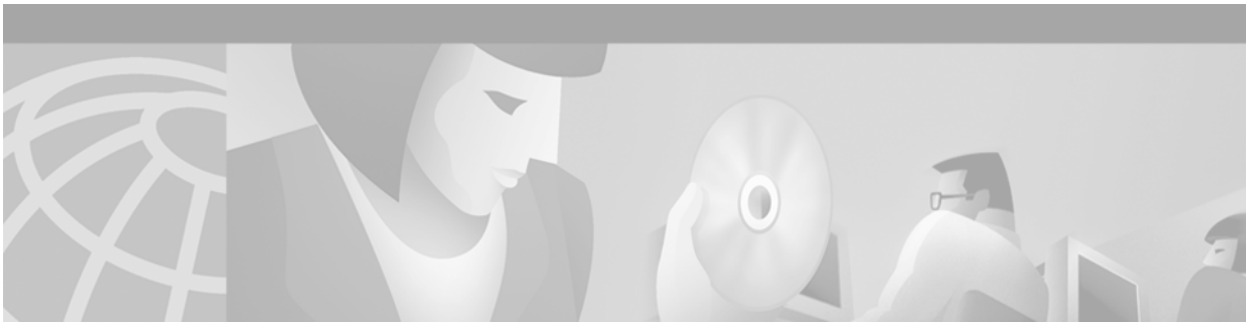

# Authentication Commands

This chapter describes the commands used to configure both AAA and non-AAA authentication methods. Authentication identifies users before they are allowed access to the network and network services. Basically, the Cisco IOS software implementation of authentication is divided into two main categories:

- AAA Authentication Methods
- Non-AAA Authentication Methods

Authentication, for the most part, is implemented through the AAA security services. We recommend that, whenever possible, AAA be used to implement authentication.

For information on how to configure authentication using either AAA or non-AAA methods, refer to the chapter "Configuring Authentication" in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the section "Authentication Examples" located at the end of the chapter "Configuring Authentication" in the *Cisco IOS Security Configuration Guide*.

# aaa authentication arap

To enable an authentication, authorization, and accounting (AAA) authentication method for AppleTalk Remote Access (ARA), use the **aaa authentication arap** command in global configuration mode. To disable this authentication, use the **no** form of this command.

**aaa authentication arap** {**default** | *list-name*} *method1* [*method2*...]

**no aaa authentication arap** {**default** | *list-name*} *method1* [*method2*...]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed methods that follow this argument as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the following list of authentication methods tried when a user logs in. |
| *method1* [*method2*...] | At least one of the keywords described in Table 3. |

## Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication arap default local
```

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server and local-case support were added as method keywords for this command. |

## Usage Guidelines

The list names and default that you set with the **aaa authentication arap** command are used with the **arap authentication** command. Note that ARAP guest logins are disabled by default when you enable AAA. To allow guest logins, you must use either the **guest** or **auth-guest** method listed in Table 3. You can only use one of these methods; they are mutually exclusive.

Create a list by entering the **aaa authentication arap** *list-name method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. See Table 3 for descriptions of method keywords.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **more system:running-config** command to view currently configured lists of authentication methods.

**Note** In Table 3, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

*Table 3 aaa authentication arap Methods*

| Keyword | Description |
|---|---|
| **guest** | Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed. |
| **auth-guest** | Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed. |
| **line** | Uses the line password for authentication. |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access group tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default group tacacs+ none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |

# aaa authentication banner

To configure a personalized banner that will be displayed at user login, use the **aaa authentication banner** command in global configuration mode. To remove the banner, use the **no** form of this command.

**aaa authentication banner** *dstringd*

**no aaa authentication banner**

## Syntax Description

| | |
|---|---|
| *d* | Any delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner. |
| *string* | Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996. |

## Defaults

Not enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(4)T | This command was introduced. |

## Usage Guidelines

Use the **aaa authentication banner** command to create a personalized message that appears when a user logs in to the system. This message or banner will replace the default message for user login.

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

**Note** The AAA authentication banner message is not displayed if TACACS+ is the first method in the method list.

## Examples

The following example shows the default login message if **aaa authentication banner** is not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

The following example configures a login banner (in this case, the phrase "Unauthorized use is prohibited.") that will be displayed when a user logs in to the system. In this case, the asterisk (*) symbol is used as the delimiter. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized use is prohibited.
Username:
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication fail-message** | Configures a personalized banner that will be displayed when a user fails login. |

# aaa authentication enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine if a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

**aaa authentication enable default** *method1* [*method2*...]

**no aaa authentication enable default** *method1* [*method2*...]

## Syntax Description

| | |
|---|---|
| *method1* [*method2*...] | At least one of the keywords described in Table 3. |

## Defaults

If the **default** list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server support was added as various method keywords for this command. |

## Usage Guidelines

Use the **aaa authentication enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 3. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the router to a RADIUS or TACACS+ server include the username "$enab15$."

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to view currently configured lists of authentication methods.

**Note** In Table 3, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

*Table 4 aaa authentication enable default Methods*

| Keyword | Description |
|---|---|
| **enable** | Uses the enable password for authentication. |
| **line** | Uses the line password for authentication. |
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication.<br>**Note** The RADIUS method does not work on a per-username basis. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication enable default group tacacs+ enable none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization** | Sets parameters that restrict network access to a user. |
| **aaa new-model** | Enables the AAA access control model. |
| **enable password** | Sets a local password to control access to various privilege levels. |

# aaa authentication fail-message

To configure a personalized banner that will be displayed when a user fails login, use the **aaa authentication fail-message** command in global configuration mode. To remove the failed login message, use the **no** form of this command.

**aaa authentication fail-message** *dstringd*

**no aaa authentication fail-message**

## Syntax Description

| | |
|---|---|
| *d* | The delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner. |
| *string* | Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996. |

## Defaults

Not enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(4)T | This command was introduced. |

## Usage Guidelines

Use the **aaa authentication fail-message** command to create a personalized message that appears when a user fails login. This message will replace the default message for failed login.

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

## Examples

The following example shows the default login message and failed login message that is displayed if **aaa authentication banner** and **aaa authentication fail-message** are not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

