



RADIUS Attribute Screening

First Published: 12.2(1)DX
Last Updated: February, 2006

History for the RADIUS Attribute Screening Feature

Release	Modification
12.2(1)DX	This feature was introduced.
12.2(2)DD	This feature was integrated into Cisco IOS Release 12.2(2)DD.
12.2(2)B	This feature was integrated into Cisco IOS Release 12.2(2)DD.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

Contents

- [Feature Overview, page 1](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 7](#)
- [Additional References, page 9](#)
- [Command Reference, page 9](#)
- [Glossary, page 19](#)

Feature Overview

The RADIUS Attribute Screening feature allows users to configure a list of “accept” or “reject” RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.



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

© 2001–2002, 2006 Cisco Systems, Inc. All rights reserved.

If a NAS accepts and processes *all* RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Benefits

The RADIUS Attribute Screening feature provides the following benefits:

Accept or Reject Lists

Users can configure an accept or reject list consisting of a selection of attributes on the NAS for a specific purpose so unwanted attributes are not accepted and processed.

Restricting Accept Lists to Relevant Accounting Attributes

Users might wish to configure an accept list that includes only relevant accounting attributes, thereby reducing unnecessary traffic and allowing users to customize their accounting data.

Restrictions

NAS Requirements

To enable this feature, your NAS should be configured for authorization with RADIUS groups.

Accept or Reject Lists Limitations

The two filters used to configure accept or reject lists are mutually exclusive; therefore, a user can configure only one access list or one reject list for each purpose, per server group.

Vendor-Specific Attributes

This feature does not support vendor-specific attribute (VSA) screening; however, a user can specify attribute 26 (Vendor-Specific) in an accept or reject list, which will accept or reject all VSAs.

Required Attributes Screening Recommendation

It is recommended that users do not reject the following required attributes:

- For authorization:
 - 6 (Service-Type)
 - 7 (Framed-Protocol)
- For accounting:
 - 4 (NAS-IP-Address)
 - 40 (Acct-Status-Type)

- 41 (Acct-Delay-Time)
- 44 (Acct-Session-ID)

If an attribute is required, the rejection will be refused, and the attribute will be allowed to pass through.

**Note**

The user will not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose—authorization or accounting. The server will determine whether an attribute is required when it is known what the attribute is to be used for.

Prerequisites

Before configuring a RADIUS accept or reject list, you must enable AAA.

For more information, refer to the AAA chapters in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Configuration Tasks

See the following section for configuration tasks for the RADIUS Attribute Screening feature. Each task in the list is identified as either optional or required.

- [Configuring RADIUS Attribute Screening](#) (required)
- [Verifying RADIUS Attribute Screening](#) (optional)

Configuring RADIUS Attribute Screening

To configure a RADIUS attribute accept or reject list for authorization or accounting, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa authentication ppp default group <i>group-name</i>	Specifies one or more AAA authentication methods for use on serial interfaces running PPP. default —Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. group <i>group-name</i> —Uses a subset of RADIUS servers for authentication as defined by the aaa group server radius command.
Step 2	Router(config)# aaa authorization network default group <i>group-name</i>	Sets parameters that restrict user access to the network. default —Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. group <i>group-name</i> —Uses a subset of RADIUS servers for authentication as defined by the aaa group server radius command.
Step 3	Router(config)# aaa group server radius <i>group-name</i>	Groups different RADIUS server hosts into distinct lists and distinct methods. <i>group-name</i> —Character string used to name the group of servers.
Step 4	Router(config-sg-radius)# server <i>ip-address</i>	Configures the IP address of the RADIUS server for the group server.

