CLI Commands

The Cisco Wireless LAN solution command-line interface (CLI) enables operators to connect an ASCII console to the Cisco Wireless LAN Controller and configure the controller and its associated access points.

Show Commands

This section lists the **show** commands to display information about your configuration settings for access points.

Show Access Point Commands

Use the **show ap** commands to see access point settings.

show ap auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap auto-rf** command.

show ap auto-rf 802.11 {**a** | **b**} *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Examples

This example shows how to display auto-RF information for an access point:

```
> show ap auto-rf 802.11a AP1
Number Of Slots.................................. 2
AP Name.......................................... AP03
MAC Address...................................... 00:0b:85:01:18:b7
  Radio Type..................................... RADIO_TYPE_80211a
  Noise Information
    Noise Profile................................ PASSED
    Channel 36...................................  -88 dBm
    Channel 40...................................  -86 dBm
    Channel 44...................................  -87 dBm
    Channel 48...................................  -85 dBm
    Channel 52...................................  -84 dBm
    Channel 56...................................  -83 dBm
    Channel 60...................................  -84 dBm
    Channel 64...................................  -85 dBm
  Interference Information
    Interference Profile......................... PASSED
    Channel 36...................................  -66 dBm @  1% busy
    Channel 40................................... -128 dBm @  0% busy
    Channel 44................................... -128 dBm @  0% busy
    Channel 48................................... -128 dBm @  0% busy
    Channel 52................................... -128 dBm @  0% busy
    Channel 56...................................  -73 dBm @  1% busy
    Channel 60...................................  -55 dBm @  1% busy
    Channel 64...................................  -69 dBm @  1% busy
  Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel 36................................... 16/ 0/ 0
    Channel 40................................... 28/ 0/ 0
    Channel 44...................................  9/ 0/ 0
    Channel 48...................................  9/ 0/ 0
    Channel 52...................................  3/ 0/ 0
    Channel 56...................................  4/ 0/ 0
    Channel 60...................................  7/ 1/ 0
    Channel 64...................................  2/ 0/ 0
  Load Information
    Load Profile................................. PASSED
    Receive Utilization.......................... 0%
    Transmit Utilization......................... 0%
    Channel Utilization.......................... 1%
    Attached Clients............................. 1 clients
  Coverage Information
    Coverage Profile............................. PASSED
    Failed Clients............................... 0 clients
```

```
Client Signal Strengths
  RSSI -100 dBm..............................  0 clients
  RSSI  -92 dBm..............................  0 clients
  RSSI  -84 dBm..............................  0 clients
  RSSI  -76 dBm..............................  0 clients
  RSSI  -68 dBm..............................  0 clients
  RSSI  -60 dBm..............................  0 clients
  RSSI  -52 dBm..............................  0 clients
Client Signal To Noise Ratios
  SNR    0 dBm..............................  0 clients
  SNR    5 dBm..............................  0 clients
  SNR   10 dBm..............................  0 clients
  SNR   15 dBm..............................  0 clients
  SNR   20 dBm..............................  0 clients
  SNR   25 dBm..............................  0 clients
  SNR   30 dBm..............................  0 clients
  SNR   35 dBm..............................  0 clients
  SNR   40 dBm..............................  0 clients
  SNR   45 dBm..............................  0 clients
Nearby RADs
  RAD 00:0b:85:01:05:08 slot 0.................  -46 dBm on 10.1.30.170
  RAD 00:0b:85:01:12:65 slot 0.................  -24 dBm on 10.1.30.170
Channel Assignment Information
  Current Channel Average Energy...............  -86 dBm
  Previous Channel Average Energy..............  -75 dBm
  Channel Change Count.........................  109
  Last Channel Change Time..................... Wed Sep 29 12:53e:34 2004
  Recommended Best Channel..................... 44
RF Parameter Recommendations
  Power Level.................................. 1
  RTS/CTS Threshold............................ 2347
  Fragmentation Threshold...................... 2346
  Antenna Pattern.............................. 0
```

show ap ccx rm

To display an access point's Cisco Client eXtensions (CCX) radio management status information, use the **show ap ccx rm** command.

show ap ccx rm *ap_name* **status**

Syntax Description

ap_name	Specified access point name.
status	Displays the CCX radio management status information for an access point.

Command Default

None.

Examples

This example shows how to display the status of the CCX radio management:

```
> show ap ccx rm AP1240-21ac status
A Radio
Channel Load Request ..................... Disabled
Noise Histogram Request .................. Disabled
Beacon Request ........................... Disabled
Frame Request ............................ Disabled
Interval ................................. 60
Iteration ................................ 10
G Radio
Channel Load Request ..................... Disabled
Noise Histogram Request .................. Disabled
Beacon Request ........................... Disabled
Frame Request ............................ Disabled
Interval ................................. 60
Iteration ................................ 10
```

Related Commands

config ap

show ap cdp

To display the Cisco Discovery Protocol (CDP) information for an access point, use the **show ap cdp** command.

show ap cdp {**all** | **ap-name** *cisco_ap* | **neighbors** {**all** | **ap-name** *cisco_ap* | **detail** *cisco_ap*}}

Syntax Description

all	Displays the CDP status on all access points.
ap-name	Displays the CDP status for a specified access point.
cisco_ap	Specified access point name.
neighbors	Displays neighbors using CDP.
detail	Displays details about a specific access point neighbor using CDP.

Command Default

None.

Examples

This example shows how to display the CDP status of all access points:

```
> show ap cdp all
AP CDP State
AP Name             AP CDP State
------------------  ----------
SB_RAP1              enable
SB_MAP1              enable
SB_MAP2              enable
SB_MAP3              enable
```

This example shows how to display the CDP status of a specified access point:

```
> show ap cdp ap-name SB_RAP1
AP CDP State
AP Name             AP CDP State
------------------  ----------
AP CDP State.......................Enabled
AP Interface-Based CDP state
 Ethernet 0.....................Enabled
 Slot 0.........................Enabled
 Slot 1.........................Enabled
```

This example shows how to display details about all neighbors using CDP:

```
> show ap cdp neighbor all
AP Name     AP IP            Neighbor Name       Neighbor IP      Neighbor Port
---------   --------------   ------------------  --------------   -------------
SB_RAP1     192.168.102.154  sjc14-41a-sw1       192.168.102.2    GigabitEthernet1/0/13
SB_RAP1     192.168.102.154  SB_MAP1             192.168.102.137  Virtual-Dot11Radio0
SB_MAP1     192.168.102.137  SB_RAP1             192.168.102.154  Virtual-Dot11Radio0
SB_MAP1     192.168.102.137  SB_MAP2             192.168.102.138  Virtual-Dot11Radio0
SB_MAP2     192.168.102.138  SB_MAP1             192.168.102.137  Virtual-Dot11Radio1
SB_MAP2     192.168.102.138  SB_MAP3             192.168.102.139  Virtual-Dot11Radio0
SB_MAP3     192.168.102.139  SB_MAP2             192.168.102.138  Virtual-Dot11Radio1
```

This example shows how to display details about a specific neighbor with a specified access point using CDP:

```
> show ap cdp neighbors ap-name SB_MAP2
AP Name      AP IP            Neighbor Name    Neighbor IP      Neighbor Port
-----------  ---------------  ---------------  --------------  -------------
SB_MAP2      192.168.102.138  SB_MAP1          192.168.102.137  Virtual-Dot11Radio1
SB_MAP2      192.168.102.138  SB_MAP3          192.168.102.139  Virtual-Dot11Radio0
```

This example shows how to display details about neighbors using CDP:

```
> show ap cdp neighbors detail SB_MAP2
AP Name:SB_MAP2
AP IP address:192.168.102.138
-------------------------
Device ID: SB_MAP1
Entry address(es): 192.168.102.137
Platform: cisco AIR-LAP1522AG-A-K9  ,  Cap
Interface: Virtual-Dot11Radio0,  Port ID (outgoing port): Virtual-Dot11Radio1
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
 Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by
advertisement version: 2
-------------------------
Device ID: SB_MAP3
Entry address(es): 192.168.102.139
Platform: cisco AIR-LAP1522AG-A-K9  ,  Capabilities: Trans-Bridge
Interface: Virtual-Dot11Radio1,  Port ID (outgoing port): Virtual-Dot11Radio0
Holdtime : 180 sec
Version :
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Experimental Version 12.4(200
81114:084420) [BLD-v124_18a_ja_throttle.20081114 208] Copyright (c) 1986-2008 by
 Cisco Systems, Inc. Compiled Fri 14-Nov-08 23:08 by
advertisement version: 2
```

Related Commands

config ap cdp

config cdp timer

show ap channel

To display the available channels for a specific mesh access point, use the **show ap channel** command.

show ap channel *ap_name*

Syntax Description

ap_name	Name of the mesh access point.

Command Default None.

Examples This example shows how to display the available channels for a particular access point:

```
> show ap channel AP47
 802.11b/g Current Channel ...........1
Allowed Channel List.....................1,2,3,4,5,6,7,8,9,10,11
802.11a Current Channel .................161
Allowed Channel List.....................36,40,44,48,52,56,60,64,100,
.........................................104,108,112,116,132,136,140,
.........................................149,153,157,161
```

Related Commands

config 802.11-a channel ap

config 802.11h channelswitch

config 802.11h setchannel

show ap config

To display the detailed configuration for a lightweight access point, use the **show ap config** command.

show ap config 802.11{**a** | **b**} [**summary**] *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a or 802.11b/g network.
802.11b	Specifies the 802.11b/g network.
summary	(Optional) Displays radio summary of all APs
cisco_ap	Lightweight access point name.

Command Default

None.

Examples

This example shows how to display the detailed configuration for an access point:

```
> show ap config 802.11a AP02
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... AP02
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Regulatory Domain............................. Unconfigured
Switch Port Number .............................. 1
MAC Address...................................... 00:0b:85:18:b6:50
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.49.240
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 1.100.49.1
CAPWAP Path MTU.................................. 1485
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default-location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. Cisco_32:ab:63
Primary Cisco Switch IP Address.................. Not Configured
Secondary Cisco Switch...........................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch............................
Tertiary Cisco Switch IP Address................. Not Configured
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Sniffer
Public Safety ................................... Global: Disabled, Local: Disabled
AP SubMode ...................................... Not Configured
Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
Logging syslog facility ......................... kern
S/W  Version .................................... 7.0.110.6
Boot  Version ................................... 12.4.18.0
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
Stats Re--More-- or (q)uit
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Enabled
```

```
PoE Power Injector MAC Addr..................... Disabled
Power Type/Mode................................. Power injector / Normal mode
Number Of Slots................................. 2
AP Model........................................ AIR-LAP1142N-A-K9
AP Image........................................ C1140-K9W8-M
IOS Version..................................... 12.4(20100502:031212)
Reset Button.................................... Enabled
AP Serial Number................................ FTX1305S180
AP Certificate Type............................. Manufacture Installed
AP User Mode.................................... AUTOMATIC
AP User Name.................................... Not Configured
AP Dot1x User Mode.............................. Not Configured
AP Dot1x User Name.............................. Not Configured
Cisco AP system logging host.................... 255.255.255.255
AP Up Time...................................... 47 days, 23 h 47 m 47 s
AP LWAPP Up Time................................ 47 days, 23 h 10 m 37 s
Join Date and Time.............................. Tue May  4 16:05:00 2010
Join Taken Time................................. 0 days, 00 h 01 m 37 s
Attributes for Slot  1
    Radio Type.................................. RADIO_TYPE_80211n-5
    Radio Subband............................... RADIO_SUBBAND_ALL
    Administrative State ....................... ADMIN_ENABLED
    Operation State ............................ UP
    Radio Role ................................. ACCESS
    CellId ..................................... 0
Station Configuration
      Configuration ............................ AUTOMATIC
      Number Of WLANs .......................... 2
      Medium Occupancy Limit ..................... 100
      CFP Period ............................... 4
      CFP MaxDuration .......................... 60
      BSSID .................................... 00:24:97:88:99:60
Operation Rate Set
        6000 Kilo Bits.......................... MANDATORY
        9000 Kilo Bits.......................... SUPPORTED
        12000 Kilo Bits......................... MANDATORY
        18000 Kilo Bits......................... SUPPORTED
        24000 Kilo Bits......................... MANDATORY
        36000 Kilo Bits......................... SUPPORTED
        48000 Kilo Bits......................... SUPPORTED
        54000 Kilo Bits......................... SUPPORTED
      MCS Set
        MCS 0................................... SUPPORTED
        MCS 1................................... SUPPORTED
        MCS 2................................... SUPPORTED
        MCS 3................................... SUPPORTED
        MCS 4................................... SUPPORTED
        MCS 5................................... SUPPORTED
        MCS 6................................... SUPPORTED
        MCS 7................................... SUPPORTED
        MCS 8................................... SUPPORTED
        MCS 9................................... SUPPORTED
        MCS 10.................................. SUPPORTED
        MCS 11.................................. SUPPORTED
        MCS 12.................................. SUPPORTED
        MCS 13.................................. SUPPORTED
        MCS 14.................................. SUPPORTED
        MCS 15.................................. SUPPORTED
      Beacon Period ............................ 100
      Fragmentation Threshold .................. 2346
      Multi Domain Capability Implemented ..... TRUE
      Multi Domain Capability Enabled ......... TRUE
      Country String ........................... US
Multi Domain Capability
      Configuration ............................ AUTOMATIC
      First Chan Num ........................... 36
      Number Of Channels ....................... 21
MAC Operation Parameters
      Configuration ............................ AUTOMATIC
      Fragmentation Threshold .................. 2346
      Packet Retry Limit ....................... 64
Tx Power
      Num Of Supported Power Levels ............ 6
```

```
      Tx Power Level 1 ..................... 14 dBm
      Tx Power Level 2 ..................... 11 dBm
      Tx Power Level 3 ..................... 8 dBm
      Tx Power Level 4 ..................... 5 dBm
      Tx Power Level 5 ..................... 2 dBm
      Tx Power Level 6 ..................... -1 dBm
      Tx Power Configuration ..................... AUTOMATIC
      Current Tx Power Level ..................... 0
Phy OFDM parameters
      Configuration ..... AUTOMATIC
      Current Channel ..... 36
      Extension Channel ..... NONE
      Channel Width..... 20 Mhz
      Allowed Channel List..... 36,40,44,48,52,56,60,64,100,
        ..... 104,108,112,116,132,136,140,
        ..... 149,153,157,161,165
      TI Threshold ..... -50
      Legacy Tx Beamforming Configuration ..... AUTOMATIC
      Legacy Tx Beamforming ..... DISABLED
      Antenna Type..... INTERNAL_ANTENNA
      Internal Antenna Gain (in .5 dBi units).... 6
      Diversity..... DIVERSITY_ENABLED
      802.11n Antennas
        Tx
         A..... ENABLED
         B..... ENABLED
        Rx
         A..... ENABLED
         B..... ENABLED
         C..... ENABLED
Performance Profile Parameters
      Configuration ..... AUTOMATIC
      Interference threshold..... 10 %
      Noise threshold..... -70 dBm
      RF utilization threshold..... 80 %
      Data-rate threshold..... 1000000 bps
      Client threshold..... 12 clients
      Coverage SNR threshold..... 16 dB
      Coverage exception level..... 25 %
      Client minimum exception level..... 3 clients
Rogue Containment Information
    Containment Count..... 0
CleanAir Management Information
        CleanAir Capable..... No
Radio Extended Configurations:
        Buffer size .....30
        Data-rate.....0
        Beacon strt .....90 ms
       Rx-Sensitivity SOP threshold ..... -80 dB
       CCA threshold ..... -60 dB
```

This example shows how to display the detailed configuration for another access point:

