show Commands

- show ap client-trace status, on page 2
- show arp, on page 3
- show avc cft, on page 3
- show avc nbar, on page 4
- show avc netflow flows, on page 4
- show avc status, on page 5
- show boot, on page 5
- show capwap, on page 6
- show capwap client, on page 7
- show capwap client trace, on page 7
- show capwap ids sig, on page 8
- show cdp, on page 8
- show class-map, on page 9
- show cleanair debug, on page 9
- show client statistics, on page 10
- show clock, on page 10
- show configuration, on page 11
- show controller ble, on page 11
- show controllers dot11Radio, on page 12
- show controllers nss status, on page 13
- show controllers wired, on page 14
- show crypto, on page 14
- show debug, on page 15
- show dhcp, on page 15
- show dot11 qos, on page 16
- show dot11 wlan wpa3, on page 16
- show filesystems, on page 17
- show flash, on page 17
- show flexconnect, on page 18
- show flexconnect oeap firewall, on page 18
- show flexconnect wlan, on page 19
- show interfaces dot11Radio, on page 20
- show interfaces network, on page 21

- show interfaces wired, on page 21
- show inventory, on page 22
- show ip, on page 22
- show lacp, on page 23
- show logging, on page 23
- show memory, on page 24
- show policy-map, on page 25
- show processes, on page 25
- show processes memory, on page 26
- show rrm, on page 27
- show rrm rogue containment, on page 28
- show rrm rogue detection, on page 29
- show running-config, on page 30
- show security data-corruption, on page 31
- show security system state, on page 31
- show spectrum, on page 32
- show tech-support, on page 33
- show version, on page 33
- show trace dot11_chn, on page 34
- show trace, on page 34
- show wips, on page 35

show ap client-trace status

To view the AP client trace details, use the **show ap client-trace status** command.

show ap client-trace { **events** { **all | mac** *word* | **system** } | **skb** { **drop-list | stats** } | **status** }

Syntax Description

events	View client trace event information
all	Displays all client trace events
system	Displays all system events
mac	Displays client trace events for specific MAC address
word	Specific client MAC address
skb	Displays client trace SKB information
drop-list	Displays client trace SKB drop list information
stats	Displays client trace SKB statistics
status	Displays client trace configuration

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the AP client trace status:

```
cisco-ap# show ap client-trace status
```

show arp

To view the ARP table, use the **show arp** command.

show arp

Syntax Description

arp	Shows ARP table

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows a sample output of the command:

```
cisco-ap# show arp

Address Age (min)     Hardware Addr
   9.11.8.1         0 84:80:2D:A0:D2:E6
9.11.32.111         0 3C:77:E6:02:33:3F
```

show avc cft

To view the AVC client flow table information, use the **show avc cft** command.

show avc cft *word*

Syntax Description

word	Client MAC address

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the AVC client flow table:

```
cisco-ap# show avc cft 02:35:2E:03:E0:F2
```

show avc nbar

To view the AVC NBAR information, use the **show avc nbar** command.

show avc nbar {**statistics** | **build** | **version**}

Syntax Description

statistics	Displays NBAR build details
build	Displays NBAR statistics
version	Displays NBAR and PP version

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the AVC NBAR build information:

```
cisco-ap# show avc nbar build
```

show avc netflow flows

To list all the flows currently cached and to be sent to the Cisco WLC, use the **show avc netflow flows** command.

show avc netflow flows {**download** | **upload**}

Syntax Description

download	Lists currently cached download flows
upload	Lists currently cached upload flows

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view all the currently cached flows:

```
cisco-ap# show avc netflow flows
```

show avc status

To list the AVC provisioning status per WLAN/VAP, use the **show avc status** command.

show avc status

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view AVC provisioning status per WLAN/VAP:

```
cisco-ap# show avc status

VAP FNF-STATUS AVC-QOS-STATUS
  0   Disabled       Disabled
  1   Disabled       Disabled
  2   Disabled       Disabled
  3   Disabled       Disabled
  4   Disabled       Disabled
  5   Disabled       Disabled
  6   Disabled       Disabled
  7   Disabled       Disabled
  8   Disabled       Disabled
  9   Disabled       Disabled
 10   Disabled       Disabled
 11   Disabled       Disabled
 12   Disabled       Disabled
 13   Disabled       Disabled
 14   Disabled       Disabled
 15   Disabled       Disabled
```

show boot

To show boot attributes, use the **show boot** command.

show boot

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view boot attributes:

```
cisco-ap# show boot

BOOT path-list:      part2
Console Baudrate:    9600
Enable Break:        yes
Manual Boot:         no
Memory Debug:        no
Crashkernel:
```

show capwap

To disaply CAPWAP options, use the **show capwap** command.

show capwap [**ip** | **mcast** | **traffic**]