	Command	Purpose
Step 5	<pre>Router(config-sg-radius)# authorization [accept reject] <i>listname</i></pre> <p>or</p> <pre>Router(config-sg-radius)# accounting [accept reject] <i>listname</i></pre>	<p>Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server.</p> <p>or</p> <p>Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request.</p> <p>Note The accept keyword indicates that all attributes will be rejected except for the attributes specified in the <i>listname</i>. The reject keyword indicates that all attributes will be accepted except for the attributes specified in the <i>listname</i> and all standard attributes.</p> <p>accept—Indicates that all attributes will be rejected except for the required attributes and the attributes specified in the <i>listname</i>.</p> <p>reject—Indicates that all attributes will be accepted except for the attributes specified in the <i>listname</i>.</p> <p><i>listname</i>—Defines the given name for the accept or reject list.</p>
Step 6	<pre>Router(config-sg-radius)# exit</pre>	<p>Exits server-group configuration mode.</p>

Command	Purpose
Step 7 Router(config)# radius-server host {hostname ip-address} [key string]	<p>Specifies a RADIUS server host.</p> <p><i>hostname</i>—Domain Name System (DNS) name of the RADIUS server host.</p> <p>key—Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server.</p> <p>This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used.</p> <p>The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.</p> <p><i>string</i>—Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.</p>
Step 8 Router(config)# radius-server attribute list listname	<p>Defines the list name given to the set of attributes defined in the attribute command.</p> <p><i>listname</i>—Specifies a name for an accept or reject list.</p> <p>Note The <i>listname</i> must be the same as the <i>listname</i> defined in Step 5.</p>
Step 9 Router(config-sg-radius)# attribute value1, [value2 [value3]...]	<p>Adds attributes to the configured accept or reject list.</p> <p><i>value1, [value2 [value3]...]</i>—Specifies which attributes to include in an accept or reject list. The value can be a single integer, such as 7, or a range of numbers, such as 56–59. At least one attribute value must be specified.</p> <p>Note This command can be used multiple times to add attributes to an accept or reject list.</p>

Verifying RADIUS Attribute Screening

To verify an accept or reject list, use one of the following commands in privileged EXEC mode:

Command	Purpose
Router# <code>debug radius</code>	Displays information associated with RADIUS.
Router# <code>debug aaa accounting</code>	Displays information on accountable events as they occur.
Router# <code>debug aaa authentication</code>	Displays information on AAA authentication.
Router# <code>show radius statistics</code>	Displays the RADIUS statistics for accounting and authentication packets.

Configuration Examples

This section provides the following configuration examples:

- [Authorization Accept Example, page 7](#)
- [Accounting Reject Example, page 7](#)
- [Authorization Reject and Accounting Accept Example, page 8](#)
- [Rejecting Required Attributes Example, page 8](#)

Authorization Accept Example

The following example shows how to configure an accept list for attribute 6 (Service-Type) and attribute 7 (Framed-Protocol); all other attributes (including VSAs) are rejected for RADIUS authorization.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
    attribute 6-7
```

Accounting Reject Example

The following example shows how to configure a reject list for attribute 66 (Tunnel-Client-Endpoint) and attribute 67 (Tunnel-Server-Endpoint); all other attributes (including VSAs) are accepted for RADIUS accounting.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 10.1.1.1
    accounting reject tnl-x-endpoint
```

```

!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
attribute 66-67

```

Authorization Reject and Accounting Accept Example

The following example shows how to configure a reject list for RADIUS authorization and configure an accept list for RADIUS accounting. Although you cannot configure more than one accept or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

```

aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization reject bad-author
accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46
!
radius-server attribute list bad-author
attribute 22,27-28,56-59

```

Rejecting Required Attributes Example

The following example shows debug output for the **debug aaa accounting** command. In this example, required attributes 44, 40, and 41 have been added to the reject list:

```

Router# debug aaa authorization

AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected

```

Additional References

The following sections provide references related to Radius Attribute Screening.

Related Documents

Related Topic	Document Title
Security Commands	<i>“Cisco IOS Security Command Reference”</i> , Release 12.4
Security Configuration Tasks	<i>“Cisco IOS Security Configuration Guide”</i> , Release 12.4

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.