> **show ap config 802.11b AP02**

```
Cisco AP Identifier..... 0
Cisco AP Name..... AP02
AP Regulatory Domain..... Unconfigured
Switch Port Number ..... 1
MAC Address..... 00:0b:85:18:b6:50
IP Address Configuration..... DHCP
IP Address..... 1.100.49.240
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 1.100.49.1
Cisco AP Location..... default-location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... Cisco_32:ab:63
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
```

```
Remote AP Debug ................................ Disabled
S/W  Version ................................... 3.1.61.0
Boot  Version .................................. 1.2.59.6
Stats Reporting Period ......................... 180
LED State....................................... Enabled
ILP Pre Standard Switch......................... Disabled
ILP Power Injector.............................. Disabled
Number Of Slots................................. 2
AP Model........................................ AS-1200
AP Serial Number................................ 044110223A
AP Certificate Type............................. Manufacture Installed
Attributes for Slot  1
    Radio Type.................................. RADIO_TYPE_80211g
    Administrative State ....................... ADMIN_ENABLED
    Operation State ............................ UP
    CellId ..................................... 0
    Station Configuration
      Configuration ............................ AUTOMATIC
      Number Of WLANs .......................... 1
      Medium Occupancy Limit ................... 100
      CFP Period ............................... 4
      CFP MaxDuration .......................... 60
      BSSID .................................... 00:0b:85:18:b6:50
      Operation Rate Set
        1000 Kilo Bits.......................... MANDATORY
        2000 Kilo Bits.......................... MANDATORY
        5500 Kilo Bits.......................... MANDATORY
        11000 Kilo Bits......................... MANDATORY
        6000 Kilo Bits.......................... SUPPORTED
        9000 Kilo Bits.......................... SUPPORTED
        12000 Kilo Bits......................... SUPPORTED
        18000 Kilo Bits......................... SUPPORTED
        24000 Kilo Bits......................... SUPPORTED
        36000 Kilo Bits......................... SUPPORTED
        48000 Kilo Bits......................... SUPPORTED
        54000 Kilo Bits......................... SUPPORTED
      Beacon Period ............................ 100
      DTIM Period .............................. 1
      Fragmentation Threshold .................. 2346
      Multi Domain Capability Implemented ..... TRUE
      Multi Domain Capability Enabled ......... TRUE
      Country String ........................... US
    Multi Domain Capability
      Configuration ............................ AUTOMATIC
      First Chan Num ........................... 1
      Number Of Channels ....................... 11
    MAC Operation Parameters
      Configuration ............................ AUTOMATIC
      RTS Threshold ............................ 2347
      Short Retry Limit ........................ 7
      Long Retry Limit ......................... 4
      Fragmentation Threshold .................. 2346
      Maximum Tx MSDU Life Time ................ 512
      Maximum Rx Life Time...................... 512
    Tx Power
      Num Of Supported Power Levels............. 5
      Tx Power Level 1 ......................... 17 dBm
      Tx Power Level 2.......................... 14 dBm
      Tx Power Level 3.......................... 11 dBm
      Tx Power Level 4.......................... 8 dBm
      Tx Power Level 5.......................... 5 dBm
      Tx Power Configuration.................... CUSTOMIZED
      Current Tx Power Level.................... 5
    Phy OFDM parameters
      Configuration............................. CUSTOMIZED
      Current Channel........................... 1
      TI Threshold.............................. -50
      Legacy Tx Beamforming Configuration ...... CUSTOMIZED
      Legacy Tx Beamforming .................... ENABLED
      Antenna Type.............................. INTERNAL_ANTENNA
      Internal Antenna Gain (in5 dBm units)..... 11
      Diversity................................. DIVERSITY_ENABLED
    Performance Profile Parameters
```

```
    Configuration.............................. AUTOMATIC
    Interference threshold..................... 10%
    Noise threshold.............................  -70 dBm
    RF utilization threshold................... 80%
    Data-rate threshold........................ 1000000 bps
    Client threshold........................... 12 clients
    Coverage SNR threshold..................... 12 dB
    Coverage exception level................... 25%
    Client minimum exception level............. 3 clients
  Rogue Containment Information
  Containment Count............................ 0
```

This example shows how to display the general configuration of a Cisco access point:

> **show ap config general cisco-ap**

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... cisco-ap
Country code..................................... US - United States
Regulatory Domain allowed by Country............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 12:12:12:12:12:12
IP Address Configuration......................... DHCP
IP Address....................................... 10.10.10.21
IP NetMask....................................... 255.255.255.0
CAPWAP Path MTU.................................. 1485
Domain.......................................
Name Server...................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ 4404
Primary Cisco Switch IP Address.................. 10.10.10.32
Secondary Cisco Switch Name......................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name....................... 4404
Tertiary Cisco Switch IP Address................. 3.3.3.3
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Global: Disabled, Local: Disabled
AP subMode ...................................... WIPS
Remote AP Debug ................................. Disabled
S/W  Version .................................... 5.1.0.0
Boot  Version ................................... 12.4.10.0
Mini IOS Version ................................ 0.0.0.0
Stats Reporting Period .......................... 180
LED State........................................ Enabled
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. PoE/Low Power (degraded mode)
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1252AG-A-K9
IOS Version...................................... 12.4(10:0)
Reset Button..................................... Enabled
AP Serial Number................................. serial_number
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation........... Enabled (Global MFP Disabled)
AP User Mode..................................... CUSTOMIZED
AP username...................................... maria
AP Dot1x User Mode............................... Not Configured
AP Dot1x username................................ Not Configured
Cisco AP system logging host..................... 255.255.255.255
AP Up Time....................................... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time................................. 4 days, 06 h 15 m 00 s
Join Date and Time............................... Mon Mar 3 06:19:47 2008
Ethernet Port Duplex............................. Auto
Ethernet Port Speed.............................. Auto
AP Link Latency.................................. Enabled
```

```
 Current Delay.................................. 0 ms
 Maximum Delay.................................. 240 ms
 Minimum Delay.................................. 0 ms
 Last updated (based on AP Up Time)............. 4 days, 06 h 17 m 20 s
Rogue Detection................................. Enabled
AP TCP MSS Adjust.............................. Disabled
Mesh preferred parent.......................... 00:24:13:0f:92:00
```

Related Commands

config ap

config ap config global

show ap config global

To display the global syslog server settings for all access points that join the controller, use the **show ap config global** command.

show ap config global

Syntax Description This command has no arguments and keywords.

Examples This example shows how to display global syslog server settings:

```
> show ap config global
AP global system logging host................................ 255.255.255.255
```

Related Commands

config ap

show ap config

show ap core-dump

To display the memory core dump information for a lightweight access point, use the **show ap core-dump** command.

show ap core-dump *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default None.

Examples This example shows how to display memory core dump information:

```
> show ap core-dump AP02
Memory core dump is disabled.
```

Related Commands

config ap core-dump

show ap crash-file

show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

show ap crash-file

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the crash file generated by the access point:

```
> show ap crash-file
```

Related Commands

config ap crash-file clear-all

config ap crash-file delete

config ap crash-file get-crash-file

config ap crash-file get-radio-core-dump

show ap data-plane

To display the data plane status for all access points or a specific access point, use the **show ap data-plane** command.

show ap data-plane {**all** | *cisco_ap*}

Syntax Description

all	Specifies all Cisco lightweight access points.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None.

Examples

This example shows how to display the data plane status of all access points:

```
> show ap data-plane all
Min Data          Data          Max Data     Last
AP Name              Round Trip      Round Trip      Round Trip    Update
------------------  -------------  -------------  -------------  ------
1130                       0.000s          0.000s       0.002s     18:51:23
1240                       0.000s          0.000s       0.000s     18:50:45
```

show ap ethernet tag

To display the VLAN tagging information of an Ethernet interface, use the **show ap ethernet tag** command.

show ap ethernet tag {**summary** | *cisco_ap*}

Syntax Description

summary	Displays the VLAN tagging information for all access points associated to the controller.
cisco_ap	Name of the Cisco lightweight access point. Displays the VLAN tagging information for a specific access point associated to the controller.

Command Default

None.

Usage Guidelines

If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the WCS, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.

Examples

This example shows how to display the VLAN tagging information for all access points associated to the controller:

```
> show ap ethernet tag summary

AP Name              Vlan Tag Configuration
------------------   -------
AP2                  7        (Failover to untagged)
charan.AP1140.II     disabled
```

Related Commands

config ap ethernet

config ap ethernet duplex

config ap ethernet tag

show ap config general

show ap eventlog

To display the contents of the event log file for an access point that is joined to the controller, use the **show ap eventlog** command.

show ap eventlog *ap_name*

Syntax Description

ap_name	Event log for the specified access point.

Command Default

None.

Examples

This example shows how to display the event log of an access point:

```
> show ap eventlog ciscoAP
AP event log download has been initiated
Waiting for download to complete
AP event log download completed.
======================= AP Event log Contents =====================
*Feb 13 11:54:17.146: %CAPWAP-3-CLIENTEVENTLOG: AP event log has been cleared from the
contoller 'admin'
*Feb 13 11:54:32.874: *** Access point reloading. Reason: Reload Command ***
*Mar 1 00:00:39.134: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:39.174: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:39.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:49.947: %CAPWAP-3-CLIENTEVENTLOG: Did not get vendor specific options from
DHCP.
...
```

show ap image

To display the detailed information about the predownloaded image for specified access points, use the **show ap image** command.

show ap image {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Name of the lightweight access point.
all	Specifies all access points.

Note If you have an AP that has the name *all*, it conflicts with the keyword **all** that specifies all access points. In this scenario, the keyword **all** takes precedence over the AP that is named *all*.

Examples

This example shows how to display images present on all access points:

```
> show ap image all
Total number of APs.............................. 7
Number of APs
Initiated........................................ 4
Predownloading................................... 0
Completed predownloading......................... 3
Not Supported.................................... 0
Failed to Predownload............................ 0
AP Name   Primary Image  Backup Image   Status           Version Next  Retry Time
Retry Count
----------------- -------------- -------------- ---------------- -------------- -----------
AP1140-1   7.0.56.0       6.0.183.38  Complete        6.0.183.38     NA                NA
AP1140-2  7.0.56.0       6.0.183.58  Initiated       6.0.183.38  23:46:43
    1
AP1130-2  7.0.56.0       6.0.183.38  Complete        6.0.183.38  NA
NA
AP1130-3  7.0.56.0       6.0.183.58  Initiated       6.0.183.38  23:43:25               1
AP1130-4  7.0.56.0       6.0.183.38  Complete        6.0.183.38  NA
    NA
AP1130-5  7.0.56.0       6.0.183.58  Initiated       6.0.183.38  23:43:00            1
AP1130-6  7.0.56.0       6.0.183.58  Initiated       6.0.183.38  23:41:33
```

Related Commands

config ap image predownload

config ap image swap

show ap inventory

To display inventory information for an access point, use the **show ap inventory** command.

show ap inventory *ap_name*

Syntax Description

ap_name	Inventory for the specified access point.

Command Default None.

Examples This example shows how to display the inventory of an access point:

```
> show ap inventory test101
NAME: "test101"    , DESCR: "Cisco Wireless Access Point"
PID: AIR-LAP1131AG-A-K9  ,  VID: V01,  SN: FTX1123T2XX
```

show ap join stats detailed

To display all join-related statistics collected for a specific access point, use the **show ap join stats detailed** command.

show ap join stats detailed *ap_mac*

Syntax Description

ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default None.

Examples This example shows how to display join information for a specific access point trying to join the controller:

```
> show ap join stats detailed 00:0b:85:02:0d:20
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23:335
- Time at last unsuccessful discovery attempt..... Not applicable
Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....RADIUS authorization is pending for
 the AP
- Time at last successful join attempt..... Aug 21 12:50:34:481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34:374
Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt... Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34:374
- Time at last unsuccessful configuration attempt..... Not applicable
Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable
Last AP disconnect details
- Reason for last AP connection failure..... Not applicable
Last join error summary
- Type of error that occurred last..... Lwapp join request rejected
- Reason for error that occurred last..... RADIUS authorization is pending for
 the AP
- Time at which the last join error occurred..... Aug 21 12:50:34:374
```

Related Commands

show ap join stats detailed

show ap join stats summary

show ap join stats summary all

show ap join stats summary

To display the last join error detail for a specific access point, use the **show ap join stats summary** command.

show ap join stats summary *ap_mac*

Syntax Description

ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default

None.

Usage Guidelines

To obtain the MAC address of the 802.11 radio interface, enter the **show interface** command on the access point.

Examples

This example shows how to display specific join information for an access point:

```
> show ap join stats summary 00:0b:85:02:0d:20
Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
rejected
Reason for error that occurred last..... RADIUS authorization
 is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

Related Commands

show ap join stats detailed

show ap join stats summary all

show ap join stats summary all

To display the MAC addresses of all the access points that are joined to the controller or that have tried to join, use the **show ap join stats summary all** command.

show ap join stats summary all

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display a summary of join information for all access points:

```
> show ap join stats summary all
Number of APs.......................................... 4
Base Mac             AP EthernetMac         AP Name          IP Address         Status
00:0b:85:57:bc:c0     00:0b:85:57:bc:c0     AP1130          10.10.163.217     Joined
00:1c:0f:81:db:80     00:1c:63:23:ac:a0     AP1140          10.10.163.216     Not joined
00:1c:0f:81:fc:20     00:1b:d5:9f:7d:b2     AP1              10.10.163.215     Joined
00:21:1b:ea:36:60     00:0c:d4:8a:6b:c1     AP2              10.10.163.214     Not joined
```

Related Commands

show ap join stats detailed

show ap join stats summary

show ap led-state

To view the LED state of all access points or a specific access point, use the **show ap led-state** command.

show ap led-state {**all** | *cisco_ap*}

Syntax Description

all	Shows the LED state for all access points.
cisco_ap	Name of the access point whose LED state is to be shown.

Command Default

Enabled.

Examples

This example shows how to get the LED state of all access points:

```
> show ap led-state all
Global LED State: Enabled (default)
```

Related Commands

config ap led-state

show ap led-flash

To display the LED flash status of an access point, use the **show ap led-flash** command.

show ap led-flash *cisco_ap*

Syntax Description

cisco_ap

Command Default None.

Examples This example shows how to

```
> show ap led-flash
```

Related Commands

config ap led-state flash

config ap led-state

show ap link-encryption

To display the MAC addresses of all the access points that are joined to the controller or that have tried to join, use the **show ap link-encryption** command.

show ap link-encryption {**all** | *cisco_ap*}

Syntax Description

all	Specifies all access points.
cisco_ap	Name of the lightweight access point.

Command Default None.

Examples This example shows how to display the link encryption status of all access points:

```
> show ap link-encryption all
             Encryption  Dnstream  Upstream    Last
AP Name           State     Count     Count  Update
------------------  ---  --------  --------  ------
1240                Dis      4406    237553   Never
1130                 En      2484    276308   19:31
```

Related Commands

config ap link-encryption

config ap link-latency

show ap monitor-mode summary

To display the current channel-optimized monitor mode settings, use the **show ap monitor-mode summary** command.

show ap monitor-mode summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display current channel-optimized monitor mode settings:

```
> show ap monitor-mode summary
AP Name            Ethernet MAC       Status     Scanning Channel List
---  ----------------  ---------- ----------------------
AP_004             xx:xx:xx:xx:xx:xx Tracking    1, 6, 11, 4
```

Related Commands

config ap mode

config ap monitor-mode

show ap packet-dump status

To display access point Packet Capture configurations, use the **show ap packet-dump status** command.

show ap packet-dump status

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as the beacon or probe response. Only packets that flow through the Radio driver in the Tx path are captured.

Examples

This example shows how to display the access point Packet Capture configurations:

```
> show ap packet-dump status
Packet Capture Status..................................... Stopped
FTP Server IP Address..................................... 0.0.0.0
FTP Server Path...........................................
FTP Server Username.......................................
FTP Server Password....................................... ********
Buffer Size for Capture................................... 2048 KB
Packet Capture Time....................................... 45 Minutes
Packet Truncate Length.................................... Unspecified
Packet Capture Classifier................................. None
```

Related Commands

config ap packet-dump

debug ap packet-dump

show ap retransmit

To display access point control packet retransmission parameters, use the**show ap retransmit** command.

show ap retransmit {**all** | *cisco_ap*}

Syntax Description

all	Specifies all access points.
cisco_ap	Name of the access point.

Command Default

None.

Examples

This example shows how to display the control packet retransmission parameters of all access points on a network:

```
> show ap retransmit all
Global control packet retransmit interval: 3 (default)
Global control packet retransmit count: 5 (default)
AP Name             Retransmit Interval  Retransmit count
------------------  -------------------  -------------------
AP_004                   3 (default)      5 (WLC default),5 (AP default)
```

Related Commands

config ap retransmit interval

show ap stats

To display the statistics for a Cisco lightweight access point, use the **show ap stats** command.

show ap stats {**802.11**{**a** | **b**} | **wlan** | **ethernet summary**} *cisco_ap* [**tsm** {*client_mac* | **all**}]

Syntax Description

802.11a	Specifies the 802.11a network
802.11b	Specifies the 802.11b/g network.
wlan	Specifies WLAN statistics.
ethernet	Specifies AP ethernet interface statistics.
summary	Displays ethernet interface summary of all the connected Cisco access points.
cisco_ap	Name of the lightweight access point.
tsm	(Optional) Specifies the traffic stream metrics.
client_mac	(Optional) MAC address of the client.
all	(Optional) Specifies all access points.

Command Default

None.