Syntax Description

client	CAPWAP client information
ids	CAPWAP ID information
ip	CAPWAP IP configuration
location	CAPWAP location information
mcast	CAPWAP multicast information
pnp	PNP information
traffic	CAPWAP traffic information

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the CAPWAP multicast information:

```
cisco-ap# show capwap mcast
```

show capwap client

To display CAPWAP client information, use the **show capwap client** command.

show capwap client {**callinfo** *info* | **detailrcb** | **rcb** | **config** | **ha** | **msginfo** | **timers** | **traffic**}

Syntax Description

callinfo *info*	CAPWAP client call information
detailrcb	CAPWAP client detailed RCB information
rcb	CAPWAP client RCB information
config	CAPWAP client config information
ha	CAPWAP client HA parameters
msginfo	CAPWAP client messages information
timers	CAPWAP client timers
traffic	CAPWAP client 802.11 traffic information

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view CAPWAP client traffic information:

```
cisco-ap# show capwap client traffic
```

show capwap client trace

To display CAPWAP trace, use the **show capwap client trace** command.

show capwap client trace {**clear** | **delete** | **disable** | **save** | **start** | **stop**}

Syntax Description

clear	Clears trace
delete	Deletes trace
disable	Disables trace at boot
enable	Enables trace at boot

save	Saves trace
start	Starts trace
stop	Stops trace

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view CAPWAP client trace:

```
cisco-ap# show capwap client trace
```

show capwap ids sig

To disaplay CAPWAP ID signatures, use the **show capwap ids sig** command.

show capwap ids sig [**list** | **stats**]

Syntax Description

list	Signature list entries
stats	Signature attack statistics

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example show how to view CAPWAP ID signature statistics:

```
cisco-ap# show capwap ids sig stats
```

show cdp

To display CDP options, use the **show cdp** command.

show cdp {**entry device** *device-name* | **inline_power** | **interface** | **neighbors** | **traffic**}

Syntax Description

entry device *device-name*	Information for specific neighbor entry whose name you must enter
inline_power	Inline power negotiation information
interface	CDP interface status and configuration
neighbors	CDP neighbor entries
traffic	CDP statistics

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view information for a specific neighbor entry:

```
cisco-ap# show cdp entry device mydevice
```

show class-map

To display CPL class map, use the **show class-map** command.

show class-map

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view CPL class map:

```
cisco-ap# show class-map
```

show cleanair debug

To display cleanair debug settings, use the **show cleanair debug** command.

show cleanair debug

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view CleanAir debug settings:

```
cisco-ap# show cleanair debug
```

show client statistics

To disaply client statistics, use the **show client statistics** command.

show client statistics *client-mac-address*

Syntax Description

client-mac-address	MAC address of the client

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view client statistics:

```
cisco-ap# show client statistics 70:DB:98:66:34:FA
```

show clock

To display the system clock, use the **show clock** command.

show clock

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the system clock:

```
cisco-ap# show clock
```

show configuration

To display the contents of the non-volatile memory, use the **show configuration** command.

show configuration rlan

Command Modes

Privileged EXEC (#)

Syntax Description

rlan	Displays the RLAN configuration.

Command History

Release	Modification
8.1.111.0	This command was introduced.
8.9	This command was enhanced by adding **rlan** parameter.
8.10.112.0	The output of this command was enhanced to show the status of broken antenna detection.

The following example shows how to view the AP configuration details:

```
cisco-ap# show configuration

AP Name                     : AP58AC.78DC.C2F0
Admin State                 : Enabled
AP Mode                     : FlexConnect
AP Submode                  : Not Configured
Location                    : default location
Reboot Reason               : Reload command
.
.
AP Link LAG status          : Disabled
AP WSA Mode                 : Enabled
Vlan Interface              : Disabled

Broken antenna detection    : Enabled (Global)
RSSI Failure Threshold      : 40
Weak RSSI                   : 60
Detection Time              : 12
If any broken antenna?      : ALL
AP58AC.78DC.C2F0#
```

show controller ble

To view Bluetooth Low Energy radio interface parameter information, use the **show controller ble** command.

show controller ble *ble-interface-number* { {**broadcast** | **counters** | **floor-tag** *floor-beacon-mac-addr* | **interface** | **local** | **scan** {**brief** | **detail** *floor-beacon-mac-addr*} | **timers**}

Syntax Description

ble-interface-number	BLE interface number that you must enter; Valid value is 0
broadcast	Displays BLE broadcast summary information

counters	Displays BLE transport counters information
floor-tag *floor-beacon-mac-addr*	Displays sync data of the floor beacon whose MAC address you must specify
interface	Displays BLE interface summary information
local	Displays sync information of host BLE radio
scan brief	Displays brief BLE scan summary information
scan detail *floor-beacon-mac-addr*	Displays BLE scan summary information in detail; you must specify the floor beacon MAC address
timers	Displays BLE timers information

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.7	This command was introduced.

