set aggressive-mode client-endpoint through show content-scan

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command in user EXEC or privileged EXEC mode.

show aaa servers [**private**| **public**]

Syntax Description

private	(Optional) Displays private AAA servers only, which are also displayed by the AAA Server MIB.
public	(Optional) Displays public AAA servers only, which are also displayed by the AAA Server MIB.

Command Modes

User EXEC (>) privileged EXEC (#)

Command History

Release	Modification
12.2(6)T	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)S	This command was modified. Support for private RADIUS servers in CISCO-AAA-SERVER-MIB was added.
15.1(4)M	This command was modified. Support for private RADIUS servers in CISCO-AAA-SERVER-MIB was added.
15.2(4)S1	This command was modified. Support for displaying the estimated outstanding and throttled transactions (access and accounting) in the command output was added.

Usage Guidelines

Only RADIUS servers are supported by the **show aaa servers** command.

The command displays information about packets sent and received for all AAA transaction types--authentication, authorization, and accounting.

Examples

The following is sample output from the **show aaa servers private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the output fields in this part of the display are described in the table below.

```
Router# show aaa servers private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
     State: current UP, duration 375742s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 5, timeouts 1, failover 0, retransmission 1
             Response: accept 4, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 14ms
             Transaction: success 4, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 5, timeouts 0, failover 0, retransmission 0
             Request: start 3, interim 0, stop 2
             Response: start 3, interim 0, stop 2
             Response: unexpected 0, server error 0, incorrect 0, time 12ms
             Transaction: success 5, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 4d8h22m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 8 hours, 22 minutes ago: 0
             low  - 8 hours, 22 minutes ago: 0
             average: 0
```

The table below describes the significant fields in the display.

Table 1: show aaa servers Field Descriptions

Field	Description
id	A unique identifier for all AAA servers defined on the router.
priority	Order of use for servers within a group.
host	IP address of the private RADIUS server host.
auth-port	UDP destination port on the AAA server that is used for authentication and authorization requests. The default value is 1645.
acct-port	UDP destination port on the AAA server that is used for accounting requests. The default value is 1646.

Field	Description
State	Describes the current state of the AAA server; the duration, in seconds, that the server has been in that state; and the duration, in seconds, that the server was in the previous state. The following states are possible: • DEAD--Indicates that the server is currently down and, in the case of failovers, this server will be omitted unless it is the last server in the group. • duration--Indicates the amount of time the server is assumed to be in the current state, either UP or DEAD. • previous duration--Indicates the amount of time the server was considered to be in the previous state. • UP--Indicates that the server is currently considered alive and attempts will be made to communicate with it.
Dead	Indicates the number of times that this server has been marked dead, and the cumulative amount of time, in seconds, that it spent in that state.

Field	Description
Authen	

Field	Description

	Provides information about authentication packets that were sent to and received from the server, and authentication transactions that were successful or that failed. The following information may be reported in this field:
	• request--Number of authentication requests that were sent to the AAA server.
	• timeouts--Number of timeouts (no responses) that were observed when a transmission was sent to this server.
	• Response--Provides statistics about responses that were observed from this server and includes the following reports:
	  • unexpected--Number of unexpected responses. A response is considered unexpected when it is received after the timeout period for the packet has expired. This may happen if the link to the server is severely congested, for example. An unexpected response can also be produced when a server generates a response for no apparent reason.
	  • server error--Number of server errors. This category is a "catchall" for error packets that do not fall into one of the previous categories.
	  • incorrect--Number of incorrect responses. A response is considered incorrect if it is of the wrong format than the one expected by the protocol. This frequently happens when an incorrect server key is configured on the router.
	  • time--Time (in milliseconds) taken to respond to an authentication packets.
	• Transaction: These fields provide information about authentication, authorization, and accounting transactions related to the server. A transaction is defined as a request for authentication, authorization, or accounting information that is sent by the AAA module, or by an AAA client (such as PPP) to an AAA protocol (RADIUS or TACACS+), which may involve multiple packet transmissions and retransmissions. Transactions may require

Field	Description
	packet retransmissions to one or more servers in a single server group, to verify success or failure. Success or failure is reported to AAA by the RADIUS and TACACS+ protocols as follows • success--Incremented when a transaction is successful. • failure--Incremented when a transaction fails; for example, packet retransmissions to another server in the server group failed or did not succeed. A negative response to an Access-Request, such as Access-Reject, is considered to be a successful transaction.
Author	The fields in this category are similar to those in the Authen: fields. An important difference, however, is that because authorization information is carried in authentication packets for the RADIUS protocol, these fields are not incremented when using RADIUS.
Account	The fields in this category are similar to those in the Authen: fields, but provide accounting transaction and packet statistics.
Elapsed time since counters last cleared	Displays the time in days, hours, and minutes that have passed since the counters were last cleared.

