



Show Commands: r to z

- [show radius acct detailed, on page 4](#)
- [show radius acct statistics, on page 5](#)
- [show radius auth detailed, on page 6](#)
- [show radius auth statistics, on page 7](#)
- [show radius avp-list, on page 8](#)
- [show radius summary, on page 9](#)
- [show redundancy interfaces, on page 10](#)
- [show redundancy latency, on page 11](#)
- [show redundancy mobilitymac, on page 12](#)
- [show redundancy peer-route summary, on page 13](#)
- [show redundancy peer-system statistics, on page 14](#)
- [show redundancy statistics, on page 15](#)
- [show redundancy summary, on page 16](#)
- [show redundancy timers, on page 17](#)
- [show remote-lan, on page 18](#)
- [show reset, on page 20](#)
- [show rfid client, on page 21](#)
- [show rfid config, on page 22](#)
- [show rfid detail, on page 23](#)
- [show rfid summary, on page 24](#)
- [show rf-profile summary, on page 25](#)
- [show rf-profile details, on page 26](#)
- [show rogue adhoc custom summary, on page 27](#)
- [show rogue adhoc detailed, on page 28](#)
- [show rogue adhoc friendly summary , on page 29](#)
- [show rogue adhoc malicious summary, on page 30](#)
- [show rogue adhoc unclassified summary , on page 31](#)
- [show rogue adhoc summary, on page 32](#)
- [show rogue ap clients, on page 33](#)
- [show rogue ap custom summary , on page 35](#)
- [show rogue ap detailed, on page 37](#)
- [show rogue ap friendly summary, on page 40](#)
- [show rogue ap malicious summary, on page 42](#)

- [show rogue ap summary](#), on page 44
- [show rogue ap unclassified summary](#), on page 47
- [show rogue auto-contain](#), on page 48
- [show rogue client detailed](#), on page 49
- [show rogue client summary](#), on page 50
- [show rogue ignore-list](#), on page 51
- [show rogue rule detailed](#), on page 53
- [show rogue rule summary](#), on page 55
- [show route kernel](#), on page 56
- [show route summary](#), on page 57
- [show rules](#), on page 58
- [show run-config](#), on page 59
- [show run-config startup-commands](#), on page 60
- [show serial](#), on page 61
- [show sessions](#), on page 62
- [show snmpcommunity](#), on page 63
- [show snmpengineID](#), on page 64
- [show snmptrap](#), on page 65
- [show snmpv3user](#), on page 66
- [show snmpversion](#), on page 67
- [show spanningtree port](#), on page 68
- [show spanningtree switch](#), on page 69
- [show stats port](#), on page 70
- [show stats switch](#), on page 72
- [show switchconfig](#), on page 74
- [show sysinfo](#), on page 75
- [show tacacs acct statistics](#), on page 77
- [show tacacs athr statistics](#), on page 78
- [show tacacs auth statistics](#), on page 79
- [show tacacs summary](#), on page 80
- [show tech-support](#), on page 81
- [show time](#), on page 82
- [show trapflags](#), on page 84
- [show traplog](#), on page 86
- [show tunnel profile summary](#), on page 87
- [show tunnel profile-detail](#), on page 88
- [show tunnel eogre-summary](#), on page 89
- [show tunnel eogre-statistics](#), on page 90
- [show tunnel eogre-domain-summary](#), on page 91
- [show tunnel eogre gateway](#), on page 92
- [show watchlist](#), on page 93
- [show wlan](#), on page 94
- [show wps ap-authentication summary](#), on page 99
- [show wps cids-sensor](#), on page 100
- [show wps mfp](#), on page 101
- [show wps shun-list](#), on page 102

- [show wps signature detail, on page 103](#)
- [show wps signature events, on page 104](#)
- [show wps signature summary, on page 106](#)
- [show wps summary, on page 108](#)
- [show wps wips statistics, on page 110](#)
- [show wps wips summary, on page 111](#)
- [show wps ap-authentication summary, on page 112](#)

show radius acct detailed

To display RADIUS accounting server information, use the **show radius acct detailed** command.

show radius acct detailed *radius_index*

| | | |
|---------------------------|---------------------|---|
| Syntax Description | <i>radius_index</i> | Radius server index. The range is from 1 to 17. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.0 | This command was introduced. |

The following example shows how to display RADIUS accounting server information:

```
(Cisco Controller) > show radius acct detailed 5

Radius Index.....5
NAI Realms.....LAB.VTV.BLR.cisco.co.in
```

show radius acct statistics

To display the RADIUS accounting server statistics for the Cisco wireless LAN controller, use the **show radius acct statistics** command.

show radius acct statistics

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display RADIUS accounting server statistics:

```
(Cisco Controller) > show radius acct statistics
Accounting Servers:
Server Index..... 1
Server Address..... 10.1.17.10
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Accounting Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

- Related Commands**
- config radius acct**
 - config radius acct ipsec authentication**
 - config radius acct ipsec disable**
 - config radius acct network**
 - show radius auth statistics**
 - show radius summary**

show radius auth detailed

To display RADIUS authentication server information, use the **show radius auth detailed** command.

show radius auth detailed *radius_index*

| | | |
|---------------------------|---------------------|---|
| Syntax Description | <i>radius_index</i> | Radius server index. The range is from 1 to 17. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.0 | This command was introduced. |

The following example shows how to display RADIUS authentication server information:

```
(Cisco Controller) > show radius auth detailed 1

Radius Index.....1
NAI Realms.....LAB.VTV.BLR.cisco.co.in
```

show radius auth statistics

To display the RADIUS authentication server statistics for the Cisco wireless LAN controller, use the **show radius auth statistics** command.

show radius auth statistics

This command has no arguments or keyword.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display RADIUS authentication server statistics:

```
(Cisco Controller) > show radius auth statistics
Authentication Servers:
  Server Index..... 1
  Server Address..... 209.165.200.10
  Msg Round Trip Time..... 0 (1/100 second)
  First Requests..... 0
  Retry Requests..... 0
  Accept Responses..... 0
  Reject Responses..... 0
  Challenge Responses..... 0
  Malformed Msgs..... 0
  Bad Authenticator Msgs..... 0
  Pending Requests..... 0
  Timeout Requests..... 0
  Unknowntype Msgs..... 0
  Other Drops..... 0
```

- Related Commands**
- config radius auth**
 - config radius auth management**
 - config radius auth network**
 - show radius summary**

show radius avp-list

To display RADIUS VSA AVPs, use the **show radius avp-list** command.

show radius avp-list *profile-name*

| | | |
|---------------------------|---------------------|---|
| Syntax Description | <i>profile-name</i> | Profile name for which downloaded AVPs to be shown. |
| Command Default | None | |
| Command History | Release | Modification |
| | 8.0 | This command was introduced. |

The following example shows how to display RADIUS VSA AVPs:

```
(Cisco Controller) > show radius avp-list
```


show radius summary

To display the RADIUS authentication and accounting server summary, use the **show radius summary** command.

show radius summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a RADIUS authentication server summary:

```
(Cisco Controller) > show radius summary
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS..... Enabled
Authentication Servers
Index Type Server Address Port State Tout RFC-3576 IPsec -
AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----
Accounting Servers
Index Type Server Address Port State Tout RFC-3576 IPsec -
AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----
```

Related Commands **show radius auth statistics**
show radius acct statistics

show redundancy interfaces

To display details of redundancy and service port IP addresses, use the **show redundancy interfaces** command.

show redundancy interfaces

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the redundancy and service port IP addresses information:

```
(Cisco Controller) >show redundancy interfaces
```

```
Redundancy Management IP Address..... 9.4.120.5
Peer Redundancy Management IP Address..... 9.4.120.3
Redundancy Port IP Address..... 169.254.120.5
Peer Redundancy Port IP Address..... 169.254.120.3
Peer Service Port IP Address..... 10.104.175.189
```

show redundancy latency

To display the average latency to reach the management gateway and the peer redundancy management IP address, use the **show redundancy latency** command .

show redundancy latency

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the average latency to reach the management gateway and the peer redundancy management IP address:

```
(Cisco Controller) >show redundancy latency
```

```
Network Latencies (RTT) for the Peer Reachability on the Redundancy Port in micro seconds for the past 10 intervals
```

```
Peer Reachability Latency[ 1 ]      : 524 usecs
Peer Reachability Latency[ 2 ]      : 524 usecs
Peer Reachability Latency[ 3 ]      : 522 usecs
Peer Reachability Latency[ 4 ]      : 526 usecs
Peer Reachability Latency[ 5 ]      : 524 usecs
Peer Reachability Latency[ 6 ]      : 524 usecs
Peer Reachability Latency[ 7 ]      : 522 usecs
Peer Reachability Latency[ 8 ]      : 522 usecs
Peer Reachability Latency[ 9 ]      : 526 usecs
Peer Reachability Latency[ 10 ]     : 523 usecs
```

```
Network Latencies (RTT) for the Management Gateway Reachability in micro seconds for the past 10 intervals
```

```
Gateway Reachability Latency[ 1 ]   : 1347 usecs
Gateway Reachability Latency[ 2 ]   : 2427 usecs
Gateway Reachability Latency[ 3 ]   : 1329 usecs
Gateway Reachability Latency[ 4 ]   : 2014 usecs
Gateway Reachability Latency[ 5 ]   : 2675 usecs
Gateway Reachability Latency[ 6 ]   : 731 usecs
Gateway Reachability Latency[ 7 ]   : 1882 usecs
Gateway Reachability Latency[ 8 ]   : 2853 usecs
Gateway Reachability Latency[ 9 ]   : 832 usecs
Gateway Reachability Latency[ 10 ]  : 3708 usecs
```

show redundancy mobilitymac

To display the High Availability (HA) mobility MAC address that is used to communicate with the peer, use the **show redundancy mobilitymac** command.

show redundancy mobilitymac

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the HA mobility MAC address used to communicate with the peer:

```
(Cisco Controller) >show redundancy mobilitymac
ff:ff:ff:ff:ff:ff
```

show redundancy peer-route summary

To display the routes assigned to the standby WLC, use the **show redundancy peer-route summary** command.

show redundancy peer-route summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display all the configured routes of the standby WLC:

```
(Cisco Controller) >show redundancy peer-route summary
Number of Routes..... 1

Destination Network      Netmask      Gateway
-----
xxx.xxx.xxx.xxx         255.255.255.0  xxx.xxx.xxx.xxx
```

show redundancy peer-system statistics

To display statistical information about the standby WLC, use the **show redundancy peer-system statistics** command.

show redundancy peer-system statistics

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|---|
| | 8.7 | The serial number and fan status of the standby WLC are added to the output of the command. |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