Examples

To view the BLE timers information, use this command:

```
cisco-ap# show controller ble 0 timers

Timers
------
Scan timer status       : Running
Scan timer interval     : 10 secs
Scan started at         : 0D:00H:04M:28S ago
Last scan done at       : 0D:00H:00M:06S ago
```

If scanning is working as expected, the 'Last scan done at' time should always be less than or equal to the scan interval set.

show controllers dot11Radio

To display dot11 interface information, use the **show controllers dot11Radio** command.

show controllers dot11Radio *dot11-interface-no* {**antenna** | { **atfconfiguration** | **statistics**} | **bandselect** | **client** { *client-mac-addr* | **all detail** } | **frequency** | **powercfg** | **powerreg** | **radiostats** | **rate** | **vlan** | **wlan** { *wlan-id* | **all detail** } }

Syntax Description

dot11-interface-no	Dot11Radio interface number.
atf configuration	Displays the AirTime Fairness configuration.
atf statistics	Displays the AirTime Fairness statistics.

bandselect	Displays the bandselect statistics.
antenna	Displays the antenna settings
client *client-mac-addr*	Displays the details of the client whose MAC address is specified.
detail	Displays the TID statistics for all the clients.
frequency	Displays the frequency information.
powercfg	Displays the configured power information.
powerreg	Displays the transmit power information.
radio-stats	Displays the radio statistics.
rate	Displays the rate information.
vlan	Displays the VLAN summary.
wlan *wlan-id*	Displays the VLAN/WLAN details of the WLAN ID specified.
detail	Displays the TID statistics for all the clients.

Command Modes

User EXEC (>)

Command History

Release	Modification
8.1.111.0	This command was introduced.
8.9	This command was enhanced by adding the **bandselect** ,**client all detail** , **wlan** parameters.

The following example shows how to view 802.11 interface information for interface number 1:

```
cisco-ap# show controllers dot11Radio 1
```

show controllers nss status

To display NSS information, use the **show controllers nss status** command.

show controllers nss status

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view NSS information:

```
cisco-ap# show controllers nss status
```

show controllers wired

To view the wired interface, use the **show controllers wired** command.

show controllers wired *wired-interface-number*

Syntax Description

wired-interface-number	Wired interface number from 0 to 3

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view information about the controllers' wired interface whose ID is 1:

```
cisco-ap# show controllers wired 1

wired1    Link encap:Ethernet  HWaddr C8:8B:6A:33:59 eMac Status: DOWN
          inet addr:9.11.8.104  Bcast:9.255.255.255  Mask:255.255.255.255
          DOWN BROADCAST RUNNING PROMISC MULTICAST  MTU:2400  Metric:1
          RX packets:38600 errors:0 dropped:1 overruns:0 frame:0
          TX packets:179018 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:80
          RX bytes:3812643 (3.6 MiB)  TX bytes:54721869 (52.1 MiB)

Gig Emac1 Counters
---------------------
0 Good octets rx, 0 Bad octets rx, 0 Unicast frames rx,
0 Broadcast frames rx, 0 Multicast frames rx, 0 64 byte frames rx,
0 65_TO_127 byte frames, 0 128_TO_255 byte frames, 0 256_TO_511 byte frames,
0 512_TO_1023 byte frames, 0 1024_TO_MAX byte frames, 0 Good octets tx,
0 Unicast frames tx, 0 Multicast frames tx, 0 Broadcast frames tx,
0 Crc errors sent, 0 Flow control rx, 0 Flow control tx,
0 Rx fifo overrun, 0 Undersized rx, 0 Fragments rx,
0 Oversize rx, 0 Jabber rx, 0 Mac rx error,
0 Bad crc event, 0 Collision, 0 Late collision,
```

show crypto

To view the crypto attributes, use the **show crypto** command.

show crypto

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the crypto attributes:

```
cisco-ap# show crypto
```

show debug

To view the debugs enabled, use the **show debug** command.

show debug

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the debugs that are in enabled state:

```
cisco-ap# show debug
```

show dhcp

To view the status of Dynamic Host Configuration Protocol (DHCP), use the **show dhcp** command.

show dhcp {**lease** | **servers**}

Syntax Description

lease	Displays the DHCP addresses leased from a server
servers	Displays the known DHCP servers

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the status of DHCP addresses leased from a server:

```
cisco-ap# show dhcp lease
```

show dot11 qos

To view the Quality of Service (QoS) parameters for 802.11 network, use the **show dot11 qos** command.

show dot11 qos

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the Quality of Service (QoS) parameters for 802.11 network:

```
cisco-ap# show dot11 qos
```

show dot11 wlan wpa3

To view the WPA3 configuration on an 802.11 network, use the **show dot11 wlan wpa3** command.

show dot11 wlan wpa3 [**transition**]

Syntax Description

transition	Shows details of WPA3 transition mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.10	This command was introduced.

