

MS-CHAP Support

Feature Summary

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is the Microsoft version of CHAP and is an extension to RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

MS-CHAP differs from the standard CHAP as follows:

- MS-CHAP is enabled by negotiating CHAP Algorithm 0x80 in LCP option 3, Authentication Protocol.
- The MS-CHAP Response packet is in a format designed to be compatible with Microsoft Windows NT 3.5 and 3.51, Microsoft Windows 95, and Microsoft LAN Manager 2.x. This format does not require the authenticator to store a clear or reversibly encrypted password.
- MS-CHAP provides an authenticator-controlled authentication retry mechanism.
- MS-CHAP provides an authenticator-controlled change password mechanism.
- MS-CHAP defines a set of “reason-for failure” codes returned in the Failure packet message field.

Depending on the security protocols you have implemented, PPP authentication using MS-CHAP can be used with or without Authentication, Authorization and Accounting (AAA) security services. If you have enabled AAA, PPP authentication using MS-CHAP can be used in conjunction with both TACACS+ and RADIUS. Two new vendor-specific RADIUS attributes (IETF Attribute 26) were added to enable RADIUS to support MS-CHAP. These new attributes are listed in Table 1.

Table 1 Vendor-Specific RADIUS Attributes for MS-CHAP

Vendor-ID Number	Vendor-Type Number	Vendor-Proprietary Attribute	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by a NAS to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets.
311	1	MSCHAP-Response	Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier.

For a complete list of supported IETF and vendor-proprietary RADIUS attributes, refer to the “RADIUS Attributes” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Benefits

MS-CHAP enables PPP authentication between a PC using Microsoft Windows 95 or Microsoft Windows NT and a Cisco router or access server.

Platforms

The following platforms support MS-CHAP:

- Cisco 2500 series
- Cisco 3600 series
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco AS5200 series
- Cisco 7000 series
- Cisco 7200 series
- Cisco 7500 series

Prerequisites

If you are using RADIUS or TACACS+, you must configure security using AAA network security services before you can configure your NAS for PPP authentication using MS-CHAP. To configure security on a Cisco router or access server using AAA, complete the following tasks:

- 1 Enable AAA by using the **aaa new-model** global configuration command. For more information about enabling AAA, refer to the “AAA Overview” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- 2 Configure security protocol parameters, such as RADIUS or TACACS+. For more information about configuring RADIUS, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*. For more information about configuring TACACS+, refer to the “Configuring TACACS+” chapter in the Cisco IOS 11.3 *Security Configuration Guide*.
- 3 Define the method lists for authentication by using the **aaa authentication** command. For more information about defining authentication method lists or configuring other authentication parameters, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- 4 Apply the method lists to a particular line or interface, if required. For more information about applying authentication method lists, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

- 5 (Optional) Configure authorization using the **aaa authorization** command. For more information about configuring authorization parameters, refer to the “Configuring Authorization” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- 6 (Optional) Configure accounting using the **aaa accounting** command. For more information about configuring accounting parameters, refer to the “Configuring Accounting” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

For detailed information about any of the commands listed above, refer to the Cisco IOS Release 11.3 *Security Command Reference*.

Supported MIBs and RFCs

No MIBs are supported by this feature.

This feature is an extension to RFC 1994, “PPP Challenge Handshake Authentication Protocol (CHAP),” dated August 1996 and written by W. Simpson.

Configuration Tasks

To enable PPP authentication using MS-CHAP, perform the following tasks in interface configuration mode

Task	Command
Enable PPP encapsulation.	encapsulation ppp
Define PPP authentication using MS-CHAP.	ppp authentication ms-chap [if-needed] [list-name default] [callin] [one-time]

If you configure **ppp authentication ms-chap** on an interface, all incoming calls on that interface that initiate a PPP connection will have to be authenticated using MS-CHAP. If you configure the **ppp authentication** command with the **callin** keyword, the access server will only authenticate the remote device if the remote device initiated the call.

Authentication method lists and the **one-time** keyword are only available if you have enabled AAA—they will not be available if you are using TACACS or Extended TACACS. If you specify the name of an authentication method list with the **ppp authentication** command, PPP will attempt to authenticate the connection using the methods defined in the specified method list. If AAA is enabled and no method list is defined by name, PPP will attempt to authenticate the connection using the methods defined as the default. The **ppp authentication** command with the **one-time** keyword enables support for one-time passwords during authentication.

The **if-needed** keyword is only available if you are using TACACS or Extended TACACS. The **ppp authentication** command with the **if-needed** keyword means that PPP will only authenticate the remote device via MS-CHAP if that device has not yet authenticated during the life of the current call. If the remote device authenticated through a standard login procedure and initiated PPP from the EXEC prompt, PPP will not authenticate through MS-CHAP if **ppp authentication chap if-needed** is configured.

Note If PPP authentication using MS-CHAP is used with username authentication, you must include the MS-CHAP secret in the local username/password database. For more information about username authentication, refer to the “Establish Username Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

Configuration Example

The following example configures a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) for PPP authentication using MS-CHAP:

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

username root password ALongPassword

radius-server host alcatraz
radius-server key myRaDiUSpassWoRd

interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication ms-chap dialins

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

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

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **aaa authentication ppp dialins radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network start-stop radius** command tracks PPP usage.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server host** command defines the name of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.

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

Command Reference

This section documents the modified **ppp authentication** command. All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

ppp authentication

To enable CHAP or PAP or both and to specify the order in which CHAP and PAP authentication are selected on the interface, use the **ppp authentication** interface configuration command. Use the **no** form of this command to disable this authentication.

```
ppp authentication {chap | chap pap | pap chap | pap | ms-chap} [if-needed]
  [list-name | default] [callin] [one-time]
no ppp authentication
```

Syntax Description

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
chap pap	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
pap chap	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
ms-chap	Enables Microsoft's version of CHAP (MS-CHAP) on a serial interface.
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.
<i>list-name</i>	(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	The name of the method list is created with the aaa authentication ppp command.
callin	Specifies authentication on incoming (received) calls only.
one-time	(Optional) Accepts the username and password in the username field.



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.

Default

PPP authentication is not enabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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 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 PAP or CHAP (or both) in either order. If you enable both 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 CHAP and some support only PAP. 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. CHAP has eliminated most of the known security holes.

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 PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

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.

Example

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

aaa authentication ppp
aaa new-model
autoselect
encapsulation ppp
ppp-use-tacacs
username