```
(Cisco Controller) >show redundancy peer-system statistics
```

```
Peer System CPU statistics:Current CPU(s) load: 0%
Individual CPU load: 0%/1%, 0%/0%, 0%/1%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%,
0%/1%
```

```
Peer System Memory Statistics:
```

```
Total System Memory.....: 1027727360 bytes (980.18 MB)
Used System Memory.....: 535404544 bytes (510.63 MB)
Free System Memory.....: 492322816 bytes (469.54 MB)
Bytes allocated from RTOS.....: 5550080 bytes (5.29 MB)
Chunks Free.....: 7 bytes
Number of mmaped regions.....: 86
Total space in mmaped regions.: 369500160 bytes (352.40 MB)
Total allocated space.....: 4200328 bytes (4.00 MB)
Total non-inuse space.....: 1349752 bytes (1.28 MB)
Top-most releasable space.....: 94664 bytes (92.44 KB)
Total allocated (incl mmap)....: 375050240 bytes (357.70 MB)
Total used (incl mmap).....: 373700488 bytes (356.41 MB)
Total free (incl mmap).....: 1349752 bytes (1.28 MB)
```

```
Peer system Power supply statistics:
```

```
Power Supply 1..... Present, OK
Power Supply 2..... Absent
```

```
Serial Number..... XXXXXXXXX
Fan Status..... OK
```

show redundancy statistics

To display the statistics information of the Redundancy Manager, use the **show redundancy statistics** command.

show redundancy statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

| Release | Modification |
|---------|--|
| 7.6 | This command was introduced in a release earlier than Release 7.6. |

Usage Guidelines

This command displays the statistics of different redundancy counters.

Local Physical Ports - Connectivity status of each physical port of the controller. 1 indicates that the port is up and 0 indicates that the port is down.

Peer Physical Ports - Connectivity status of each physical port of the peer controller. 1 indicates that the port is up and 0 indicates that the port is down.

The following example shows how to display the statistics information of the Redundancy Manager:

```
(Cisco Controller) >show redundancy statistics

Redundancy Manager Statistics

Keep Alive Request Send Counter      : 16
Keep Alive Response Receive Counter  : 16

Keep Alive Request Receive Counter    : 500322
Keep Alive Response Send Counter     : 500322

Ping Request to Default GW Counter   : 63360
Ping Response from Default GW Counter : 63360

Ping Request to Peer Counter         : 12
Ping Response from Peer Counter      : 3

Keep Alive Loss Counter              : 0
Default GW Loss Counter              : 0

Local Physical Ports 1...8          : 10000000
Peer Physical Ports 1...8           : 10000000
```

show redundancy summary

To display the redundancy summary information, use the **show redundancy summary** command.

show redundancy summary

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the redundancy summary information of the controller:

```
(Cisco Controller) >show redundancy summary
Redundancy Mode = SSO DISABLED
  Local State = ACTIVE
  Peer State = N/A
    Unit = Primary
      Unit ID = 88:43:E1:7E:03:80
Redundancy State = N/A
  Mobility MAC = 88:43:E1:7E:03:80
Network Monitor = ENABLED
Link Encryption = DISABLED

BulkSync Status = <Status>
Average Redundancy Peer Reachability Latency = 1390 usecs
Average Management Gateway Reachability Latency = 1165 usecs

Redundancy Management IP Address..... 9.4.92.12
Peer Redundancy Management IP Address..... 9.4.92.14
Redundancy Port IP Address..... 169.254.92.12
Peer Redundancy Port IP Address..... 169.254.92.14
```


show redundancy timers

To display details of the Redundancy Manager timers, use the **show redundancy timers** command.

show redundancy timers

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the details of the Redundancy Manager timers:

```
(Cisco Controller) >show redundancy timers
      Keep Alive Timer      : 100 msec
      Peer Search Timer     : 120 sec
```

show remote-lan

To display information about remote LAN configuration, use the **show remote-lan** command.

show remote-lan { **summary** | *remote-lan-id* }

| Syntax Description | summary | Displays a summary of all remote LANs. |
|--------------------|----------------------|--|
| | <i>remote-lan-id</i> | Remote LAN identifier. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of all remote LANs:

```
(Cisco Controller) >show remote-lan summary
Number of Remote LANS..... 2
RLAN ID  RLAN Profile Name                Status  Interface Name
-----  -
2         remote                                Disabled management
8         test                                  Disabled management
```

The following example shows configuration information about the remote LAN with the *remote-lan-id* 2:

```
(Cisco Controller) >show remote-lan 2
Remote LAN Identifier..... 2
Profile Name..... remote
Status..... Disabled
MAC Filtering..... Disabled
AAA Policy Override..... Disabled
Network Admission Control
  Radius-NAC State..... Disabled
  SNMP-NAC State..... Disabled
  Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Number of Active Clients..... 0
Exclusionlist..... Disabled
Session Timeout..... Infinity
CHD per Remote LAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Remote LAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Disabled
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Dynamic Interface..... Disabled
Security
  Web Based Authentication..... Enabled
```

```
ACL..... Unconfigured
Web Authentication server precedence:
1..... local
2..... radius
3..... ldap
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
```

show reset

To display the scheduled system reset parameters, use the **show reset** command.

show reset

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display the scheduled system reset parameters:

```
> show reset
System reset is scheduled for Mar 27 01 :01 :01 2010
Current local time and date is Mar 24 02:57:44 2010
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

Related Commands

- reset system at**
- reset system in**
- reset system cancel**
- reset system notify-time**

show rfid client

To display the radio frequency identification (RFID) tags that are associated to the controller as clients, use the **show rfid client** command.

show rfid client

Syntax Description This command has no arguments or keywords.

Command Default None.

Usage Guidelines When the RFID tag is not in client mode, the above fields are blank.

This example shows how to display the RFID tag that is associated to the controller as clients:

```
> show rfid client
-----
RFID Mac          VENDOR      Heard      Associated AP      Chnl      Client State
-----
00:14:7e:00:0b:b1 Pango        35         AP0019.e75c.fef4   1         Probing
```

Related Commands

- config rfid status**
- config rfid timeout**
- show rfid config**
- show rfid detail**
- show rfid summary**

show rfid config

To display the current radio frequency identification (RFID) configuration settings, use the **show rfid config** command.

show rfid config

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display the current RFID configuration settings:

```
> show rfid config
RFID Tag Data Collection ..... Enabled
RFID Tag Auto-Timeout ..... Enabled
RFID Client Data Collection ..... Disabled
RFID Data Timeout ..... 200 seconds
```

Related Commands

- config rfid status**
- config rfid timeout**
- show rfid client**
- show rfid detail**
- show rfid summary**

show rfid detail

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show rfid detail** command.

show rfid detail *mac_address*

| | | |
|---------------------------|--------------------|-----------------------------|
| Syntax Description | <i>mac_address</i> | MAC address of an RFID tag. |
|---------------------------|--------------------|-----------------------------|

Command Default None.

This example shows how to display detailed RFID information:

```
> show rfid detail 00:12:b8:00:20:52
RFID address..... 00:12:b8:00:20:52
Vendor..... G2
Last Heard..... 51 seconds ago
Packets Received..... 2
Bytes Received..... 324
Cisco Type.....
Content Header
=====
Version..... 0
Tx Power..... 12 dBm
Channel..... 1
Reg Class..... 12
Burst Length..... 1
CCX Payload
=====
Last Sequence Control..... 0
Payload length..... 127
Last Sequence Control..... 0
Payload length..... 127
Payload Data Hex Dump
01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03
Nearby AP Statistics:
lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

- Related Commands**
- config rfid status**
 - config rfid timeout**
 - show rfid config**
 - show rfid client**
 - show rfid summary**

show rfid summary

To display a summary of the radio frequency identification (RFID) information for a specified tag, use the **show rfid summary** command.

show rfid summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary of RFID information:

```
> show rfid summary
Total Number of RFID : 5
-----
RFID ID      VENDOR      Closest AP      RSSI  Time Since Last Heard
-----
00:04:f1:00:00:04 Wherenet  ap:1120          -51   858 seconds ago
00:0c:cc:5c:06:d3 Aerosct   ap:1120          -51    68 seconds ago
00:0c:cc:5c:08:45 Aerosct   AP_1130         -54   477 seconds ago
00:0c:cc:5c:08:4b Aerosct   wolverine       -54   332 seconds ago
00:0c:cc:5c:08:52 Aerosct   ap:1120          -51   699 seconds ago
```

Related Commands

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid config

show rf-profile summary

To display a summary of RF profiles in the controller, use the **show rf-profile summary** command.

show rf-profile summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following is the output of the **show rf-profile summary** command:

```
(Cisco Controller) >show rf-profile summary
Number of RF Profiles..... 2
Out Of Box State..... Disabled
RF Profile Name           Band      Description           Applied
-----
T1a                       5 GHz    <none>                No
T1b                       2.4 GHz  <none>                No
```

show rf-profile details

To display the RF profile details in the Cisco wireless LAN controller, use the **show rf-profile details** command.

show rf-profile details *rf-profile-name*

| | | |
|---------------------------|------------------------|--|
| Syntax Description | <i>rf-profile-name</i> | Name of the RF profile. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |
| | 8.0 | The output was updated to include the Rx SOP threshold. |

The following is the output of the **show rf-profile details** command::

```
(Cisco Controller) >show rf-profile details T1a
Description..... <none>
Radio policy..... 5 GHz
Transmit Power Threshold v1..... -70 dBm
Transmit Power Threshold v2..... -67 dBm
Min Transmit Power..... -10 dBm
Max Transmit Power..... 30 dBm
Rx Sop Threshold..... Medium
802.11a Operational Rates
  802.11a 6M Rate..... Mandatory
  802.11a 9M Rate..... Supported
  802.11a 12M Rate..... Mandatory
  802.11a 18M Rate..... Supported
  802.11a 24M Rate..... Mandatory
  802.11a 36M Rate..... Supported
  802.11a 48M Rate..... Supported
  802.11a 54M Rate..... Supported
Max Clients..... 200
Client Trap Threshold..... 50
Multicast Data Rate..... 0
Rx Sop Threshold..... 0 dBm
Cca Threshold..... 0 dBm
Slot Admin State:..... Enabled
Band Select Probe Response..... Disabled
Band Select Cycle Count..... 2 cycles
Band Select Cycle Threshold..... 200 milliseconds
Band Select Expire Suppression..... 20 seconds
Band Select Expire Dual Band..... 60 seconds
Band Select Client Rssi..... -80 dBm
Load Balancing Denial..... 3 count
Load Balancing Window..... 5 clients
Coverage Data..... -80 dBm
Coverage Voice..... -80 dBm
Coverage Exception..... 3 clients
Coverage Level..... 25 %
```

show rogue adhoc custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue adhoc custom summary** command.

show rogue adhoc custom summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc custom summary
Number of Adhocs.....0

MAC Address          State                # APs # Clients Last Heard
-----
-----
```