The following example shows how to view the WPA3 configuration on an 802.11 network:

```
cisco-ap# show dot11 wlan wpa3
```

show filesystems

To view the filesystem information, use the **show filesystems** command.

show filesystems

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the filesystem information:

```
cisco-ap# show filesystems

Filesystem                Size      Used Available Use% Mounted on
/dev/ubivol/storage      57.5M      1.9M     52.6M   4% /storage
```

show flash

To view the flash contents, use the **show flash** command.

show flash [**cores** [**detail** *core-file-name*] | **crash** | **syslogs**]

Syntax Description

cores	Displays the core files in flash
detail	Displays the core file contents
core-file-name	The core file name
crash	Displays the crash files in flash
syslogs	Displays the syslogs files in flash

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the details of a core file in flash:

```
cisco-ap# show flash cores detail filename1
```

show flexconnect

To view the flexconnect information for an access point, use the **show flexconnect** command.

show flexconnect {**calea** | **cckm** | **client** [**aaa-override** | **counter** | **priority**] | **dot11r** | **mcast** | **oeap** | **pmk** | **status** | **vlan-acl** | **wlan**}

Syntax Description

calea	Displays the calea information
cckm	Displays the CCKM cache entry information
client	Displays the client information
aaa-override	Specifies the AAA override parameters
counter	Specifies the counter for all clients
priority	Specifies the client priority
dot11r	Displays the 802.11r cache entry information
mcast	Displays the multicast information
oeap	Displays the FlexConnect OEAP information
pmk	Displays the OKC or PMK cache entry information
status	Displays the standalone status
vlan-acl	Displays the VLAN ACL mapping
wlan	Displays the WLAN configuration

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the information about a client of a FlexConnect AP:

```
cisco-ap# show flexconnect client
```

show flexconnect oeap firewall

To view the OEAP firewall information, use the **show flexconnect oeap firewall** command.

show flexconnect oeap firewall [**dmz** | **filtering** | **forwarding**]

Syntax Description

dmz	Displays the OEAP firewall DMZ information
filtering	Displays the OEAP firewall filtering information
forwarding	Displays the OEAP firewall port forwarding information

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the OEAP firewall DMZ information:

```
cisco-ap# show flexconnect oeap firewall dmz
```

show flexconnect wlan

To view the WLAN configuration for Flexconnect AP mode, use the **show flexconnect wlan** command.

show flexconnect wlan [**l2acl** | **qos** | **vlan**]

Syntax Description

l2acl	Specifies the Layer 2 ACL mapping for WLAN
qos	Specifies the QoS parameters for WLAN
vlan	Specifies the VLAN mapping for WLAN

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the WLAN Layer 2 ACL mapping for the Flexconnect AP:

```
cisco-ap# show flexconnect wlan l2acl
```

show interfaces dot11Radio

To view the interface status and configuration for an 802.11 radio, use the **show interfaces dot11Radio** command.

show interfaces dot11Radio *radio-interface-number* {**dfs** | **memory** [*memory-address length* | **firmware**] | **mumimo** *wlan-number* | **sniffer** | **statistics** | **wlan***wlan-id* **datapathcounters** | **statistics** }

Syntax Description

radio-interface-number	Specifies the interface number for 802.11 radio. The valid range is from 0 to 1
dfs	Displays the DFS statistics
memory	Displays the dump radio memory
memory-address	Specifies the memory address. The valid range is between 0 and ffffffff
length	Specifies the length. The valid range is from 0 to 64
firmware	Dumps firmware logs
mumimo	Displays the multiuser MIMO statistics information
wlan-number	The 802.11-specific value whose valid range is from 0 to 15.
sniffer	Displays the sniffer mode statistics
statistics	Displays the statistics information for 802.11 radio **Note** Cisco 1852, 9117, 9130 APs do not include the beacon tx statistics under the 802.11 tx statistics counter.
wlan *wlan-id*	Displays the specified WLAN information
datapath	Displays the datapath counters.
counters	Displays the datapath counters and drops.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.
8.9	This command was enhanced by adding the **datapath** parameter.

The following example shows how to view the DFS statistics for a 802.11 interface whose number is 1:

```
cisco-ap# show interfaces dot11Radio 1 dfs

DFS Data:
```

```
Radar Detected:          0
Inactive Radar Detected: 0
```

show interfaces network

To view the Linux network interfaces, use the **show interfaces network** command.

show interfaces network

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the Linux network interfaces:

```
cisco-ap# show interfaces network
```

show interfaces wired

To view the wired interface, use the **show interfaces wired** command.

show interfaces wired *wired-interface-number* {**MIB-stats** | **datapath counters**}

Syntax Description

wired-interface-number	Wired interface number; valid range is between 0 to 3
MIB-stats	Displays the AP internal-Switch MIB counters.
datapath	Displays the datapath counters.
counters	Displays the datapath counters and drops.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.
8.9	This command was enhanced by adding the **datapath** parameter.

