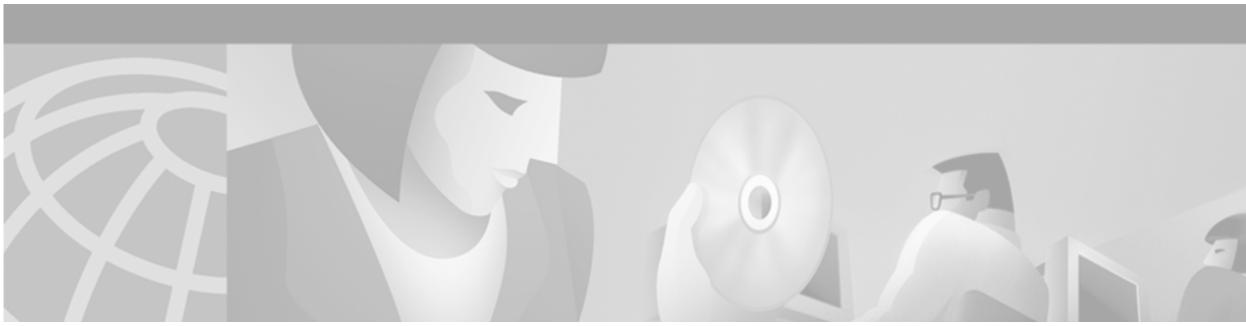

RADIUS Attribute Screening

This feature module describes the RADIUS Attribute Screening feature in Cisco IOS Release 12.2(1)DX. It includes the following sections:

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.

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:

- 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.
- Users may 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.

Related Documents

- *Cisco IOS Security Command Reference*, Release 12.2
- *Cisco IOS Security Configuration Guide*, Release 12.2

Supported Platforms

- Cisco 7200 series
- Cisco 7401 ASR router

Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you want to establish an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

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** *group-name*	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 2	Router(config)# **aaa authorization network default group** *group-name*	Sets parameters that restrict network access to the user.
Step 3	Router(config)# **aaa group server radius** *group-name*	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 4	Router(config-sg-radius)# **server** *ip-address*	Configures the IP address of the RADIUS server for the group server,
Step 5	Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname* and/or Router(config-sg-radius)# **accounting** [**accept** | **reject**] *listname*	Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server. or Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request. **Note** The **accept** keyword indicates that all attributes will be rejected except for the attributes specified in the *listname*. The **reject** keyword indicates that all attributes will be accepted except for the attributes specified in the *listname* and all standard attributes.
Step 6	Router(config-sg-radius)# **exit**	Exits server-group configuration mode.
Step 7	Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key** *string*]	Specifies a RADIUS server host.

	Command	Purpose
Step 8	`Router(config)# `**`radius-server attribute list`** *`listname`*	Defines the list name given to the set of attributes defined in the **attribute** command. **Note** The *listname* must be the same as the *listname* defined in Step 5.
Step 9	`Router(config-sg-radius)# `**`attribute`** *`value1`*`,[`*`value2`* `[`*`value3...`*`]]`	Adds attributes to the configured accept or reject list. The *value* attribute can specify a single attribute (for instance, 22) or a range of attributes (for instance, 20-30). **Note** This command can be used multiple times to add attributes to an accept or reject list.

Verifying RADIUS Attribute Screening

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

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

Configuration Examples

This section provides the following configuration examples:

- Authorization Accept Example
- Accounting Reject Example
- Authorization Reject and Accounting Accept Example
- Rejecting Required Attributes Example

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 1.1.1.1
    authorization accept min-author
!
radius-server host 1.1.1.1 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 1.1.1.1
    accounting reject tnl-x-endpoint
!
radius-server host 1.1.1.1 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 1.1.1.1
    authorization reject bad-author
    accounting accept usage-only
!
radius-server host 1.1.1.1 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 “standard.”

```
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
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

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

accounting (server-group configuration)

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**] *listname*

Syntax Description

accept	(Optional) Indicates that all attributes will be rejected except for required attributes and the attributes specified in the *listname*.
reject	(Optional) Indicates that all attributes will be accepted except for the attributes specified in the *listname*.
listname	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.

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**, which is used with the **attribute** 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 1.1.1.1
    accounting accept usage-only
!
radius-server host 1.1.1.1 key mykey1
radius-server attribute list usage-only
    attribute 1,40,42-43,46
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
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.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
attribute	Adds attributes to an accept or reject list.
radius-server attribute list	Defines an accept or reject list name.

authorization (server-group configuration)

To specify an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server, use the **authorization** command in server-group configuration mode.

authorization [**accept** | **reject**] *listname*

Syntax Description

accept	(Optional) Indicates that all attributes will be rejected except for required attributes and the attributes specified in the *listname*.
reject	(Optional) Indicates that all attributes will be accepted except for the attributes specified in the *listname*.
listname	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.

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**, which is used with the **attribute** 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 1.1.1.1
    authorization accept min-author
!
radius-server host 1.1.1.1 key mykey1
radius-server attribute list min-author
    attribute 6-7
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
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.
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	Adds attributes to an accept or reject list.
radius-server attribute list	Defines an accept or reject list name.

attribute

To add attributes to an accept or reject list, use the **attribute** command in server-group configuration mode. To remove attributes from the list, use the **no** form of this command.

attribute *value1* [*value2* [*value3*]...]

no attribute *value1* [*value2* [*value3*]...]

Syntax Description

value1 [*value2* [*value3*]...]	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.

Defaults

If this command is not enabled, all attributes are sent to the network access server (NAS).

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.

Usage Guidelines

Used in conjunction with the **radius-server attribute list** command (which defines the list name), the **attribute** command can be used to add attributes to an accept or reject list (also known as a filter). Filters are used to prevent the network access server (NAS) from receiving and processing unwanted attributes for authorization or accounting.

The **attribute** command can be used multiple times to add attributes to a filter. However, if a required attribute is specified in a reject list, the NAS will override the command and accept the attribute. Required attributes are as follows:

- 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)

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.

Examples

The following example shows how to add attributes 12, 217, 6-10, 13, 64-69, and 218 to the list name “standard”:

```
radius-server attribute list standard
   attribute 12,217,6-10,13
   attribute 64-69,218
```

Related Commands

Command	Description
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.
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.

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode.

radius-server attribute list *listname*

Syntax Description

listname	Specifies a 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.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authentication 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** 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:

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
    server 1.1.1.1
    authorization reject bad-author
    accounting accept usage-only
!
radius-server host 1.1.1.1 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
```

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.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
attribute	Adds attributes to an accept or reject list.
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".