Examples

This example shows how to display statistics of an access point for the 802.11b network:

```
> show ap stats 802.11a Ibiza

Number Of Slots.................................. 2
AP Name.......................................... Ibiza
MAC Address...................................... 44:2b:03:9a:8a:73
Radio Type....................................... RADIO_TYPE_80211a
Stats Information
  Number of Users................................ 0
  TxFragmentCount................................ 84628
  MulticastTxFrameCnt............................ 84628
  FailedCount.................................... 0
  RetryCount..................................... 0
  MultipleRetryCount............................. 0
  FrameDuplicateCount............................ 0
  RtsSuccessCount................................ 1
  RtsFailureCount................................ 0
  AckFailureCount................................ 0
  RxIncompleteFragment........................... 0
  MulticastRxFrameCnt............................ 0
  FcsErrorCount.................................. 20348857
  TxFrameCount................................... 84628
  WepUndecryptableCount.......................... 19907
  TxFramesDropped................................ 0
Rate Limiting Stats:
```

```
  Wlan 1:
    Number of Data Packets Received.............. 592
    Number of Data Rx Packets Dropped............ 160
    Number of Data Bytes Received................ 160783
    Number of Data Rx Bytes Dropped.............. 0
    Number of Realtime Packets Received.......... 592
    Number of Realtime Rx Packets Dropped........ 0
    Number of Realtime Bytes Received............ 160783
    Number of Realtime Rx Bytes Dropped.......... 0
    Number of Data Packets Sent.................. 131
    Number of Data Tx Packets Dropped............ 0
    Number of Data Bytes Sent.................... 23436
    Number of Data Tx Bytes Dropped.............. 0
    Number of Realtime Packets Sent.............. 131
    Number of Realtime Tx Packets Dropped........ 0
    Number of Realtime Bytes Sent................ 23436
    Number of Realtime Tx Bytes Dropped.......... 0
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)......... 0
  Voice Roam Bandwidth in use(% of config bw).... 0
    Total channel MT free........................ 0
    Total voice MT free.......................... 0
    Na Direct.................................... 0
    Na Roam...................................... 0
  Video Bandwidth in use(% of config bw)......... 0
  Video Roam Bandwidth in use(% of config bw).... 0
  Total BW in use for Voice(%)................... 0
  Total BW in use for SIP Preferred call(%)...... 0
WMM TSPEC CAC Call Stats
  Total num of voice calls in progress........... 0
  Num of roaming voice calls in progress......... 0
  Total Num of voice calls since AP joined....... 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of exp bw requests received.......... 0
  Total Num of exp bw requests admitted.......... 0
  Num of voice calls rejected since AP joined.... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficent bw.... 0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate.......... 0
  Num of calls rejected due to QoS policy........ 0
SIP CAC Call Stats
  Total Num of calls in progress................. 0
  Num of roaming calls in progress............... 0
  Total Num of calls since AP joined............. 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of Preferred calls received.......... 0
  Total Num of Preferred calls accepted.......... 0
  Total Num of ongoing Preferred calls........... 0
  Total Num of calls rejected(Insuff BW)......... 0
  Total Num of roam calls rejected(Insuff BW).... 0
WMM Video TSPEC CAC Call Stats
  Total num of video calls in progress........... 0
  Num of roaming video calls in progress......... 0
  Total Num of video calls since AP joined....... 0
  Total Num of video roaming calls since AP j.... 0
  Num of video calls rejected since AP joined.... 0
  Num of video roam calls rejected since AP j.... 0
  Num of video calls rejected due to insuffic.... 0
  Num of video calls rejected due to invalid .... 0
  Num of video calls rejected due to PHY rate.... 0
  Num of video calls rejected due to QoS poli.... 0
SIP Video CAC Call Stats
  Total Num of video calls in progress........... 0
  Num of video roaming calls in progress......... 0
  Total Num of video calls since AP joined....... 0
  Total Num of video roaming calls since AP j.... 0
  Total Num of video calls rejected(Insuff BW.... 0
  Total Num of video roam calls rejected(Insu.... 0
Band Select Stats
  Num of dual band client ....................... 0
  Num of dual band client added.................. 0
  Num of dual band client expired ............... 0
```

```
Num of dual band client replaced..... 0
Num of dual band client detected ..... 0
Num of suppressed client ..... 0
Num of suppressed client expired..... 0
Num of suppressed client replaced..... 0
```

Related Commands **config ap static-ip**

config ap static-timer

show ap summary

To display a summary of all lightweight access points attached to the controller, use the **show ap summary** command.

show ap summary [*cisco_ap*]

Syntax Description

cisco_ap	(Optional) Type sequence of characters that make up the name of a specific AP or a group of APs, or enter a wild character search pattern.

Command Default

None.

Usage Guidelines

A list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the controller port number appears. When you specify

Examples

This example shows how to display a summary of all connected access points:

```
> show ap summary
Number of APs.................................... 2
Global AP username............................... user
Global AP Dot1x username......................... Not Configured
Number of APs.................................... 2
Global AP username............................... user
Global AP Dot1x username......................... Not Configured
AP Name   Slots  AP Model           Ethernet MAC       Location    Port Country  Priority
--------  -----  ----------------   -----------------  ----------  ---- -------  --------
wolverine 2      AIR-LAP1252AG-A-K9  00:1b:d5:13:39:74  Reception   1    US       3
ap:1120   1      AIR-LAP1121G-A-K9   00:1b:d5:a9:ad:08  Hall 235    1    US       1
```

Related Commands

config ap

show ap tcp-mss-adjust

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap tcp-mss-adjust** command.

show ap tcp-mss-adjust {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Specified lightweight access point name.
all	Specifies all access points.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Examples

This example shows how to display Transmission Control Protocol (TCP) maximum segment size (MSS) information of all access points:

```
> show ap tcp-mss-adjust all
AP Name            TCP State MSS Size
------------------ --------- -------
AP-1140            enabled   536
AP-1240            disabled  -
AP-1130            disabled  -
```

Related Commands

config ap tcp-adjust-mss

show ap wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap wlan** command.

show ap wlan 802.11{**a** | **b**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
ap_name	Lightweight access point name.

Command Default None.

Examples This example shows how to display BSSIDs of an access point for the 802.11b network:

```
> show ap wlan 802.11b AP01
Site Name..................................... MY_AP_GROUP1
Site Description.............................. MY_AP_GROUP1
WLAN ID          Interface          BSSID
-------         -----------        --------------------------
1               management           00:1c:0f:81:fc:20
2               dynamic              00:1c:0f:81:fc:21
```

Related Commands **config ap wlan**

Show Redundancy Commands

Use the **show redundancy** commands to display redundancy information of the active and standby controllers.

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.

Examples This example shows how to display the redundancy summary information of the 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

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
```

Related Commands

show redundancy interfaces

show redundancy summary

show redundancy peer-route

show redundancy statistics

show redundancy timers

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

debug rmgr

debug rsyncmgr

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.

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

```
> 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
```

Related Commands

show redundancy interfaces

show redundancy summary

show redundancy peer-route

show redundancy statistics

show redundancy timers

show redundancy mobilitymac

config redundancy interface address peer-service-port

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.

Examples This example shows how to display the redundancy and service port IP addresses information:

```
> 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
```

Related Commands

show redundancy latency

show redundancy summary

show redundancy peer-route

show redundancy statistics

show redundancy timers

show redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

show redundancy mobilitymac

To display the HA mobility MAC address 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.

Examples This example shows how to display the HA mobility MAC address used to communicate with the peer:

```
> show redundancy mobilitymac
          ff:ff:ff:ff:ff:ff
```

Related Commands

config redundancy mobilitymac

show redundancy latency

show redundancy summary

show redundancy peer-route

show redundancy statistics

show redundancy timers

debug rfac

debug rmgr

debug rsyncmgr

show redundancy peer-route summary

To display the routes assigned to the standby controller, 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.

Examples This example shows how to display all the configured routes of the standby 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
```

Related Commands

show redundancy latency

show redundancy summary

show redundancy peer-route

show redundancy statistics

show redundancy timers

show redundancy mobilitymac

config redundancy peer-route

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.

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.

Examples This example shows how to display the statistics information of the Redundancy Manager:

```
> 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
```

Related Commands

show redundancy latency

show redundancy summary

show redundancy peer-route

show redundancy timers

show redundancy mobilitymac

config redundancy timer peer-search-timer

config redundancy timer keep-alive-timer

debug rfac

debug rmgr

debug rsyncmgr

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.

Examples This example shows how to display the details of the Redundancy Manager timers:

```
> show redundancy timers
          Keep Alive Timer         : 100 msecs
          Peer Search Timer        : 120 secs
```

Related Commands

show redundancy latency

show redundancy summary

show redundancy peer-route

show redundancy statistics

config redundancy timer peer-search-timer

config redundancy timer keep-alive-timer

debug rfac

debug rmgr

debug rsyncmgr

Other Show Commands

This section lists the other **show** commands to display information about your configuration settings for access points.

show advanced backup-controller

To display a list of primary and secondary backup controllers, use the **show advanced backup-controller** command.

show advanced backup-controller

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the backup controller information:

```
> show advanced backup-controller
AP primary Backup Controller ..................  controller 10.10.10.10
AP secondary Backup Controller ................  0.0.0.0
```

Related Commands

config advanced backup-controller primary

config advanced backup-controller secondary

show advanced max-1x-sessions

To display the maximum number of simultaneous 802.1X sessions allowed per access point, use the **show advanced max-1x-sessions** command.

show advanced max-1x-sessions

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the maximum 802.1X sessions per access point:

```
> show advanced max-1x-sessions
Max 802.1x session per AP at a given time........ 0
```

Related Commands

show advanced statistics

show advanced probe

To display the number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds, use the **show advanced probe** command.

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the probe settings for the WLAN controller:

```
> show advanced probe
Probe request filtering............................. Enabled
Probes fwd to controller per client per radio.... 12
Probe request rate-limiting interval.............. 100 msec
```

Related Commands

config advanced probe filter

config advanced probe limit

show advanced rate

To display whether control path rate limiting is enabled or disabled, use the **show advanced rate** command.

show advanced rate

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the switch control path rate limiting mode:

```
> show advanced rate
Control Path Rate Limiting.....................  Disabled
```

Related Commands

config advanced rate

config advanced eap

show advanced timers

To display the mobility anchor, authentication response, and rogue access point entry timers, use the **show advanced timers** command.

show advanced timers

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are shown in the “Examples” section.

Examples

This example shows how to display the system timers setting:

```
> show advanced timers
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds)..................... 1200
AP Heart Beat Timeout (seconds)................... 30
AP Discovery Timeout (seconds).................... 10
AP Local mode Fast Heartbeat (seconds)........... disable
AP flexconnect mode Fast Heartbeat (seconds)........... disable
AP Primary Discovery Timeout (seconds)........... 120
```

Related Commands

config advanced timers ap-discovery-timeout

config advanced timers ap-fast-heartbeat

config advanced timers ap-heartbeat-timeout

config advanced timers ap-primary-discovery-timeout

config advanced timers auth-timeout

config advanced timers eap-identity-request-delay

config advanced timers eap-timeout

show client ap

To display the clients on a Cisco lightweight access point, use the **show client ap** command.

show client ap 802.11{**a** | **b**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Usage Guidelines

The **show client ap** command may list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the exclusion list (blacklisted).

Examples

This example shows how to display client information on an access point:

```
> show client ap 802.11b AP1
MAC Address        AP Id   Status         WLAN Id    Authenticated
-----------------  ------  -------------  ---------  -------------
xx:xx:xx:xx:xx:xx      1   Associated     1          No
```

Related Commands

show client detail

show client summary

show client username

show country

show exclusionlist

show auth-list

To display the access point authorization list, use the **show auth-list** command.

show auth-list

Syntax Description

This command has no arguments or keywords.

Examples

This example shows how to display the access point authorization list:

```
> show auth-list
Authorize APs against AAA..................... disabled
Allow APs with Self-signed Certificate (SSC)... disabled
Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------
xx:xx:xx:xx:xx:xx         MIC
```

Related Commands

clear tacacs auth statistics

clear stats local-auth

config auth-list add

config auth-list ap-policy

config auth-list delete

show boot

To display the primary and backup software build numbers with an indication of which is active, use the **show boot** command.

show boot

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

Each Cisco wireless LAN controller retains one primary and one backup operating system software load in nonvolatile RAM to allow controllers to boot off the primary load (default) or revert to the backup load when desired.

Examples

This example shows how to display the default boot image information:

```
> show boot
Primary Boot Image.............................. 3.2.13.0 (active)
Backup Boot Image.............................. 3.2.15.0
```

Related Commands

config boot

show call-control ap

Note The **show call-control ap** command is applicable only for SIP based calls.

To see the metrics for successful calls or the traps generated for failed calls, use the **show call-control ap** command.

show call-control ap {**802.11a** | **802.11b**} *cisco_ap* {**metrics** | **traps**}

Syntax Description

802.11a	Specifies the 802.11a network
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco access point name.
metrics	Specifies the call metrics information.
traps	Specifies the trap information for call control.

Command Default

None.

Examples

This example shows how to display the metrics for successful calls generated for an access point:

```
> show call-control ap 802.11a Cisco_AP metrics
Total Call Duration in Seconds..................... 120
Number of Calls.................................... 10
Number of calls for given client is................ 1
```

This example shows how to display the metrics for the traps generated for an access point:

```
> show call-control ap 802.11a Cisco_AP traps
Number of traps sent in one min.................... 2
Last SIP error code................................ 404
Last sent trap timestamp..................... Jun 20 10:05:06
```

Usage Guidelines

To aid in troubleshooting, the output of this command shows an error code for any failed calls. The following table explains the possible error codes for failed calls.

Table 1: Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.

Error Code	Integer	Description
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptable	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header field sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header field.
480	temporarilyNotAvailable	The callee’s end system was contacted successfully, but the callee is currently unavailable.

Error Code	Integer	Description
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header field with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

show country

To display the configured country and the radio types supported, use the **show country** command.

show country

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the configured countries and supported radio types:

```
> show country
Configured Country..............................  United States
Configured Country Codes
US  - United States.............................  802.11a / 802.11b / 802.11g
```

Related Commands

config country

show country channels

show country supported

show country channels

To display the radio channels supported in the configured country, use the **show country channels** command.

show country channels

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the auto-RF channels for the configured countries:

```
> show country channels
Configured Country..............................  United States
      KEY: * = Channel is legal in this country and may be configured manually.
Configured Country..............................  United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG :
Channels :                   1 1 1 1 1
         : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
     US  : A * * * * A * * * * A . . .
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A :  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
         : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
     US  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
---------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Related Commands

config country

show country

show country supported

show country supported

To display a list of the supported country options, use the **show country supported** command.

show country supported

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display a list of all the supported countries:

```
> show country supported
Configured Country..................................... United States
Supported Country Codes
AR  - Argentina................................... 802.11a / 802.11b / 802.11g
AT  - Austria..................................... 802.11a / 802.11b / 802.11g
AU  - Australia................................... 802.11a / 802.11b / 802.11g
BR  - Brazil...................................... 802.11a / 802.11b / 802.11g
BE  - Belgium..................................... 802.11a / 802.11b / 802.11g
BG  - Bulgaria.................................... 802.11a / 802.11b / 802.11g
CA  - Canada...................................... 802.11a / 802.11b / 802.11g
CH  - Switzerland................................. 802.11a / 802.11b / 802.11g
CL  - Chile.......................................           802.11b / 802.11g
CN  - China....................................... 802.11a / 802.11b / 802.11g
CO  - Colombia....................................           802.11b / 802.11g
CY  - Cyprus...................................... 802.11a / 802.11b / 802.11g
CZ  - Czech Republic.............................. 802.11a / 802.11b
DE  - Germany..................................... 802.11a / 802.11b / 802.11g
DK  - Denmark..................................... 802.11a / 802.11b / 802.11g
EE  - Estonia..................................... 802.11a / 802.11b / 802.11g
ES  - Spain....................................... 802.11a / 802.11b / 802.11g
FI  - Finland..................................... 802.11a / 802.11b / 802.11g
FR  - France...................................... 802.11a / 802.11b / 802.11g
GB  - United Kingdom.............................. 802.11a / 802.11b / 802.11g
GI  - Gibraltar................................... 802.11a / 802.11b / 802.11g
GR  - Greece...................................... 802.11a / 802.11b / 802.11g
HK  - Hong Kong................................... 802.11a / 802.11b / 802.11g
HU  - Hungary..................................... 802.11a / 802.11b / 802.11g
ID  - Indonesia...................................           802.11b / 802.11g
IE  - Ireland..................................... 802.11a / 802.11b / 802.11g
IN  - India....................................... 802.11a / 802.11b / 802.11g
IL  - Israel...................................... 802.11a / 802.11b / 802.11g
ILO - Israel (outdoor)............................           802.11b / 802.11g
IS  - Iceland..................................... 802.11a / 802.11b / 802.11g
IT  - Italy....................................... 802.11a / 802.11b / 802.11g
JP  - Japan (J)................................... 802.11a / 802.11b / 802.11g
J2  - Japan 2(P).................................. 802.11a / 802.11b / 802.11g
J3  - Japan 3(U).................................. 802.11a / 802.11b / 802.11g
KR  - Korea Republic (C).......................... 802.11a / 802.11b / 802.11g
KE  - Korea Extended (K).......................... 802.11a / 802.11b / 802.11g
LI  - Liechtenstein............................... 802.11a / 802.11b / 802.11g
LT  - Lithuania................................... 802.11a / 802.11b / 802.11g
LU  - Luxembourg.................................. 802.11a / 802.11b / 802.11g
LV  - Latvia...................................... 802.11a / 802.11b / 802.11g
MC  - Monaco...................................... 802.11a / 802.11b / 802.11g
MT  - Malta....................................... 802.11a / 802.11b / 802.11g
MX  - Mexico...................................... 802.11a / 802.11b / 802.11g
MY  - Malaysia.................................... 802.11a / 802.11b / 802.11g
NL  - Netherlands................................. 802.11a / 802.11b / 802.11g
NZ  - New Zealand................................. 802.11a / 802.11b / 802.11g
```