- **accounting (server-group)**
- **authorization (server-group)**
- **attribute**
- **radius-server attribute list**

accounting (server-group)

To specify an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request, use the **accounting** command in server-group configuration mode.

accounting [**accept** | **reject**] *list-name*

no accounting [**accept** | **reject**] *list name*

Syntax Description		
accept	(Optional) All attributes will be rejected except for required attributes and the attributes specified in the <i>listname</i> .	
reject	(Optional) All attributes will be accepted except for the attributes specified in the <i>listname</i> .	
<i>list-name</i>	Given name for the accept or reject list.	

Defaults If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes Server-group configuration

Command History	Release	Modification
	12.2(1)DX	This command was introduced.
	12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(13)T	Platform support was added for the Cisco 7401ASR.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines An accept or reject list (also known as a filter) for RADIUS accounting allows users to send only the accounting attributes their business requires, thereby reducing unnecessary traffic and allowing users to customize their own accounting data.

Only one filter may be used for RADIUS accounting per server group.



Note

The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute** (server-group configuration) command to add to an accept or reject list.

Examples

The following example shows how to specify accept list “usage-only” for RADIUS accounting:

```

aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
  server 10.1.1.1
  accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
  attribute 1,40,42-43,46

```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server attribute list	Defines an accept or reject list name.

authorization (server-group)

To filter attributes in outbound Access Requests to the RADIUS server for purposes of authentication or authorization, use the **authorization** command in server-group configuration mode. To remove the filter on the authorization request or reply, use the **no** form of the command.

authorization [**request** | **reply**] [**accept** | **reject**] *list-name*

no authorization [**request** | **reply**] [**accept** | **reject**] *list-name*

Syntax Description		
request	(Optional)	Defines filters for outgoing authorization Access Requests.
reply	(Optional)	Defines filters for incoming authorization Accept or Reject packets and for outgoing accounting requests.
accept	(Optional)	Indicates that the required attributes and the attributes specified in the <i>list-name</i> argument will be accepted. All other attributes will be rejected.
reject	(Optional)	Indicates that the attributes specified in the <i>list-name</i> will be rejected. All other attributes will be accepted.
<i>list-name</i>		Defines the given name for the accept or reject list.

Defaults If specific attributes are not accepted or rejected, all attributes will be accepted.

Command Modes Server-group configuration

Command History	Release	Modification
	12.2(1)DX	This command was introduced.
	12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(13)T	Platform support was added for the Cisco 7401ASR.
	12.3(3)B	The request and reply keywords were added.
	12.3(7)T	The request and reply keywords were integrated into Cisco IOS Release 12.3(7)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines An accept or reject list (also known as a filter) for RADIUS authorization allows users to configure the network access server (NAS) to restrict the use of specific attributes, thereby preventing the NAS from processing unwanted attributes.

Only one filter may be used for RADIUS authorization per server group.

**Note**

The listname must be the same as the listname defined in the **radius-server attribute list** command, which is used with the **attribute (server-group configuration)** command to add to an accept or reject list.

Examples

The following example shows how to configure accept list “min-author” in an Access-Accept packet from the RADIUS server:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
  server 10.1.1.1
  authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
  attribute 6-7
```

The following example shows that the attribute “all-attr” will be rejected in all outbound authorization Access Request messages:

```
aaa group server radius ras
  server 172.19.192.238 auth-port 1745 acct-port 1746
  authorization request reject all-attr
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to the user.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
radius-server attribute list	Defines an accept or reject list name.

attribute

To configure an attribute in a local service profile, use the **attribute** command in profile configuration mode. To delete an attribute from a service profile, use the **no** form of this command.

attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

no attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description

<i>radius-attribute-id</i>	RADIUS attribute ID to be configured.
<i>vendor-id</i>	(Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute (VSA). The Cisco vendor ID is 9.
<i>cisco-vsa-type</i>	(Optional) Cisco VSA type. Required if the vendor ID is 9, indicating a Cisco VSA.
<i>attribute-value</i>	Attribute value. The following optional attribute values are also supported: <ul style="list-style-type: none"> L<i>interval</i>—Required to change an interim accounting interval. Specifies the new accounting interval in seconds. Q—Configures the token bucket parameters for the Service Selection Gateway (SSG) Hierarchical Policing feature.