- Related Commands**
- show rogue adhoc detailed
 - show rogue adhoc summary
 - show rogue adhoc friendly summary
 - show rogue adhoc malicious summary
 - show rogue adhoc unclassified summary
 - config rogue adhoc

show rogue adhoc detailed

To display details of an ad-hoc rogue access point detected by the Cisco wireless LAN controller, use the **show rogue adhoc client detailed** command.

show rogue adhoc detailed *MAC_address*

| | | |
|---------------------------|--------------------|--|
| Syntax Description | <i>MAC_address</i> | Adhoc rogue MAC address. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display detailed ad-hoc rogue MAC address information:

```
(Cisco Controller) > show rogue adhoc client detailed 02:61:ce:8e:a8:8c
Adhoc Rogue MAC address..... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID..... 02:61:ce:8e:a8:8c
State..... Alert
First Time Adhoc Rogue was Reported..... Tue Dec 11 20:45:45
2007
Last Time Adhoc Rogue was Reported..... Tue Dec 11 20:45:45
2007
Reported By
AP 1
MAC Address..... 00:14:1b:58:4a:e0
Name..... AP0014.1ced.2a60
Radio Type..... 802.11b
SSID..... rf4k3ap
Channel..... 3
RSSI..... -56 dBm
SNR..... 15 dB
Encryption..... Disabled
ShortPreamble..... Disabled
WPA Support..... Disabled
Last reported by this AP..... Tue Dec 11 20:45:45 2007
```

| | |
|-------------------------|---------------------------------|
| Related Commands | config rogue adhoc |
| | show rogue ignore-list |
| | show rogue rule summary |
| | show rogue rule detailed |
| | config rogue rule |
| | show rogue adhoc summary |

show rogue adhoc friendly summary

To display information about friendly rogue ad-hoc rogue access points, use the **show rogue adhoc friendly summary** command.

show rogue adhoc friendly summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display information about friendly rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc friendly summary
Number of Adhocs.....0

MAC Address          State                # APs # Clients Last Heard
-----
-----
```

- Related Commands**
- show rogue adhoc custom summary
 - show rogue adhoc detailed
 - show rogue adhoc summary
 - show rogue adhoc malicious summary
 - show rogue adhoc unclassified summary
 - config rogue adhoc

show rogue adhoc malicious summary

To display information about malicious rogue ad-hoc rogue access points, use the **show rogue adhoc malicious summary** command.

show rogue adhoc malicious summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display details of malicious rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc malicious summary
Number of Adhocs.....0
```

```
MAC Address          State                # APs # Clients Last Heard
-----
-----
```

Related Commands

- show rogue adhoc custom summary**
- show rogue adhoc detailed**
- show rogue adhoc summary**
- show rogue adhoc friendly summary**
- show rogue adhoc unclassified summary**
- config rogue adhoc**

show rogue adhoc unclassified summary

To display information about unclassified rogue ad-hoc rogue access points, use the **show rogue adhoc unclassified summary** command.

show rogue adhoc unclassified summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display information about unclassified rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc unclassified summary
Number of Adhocs.....0

MAC Address          State                # APs # Clients Last Heard
-----
-----
```

- Related Commands**
- show rogue adhoc custom summary
 - show rogue adhoc detailed
 - show rogue adhoc summary
 - show rogue adhoc friendly summary
 - show rogue adhoc malicious summary
 - config rogue adhoc

show rogue adhoc summary

To display a summary of the ad-hoc rogue access points detected by the Cisco wireless LAN controller, use the **show rogue adhoc summary** command.

show rogue adhoc summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of all ad-hoc rogues:

```
(Cisco Controller) > show rogue adhoc summary
Detect and report Ad-Hoc Networks..... Enabled
Client MAC Address   Adhoc BSSID   State # APs   Last Heard
-----
xx:xx:xx:xx:xx:xx   super        Alert   1         Sat Aug 9 21:12:50
 2004
xx:xx:xx:xx:xx:xx           Alert   1         Aug 9 21:12:50
 2003
xx:xx:xx:xx:xx:xx           Alert   1         Sat Aug 9 21:10:50
 2003
```

Related Commands

- config rogue adhoc**
- show rogue ignore-list**
- show rogue rule summary**
- show rogue rule detailed**
- config rogue rule**
- show rogue adhoc detailed**

show rogue ap clients

To display details of rogue access point clients detected by the Cisco wireless LAN controller, use the **show rogue ap clients** command.

show rogue ap clients *ap_mac_address*

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | <i>ap_mac_address</i> | Rogue access point MAC address. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display details of rogue access point clients:

```
(Cisco Controller) > show rogue ap clients xx:xx:xx:xx:xx:xx
MAC Address State # APs Last Heard
-----
00:bb:cd:12:ab:ff Alert 1 Fri Nov 30 11:26:23 2007
```

- Related Commands**
- config rogue adhoc
 - config rogue ap classify
 - config rogue ap friendly
 - config rogue ap rldp
 - config rogue ap timeout
 - config rogue ap valid-client
 - config rogue client
 - config trapflags rogueap
 - show rogue ap detailed
 - show rogue ap summary
 - show rogue ap friendly summary
 - show rogue ap malicious summary
 - show rogue ap unclassified summary
 - show rogue client detailed
 - show rogue client summary
 - show rogue ignore-list
 - show rogue rule detailed

show rogue ap clients

show rogue rule summary

show rogue ap custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue ap custom summary** command.

show rogue ap custom summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue ap custom summary
Number of APs.....0

MAC Address          State                # APs # Clients Last Heard
-----
-----
```

- Related Commands**
- config rogue adhoc
 - config rogue ap classify
 - config rogue ap friendly
 - config rogue ap rldp
 - config rogue ap timeout
 - config rogue ap valid-client
 - config rogue client
 - config trapflags rogueap
 - show rogue ap clients
 - show rogue ap detailed
 - show rogue ap summary
 - show rogue ap malicious summary
 - show rogue ap unclassified summary
 - show rogue client detailed
 - show rogue client summary
 - show rogue ignore-list

show rogue ap custom summary

show rogue rule detailed

show rogue rule summary

show rogue ap detailed

To display details of a rogue access point detected by the Cisco wireless LAN controller, use the **show rogue-ap detailed** command.

show rogue ap detailed *ap_mac_address*

| | | |
|---------------------------|-----------------------|--|
| Syntax Description | <i>ap_mac_address</i> | Rogue access point MAC address. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display detailed information of a rogue access point:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..... 00:0b:85:63:d1:94
Is Rogue on Wired Network..... No
Classification..... Unclassified
State..... Alert
First Time Rogue was Reported..... Fri Nov 30 11:24:56
2007
Last Time Rogue was Reported..... Fri Nov 30 11:24:56
2007
Reported By
AP 1
MAC Address..... 00:12:44:bb:25:d0
Name..... flexconnect
Radio Type..... 802.11g
SSID..... edu-eap
Channel..... 6
RSSI..... -61 dBm
SNR..... -1 dB
Encryption..... Enabled
ShortPreamble..... Enabled
WPA Support..... Disabled
Last reported by this AP..... Fri Nov 30 11:24:56 2007
```

This example shows how to display detailed information of a rogue access point with a customized classification:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..... 00:17:0f:34:48:a0
Is Rogue on Wired Network..... No
Classification..... custom
```

```

Severity Score ..... 1
Class Name.....VeryMalicious
Class Change by..... Rogue Rule
Classified at ..... -60 dBm
Classified by..... c4:0a:cb:a1:18:80

State..... Contained
State change by..... Rogue Rule
First Time Rogue was Reported..... Mon Jun  4 10:31:18
2012
Last Time Rogue was Reported..... Mon Jun  4 10:31:18
2012
Reported By
  AP 1
    MAC Address..... c4:0a:cb:a1:18:80
    Name..... SHIELD-3600-2027
    Radio Type..... 802.11g
    SSID..... sri
    Channel..... 11
    RSSI..... -87 dBm
    SNR..... 4 dB
    Encryption..... Enabled
    ShortPreamble..... Enabled
    WPA Support..... Enabled
    Last reported by this AP..... Mon Jun  4 10:31:18
2012

```

Related Commands

```

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap valid-client
config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary

```

show rogue ignore-list
show rogue rule detailed
show rogue rule summary

show rogue ap friendly summary

To display a list of the friendly rogue access points detected by the controller, use the **show rogue ap friendly summary** command.

show rogue ap friendly summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of all friendly rogue access points:

```
(Cisco Controller) > show rogue ap friendly summary
Number of APs..... 1
MAC Address      State      # APs  # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Internal    1     0  Tue Nov 27 13:52:04 2007
```

Related Commands

- config rogue adhoc
- config rogue ap classify
- config rogue ap friendly
- config rogue ap rldp
- config rogue ap timeout
- config rogue ap valid-client
- config rogue client
- config trapflags rogueap
- show rogue ap clients
- show rogue ap detailed
- show rogue ap summary
- show rogue ap malicious summary
- show rogue ap unclassified summary
- show rogue client detailed
- show rogue client summary
- show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap malicious summary

To display a list of the malicious rogue access points detected by the controller, use the **show rogue ap malicious summary** command.

show rogue ap malicious summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of all malicious rogue access points:

```
(Cisco Controller) > show rogue ap malicious summary
Number of APs..... 2
MAC Address      State      # APs  # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert          1    0 Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert          1    0 Tue Nov 27 13:52:04 2007
```

Related Commands

- config rogue adhoc**
- config rogue ap classify**
- config rogue ap friendly**
- config rogue ap rldp**
- config rogue ap timeout**
- config rogue ap valid-client**
- config rogue client**
- config trapflags rogueap**
- show rogue ap clients**
- show rogue ap detailed**
- show rogue ap summary**
- show rogue ap friendly summary**
- show rogue ap unclassified summary**
- show rogue client detailed**
- show rogue client summary**

show rogue ignore-list
show rogue rule detailed
show rogue rule summary

show rogue ap summary

To display a summary of the rogue access points detected by the Cisco wireless LAN controller, use the **show rogue-ap summary** command.

