MSCHAP Version 2

First Published: January 23, 2003
Last Updated: October 14, 2009

The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows 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).

For Cisco IOS Release 12.4(6)T, MSCHAP V2 now supports a new feature: AAA Support for MSCHAPv2 Password Aging. Prior to Cisco IOS Release 12.4(6)T, when Password Authentication Protocol (PAP)-based clients sent username and password values to the authentication, authorization, and accounting (AAA) subsystem, AAA generated an authentication request to the RADIUS server. If the password expired, the RADIUS server replied with an authentication failure message. The reason for the authentication failure was not passed back to AAA subsystem; thus, users were denied access because of authentication failure but were not informed why they were denied access.

The Password Aging feature, available in Cisco IOS Release 12.4(6)T, notifies crypto-based clients that the password has expired and provides a generic way for the user to change the password. The Password Aging feature supports only crypto-based clients.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for MSCHAP Version 2" section on page 11.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Contents

Prerequisites for MSCHAP Version 2

- 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.
- Be sure that the client operating system supports all MSCHAP V2 capabilities.
- For Cisco IOS Release 12.4(6)T, the Password Aging feature only supports RADIUS authentication for crypto-based clients.
- To ensure that the MSCHAP Version 2 features correctly interpret the authentication failure attributes sent by the RADIUS server, you must configure the **ppp max-bad-auth** command and set the number of authentication retries at two or more.
- In order for the MSCHAP Version 2 feature to support the ability to change a password, the authentication failure attribute, which is sent by the RADIUS server, must be correctly interpreted as described in "Configuring MSCHAP V2 Authentication" section on page 3.

  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 feature from working. You must download a patch from Microsoft at the following URL:

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

For more information on completing these tasks, see the section "PPP Configuration" in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T. The RADIUS server must be configured for authentication. Refer to vendor-specific documentation for information on configuring RADIUS authentication on the RADIUS server.

Restrictions for MSCHAP Version 2

- MSCHAP V2 authentication is not compatible with MSCHAP V1 authentication.
- The change password option is supported only for RADIUS authentication and is not available for local authentication.

Information About MSCHAP Version 2

MSCHAP V2 authentication is the default authentication method used by the Microsoft Windows 2000 operating system. Cisco routers that support this authentication method enable Microsoft Windows 2000 operating system users to establish remote PPP sessions without configuring an authentication method on the client.

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

Note 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.

How to Configure MSCHAP Version 2

See the following sections for configuration tasks for the MSCHAP Version 2 feature.

- "Configuring MSCHAP V2 Authentication" section on page 3 (required)
- "Verifying MSCHAP V2 Configuration" section on page 5 (optional)
- "Configuring Password Aging for Crypto-Based Clients" section on page 5 (optional)

Configuring MSCHAP V2 Authentication

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **ppp max-bad-auth** *number*
6. **ppp authentication ms-chap-v2**
7. **end**

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send authentication** **Example:** `Router(config)# radius-server vsa send authentication`	Configures the NAS to recognize and use vendor-specific attributes.
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 5	**ppp max-bad-auth** *number* **Example:** `Router(config-if)# ppp max-bad-auth 2`	Configures a point-to-point interface to reset immediately after an authentication failure or within a specified number of authentication retries. • The default value for the *number* argument is 0 seconds (immediately). • The range is between 0 and 255. **Note** The *number* argument must be set to a value of at least 2 for authentication failure attributes to be interpreted by the NAS.
Step 6	**ppp authentication ms-chap-v2** **Example:** `Router(config-if)# ppp authentication ms-chap-v2`	Enables MSCHAP V2 authentication on a NAS.
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Verifying MSCHAP V2 Configuration

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

SUMMARY STEPS

1. **show running-config interface** *type number*
2. **debug ppp negotiation**
3. **debug ppp authentication**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show running-config interface** *type number* **Example:** `Router# show running-config interface Asynch65`	Verifies the configuration of MSCHAP V2 as the authentication method for the specified interface.
Step 2	**debug ppp negotiation** **Example:** `Router# debug ppp negotiation`	Verifies successful MSCHAP V2 negotiation.
Step 3	**debug ppp authentication** **Example:** `Router# debug ppp authentication`	Verifies successful MSCHAP V2 authentication.

