



# RADIUS Timeout Set During Pre-Authentication

---

**First Published: March 17, 2003**

**Last Updated: October 5, 2009**

Some call sessions for Internet Service Provider (ISP) subscribers are billed through authentication, authorization, and accounting (AAA) messages in a prepaid time model. When these subscribers are preauthenticated, a RADIUS server checks for any remaining credit in the prepaid time model and sets a session timeout based on the credit available. The RADIUS Timeout Set During Pre-Authentication feature is useful in situations where the PPP authentication that follows the preauthentication phase of these call sessions does not return the Session-Timeout value (RADIUS attribute 27), and therefore allows the ISP to add call setup time to the subscriber's bill.

## 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 RADIUS Timeout Set During Pre-Authentication”](#) section on [page 5](#).

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 the RADIUS Timeout Set During Pre-Authentication Feature, page 2](#)
- [Information About the RADIUS Timeout Set During Pre-Authentication Feature, page 2](#)
- [How to Configure the RADIUS Timeout Set During Pre-Authentication Feature, page 2](#)
- [Additional References, page 3](#)
- [Feature Information for RADIUS Timeout Set During Pre-Authentication, page 5](#)



---

**Americas Headquarters:**

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

## Prerequisites for the RADIUS Timeout Set During Pre-Authentication Feature

- This feature is specific to RADIUS. Basic AAA authentication and preauthentication must be configured.
- Preauthentication and normal PPP authentication are required for legacy functionality.

## Information About the RADIUS Timeout Set During Pre-Authentication Feature

You need to understand the following concept about the RADIUS Timeout Set During Pre-Authentication feature:

- [RADIUS Attribute 27 and the PPP Authentication Phase, page 2](#)

## RADIUS Attribute 27 and the PPP Authentication Phase

The RADIUS Timeout Set During Pre-Authentication feature was developed for ISPs that want to bill dial-in subscribers for call setup time and the entire duration of the call session. These subscribers are billed through AAA messages in a prepaid time model. When the subscribers are preauthenticated, a RADIUS server checks for any remaining credit in the prepaid time model and sets a session timeout (in minutes or seconds) based on the credit available. This time can range from a few seconds for ISDN users, to much longer for asynchronous dial-up subscribers.

Until the RADIUS Timeout Set During Pre-Authentication feature was developed, the value of RADIUS attribute 27, which is returned during the preauthentication phase of a call, was either ignored or overwritten during the PPP authentication phase. Even when the PPP authentication phase did not return a value for attribute 27, the old value obtained during the preauthentication phase was being ignored.

With the RADIUS Timeout Set During Pre-Authentication feature introduced for Cisco IOS Release 12.2(15)T, if the PPP authentication phase does not return a value for attribute 27, the old value that was returned during the preauthentication phase is saved and used to time out the session; attribute 27 is saved in a preauthentication database for future use. However, if the PPP authentication user profile has a session timeout configured and PPP authentication succeeds, the new value downloaded during PPP authentication overwrites the old attribute 27 value. By setting the session timeout value in the preauthentication phase itself, the service provider can bill the subscriber for the call setup time and the call duration.

## How to Configure the RADIUS Timeout Set During Pre-Authentication Feature

No new configuration is required. The RADIUS Timeout Set During Pre-Authentication feature is included in all Cisco platforms that support preauthentication, and that have RADIUS attribute 27, Session-Timeout, specified in a preauthentication user profile.

## Additional References

- The following sections provide references related to the RADIUS Timeout Set During Pre-Authentication feature.

## Related Documents

| Related Topic                       | Document Title   |
|-------------------------------------|--|
| RADIUS attributes and user profiles | <a href="#">“RADIUS Attributes Overview and RADIUS IETF Attributes” module</a> |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description   | Link   |
|---|--|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for RADIUS Timeout Set During Pre-Authentication

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 RADIUS Timeout Set During Pre-Authentication

| Feature Name                                 | Releases                | Feature Information   |
|--|-------------------------|---|
| RADIUS Timeout Set During Pre-Authentication | 12.2(15)T<br>12.2(28)SB | The RADIUS Timeout Set During Pre-Authentication feature is useful in situations where the PPP authentication that follows the preauthentication phase of these call sessions does not return the Session-Timeout value (RADIUS attribute 27), and therefore allows the ISP to add call setup time to the subscriber's bill.<br><br>This feature was introduced in Cisco IOS Release 12.2(15)T.<br><br>This feature was integrated into Cisco IOS Release 12.2(28)SB. |

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

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

© 2003–2009 Cisco Systems, Inc. All rights reserved.