```
% Authentication failed.
```

The following example configures both a login banner (“Unauthorized use is prohibited.”) and a login-fail message (“Failed login. Try again.”). The login message will be displayed when a user logs in to the system. The failed-login message will display when a user tries to log in to the system and fails. (RADIUS is specified as the default login authentication method.) In this example, the asterisk (*) is used as the delimiting character.

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized use is prohibited.
Username:
Password:
Failed login. Try again.
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication banner** | Configures a personalized banner that will be displayed at user login. |

# aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

**aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]

**no aaa authentication login** {**default** | *list-name*} *method1* [*method2*...]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in. |
| *method1* [*method2*...] | At least one of the keywords described in Table 5. |

## Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

**Note** On the console, login will succeed without any authentication checks if **default** is not set.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server and local-case support were added as method keywords for this command. |

## Usage Guidelines

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method* command for a particular protocol, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. Method keywords are described in Table 5.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

**Note** In Table 5, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

*Table 5 aaa authentication login Methods*

| Keyword | Description |
|---|---|
| **enable** | Uses the enable password for authentication. |
| **krb5** | Uses Kerberos 5 for authentication. |
| **krb5-telnet** | Uses Kerberos 5 telnet authentication protocol when using Telnet to connect to the router. |
| **line** | Uses the line password for authentication. |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access group tacacs+ enable none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ enable none
```

The following example sets authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default krb5
```

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. |
| **login authentication** | Enables AAA authentication for logins. |

# aaa authentication nasi

To specify authentication, authorization, and accounting (AAA) authentication for Netware Asynchronous Services Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** command in global configuration mode. To disable authentication for NASI clients, use the **no** form of this command.

**aaa authentication nasi** {**default** | *list-name*} *method1* [*method2*...]

**no aaa authentication nasi** {**default** | *list-name*} *method1* [*method2*...]

## Syntax Description

| | |
|---|---|
| **default** | Makes the listed authentication methods that follow this argument the default list of methods used when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods activated when a user logs in. |
| *method1* [*method2*...] | At least one of the methods described in Table 6. |

## Defaults

If the **default** list is not set, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication nasi default local
```

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.0(5)T | Group server support and **local-case** were added as method keywords for this command. |

## Usage Guidelines

The default and optional list names that you create with the **aaa authentication nasi** command are used with the **nasi authentication** command.

Create a list by entering the **aaa authentication nasi** command, where *list-name* is any character string that names the list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. Method keywords are described in Table 6.

To create a default list that is used if no list is assigned to a line with the **nasi authentication** command, use the default argument followed by the methods that you want to use in default situations.

The remaining methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

**Note** In Table 6, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

*Table 6 aaa authentication nasi Methods*

| Keyword | Description |
|---|---|
| **enable** | Uses the enable password for authentication. |
| **line** | Uses the line password for authentication. |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates an AAA authentication list called *list1*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication nasi list1 group tacacs+ enable none
```

The following example creates the same list, but sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication nasi default group tacacs+ enable none
```

## Related Commands

| Command | Description |
|---|---|
| **ip trigger-authentication (global)** | Enables the automated part of double authentication at a device. |
| **ipx nasi-server enable** | Enables NASI clients to connect to asynchronous devices attached to a router. |
| **nasi authentication** | Enables AAA authentication for NASI clients connecting to a router. |
| **show ipx nasi connections** | Displays the status of NASI connections. |
| **show ipx spx-protocol** | Displays the status of the SPX protocol stack and related counters. |

# aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

**aaa authentication password-prompt** *text-string*

**no aaa authentication password-prompt** *text-string*

## Syntax Description

| | |
|---|---|
| *text-string* | String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”). |

## Defaults

There is no user-defined *text-string*, and the password prompt appears as “Password.”

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |

## Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

The **aaa authentication password-prompt** command works when RADIUS is used as the login method. The password prompt that is defined in the command will be shown even when the RADIUS server is unreachable. The **aaa authentication password-prompt** command does not work with TACACS+. TACACS+ supplies the network access server (NAS) with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the **aaa authentication password-prompt** command. If the TACACS+ server is not reachable, the password prompt that is defined in the **aaa authentication password-prompt** command may be used.

## Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt “Enter your password now:”
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication username-prompt** | Changes the text displayed when users are prompted to enter a username. |
| **aaa new-model** | Enables the AAA access control model. |
| **enable password** | Sets a local password to control access to various privilege levels. |

# aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

**aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]

**no aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]

## Syntax Description

| | |
|---|---|
| **default** | Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in. |
| *list-name* | Character string used to name the list of authentication methods tried when a user logs in. |
| *method1* [*method2*...] | Identifies the list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in Table 7. |

## Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as that created by the following command:

```
aaa authentication ppp default local
```

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(5)T | Group server support and **local-case** were added as method keywords. |

## Usage Guidelines

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method* command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 7.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

**Note** In Table 7, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

*Table 7 aaa authentication ppp Methods*

| Keyword | Description |
|---|---|
| **if-needed** | Does not authenticate if the user has already been authenticated on a tty line. |
| **krb5** | Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication). |
| **local** | Uses the local username database for authentication. |
| **local-case** | Uses case-sensitive local username authentication. |
| **none** | Uses no authentication. |
| **group radius** | Uses the list of all RADIUS servers for authentication. |
| **group tacacs+** | Uses the list of all TACACS+ servers for authentication. |
| **group** *group-name* | Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command. |

## Examples

The following example creates a AAA authentication list called *MIS-access* for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server radius** | Groups different RADIUS server hosts into distinct lists and distinct methods. |
| **aaa group server tacacs+** | Groups different server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **more system:running-config** | Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information. |
| **ppp authentication** | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |
| **radius-server host** | Specifies a RADIUS server host. |
| **tacacs+-server host** | Specifies a TACACS host. |

# aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

**aaa authentication username-prompt** *text-string*

**no aaa authentication username-prompt** *text-string*

## Syntax Description

| | |
|---|---|
| *text-string* | String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”). |

## Defaults

There is no user-defined *text-string*, and the username prompt appears as “Username.”

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |

## Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.

**Note** The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

## Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt “Enter your name here:”
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication password-prompt** | Changes the text that is displayed when users are prompted for a password. |
| **aaa new-model** | Enables the AAA access control model. |
| **enable password** | Sets a local password to control access to various privilege levels. |

# aaa dnis map authentication login group

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group for the login service (this server group will be used for AAA authentication), use the **aaa dnis map authentication login group** command in global configuration mode. To unmap this DNIS number from the defined server group, use the **no** form of this command.