The following example shows how to view the wired interface whose number is 1:

```
cisco-ap# show interfaces wired 1
```

show inventory

To view the physical inventory, use the **show inventory** command.

show inventory

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the physical inventory:

```
cisco-ap# show inventory

NAME: AP2800, DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9 , VID: V01, SN: XXXXXXXXXXX
```

show ip

To view the IP information, use the **show ip** command.

show ip {**access-lists** | **interface brief** | **route** | **tunnel** [**eogre** {**domain** | **forwarding-table** | **gateway**} | **fabric** | **summary**| **sip-snooping**{ **stats**| **status**}]}

Syntax Description

access-lists	Lists the IP access lists
interface	Displays the IP interface status and configuration
brief	Displays the brief summary of IP status and configuration
route	Displays the IP routing table
tunnel	Displays the IP tunnel information
eogre	Displays the EoGRE tunnel information
domain	Displays the EoGRE tunnel domain information
forwarding-table	Displays the EoGRE tunnel encapsulation and decapsulation information
gateway	Displays the EoGRE tunnel gateway information
fabric	Displays the IP fabric tunnel information
summary	Displays the information for all tunnels

sip-snooping	Displays the SIP snooping options.
stats	Displays the transmitted and received SIP snooping statistics.
status	Displays the SIP snooping status.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.
8.9	This command was enhanced by adding the **sip-snooping** parameter.

The following example shows how to view information about the lists the IP access lists:

```
cisco-ap# show ip access-lists
```

show lacp

To view the Link Aggregation Control Protocol (LACP) options, use the **show lacp** command.

show lacp {**counters** | **internal** | **neighbors**}

Syntax Description

counters	Displays traffic information
internal	Displays internal information
neighbors	Displays LACP neighbor entries

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the LACP traffic information:

```
cisco-ap# show lacp counters
```

show logging

To view the contents of logging buffers, use the **show logging** command.

show logging

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the contents of logging buffers:

```
cisco-ap# show logging
```

show memory

To display memory usage on an access point, use the **show memory** command.

show memory [**detail** | **pool** | **summary**]

Syntax Description

detail	Displays detailed system memory usage
pool	Displays system memory pool
summary	Display system memory usage statistics

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the system memory usage statistics:

```
cisco-ap# show memory
Memory summary:
MemTotal:        1030608 kB
MemFree:          713832 kB
MemAvailable:     710492 kB
Buffers:               0 kB
Cached:            88224 kB
SwapCached:            0 kB
Active:            28932 kB
Inactive:          82872 kB
Active(anon):      28900 kB
Inactive(anon):    82812 kB
Active(file):         32 kB
Inactive(file):       60 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:         23580 kB
Mapped:            11380 kB
```

```
Shmem:             88132 kB
Slab:             132140 kB
SReclaimable:       3368 kB
SUnreclaim:       128772 kB
KernelStack:         864 kB
PageTables:          748 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:      515304 kB
Committed_AS:     193960 kB
VmallocTotal:    1024000 kB
VmallocUsed:       69808 kB
VmallocChunk:     915324 kB

System Memory:
             total         used         free       shared      buffers
Mem:       1030608       316848       713760            0            0
-/+ buffers:             316848       713760
Swap:            0            0            0
```

show policy-map

To view policy maps on access point, use the **show policy-map** command.

show policy-map

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the policy maps on the access point:

```
cisco-apshow policy-map
```

show processes

To view process utilization details, use the **show processes** command.

showprocesses {**cpu** *cpu-number* | **dmalloc** {**capwap** | **wcp**} | **status**}

Syntax Description

cpu *cpu-number*	Displays the specified CPU's utilization of the processes; valid range of values for the CPU number is between 0 to 3
dmalloc	Displays the process utilization of the dmalloc processes
capwap	Displays dmalloc statistics for CAPWAP
wcp	Displays dmalloc statistics for WCP

status	Displays watchdog process status

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the process watchdog status:

```
cisco-ap# show processes status
            Process               Alive          Monitored
              capwapd               True               True
           switchdrvr               True              False
                 wcpd               True               True
               kclick               True               True
            cleanaird               True               True
              mrvlfwd               True               True
```

show processes memory

To display the processes on the access point, use the **show processes memory** command.

show processes memory {**maps** | **smaps**} **pid** *pid-number*

Syntax Description

maps	Displays maps for the processes
smaps	Displays smaps for the processes
pid *pid-number*	Process ID that you have to specify