```
NO  - Norway..................................... 802.11a / 802.11b / 802.11g
PA  - Panama.....................................           802.11b / 802.11g
PE  - Peru.......................................           802.11b / 802.11g
PH  - Philippines................................ 802.11a / 802.11b / 802.11g
PL  - Poland..................................... 802.11a / 802.11b / 802.11g
PT  - Portugal................................... 802.11a / 802.11b / 802.11g
RU  - Russian Federation......................... 802.11a / 802.11b / 802.11g
RO  - Romania.................................... 802.11a / 802.11b / 802.11g
SA  - Saudi Arabia............................... 802.11a / 802.11b / 802.11g
SE  - Sweden..................................... 802.11a / 802.11b / 802.11g
SG  - Singapore.................................. 802.11a / 802.11b / 802.11g
SI  - Slovenia................................... 802.11a / 802.11b / 802.11g
SK  - Slovak Republic............................ 802.11a / 802.11b / 802.11g
TH  - Thailand...................................           802.11b / 802.11g
TR  - Turkey.....................................           802.11b / 802.11g
TW  - Taiwan..................................... 802.11a / 802.11b / 802.11g
UA  - Ukraine.................................... 802.11a / 802.11b / 802.11g
US  - United States.............................. 802.11a / 802.11b / 802.11g
USL - United States (Legacy)..................... 802.11a / 802.11b / 802.11g
USX - United States (US + chan165)............... 802.11a / 802.11b / 802.11g
VE  - Venezuela..................................           802.11b / 802.11g
ZA  - South Africa............................... 802.11a / 802.11b / 802.11g
```

Related Commands

config country

show country channels

show country

show dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show dtls connections** command.

show dtls connections

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the established DTLS connections:

```
> show dtls connections
AP Name          Local Port    Peer IP          Peer Port     Ciphersuite
---------------- ------------- ---------------- ------------- ----------------------
1130             Capwap_Ctrl   1.100.163.210    23678         TLS_RSA _WITH_AES_128_CBC_SHA
1130             Capwap_Data   1.100.163.210    23678         TLS_RSA _WITH_AES_128_CBC_SHA
1240             Capwap_Ctrl   1.100.163.209    59674         TLS_RSA _WITH_AES_128_CBC_SHA
```

show known ap

To display known Cisco lightweight access point information, use the **show known ap** command.

show known ap {**summary** | **detailed** *MAC*}

Syntax Description

summary	Displays a list of all known access points.
detailed	Provides detailed information for all known access points.
MAC	MAC address of the known AP.

Command Default

None.

Examples

This example shows how to display a summary of all known access points:

```
> show known ap summary
MAC Address         State        # APs  # Clients   Last Heard
-----------         -----------  -----   --------   -----------------
```

Related Commands

config ap

show ipv6 ra-guard

To display the RA guard statistics, use the **show ipv6 ra-guard** command.

show ipv6 ra-guard {**ap** | **wlc**} **summary**

Syntax Description

ap	Displays Cisco access point details.
wlc	Displays Cisco controller details.
summary	Displays RA guard statistics.

Command Default

None.

Examples

This example shows how to display the RA guard statistics for an access point:

```
> show ipv6 ra-guard ap summary
IPv6 RA Guard on AP..................... Enabled
RA Dropped per client:
MAC Address       AP Name           WLAN/GLAN      Number of RA Dropped
----------------- ----------------- -------------- ---------------------
00:40:96:b9:4b:89 Bhavik_1130_1_p13 2              19
----------------- ----------------- -------------- ---------------------
Total RA Dropped on AP.....................      19
```

This example shows how to display the RA guard statistics for a controller:

```
> show ipv6 ra-guard wlc summary
IPv6 RA Guard on WLC..................... Enabled
```

Related Commands

config ipv6 ra-guard

show msglog

To display the message logs written to the Cisco wireless LAN controller database, use the **show msglog** command.

show msglog

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

If there are more that 15 entries, you are prompted to display the messages shown in the example.

Examples

This example shows how to display message logs:

```
> show msglog
Message Log Severity Level..................... ERROR
Thu Aug  4 14:30:08 2005  [ERROR] spam_lrad.c 1540: AP 00:0b:85:18:b6:50 associated. Last
AP failure was due to Link Failure
Thu Aug  4 14:30:08 2005  [ERROR] spam_lrad.c 13840: Updating IP info for AP 00:
0b:85:18:b6:50 -- static 0, 1.100.49.240/255.255.255.0, gtw 1.100.49.1
Thu Aug  4 14:29:32 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Thu Aug  4 14:29:32 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a switch group
reset
Thu Aug  4 14:29:32 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Thu Aug  4 14:29:22 2005  [ERROR] sim.c 2841: Unable to get link state for primary port 0
of interface ap-manager
Thu Aug  4 14:29:22 2005  [ERROR] dtl_l2_dot1q.c 767: Unable to get USP
Thu Aug  4 14:29:22 2005  Previous message occurred 2 times
Thu Aug  4 14:29:14 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake called with
NULL pointer: osapi_bsntime.c:927
Thu Aug  4 14:29:14 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake called with
NULL pointer: osapi_bsntime.c:919
Thu Aug  4 14:29:14 2005  [CRITICAL] hwutils.c 1861: Security Module not found
Thu Aug  4 14:29:13 2005  [CRITICAL] bootos.c 791: Starting code...
```

show network summary

To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command.

show network summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display a summary configuration:

```
> show network summary
RF-Network Name............................. RF
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL.........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
AP Multicast/Broadcast Mode................. Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Disabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
AP Join Priority............................ Disable
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Disable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disable
Web Auth Secure Web  ....................... Enable
Fast SSID Change ........................... Disabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
CCX-lite status ............................ Disable
oeap-600 dual-rlan-ports ................... Disable
oeap-600 local-network ..................... Enable
mDNS snooping............................... Disabled
```

```
mDNS Query Interval..................... 15 minutes
```

Related Commands

config network

show network multicast mgid summary

show network multicast mgid detail

show network

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.

Examples

This example shows how to display the client watchlist information:

```
> show watchlist
client watchlist state is disabled
```

Related Commands

config watchlist add

config watchlist delete

config watchlist disable

config watchlist enable

CAPWAP Access Point Commands

Use the **capwap ap** commands to configure CAPWAP access point settings.

capwap ap controller ip address

To configure the controller IP address into the CAPWAP access point from the access point's console port, use the **capwap ap controller ip address** command.

capwap ap controller ip address *controller_ip_address*

Syntax Description

controller_ip_address	IP address of the controller.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the controller IP address 10.23.90.81 into the CAPWAP access point:

```
> capwap ap controller ip address 10.23.90.81
```

Related Commands

capwap ap dot1x
capwap ap hostname
capwap ap ip address
capwap ap ip default-gateway
capwap ap log-server
capwap ap primary-base
capwap ap primed-timer
capwap ap secondary-base
capwap ap tertiary-base

capwap ap dot1x

To configure the dot1x username and password into the CAPWAP access point from the access point's console port, use the **capwap ap dot1x** command.

capwap ap dot1x username *user_name* **password** *password*

Syntax Description

user_name	Dot1x username.
password	Dot1x password.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the dot1x username ABC and password pass01:

```
> capwap ap dot1x username ABC password pass01
```

Related Commands

capwap ap controller ip address

capwap ap hostname

capwap ap ip address

capwap ap ip default-gateway

capwap ap log-server

capwap ap primary-base

capwap ap primed-timer

capwap ap secondary-base

capwap ap tertiary-base

capwap ap hostname

To configure the access point host name from the access point's console port, use the **capwap ap hostname** command.

capwap ap hostname *host_name*

Syntax Description

host_name	Hostname of the access point.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases. This command is available only for Lightweight AP IOS Software recovery image (rcvk9w8) without any private-config. You can remove the private-config by using the **clear capwap private-config** command.

Examples

This example shows how to configure the hostname WLC into the capwap access point:

```
> capwap ap hostname WLC
```

Related Commands

capwap ap controller ip address

capwap ap dot1x

capwap ap ip address

capwap ap ip default-gateway

capwap ap log-server

capwap ap primary-base

capwap ap primed-timer

capwap ap secondary-base

capwap ap tertiary-base

capwap ap ip address

To configure the IP address into the CAPWAP access point from the access point's console port, use the **capwap ap ip address** command.

capwap ap ip address *ip_address*

Syntax Description

ip_address	IP address.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the IP address 10.0.0.0.1 into capwap access point:

```
> capwap ap ip address 10.0.0.0.1
```

Related Commands

capwap ap controller ip address

capwap ap dot1x

capwap ap hostname

capwap ap ip default-gateway

capwap ap log-server

capwap ap ip address

capwap ap primary-base

capwap ap secondary-base

capwap ap tertiary-base

capwap ap ip default-gateway

To configure the default gateway from the access point's console port, use the **capwap ap ip default-gateway** command.

capwap ap ip default-gateway *default_gateway*

Syntax Description

default_gateway	Default gateway address of the capwap access point.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the capwap access point with the default gateway address 10.0.0.1:

```
> capwap ap ip default-gateway 10.0.0.1
```

Related Commands

capwap ap controller ip address
capwap ap dot1x
capwap ap hostname
capwap ap ip address
capwap ap log-server
capwap ap primary-base
capwap ap primary-base
capwap ap secondary-base
capwap ap tertiary-base

capwap ap log-server

To configure the system log server to log all the capwap errors, use the **capwap ap log-server** command.

capwap ap log-server *ip_address*

Syntax Description

ip_address	IP address of the syslog server.

Command Default None.

Usage Guidelines This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples This example shows how to configure the syslog server with the IP address 10.0.0.1:

```
> capwap ap log-server 10.0.0.1
```

Related Commands

capwap ap controller ip address
capwap ap dot1x
capwap ap ip address
capwap ap hostname
capwap ap ip default-gateway
capwap ap log-server
capwap ap primary-base
capwap ap primary-base
capwap ap secondary-base
capwap ap tertiary-base

capwap ap primary-base

To configure the primary controller name and IP address into the capwap access point from the access point's console port, use the **capwap ap primary-base** command.

capwap ap primary-base *controller_name controller_ip_address*

Syntax Description

controller_name	Name of the primary controller.
controller_ip_address	IP address of the primary controller.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the primary controller name WLC1 and primary controller IP address 10.92.109.1 into the capwap access point:

```
> capwap ap primary-base WLC1 10.92.109.1
```

Related Commands

capwap ap controller ip address

capwap ap dot1x

capwap ap ip address

capwap ap hostname

capwap ap ip default-gateway

capwap ap log-server

capwap ap secondary-base

capwap ap tertiary-base

capwap ap primed-timer

To configure the primed timer into the CAPWAP access point, use the **capwap ap primed-timer** command.

capwap ap primed-timer {**enable** | **disable**}

Syntax Description

enable	Enables the primed timer settings
disable	Disables the primed timer settings.

Command Default None.

Usage Guidelines This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples This example shows how to enable the primed-timer settings:

> **capwap ap primed-timer enable**

Related Commands

capwap ap controller ip address
capwap ap dot1x
capwap ap hostname
capwap ap ip default-gateway
capwap ap log-server
capwap ap ip address
capwap ap primary-base
capwap ap secondary-base
capwap ap tertiary-base

capwap ap secondary-base

To configure the secondary controller name and IP address into the CAPWAP access point from the access point's console port, use the **capwap ap secondary-base** command.

capwap ap secondary-base *controller_name controller_ip_address*

Syntax Description

controller_name	Name of the secondary controller.
controller_ip_address	IP address of the secondary controller.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the secondary controller name WLC2 and secondary controller IP address 10.92.108.2 into the CAPWAP access point:

```
> capwap ap secondary-base WLC2 10.92.108.2
```

Related Commands

capwap ap controller ip address

capwap ap dot1x

capwap ap ip address

capwap ap hostname

capwap ap ip default-gateway

capwap ap log-server

capwap ap primary-base

capwap ap tertiary-base

capwap ap tertiary-base

To configure the tertiary controller name and IP address into the capwap access point from the access point's console port, use the **capwap ap tertiary-base** command.

capwap ap tertiary-base *controller_name controller_ip_address*

Syntax Description

controller_name	Name of the tertiary controller.
controller_ip_address	IP address of the tertiary controller.

Command Default

None.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to configure the tertiary controller name WLC3 and secondary controller IP address 10.80.72.2 into the capwap access point:

```
> capwap ap tertiary-base WLC3 10.80.72.2
```

Related Commands

capwap ap controller ip address

capwap ap dot1x

capwap ap ip address

capwap ap hostname

capwap ap ip default-gateway

capwap ap log-server

capwap ap primary-base

capwap ap secondary-base

lwapp ap controller ip address

To configure the controller IP address into the FlexConnect access point from the access point's console port, use the **lwapp ap controller ip address** command.

lwapp ap controller ip address *ip_address*

Syntax Description

ip_address	IP address of the controller.

Command Default None.

Usage Guidelines This command must be entered from an access point's console port.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples This example shows how to configure the controller IP address 10.92.109.1 into the FlexConnect access point:

```
> lwapp ap controller ip address 10.92.109.1
```

Related Commands

clear lwapp private-config

debug lwapp console cli

Config Commands

This section lists the **config** commands to configure access points.

config 802.11-a antenna extAntGain

To configure the external antenna gain for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a antenna extAntGain** commands.

config {**802.11-a49** | **802.11-a58**} **antenna extAntGain** *ant_gain cisco_ap* {**global** | *channel_no*}

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
ant_gain	Value in .5-dBi units (for instance, 2.5 dBi = 5).
cisco_ap	Name of the access point to which the command applies.
global	Specifies the antenna gain value to all channels.
channel_no	Antenna gain value for a specific channel.

Command Default

Disabled.

Usage Guidelines

Before you enter the **config 802.11-a antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11-a disable** command.

After you configure the external antenna gain, use the **config 802.11-a enable** command to re-enable the 802.11 Cisco radio.

Examples

This example shows how to configure an *802.11-a49* external antenna gain of *10 dBi* for *AP1*:

```
> config 802.11-a antenna extAntGain 10 AP1
```

Related Commands

config 802.11-a

config 802.11-a channel ap

config 802.11-a txpower ap

show 802.11a

config 802.11-a channel ap

To configure the channel properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a channel ap** command.

config {**802.11-a49** | **802.11-a58**} **channel ap** *cisco_ap* {**global** | *channel_no*}

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
cisco_ap	Name of the access point to which the command applies.
global	Enables the Dynamic Channel Assignment (DCA) on all 4.9-GHz and 5.8-GHz subband radios.
channel_no	Custom channel for a specific mesh access point. The range is 1 through 26, inclusive, for a 4.9-GHz band and 149 through 165, inclusive, for a 5.8-GHz band.

Command Default

Disabled.

Examples

This example shows how to set the channel properties:

```
> config 802.11-a channel ap
```

Related Commands

config 802.11-a

config 802.11-a antenna extAntGain

config 802.11-a txpower ap

config 802.11-a txpower ap

To configure the transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a txpower ap** command.

config {**802.11-a49** | **802.11-a58**} **txpower ap** *cisco_ap* {**global** | *power_level*}

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
txpower	Configures transmission power properties.
ap	Configures access point channel settings.
cisco_ap	Name of the access point to which the command applies.
global	Applies the transmission power value to all channels.
power_level	Transmission power value to the designated mesh access point. Valid values are 1 through 5, inclusive.

Command Default

Disabled.

Examples

This example shows how to configure an *802.11-a49* transmission power level of *4* for *AP1*:

```
> config 802.11-a txpower ap 4 AP1
```

Related Commands

config 802.11-a

config 802.11 channel ap

config 802.11 antenna extAntGain

config 802.11 antenna diversity

To configure the diversity option for 802.11 antennas, use the **config 802.11 antenna diversity** command.

config 802.11{**a** | **b**} **antenna diversity** {**enable** | **sideA** | **sideB**} *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the diversity.
sideA	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Examples

This example shows how to enable antenna diversity for AP01 on an 802.11b network:

```
> config 802.11a antenna diversity enable AP01
```

This example shows how to enable diversity for AP01 on an 802.11a network, using an external antenna connected to the Cisco lightweight access point left port (sideA):

```
> config 802.11a antenna diversity sideA AP01
```

Related Commands

config 802.11 disable

config 802.11 enable

config 802.11 antenna extAntGain

config 802.11 antenna mode

config 802.11 antenna selection

show 802.11a

show 802.11b

config 802.11 antenna extAntGain

To configure external antenna gain for an 802.11 network, use the **config 802.11 antenna extAntGain** command.

config 802.11 {**a** | **b**} **antenna extAntGain** *antenna_gain cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
antenna_gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Usage Guidelines

Before you enter the **config 802.11 antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the external antenna gain, use the **config 802.11 enable** command to enable the 802.11 Cisco radio.

Examples

This example shows how to configure an *802.11a* external antenna gain of *0.5 dBm* for *AP1*:

```
> config 802.11 antenna extAntGain 1 AP1
```

Related Commands

config 802.11 disable

config 802.11 enable

config 802.11 antenna mode

config 802.11 antenna selection

show 802.11a

show 802.11b

config 802.11 antenna mode

To configure the Cisco lightweight access point to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern, use the **config 802.11 antenna mode** command.

config 802.11 {**a** | **b**} **antenna mode** {**omni** | **sectorA** | **sectorB**} *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
omni	Specifies to use both internal antennas.
sectorA	Specifies to use only the side A internal antenna.
sectorB	Specifies to use only the side B internal antenna.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Examples

This example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

```
> config 802.11 antenna mode omni AP01
```

Related Commands

config 802.11 disable

config 802.11 enable

config 802.11 antenna extAntGain

config 802.11 antenna diversity

config 802.11 antenna selection

show 802.11a

show 802.11b

config 802.11 antenna selection

To select the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network, use the **config 802.11 antenna selection** command.

config 802.11 {**a** | **b**} **antenna selection** {**internal** | **external**} *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
internal	Specifies the internal antenna.
external	Specifies the external antenna.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Examples

This example shows how to configure access point AP02 on an 802.11b network to use the internal antenna:

```
> config 802.11a antenna selection internal AP02
```

Related Commands

config 802.11 disable

config 802.11 enable

config 802.11 antenna extAntGain

config 802.11 antenna mode

config 802.11 antenna diversity

show 802.11a

show 802.11b

config 802.11 disable

To disable radio transmission for an entire 802.11 network or for an individual Cisco radio, use the **config 802.11 disable** command.

config 802.11{**a** | **b**} **disable** {**network** | *cisco_ap*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
network	Disables transmission for the entire 802.11a network.
cisco_ap	Individual Cisco lightweight access point radio.

Command Default

The transmission is enabled for the entire network by default.

Usage Guidelines

Note You must use this command to disable the network before using many config 802.11 commands.

This command can be used any time that the CLI interface is active.

Examples

This example shows how to disable the entire 802.11a network:

```
> config 802.11a disable network
```

This example shows how to disable access point AP01 802.11b transmissions:

```
> config 802.11b disable AP01
```

Related Commands

show sysinfo

show 802.11a

config 802.11a enable

config 802.11b disable

config 802.11b enable

config 802.11a beaconperiod

config advanced backup-controller primary

To configure a primary backup controller for a specific controller, use the **config advanced backup-controller primary** command.

config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

Syntax Description

backup_controller_name	Name of the backup controller.
backup_controller_ip_address	IP address of the backup controller.

Command Default

None.

Usage Guidelines

To delete a primary backup controller entry, enter 0.0.0.0 for the controller IP address.

Examples

This example shows how to configure the primary backup controller:

```
> config advanced backup-controller primary Controller_1 10.10.10.10
```

Related Commands

show advanced backup-controller

config advanced backup-controller secondary

To configure a secondary backup controller for a specific controller, use the **config advanced backup-controller secondary** command.

config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

Syntax Description

backup_controller_name	Name of the backup controller.
backup_controller_ip_address	IP address of the backup controller.

Command Default

None.

Usage Guidelines

To delete a secondary backup controller entry, enter 0.0.0.0 for the controller IP address.

Examples

This example shows how to configure a secondary backup controller:

```
> config advanced backup-controller secondary Controller_1 10.10.10.10
```

Related Commands

show advanced backup-controller

config advanced client-handoff

To set the client handoff to occur after a selected number of 802.11 data packet excessive retries, use the **config advanced client-handoff** command.

config advanced client-handoff *num_of_retries*

Syntax Description

num_of_retries	Number of excessive retries before client handoff (from 0 to 255).

Command Default

0 excessive retries (disabled).

Usage Guidelines

This command is supported only for the1000/1510 series access points.

Examples

This example shows how to set the client handoff to 100 excessive retries:

```
> config advanced client-handoff 100
```

Related Commands

show advanced client-handoff

config advanced dot11-padding

To enable or disable over-the-air frame padding, use the **config advanced dot11-padding** command.

config advanced dot11-padding {**enable** | **disable**}

Syntax Description

enable	Enables this command.
disable	Disables this command.

Command Default

Disabled.

Examples

This example shows how to enable over-the-air frame padding:

```
> config advanced dot11-padding enable
```

Related Commands

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

config advanced assoc-limit

To configure the rate at which access point radios send association and authentication requests to the controller, use the **config advanced assoc-limit** command.

config advanced assoc-limit {**enable** [*number of associations per interval* | *interval*] | **disable**}

Syntax Description

enable	Enable this feature.
disable	Disables this feature.
number of associations per interval	(Optional) Number of association request per access point slot in a given interval. The range is from 1 to 100.
interval	(Optional) Association request limit interval. The range is from 100 to 10000 milliseconds.

Command Default

Disabled.

Usage Guidelines

When 200 or more wireless clients try to associate to a controller at the same time, the clients no longer become stuck in the DHCP_REQD state when you use the **config advanced assoc-limit** command to limit association requests from access points.

Examples

This example shows how to configure the number of association requests per access point slot in a given interval of 20 with the association request limit interval of 250:

```
> config advanced assoc-limit enable 20 250
```

config advanced max-1x-sessions

To configure the maximum number of simultaneous 802.1X sessions allowed per access point, use the **config advanced max-1x-sessions** command.

config advanced max-1x-sessions *no_of_sessions*

Syntax Description

no_of_sessions	Number of maximum 802.1x session initiation per AP at a time. The range is from 0 to 255, where 0 indicates unlimited.

Command Default

None.

Examples

This example shows how to configure the maximum number of simultaneous 802.1X sessions:

```
> config advanced max-1x-sessions 200
```

config advanced rate

To enable or disable switch control path rate limiting, use the **config advanced rate** command.

config advanced rate {**enable** | **disable**}

Syntax Description

enable	Enables the switch control path rate limiting feature.
disable	Disables the switch control path rate limiting feature.

Command Default

None.

Examples

This example shows how to enable switch control path rate limiting:

```
> config advanced rate enable
```

config advanced probe filter

To enable or disable the filtering of probe requests forwarded from an access point to the controller, use the **config advanced probe filter** command.

config advanced probe filter {**enable** | **disable**}

Syntax Description

enable	Enables the filtering of probe requests.
disable	Disables the filtering of probe requests.

Command Default

None.

Examples

This example shows how to enable the filtering of probe requests forwarded from an access point to the controller:

```
> config advanced probe filter enable
```

Related Commands

config advanced probe limit

config radius acct ipsec authentication

show advanced probe

show radius acct statistics

config advanced probe limit

To limit the number of probes sent to the WLAN controller per access point per client in a given interval, use the **config advanced probe limit** command.

config advanced probe limit *num_probes interval*

Syntax Description

num_probes	Number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
interval	Probe limit interval (from 100 to 10000 milliseconds).

Command Default

The default number of probe requests is 2. The default interval is 500 milliseconds.

Examples

This example shows how to set the number of probes per access point per client to 5 and the probe interval to 800 milliseconds:

```
> config advanced probe limit 5 800
```

Related Commands

config radius acct ipsec authentication

show advanced probe

show radius acct statistics

config certificate lsc

To configure Locally Significant Certificate (LSC) certificates, use the **config certificate lsc** commands.

config certificate lsc {**enable** | **disable** | **ca-server** *http://url:port/path* | **ca-cert** {**add** | **delete**} | **subject-params** *country state city orgn dept email* | **other-params** *keysize*} | **ap-provision** {**auth-list** {**add** | **delete**} *ap_mac* | **revert-cert** *retries*}

Syntax Description

enable	Enables LSC certificates on the controller.
disable	Disables LSC certificates on the controller.
ca-server	Specifies the Certificate Authority (CA) server settings.
http://url:port/path	Domain name or IP address of the CA server.
ca-cert	Specifies CA certificate database settings.
add	Obtains a CA certificate from the CA server and adds it to the controller's certificate database.
delete	Deletes a CA certificate from the controller's certificate database.
subject-params	Specifies the device certificate settings.
country state city orgn dept email	Country, state, city, organization, department, and email of the certificate authority. **Note** The common name (CN) is generated automatically on the access point using the current MIC/SSC format *Cxxxx-MacAddr*, where *xxxx* is the product number.
other-params	Specifies the device certificate key size settings.
keysize	Value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Specifies the access point provision list settings.
auth-list	Specifies the provision list authorization settings.
ap_mac	MAC address of access point to be added or deleted from the provision list.
revert-cert	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.
retries	Value from 0 to 255; the default value is 3. **Note** If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate. If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Command Default The default value of *keysize* is 2048 bits. The default value of *retries* is 3.

Usage Guidelines You can configure only one CA server. To configure a different CA server, delete the configured CA server by using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with an MIC or SSC certificate that join the controller are LSC provisioned.

Examples This example shows how to enable the LSC settings:

```
> config certificate lsc enable
```

This example shows how to enable the LSC settings for Certificate Authority (CA) server settings:

```
> config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

This example shows how to add a CA certificate from the CA server and add it to the controller's certificate database:

```
> config certificate lsc ca-cert add
```

This example shows how to configure an LSC certificate with the keysize of 2048 bits:

```
> config certificate lsc keysize 2048
```

Related Commands

config certificate

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config country

To configure the controller's country code, use the **config country** command.

config country *country_code*

Syntax Description

country_code	Two-letter or three-letter country code.

Command Default

us (country code of the United States of America).

Usage Guidelines

Cisco wireless LAN controllers must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password protected by the installer to maintain compliance with regulatory requirements and to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

You can use the **show country** command to display a list of supported countries.

Examples

This example shows how to configure the controller's country code to DE:

```
> config country DE
```

Related Commands

show country

config certificate ssc

To configure Self Signed Certificates (SSC) certificates, use the **config certificate ssc** command.

config certificate ssc hash validation {**enable** | **disable**}

Syntax Description

hash	Configures the SSC hash key.
validation	Configures hash validation of the SSC certificate.
enable	Enables hash validation of the SSC certificate.
disable	Disables hash validation of the SSC certificate.

Command Default

Enabled.

Usage Guidelines

When you enable the SSC hash validation, an AP validates the SSC certificate of the virtual controller. When an AP validates the SSC certificate, it checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the validation passes and the AP moves to the Run state. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. Hence, an AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC certificate, the AP bypasses the hash validation and directly moves to the Run state.

APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated to a physical controller and if hash validation is disabled, it joins any virtual controller without hash validation.

Examples

This example shows how to enable hash validation of the SSC certificate:

```
> config certificate ssc hash validation enable
```

Related Commands

show certificate ssc

show mobility group member

config mobility group member hash

config certificate

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config ipv6 ra-guard

To configure the filter for RA packets originating from client on an AP, use the **config ipv6 ra-guard** command.

config ipv6 ra-guard ap {**enable** | **disable**}

Syntax Description

enable	Enables Router Advertisement Guard on an AP.
disable	Disables Router Advertisement Guard on an AP.

Command Default

None.

Examples

This example shows how to enable IPv6 RA guard:

```
> config ipv6 ra-guard
```

Related Commands

show ipv6 ra-guard

config known ap

To configure a known Cisco lightweight access point, use the **config known ap** command.

config known ap {**add** | **alert** | **delete**} *MAC*

Syntax Description

add	Adds a new known access point entry.
alert	Generates a trap upon detection of the access point.
delete	Deletes an existing known access point entry.
MAC	MAC address of the known Cisco lightweight access point.

Command Default

None.

Examples

This example shows how to add a new access point entry ac:10:02:72:2f:bf on a known access point:

```
> config known ap add ac:10:02:72:2f:bf 12
```

Related Commands

config ap

config wgb vlan

To configure WGB VLAN client support, use the **config wgb vlan** command.

config wgb vlan {**enable** | **disable**}

Syntax Description

enable	Enables wired clients behind a WGB to connect to an anchor controller in a DMZ.
disable	Disables wired clients behind a WGB from connecting to an anchor controller in a DMZ.

Command Default

None.

Examples

This example shows how to enable WGB VLAN client support:

```
> config wgb vlan enable
```

Configure Advanced Timers Commands

User the **advanced timers** commands to configure advanced 802.11a settings.

config advanced timers ap-discovery-timeout

To configure the Cisco lightweight access point discovery time-out, use the **config advanced timers ap-discovery-timeout** command.

config advanced timers ap-discovery-timeout *seconds*

Syntax Description

seconds	Cisco lightweight access point discovery timeout value between 1 and 10 seconds.

Command Default

10 seconds.

Usage Guidelines

The Cisco lightweight access point discovery timeout is how often a Cisco wireless LAN controller attempts to discover unconnected Cisco lightweight access points.

Examples

This example shows how to configure an access point discovery-timeout with the timeout value of 20:

```
> config advanced timers ap-discovery-timeout 20
```

Related Commands

show advanced timers

config advanced timers ap-heartbeat-timeout

config advanced timers ap-fast-heartbeat

config advanced timers ap-primary-discovery-timeout

config advanced timers auth-timeout

config advanced timers ap-fast-heartbeat

To enable or disable the fast heartbeat timer which reduces the amount of time it takes to detect a controller failure for local, FlexConnect, or all access points, use the **config advanced timers ap-fast-heartbeat** command.

config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable** | **disable** } *interval*

Syntax Description

local	Configures the fast heartbeat interval for access points in local mode only.
flexconnect	Configures the fast heartbeat interval for access points in FlexConnect mode only.
all	Configures the fast heartbeat interval for all access points.
enable	Enables the fast heartbeat interval.
disable	Disables the fast heartbeat interval.
interval	Small heartbeat interval (between 1 and 10 seconds, inclusive), which reduces the amount of time it takes to detect a controller failure.

Command Default

Disabled.

Examples

This example shows how to enable the fast heartbeat interval for access point in local mode:

```
> config advanced timers ap-fast-heartbeat local enable 5
```

This example shows how to enable the fast heartbeat interval for access point in FlexConnect mode:

```
> config advanced timers ap-fast-heartbeat flexconnect enable 8
```

This example shows how to enable the fast heartbeat interval for all access points:

```
> config advanced timers ap-fast-heartbeat all enable 6
```

This example shows how to disable the fast heartbeat interval for all access point:

```
> config advanced timers ap-fast-heartbeat all disable
```

Related Commands

show advanced timers

config advanced timers ap-discovery-timeout

config advanced timers ap-heartbeat-timeout

config advanced timers ap-primary-discovery-timeout

config advanced timers auth-timeout

config advanced timers ap-heartbeat-timeout

To configure the Cisco lightweight access point heartbeat timeout, use the **config advanced timers ap-heartbeat-timeout** command.

config advanced timers ap-heartbeat-timeout *seconds*

Syntax Description

seconds	Cisco lightweight access point heartbeat timeout value between 1 and 30 seconds.

Command Default

30 seconds.

Usage Guidelines

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco wireless LAN controller.

This *seconds* value should be at least three times larger than the fast heartbeat timer.

Examples

This example shows how to configure an access point heartbeat timeout to 20:

```
> config advanced timers ap-heartbeat-timeout 20
```

Related Commands

show advanced timers

config advanced timers ap-discovery-timeout

config advanced timers ap-fast-heartbeat

config advanced timers ap-primary-discovery-timeout

config advanced timers auth-timeout

config advanced timers ap-primary-discovery-timeout

To configure the access point primary discovery request timer, use the **config advanced timers ap-primary-discovery-timeout** command.

config advanced timers ap-primary-discovery-timeout *interval*

Syntax Description

interval	Access point primary discovery request timer between 30 and 3600 seconds.