**aaa dnis map** *dnis-number* **authentication login group** *server-group-name*

**no aaa dnis map** *dnis-number* **authentication login group** *server-group-name*

## Syntax Description

| | |
|---|---|
| *dnis-number* | Number of the DNIS. |
| *server-group-name* | Character string used to name a group of security servers associated in a server group. |

## Defaults

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1 | This command was introduced. |

## Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group; thus, the server group can process the AAA authentication requests for login service for users dialing into the network using that particular DNIS.

To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

## Examples

The following example shows how to map DNIS number 7777 to the RADIUS server group called group1. group1 will use RADIUS server 172.30.0.0 for AAA authentication requests for login service for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
 exit
aaa dnis map enable
aaa dnis map 7777 authentication login group group1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa dnis map accounting network group** | Maps a DNIS number to a particular accounting server group. |
| **aaa dnis map enable** | Enables AAA server selection based on DNIS. |
| **aaa group server** | Groups different server hosts into distinct lists and methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |

# aaa dnis map authentication ppp group

To map a Dialed Number Information Service (DNIS) number to a particular authentication server group (this server group will be used for authentication, authorization, and accounting (AAA) authentication), use the **aaa dnis map authentication ppp group** command in global configuration mode. To remove the DNIS number from the defined server group, use the **no** form of this command.

**aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*

**no aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*

## Syntax Description

| | |
|---|---|
| *dnis-number* | Number of the DNIS. |
| *server-group-name* | Character string used to name a group of security servers associated in a server group. |

## Defaults

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |

## Usage Guidelines

This command lets you assign a DNIS number to a particular AAA server group, so that the server group can process authentication requests for users dialing in to the network using that particular DNIS. To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

## Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 authentication ppp group group1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa dnis map accounting network group** | Maps a DNIS number to a particular accounting server group. |
| **aaa dnis map enable** | Enables AAA server selection based on DNIS. |
| **aaa group server** | Groups different server hosts into distinct lists and distinct methods. |
| **aaa new-model** | Enables the AAA access control model. |
| **radius-server host** | Specifies a RADIUS server host. |

# aaa nas redirected-station

To include the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication, use the **aaa nas redirected-station** command in global configuration mode. To leave the original number out of the information sent to the authentication server, use the **no** form of this command.

**aaa nas redirected-station**

**no aaa nas redirected-station**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The original number is not included in the information sent to the authentication server.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1 T | This command was introduced. |

## Usage Guidelines

If a customer is being authenticated by a RADIUS or TACACS+ server and the number dialed by the cable modem (or other device) is redirected to another number for authentication, the **aaa nas redirected-station** command will enable the original number to be included in the information sent to the authentication server.

This functionality allows the service provider to determine whether the customer dialed a number that requires special billing arrangements, such as a toll-free number.

The original number can be sent as a Cisco Vendor Specific Attribute (VSA) for TACACS+ servers and as RADIUS Attribute 93 (Ascend-Redirect-Number) for RADIUS servers. The RADIUS Attribute 93 is sent by default; to also send a VSA attribute for TACACS+ servers, use the **radius-server vsa send accounting** and **radius-server vsa send authentication** commands. To configure the RADIUS server to use RADIUS Attribute 93, add the non-standard option to the **radius-server host** command.

**Note** This feature is valid only when using port adapters that are configured for a T1 or E1 ISDN PRI or BRI interface. In addition, the telco switch performing the number redirection must be able to provide the redirected number in the Q.931 Digital Subscriber Signaling System Network Layer.

## Examples

The following example enables the original number to be forwarded to the authentication server:

```
!
aaa authorization config-commands
aaa accounting exec default start-stop group radius
aaa accounting system default start-stop broadcast group apn23
aaa nas redirected-station
```

```
aaa session-id common
ip subnet-zero
!
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server host** | Specifies a RADIUS server host. |
| **radius-server vsa** | Configures the network access server to recognize and use vendor-specific attributes. |

# aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

**aaa new-model**

**no aaa new-model**

## Syntax Description

This command has no arguments or keywords.

## Defaults

AAA is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |

## Usage Guidelines

This command enables the AAA access control system.

## Examples

The following example initializes AAA:

```
aaa new-model
```

## Related Commands

| Command | Description |
|---|---|
| **aaa accounting** | Enables AAA accounting of requested services for billing or security purposes. |
| **aaa authentication arap** | Enables an AAA authentication method for ARAP using TACACS+. |
| **aaa authentication enable default** | Enables AAA authentication to determine if a user can access the privileged command level. |
| **aaa authentication login** | Sets AAA authentication at login. |
| **aaa authentication ppp** | Specifies one or more AAA authentication method for use on serial interfaces running PPP. |
| **aaa authorization** | Sets parameters that restrict user access to a network. |

# aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** global configuration command. To disable this feature, use the **no** form of this command.

**aaa pod server** [**port** *port-number*] [**auth-type** {**any** | **all** | **session-key**}] **server-key** *string*

**no aaa pod server**

## Syntax Description

| | |
|---|---|
| **port** *port-number* | (Optional) The network access server port to use for packet of disconnect requests. If no port is specified, port 1700 is used. |
| **auth-type** | (Optional) The type of authorization required for disconnecting sessions. If no authentication type is specified, **auth-type** is the default. |
| **any** | (Optional) Specifies that the session that matches all attributes sent in the POD packet is disconnected. The POD packet can contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). |
| **all** | (Optional) Only a session that matches all four key attributes is disconnected. **All** is the default. |
| **session-key** | (Optional) Specifies that the session that has a matching session-key attribute is disconnected. All other attributes are ignored. |
| **server-key** *string* | The secret text string that is shared between the network access server and the client workstation. This secret string must be the same on both systems. |

## Defaults

The POD server function is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |

## Usage Guidelines

For a session to be disconnected, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the **auth-type** attribute defined in the command. If no **auth-type** is specified, all four values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- User-Name
- Framed-IP-Address
- Session-Id
- Server-Key

## Examples

The following example enables POD and sets the secret key to "ab9123."