show rogue ap summary {ssid | channel}

| Syntax Description | | |
|--------------------|----------------|---|
| | <i>ssid</i> | Displays specific user-configured SSID of the rogue access point. |
| | <i>channel</i> | Displays specific user-configured radio type and channel of the rogue access point. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |
| | 8.0 | The new keywords SSID and channel are added. |

The following example shows how to display a summary of all rogue access points:

```
(Cisco Controller) > show rogue ap summary

Rogue Location Discovery Protocol..... Disabled
Rogue ap timeout..... 1200
Rogue on wire Auto-Contain..... Disabled
Rogue using our SSID Auto-Contain..... Disabled
Valid client on rogue AP Auto-Contain..... Disabled
Rogue AP timeout..... 1200
Rogue Detection Report Interval..... 10
Rogue Detection Min Rssi..... -128
Rogue Detection Transient Interval..... 0
Rogue Detection Client Num Thershold..... 0
Total Rogues (AP+Ad-hoc) supported..... 2000
Total Rogues classified..... 729

MAC Address          Classification      # APs # Clients Last Heard
-----
xx:xx:xx:xx:xx:xx  friendly          1     0     Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious         1     0     Thu Aug  4 19:00:11 2005
xx:xx:xx:xx:xx:xx  malicious         1     0     Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious         1     0     Thu Aug  4 18:57:11 2005
```

The following example shows how to display a summary of all rogue access points with SSID as extended parameter.

```
(Cisco Controller) > show rogue ap summary ssid

MAC Address          Class              State      SSID  Security
-----
xx:xx:xx:xx:xx:xx  Unclassified      Alert      xxx   Open
```

```
xx:xx:xx:xx:xx:xx  Unclassified    Alert    xxx    Open
xx:xx:xx:xx:xx:xx  Pending        Pending  xxx    Open
xx:xx:xx:xx:xx:xx  Unclassified    Alert    xxx    WEP/WPA
```

The following example shows how to display a summary of all rogue access points with channel as extended parameter.

```
(Cisco Controller) > show rogue ap summary channel
```

| MAC Address | Class | State | Det | RadioType | Channel | RSSIlast/Max) |
|-------------------|--------------|-------|---------|-----------|---------|---------------|
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | 802.11g | | 11 | -53 / -48 |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | 802.11g | | 11 | -53 / -48 |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | 802.11a | | 149 | -74 / -69 |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | 802.11a | | 149 | -74 / -69 |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | 802.11a | | 149 | -74 / -69 |

The following example shows how to display a summary of all rogue access points with both SSID and channel as extended parameters.

```
(Cisco Controller) > show rogue ap summary ssid channel
```

| MAC Address | Class | State | SSID | Security | Det | RadioType |
|-------------------|-----------------|-------|----------------|----------|-----------|-----------|
| Channel | RSSI (last/Max) | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | dd | WEP/WPA | 802.11n5G | |
| 56 | -73 / -62 | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | SSID IS HIDDEN | Open | 802.11a | |
| 149 | -68 / -66 | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | wlan16 | WEP/WPA | 802.11n5G | |
| 149 | -71 / -71 | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | wlan15 | WEP/WPA | 802.11n5G | |
| 149 | -71 / -71 | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | wlan14 | WEP/WPA | 802.11n5G | |
| 149 | -71 / -71 | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | wlan13 | WEP/WPA | 802.11n5G | |
| 149 | -71 / -70 | | | | | |
| xx:xx:xx:xx:xx:xx | Unclassified | Alert | wlan12 | WEP/WPA | 802.11n5G | |
| 149 | -71 / -71 | | | | | |

Related Commands

- config rogue adhoc
- config rogue ap classify
- config rogue ap friendly
- config rogue ap rldp
- config rogue ap timeout
- config rogue ap valid-client
- config rogue client
- config trapflags rogueap
- show rogue ap clients
- show rogue ap detailed
- show rogue ap friendly summary
- show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap unclassified summary

To display a list of the unclassified rogue access points detected by the controller, use the **show rogue ap unclassified summary** command.

show rogue ap unclassified summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a list of all unclassified rogue access points:

```
(Cisco Controller) > show rogue ap unclassified summary
Number of APs..... 164
MAC Address      State # APs # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert  1     0   Fri Nov 30 11:12:52 2007
XX:XX:XX:XX:XX:XX Alert  1     0   Fri Nov 30 11:29:01 2007
XX:XX:XX:XX:XX:XX Alert  1     0   Fri Nov 30 11:26:23 2007
XX:XX:XX:XX:XX:XX Alert  1     0   Fri Nov 30 11:26:23 2007
```

show rogue auto-contain

To display information about rogue auto-containment, use the **show rogue auto-contain** command.

show rogue auto-contain

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display information about rogue auto-containment:

```
(Cisco Controller) > show rogue auto-contain
Containment Level..... 3
monitor_ap_only..... false
```

Related Commands

- config rogue adhoc**
- config rogue auto-contain level**

show rogue client detailed

To display details of a rogue client detected by a Cisco wireless LAN controller, use the **show rogue client detailed** command.

show rogue client detailed *Rogue_AP MAC_address*

| | | |
|---------------------------|--------------------|--|
| Syntax Description | <i>Rogue_AP</i> | Rogue AP address. |
| | <i>MAC_address</i> | Rogue client MAC address. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |
| | 8.1 | The <i>Rogue_AP</i> parameter to the show rogue client detailed command is added. |

The following example shows how to display detailed information for a rogue client:

```
(Cisco Controller) > show rogue client detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..... 00:0b:85:23:ea:d1
State..... Alert
First Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Rogue Client IP address..... Not known
Reported By
AP 1
MAC Address..... 00:15:c7:82:b6:b0
Name..... AP0016.47b2.31ea
Radio Type..... 802.11a
RSSI..... -71 dBm
SNR..... 23 dB
Channel..... 149
Last reported by this AP..... Mon Dec 3 21:50:36 2007
```

- Related Commands**
- show rogue client summary**
 - show rogue ignore-list**
 - config rogue rule client**
 - config rogue rule**

show rogue client summary

To display a summary of the rogue clients detected by the Cisco wireless LAN controller, use the **show rogue client summary** command.

show rogue client summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a list of all rogue clients:

```
(Cisco Controller) > show rogue client summary
Validate rogue clients against AAA..... Disabled
Total Rogue Clients supported..... 2500
Total Rogue Clients present..... 3
MAC Address          State          # APs Last Heard
-----
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 18:57:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:12:08 2005
```

Related Commands **show rogue client detailed**

show rogue ignore-list

config rogue client

config rogue rule

show rogue ignore-list

To display a list of rogue access points that are configured to be ignored, use the **show rogue ignore-list** command.

show rogue ignore-list

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

| Release | Modification |
|---------|--|
| 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a list of all rogue access points that are configured to be ignored.

```
(Cisco Controller) > show rogue ignore-list
```

```
MAC Address
-----
xx:xx:xx:xx:xx:xx
```

Related Commands

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
config rogue rule
config trapflags rogueap
show rogue client detailed
show rogue ignore-list
show rogue rule summary
show rogue client summary
show rogue ap unclassified summary
show rogue ap malicious summary
show rogue ap friendly summary

config rogue client

show rogue ap summary

show rogue ap clients

show rogue ap detailed

config rogue rule

show rogue rule detailed

To display detailed information for a specific rogue classification rule, use the **show rogue rule detailed** command.

show rogue rule detailed *rule_name*

| | | |
|---------------------------|------------------|--|
| Syntax Description | <i>rule_name</i> | Rogue rule name. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display detailed information on a specific rogue classification rule:

```
(Cisco Controller) > show rogue rule detailed Rule2
Priority..... 2
Rule Name..... Rule2
State..... Enabled
Type..... Malicious
Severity Score..... 1
Class Name..... Very_Malicious
Notify..... All
State ..... Contain
Match Operation..... Any
Hit Count..... 352
Total Conditions..... 2
Condition 1
  type..... Client-count
  value..... 10
Condition 2
  type..... Duration
  value (seconds)..... 2000
Condition 3
  type..... Managed-ssid
  value..... Enabled
Condition 4
  type..... No-encryption
  value..... Enabled
Condition 5
  type..... Rssi
  value (dBm)..... -50
Condition 6
  type..... Ssid
  SSID Count..... 1
  SSID 1..... test
```

Related Commands **config rogue rule**
show rogue ignore-list

show rogue rule summary

show rogue rule summary

To display the rogue classification rules that are configured on the controller, use the **show rogue rule summary** command.

show rogue rule summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name           State   Type           Match Hit Count
-----
1         mtest                   Enabled Malicious      All    0
2         asdfasdf                 Enabled Malicious      All    0
```

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name           Rule state Class Type   Notify
State   Match Hit Count
-----
1         rule2                   Enabled  Friendly Global
Alert   All    234
2         rule1                   Enabled  Custom  Global
Alert   All    0
```

- Related Commands**
- config rogue rule
 - show rogue ignore-list
 - show rogue rule detailed

show route kernel

To display the kernel route cache information, use the **show route kernel** command.

show route kernel

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display the kernel route cache information:

```
> show route kernel
Iface  Destination  Gateway  Flags  RefCnt  Use  Metric  Mask  MTU  Window  IRTT
dt10   14010100    00000000 0001   0       0    0       FFFFFFF0 0    0       0
dt10   28282800    00000000 0001   0       0    0       FFFFFFF0 0    0       0
dt10   34010100    00000000 0001   0       0    0       FFFFFFF0 0    0       0
eth0   02020200    00000000 0001   0       0    0       FFFFFFF0 0    0       0
dt10   33010100    00000000 0001   0       0    0       FFFFFFF0 0    0       0
dt10   0A010100    00000000 0001   0       0    0       FFFFFFF0 0    0       0
dt10   32010100    00000000 0001   0       0    0       FFFFFFF0 0    0       0
dt10   0A000000    0202020A 0003   0       0    0       FF000000 0    0       0
lo     7F000000    00000000 0001   0       0    0       FF000000 0    0       0
dt10   00000000    0A010109 0003   0       0    0       00000000 0    0       0
```

Related Commands

- clear arp**
- debug arp**
- show arp kernel**
- config route add**
- config route delete**

show route summary

To display the routes assigned to the Cisco wireless LAN controller service port, use the **show route summary** command.

show route summary

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display all the configured routes:

```
> show route summary
Number of Routes..... 1
Destination Network      Genmask      Gateway
-----
xxx.xxx.xxx.xxx         255.255.255.0  xxx.xxx.xxx.xxx
```

Related Commands **config route**

show rules

To display the active internal firewall rules, use the **show rules** command.

show rules

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display active internal firewall rules:

```
(Cisco Controller) > show rules
-----
Rule ID.....: 3
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Source IP range:
    (Local stack)
Destination IP range:
    (Local stack)
-----
Rule ID.....: 25
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Service Info
    Service name.....: GDB
    Protocol.....: 6
    Source port low.....: 0
    Source port high.....: 0
    Dest port low.....: 1000
    Dest port high.....: 1000
Source IP range:
IP High.....: 0.0.0.0
    Interface.....: ANY
Destination IP range:
    (Local stack)
-----
```

show run-config

To display a comprehensive view of the current Cisco wireless LAN controller configuration, use the **show run-config all** command.

show run-config {all | commands} [no-ap | commands]

| Syntax Description | all | Shows all the commands under the show run-config. |
|--------------------|-----------------|---|
| | no-ap | (Optional) Excludes access point configuration settings. |
| | commands | (Optional) Displays a list of user-configured commands on |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |
| | 8.2 | This command was introduced . |

Usage Guidelines These commands have replaced the **show running-config** command.