Command Default

120 seconds.

Examples

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
> config advanced timers ap-primary-discovery-timeout 1200
```

Related Commands

show advanced timers

config advanced timers ap-discovery-timeout

config advanced timers ap-fast-heartbeat

config advanced timers ap-heartbeat-timeout

config advanced timers auth-timeout

config advanced timers auth-timeout

To configure the authentication timeout, use the **config advanced timers auth-timeout** command.

config advanced timers auth-timeout *seconds*

Syntax Description

seconds	Authentication response timeout value in seconds between 10 and 600.

Command Default

10 seconds.

Examples

This example shows how to configure the authentication timeout to 20 seconds:

```
> config advanced timers auth-timeout 20
```

Related Commands

show advanced timers
config advanced timers ap-discovery-timeout
config advanced timers ap-heartbeat-timeout
config advanced timers ap-primary-discovery-timeout
config advanced timers ap-fast-heartbeat

config advanced timers eap-timeout

To configure the Extensible Authentication Protocol (EAP) expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description

seconds	EAP timeout value in seconds between 8 and 120.

Command Default None.

Examples This example shows how to configure the EAP expiration timeout to 10 seconds:

```
> config advanced timers eap-timeout 10
```

Related Commands **show advanced timers**

config advanced timers eap-identity-request-delay

To configure the advanced Extensible Authentication Protocol (EAP) identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

config advanced timers eap-identity-request-delay *seconds*

Syntax Description

seconds	Advanced EAP identity request delay in number of seconds between 0 and 10.

Command Default None.

Examples This example shows how to configure the advanced EAP identity request delay to 8 seconds:

```
> config advanced timers eap-identity-request-delay 8
```

Related Commands

config advanced timers auth-timeout

config advanced timers rogue-ap

show advanced timers

Configure Access Point Commands

Use the **config ap** commands to configure access point settings.

config ap

To enable or disable a Cisco lightweight access point or to add or delete a third-party (foreign) access point, use the **config ap** command.

config ap {{**enable** | **disable**} *cisco_ap* | {**add** | **delete**} *MAC port* {**enable** | **disable**} *IP_address*}

Syntax Description

enable	Enables the Cisco lightweight access point.
disable	Disables the Cisco lightweight access point.
cisco_ap	Name of the Cisco lightweight access point.
add	Adds foreign access points.
delete	Deletes foreign access points.
MAC	MAC address of a foreign access point.
port	Port number through which the foreign access point can be reached.
IP_address	IP address of the foreign access point.

Command Default

None.

Examples

This example shows how to disable lightweight access point AP1:

```
> config ap disable AP1
```

This example shows how to add a foreign access point with MAC address 12:12:12:12:12:12 and IP address 192.12.12.1 from port 2033:

> **config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1**

Related Commands

Configure Access Point Commands

Show Access Point Commands

config ap bhrate

To configure the Cisco bridge backhaul Tx rate, use the **config ap bhrate** command.

config ap bhrate {*rate* | **auto**} *cisco_ap*

Syntax Description

rate	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
auto	Configures the auto data rate.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

Auto.

Usage Guidelines

In previous software releases, the default value for bridge data rate was 24000 (24 Mbps). In controller software release 6.0, the default value for bridge data rate is **auto**. If you configured the default bridge data rate value (24000) in a previous controller software release, the bridge data rate is configured with the new default value (auto) when you upgrade to controller software release 6.0. However, if you configured a non default value (for example, 18000) in a previous controller software release, that configuration setting is preserved when you upgrade to software release 6.0.

When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

Examples

This example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
> config ap bhrate 54000 AP1
```

Related Commands

config ap

config ap autoconvert

To automatically convert all access points to a FlexConnect mode or monitor mode upon joining the controller, use the **config ap autoconvert** command:

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

Syntax Description

flexconnect	Configures all the access points automatically to FlexConnect mode.
monitor	Configures all the access points automatically to monitor mode.
disable	Disables the autoconvert option on the access points.

Command Default

None.

Usage Guidelines

When access points in local mode connect to a Cisco 7500 Series Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Controller, the access points must be in FlexConnect mode or monitor mode.

Examples

This example shows how to automatically convert all access points to the FlexConnect mode:

```
> config ap autoconvert flexconnect
```

This example shows how to disable the autoconvert option on the APs:

```
> config ap autoconvert disable
```

Related Commands

config ap

show ap

config ap bhrate

To configure the Cisco bridge backhaul Tx rate, use the **config ap bhrate** command.

config ap bhrate {*rate* | **auto**} *cisco_ap*

Syntax Description

rate	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
auto	Configures the auto data rate.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

Auto.

Usage Guidelines

In previous software releases, the default value for bridge data rate was 24000 (24 Mbps). In controller software release 6.0, the default value for bridge data rate is **auto**. If you configured the default bridge data rate value (24000) in a previous controller software release, the bridge data rate is configured with the new default value (auto) when you upgrade to controller software release 6.0. However, if you configured a non default value (for example, 18000) in a previous controller software release, that configuration setting is preserved when you upgrade to software release 6.0.

When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

Examples

This example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
> config ap bhrate 54000 AP01
```

Related Commands

config ap

config ap bridgegroupname

To set or delete a bridge group name on a Cisco lightweight access point, use the **config ap bridgegroupname** command.

config ap bridgegroupname {**set** *groupname* | **delete**} *cisco_ap*

Syntax Description

set	Sets a Cisco lightweight access point's bridge group name.
groupname	Bridge group name.
delete	Deletes a Cisco lightweight access point's bridge group name.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None.

Usage Guidelines

Only access points with the same bridge group name can connect to each other. Changing the AP bridgegroupname may strand the bridge AP.

Examples

This example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:

```
> config ap bridgegroupname delete AP02
Changing the AP's bridgegroupname may strand the bridge AP. Please continue with caution.
Changing the AP's bridgegroupname will also cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Related Commands

config ap

config ap bridging

To enable or disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **config ap bridging** command.

config ap bridging {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the Ethernet-to-Ethernet bridging on a Cisco lightweight access point.
disable	Disables Ethernet-to-Ethernet bridging.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None.

Examples

This example shows how to enable bridging on an access point:

```
> config ap bridging enable nyc04-44-1240
```

This example shows hot to disable bridging on an access point:

```
> config ap bridging disable nyc04-44-1240
```

Related Commands

config ap

config ap cdp

To enable or disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **config ap cdp** command.

config ap cdp {**enable** | **disable** | **interface** {**ethernet** *interface_number* | **slot** *slot_id*}} {*cisco_ap* | **all**}

Syntax Description

enable	Enables CDP on an access point.
disable	Disables CDP on an access point.
interface	Configures CDP in a specific interface.
ethernet	Configures CDP for an ethernet interface.
interface_number	Ethernet interface number between 0 and 3.
slot	Configures CDP for a radio interface.
slot_id	Slot number between 0 and 3.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Command Default

Enabled on radio interfaces of mesh APs and disabled on radio interfaces of non-mesh APs. Enabled on Ethernet interfaces of all APs.

Usage Guidelines

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.

Note CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the controller, you may disable and then reenable CDP on individual access points using the **config ap cdp** {**enable** | **disable**} *cisco_ap command*. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

Examples

This example shows how to enable CDP on all access points:

```
> config ap cdp enable all
```

This example shows how to disable CDP on ap02 access point:

```
> config ap cdp disable ap02
```

This example shows how to enable CDP for Ethernet interface number 2 on all access points:

```
> config ap cdp ethernet 2 enable all
```

Related Commands

config cdp timer

show ap cdp

config ap core-dump

To configure a Cisco lightweight access point's memory core dump, use the **config ap core-dump** command.

config ap core-dump {**disable** | **enable** *tftp_server_ipaddress filename* {**compress** | **uncompress**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables the Cisco lightweight access point's memory core dump setting.
disable	Disables the Cisco lightweight access point's memory core dump setting.
tftp_server_ipaddress	IP address of the TFTP server to which the access point sends core dump files.
filename	Name that the access point uses to label the core file.
compress	Compresses the core dump file.
uncompress	Uncompresses the core dump file.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points.

Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Command Default

None.

Usage Guidelines

The access point must be able to reach the TFTP server.

Examples

This example shows how to configure and compress the core dump file:

```
> config ap core-dump enable 192.1.1.1 log compress AP02
```

Related Commands

config ap crash-file clear-all

config ap crash-file delete

config ap crash-file get-crash-file

config ap crash-file get-radio-core-dump

config ap port

config ap crash-file clear-all

To delete all crash and radio core dump files, use the **config ap crash-file clear-all** command.

config ap crash-file clear-all

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to delete all crash files:

```
> config ap crash-file clear-all
```

Related Commands

config ap core-dump

config ap crash-file delete

config ap crash-file get-crash-file

config ap crash-file get-radio-core-dump

config ap port

config ap crash-file delete

To delete a single crash or radio core dump file, use the **config ap crash-file delete** command.

config ap crash-file delete *filename*

Syntax Description

filename	Name of the file to delete.

Command Default None.

Examples This example shows how to delete crash file 1:

```
> config ap crash-file delete crash_file_1
```

Related Commands

config ap crash-file clear-all
config ap crash-file core-dump
config ap crash-file get-crash-file
config ap crash-file get-radio-core-dump
config ap port

config ap crash-file get-crash-file

To collect the latest crash data for a Cisco lightweight access point, use the **config ap crash-file get-crash-file** command.

config ap crash-file get-crash-file *cisco_ap*

Syntax Description

cisco_ap	Name of the Cisco lightweight access point.

Command Default None.

Usage Guidelines Use the **transfer upload datatype** command to transfer the collected data to the Cisco wireless LAN controller.

Examples This example shows how to collect the latest crash data for access point AP3:

```
> config ap crash-file get-crash-file AP3
```

Related Commands

config ap crash-file core-dump

config ap crash-file crash-file delete

config ap crash-file clear-all

config ap crash-file get-radio-core-dump

config ap port

config ap crash-file get-radio-core-dump

To get a Cisco lightweight access point's radio core dump, use the **config ap crash-file get-radio-core-dump** command.

config ap crash-file get-radio-core-dump *slot_id cisco_ap*

Syntax Description

slot_id	Slot ID (either 0 or 1).
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None.

Examples

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
> config ap crash-file get-radio-core-dump 0 AP02
```

Related Commands

config ap crash-file clear-all

config ap crash-file delete

config ap crash-file get-crash-file

config ap crash-file core-dump

config ap port

config ap dot1xuser

To configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future, use the **config ap dot1xuser** command**.**

config ap dot1xuser add username *user* **password** *password* {**all** | *cisco_ap*}

Syntax Description

add username	Specifies to add a username.
user	Username.
password	Specifies to add a password.
password	Password.
cisco_ap	Specific access point.
all	Specifies all access points.

Command Default

None.

Usage Guidelines

You must enter a strong *password*. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

You can set the values for a specific access point.

Examples

This example shows how to configure the global authentication username and password for all access points:

```
> config ap dot1xuser add username cisco123 password cisco2020 all
```

Related Commands

config ap dot1xuser delete

config ap dot1xuser disable

show ap summary

config ap dot1xuser delete

To force a specific access point to use the controller's global authentication settings, use the **config ap dot1xuser delete** command.

config ap dot1xuser delete *cisco_ap*

Syntax Description

cisco_ap	Access point.

Command Default

None.

Examples

This example shows how to delete access point AP01 to use the controller's global authentication settings:

```
> config ap dot1xuser delete AP01
```

Related Commands

config ap dot1xuser

config ap dot1xuser disable

show ap summary

config ap dot1xuser disable

To disable authentication for all access points or for a specific access point, use the **config ap dot1xuser disable** command.

config ap dot1xuser disable {**all** | *cisco_ap*}

Syntax Description

disable	Disables authentication.
all	Specifies all access points.
cisco_ap	Access point.

Command Default

None.

Usage Guidelines

You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Examples

This example shows how to disable the authentication for access point cisco_ap1:

```
> config ap dot1xuser disable
```

Related Commands

config ap dot1xuser delete

config ap dot1xuser

show ap summary

config ap ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **config ap ethernet duplex** command.

config ap ethernet duplex [**auto** | **half** | **full**] **speed** [**auto** | **10** | **100** | **1000**] { **all** | *cisco_ap*}

Syntax Description

auto	(Optional) Specifies the Ethernet port duplex auto settings.
half	(Optional) Specifies the Ethernet port duplex half settings.
full	(Optional) Specifies the Ethernet port duplex full settings.
speed	Specifies the Ethernet port speed settings.
auto	(Optional) Specifies the Ethernet port speed to auto.
10	(Optional) Specifies the Ethernet port speed to 10 Mbps.
100	(Optional) Specifies the Ethernet port speed to 100 Mbps.
1000	(Optional) Specifies the Ethernet port speed to 1000 Mbps.
all	Specifies the Ethernet port setting for all connected access points.
cisco_ap	Cisco access point.

Command Default

None.

Examples

This example shows how to configure the Ethernet port duplex half settings as 10 Mbps for all access points:

```
> config ap ethernet duplex half speed 10 all
```

Related Commands

config ap ethernet

config ap ethernet tag

config ap

show ap summary

config ap ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **config ap ethernet duplex** command.

config ap ethernet duplex [**auto** | **half** | **full**] **speed** [**auto** | **10** | **100** | **1000**] { **all** | *cisco_ap*}

Syntax Description

auto	(Optional) Specifies the Ethernet port duplex auto settings.
half	(Optional) Specifies the Ethernet port duplex half settings.
full	(Optional) Specifies the Ethernet port duplex full settings.
speed	Specifies the Ethernet port speed settings.
auto	(Optional) Specifies the Ethernet port speed to auto.
10	(Optional) Specifies the Ethernet port speed to 10 Mbps.
100	(Optional) Specifies the Ethernet port speed to 100 Mbps.
1000	(Optional) Specifies the Ethernet port speed to 1000 Mbps.
all	Specifies the Ethernet port setting for all connected access points.
cisco_ap	Cisco access point.

Command Default

None.

Examples

This example shows how to configure the Ethernet port duplex half settings as 10 Mbps for all access points:

```
> config ap ethernet duplex half speed 10 all
```

Related Commands

config ap ethernet

config ap ethernet tag

config ap

show ap summary

config ap ethernet tag

To configure VLAN tagging of the Control and Provisioning of Wireless Access Points protocol (CAPWAP) packets, use the **config ap ethernet tag** command.

config ap ethernet tag {**id** *vlan_id* | **disable**} {*cisco_ap* | **all**}

Syntax Description

id	Specifies the VLAN id.
vlan_id	ID of the trunk VLAN.
disable	Disables the VLAN tag feature. When you disable VLAN tagging, the access point untags the CAPWAP packets.
cisco_ap	Name of the Cisco AP.
all	Configures VLAN tagging on all the Cisco access points.

Command Default

None.

Usage Guidelines

After you configure VLAN tagging, the configuration comes into effect only after the access point reboots.

You cannot configure VLAN tagging on mesh access points.

If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the WCS, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.

Examples

This example shows how to configure VLAN tagging on a trunk VLAN:

```
> config ap ethernet tag 6 AP1
```

Related Commands

config ap ethernet

config ap ethernet duplex

show ap ethernet tag

show ap config general

config ap group-name

To specify a descriptive group name for a Cisco lightweight access point, use the **config ap group-name** command.

config ap group-name *groupname cisco_ap*

Syntax Description

groupname	Descriptive name for the access point group.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

Examples

This example shows how to configure a descriptive name for access point AP01:

```
> config ap group-name superusers AP01
```

Related Commands

config ap group-name

config wlan apgroup

show ap summary

show ap wlan

config ap hotspot

To configure HotSpot parameters on an access point, use the **config ap hotspot** command.

config ap hotspot venue {**type** *group_code type_code* | **name** {**add** *language_code venue_name* | **delete**}} *cisco_ap*

Syntax Description

venue	Configures venue information for given AP group.
type	Configures the type of venue for given AP group.
group_code	Venue group information for given AP group. The following options are available: • 0—UNSPECIFIED • 1—ASSEMBLY • 2—BUSINESS • 3—EDUCATIONAL • 4—FACTORY-INDUSTRIAL • 5—INSTITUTIONAL • 6—MERCANTILE • 7—RESIDENTIAL • 8—STORAGE • 9—UTILITY-MISC • 10—VEHICULAR • 11—OUTDOOR

type_code

Venue type information for the AP group.

For venue group 1 (ASSEMBLY), the following options are available:

- 0—UNSPECIFIED ASSEMBLY
- 1—ARENA
- 2—STADIUM
- 3—PASSENGER TERMINAL
- 4—AMPHITHEATER
- 5—AMUSEMENT PARK
- 6—PLACE OF WORSHIP
- 7—CONVENTION CENTER
- 8—LIBRARY
- 9—MUSEUM
- 10—RESTAURANT
- 11—THEATER
- 12—BAR
- 13—COFFEE SHOP
- 14—ZOO OR AQUARIUM
- 15—EMERGENCY COORDINATION CENTER

For venue group 2 (BUSINESS), the following options are available:

- 0—UNSPECIFIED BUSINESS
- 1—DOCTOR OR DENTIST OFFICE
- 2—BANK
- 3—FIRE STATION
- 4—POLICE STATION
- 6—POST OFFICE
- 7—PROFESSIONAL OFFICE
- 8—RESEARCH AND DEVELOPMENT FACILITY
- 9—ATTORNEY OFFICE

For venue group 3 (EDUCATIONAL), the following options are available:

- 0—UNSPECIFIED EDUCATIONAL
- 1—PRIMARY SCHOOL
- 2—SECONDARY SCHOOL

- 3—UNIVERSITY OR COLLEGE

For venue group 4 (FACTORY-INDUSTRIAL), the following options are available:

- 0—UNSPECIFIED FACTORY AND INDUSTRIAL
- 1—FACTORY

For venue group 5 (INSTITUTIONAL), the following options are available:

- 0—UNSPECIFIED INSTITUTIONAL
- 1—HOSPITAL
- 2—LONG-TERM CARE FACILITY
- 3—ALCOHOL AND DRUG RE-HABILITATION CENTER
- 4—GROUP HOME
- 5 :PRISON OR JAIL

type_code

For venue group 6 (MERCANTILE), the following options are available:

- 0—UNSPECIFIED MERCANTILE
- 1—RETAIL STORE
- 2—GROCERY MARKET
- 3—AUTOMOTIVE SERVICE STATION
- 4—SHOPPING MALL
- 5—GAS STATION

For venue group 7 (RESIDENTIAL), the following options are available:

- 0—UNSPECIFIED RESIDENTIAL
- 1—PRIVATE RESIDENCE
- 2—HOTEL OR MOTEL
- 3—DORMITORY
- 4—BOARDING HOUSE

For venue group 8 (STORAGE), the option is:

- 0—UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the option is:

- 0—UNSPECIFIED UTILITY AND MISCELLANEOUS

For venue group 10 (VEHICULAR), the following options are available:

- 0—UNSPECIFIED VEHICULAR
- 1—AUTOMOBILE OR TRUCK
- 2—AIRPLANE
- 3—BUS
- 4—FERRY
- 5—SHIP OR BOAT
- 6—TRAIN
- 7—MOTOR BIKE

For venue group 11 (OUTDOOR), the following options are available:

- 0—UNSPECIFIED OUTDOOR
- 1—MINI-MESH NETWORK
- 2—CITY PARK
- 3—REST AREA

- 4—TRAFFIC CONTROL
- 5—BUS STOP
- 6—KIOSK

name	Configures the name of venue for this access point.
language_code	ISO-639 encoded string defining the language used at the venue. This string is a three-character language code. For example, you can enter ENG for English.
venue_name	Venue name for this access point. This name is associated with the basic service set (BSS) and is used in cases where the SSID does not provide enough information about the venue. The venue name is case sensitive and can be up to 252 alphanumeric characters.
add	Adds the HotSpot venue name for this access point.
delete	Deletes the HotSpot venue name for this access point.
cisco_ap	Name of the Cisco access point.

Examples

This example shows how to configure the venue group as educational and venue type as university:

```
> config ap hotspot venue type 3 3
```

Related Commands

show wlan

debug hotspot events

debug hotspot packets

config wlan apgroup hotspot venue

config wlan apgroup hotspot operating-class

config wlan hotspot

config advanced hotspot

show advanced hotspot

config wlan security wpa gtk-random

config ap image predownload

To configure an image on a specified access point, use the **config ap image predownload** command.

config ap image predownload {**abort** | **primary** | **backup**} {*cisco_ap* | **all**}

Syntax Description

abort	Aborts the predownload image process.
primary	Predownloads an image to a Cisco access point from the controller's primary image.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points to predownload an image.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Command Default None.

Examples This example shows how to predownload an image to an access point from the primary image:

```
> config ap image predownload primary all
```

Related Commands

config ap image swap

show ap image

config ap image swap

To swap an access point's primary and backup images, use the **config ap image swap** command.

config ap image swap {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points to interchange the boot images.

Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Command Default None.

Examples This example shows how to swap an access point's primary and secondary images:

```
> config ap image swap all
```

Related Commands

config ap image predownload

show ap image

config ap led-state

To enable or disable the LED-State for an access point, or to configure the flashing of LEDs, use the **config ap led-state** command.

config ap led-state {**enable** | **disable**} {*cisco_ap* | **all**}

config ap led-state flash {*seconds* | **indefinite** | **disable**} {*cisco_ap* | **dual-band**}

Syntax Description

enable	Enables the access point's LED state.
disable	Disables the access point's LED state.
cisco_ap	Name of a Cisco lightweight access point.
flash	Configure the flashing of LEDs for an access point.
seconds	Duration that the LEDs have to flash. The range is from 1 to 3600 seconds.
indefinite	Configures indefinite flashing of the access point's LED.
dual-band	Configures the LED state for all dual-band access points.

Usage Guidelines

Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

LEDs on access points with dual-band radio module will flash green and blue when you execute the led state flash command.

Command Default

None.

Examples

This example shows how to enable the LED state for an access point:

```
> config ap led-state enable AP02
```

This example shows how to enable the flashing of LEDs for dual-band access points:

```
> config ap led-state flash 20 dual-band
```

Related Commands

config ap

config ap link-encryption

To enable or disable the Datagram Transport Layer Security (DTLS) data encryption for access points on the 5500 series controller, use the **config ap link-encryption** command.

Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

config ap link-encryption {**enable** | **disable**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables the DTLS data encryption for access points.
disable	Disables the DTLS data encryption for access points.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points.

Command Default

DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points.

Usage Guidelines

Only Cisco 5500 Series Controllers support DTLS data encryption. This feature is not available on other controller platforms. If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted.

Only Cisco 1130, 1140, 1240, and 1250 series access points support DTLS data encryption, and data-encrypted access points can join a Cisco 5500 Series Controller only if the wplus license is installed on the controller. If the wplus license is not installed, the access points cannot join the controller.

Examples

This example shows how to enable the data encryption for an access point:

```
> config ap link-encryption enable AP02
```

Related Commands

config ap

show dtls connections

config ap link-latency

To enable or disable link latency for a specific access point or for all access points currently associated to the controller, use the **config ap link-latency** command:

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

config ap link-latency {**enable** | **disable** | **reset**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables the link latency for an access point.
disable	Disables the link latency for an access point.
reset	Resets all link latency for all access points.
cisco_ap	Name of the Cisco lightweight access point.
all	Specifies all access points.

Command Default

Link latency is disabled by default.

Usage Guidelines

This command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Examples

This example shows how to enable the link latency for all access points:

```
> config ap link-latency enable all
```

Related Commands

show ap config

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command.

config ap location *location cisco_ap*

Syntax Description

location	Location name of the access point (enclosed by double quotation marks).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

Examples

This example shows how to configure the descriptive location for access point AP1:

```
> config ap location "Building 1" AP1
```

Related Commands

show ap summary

config ap logging syslog level

To set the severity level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog level** command.

config ap logging syslog level *severity_level* {*cisco_ap* | **all**}

Syntax Description

severity_level	Severity levels are as follows: • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7
cisco_ap	Cisco access point.
all	Specifies all access points.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Command Default None.

Usage Guidelines If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

Examples This example shows how to set the severity for filtering syslog messages to 3:

```
> config ap logging syslog level 3
```

Related Commands

config logging syslog host

config logging syslog facility

show logging

config ap mgmtuser add

To configure username, password, and secret password for AP management, use the **config ap mgmtuser add** command.

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* {**all** | *cisco_ap*}

Syntax Description

username	Configures the username for AP management.
AP_username	Management username.
password	Configures the password for AP management.
AP_password	AP management password.
secret	Configures the secret password for privileged AP management.
secret	AP managemetn secret password.
all	Applies configuration to every AP that does not have a specific username.
cisco_ap	Cisco access point.

Command Default

None.

Usage Guidelines

The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password sould not contain management username or reverse of usename.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

The following requirement is enforced on the secret password:

- The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

Examples

This example shows how to add a username, password, and secret password for AP management:

```
> config ap mgmtuser add username acd password Arc_1234 secret Mid_45 all
```

Related Commands **config ap mgmtuser delete**

config ap mgmtuser delete

To force a specific access point to use the controller's global credentials, use the **config ap mgmtuser delete** command.

config ap mgmtuser delete *cisco_ap*

Syntax Description

cisco_ap	Access point.

Command Default

None.

Examples

This example shows how to delete the credentials of an access point:

```
> config ap mgmtuser delete cisco_ap1
```

Related Commands

show ap summary

config ap mode

To change a Cisco wireless LAN controller communication option for an individual Cisco lightweight access point, use the **config ap mode** command.

config ap mode {**bridge** | **flexconnect** {**submode** {**none** | **wips**} | **local** {**submode** {**none** | **wips**} | **reap** | **rogue** | **sniffer** | **se-connect** | **monitor** {**submode** {**none** | **wips**} } *cisco_ap*

Syntax Description

bridge	Converts from a lightweight access point to a mesh access point (bridge mode).
flexconnect	Enables FlexConnect mode on an access point.
local	Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode).
reap	Enables remote edge access point mode on an access point.
rogue	Enables wired rogue detector mode on an access point.
sniffer	Enables wireless sniffer mode on an access point.
se-connect	Enables spectrum expert mode on an access point.
submode	(Optional) Configures wIPS submode on an access point.
none	Disables the wIPS on an access point.
wips	Enables the wIPS submode on an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Local.

Usage Guidelines

The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

Examples

This example shows how to set the controller to communicate with access point AP91 in bridge mode:

```
> config ap mode bridge AP91
```

This example shows how to set the controller to communicate with access point AP01 in local mode:

```
> config ap mode local AP01
```

This example shows how to set the controller to communicate with access point AP91 in remote office (REAP) mode:

```
> config ap mode flexconnect AP91
```

This example shows how to set the controller to communicate with access point AP91 in a wired rogue access point detector mode:

```
> config ap mode rogue AP91
```

This example shows how to set the controller to communicate with access point AP02 in wireless sniffer mode:

> **config ap mode sniffer AP02**

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

config ap monitor-mode

To configure Cisco lightweight access point channel optimization, use the **config ap monitor-mode** command.

config ap monitor-mode {**802.11b fast-channel** | **no-optimization** | **tracking-opt** | **wips-optimized**} *cisco_ap*

Syntax Description

802.11b fast-channel	Configures 802.11b scanning channels for a monitor-mode access point.
no-optimization	Specifies no channel scanning optimization for the access point.
tracking-opt	Enables tracking optimized channel scanning for the access point.
wips-optimized	Enables wIPS optimized channel scanning for the access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None.

Examples

This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
> config ap monitor-mode wips-optimized AP01
```

Related Commands

config 802.11 enable

config ap mode

show wps wips summary

show ap config

show ap monitor-mode summary

show wps wips statistics

config ap name

To modify the name of a Cisco lightweight access point, use the **config ap name** command.

config ap name *new_name old_name*

Syntax Description

new_name	Desired Cisco lightweight access point name.
old_name	Current Cisco lightweight access point name.

Command Default None.

Examples This example shows how to modify the name of access point AP1 to AP2:

```
> config ap name AP1 AP2
```

Related Commands **show ap config**

config ap packet-dump

To configure the Packet Capture parameters on access points, use the **config ap packet-dump** command.

config ap packet-dump {**buffer-size** *size* | **capture-time** *time* | **classifier** {**arp** {**enable** | **disable**} | **broadcast** {**enable** | **disable**} | **control** {**enable** | **disable**} | **data** {**enable** | **disable**} | **dot1x** {**enable** | **disable**} | **iapp** {**enable** | **disable**} | **ip** {**enable** | **disable**} | **management** {**enable** | **disable**} | **multicast** {**enable** | **disable**} | **tcp** {**enable** | **disable** | **port** *tcp_port* } | **udp** {**enable** | **disable** | **port** *udp_port* }} | **ftp** *server_ip* | **start** *mac_address cisco_ap* | **stop** | **truncate** *length*}

Syntax Description

buffer-size	Configures the buffer size for Packet Capture in the access point.
size	Size of the buffer. The range is from 1024 to 4096 KB.
capture-time	Configures the timer value for Packet Capture.
time	Timer value for Packet Capture. The range is from 1 to 60 minutes.
classifier	Configures the classifier information for Packet Capture. You can specify the type of packets that needs to be captured.
arp	Captures ARP packets.
enable	Enables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, Inter Access Point Protocol (IAPP), IP, 802.11 management, or multicast packets.
disable	Disables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, IAPP, IP, 802.11management, or multicast packets.
broadcast	Captures broadcast packets.
control	Captures 802.11 control packets.
data	Captures 802.11 data packets.
dot1x	Captures dot1x packets.
iapp	Captures IAPP packets.
ip	Captures IP packets.
management	Captures 802.11 management packets.
multicast	Captures multicast packets.
tcp	Captures TCP packets.
tcp_port	TCP port number. The range is from 1 to 65535.

udp	Captures TCP packets.
udp_port	UDP port number. The range is from 1 to 65535.
ftp	Configures FTP parameters for Packet Capture.
server_ip	FTP server IP address.
start	Starts Packet Capture from the access point.
mac_address	Client MAC Address for Packet Capture.
cisco_ap	Name of the Cisco access point.
stop	Stops Packet Capture from the access point.
truncate	Truncates the packet to the specified length during Packet Capture.
length	Length of the packet after truncation. The range is from 20 to 1500.

Command Default

The default buffer size is 2 MB. The default capture time is 10 mins.

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as a beacon or probe response. Only packets that flow through the Radio driver in the Tx path will be captured.

Use the command **config ap packet-dump start** to start the Packet Capture from the access point. When you start Packet Capture, the controller sends a Control and Provisioning of Wireless Access Points protocol (CAPWAP) message to the access point to which the client is associated and captures packets. You must configure the FTP server and ensure that the client is associated to the access point before you start Packet Capture. If the client is not associated to the access point, you must specify the name of the access point.

Examples

This example shows how to start Packet Capture from an access point:

```
> config ap packet-dump start 00:0d:28:f4:c0:45 AP1
```

This example shows how to capture 802.11 control packets from an access point:

```
> config ap packet-dump classifier control enable
```

Related Commands

show ap packet-dump status

debug ap packet-dump

config ap port

To configure the port for a foreign access point, use the **config ap port** command.

config ap port *MAC port*

Syntax Description

MAC	Foreign access point MAC address.
port	Port number for accessing the foreign access point.

Command Default

None.

Examples

This example shows how to configure the port for a foreign access point MAC address:

```
> config ap port 12:12:12:12:12:12 20
```

Related Commands

config ap

config ap power injector

To configure the power injector state for an access point, use the **config ap power injector** command.

config ap power injector {**enable** | **disable**} {*cisco_ap* | **all**} {**installed** | **override** | *switch_MAC*}

Syntax Description

enable	Enables the power injector state for an access point.
disable	Disables the power injector state for an access point.
cisco_ap	Name of the Cisco lightweight access point.
all	Specifies all Cisco lightweight access points connected to the controller.
installed	Detects the MAC address of the current switch port that has a power injector.
override	Overrides the safety checks and assumes a power injector is always installed.
switch_MAC	MAC address of the switch port with an installed power injector.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Command Default None.

Examples This example shows how to enable the power injector state for all access points:

```
> config ap power injector enable all 12:12:12:12:12:12
```

Related Commands **config ap**

config ap power pre-standard

To enable or disable the inline power Cisco pre-standard switch state for an access point, use the **config ap power pre-standard** command.

config ap power pre-standard {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the inline power Cisco pre-standard switch state for an access point.
disable	Disables the inline power Cisco pre-standard switch state for an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default Disabled.