```
aaa pod server server-key ab9123
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication** | Enables authentication. |
| **aaa accounting** | Enables accounting records. |
| **aaa accounting delay-start** | Delays generation of the start accounting record until the user IP address is established. |
| **debug aaa pod** | Displays debug messages related to POD packets. |
| **radius-server host** | Identifies a RADIUS host. |

# aaa preauth

To enter authentication, authorization, and accounting (AAA) preauthentication configuration mode, use the **aaa preauth** command in global configuration mode. To disable preauthentication, use the **no** form of this command.

**aaa preauth**

**no aaa preauth**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Preauthentication is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |

## Usage Guidelines

To enter AAA preauthentication configuration mode, use the **aaa preauth** command. To configure preauthentication, use a combination of the **aaa preauth** commands: **group**, **clid**, **ctype**, **dnis**, and **dnis bypass**. You must configure the **group** command. You must also configure one or more of the **clid**, **ctype**, **dnis**, or **dnis bypass** commands.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

You can use the **clid**, **ctype**, or **dnis** commands to define the list of the preauthentication elements. For each preauthentication element, you can also define options such as password (for all the elements, the default password is cisco). If you specify multiple elements, the preauthentication process will be performed on each element according to the order of the elements that you configure with the preauthentication commands. In this case, more than one RADIUS preauthentication profile is returned, but only the last preauthentication profile will be applied to the authentication and authorization later on, if applicable.

## Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 dnis password Ascend-DNIS
```

## Related Commands

| Command | Description |
|---|---|
| **dnis (AAA preauthentication)** | Enables AAA preauthentication using DNIS. |
| **group** | Selects the security server to use for AAA preauthentication. |
| **isdn guard-timer** | Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request. |

# aaa processes

To allocate a specific number of background processes to be used to process authentication, authorization, and accounting (AAA) authentication and authorization requests for PPP, use the **aaa processes** command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

**aaa processes** *number*

**no aaa processes** *number*

## Syntax Description

| | |
|---|---|
| *number* | Specifies the number of background processes allocated for AAA requests for PPP. Valid entries are 1 to 2147483647. |

## Defaults

The default for this command is one allocated background process.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3(2)AA | This command was introduced. |

## Usage Guidelines

Use the **aaa processes** command to allocate a specific number of background processes to simultaneously handle multiple AAA authentication and authorization requests for PPP. Previously, only one background process handled all AAA requests for PPP, so only one new user could be authenticated or authorized at a time. This command configures the number of processes used to handle AAA requests for PPP, increasing the number of users that can be simultaneously authenticated or authorized.

The argument *number* defines the number of background processes earmarked to process AAA authentication and authorization requests for PPP. This argument also defines the number of new users that can be simultaneously authenticated and can be increased or decreased at any time.

## Examples

The following examples shows the **aaa processes** command within a standard AAA configuration. The authentication method list “dialins” specifies RADIUS as the method of authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP. Ten background processes have been allocated to handle AAA requests for PPP.

```
aaa new-model
aaa authentication ppp dialins group radius local
aaa processes 10
interface 5
encap ppp
ppp authentication pap dialins
```

## Related Commands

| Command | Description |
|---|---|
| show ppp queues | Monitors the number of requests processed by each AAA background process. |

# access-profile

To apply your per-user authorization attributes to an interface during a PPP session, use the **access-profile** command in privileged EXEC mode. Use the default form of the command (no keywords) to cause existing access control lists (ACLs) to be removed and ACLs defined in your per-user configuration to be installed.

**access-profile** [**merge** | **replace**] [**ignore-sanity-checks**]

## Syntax Description

| | |
|---|---|
| **merge** | (Optional) Like the default form of the command, this option removes existing ACLs while retaining other existing authorization attributes for the interface.<br><br>However, using this option also installs per-user authorization attributes in addition to the existing attributes. (The default form of the command installs only new ACLs.) The per-user authorization attributes come from all attribute-value pairs defined in the authentication, authorization, and accounting (AAA) per-user configuration (the user's authorization profile).<br><br>The resulting authorization attributes of the interface are a combination of the previous and new configurations. |
| **replace** | (Optional) This option removes existing ACLs *and* all other existing authorization attributes for the interface.<br><br>A complete new authorization configuration is then installed, using all AV pairs defined in the AAA per-user configuration.<br><br>This option is not normally recommended because it initially deletes *all* existing configurations, including static routes. This could be detrimental if the new user profile does not reinstall appropriate static routes and other critical information. |
| **ignore-sanity-checks** | (Optional) Enables you to use any AV pairs, whether or not they are valid. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 F | This command was introduced. |

## Usage Guidelines

Remote users can use this command to activate double authentication for a PPP session. Double authentication must be correctly configured for this command to have the desired effect.

You should use this command when remote users establish a PPP link to gain local network access.

After you have been authenticated with CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol), you will have limited authorization. To activate double authentication and gain your appropriate user network authorization, you must open a Telnet session to the network access server and execute the **access-profile** command. (This command could also be set up as an autocommand, which would eliminate the need to enter the command manually.)

This command causes all subsequent network authorizations to be made in *your* username instead of in the remote *host's* username.

Any changes to the interface caused by this command will stay in effect for as long as the interface stays up. These changes will be removed when the interface goes down. This command does not affect the normal operation of the router or the interface.

The default form of the command, **access-profile**, causes existing ACLs to be unconfigured (removed), and new ACLs to be installed. The new ACLs come from your per-user configuration on an AAA server (such as a TACACS+ server). The ACL replacement constitutes a reauthorization of your network privileges.

The default form of the command can fail if your per-user configuration contains statements other than ACL AV pairs. Any protocols with non-ACL statements will be deconfigured, and no traffic for that protocol can pass over the PPP link.

The **access-profile merge** form of the command causes existing ACLs to be unconfigured (removed) and new authorization information (including new ACLs) to be added to the interface. This new authorization information consists of your complete per-user configuration on an AAA server. If any of the new authorization statements conflict with existing statements, the new statements could "override" the old statements or be ignored, depending on the statement and applicable parser rules. The resulting interface configuration is a combination of the original configuration and the newly installed per-user configuration.

**Caution** The new user authorization profile (per-user configuration) must *not* contain any invalid mandatory AV pairs, otherwise the command will fail and the PPP protocol (containing the invalid pair) will be dropped. If invalid AV pairs are included as *optional* in the user profile, the command will succeed, but the invalid AV pair will be ignored. Invalid AV pair types are listed later in this section.

The **access-profile replace** form of the command causes the entire existing authorization configuration to be removed from the interface, and the complete per-user authorization configuration to be added. This per-user authorization consists of your complete per-user configuration on an AAA server.

**Caution** Use extreme caution when using the **access-profile replace** form of the command. It might have detrimental and unexpected results, because this option deletes *all* authorization configuration information (including static routes) before reinstalling the new authorization configuration.

#### Invalid AV pair types

- addr
- addr-pool
- zonelist
- tunnel-id
- ip-addresses
- x25-addresses
- frame-relay
- source-ip

**Note** These AV pair types are "invalid" only when used with double authentication, in the user-specific authorization profile; they cause the **access-profile** command to fail. However, these AV pair types can be appropriate when used in other contexts.

## Examples

The following example activates double authentication for a remote user. This example assumes that the **access-profile** command was *not* configured as an autocommand.

The remote user connects to the corporate headquarters network as shown in Figure 2.

***Figure 2 Network Topology for Activating Double Authentication (Example)***


The remote user runs a terminal emulation application to Telnet to the corporate network access server, a Cisco AS5200 universal access server local host named "hqnas." The remote user, named Bob, has the username "BobUser."

The following example replaces ACLs on the local host PPP interface. The ACLs previously applied to the interface during PPP authorization are replaced with ACLs defined in the per-user configuration AV pairs.

The remote user establishes a Telnet session to the local host and logs in:

```
login: BobUser
Password: <welcome>
hqnas> access-profile
```

Bob is reauthenticated when he logs in to hqnas, because hqnas is configured for login AAA authentication using the corporate RADIUS server. When Bob enters the **access-profile** command, he is reauthorized with his per-user configuration privileges. This causes the access lists and filters in his per-user configuration to be applied to the network access server interface.

After the reauthorization is complete, Bob is automatically logged out of the Cisco AS5200 local host.

## Related Commands

| Command | Description |
|---|---|
| **connect** | Logs in to a host that supports Telnet, rlogin, or LAT. |
| **telnet** | Logs in to a host that supports Telnet. |

# arap authentication

To enable authentication, authorization, and accounting (AAA) authentication for AppleTalk Remote Access Protocol (ARAP) on a line, use the **arap authentication** command in line configuration mode. To disable authentication for an ARAP line, use the **no** form of the command

**arap authentication** {**default** | *list-name*} [**one-time**]

**no arap authentication** {**default** | *list-name*}

**Caution** If you use a *list-name* value that was not configured with the **aaa authentication arap** command, ARAP will be disabled on this line.

## Syntax Description

| | |
|---|---|
| **default** | Default list created with the **aaa authentication arap** command. |
| *list-name* | Indicated list created with the **aaa authentication arap** command. |
| **one-time** | (Optional) Accepts the username and password in the username field. |

## Defaults

ARAP authentication uses the default set with **aaa authentication arap** command. If no default is set, the local user database is checked.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 11.0 | The **one-time** keyword was added. |

## Usage Guidelines

This command is a per-line command that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line). You create defaults and lists with the **aaa authentication arap** command. Entering the **no** version of **arap authentication** has the same effect as entering the command with the **default** keyword. Before issuing this command, create a list of authentication processes by using the **aaa authentication arap** global configuration command.

## Examples

The following example specifies that the TACACS+ authentication list called *MIS-access* is used on ARAP line 7:

```
line 7
 arap authentication MIS-access
```

## Related Commands

| Command | Description |
|---|---|
| aaa authentication arap | Enables an AAA authentication method for ARAP using TACACS+. |

# clear ip trigger-authentication

To clear the list of remote hosts for which automated double authentication has been attempted, use the **clear ip trigger-authentication** command in privileged EXEC mode.

**clear ip trigger-authentication**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

Use this command when troubleshooting automated double authentication. This command clears the entries in the list of remote hosts displayed by the **show ip trigger-authentication** command.

## Examples

The following example clears the remote host table:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host          Time Stamp
172.21.127.114       2940514234
router# clear ip trigger-authentication
router# show ip trigger-authentication
router#
```

## Related Commands

| Command | Description |
|---|---|
| show ip trigger-authentication | Displays the list of remote hosts for which automated double authentication has been attempted. |

# dnis (AAA preauthentication)

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** authentication, authorization, and accounting (AAA) preauthentication configuration command. To remove the **dnis** command from your configuration, use the **no** form of this command.

**dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

**no dnis** [**if-avail** | **required**] [**accept-stop**] [**password** *string*]

## Syntax Description

| | |
|---|---|
| **if-avail** | (Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes. |
| **required** | (Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails. |
| **accept-stop** | (Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element. |
| **password** *string* | (Optional) Password to use in the Access-Request packet. The default is cisco. |

## Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

## Command Modes

AAA preauthentication configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |

## Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

## Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 group radius
 dnis password Ascend-DNIS
```

## Related Commands

| Command | Description |
|---|---|
| **aaa preauth** | Enters AAA preauthentication mode. |
| **group** | Selects the security server to use for AAA preauthentication. |
| **isdn guard-timer** | Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request. |

# group

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

**group** {**tacacs+** *server-group*}

**no group** {**tacacs+** *server-group*}

## Syntax Description

| | |
|---|---|
| **tacacs+** | Uses a TACACS+ server for authentication. |
| *server-group* | Name of the server group to use for authentication. |

## Defaults

No method list is configured.

## Command Modes

AAA preauthentication configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |

## Usage Guidelines

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

## Examples

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
 group abc123
 dnis password aaa-DNIS
```

## Related Commands

| Command | Description |
|---|---|
| **aaa preauth** | Enters AAA preauthentication mode. |
| **dnis (AAA preauthentication)** | Enables AAA preauthentication using DNIS. |

# ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** command in global configuration mode. To disable the automated part of double authentication, use the **no** form of this command.

**ip trigger-authentication** [**timeout** *seconds*] [**port** *number*]

**no ip trigger-authentication**

## Syntax Description

| | |
|---|---|
| **timeout** *seconds* | (Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds. See "The Timeout Keyword" in the Usage Guidelines section for details. |
| **port** *number* | (Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500. See "The Port Keyword" in the Usage Guidelines section for details. |

## Defaults

The default timeout is 90 seconds, and the default port number is 7500.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

Configure this command on the local device (router or network access server) that remote users dial in to. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

### The Timeout Keyword

During the second authentication stage of double authentication—when the remote user is authenticated—the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user's host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.

