

# Authentication, Authorization, and Accounting



## Introduction

Over the years, authentication, authorization, and accounting (AAA) has changed dramatically as users of new-world access technologies seek a way to authenticate, authorize, and start accounting records for billing user time on their networks.

Cisco Systems has a rich and robust AAA implementation that enables a wide range of application clients including:

- 802.11b
- Cable and DSL
- Dial
- Firewall
- Gateway General Packet Radio Service (GPRS) and GPRS Support Node (GGSN)
- IP Security (IPSec)
- Multiprotocol Label Switching (MPLS)
- Open Settlement Protocol (OSP)
- Packet Data Serving Node (PDSN)
- Public Key Infrastructure (PKI)
- Session Initiation Protocol (SIP)
- Telco Data Communication Networks (DCNs)
- Tunneling
- Voice over IP (VoIP)
- Remote Access Dial-In User Service (RADIUS)

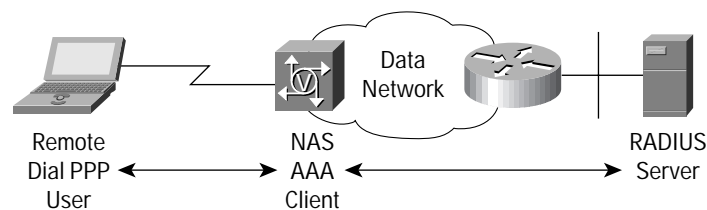
Cisco IOS<sup>®</sup> Software AAA network security services provide the primary framework to set up access control on a router or access server. Cisco IOS AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Cisco IOS AAA provides the following benefits:

- Increased flexibility and control
- Scalability
- Standardized authentication methods (RADIUS, Terminal Access Controller Access Control System Plus [TACACS+], and Kerberos)

The Cisco IOS AAA client resides on a router or network access server (NAS) and can locally perform all authentication, authorization, and accounting functions. This model does not scale because there can be a large amount of stored data. The RADIUS protocol enables use of an external server so that AAA can query and receive responses. The RADIUS protocol is based on a client/server model. A NAS such as a Cisco AS5200 Access Server operates as a client of RADIUS. The client passes user information to a designated RADIUS server and then acts on the response that is returned. The RADIUS database might contain thousands of user profiles for security, network access, and billing records, as well as other connection-related data.

Figure 1 AAA Client-to-RADIUS Server Relationship



### Need for AAA Services

Security for user access to the network and the ability to dynamically define a user's profile to gain access to network resources has a legacy dating back to asynchronous dial access. AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server. Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes.

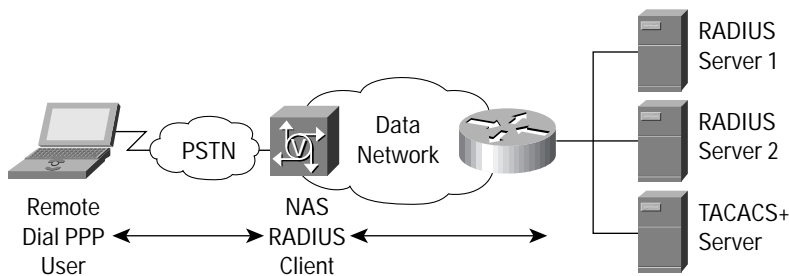
AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+. The information can also be stored locally on the access server or router. Remote security servers, such as RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

### Traditional AAA Usage

Figure 2 shows the original use of AAA: authenticating and maintaining accounting records for a dial Point-to-Point Protocol (PPP) user. In this implementation, a user dials a phone number corresponding to a port on one of the NASs at the edge of the data network. When the user ID and password are configured, the server looks locally at the NAS database or makes a query to a preconfigured RADIUS server to determine whether to permit or deny access to the network. If the user is permitted, the RADIUS server typically sends a configuration or AV pair to the NAS, which dictates the type of service permitted for that user.