Configuring Password Aging for Crypto-Based Clients

The AAA security services facilitate a variety of login authentication methods. Use the **aaa authentication login** command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the **aaa authentication login** command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the **login authentication** line configuration command.

After the RADIUS server requests a new password, AAA queries the crypto client, which in turn prompts the user to enter a new password.

To configure login authentication and password aging for crypto-based clients, use the following commands beginning in global configuration mode.

Note The AAA Password Expiry infrastructure notifies the Easy VPN client that the password has expired and provides a generic way for the user to change the password. Please use RADIUS-server domain-stripping feature wisely in combination with AAA password expiry support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2*...]
5. **crypto map** *map-name* **client authentication list** *list-name*

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa authentication login** {**default** | *list-name*} **passwd-expiry** *method1* [*method2...*] **Example:** `Router(config)# aaa authentication login userauthen passwd-expiry group radius`	Enables password aging for crypto-based clients on a local authentication list.
Step 5	**crypto map** *map-name* **client authentication list** *list-name* **Example:** `Router(config)# crypto map clientmap client authentication list userauthen`	Configures user authentication (a list of authentication methods) on an existing crypto map.

Configuration Examples

This section provides the following configuration examples:

- "Configuring Local Authentication: Example" section on page 7
- "Configuring RADIUS Authentication: Example" section on page 7
- "Configuring Password Aging with Crypto Authentication: Example" section on page 7

Configuring 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
```

Configuring 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
```

Configuring Password Aging with Crypto Authentication: Example

The following example configures password aging by using AAA with a crypto-based client:

```
aaa authentication login userauthen passwd-expiry group radius
!
aaa session-id common
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group 3000client
 key cisco123
 dns 10.1.1.10
 wins 10.1.1.20
 domain cisco.com
 pool ippool
 acl 153
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 10
 set transform-set myset
!
crypto map clientmap client authentication list userauthen
```

```
!
radius-server host 10.140.15.203 auth-port 1645 acct-port 1646
radius-server domain-stripping prefix-delimiter $
radius-server key cisco123
radius-server vsa send authentication
radius-server vsa send authentication 3gpp2
!
end
```

Additional References

The following sections provide references related to the MSCHAP Version 2 feature.

Related Documents

Related Topic	Document Title
Configuring PPP interfaces	The section "PPP Configuration" in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4T.
Descriptions of the tasks and commands necessary to configure and maintain Cisco networking devices	*Cisco IOS Dial Technologies Command Reference*
Lists of IOS Security Commands	*Cisco IOS Security Command Reference*
Configuring PPP authentication using AAA	The section "Configuring PPP Authentication Using AAA" in the "Configuring Authentication" module in the *Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T.
Configuring RADIUS Authentication	"Configuring RADIUS" module in the *Cisco IOS Security Configuration Guide: Securing User Services*, Release 12.4T.

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	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	*Point-to-Point Protocol (PPP)*
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*
RFC 2759	*Microsoft PPP CHAP Extensions, Version 2*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for MSCHAP Version 2

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for MSCHAP Version 2

Feature Name	Releases	Feature Information
MSCHAP Version 2	12.2(2)XB5 12.2(13)T 12.4(6)T	The MSCHAP Version 2 feature (introduced in Cisco IOS Release 12.2(2)XB5) allows 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). In 12.2(2)XB5, this feature was introduced. In 12.2(13)T, this feature was integrated into Cisco IOS Release 12.2(13)T. In 12.4(6)T, this feature was updated to include the crypto-based Password Aging feature. The following commands were introduced or modified: **aaa authentication login**, and **ppp authentication ms-chap-v2.**