Note In case of Intelligent Services Gateway (ISG), the estimated outstanding accounting transactions will take some time to become zero. This is because there is a constant churn in the interim accounting requests.

The fields in the output of the **show aaa servers**command are mapped to Simple Network Management Protocol (SNMP) objects in the Cisco AAA-SERVER-MIB and are used in SNMP reporting. The first line of the sample output of the **show aaa servers**command (RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646) is mapped to the Cisco AAA-SERVER-MIB as follows:

- id maps to casIndex
- priority maps to casPriority
- host maps to casAddress
- auth-port maps to casAuthenPort
- acct-port maps to casAcctPort

Mapping the following set of objects listed in the Cisco AAA-SERVER-MIB map to fields displayed by the **show aaa servers** command is more straightforward. For example, the casAuthenRequests field corresponds to the Authen: request portion of the report, casAuthenRequestTimeouts corresponds to the Authen: timeouts portion of the report, and so on.

- casAuthenRequests
- casAuthenRequestTimeouts
- casAuthenUnexpectedResponses
- casAuthenServerErrorResponses
- casAuthenIncorrectResponses
- casAuthenResponseTime
- casAuthenTransactionSuccesses
- casAuthenTransactionFailures
- casAuthorRequests
- casAuthorRequestTimeouts
- casAuthorUnexpectedResponses
- casAuthorServerErrorResponses
- casAuthorIncorrectResponses
- casAuthorResponseTime
- casAuthorTransactionSuccesses
- casAuthorTransactionFailures
- casAcctRequests
- casAcctRequestTimeouts
- casAcctUnexpectedResponses
- casAcctServerErrorResponses
- casAcctIncorrectResponses
- casAcctResponseTime
- casAcctTransactionSuccesses
- casAcctTransactionFailures
- casState
- casCurrentStateDuration
- casPreviousStateDuration
- casTotalDeadTime
- casDeadCount

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.

Related Commands

Command	Description
radius-server dead-criteria	Forces one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant.
server-private	Associates a particular private RADIUS server with a defined server group.

show access-lists

To display the contents of current access lists, use the **show access-lists** command in user EXEC or privileged EXEC mode.

show access-lists [*access-list-number*| *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
access-list-name	(Optional) Name of the IP access list to display.

Command Default

The system displays all access lists.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)S	The output was modified to identify the compiled ACLs.
12.1(1)E	This command was implemented on the Cisco 7200 series.
12.1(5)T	The command output was modified to identify compiled ACLs.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(2)T	The command output was modified to show information for IPv6 access lists.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The show access-lists command is used to display the current ACLs operating in the router. Each access list is flagged using the Compiled indication if it is operating as an accelerated ACL.

The display also shows how many packets have been matched against each entry in the ACLs, enabling the user to monitor the particular packets that have been permitted or denied. This command also indicates whether the access list is running as a compiled access list.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101
Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the show access-lists command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

Note The permit and deny information displayed by the show access-lists command may not be in the same order as that entered using the access-list command.

```
Router# show access-lists
Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists
IPv6 access list list2
     deny ipv6 FEC0:0:0:2::/64 any sequence 10
     permit ipv6 any any sequence 20
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

show authentication interface

To display information about the Auth Manager for a given interface, use the **show authentication interface**command in privileged EXEC mode.

show authentication interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **show authentication interface** command to display information about the Auth Manager for a given interface.

Examples

The following is sample output from the **show authentication interface** command:

```
Switch# show authentication interface g1/0/23
Client list:
  MAC Address     Domain   Status         Handle      Interface
  000e.84af.59bd  DATA     Authz Success  0xE0000000  GigabitEthernet1/0/23
Available methods list:
  Handle  Priority  Name
  3        0        dot1x
Runnable methods list:
  Handle  Priority  Name
  3        0        dot1x
```

The table below describes the significant fields shown in the display. Other fields are self-explanatory.

Table 2: show authentication interface Field Descriptions

Field	Description
MAC Address	The MAC address of the client.

Field	Description
Domain	The domain of the client--either DATA or voice.
Status	The status of the authentication session. The possible values are: • Authc Failed--an authentication method has run for this session and authentication failed. • Authc Success--an authentication method has run for this session and authentication was successful. • Authz Failed--a feature has failed and the session has terminated. • Authz Success--all features have been applied to the session and the session is active. • Idle--this session has been initialized but no authentication methods have run. This is an intermediate state. • No methods--no authentication method has provided a result for this session. • Running--an authentication method is running for this session.
Interface	The type and number of the authentication interface.
Available methods list	Summary information for the authentication methods available on the interface.
Runnable methods list	Summary information for the authentication methods that can run on the interface.

Related Commands

Command	Description
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about the current Auth Manager sessions.

show authentication registrations

To display information about the authentication methods that are registered with the Auth Manager, use the **show authentication registrations**command in privileged EXEC mode.

show authentication registrations

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **show authentication re gistrations** command to display information about all methods registered with the Auth Manager.

Examples

The following is sample output for the show authentication registrations command:

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
   Handle   Priority   Name
     3         0       dot1x
     2         1       mab
     1         2       webauth
```

