



Preauthentication Enhancements for Callback

This feature module describes the Preauthentication Enhancements for Callback feature and includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 3
- Configuration Examples, page 3
- Command Reference, page 4
- Glossary, page 5

Feature Overview

The Preauthentication Enhancements for Callback feature allows users to dial in to the network access server (NAS) without being charged. This feature enables telecommuters, and other remote network users who dial in, to have the charges applied back to the NAS that they are dialing in to.

When callback is required, the NAS hangs up the current call and dials the caller back. When the NAS performs the callback, only information for the outgoing connection is applied. The rest of the attributes from the preauthentication access-accept message are discarded.



Note

The destination IP address is not required to be returned from the RADIUS server.

How It Works

In the case of two-way authentication, the callback box will need to authenticate the NAS. The authentication username and password can be included in the access-accept message for preauthentication, and do not need to be configured locally on the NAS.

Two Cisco vendor-specific attributes (VSAs) for preauthentication are added to Attribute 26 as follows:

cisco-avpair = "preauth:send-name=<string>"

cisco-avpair = "preauth:send-secret=<string>"



Note

PPP authentication must be configured with RADIUS.

To apply for Password Authentication Protocol (PAP), do not configure the **ppp pap sent-name password** command on the interface. For PAP, "preauth:send-name" and "preauth:send-secret" will be used as the PAP username and PAP password for outbound authentication. For Challenge Handshake Authentication Protocol (CHAP), "preauth:send-name" will be used not only for outbound authentication, but also for inbound authentication.

For a CHAP inbound case, the NAS will use the name defined in "preauth:send-name" in the challenge packet to the caller box. For a CHAP outbound case, both "preauth:send-name" and "preauth:send-secret" will be used in the response packet.

Benefits

With the addition of this feature, when a caller dials in to the NAS, the charges are applied back to the NAS. Previously, a caller would be charged when dialing in to the NAS.

Restrictions

- This feature does not work when resource pooling is enabled.
- This feature does not support rotary group configurations.

Related Features and Technologies

- Preauthentication
- RADIUS

Related Documents

- *Cisco IOS Dial Services Configuration Guide: Terminal Services*, Release 12.1
- *Cisco IOS Dial Services Configuration Guide: Network Services*, Release 12.1
- *Cisco IOS Dial Services Command Reference*, Release 12.1
- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1
- *Preauthentication with ISDN PRI and Channel-Associated Signalling*, Release 12.1(3)T feature module
- *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*, Release 12.0(7)T feature module

Supported Platforms

- Cisco AS5300
- Cisco AS5800

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of MIBs supported by platform and Cisco IOS release and to download MIB modules, go to the Cisco MIB web site on Cisco Connection Online (CCO) at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

To use the Preauthentication Enhancements for Callback feature, you must be running the supporting preauthentication application on a RADIUS server in your network.

Configuration Tasks

None

Configuration Examples

This section provides the following configuration example: Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback Example.

Setting Up the RADIUS Profile for Preauthentication Enhancements for Callback Example

The following example shows a RADIUS profile configuration with a callback number of 555-1111 and the service type set to outbound. The `cisco-avpair = "preauth:send-name=<string>"` uses the string "andy", and the `cisco-avpair = "preauth:send-secret=<string>"` uses the password "cisco."

```
5551111 password = "cisco", Service-Type = Outbound
  Service-Type = Callback-Framed
  Framed-Protocol = PPP,
  Dialback-No = "5551212"
  Class = "ISP12"
  cisco-avpair = "preauth:send-name=andy"
  cisco-avpair = "preauth:send-secret=cisco"
```

Command Reference

None

Glossary

AAA—authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

authentication, authorization, and accounting—See AAA.

Challenge Handshake Authentication Protocol—See CHAP.

channel-associated signalling—See CAS.

CHAP—Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access. Compare to PAP.

NAS—network access server. Cisco platform (or collection of platforms such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the Public Switched Telephone Network).

network access server—See NAS.

PAP—Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines. Compare with CHAP.

Password Authentication Protocol—See PAP.

Point-to-Point Protocol—See PPP.

PPP—Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

RADIUS—Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

Remote Authentication Dial-In User Service—See RADIUS.

vendor-specific attribute—See VSA.

VSA—vendor-specific attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = "protocol:attribute=value".