Figure 2 Traditional AAA Implementation



### VoIP Prepaid Billing Solution

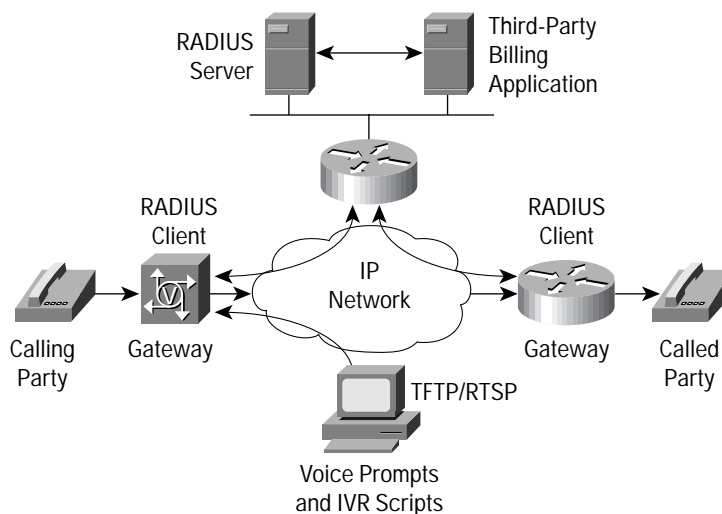
Cisco's prepaid billing VoIP implementation (Figure 3) uses the RADIUS protocol to communicate AAA information between the voice gateways and the billing application.

The market for this prepaid service includes tourists, immigrant communities, mobile populations such as military personnel, and people with limited credit histories who cannot otherwise get a private telephone line in their homes. These users can all gain immediate access to long-distance or international calling services from wherever they are located through the use of plastic prepaid calling cards that can be purchased at supermarkets and many other types of retail outlets.

The Cisco distributed VoIP prepaid calling solution requires that each voice gateway in the service provider's network run the prepaid Interactive Voice Response (IVR) script. The scripts and preferred language prompts are stored on, and run from, each gateway. The prepaid IVR script determines which audio prompts to play to the caller and collects the caller's responses entered using the telephone handset and extracted using Dual-Tone Multifrequency (DTMF) detection on each gateway. The mechanisms for timing and terminating calls also run in the VoIP gateways, ensuring that the call is disconnected if its authorized duration expires.

The prepaid calling billing application maintains all of the callers' records, authenticates the callers, rates and authorizes the calls, and updates callers' card balances at the end of all calls.

Figure 3 VoIP Prepaid Call Solution Using AAA



## The RADIUS Protocol

Implemented by several vendors of network access servers, RADIUS has gained support among a wide customer base, including Internet service providers (ISPs). Cisco supports several RADIUS server implementations such as the Access Registrar (AR) and Access Control Server (ACS).

The RADIUS protocol carries authentication, authorization and configuration information between a NAS and a RADIUS authentication server. Requests and responses carried by the RADIUS protocol are called RADIUS *attributes*. These attributes can be username, Service-Type, and so on. These attributes provide the information needed by a RADIUS server to authenticate users and to establish authorized network service for them. The RADIUS protocol also carries accounting information between a NAS and a RADIUS accounting server.

## DIAMETER Protocol

DIAMETER is a new framework in the Internet Engineering Task Force (IETF) for the next-generation AAA server. Requirements for DIAMETER are being defined by the Mobile IP ROAMOPS (Roaming Operations) TR45.6 working group, as well as by other new-world technologies where there is a need to provide authentication or authorization to network resources or to capture accounting for billing of network resource usage such as a voice call.

The DIAMETER base protocol provides an AAA framework for Mobile-IP, NASREQ, and ROAMOPS. The DIAMETER protocol does not address flaws within the RADIUS model. DIAMETER does not use the same RADIUS protocol data unit, but is backward compatible with RADIUS to ease migration. A primary difference between DIAMETER and RADIUS is that DIAMETER allows peers to exchange a variety of messages.

According to the DIAMETER RFC: “The basic concept behind DIAMETER is to provide a base protocol that can be extended in order to provide AAA services to new access technologies. Currently, the protocol only concerns itself with Internet access, both in the traditional PPP sense as well as taking into account the ROAMOPS model, and Mobile-IP.”

DIAMETER is currently not supported in the Cisco IOS Software.

### Benefits of DIAMETER

Characteristic	DIAMETER Support
Peer-to-peer bidirectional	<ul style="list-style-type: none"><li>• Framework enables push and pull application models or architectures (RADIUS is unidirectional)</li></ul>
Very efficient	<ul style="list-style-type: none"><li>• Can support 32-bit VSAs which translates to efficiency (RADIUS = 8 bits)</li><li>• Handles many more pending AAA requests</li><li>• 32-bit alignment takes advantage of new hardware processor technologies</li></ul>
Extremely reliable, highly available	<ul style="list-style-type: none"><li>• AAA client/server send/receive acknowledgment mechanism for receipt of requests</li><li>• Server supports “keepalives” notifying of failure or pending failure</li></ul>
Secure	<ul style="list-style-type: none"><li>• Authentication replay attack prevention through encryption</li></ul>



## Differences between RADIUS and DIAMETER

The DIAMETER protocol is backwardly compatible with RADIUS. DIAMETER is the next-generation AAA protocol and overcomes the following RADIUS deficiencies.

