Offload Server Accounting Enhancement

First Published: 12.2(4)T
Last Updated: February 28, 2006

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their network access servers (NASs) and the offload server.

History for the Offload Server Accounting Enhancement Feature

Release	Modification
12.2(4)T	This feature was introduced.
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

CISCO SYSTEMS

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

Feature Overview

The Offload Server Accounting Enhancement feature allows users to configure their network access servers (NAS) to synchronize authentication and accounting information—NAS-IP-Address (attribute 4) and Class (attribute 25)—with the offload server.

An offload server interacts with a NAS via Virtual Private Network (VPN) to perform required Point-to-Point Protocol (PPP) negotiation for calls. The NAS performs call preauthentication, whereas the offload server performs user authentication. T his feature allows the authentication and accounting data of the NAS to synchronize with the offload server as follows:

- During preauthentication, the NAS generates a unique session-id, adding the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and retrieves a Class attribute. The new session-id is sent in preauthentication requests and resource accounting requests; the Class attribute is sent in resource accounting requests.

Note Unique session-ids are needed when multiple NASs are being processed by one offload server.

- The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted to the offload server via Layer 2 Forwarding (L2F) options.
- The offload server will include the new, unique session-id in user access requests and user session accounting requests. The Class attribute that was passed from the NAS will be included in the user access request, but a new Class attribute will be received in the user access reply; this new Class attribute should be included in user session accounting requests.

Benefits

The Offload Server Accounting Enhancement feature allows users to maintain authentication and accounting information between their NAS and offload server.

Although NASs can already synchronize information with an offload server, this feature extends the functionality to include a unique session-id, adding the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and Class (attribute 25) information collected by the NASs.

Prerequisites

Before configuring the Offload Server Accounting Enhancement feature, you must perform the following tasks:

- Enable AAA. (For more information, refer to chapter “Configuring Authentication” of the *Cisco IOS Security Configuration Guide*, Release 12.4.)
- Enable VPN. (For more information, refer to the chapter “Configuring Virtual Private Networks” of the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4.)

Configuration Tasks

See the following sections for configuration tasks for the Offload Server Accounting Enhancement feature. Each task in the list is identified as either required or optional.

Configuring Unique Session IDs

To maintain unique session IDs among NASs, use the following global configuration command. When multiple NASs are being processed by one offload server, this feature must be enabled by all NASs and by the offload server to ensure a common and unique session-id.

Command	Purpose
`Router(config)# radius-server attribute 44 extend-with-addr`	Adds the accounting IP address in front of the existing AAA session ID. **Note** The unique session-id is different from other NAS session-ids because it adds the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address).

Configuring Offload Server to Synchronize with NAS Clients

To configure the offload server to synchronize accounting session information with the NAS clients, use the following global configuration command:

Command	Purpose
`Router(config)# radius-server attribute 44 sync-with-client`	Configures the offload server to synchronize accounting session information with the NAS clients.

Verifying Offload Server Accounting

To verify whether the NAS has synchronized authentication and accounting data with the offload server, use the following commands in privileged EXEC mode:

Command	Purpose
`Router# more system:running-config`	Displays the contents of the current running configuration file. (Note that the **more system:running-config** command has replaced the **show running-config** command.)
`Router(config)# debug radius`	Displays information associated with RADIUS. The output of this command shows whether attribute 44 is being sent in access requests. The output, however, does not show the entire value for attribute 44. To view the entire value for attribute 44, refer to your RADIUS server log.

Configuration Examples

This section provides the following configuration examples:

Unique Session ID Configuration Example

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
radius-server attribute 44 extend-with-addr
```

Offload Server Synchronization with NAS Clients Example

The following example shows how to configure the offload server to synchronize accounting session information with NAS clients:

```
radius-server attribute 44 sync-with-client
```

Additional References

The following sections provide references related to Offload Server Accounting Enhancement.

Related Documents

Related Topic	Document Title
Configuring Virtual Private Networks	"Configuring Virtual Private Networks" chapter in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.2
Security Configuration Guide	*Cisco IOS Security Configuration Guide*, Release 12.4
Security Commands	*Cisco IOS Security Command Reference*, Release 12.2

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
None	—

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 modified commands only.

- **radius-server attribute 44 extend-with-addr**
- **radius-server attribute 44 sync-with-client**

radius-server attribute 44 extend-with-addr

To add the accounting IP address before the existing session ID, use the **radius-server attribute 44 extend-with-addr** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 extend-with-addr

no radius-server attribute 44 extend-with-addr

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The **radius-server attribute 44 extend-with-addr** command adds Acct-Session-Id (attribute 44) before the existing session ID (NAS-IP-Address).

When multiple network access servers (NAS) are being processed by one offload server, enable this command on all NASs and the offload server to ensure a common and unique session ID.

Note This command should be enabled only when offload servers are used.

Examples

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 extend-with-addr
```

Related Commands

Command	Description
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.
radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

radius-server attribute 44 sync-with-client

To configure the offload server to synchronize accounting session information with the network access server (NAS) clients, use the **radius-server attribute 44 sync-with-client** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server attribute 44 sync-with-client

no radius-server attribute 44 sync-with-client

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use the **radius-server attribute 44 sync-with-client** command to allow the offload server to synchronize accounting session information with the NAS clients. The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted from the client to the offload server via Layer 2 Forwarding (L2F) options.

Examples

The following example shows how to configure the offload server to synchronize accounting session information with the NAS clients:

```
radius-server attribute 44 sync-with-client
```

Related Commands

Command	Description
radius-server attribute 44 extend-with-addr	Adds the accounting IP address before the existing session ID.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.

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.

Acct-Session-ID (attribute 44)—A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

Class (attribute 25)—An accounting attribute. Arbitrary value that the network access server includes in all accounting packets for this user if the attribute is supplied by the RADIUS server.

L2F—Layer 2 Forwarding. A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

NAS—network access server. A 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).

NAS-IP Address (attribute 4)—Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.

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. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VPN—A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the LNS instead of the LAC.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.