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the list of processes utilizing the memory on the access point:

```
cisco-ap# show processes memory

Mem total:1030608 anon:23876 map:11424 free:712728
 slab:132748 buf:0 cache:88284 dirty:0 write:0
Swap total:0 free:0
  PID   VSZ^VSZRW   RSS (SHR) DIRTY (SHR) STACK COMMAND
 6227 56500 53464  1168   732  1144   732   132 /usr/sbin/mrvlfwd
 6283 27536 20668 13032  2400 13032  2400   132 /usr/sbin/capwapd
 6297 24880 10612 14536  1376 14536  1376   132 wcpd
```

```
 6255  9612  6600  1508  1052  1508  1052   132 /usr/sbin/cleanaird
 5122  9556  4144  2664  2012  2664  2012   132 /usr/bin/capwap_brain
29097  7148  1536  3560  2392  3556  2388   132 /usr/sbin/cisco_shell
 3142  6828  1216  2992  2264  2992  2264   132 /usr/sbin/cisco_shell
 5106  4588   404  1912  1644  1912  1644   132 /usr/bin/fastcgi -s /tmp/fcgi_sock
 5108  4588   404  1912  1644  1912  1644   132 /usr/bin/slowfcgi -s /tmp/slow_fcgi_sock
 6084  4544   452   928   360   928   360   132 /usr/sbin/lighttpd -f /etc/lighttpd.conf
 6214  3692   344  1420   960  1420   960   132 tamd_proc ap-tam 1 0 -debug err
 6213  3556   340  1460  1104  1460  1104   132 tams_proc -debug err
 6133  3396   400  1196   976  1196   976   132 /usr/bin/poder_agent
 4689  3176   336  1012   812  1012   812   132 /usr/bin/sync_log /storage/syslogs/13
 6143  3140   304  1428  1204  1428  1204   132 /usr/bin/failover
 4716  3136   284   616   436   616   436   132 watchdogd
 6121  3116   280   988   820   988   820   132 bigacl_d
 5084  3112   272   952   804   952   804   132 /usr/bin/led_core
 6181  1884   320  1044   260  1044   260   132 perl /usr/bin/drt.pl
    1  1596   196   492   412   492   412   132 init
30914  1596   196   428   344   428   344   132 top -m -b -n 1
 6145  1596   196   248   176   248   176   132 {S80cisco} /bin/sh /etc/init.d/S80cisco
start
30912  1592   192   424   356   424   356   132 {show_process_me} /bin/ash
/usr/bin/cli_scripts/show_process_memory.sh 0 0 0 0 0 0 0 0 0 0
30911  1592   192   400   336   400   336   132 /bin/sh -c
/usr/bin/cli_scripts/show_process_memory.sh 0 0 0 0 0 0 0 0 0 0 | more
 4684  1592   192   368   304   368   304   132 syslogd -S -s 100 -b 1 -L -R 255.255.255.255
30913  1592   192   332   264   332   264   132 more
 4688  1584   184   344   284   344   284   132 klogd
 4686  1584   184   320   264   320   264   132 printkd
30906  1584   184   284   228   284   228   132 sleep 10
29085  1452   332   640   416   640   416   132 /usr/sbin/dropbear -E -j -k -d
/storage/dropbear/dropbear_dss_host_key -r /storage/dropbear/dropbear_rsa_host_key
 6209  1384   264   416   364   416   364   132 /usr/sbin/dropbear -E -j -k -d
/storage/dropbear/dropbear_dss_host_key -r /storage/dropbear/dropbear_rsa_host_key
 8411  1096   212   444   336   444   336   132 dnsmasq -C /etc/dnsmasq.host.conf
 6115  1096   212   436   340   436   340   132 dnsmasq -C /etc/dnsmasq.vaperr.conf
```

show rrm

To view the Radio Resource Management (RRM) properties, use the **show rrm** command.

show rrm {**hyperlocation** [*level1-list*] | **neighbor-list** [**details**] | **receive** {**configuration** | **statistics**}}

Syntax Description

hyperlocation	*level1-list*	Displays status of Cisco Hyperlocation on the AP
neighbor-list		Displays neighbor-list statistics
receive		Receive signal strength indicator (RSSI) of the AP
rogue		Displays rogue-related information

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Usage Guidelines

The following example shows how to view the level 1 channel scan list in Hyperlocation:

```
cisco-ap# show rrm hyperlocation level1-list
Level-1 List for 2.4GHz Band
====================================
Channel   Width         Serving MAC   Max Clients
-------   -----   -----------------   -----------


Level-1 List for 5GHz Band
====================================
Channel   Width         Serving MAC   Max Clients
-------   -----   -----------------   -----------
```

show rrm rogue containment

To view rogue containment information on an access point, use the **show rrm rogue containment** command.