Characteristic	RADIUS Deficiency	DIAMETER Improvement
Strict limitation of attribute data	Only 1 byte reserved for the length of a data field (max. 255) in its attribute header	Reserves 2 bytes for its length of a data field (max. 16535)
Inefficient retransmission algorithm	Only 1 byte as identifier field to identify retransmissions. This limits the number of requests that can be pending (max. 255)	Reserved 4 bytes for this purpose (max. 2 <sup>32</sup> )
Inability to control flow to servers	Operates over User Datagram Protocol (UDP) and has no standard scheme to regulate UDP flow	Scheme that regulates the flow of UDP packets (windowing scheme)
End-to-end message acknowledgment	Client expects a successful or failed response after a request, but does not know whether the server has received the request	Client expects a success of failed response or an acknowledgment of the received request by the server
Silent discarding of packets	Packets that do not contain the expected information, or that have errors, are silently discarded. This might cause the client to operate as if the server is down because it does not receive any response. It would then try to send packets to a secondary server	Server can notify the client of problem by sending an error message
No failover server support	Server has no way of indicating that it is going down or is currently running	Supports keep-alive messages and messages that indicate that a server is going down for a time period
Authentication replay attacks	When using PPP CHAP any RADIUS client can generate a challenge response sequence, which can be intercepted by any RADIUS client or proxy server in the chain. Another RADIUS client can then replay this challenge response sequence at any time (partly solved by the RADIUS extension using the EAP protocol)	Challenge/response attributes can be secured using end-to-end encryption and authentication
Hop-by-hop security	Supports only hop-by-hop security; every hop can easily modify information that cannot be traced to its origin	Supports end-to-end security, which guarantees that information cannot be modified without notice
No support for user-specific commands	Supports vendor-specific attributes, but not vendor-specific commands	Supports vendor specific command codes
Heavy processing costs	Does not impose any alignment requirements, which adds an unnecessary burden on most processors	Has a 32-bit alignment requirement, which can be handled efficiently by most processors

## Summary

Cisco IOS AAA service shares a deep heritage with the traditional data dial technology market and is considered by many technology groups to possess attributes and services that are applicable to this market.

The crucial issue that must be evaluated is what applicable services can use the current RADIUS protocol implementation. Retrofitting new functionality that was never intended for RADIUS in an attempt to fit into the new world must be avoided. Many new-world technologies are requiring a secure, peer-to-peer, and reliable framework that not only has the richness of RADIUS but also the flexibility and robustness of DIAMETER, the next-generation AAA protocol.

## For More Information

For further technical information, refer to “RADIUS Support in Cisco IOS Software,” or to the Cisco configuration documentation.

AAA Web site:

[http://www.cisco.com/en/US/products/ps6663/products\\_ios\\_protocol\\_option\\_home.html](http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html)

## References

### RADIUS IETF Standard RFCs

The RADIUS protocol specifications consist of RFCs for authentication, accounting, and extensions.

- RFC 2865 - Remote Authentication Dial In User Service (RADIUS) (obsoletes RFC 2138)
- RFC 2866 - RADIUS Accounting (obsoletes RFC 2139)
- RFC 2867 - RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868 - RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 - RADIUS Extensions
- DRAFT RFC - Introduction to Accounting Management
- DRAFT RFC - Accounting Attributes and Record Formats
- DRAFT RFC - Criteria for Evaluating AAA Protocols for Network Access
- DRAFT RFC - Criteria for Evaluating NAS Protocols
- DRAFT RFC - Network Access Server Requirements Next Generation (NASREQNG) NAS Model
- DRAFT RFC - Network Access Servers Requirements: Extended RADIUS Practices

### DIAMETER RFCs

The DIAMETER protocol specification consists of IETF drafts such as the base protocol and extensions or applications such as Mobile IP, MIBs, and so on.

- <http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-07.txt>
- <http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-nasreq-07.txt>
- <http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-mobileip-07.txt>
- <http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-cms-sec-02.txt>
- <http://search.ietf.org/internet-drafts/draft-ietf-aaa-DIAMETER-api-01.txt>
- <http://search.ietf.org/internet-drafts/draft-koehler-aaa-DIAMETER-base-protocol-mib-01.txt>
- <http://search.ietf.org/internet-drafts/draft-le-aaa-DIAMETER-mobileipv6-00.txt>
- <http://search.ietf.org/rfc/rfc2002.txt>



**Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**

Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
www-europe.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney  
NSW 2060 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

**Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the**

**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0108R)

LW2789 10/01

Printed in the USA