Some WLAN controllers may have no Crypto Accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The **show run-config all** command shows only values configured by the user. It does not show system-configured default values.

The following is a sample output of the **show run-config all** command:

```
(Cisco Controller) > show run-config all
Press Enter to continue...
System Inventory
Switch Description..... Cisco Controller
Machine Model.....
Serial Number..... FLS0923003B
Burned-in MAC Address..... xx:xx:xx:xx:xx:xx
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
Press Enter to continue Or <Ctl Z> to abort...
```

show run-config startup-commands

To display a comprehensive view of the current Cisco wireless LAN controller configuration, use the **showrun-configstartup-commands** command.

show run-configstartup-commands

| Syntax Description | run-config | Displays the running configuration commands. |
|--------------------|------------------|---|
| | startup-commands | Display list of configured startup commands on Wireless LAN Controller. |

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--------------|
| | 8.0 | |

Usage Guidelines The configuration commands on the Wireless LAN controller are uploaded to the TFTP or NCS servers using the transfer upload process. The **show run-config startup-commands** command enables the Wireless LAN controller to generate running-configuration in CLI format. The configuration commands generated can be used as backup configuration to restore the network.

Example

The following is a sample output of the **show run-config startup-commands** command:

show run-config startup-commands

```
(Cisco Controller) >show run-config
  startup-commands

(Cisco Controller) >show run-config startup-commands

This may take some time.
Are you sure you want to proceed? (y/N) y
```

```
config location expiry tags 5
config mdns profile service add default-mdns-profile AirPrint
config mdns profile service add default-mdns-profile AirTunes
config mdns profile service add default-mdns-profile AppleTV
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_1
config mdns profile service add default-mdns-profile HP_Photosmart_Printer_2
config mdns profile service add default-mdns-profile Printer
config mdns profile create default-
```

show serial

To display the serial (console) port configuration, use the **show serial** command.

show serial

| | | |
|---------------------------|--|--|
| Syntax Description | This command has no arguments or keywords. | |
| Command Default | The default values for Baud rate, Character, Flow Control, Stop Bits, Parity type of the port configuration are 9600, 8, off, 1, none. | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display EIA-232 parameters and the serial port inactivity timeout:

```
(Cisco Controller) > show serial
Serial Port Login Timeout (minutes)..... 45
Baud Rate..... 9600
Character Size..... 8
Flow Control:..... Disable
Stop Bits..... 1
Parity Type:..... none
```

show sessions

To display the console port login timeout and maximum number of simultaneous command-line interface (CLI) sessions, use the **show sessions** command.

show sessions

Syntax Description This command has no arguments or keywords.

Command Default 5 minutes, 5 sessions.

This example shows how to display the CLI session configuration setting:

```
> show sessions
CLI Login Timeout (minutes)..... 0
Maximum Number of CLI Sessions..... 5
```

The response indicates that the CLI sessions never time out and that the Cisco wireless LAN controller can host up to five simultaneous CLI sessions.

Related Commands **config sessions maxsessions**
config sessions timeout

show snmpcommunity

To display Simple Network Management Protocol (SNMP) community entries, use the **show snmpcommunity** command.

show snmpcommunity

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP community entries:

```
> show snmpcommunity
SNMP Community Name Client IP Address Client IP Mask Access Mode Status
-----
public              0.0.0.0          0.0.0.0          Read Only   Enable
*****             0.0.0.0          0.0.0.0          Read/Write  Enable
```

Related Commands

config snmp community accessmode
config snmp community create
config snmp community delete
config snmp community ipaddr
config snmp community mode
config snmp syscontact

show snmpengineID

To display the SNMP engine ID, use the **show snmpengineID** command.

show snmpengineID

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display the SNMP engine ID:

```
> show snmpengineID
SNMP EngineId... ffffffff
```

Related Commands **config snmp engineID**

show snmptrap

To display Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP trap receivers and their status:

```
> show snmptrap
SNMP Trap Receiver Name      IP Address      Status
-----
xxx.xxx.xxx.xxx             xxx.xxx.xxx.xxx  Enable
```

show snmpv3user

To display Simple Network Management Protocol (SNMP) version 3 configuration, use the **show snmpv3user** command.

show snmpv3user

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP version 3 configuration information:

```
> show snmpv3user
SNMP v3 username      AccessMode  Authentication  Encryption
-----
default                Read/Write  HMAC-SHA       CFB-AES
```

Related Commands

config snmp v3user create

config snmp v3user delete

show snmpversion

To display which versions of Simple Network Management Protocol (SNMP) are enabled or disabled on your controller, use the **show snmpversion** command.

show snmpversion

Syntax Description This command has no arguments or keywords.

Command Default Enable.

This example shows how to display the SNMP v1/v2/v3 status:

```
> show snmpversion
SNMP v1 Mode..... Disable
SNMP v2c Mode..... Enable
SNMP v3 Mode..... Enable
```

Related Commands `config snmp version`

show spanningtree port

To display the Cisco wireless LAN controller spanning tree port configuration, use the **show spanningtree port** command.

show spanningtree port *port*

| | | |
|---------------------------|--|--|
| Syntax Description | <i>port</i> | Physical port number: <ul style="list-style-type: none"> • 1 through 4 on Cisco 2100 Series Wireless LAN Controller. • 1 or 2 on Cisco 4402 Series Wireless LAN Controller. • 1 through 4 on Cisco 4404 Series Wireless LAN Controller. |
| Command Default | The default SPT configuration output values are 800C, Disabled, 802.1D, 128, 100, Auto. | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |
| Usage Guidelines | When the a Cisco 4400 Series wireless LAN controller is configured for port redundancy, the Spanning Tree Protocol (STP) must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. STP can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller. | |



Note Some WLAN controllers do not support the spanning tree function.

The following example shows how to display spanning tree values on a per port basis:

```
(Cisco Controller) > show spanningtree port 3
STP Port ID..... 800C
STP Port State..... Disabled
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 100
STP Port Path Cost Mode..... Auto
```

show spanningtree switch

To display the Cisco wireless LAN controller network (DS port) spanning tree configuration, use the **show spanningtree switch** command.

show spanningtree switch

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

Usage Guidelines Some WLAN controllers do not support the spanning tree function.

The following example shows how to display spanning tree values on a per switch basis:

```
(Cisco Controller) > show spanningtree switch
STP Specification..... IEEE 802.1D
STP Base MAC Address..... 00:0B:85:02:0D:20
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15
```

show stats port

To display physical port receive and transmit statistics, use the **show stats port** command.

show stats port { **detailed** *port* | **summary** *port* }

| Syntax Description | | |
|------------------------|---|--|
| detailed | Displays detailed port statistics. | |
| summary | Displays port summary statistics. | |
| <i>port</i> | Physical port number: | |
| | <ul style="list-style-type: none"> • 1 through 4 on Cisco 2100 Series Wireless LAN Controllers. • 1 or 2 on Cisco 4402 Series Wireless LAN Controllers. • 1 through 4 on Cisco 4404 Series Wireless LAN Controllers. • 1 on Cisco WLCM Series Wireless LAN Controllers. | |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the port summary information:

```
(Cisco Controller) > show stats port summary
Packets Received Without Error..... 399958
Packets Received With Error..... 0
Broadcast Packets Received..... 8350
Packets Transmitted Without Error..... 106060
Transmit Packets Errors..... 0
Collisions Frames..... 0
Time Since Counters Last Cleared..... 2 day 11 hr 16 min 23 sec
```

The following example shows how to display the detailed port information:

```
(Cisco Controller) > show stats port detailed 1
PACKETS RECEIVED (OCTETS)
Total Bytes..... 267799881
64 byte pkts      :918281
65-127 byte pkts :354016      128-255 byte pkts :1283092
```

```

256-511 byte pkts      :8406                512-1023 byte pkts  :3006
1024-1518 byte pkts   :1184                1519-1530 byte pkts :0
> 1530 byte pkts      :2
PACKETS RECEIVED SUCCESSFULLY
Total..... 2567987
Unicast Pkts :2547844      Multicast Pkts:0      Broadcast Pkts:20143
PACKETS RECEIVED WITH MAC ERRORS
Total..... 0
Jabbers      :0              Undersize :0              Alignment :0
FCS Errors:0              Overruns  :0
RECEIVED PACKETS NOT FORWARDED
Total..... 0
Local Traffic Frames:0              RX Pause Frames      :0
Unacceptable Frames :0              VLAN Membership      :0
VLAN Viable Discards:0              MulticastTree Viable:0
ReserveAddr Discards:0
CFI Discards      :0              Upstream Threshold   :0
PACKETS TRANSMITTED (OCTETS)
Total Bytes..... 353831
64 byte pkts      :0              65-127 byte pkts    :0
128-255 byte pkts :0              256-511 byte pkts   :0
512-1023 byte pkts :0              1024-1518 byte pkts :2
1519-1530 byte pkts :0              Max Info              :1522
PACKETS TRANSMITTED SUCCESSFULLY
Total..... 5875
Unicast Pkts :5868              Multicast Pkts:0      Broadcast Pkts:7
TRANSMIT ERRORS
Total Errors..... 0
FCS Error      :0              TX Oversized :0              Underrun Error:0
TRANSMIT DISCARDS
Total Discards..... 0
Single Coll Frames :0              Multiple Coll Frames:0
Excessive Coll Frame:0              Port Membership      :0
VLAN Viable Discards:0
PROTOCOL STATISTICS
BPDUs Received      :6              BPDUs Transmitted    :0
802.3x RX PauseFrame:0
Time Since Counters Last Cleared..... 2 day 0 hr 39 min 59 sec
    
```

show stats switch

To display the network (DS port) receive and transmit statistics, use the **show stats switch** command.