show rrm rogue containment {**ignore** | **info**} **Dot11Radio** *radio-interface-number*

Syntax Description

ignore	Displays list of rogue APs that are configured to be ignored
info	Displays rogue contaimnent configuration and statistics for an AP
Dot11Radio	Specifies the **Dot11Radio** interface keyword.
radio-interface-number	Slot of the radio interface; valid values are 0 and 1

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the rogue containment and statistics for the 802.11 interface numbered 1:

```
cisco-ap# show rrm rogue containment info Dot11Radio 1
Rogue Containment Info and Stats for slot 1:
bssid client-addr contain-type channels

      Request Status count
              Submit     0
             Success     0
             Timeout     0
               Error     0
               Tuned     0
             Flushed     0
         Bad Channel     0
        Tail Dropped     0
           Cancelled     0
NDP DFS Tx Cancelled     0
           Tx Failed     0
             Created     0
```

show rrm rogue detection

To view RRM rogue detection configuration parameters, use the **show rrm rogue detection** command.

show rrm rogue detection {**adhoc** | **ap** | **clients** | **config** | **rx-stats**} **Dot11Radio** *radio-interface-number*

Syntax Description

adhoc	Displays the primary ad hoc rogue AP list for a 802.11 radio slot; valid values are 0 and 1
ap	Displays rogue detection parameters for the AP for a 802.11 radio slot; valid values are 0 and 1
clients	Displays primary list of rogue clients
config	Displays rogue detection configuration on the AP
rx-stats	Displays rogue detection receive statistics on the 802.11 interfaces of an AP
Dot11Radio	Specifies 802.11 radio intereface
radio-interface-number	The 802.11 radio interface number; valid values are 0 and 1

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the RRM rogue detection configuration details:

```
cisco-ap# show rrm rogue detection config

Rogue Detection Configuration for Slot 0:
Rogue Detection Mode : Enabled
Rogue Detection Report Interval : 10
Rogue Detection Minimum Rssi : -90
Rogue Detection Transient Interval : 0
Rogue Detection Flex Contain : Disabled
Rogue Detection Flex Contain Adhoc : Disabled
Rogue Detection Flex Contain SSID : Disabled
Rogue Containment Autorate : Disabled
Scan Duration : 180000
Channel Count : 11
Transient Threshold : 0

Rogue Detection Configuration for Slot 1:
Rogue Detection Mode : Enabled
Rogue Detection Report Interval : 10
Rogue Detection Minimum Rssi : -90
Rogue Detection Transient Interval : 0
Rogue Detection Flex Contain : Disabled
Rogue Detection Flex Contain Adhoc : Disabled
Rogue Detection Flex Contain SSID : Disabled
```

```
Rogue Containment Autorate : Disabled
Scan Duration : 180000
Channel Count : 25
Transient Threshold : 0
```

show running-config

To display the contents of the currently running configuration on the access point, use the **show running-config** command.

show running-config

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the contents of the currently running configuration on the access point:

```
cisco-ap# show running-config

AP Name                      : ap1540
Admin State                  : Enabled
AP Mode                      : Local
AP Submode                   : None
Location                     : default location
Reboot Reason                : Config Mwar
Primary controller name      : cisco_3504
Primary controller IP        : <controller-ip-address>
Secondary controller name    :
Secondary controller IP      :
Tertiary controller name     :
Tertiary controller IP       :
Controller from DHCP offer   : <controller-dhcp-server-address>
Controller from DNS server   : <controller-dns-server-address>
AP join priority             : 1
IP Prefer-mode               : IPv4
CAPWAP UDP-Lite              : Unconfigured
Last Joined Controller name: wlc3504
DTLS Encryption State        : Disabled
Discovery Timer              : 10
Heartbeat Timer              : 30
CDP State                    : Enabled
Watchdog monitoring          : Enabled
IOX                          : Disabled
RRM State                    : Enabled
LSC State                    : Disabled
SSH State                    : Enabled
AP Username                  : admin
Session Timeout              : 0
Extlog Host                  : 0.0.0.0
Extlog Flags                 : 0
Extlog Status Interval       : 0
Syslog Host                  : <syslog-host-ip-address>
```

```
Syslog Facility            : 0
Syslog Level               : errors
Core Dump TFTP IP Addr     :
Core Dump File Compression : Disabled
Core Dump Filename         :
Client Trace Status        : Enabled(All)
Client Trace All Clients   : Enabled
Client Trace Filter        : 0x0000000E
Client Trace Out ConsoleLog: Disabled
WLC Link LAG status        : Disabled
AP Link LAG status         : Disabled
AP WSA Mode                : Disabled
```

show security data-corruption

To view data inconsistency errors, use the **show security data-corruption** command.

show security data-corruption

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.7	This command was introduced.

