



MSCHAP Version 2

First Published: 12.(2)XB5

Last Updated: February 28, 2006

The MSCHAP Version 2 feature allows users of the Microsoft Windows 2000 operating system to establish remote PPP sessions without having to first configure an authentication method on the client. This feature introduces mutual authentication between peers and allows the client to change the account password if the RADIUS server reports that the password has expired.

History for the MSCHAP Version 2 Feature

Release	Modification
12.2(2)XB5	This feature was introduced.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 2](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)



Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2004–2005 Cisco Systems, Inc. All rights reserved.

Feature Overview

The MSCHAP Version 2 feature in Cisco IOS Release 12.2(13)T introduces the ability of Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS). MSCHAP V2 authentication is an updated version of MSCHAP that is similar to but incompatible with MSCHAP Version 1 (V1). MSCHAP V2 introduces mutual authentication between peers and a change password feature.

Benefits

MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Support of this authentication method on Cisco routers will enable users of the Microsoft Windows 2000 operating system to establish remote PPP sessions without needing to first configure an authentication method on the client.

MSCHAP V2 authentication introduces an additional feature not available with MSCHAP V1 or standard CHAP authentication, the change password feature. This feature allows the client to change the account password if the RADIUS server reports that the password has expired.

Restrictions

The client operating system must support all MSCHAP V2 capabilities.

MSCHAP V2 authentication is not compatible with MSCHAP V1 authentication.

The change password feature is supported only for RADIUS authentication. This feature is not available for local authentication.

In order for the MSCHAP Version 2 feature to correctly interpret the authentication failure attribute sent by the RADIUS server, the **ppp max-bad-auth** command must be configured and the number of authentication retries must be set at two or more.

In order for the MSCHAP Version 2 feature to support the ability to change a password, the authentication failure attribute sent by the RADIUS server must be correctly interpreted as described in this section. In addition, the **radius server vsa send authentication** command must be configured, allowing the RADIUS client to send a vendor-specific attribute to the RADIUS server. The change password feature is supported only for RADIUS authentication.

The Microsoft Windows 2000, Microsoft Windows XP, and Microsoft Windows NT operating systems have a known caveat that prevents the change password function from working. This caveat can be fixed by downloading a patch from Microsoft at the following URL:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q326770>

Prerequisites

Before enabling MSCHAP V2 authentication on the NAS, you must perform the following tasks:

- Configure an interface type and enter interface configuration mode by using the **interface** command.
- Configure the interface for PPP encapsulation by using the **encapsulation** command.

For more information on completing these tasks, refer to the section “PPP Configuration” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

The RADIUS server must be configured for authentication. Refer to vendor-specific documentation for information on configuring RADIUS authentication on the RADIUS server.

Configuration Tasks

See the following sections for configuration tasks for the MSCHAP Version 2 feature. Each task in the list is identified as either required or optional.

- [Configuring MSCHAP V2 Authentication, page 3](#) (required)
- [Verifying MSCHAP V2 Configuration, page 3](#) (optional)

Configuring MSCHAP V2 Authentication

MSCHAP V2 authentication requires prior configuration of an interface type and PPP encapsulation. For more information on configuring PPP, refer to the section “PPP Configuration” in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2.

To configure the NAS to accept MSCHAP V2 authentication for local or RADIUS authentication, and to allow proper interpretation of authentication failure attributes and vendor-specific RADIUS attributes for RADIUS authentication, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router# radius-server vsa send authentication	Configures the NAS to recognize and use vendor-specific attributes.
Step 2	Router# interface <i>type number</i>	Configures an interface type and enters interface configuration mode.
Step 3	Router(config-if)# ppp max-bad-auth <i>number</i>	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries. The <i>number</i> argument must be set to a value of at least 2 for authentication failure attributes to be interpreted by the NAS.
Step 4	Router(config-if)# ppp authentication ms-chap-v2	Enables MSCHAP V2 authentication on a NAS.