show stats switch {**detailed** | **summary**}

| | | |
|---------------------------|-----------------|--|
| Syntax Description | detailed | Displays detailed switch statistics. |
| | summary | Displays switch summary statistics. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display switch summary statistics:

```
(Cisco Controller) > show stats switch summary
Packets Received Without Error..... 136410
Broadcast Packets Received..... 18805
Packets Received With Error..... 0
Packets Transmitted Without Error..... 78002
Broadcast Packets Transmitted..... 3340
Transmit Packet Errors..... 2
Address Entries Currently In Use..... 26
VLAN Entries Currently In Use..... 1
Time Since Counters Last Cleared..... 2 day 11 hr 22 min 17 sec
```

The following example shows how to display detailed switch statistics:

```
(Cisco Controller) > show stats switch detailed
RECEIVE
Octets..... 19351718
Total Pkts..... 183468
Unicast Pkts..... 180230
Multicast Pkts..... 3219
Broadcast Pkts..... 19
Pkts Discarded..... 0
TRANSMIT
Octets..... 354251
Total Pkts..... 5882
Unicast Pkts..... 5875
Multicast Pkts..... 0
Broadcast Pkts..... 7
Pkts Discarded..... 0
ADDRESS ENTRIES
```



```
Most Ever Used..... 1
Currently In Use..... 1
VLAN ENTRIES
Maximum..... 128
Most Ever Used..... 1
Static In Use..... 1
Dynamic In Use..... 0
VLANs Deleted..... 0
Time Since Ctrs Last Cleared..... 2 day 0 hr 43 min 22
sec
```

show switchconfig

To display parameters that apply to the Cisco wireless LAN controller, use the **show switchconfig** command.

show switchconfig

Syntax Description This command has no arguments or keywords.

Command Default Enabled.

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

This example shows how to display parameters that apply to the Cisco wireless LAN controller:

```
(Cisco Controller) >> show switchconfig
802.3x Flow Control Mode..... Disabled
FIPS prerequisite features..... Enabled
Boot Break..... Enabled
secret obfuscation..... Enabled
Strong Password Check Features:
  case-check .....Disabled
  consecutive-check ....Disabled
  default-check .....Disabled
  username-check .....Disabled
```

Related Commands

- config switchconfig mode**
- config switchconfig secret-obfuscation**
- config switchconfig strong-pwd**
- config switchconfig flowcontrol**
- config switchconfig fips-prerequisite**
- show stats switch**

show sysinfo

To display high-level Cisco WLC information, use the **show sysinfo** command.

show sysinfo

Syntax Description This command has no arguments or keywords.

Command Default None

This example shows a sample output of the command run on Cisco 8540 Wireless Controller using Release 8.3:

```
(Cisco Controller) >show sysinfo

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 8.3.100.0
RTOS Version..... 8.3.100.0
Bootloader Version..... 8.0.110.0
Emergency Image Version..... 8.0.110.0

OUI File Last Update Time..... Sun Sep 07 10:44:07 IST 2014

Build Type..... DATA + WPS

System Name..... TestSpartan8500Dev1
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.9.1.1615
Redundancy Mode..... Disabled
IP Address..... 8.1.4.2
IPv6 Address..... ::
System Up Time..... 0 days 17 hrs 20 mins 58 secs

--More-- or (q)uit
System Timezone Location.....
System Stats Realtime Interval..... 5
System Stats Normal Interval..... 180

Configured Country..... Multiple Countries : IN,US
Operating Environment..... Commercial (10 to 35 C)
Internal Temp Alarm Limits..... 10 to 38 C
Internal Temperature..... +21 C
Fan Status..... OK

RAID Volume Status
Drive 0..... Good
Drive 1..... Good

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 7
Number of Active Clients..... 1

OUI Classification Failure Count..... 0
```

```
Burned-in MAC Address..... F4:CF:E2:0A:27:00
Power Supply 1..... Present, OK

--More-- or (q)uit
Power Supply 2..... Present, OK
Maximum number of APs supported..... 6000
System Nas-Id.....
WLC MIC Certificate Types..... SHA1/SHA2
Licensing Type..... RTU
```

show tacacs acct statistics

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show tacacs acct statistics** command.

show tacacs acct statistics

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display detailed RFID information:

```
(Cisco Controller) > show tacacs acct statistics
Accounting Servers:
Server Index..... 1
Server Address..... 10.0.0.0
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 1
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... -1
Timeout Requests..... 1
Unknowntype Msgs..... 0
Other Drops..... 0
```

show tacacs athr statistics

To display TACACS+ server authorization statistics, use the **show tacacs athr statistics** command.

show tacacs athr statistics

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display TACACS server authorization statistics:

```
(Cisco Controller) > show tacacs athr statistics
Authorization Servers:
Server Index..... 3
Server Address..... 10.0.0.3
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Received Responses..... 0
Authorization Success..... 0
Authorization Failure..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

Related Commands

- config tacacs acct**
- config tacacs athr**
- config tacacs auth**
- show tacacs auth statistics**
- show tacacs summary**

show tacacs auth statistics

To display TACACS+ server authentication statistics, use the **show tacacs auth statistics** command.

show tacacs auth statistics

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display TACACS server authentication statistics:

```
(Cisco Controller) > show tacacs auth statistics
Authentication Servers:
Server Index..... 2
Server Address..... 10.0.0.2
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

show tacacs summary

To display TACACS+ server summary information, use the **show tacacs summary** command.

show tacacs summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display TACACS server summary information:

```
(Cisco Controller) > show tacacs summary
Authentication Servers
Idx  Server Address      Port   State   Tout
---  -
2    10.0.0.1             49     Enabled 30
Accounting Servers
Idx  Server Address      Port   State   Tout
---  -
1    10.0.0.0             49     Enabled  5
Authorization Servers
Idx  Server Address      Port   State   Tout
---  -
3    10.0.0.3             49     Enabled  5
Idx  Server Address      Port   State   Tout
---  -
4    2001:9:6:40::623    49     Enabled  5
...
```

Related Commands

- config tacacs acct**
- config tacacs athr**
- config tacacs auth**
- show tacacs summary**
- show tacacs athr statistics**
- show tacacs auth statistics**

show tech-support

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display system resource information:

```
> show tech-support
Current CPU Load..... 0%
System Buffers
  Max Free Buffers..... 4608
  Free Buffers..... 4604
  Buffers In Use..... 4
Web Server Resources
  Descriptors Allocated..... 152
  Descriptors Used..... 3
  Segments Allocated..... 152
  Segments Used..... 3
System Resources
  Uptime..... 747040 Secs
  Total Ram..... 127552 Kbytes
  Free Ram..... 19540 Kbytes
  Shared Ram..... 0 Kbytes
  Buffer Ram..... 460 Kbytes
```

show time

To display the Cisco wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display the controller time and date when authentication is not enabled:

```
> show time
Time..... Wed Apr 13 09:29:15 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
  NTP Polling Interval..... 3600
  Index      NTP Key Index      NTP Server      NTP Msg Auth Status
  -----
  1          0          9.2.60.60      AUTH DISABLED
```

This example shows successful authentication of NTP Message results in the AUTH Success:

```
> show time
Time..... Thu Apr 7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
  NTP Polling Interval..... 3600
  Index      NTP Key Index      NTP Server      NTP Msg Auth Status
  -----
  1          1          9.2.60.60      AUTH SUCCESS
```

This example shows that if the packet received has errors, then the NTP Msg Auth status will show AUTH Failure:

```
> show time
Time..... Thu Apr 7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata
NTP Servers
  NTP Polling Interval..... 3600
  Index      NTP Key Index      NTP Server      NTP Msg Auth Status
  -----
  1          10         9.2.60.60      AUTH FAILURE
```

This example shows that if there is no response from NTP server for the packets, the NTP Msg Auth status will be blank:

```
> show time
Time..... Thu Apr 7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai,
Kolkata
```

```
NTP Servers
NTP Polling Interval..... 3600
-----
Index      NTP Key Index      NTP Server      NTP Msg Auth Status
-----
1          11                 9.2.60.60
```

Related Commands

config time manual
config time ntp
config time timezone
config time timezone location

show trapflags

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap flags, use the **show trapflags** command.

show trapflags

Syntax Description This command has no arguments or keywords.

Command Default None.

This example shows how to display controller SNMP trap flags:

```
> show trapflags
Authentication Flag..... Enable
Link Up/Down Flag..... Enable
Multiple Users Flag..... Enable
Spanning Tree Flag..... Enable
Client Related Traps
  802.11 Disassociation..... Disable
  802.11 Association..... Disabled
  802.11 Deauthenticate..... Disable
  802.11 Authenticate Failure..... Disable
  802.11 Association Failure..... Disable
  Authentication..... Disabled
  Excluded..... Disable
  Max Client Warning Threshold..... 90%
Nac-Alert Traps..... Disabled
RFID Related Traps
  Max RFIDs Warning Threshold..... 90%

802.11 Security related traps
  WEP Decrypt Error..... Enable
  IDS Signature Attack..... Disable

Cisco AP
  Register..... Enable
  InterfaceUp..... Enable
Auto-RF Profiles
  Load..... Enable
  Noise..... Enable
  Interference..... Enable
  Coverage..... Enable
Auto-RF Thresholds
  tx-power..... Enable
  channel..... Enable
  antenna..... Enable
AAA
  auth..... Enable
  servers..... Enable
rogueap..... Enable
adjchannel-rogueap..... Disabled
wps..... Enable
configsave..... Enable
IP Security
  esp-auth..... Enable
  esp-replay..... Enable
  invalidSPI..... Enable
```

```

ike-neg..... Enable
suite-neg..... Enable
invalid-cookie..... Enable
Mesh
auth failure..... Enabled
child excluded parent..... Enabled
parent change..... Enabled
child moved..... Enabled
excessive parent change..... Enabled
onset SNR..... Enabled
abate SNR..... Enabled
console login..... Enabled
excessive association..... Enabled
default bridge group name..... Enabled
excessive hop count..... Disabled
excessive children..... Enabled
sec backhaul change..... Disabled