The table below describes the significant fields shown in the display.

Table 3: show authentication registrations Field Descriptions

Field	Description
Priority	The priority of the method. If the priority for authentication methods has not been configured with the **authentication priority** command, then the default priority is displayed. The default from highest to lowest is dot1x, mab, and webauth.
Name	The name of the authentication method. The values can be dot1x, mab, or webauth.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication sessions	Displays information about current Auth Manager sessions.

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication sessions** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions** command displays information for all authentication methods and authorization features.

Cisco IOS XE Release 3SE and Later Releases

show authentication sessions [**[database]**| [**handle** *handle-number*| **interface** *type number*| **mac** *mac-address*| **method** *method-name* [**interface** *type number*]| **session-id** *session-id*]] **[details]**

All Other Releases

show authentication sessions [**handle** *handle-number*| **interface** *type number*| **mac** *mac-address*| **method** *method-name* **interface** *type number*| **session-id** *session-id*]

Syntax Description

database	(Optional) Displays session data stored in the session database. This keyword allows you to see information like the VLAN ID, which is not cached internally. A warning message displays if data stored in the session database does not match the internally cached data.
handle *handle-id*	(Optional) Specifies the particular handle for which to display Auth Manager information.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed. To display the valid keywords and arguments for interfaces, use the question mark (?) online help function.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.

method *method-name*	(Optional) Specifies the particular authentication method for which to display Auth Manager information. Valid methods are one of the following: • **dot1x**—IEEE 802.1X authentication method. • **mab**—MAC authentication bypass (MAB) method. • **webauth**—Web authentication method. If you specify a method, you can also specify an interface.
session-id *session-id*	(Optional) Specifies the particular session for which to display Auth Manager information.
details	(Optional) Displays detailed information for each session instead of displaying a single-line summary for sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SXI	This command was changed to add the **handle** *handle* keyword and argument and add information to the output.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
Cisco IOS XE Release 3.2SE	This command was modified. The **database** and **details** keywords were added.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

Examples

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/47

Interface:  GigabitEthernet2/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
           Interface:  GigabitEthernet2/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

The following example shows how to display the authentication session for a specified session ID:

```
Device# show authentication sessions session-id 0B0101C70000004F2ED55218

           Interface:  GigabitEthernet9/2
          MAC Address:  0000.0000.0011
           IP Address:  20.0.0.7
             Username:  johndoe
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Critical Auth
          Vlan policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0B0101C70000004F2ED55218
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

The following examples show how to display all clients authorized by the specified authentication method:

```
Device# show authentication sessions method mab

No Auth Manager contexts match supplied criteria
```

```
Device# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

The table below describes the significant fields shown in the displays.

Table 4: show authentication sessions Field Descriptions

Field	Description
Interface	The type and number of the authentication interface.
MAC Address	The MAC address of the client.
Domain	The name of the domain, either DATA or VOICE.
Status	The status of the authentication session. The possible values are: • Authc Failed—An authentication method has run for this session and authentication failed. • Authc Success—An authentication method has run for this session and authentication was successful. • Authz Failed—A feature has failed and the session has terminated. • Authz Success—All features have been applied to the session and the session is active. • Idle—This session has been initialized but no authentication methods have run. This is an intermediate state. • No methods—No authentication method has provided a result for this session. • Running—An authentication method is running for this session.
Handle	The context handle.

Field	Description
State	The operating states for the reported authentication sessions. The possible values are: • Not run—The method has not run for this session. • Running—The method is running for this session. • Failed over—The method has failed and the next method is expected to provide a result. • Success—The method has provided a successful authentication result for the session. • Authc Failed—The method has provided a failed authentication result for the session.

Related Commands

Command	Description
show access-sessions	Displays information about session aware networking sessions.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication statistics	Displays statistics for Auth Manager sessions.
show dot1x	Displays details for an identity profile specific to the use of the 802.1X authentication method.