Verifying MSCHAP V2 Configuration

To verify that the MSCHAP Version 2 feature is configured properly, perform the following steps:

- Step 1** Enter the **show running-config** command with the **interface** *type number* keyword and argument combination to verify the configuration of MSCHAP V2 as the authentication method for that interface:

```
Router# show running-config interface async 65

interface Async65
ip address 10.0.0.2 255.0.0.0
encapsulation ppp
async mode dedicated
```

```
no peer default ip address
ppp max-bad-auth 3
ppp authentication ms-chap-v2
```

Step 2 Enter the **debug ppp** command with the **negotiation** keyword to verify successful MSCHAP V2 negotiation:

```
Router# debug ppp negotiation
```

```
*Jan 15 13:24:43.999:Se0/0 PPP:Using configured call direction
*Jan 15 13:24:43.999:Se0/0 PPP:Treating connection as a callin
*Jan 15 13:24:43.999:Se0/0 PPP:Phase is ESTABLISHING, Passive Open
*Jan 15 13:24:43.999:Se0/0 LCP:State is Listen
*Jan 15 13:24:44.023:Se0/0 LCP:I CONFREQ [Listen] id 1 len 14
*Jan 15 13:24:44.023:Se0/0 LCP: MRU 1492 (0x010405D4)
*Jan 15 13:24:44.023:Se0/0 LCP: MagicNumber 0x308783B9 (0x0506308783B9)
*Jan 15 13:24:44.023:Se0/0 LCP:O CONFREQ [Listen] id 1 len 19
*Jan 15 13:24:44.023:Se0/0 LCP: MRU 1492 (0x010405D4)
*Jan 15 13:24:44.023:Se0/0 LCP: AuthProto MS-CHAP-V2 (0x0305C22381)
*Jan 15 13:24:44.023:Se0/0 LCP: MagicNumber 0x308A180D (0x0506308A180D)
*Jan 15 13:24:44.027:Se0/0 LCP:O CONFACK [Listen] id 1 len 14
*Jan 15 13:24:44.027:Se0/0 LCP: MRU 1492 (0x010405D4)
*Jan 15 13:24:44.027:Se0/0 LCP: MagicNumber 0x308783B9 (0x0506308783B9)
*Jan 15 13:24:44.027:Se0/0 LCP:I CONFACK [ACKsent] id 1 len 19
*Jan 15 13:24:44.027:Se0/0 LCP: MRU 1492 (0x010405D4)
*Jan 15 13:24:44.027:Se0/0 LCP: AuthProto MS-CHAP-V2 (0x0305C22381)
*Jan 15 13:24:44.027:Se0/0 LCP: MagicNumber 0x308A180D (0x0506308A180D)
*Jan 15 13:24:44.027:Se0/0 LCP:State is Open
*Jan 15 13:24:44.027:Se0/0 PPP:Phase is AUTHENTICATING, by this end
*Jan 15 13:24:44.027:Se0/0 MS-CHAP-V2:O CHALLENGE id 1 len 24 from "lac"
*Jan 15 13:24:44.031:Se0/0 MS-CHAP-V2:I RESPONSE id 1 len 58 from "haag"
*Jan 15 13:24:44.031:Se0/0 PPP:Phase is FORWARDING, Attempting Forward
*Jan 15 13:24:44.031:Se0/0 PPP:Phase is AUTHENTICATING, Unauthenticated User
*Jan 15 13:24:44.039:Se0/0 PPP:Phase is FORWARDING, Attempting Forward
*Jan 15 13:24:44.043:Se0/0 PPP:Phase is AUTHENTICATING, Authenticated User
*Jan 15 13:24:44.043:Se0/0 MS-CHAP-V2:O SUCCESS id 1 len 46 msg is
"S=4EE927A06B0D624448F27B4BDDA51B5620396EC3"
*Jan 15 13:24:44.043:Se0/0 PPP:Phase is UP
```