```

Related Commands**config trapflags 802.11-Security****config trapflags aaa****config trapflags ap****config trapflags authentication****config trapflags client****config trapflags configsave****config trapflags IPsec****config trapflags linkmode**

show traplog

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap log, use the **show traplog** command.

show traplog

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| | | |
|------------------------|----------------|--|
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following is a sample output of the **show traplog** command:

```
(Cisco Controller) > show traplog
Number of Traps Since Last Reset..... 2447
Number of Traps Since Log Last Displayed... 2447
Log System Time                Trap
-----
 0 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:62:fe detected on Base Rad
io MAC : 00:0b:85:18:b6:50 Interface no:1(802.11
b/g) with RSSI: -78 and SNR: 10
 1 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:52:19:d8 detected on Base Rad
io MAC : 00:0b:85:18:b6:50 Interface no:1(802.11
b/g) with RSSI: -72 and SNR: 16
 2 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:26:a1:8d detected on Base Rad
io MAC : 00:0b:85:18:b6:50 Interface no:1(802.11
b/g) with RSSI: -82 and SNR: 6
 3 Thu Aug  4 19:54:14 2005 Rogue AP : 00:0b:85:14:b3:4f detected on Base Rad
io MAC : 00:0b:85:18:b6:50 Interface no:1(802.11
b/g) with RSSI: -56 and SNR: 30
Would you like to display more entries? (y/n)
```

show tunnel profile summary

To show the summary of all the profiles, use the **show tunnel profile** command.

```
show tunnel profile { summary | detail { <profile-name> profile-name }
```

| Syntax Description | | |
|--------------------|---------------------|--------------------------------------|
| | <i>summary</i> | Summary of all profiles. |
| | <i>detail</i> | Shows details of a specific profile. |
| | <i>profile-name</i> | Name of the profile. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.1 | This command was introduced. |

The following example shows how to display the summary of all the profiles:

```
show tunnel profile summary
```

show tunnel profile-detail

To show details of a specific profile, use the **show tunnel profile** command.

show tunnel profile*detail**profile-name*

| Syntax Description | detail | Displays details of a specific profile. |
|--------------------|---------------------|---|
| | <i>profile-name</i> | Name of the profile. |

| Command Default | None |
|-----------------|------|
|-----------------|------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 8.1 | This command was introduced. |

The following example shows how to display specific profile details:

```
show tunnel profile detail test
```


show tunnel eogre-summary

To show the global configuration summary, use the **show tunnel eogre** command.

show tunnel eogre summary

| | |
|---------------------------|---|
| Syntax Description | summary Displays the global configuration summary. |
| Command Default | None |
| Command History | Release Modification |
| | 8.1 This command was introduced. |

The following example shows how to display the global configuration details:

```
(Cisco Controller) > show tunnel eogre summary
```

show tunnel eogre-statistics

To display the EoGRE Tunnel statistics, use the **show tunnel eogre** command.

show tunnel eogrestatistics

| Syntax Description | statistics Displays the EoGRE Tunnel statistics. | | | | |
|---------------------------|---|---------|--------------|-----|------------------------------|
| Command Default | None | | | | |
| Command History | <table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>8.1</td><td>This command was introduced.</td></tr></tbody></table> | Release | Modification | 8.1 | This command was introduced. |
| Release | Modification | | | | |
| 8.1 | This command was introduced. | | | | |

The following example shows how to display the EoGRE Tunnel statistics details:

```
show tunnel eogre statistics
```

show tunnel eogre-domain-summary

To display the EoGRE domain summary, use the **show tunnel eogre** command.

show tunnel eogredomainsummary

| | |
|---------------------------|---|
| Syntax Description | summary Displays the EoGRE domain summary. |
| Command Default | None |
| Command History | Release Modification |
| | 8.1 This command was introduced. |

The following example shows how to display the EoGRE domain summary:

```
show tunnel eogre domain summary
```

show tunnel eogre gateway

To view the EoGRE tunnel gateway summary and statistics, use the **show tunnel eogre** command.

show tunnel eogre gateway { **summary** | **statistics** }

Syntax Description

summary Displays the EoGRE tunnel gateway summary.

statistics Displays the EoGRE tunnel gateway statistics.

Command Default

None

Usage Guidelines

The **show tunnel eogre gateway summary** command lists details of only the FlexConnect central switching clients and Local Mode AP clients. To view the details of FlexConnect local switching clients, use the **show ap eogre gateway *ap-name*** command.

Command History

Release Modification

8.1 This command was introduced.

8.5 The **statistics** parameter was added.

show watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

| | |
|---------------------------|--|
| Syntax Description | This command has no arguments or keywords. |
|---------------------------|--|

| | |
|------------------------|------|
| Command Default | None |
|------------------------|------|

| Command History | Release | Modification |
|------------------------|----------------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the client watchlist information:

```
(Cisco Controller) >show watchlist  
client watchlist state is disabled
```

show wlan

To display configuration information for a specified wireless LAN or a foreign access point, or to display wireless LAN summary information, use the **show wlan** command.

show wlan { **apgroups** | **summary** | *wlan_id* | **foreignAp** | **lobby-admin-access** }

| Syntax Description | | |
|---------------------------|--|---|
| apgroups | | Displays access point group information. |
| summary | | Displays a summary of all wireless LANs. |
| <i>wlan_id</i> | | Displays the configuration of a WLAN. The Wireless LAN identifier ranges from 1 to 512. |
| foreignAp | | Displays the configuration for support of foreign access points. |
| lobby-admin-access | | Display all wlangs that have lobby-admin-access enabled. |

Command Default None

Usage Guidelines For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |
| | 8.4 | Shows WLANs which have lobby-admin-access enabled. |

The following example shows how to display a summary of wireless LANs for wlan_id 1:

```
(Cisco Controller) >show wlan 1
WLAN Identifier..... 1
Profile Name..... aicha
Network Name (SSID)..... aicha
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control
  RADIUS Profiling Status ..... Disabled
  DHCP ..... Disabled
  HTTP ..... Disabled
Client Profiling Status ..... Disabled
  DHCP ..... Disabled
  HTTP ..... Disabled
  Radius-NAC State..... Enabled
  SNMP-NAC State..... Enabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
```

```

Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
User Idle Timeout..... 300 seconds
User Idle Threshold..... 0 Bytes
NAS-identifier..... Talwar1
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Multicast Interface..... Not Configured
WLAN IPv4 ACL..... unconfigured
WLAN IPv6 ACL..... unconfigured
mDNS Status..... Disabled
mDNS Profile Name..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Enabled
PMIPv6 Mobility Type..... none
Quality of Service..... Silver (best effort)
Per-SSID Rate Limits..... Upstream      Downstream
Average Data Rate..... 0              0
Average Realtime Data Rate..... 0        0
Burst Data Rate..... 0                0
Burst Realtime Data Rate..... 0          0
Per-Client Rate Limits..... Upstream    Downstream
Average Data Rate..... 0              0
Average Realtime Data Rate..... 0        0
Burst Data Rate..... 0                0
Burst Realtime Data Rate..... 0          0
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
WMM UAPSD Compliant Client Support..... Disabled
Media Stream Multicast-direct..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
Passive Client Feature..... Disabled
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Enabled (Profile 'Controller_Local_EAP')
Radius NAI-Realm..... Enabled
Security
  802.11 Authentication:..... Open System
  FT Support..... Disabled
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
    WPA2 (RSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
Auth Key Management

```

```

      802.1x..... Enabled
      PSK..... Disabled
      CCKM..... Enabled
      FT(802.11r)..... Disabled
      FT-PSK(802.11r)..... Disabled
      PMF-1X(802.11w)..... Enabled
      PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-Air mode..... Enabled
FT Over-The-Ds mode..... Enabled
      GTK Randomization..... Disabled
      SKC Cache Support..... Disabled
      CCKM TSF Tolerance..... 1000
      Wi-Fi Direct policy configured..... Disabled
      EAP-Passthrough..... Disabled
CKIP ..... Disabled
      IP Security..... Disabled
      IP Security Passthru..... Disabled
      Web Based Authentication..... Disabled
      Web-Passthrough..... Disabled
      Conditional Web Redirect..... Disabled
      Splash-Page Web Redirect..... Disabled
      Auto Anchor..... Disabled
      FlexConnect Local Switching..... Enabled
      flexconnect Central Dhcp Flag..... Disabled
      flexconnect nat-pat Flag..... Disabled
      flexconnect Dns Override Flag..... Disabled
      FlexConnect Vlan based Central Switching .... Disabled
      FlexConnect Local Authentication..... Disabled
      FlexConnect Learn IP Address..... Enabled
      Client MFP..... Optional
      PMF..... Disabled
      PMF Association Comeback Time..... 1
      PMF SA Query RetryTimeout..... 200
      Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Disabled
Roamed Call Re-Anchor Policy..... Disabled
SIP CAC Fail Send-486-Busy Policy..... Enabled
SIP CAC Fail Send Dis-Association Policy..... Disabled
KTS based CAC Policy..... Disabled
Band Select..... Disabled
Load Balancing..... Disabled
Mobility Anchor List
WLAN ID      IP Address      Status
-----
802.11u..... Enabled
      Network Access type..... Chargeable Public Network
      Internet service..... Enabled
      Network Authentication type..... Not Applicable
      HESSID..... 00:00:00:00:00:00
      IP Address Type Configuration
      IPv4 Address type..... Available
      IPv6 Address type..... Not Known

Roaming Consortium List
      Index      OUI List      In Beacon
      -----
      1          313131      Yes
      2          DDBBCC      No
      3          DDDDDD      Yes

Realm configuration summary
      Realm index..... 1
      Realm name..... jobin
      EAP index..... 1

```



```

EAP method..... Unsupported
Index   Inner Authentication           Authentication Method
-----
1       Credential Type                 SIM
2       Tunneled Eap Credential Type    SIM
3       Credential Type                 SIM
4       Credential Type                 USIM
5       Credential Type                 Hardware Token
6       Credential Type                 SoftToken
Domain name configuration summary
Index   Domain name
-----
1       rom3
2       ram
3       rom1

Hotspot 2.0..... Enabled

Operator name configuration summary
Index   Language   Operator name
-----
1       ros        Robin

Port config summary
Index   IP protocol  Port number  Status
-----
1       1            1            0      Closed
2       1            1            0      Closed
3       1            1            0      Closed
4       1            1            0      Closed
5       1            1            0      Closed
6       1            1            0      Closed
7       1            1            0      Closed

WAN Metrics Info
Link status..... Up
Symmetric Link..... No
Downlink speed..... 4 kbps
Uplink speed..... 4 kbps

MSAP Services..... Disabled
Local Policy
-----
Priority  Policy Name
-----
1       Teacher_access_policy
    
```

The following example shows how to display a summary of all WLANs:

```

(Cisco Controller) >show wlan summary
Number of WLANs..... 1

WLAN ID  WLAN Profile Name / SSID           Status   Interface Name   PMIPv6
Mobility
-----
1       apsso / apsso                       Disabled management   none
    
```

The following example shows how to display the configuration for support of foreign access points:

```

(Cisco Controller) >show wlan foreignap
    
```

Foreign AP support is not enabled.

