of this command to disable this feature.

```
ppp accounting [default | list-name]  
no ppp accounting
```

Syntax Description

default The name of the method list is created with the **aaa accounting** command.

list-name Specifies the name of a list of accounting methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa accounting** command.

Default

Accounting is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3T.

After you enable the **aaa accounting** command and define a named accounting method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for accounting services to take place. Use the **ppp accounting** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Example

The following example enables accounting on asynchronous interface 4 and uses the accounting method list named charlie:

```
interface async 4  
  encapsulation ppp  
  ppp accounting charlie
```

Related Commands

aaa accounting

ppp authorization

To enable AAA authorization on the selected interface, use the **ppp authorization** interface configuration command. Use the **no** form of this command to disable this feature.

```
ppp authorization [default | list-name]  
no ppp authorization
```

Syntax Description

default The name of the method list is created with the **aaa authorization** command.

list-name (Optional) Specifies the name of a list of authorization methods to use. If no list name is specified, the system uses the default. The list is created with the **aaa authorization** command.

Default

Authorization is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3T.

After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list), you must apply the defined lists to the appropriate interfaces for authorization to take place. Use the **ppp authorization** command to apply the specified method lists (or if none is specified, the default method list) to the selected interface.

Example

The following example enables authorization on asynchronous interface 4 and uses the method list named charlie:

```
interface async 4  
  encapsulation ppp  
  ppp authorization charlie
```

Related Commands

aaa authorization