(This timeout also applies to how long entries will remain in the remote host table; see the **show ip trigger-authentication** command for details.)

### The Port Keyword

As described in the previous section, the local device sends a UDP packet to the remote user's host to request the user's username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is used by another application, you should change the port number using the **port** keyword. If you change the port number you need to change it in both places—both on the local device and in the remote host client software.

## Examples

The following example globally enables automated double authentication and sets the timeout to 120 seconds:

```
ip trigger-authentication timeout 120
```

## Related Commands

| Command | Description |
|---|---|
| **ip trigger-authentication (interface)** | Specifies automated double authentication at an interface. |
| **show ip trigger-authentication** | Displays the list of remote hosts for which automated double authentication has been attempted. |

# ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the **ip trigger-authentication** command in interface configuration mode. To turn off automated double authentication at an interface, use the **no** form of this command.

**ip trigger-authentication**

**no ip trigger-authentication**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Automated double authentication is not enabled for specific interfaces.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the **ip trigger-authentication** (global) command.

This command causes double authentication to occur automatically when users dial into the interface.

## Examples

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
 ip trigger-authentication
 encapsulation ppp
 ppp authentication chap
```

## Related Commands

| Command | Description |
|---|---|
| **ip trigger-authentication (global)** | Enables the automated part of double authentication at a device. |

# login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication** command in line configuration mode. To return to the default specified by the **aaa authentication login** command, use the **no** form of this command.

**login authentication** {**default** | *list-name*}

**no login authentication** {**default** | *list-name*}

## Syntax Description

| | |
|---|---|
| **default** | Uses the default list created with the **aaa authentication login** command. |
| *list-name* | Uses the indicated list created with the **aaa authentication login** command. |

## Defaults

Uses the default set with **aaa authentication login**.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).

**Caution** If you use a *list-name* value that was not configured with the **aaa authentication login** command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login** command.

## Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called *list1* is to be used on line 7:

```
line 7
 login authentication list1
```

**Related Commands**

| Command | Description |
|---|---|
| aaa authentication login | Sets AAA authentication at login. |

# nasi authentication

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

**nasi authentication** {**default** | *list-name*}

**no nasi authentication** {**default** | *list-name*}

## Syntax Description

| | |
|---|---|
| **default** | Uses the default list created with the **aaa authentication nasi** command. |
| *list-name* | Uses the list created with the **aaa authentication nasi** command. |

## Defaults

Uses the default set with the **aaa authentication nasi** command.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |

## Usage Guidelines

This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is not specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.

**Caution** If you use a *list-name* value that was not configured with the **aaa authentication nasi** command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

## Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4
 nasi authentication default
```

The following example specifies that the AAA authentication list called *list1* be used on line 7:

```
line 7
 nasi authentication list1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication nasi** | Specifies AAA authentication for NASI clients connecting through the access server. |
| **ipx nasi-server enable** | Enables NASI clients to connect to asynchronous devices attached to a router. |
| **show ipx nasi connections** | Displays the status of NASI connections. |
| **show ipx spx-protocol** | Displays the status of the SPX protocol stack and related counters. |

# ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) or both and to specify the order in which CHAP and PAP authentication are selected on the interface, use the **ppp authentication** command in interface configuration mode. To disable this authentication, use the **no** form of this command.

**ppp authentication** {*protocol1* [*protocol2...*]} [**if-needed**] [*list-name* | **default**] [**callin**] [**one-time**] [**optional**]

**no ppp authentication**

## Syntax Description

| | |
|---|---|
| *protocol1* [*protocol2...*] | Specify at least one of the keywords described in Table 8. |
| **if-needed** | (Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces. |
| *list-name* | (Optional) Used with AAA. Specifies the name of a list of methods of authentication to use. If no list name is specified, the system uses the default. The list is created with the **aaa authentication ppp** command. |
| **default** | (Optional) The name of the method list is created with the **aaa authentication ppp** command. |
| **callin** | (Optional) Specifies authentication on incoming (received) calls only. |
| **one-time** | (Optional) Accepts the username and password in the username field. |
| **optional** | (Optional) Accepts the connection even if the peer refuses to accept the authentication methods that the router has requested. |

## Defaults

PPP authentication is not enabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.1(0.1) | The **optional** keyword was added. |

## Usage Guidelines

When you enable CHAP or PAP authentication (or both), the local router requires the remote device to prove its identity before allowing data traffic to flow. PAP authentication requires the remote device to send a name and a password, which is checked against a matching entry in the local username database or in the remote security server database. CHAP authentication sends a challenge message to the remote device. The remote device encrypts the challenge value with a shared secret and returns the encrypted value and its name to the local router in a Response message. The local router attempts to match the

remote device's name with an associated secret stored in the local username or remote security server database; it uses the stored secret to encrypt the original challenge and verify that the encrypted values match.

You can enable CHAP, MS-CHAP, or PAP in any order. If you enable all three methods, the first method specified is requested during link negotiation. If the peer suggests using the second method, or refuses the first method, the second method is tried. Some remote devices support only one method. Base the order in which you specify methods on the remote device's ability to correctly negotiate the appropriate method, and on the level of data line security you require. PAP usernames and passwords are sent as clear text strings, which can be intercepted and reused.

**Caution** If you use a *list-name* value that was not configured with the **aaa authentication ppp** command, you will disable PPP on this interface.

Table 8 lists the protocols used to negotiate PPP authentication.

***Table 8 ppp authentication Protocols***

| | |
|---|---|
| **chap** | Enables CHAP on a serial interface. |
| **ms-chap** | Enables Microsoft's version of CHAP (MS-CHAP) on a serial interface. |
| **pap** | Enables PAP on a serial interface. |

Enabling or disabling PPP authentication does not affect the local router's ability to authenticate itself to the remote device.

If you are using autoselect on a tty line, you can use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

MS-CHAP is the Microsoft version of CHAP. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a personal computer using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server.

Enabling or disabling PPP authentication does not affect the local router's willingness to authenticate itself to the remote device.

If you are using autoselect on a tty line, you probably want to use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

## Examples

The following example enables CHAP on asynchronous interface 4 and uses the authentication list MIS-access:

```
interface async 4
 encapsulation ppp
 ppp authentication chap MIS-access
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication method for use on serial interfaces running PPP. |
| **aaa new-model** | Enables the AAA access control model. |

| Command | Description |
|---|---|
| **autoselect** | Configures a line to start an ARAP, PPP, or SLIP session. |
| **encapsulation** | Sets the encapsulation method used by the interface. |
| **username** | Establishes a username-based authentication system, such as PPP CHAP and PAP. |

# ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when authenticating with Challenge Handshake Authentication Protocol (CHAP), use the **ppp chap hostname** command in interface configuration mode. To disable this function, use the **no** form of the command.