The following example shows how to display the AP groups:

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..... 1
Site Name..... APuser
Site Description..... <none>
Venue Name..... Not configured
Venue Group Code.....Unspecified
Venue Type Code.....Unspecified
Language Code..... Not configured
AP Operating Class..... 83,84,112,113,115,116,117,118,123
RF Profile
-----
2.4 GHz band..... <none>
5 GHz band..... <none>
WLAN ID          Interface          Network Admission Control          Radio Policy
-----
 14              int_4              Disabled                            All
AP Name          Slots  AP Model          Ethernet MAC          Location          Port
Country  Priority
-----
Ibiza           2      AIR-CAP2602I-A-K9  44:2b:03:9a:8a:73  default location  1
US             1
Larch           2      AIR-CAP3502E-A-K9  f8:66:f2:ab:23:95  default location  1
US             1
Zest            2      AIR-CAP3502I-A-K9  00:22:90:91:6d:b6          ren  1
US             1

Number of Clients..... 1

MAC Address      AP Name      Status      Device Type
-----
24:77:03:89:9b:f8      ap2      Associated      Android
```

show wps ap-authentication summary

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

show wps ap-authentication summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

| Release | Modification |
|----------------|--|
| 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

Related Commands

config wps ap-authentication

show wps cids-sensor

To display Intrusion Detection System (IDS) sensor summary information or detailed information on a specified Wireless Protection System (WPS) IDS sensor, use the **show wps cids-sensor** command.

show wps cids-sensor {**summary** | **detail** *index*}

| Syntax Description | summary | Displays a summary of sensor settings. |
|--------------------|---------------|--|
| | detail | Displays all settings for the selected sensor. |
| | <i>index</i> | IDS sensor identifier. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display all settings for the selected sensor:

```
(Cisco Controller) > show wps cids-sensor detail1
IP Address..... 10.0.0.51
Port..... 443
Query Interval..... 60
Username..... Sensor_user1
Cert Fingerprint..... SHA1:
00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00
Query State..... Disabled
Last Query Result..... Unknown
Number of Queries Sent..... 0
```

Related Commands **config wps ap-authentication**

show wps mfp

To display Management Frame Protection (MFP) information, use the **show wps mfp** command.

show wps mfp {summary | statistics}

| | | |
|---------------------------|-------------------|--|
| Syntax Description | summary | Displays the MFP configuration and status. |
| | statistics | Displays MFP statistics. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of the MFP configuration and status:

```
(Cisco Controller) > show wps mfp summary
Global Infrastructure MFP state..... DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..... False

WLAN ID  WLAN Name                WLAN      Infra.    Client
-----  -
1         homeap                          Disabled  *Enabled  Optional but inactive
(WPA2 not configured)
2         7921                            Enabled   *Enabled  Optional but inactive
(WPA2 not configured)
3         open1                           Enabled   *Enabled  Optional but inactive
(WPA2 not configured)
4         7920                            Enabled   *Enabled  Optional but inactive
(WPA2 not configured)

AP Name          Infra.    Operational  --Infra. Capability--
Validation      Radio    State         Protection  Validation
-----  -
AP1252AG-EW     *Enabled  b/g          Down        Full        Full
a              Down        Full        Full
```

The following example shows how to display the MFP statistics:

```
(Cisco Controller) > show wps mfp statistics
BSSID          Radio Validator AP      Last Source Addr  Found  Error Type
Count          Frame Types
-----  -
no errors
```

Related Commands **config wps mfp**

show wps shun-list

To display the Intrusion Detection System (IDS) sensor shun list, use the **show wps shun-list** command.

show wps shun-list

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the IDS system sensor shun list:

```
(Cisco Controller) > show wps shun-list
```

Related Commands **config wps shun-list re-sync**

show wps signature detail

To display installed signatures, use the **show wps signature detail** command.

show wps signature detail *sig-id*

| | | |
|---------------------------|----------------|--|
| Syntax Description | <i>sig-id</i> | Signature ID of an installed signature. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

This example shows how to display information on the attacks detected by standard signature 1:

```
(Cisco Controller) > show wps signature detail 1
Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 500 pkts/interval
Signature Mac Frequency..... 300 pkts/interval
Interval..... 10 sec
Quiet Time..... 300 sec
Description..... Broadcast Deauthentication Frame
Patterns:
    0 (Header):0x0:0x0
    4 (Header):0x0:0x0
```

- Related Commands**
- config wps signature**
 - config wps signature frequency**
 - config wps signature mac-frequency**
 - config wps signature interval**
 - config wps signature quiet-time**
 - config wps signature reset**
 - show wps signature events**
 - show wps signature summary**
 - show wps summary**

show wps signature events

To display more information about the attacks detected by a particular standard or custom signature, use the **show wps signature events** command.

show wps signature events {**summary** | {**standard** | **custom**} *precedenceID* {**summary** | **detailed**}

| Syntax Description | | |
|---------------------|---------|--|
| summary | | Displays all tracking signature summary information. |
| standard | | Displays Standard Intrusion Detection System (IDS) signature settings. |
| custom | | Displays custom IDS signature settings. |
| <i>precedenceID</i> | | Signature precedence identification value. |
| detailed | | Displays tracking source MAC address details. |
| Command Default | None | |
| Command History | Release | Modification |
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the number of attacks detected by all enabled signatures:

```
(Cisco Controller) > show wps signature events summary
Precedence  Signature Name      Type      # Events
-----
1           Bcast deauth             Standard   2
2           NULL probe resp 1        Standard   1
```

This example shows how to display a summary of information on the attacks detected by standard signature 1:

```
(Cisco Controller) > show wps signature events standard 1 summary
Precedence..... 1
Signature Name..... Bcast deauth
Type..... Standard
Number of active events..... 2
Source MAC Addr   Track Method   Frequency # APs Last Heard
-----
00:a0:f8:58:60:dd Per Signature  50           1    Wed Oct 25 15:03:05
2006
00:a0:f8:58:60:dd Per Mac       30           1    Wed Oct 25 15:02:53
2006
```

Related Commands

config wps signature frequency
config wps signature mac-frequency
config wps signature interval
config wps signature quiet-time
config wps signature reset
config wps signature
show wps signature summary
show wps summary

show wps signature summary

To see individual summaries of all of the standard and custom signatures installed on the controller, use the **show wps signature summary** command.

show wps signature summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of all of the standard and custom signatures:

```
(Cisco Controller) > show wps signature summary
Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 50 pkts/interval
Signature Mac Frequency..... 30 pkts/interval
Interval..... 1 sec
Quiet Time..... 300 sec
Description..... Broadcast
Deauthentication Frame
Patterns:
          0 (Header) :0x00c0:0x00ff
          4 (Header) :0x01:0x01
...
```

Related Commands

- config wps signature frequency**
- config wps signature interval**
- config wps signature quiet-time**
- config wps signature reset**
- show wps signature events**
- show wps summary**
- config wps signature mac-frequency**

config wps signature

show wps summary

To display Wireless Protection System (WPS) summary information, use the **show wps summary** command.

show wps summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display WPS summary information:

```
(Cisco Controller) > show wps summary
Auto-Immune
  Auto-Immune..... Disabled
Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled
Trusted AP Policy
  Management Frame Protection..... Disabled
  Mis-configured AP Action..... Alarm Only
    Enforced encryption policy..... none
    Enforced preamble policy..... none
    Enforced radio type policy..... none
  Validate SSID..... Disabled
  Alert if Trusted AP is missing..... Disabled
  Trusted AP timeout..... 120
Untrusted AP Policy
  Rogue Location Discovery Protocol..... Disabled
  RLDP Action..... Alarm Only
Rogue APs
  Rogues AP advertising my SSID..... Alarm Only
  Detect and report Ad-Hoc Networks..... Enabled
Rogue Clients
  Validate rogue clients against AAA..... Enabled
  Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1300
Signature Policy
  Signature Processing..... Enabled
...
```

Related Commands

config wps signature frequency
config wps signature interval
config wps signature quiet-time
config wps signature reset
show wps signature events
show wps signature mac-frequency
show wps summary
config wps signature
config wps signature interval

show wps wips statistics

To display the current state of the Cisco Wireless Intrusion Prevention System (wIPS) operation on the controller, use the **show wps wips statistics** command.

show wps wips statistics

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display the statistics of the wIPS operation:

```
(Cisco Controller) > show wps wips statistics
Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests..... 0
Policy Update Responses..... 0
Policy Delete Requests..... 0
Policy Delete Responses..... 0
Alarm Updates..... 13572
Device Updates..... 8376
Device Update Requests..... 0
Device Update Responses..... 0
Forensic Updates..... 1001
Invalid WIPS Payloads..... 0
Invalid Messages Received..... 0
NMSP Transmitted Packets..... 22950
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet..... 1377
```

Related Commands

- config 802.11 enable**
- config ap mode**
- config ap monitor-mode**
- show ap config**
- show ap monitor-mode summary**
- show wps wips summary**

show wps wips summary

To display the adaptive Cisco Wireless Intrusion Prevention System (wIPS) configuration that the Wireless Control System (WCS) forwards to the controller, use the **show wps wips summary** command.

show wps wips summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of the wIPS configuration:

```
(Cisco Controller) > show wps wips summary
Policy Name..... Default
Policy Version..... 3
```

- Related Commands**
- config 802.11 enable**
 - config ap mode**
 - config ap monitor-mode**
 - show ap config**
 - show ap monitor-mode summary**
 - show wps wips statistics**

show wps ap-authentication summary

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

show wps ap-authentication summary

Syntax Description This command has no arguments or keywords.

Command Default None

| Command History | Release | Modification |
|-----------------|---------|--|
| | 7.6 | This command was introduced in a release earlier than Release 7.6. |

The following example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

Related Commands [config wps ap-authentication](#)