Examples

The following example shows how to view data inconsistency errors:

```
cisco-ap# show security data-corruption
```

show security system state

To view the current state of system-level security, use the **show security system state** command.

show security system state

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.7	This command was introduced.

Examples

To view the current state of system-level security, use this command:

```
cisco-ap# show security system state

 XSPACE:
                Non-Executable stack:      Yes
                Non-Executable heap:       Yes
                Non-Writable text:         Yes
  OSC:
                Version:                1.1.0
  SafeC:
                Version:                3.1.1
```

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

Table 1: show security system state Field Descriptions

Field	Description
Non-Executable stack	Indicates whether the system prevents execution from the stack
Non-Executable heap	Indicates whether the system prevents execution from the heap
Non-Writable text	Indicates whether the system prevents the text section from being writable
OSC version	Indicates the version of the OSC library used by the applications
SafeC version	Indicates the version of the SafeC library used by the applications

show spectrum

To view the show commands of the spectrum firmware, use the **show spectrum** command.

show spectrum {**list** | **recover** | **status** }

Syntax Description

list	Lists the spectrum FW data files
recover	Displays the spectrum FW recover count
status	Displays the spectrum FW status

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the spectrum firmware status:

```
cisco-ap# show spectrum status

Spectrum FW status slot 0:
  version:  1.15.4
  status:   up, crashes 0, resets 0, radio reloads 0
  load:     37.00  34.75  33.50  33.25
  NSI Key:  26c1bd25893a4b6dd3a00fe71735d067
  NSI:      not configured
  reg_wdog: 255 26309 0
  dfs_wdog: 0
  dfs_freq: 0
Spectrum FW status slot 1:
  version:  1.15.4
  status:   up, crashes 0, resets 0, radio reloads 0
  load:     37.25  38.00  38.75  39.00
  NSI Key:  26c1bd25893a4b6dd3a00fe71735d067
  NSI:      not configured
  reg_wdog: 255 26309 0
  dfs_wdog: 0
  dfs_freq: 0
```

show tech-support

To automatically run show commands that display system information, use the **show tech-support** command.

show tech-support

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to automatically run show commands that display system information:

```
cisco-ap# show tech-support
```

show version

To view the software version information of the AP, use the **show version** command.

show version

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the software version information of the AP:

```
cisco-ap# show version
```

show trace dot11_chn

To view off-channel events on 802.11 channel of an AP, use the **show trace dot11_chn** command.

show trace dot11_chn {**enable** | **disable** | **statistics**}

Syntax Description

enable	Enables displaying of off-channel events on the 802.11 radio 0 and 1
disable	Disables displaying of off-channel events on the 802.11 radios 0 and 1
statistics	Displays off-channel event statistics on 802.11 radios 0 and 1

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to view off-channel event statistics on 802.11 radios:

```
cisco-ap# show trace dot11_chn statistics

Dot11Radio0 Off-Channel Statistics:
total_count in_prog_count last-chan last-type last-dur
          0             0         0         0        0

Dot11Radio1 Off-Channel Statistics:
total_count in_prog_count last-chan last-type last-dur
          0             0         0         0        0
```

show trace

To view trace logs on the AP, use the **show trace** command.

```
show trace
```

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the trace logs on the AP:

```
cisco-ap# show trace
```

show wips

To view details of the AP that is configured in wIPS mode, use the **show wips** command.

show wips {**alarm** *alarm-id* | **analyzer** | **buffer** | **channel** *channelno* | **infrastructure-device** | **neighbors** | **node mac** *mac-address* | **node number** *number* | **object** | **policy** *policy-id* | **policy ssid** | **session** *mac-address* | **stats** | **violation node** *mac-address* | **violation channel** *channel-number*}

Syntax Description

alarm	Displays statistics of the configured alarm if the AP is configured in wIPS mode; valid values are between 0 and 255
alarm-id	Alarm ID; valid values are between 0 and 255
analyzer	Displays analyzer related statistics
buffer	Displays statistics of the buffer
channel	Displays channel related statistics
channelno	Channel number; valid values are between 0 and 255
infrastructure-device	Displays AP infrastructure information
neighbors	Displays statistics of neighbors.
node	Displays AP node information
mac *mac-address*	MAC address of the node.
node	Node.
number *number*	Node number; valid values are between 1 and 500
object	AP object store
policy {*policy-id* |**ssid**	AP policy; you must specify either a policy ID or the policy SSID.
session *mac-address*	Displays node session details; you must enter the MAC address of the node

stats	Displays AP statistics
violation	Tracks AP violations
node *mac-address*	Tracks node-based violations
channel *channel-number alarm-id*	Tracks channel-based violations; you must enter channel numbeer and alarm ID

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows how to view the wIPS statistics information on the AP:

```
cisco-ap# show wips stats
```