**ppp chap hostname** *hostname*

**no ppp chap hostname** *hostname*

## Syntax Description

| | |
|---|---|
| *hostname* | The name sent in the CHAP challenge. |

## Defaults

Disabled. The router name is sent in any CHAP challenges.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |

## Usage Guidelines

The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group to use so that only one username must be configured on the dialing routers.

This command is normally used with local CHAP authentication (when the router authenticates to the peer), but it can also be used for remote CHAP authentication.

## Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specifies “ppp” as the encapsulation method used by all member interfaces. This example shows that CHAP authentication is used on received calls only and the username ISPCorp will be sent in all CHAP challenges and responses.

```
interface dialer 0
 encapsulation ppp
 ppp authentication chap callin
 ppp chap hostname ISPCorp
```

## Related Commands

| Command | Description |
|---|---|
| aaa authentication ppp | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| ppp authentication | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |
| ppp chap password | Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer. |
| ppp chap refuse | Refuses CHAP authentication from peers requesting it. |
| ppp chap wait | Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router. |

# ppp chap password

To enable a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common Challenge Handshake Authentication Protocol (CHAP) secret password to use in response to challenges from an unknown peer, use the **ppp chap password** command in interface configuration mode. To disable the PPP CHAP password, use the **no** form of this command.

**ppp chap password** *secret*

**no ppp chap password** *secret*

## Syntax Description

| | |
|---|---|
| *secret* | The secret used to compute the response value for any CHAP challenge from an unknown peer. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |

## Usage Guidelines

This command allows you to replace several username and password configuration commands with a single copy of this command on any dialer interface or asynchronous group interface.

This command is used for remote CHAP authentication only (when routers authenticate to the peer) and does not affect local CHAP authentication.

## Examples

The commands in the following example specify ISDN BRI number 0. The method of encapsulation on the interface is PPP. If a CHAP challenge is received from a peer whose name is not found in the global list of usernames, the encrypted secret 7 1267234591 is decrypted and used to create a CHAP response value.

```
interface bri 0
 encapsulation ppp
 ppp chap password 7 1234567891
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **ppp authentication** | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |

| Command | Description |
|---|---|
| **ppp chap hostname** | Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP. |
| **ppp chap refuse** | Refuses CHAP authentication from peers requesting it. |
| **ppp chap wait** | Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router. |

# ppp chap refuse

To refuse Challenge Handshake Authentication Protocol (CHAP) authentication from peers requesting it, use the **ppp chap refuse** command in interface configuration mode. To allow CHAP authentication, use the **no** form of this command.

**ppp chap refuse** [**callin**]

**no ppp chap refuse** [**callin**]

## Syntax Description

| | |
|---|---|
| **callin** | (Optional) This keyword specifies that the router will refuse to answer CHAP authentication challenges received from the peer, but will still require the peer to answer any CHAP challenges the router sends. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

This command specifies that CHAP authentication is disabled for all calls, meaning that all attempts by the peer to force the user to authenticate using CHAP will be refused. If the **callin** keyword is used, CHAP authentication is disabled for incoming calls from the peer, but will still be performed on outgoing calls to the peer.

If outbound Password Authentication Protocol (PAP) has been enabled (using the **ppp pap sent-username** command), PAP will be suggested as the authentication method in the refusal packet.

## Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables CHAP authentication from occurring if a peer calls in requesting CHAP authentication.

```
interface bri 0
 encapsulation ppp
 ppp chap refuse
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **ppp authentication** | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |

| Command | Description |
|---|---|
| **ppp chap hostname** | Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP. |
| **ppp chap password** | Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer. |
| **ppp chap wait** | Specifies that the router will not authenticate to a peer requesting CHAP authentication until after the peer has authenticated itself to the router. |

# ppp chap wait

To specify that the router will not authenticate to a peer requesting Challenge Handshake Authentication Protocol (CHAP) authentication until after the peer has authenticated itself to the router, use the **ppp chap wait** command in interface configuration mode. To allow the router to respond immediately to an authentication challenge, use the **no** form of this command.

**ppp chap wait** *secret*

**no ppp chap wait** *secret*

## Syntax Description

| | |
|---|---|
| *secret* | The secret used to compute the response value for any CHAP challenge from an unknown peer. |

## Defaults

Enabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |

## Usage Guidelines

This command (which is enabled by default) specifies that the router will not authenticate to a peer requesting CHAP authentication until the peer has authenticated itself to the router. The **no** form of this command specifies that the router will respond immediately to an authentication challenge.

## Examples

The following example specifies ISDN BRI number 0. The method of encapsulation on the interface is PPP. This example disables the default, meaning that users do not have to wait for peers to complete CHAP authentication before authenticating themselves.

```
interface bri 0
 encapsulation ppp
 no ppp chap wait
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| **ppp authentication** | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |
| **ppp chap hostname** | Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP. |

| Command | Description |
|---|---|
| ppp chap password | Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer. |
| ppp chap refuse | Refuses CHAP authentication from peers requesting it. |

# ppp pap refuse

To refuse a peer request to authenticate remotely with PPP using Password Authentication Protocol, use the **ppp pap refuse** interface configuration command. To disable the refusal, use the **no** form of this command.

**ppp pap refuse**

**no ppp pap refuse**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |

## Usage Guidelines

Use this command to refuse remote PAP support; for example, to respond to the peer request to authenticate with PAP.

This is a per-interface command.

## Examples

The following example shows how to enable the **ppp pap** command to refuse a peer request for remote authentication:

```
interface dialer 0
 encapsulation ppp
 ppp pap refuse
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication ppp** | Specifies one or more AAA authentication methods for use on serial interfaces running PPP and TACACS+. |
| **encapsulation ppp** | Sets PPP as the encapsulation method used by a serial or ISDN interface. |
| **ppp authentication** | Enables CHAP or PAP or both, and specifies the order in which CHAP and PAP authentication are selected on the interface. |
| **ppp pap sent-username** | Reenables remote PAP support for an interface and uses the **sent-username** and **password** in the PAP authentication request packet to the peer. |

# ppp pap sent-username

To reenable remote Password Authentication Protocol (PAP) support for an interface and use the **sent-username** and **password** in the PAP authentication request packet to the peer, use the **ppp pap sent-username** command in interface configuration mode. To disable remote PAP support, use the **no** form of this command.

