



# Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements

---

This feature module describes the Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements 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 4
- Glossary, page 5

## Feature Overview

Preauthentication allows a Cisco network access server (NAS) to decide—on the basis of the Dialed Number Identification Service (DNIS) number—whether to answer an incoming call. When an incoming call arrives from the public network switch but before it is answered, the NAS sends the DNIS number to a RADIUS server for authorization.

The Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements feature provides additional support for preauthentication, which was introduced in a previous Cisco IOS release. For more information about preauthentication, refer to the Cisco IOS Release 12.1(3)T feature module entitled *Preauthentication with ISDN PRI and Channel-Associated Signalling*.

This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication on the basis of the Calling Line Identification (CLID) number in the same transaction. For more information about attribute 44 and how it works with preauthentication, refer to the Cisco IOS Release 12.0(7)T feature module entitled *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

## How It Works

In the case of two-way authentication, the calling networking device will need to authenticate the NAS. The Password Authentication Protocol (PAP) username and password or Challenge Handshake Authentication Protocol (CHAP) username and password need not be configured locally on the NAS. Instead, username and password can be included in the access-accept messages for preauthentication.



### Note

The **ppp authentication** command must be configured with the **radius** method.

To apply for PAP, do not configure the **ppp pap sent-name password** command on the interface. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication.

For 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 networking device. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.

## Benefits

The Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements feature provides support for one new RADIUS attribute service type and two new attribute-value pairs.

Before Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements	Using Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements
Attribute 6 can be set to Service-Type = Outbound	Attribute 6 can also be set to Service-Type = Framed-User
Supports attribute 26 with VSAs “preauth:auth-required” with values 0 or 1 and “preauth:auth-type” with values “pap”, “chap”, and “ms-chap”.	Also supports new VSAs “preauth:send-name” with text and “preauth:send-secret” with text.

## Restrictions

This feature does not work when resource pooling is enabled.

## Related Features and Technologies

RADIUS

## Related Documents

The following documents provide information related to the Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements feature:

- *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

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 with ISDN PRI and Channel-Associated Signalling Enhancements 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 with ISDN PRI and Channel-Associated Signalling Enhancements Example.

### Setting Up the RADIUS Profile for Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements Example

The following example shows a configuration that specifies two-way authentication:

```
5551111 password = "cisco", Service-Type = Outbound
  Service-Type = Framed-User
  cisco-avpair = "preauth:auth-required=1"
  cisco-avpair = "preauth:auth-type=pap"
  cisco-avpair = "preauth:send-name=andy"
  cisco-avpair = "preauth:send-secret=cisco"
  class = "<some class>"
```

## 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.

**Caller ID**—See CLID.

**Calling Line Identification**—See CLID.

**CAS**—channel-associated signalling. Call signalling that enables the access server to send or receive analog calls.

**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.

**CLID**—Calling Line Identification. Also called Caller ID. CLID provides the number from which a call originates.

**Dialed Number Identification Service**—See DNIS.

**DNIS**—Dialed Number Identification Service. A service that provides a dialed number.

**Integrated Services Digital Network**—See ISDN.

**ISDN**—Integrated Services Digital Network. Communication protocol, offered by telephone companies, that permits telephone networks to carry data, voice, and other source traffic.

**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.

**PRI**—Primary Rate Interface. ISDN interface to primary rate access. Primary rate access consists of a single 64-Kbps D channel plus 23 (T1) or 30 (E1) B channels for voice or data.

**Primary Rate Interface**—See PRI.

**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".