Defaults

For the **L***interval* option: If the L option is not defined, the accounting records for a service profile will be sent at the interval configured by the **ssg accounting interval** command. If the **ssg accounting interval** command is not set, the accounting records are sent every 600 seconds.

Otherwise, no default behavior or values are set.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(4)B	The L and Q attributes were introduced as an <i>attribute-value</i> .
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified for Cisco IOS Release 12.2(13)T.
12.4	This command was integrated into Cisco IOS Release 12.4.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

To change the SSG accounting interval for a service profile, use the *Linterval* option in the **attribute** command. For example, if L80 is entered as the attribute value, the service profile sends accounting information every 80 seconds. Interim accounting can be disabled by entering the value (in seconds) as 0 (for instance, L0). When interim accounting is disabled, the normal accounting stops and starts are still sent.

For the SSG Hierarchical Policing feature, use the Q option to configure the token bucket parameters (token rate, normal burst, and excess burst). The syntax for the Q option is as follows:

```
Router(config-prof)# attribute radius-attribute-id vendor-id cisco-vs-a-type
"QU;upstream-committed-rate;upstream-normal-burst;
[upstream-excess-burst];D;downstream-committed-rate;
downstream-normal-burst;[downstream-excess-burst]"
```

The variables are used to configure upstream (U) and downstream (D) policing. The upstream traffic is the traffic that travels from the subscriber to the network, and the downstream traffic is the traffic that travels from the network to the subscriber.

Examples

In the following example, the Cisco AV pair Upstream Access Control List (inac1) attribute is configured in the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inac1#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called "cisco.com":

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, the local profile "cisco.com" is configured to send an interim accounting update every 90 seconds:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "L90"
```

In the following example, the SSG Hierarchical Policing parameters are set for upstream and downstream traffic:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 251 "QU:8000:16000:20000:D10000:20000:30000"
```

In the following example, an open garden service called "opencisco.com" is defined.

```
Router(config)# local-profile opencisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden opencisco.com
```

Related Commands

Command	Description
debug ssg data	Displays SSG QoS information.
local-profile	Configures a local service profile.
show ssg connection	Displays information about a particular SSG connection, including the policing parameters.

Command	Description
show ssg host	Displays information about an SSG host, including whether policing is enabled or disabled and the policing configurations of a particular host.
show ssg open-garden	Displays a list of all configured open garden services.
ssg accounting interval	Specifies the interval at which accounting updates are sent to the server.
ssg open-garden	Designates a service, defined in a local service profile, to be an open garden service.
ssg qos police	Enables SSG Hierarchical Policing on a router.

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the no form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name Name for an accept or reject list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute** (server-group configuration) command, which adds attributes to an accept or reject list.



Note

The listname must be the same as the listname defined in the **accounting** or **authorization** configuration command.

Examples

The following example shows how to configure the reject list “bad-author” for RADIUS authorization and accept list “usage-only” for RADIUS accounting:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# authorization reject bad-author
```

```

Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
Router(config)# radius-server host 10.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-author
Router(config-radius-attrl)# attribute 22,27-28,56-59

```

**Note**

Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

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.

attribute—RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

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).

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.

VSA—Vendor-specific attribute. VSAs are derived from one IETF attribute—vendor-specific (attribute 26). Attribute 26 allows a vendor to create and implement an additional 255 attributes. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26; essentially, Vendor-Specific = "protocol:attribute=value".

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2001–2002, 2006 Cisco Systems, Inc. All rights reserved.