**ppp pap sent-username** *username* **password** *password*

**no ppp pap sent-username**

## Syntax Description

| | |
|---|---|
| *username* | Username sent in the PAP authentication request. |
| **password** | Password sent in the PAP authentication request. |
| *password* | Must contain from 1 to 25 uppercase and lowercase alphanumeric characters. |

## Defaults

Remote PAP support disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |

## Usage Guidelines

Use this command to reenable remote PAP support (for example, to respond to the peer's request to authenticate with PAP) and to specify the parameters to be used when sending the PAP authentication request.

This is a per-interface command. You must configure this command for each interface.

## Examples

The following example identifies dialer interface 0 as the dialer rotary group leader and specify PPP as the method of encapsulation used by the interface. Authentication is by CHAP or PAP on received calls only. ISPCorp is the username sent to the peer if the peer requires the router to authenticate with PAP.

```
interface dialer0
 encapsulation ppp
 ppp authentication chap pap callin
 ppp chap hostname ISPCorp
 ppp pap sent username ISPCorp password 7 fjhfeu
```

## Related Commands

| Command | Description |
|---|---|
| aaa authentication ppp | Specifies one or more AAA authentication methods for use on serial interfaces running PPP. |
| ppp authentication | Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface. |
| ppp chap hostname | Creates a pool of dialup routers that all appear to be the same host when authenticating with CHAP. |
| ppp chap password | Enables a router calling a collection of routers that do not support this command (such as routers running older Cisco IOS software images) to configure a common CHAP secret password to use in response to challenges from an unknown peer. |

# show ip trigger-authentication

To view the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** command in privileged EXEC mode.

**show ip trigger-authentication**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3 T | This command was introduced. |

## Usage Guidelines

Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a User Datagram Protocol (UDP) packet to the remote user's host. When the UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command. You can change the timeout period with the **ip trigger-authentication** (global) command.

Use this command to view the list of remote hosts for which automated double authentication has been attempted.

## Examples

The following example shows output from the **show ip trigger-authentication** command:

```
Router# show ip trigger-authentication

Trigger-authentication Host Table:
Remote Host          Time Stamp
172.21.127.114       2940514234
```

This output shows that automated double authentication was attempted for a remote user; the remote user's host has the IP address 172.21.127.114. The attempt to automatically double authenticate occurred when the local host (myfirewall) sent the remote host (172.21.127.114) a packet to UDP port 7500. (The default port was not changed in this example.)

## Related Commands

| Command | Description |
|---|---|
| clear ip trigger-authentication | Clears the list of remote hosts for which automated double authentication has been attempted. |

# show ppp queues

To monitor the number of requests processed by each authentication, authorization, and accounting (AAA) background process, use the **show ppp queues** command in privileged EXEC mode.

**show ppp queues**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3(2)AA | This command was introduced. |

## Usage Guidelines

Use the **show ppp queues** command to display the number of requests handled by each AAA background process, the average amount of time it takes to complete each request, and the requests still pending in the work queue. This information can help you balance the data load between the network access server and the AAA server.

This command displays information about the background processes configured by the **aaa processes** global configuration command. Each line in the display contains information about one of the background processes. If there are AAA requests in the queue when you enter this command, the requests will be printed as well as the background process data.

## Examples

The following example shows output from the **show ppp queues** command:

```
Router# show ppp queues

Proc #0   pid=73  authens=59   avg. rtt=118s. authors=160  avg. rtt=94s.
Proc #1   pid=74  authens=52   avg. rtt=119s. authors=127  avg. rtt=115s.
Proc #2   pid=75  authens=69   avg. rtt=130s. authors=80   avg. rtt=122s.
Proc #3   pid=76  authens=44   avg. rtt=114s. authors=55   avg. rtt=106s.
Proc #4   pid=77  authens=70   avg. rtt=141s. authors=76   avg. rtt=118s.
Proc #5   pid=78  authens=64   avg. rtt=131s. authors=97   avg. rtt=113s.
Proc #6   pid=79  authens=56   avg. rtt=121s. authors=57   avg. rtt=117s.
Proc #7   pid=80  authens=43   avg. rtt=126s. authors=54   avg. rtt=105s.
Proc #8   pid=81  authens=139  avg. rtt=141s. authors=120  avg. rtt=122s.
Proc #9   pid=82  authens=63   avg. rtt=128s. authors=199  avg. rtt=80s.
queue len=0 max len=499
```

Table 9 describes the fields shown in the example.

*Table 9 show ppp queues Field Descriptions*

| Field | Description |
|---|---|
| Proc # | Identifies the background process allocated by the **aaa processes** command to handle AAA requests for PPP. All of the data in this row relates to this process. |
| pid= | Identification number of the background process. |
| authens= | Number of authentication requests the process has performed. |
| avg. rtt= | Average delay (in seconds) until the authentication request was completed. |
| authors= | Number of authorization requests the process has performed. |
| avg. rtt= | Average delay (in seconds) until the authorization request was completed. |
| queue len= | Current queue length. |
| max len= | Maximum length the queue ever reached. |

## Related Commands

| Command | Description |
|---|---|
| **aaa processes** | Allocates a specific number of background processes to be used to process AAA authentication and authorization requests for PPP. |

# timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response** command in line configuration mode. To set the timeout value to 0 seconds, use the **no** form of this command.

**timeout login response** *seconds*

**no timeout login response** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds. |

## Defaults

The default login timeout value is 30 seconds.

## Command Modes

Line configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |

## Examples

The following example changes the login timeout value to 60 seconds:

```
line 10
 timeout login response 60
```