Step 3 Enter the **debug ppp** command with the **authentication** keyword to verify successful MSCHAP V2 authentication:

```
Router# debug ppp authentication
```

```
*Jan 15 13:26:28.659:Se0/0 PPP:Authorization required
*Jan 15 13:26:28.659:Se0/0 PPP:Using configured call direction
*Jan 15 13:26:28.659:Se0/0 PPP:Treating connection as a callin
*Jan 15 13:26:28.687:Se0/0 MS-CHAP-V2:O CHALLENGE id 1 len 24 from "lac"
*Jan 15 13:26:28.691:Se0/0 MS-CHAP-V2:I RESPONSE id 1 len 58 from "haag"
*Jan 15 13:26:28.691:Se0/0 PPP:Sent MSCHAP-V2 LOGIN Request to AAA
*Jan 15 13:26:28.695:Se0/0 PPP:Received LOGIN Response from AAA = PASS
*Jan 15 13:26:28.703:Se0/0 MS-CHAP-V2:O SUCCESS id 1 len 46 msg is "S=87F5A4BE"
```

Configuration Examples

This section provides the following configuration examples:

- [Local Authentication: Example, page 5](#)
- [RADIUS Authentication: Example, page 5](#)

Local Authentication: Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  username client password secret
```

RADIUS Authentication: Example

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
  ip address 10.0.0.2 255.0.0.0
  encapsulation ppp
  async mode dedicated
  no peer default ip address
  ppp max-bad-auth 3
  ppp authentication ms-chap-v2
  exit
aaa authentication ppp default group radius
radius-server host 10.0.0.2 255.0.0.0
radius-server key secret
radius-server vsa send authentication
```

Additional References

The following sections provide references related to MSChap Version 2.

Related Documents

Related Topic	Document Title
PPP Configuration	“PPP Configuration” chapter in the <i>Cisco IOS Dial Technologies Configuration Guide</i> , Release 12.4
Dial Technologies	<i>Cisco IOS Dial Technologies Command Reference</i> , Release 12.4
Configuring PPP Authentication Using AAA	The section “Configuring PPP Authentication Using AAA” in the chapter “Configuring Authentication” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring RADIUS	“Configuring RADIUS” chapter in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4

Standards

Standard	Title
None	—

MIBs

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

RFCs

RFC	Title
RFC 1661	<i>The Point-to-Point Protocol (PPP)</i>
RFC 2548	<i>Microsoft Vendor-Specific RADIUS Attributes</i>

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents a modified command only.

- [ppp authentication ms-chap-v2](#)

ppp authentication ms-chap-v2

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication on a network access server (NAS), use the **ppp authentication ms-chap-v2** command in interface configuration mode. To disable MSCHAP V2 authentication, use the **no** form of this command.

ppp authentication ms-chap-v2

no ppp authentication ms-chap-v2

Syntax Description This command has no arguments or keywords.

Command Default MSCHAP V2 authentication is disabled.

Command Modes Interface configuration

Command History

Release	Modification
12.2(2)XB5	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

To enable MSCHAP V2 authentication, first configure PPP on the NAS. For the NAS to properly interpret authentication failure attributes and vendor-specific attributes, the **ppp max-bad-auth** command must be configured to allow at least two authentication retries and the **radius-server vsa send** command and **authentication** keyword must be enabled. The NAS must be able to interpret authentication failure attributes and vendor-specific attributes to support the ability to change an expired password.

Examples

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication locally:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 ppp max-bad-auth 3
 ppp authentication ms-chap-v2
 username client password secret
```

The following example configures PPP on an asynchronous interface and enables MSCHAP V2 authentication via RADIUS:

```
interface Async65
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
```

```

async mode dedicated
no peer default ip address
ppp max-bad-auth 3
ppp authentication ms-chap-v2
exit
aaa authentication ppp default group radius
radius-server host 10.0.0.2 255.0.0.0
radius-server key secret
radius-server vsa send authentication

```

Related Commands	Command	Description
	debug aaa authentication	Displays information on AAA/TACACS+ authorization.
	debug ppp	Displays information on traffic and exchanges in a network that is implementing PPP.
	debug radius	Displays information associated with RADIUS.
	ppp max-bad-auth	Configures a point-to-point interface not to reset itself immediately after an authentication failure but instead to allow a specified number of authentication retries.
	radius-server vsa send	Configures the network access server to recognize and use VSAs.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002, 2004–2005 Cisco Systems, Inc. All rights reserved.