Examples This example shows how to enable the inline power Cisco pre-standard switch state for access point AP02:

```
> config ap power pre-standard enable AP02
```

Related Commands **config ap**

config ap primary-base

To set the Cisco lightweight access point primary Cisco wireless LAN controller, use the **config ap primary-base** command.

config ap primary-base *controller_name cisco_ap* [*controller_ip_address*]

Syntax Description

controller_name	Name of the Cisco wireless LAN controller.
cisco_ap	Cisco lightweight access point name.
controller_ip_address	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. **Note** For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Command Default

None.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

Examples

This example shows how to set an access point primary Wireless LAN controller:

```
> config ap primary-base SW_1 AP2
```

Related Commands

show sysinfo

config sysname

config ap secondary-base

config ap tertiary-base

config ap priority

To assign a priority designation to an access point that allows it to reauthenticate after a controller failure by priority rather than on a first-come-until-full basis, use the **config ap priority** command.

config ap priority {**1** | **2** | **3** | **4**} *cisco_ap*

Syntax Description

1	Specifies low priority.
2	Specifies medium priority.
3	Specifies high priority.
4	Specifies the highest (critical) priority.
cisco_ap	Cisco lightweight access point name.

Command Default

1 - Low priority.

Usage Guidelines

In a failover situation, if the backup controller does not have enough ports to allow all the access points in the affected area to reauthenticate, it gives priority to higher-priority access points over lower-priority ones, even if it means replacing lower-priority access points.

Examples

This example shows how to assign a priority designation to access point AP02 that allows it to reauthenticate after a controller failure by assigning a reauthentication priority 3:

```
> config ap priority 3 AP02
```

Related Commands

config network ap-priority

show ap summary

show network summary

config ap reporting-period

To reset a Cisco lightweight access point, use the **config ap reporting-period** command.

config ap reporting-period *period*

Syntax Description

period	Time period in seconds between 10 and 120.

Command Default

None.

Examples

This example shows how to reset an access point reporting period to 120 seconds:

```
> config ap reporting-period 120
```

Related Commands

show ap config 802.11a

show ap config 802.11ab

config ap reset

To reset a Cisco lightweight access point, use the **config ap reset** command.

config ap reset *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default None.

Examples This example shows how to reset an access point:

```
> config ap reset AP2
```

Related Commands **show ap config**

config ap retransmit interval

To configure the access point control packet retransmission interval, use the **config ap retransmit interval** command.

config ap retransmit interval *seconds* {**all** | *cisco_ap*}

Syntax Description

seconds	AP control packet retransmission timeout between 2 and 5 seconds.
all	Specifies all access points.
cisco_ap	Cisco lightweight access point name.

Command Default None.

Examples This example shows how to configure the retransmission interval for all access points globally:

```
> config ap retransmit interval 4 all
```

Related Commands **show ap config**

config ap retransmit count

To configure the access point control packet retransmission count, use the **config ap retransmit count** command.

config ap retransmit count *count* {**all** | *cisco_ap*}

Syntax Description

count	Number of times control packet will be retransmitted. The range is from 3 to 8.
all	Specifies all access points.
cisco_ap	Cisco lightweight access point name.

Command Default None.

Examples This example shows how to configure the retransmission retry count for a specific access point:

```
> config ap retransmit count 6 cisco_ap
```

Related Commands **show ap config**

config ap role

To specify the role of an access point in a mesh network, use the **config ap role** command.

config ap role {**rootAP** | **meshAP**} *cisco_ap*

Syntax Description

rootAP	Designates the mesh access point as a root access point (RAP).
meshAP	Designates the mesh access point as a mesh access point (MAP).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

meshAP.

Usage Guidelines

Use the **meshAP** keyword if the access point has a wireless connection to the controller, or use the **rootAP** keyword if the access point has a wired connection to the controller. Changing the AP's role will cause the AP to reboot.

Examples

This example shows how to designate mesh access point AP02 as a root access point:

```
> config ap role rootAP AP02
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

Related Commands

show ap config

config ap rst-button

To configure the Reset button for an access point, use the **config ap rst-button** command.

config ap rst-button {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the Reset button for an access point.
disable	Disables the Reset button for an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default None.

Examples This example shows how to configure the reset button for access point AP03:

```
> config ap rst-button enable AP03
```

Related Commands **config ap**

config ap secondary-base

To set the Cisco lightweight access point secondary Cisco wireless LAN controller, use the **config ap secondary-base** command.

config ap secondary-base *controller_name cisco_ap* [*controller_ip_address*]

Syntax Description

controller_name	Name of the Cisco wireless LAN controller.
cisco_ap	Cisco lightweight access point name.
controller_ip_address	(Optional). If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. **Note** For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Command Default

None.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

Examples

This example shows how to set an access point secondary Cisco wireless controller:

```
> config ap secondary-base SW_1 AP2
```

Related Commands

show sysinfo

config sysname

config ap primary-base

config ap tertiary-base

config ap sniff

To enable or disable sniffing on an access point, use the **config ap sniff** command.

config ap sniff {**802.11a** | **802.11b**} {**enable** *channel server_ip* | **disable**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
enable	Enables sniffing on an access point.
channel	Channel to be sniffed.
server_ip	IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.
disable	Disables sniffing on an access point.
cisco_ap	Access point configured as the sniffer.

Command Default

Channel 36.

Usage Guidelines

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnipeek, Airopeek, AirMagnet, or Wireshark software. It includes information on the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets sent by the access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed:

- socket.dll file to the Plug-ins folder (for example, C:\Program Files\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder (for example, C:\Program Files\WildPackets\AiroPeek\1033\PluginRes)

Examples

This example shows how to enable the sniffing on the 802.11a an access point primary Wireless LAN controller:

```
> config ap sniff 80211a enable 23 11.22.44.55 AP01
```

Related Commands

show ap config

config ap sniff 802.11b

config ap ssh

To enable Secure Shell (SSH) connectivity on an access point, use the **config ap ssh** command.

config ap ssh {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the SSH connectivity on an access point.
disable	Disables the SSH connectivity on an access point.
cisco_ap	Cisco access point name.

Command Default None.

Usage Guidelines The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.

Examples This example shows how to enable SSH connectivity on access point Cisco_ap2:

```
> config ap ssh enable cisco_ap2
```

Related Commands

config ap

show ap stats

config network ssh

config ap static-ip

To configure Cisco lightweight access point static IP address settings, use the **config ap static-ip** command.

config ap static-ip {**enable** *cisco_ap ip_address net_mask gateway* | **disable** *cisco_ap* **add** {**domain** {*cisco_ap* | **all**} *domain_name*} | {**nameserver** {*cisco_ap* | **all**} *dns_ip_address*} | **delete** {**domain** | **nameserver**} {*cisco_ap* | **all**}}

Syntax Description

enable	Enables the Cisco lightweight access point static IP address.
disable	Disables the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address.
cisco_ap	Cisco lightweight access point name.
ip_address	Cisco lightweight access point IP address
net_mask	Cisco lightweight access point network mask.
gateway	IP address of the Cisco lightweight access point gateway.
add	Adds a domain or DNS server.
domain	Specifies the domain to which a specific access point or all access points belong.
all	Specifies all access points.
domain_name	Specifies a domain name.
nameserver	Specifies a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.
dns_ip_address	DNS server IP address.
delete	Deletes a domain or DNS server.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Command Default None.

Usage Guidelines

An access point cannot discover the controller using Domain Name System (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.

After you enter the IP, netmask, and gateway addresses, save your configuration to reboot the access point. After the access point rejoins the controller, you can enter the domain and DNS server information.

Examples

This example shows how to configure an access point static IP address:

```
> config ap static-ip enable AP2 1.1.1.1 255.255.255.0 209.165.200.254
```

Related Commands

show sysinfo

config sysname

config ap secondary-base

config ap primary-base

config ap stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco wireless LAN controller, use the **config ap stats-timer** command.

config ap stats-timer *period cisco_ap*

Syntax Description

period	Time in seconds from 0 to 65535. A zero value disables the timer.
cisco_ap	Cisco lightweight access point name.

Command Default

0 (disabled).

Usage Guidelines

A value of 0 (zero) means that the Cisco lightweight access point does not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

Examples

This example shows how to set the stats timer to 600 seconds for access point AP2:

```
> config ap stats-timer 600 AP2
```

Related Commands

config ap disable

config ap syslog host global

To configure a global syslog server for all access points that join the controller, use the **config ap syslog host global** command.

config ap syslog host global *syslog_server_IP_address*

Syntax Description

syslog_server_IP_address	IP address of the syslog server.

Command Default

255.255.255.255.

Usage Guidelines

By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

Examples

This example shows how to configure a global syslog server for all access points:

```
> config ap syslog host global 255.255.255.255
```

Related Commands

config ap syslog host specific

show ap

config global

show ap

config general

config ap syslog host specific

To configure a syslog server for a specific access point, use the **config ap syslog host specific** command.

config ap syslog host specific *cisco_ap syslog_server_IP_address*

Syntax Description

cisco_ap	Cisco lightweight access point.
syslog_server_IP_address	IP address of the syslog server.

Command Default

0.0.0.0.

Usage Guidelines

By default, the syslog server IP address for each access point is 0.0.0.0, indicating that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Examples

This example shows how to configure a syslog server:

```
> config ap syslog host specific 0.0.0.0
```

Related Commands

config ap syslog host global

show ap config global

show ap config general

config ap tcp-adjust-mss

To enable or disable the TCP maximum segment size (MSS) on a particular access point or on all access points, use the **config ap tcp-adjust-mss** command.

config ap tcp-adjust-mss {**enable** | **disable**} {*cisco_ap* | **all**} *size*

Syntax Description

enable	Enables the TCP maximum segment size on an access point.
disable	Disables the TCP maximum segment size on an access point.
cisco_ap	Cisco access point name.
all	Specifies all access points.
size	Maximum segment size, from 536 to 1363 bytes.

Note If an AP itself is configured with the name ‘all’, then the ‘all access points’ case takes precedence over the AP that is named ‘all’.

Command Default None.

Usage Guidelines When you enable this feature, the access point checks for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Examples This example shows how to enable the TCP MSS on access point Cisco_ap1 with a segment size of 1200 bytes:

```
> config ap tcp-adjust-mss enable cisco_ap1 1200
```

Related Commands **show ap tcp-mss-adjust**

config ap telnet

To enable Telnet connectivity on an access point, use the **config ap telnet** command.

config ap telnet {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the Telnet connectivity on an access point.
disable	Disables the Telnet connectivity on an access point.
cisco_ap	Cisco access point name.

Command Default

None.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.

Examples

This example shows how to enable Telnet connectivity on access point cisco_ap1:

```
> config ap telnet enable cisco_ap1
```

This example shows how to disable Telnet connectivity on access point cisco_ap1:

```
> config ap telnet disable cisco_ap1
```

Related Commands

config ap

config network telnet

show ap config

config ap tertiary-base

To set the Cisco lightweight access point tertiary Cisco wireless LAN controller, use the **config ap tertiary-base** command.

config ap tertiary-base *controller_name cisco_ap* [*controller_ip_address*]

Syntax Description

controller_name	Name of the Cisco wireless LAN controller.
cisco_ap	Cisco lightweight access point name.
controller_ip_address	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. **Note** For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Command Default

None.

Usage Guidelines

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operations and in the event of a hardware reset.

Examples

This example shows how to set the access point tertiary wireless LAN controller:

```
> config ap tertiary-base SW_1 AP02
```

Related Commands

show sysinfo

config sysname

config ap secondary-base

config ap primary-base

config ap tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **config ap ftp-downgrade** command.

config ap tftp-downgrade {*tftp_ip_address* | *image_filename* | *ap_name*}

Syntax Description

tftp_ip_address	IP address of the TFTP server.
image_filename	Filename of the access point image file on the TFTP server.
ap_name	Access point name.

Command Default

None.

Examples

This example shows how to configure the settings for downgrading access point ap1240_102301:

```
> config ap ftp-downgrade 209.165.200.224 1238.tar ap1240_102301
```

Related Commands

show version

show running-config

config ap username

To assign a username and password to access either a specific access point or all access points, use the **config ap username** command.

config ap username *user_id* **password** *passwd* [**all** | *ap_name*]

Syntax Description

user_id	Administrator username.
passwd	Administrator password.
all	(Optional) Specifies all access points.
ap_name	Name of a specific access point.

Command Default

None.

Examples

This example shows how to assign a username and password to a specific access point:

```
> config ap username jack password blue la204
```

This example shows how to assign the same username and password to a all access points:

```
> config ap username jack password blue all
```

config ap venue

To configure the venue information for 802.11u network on an access point, use the **config ap venue** command.

config ap venue {**add***venue_name venue-group venue-type lang-code cisco-ap* | **delete**}

Syntax Description

add	Adds venue information.
venue_name	Venue name.
venue_group	Venue group category. See the table below for details on venue group mappings.
venue_type	Venue type. This value depends on the venue-group specified. See the table below for venue group mappings.
lang_code	Language used. An ISO-14962-1997 encoded string that defines the language. This string is a three character language code. Enter the first three letters of the language in English (for example, eng for English).
cisco_ap	Name of the access point.
deletes	Deletes venue information.

Command Default

None.

Examples

The command shows how to set the venue details for an access point named cisco-ap1:

```
> config ap venue add test 11 34 eng cisco-ap1
```

Table 2: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	

Venue Group Name	Value	Venue Type for Group
ASSEMBLY	1	• 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER
BUSINESS	2	• 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE

Venue Group Name	Value	Venue Type for Group
EDUCATIONAL	3	• 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE
FACTORY-INDUSTRIAL	4	• 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	• 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL
MERCANTILE	6	• 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	• 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE

Venue Group Name	Value	Venue Type for Group
STORAGE	8	UNSPECIFIED STORAGE
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS
VEHICULAR	10	• 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE
OUTDOOR	11	• 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

Related Commands

config wlan mobile-concierge dot11u

config wlan mobile-concierge hotspot2

config wlan mobile-concierge msap

config ap wlan

To enable or disable wireless LAN override for a Cisco lightweight access point radio, use the **config ap wlan** command.

config ap wlan {**enable** | **disable**} {**802.11a** | **802.11b**} *wlan_id cisco_ap*

Syntax Description

enable	Enables the wireless LAN override on an access point.
disable	Disables the wireless LAN override on an access point.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
wlan_id	Cisco wireless LAN controller ID assigned to a wireless LAN.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Examples

This example shows how to enable wireless LAN override on the AP03 802.11a radio:

```
> config ap wlan 802.11a AP03
```

Related Commands

show ap wlan

Configure Advanced 802.11 Profile Commands

Use the **config advanced 802.11 profile** commands to configure Cisco lightweight access point profile settings on supported 802.11 networks.

config advanced 802.11 profile clients

To set the Cisco lightweight access point clients threshold between 1 and 75 clients, use the **config advanced 802.11 profile clients** command.

config advanced 802.11 {**a** | **b**} **profile clients** {**global** | *cisco_ap*} *clients*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
clients	802.11a Cisco lightweight access point client threshold between 1 and 75 clients.

Command Default

12 clients.

Examples

This example shows how to set all Cisco lightweight access point clients thresholds to 25 clients:

```
> config advanced 802.11 profile clients global 25
Global client count profile set.
```

This example shows how to set the AP1 clients threshold to 75 clients:

```
> config advanced 802.11 profile clients AP1 75
Global client count profile set.
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile clients

config advanced 802.11 profile customize

To turn customizing on or off for an 802.11a Cisco lightweight access point performance profile, use the **config advanced 802.11 profile customize** command.

config advanced 802.11 {**a** | **b**} **profile customize** *cisco_ap* {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point.
on	Customizes performance profiles for this Cisco lightweight access point.
off	Uses global default performance profiles for this Cisco lightweight access point.

Command Default

Off.

Examples

This example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
> config advanced 802.11 profile customize AP1 on
```

Related Commands

show advanced 802.11 profile

config advanced 802.11b profile customize

config advanced 802.11 profile foreign

To set the foreign 802.11a transmitter interference threshold between 0 and 100 percent, use the **config advanced 802.11 profile foreign** command.

config advanced 802.11 {**a** | **b**} **profile foreign** {**global** | *cisco_ap*} *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
percent	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Command Default

10.

Examples

This example shows how to set the foreign 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
> config advanced 802.11a profile foreign global 50
```

This example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
> config advanced 802.11 profile foreign AP1 0
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile foreign

config advanced 802.11 profile noise

To set the 802.11a foreign noise threshold between –127 and 0 dBm, use the **config advanced 802.11 profile noise** command.

config advanced 802.11 {**a** | **b**} **profile noise** {**global** | *cisco_ap*} *dBm*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
cisco_ap	Cisco lightweight access point name.
dBm	802.11a foreign noise threshold between –127 and 0 dBm.

Command Default

–70 dBm.

Examples

This example shows how to set the 802.11a foreign noise threshold for all Cisco lightweight access points to –127 dBm:

```
> config advanced 802.11a profile noise global -127
```

This example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
> config advanced 802.11a profile noise AP1 0
```

Related Commands

show advanced 802.11 profile

config advanced 802.11b profile noise

config advanced 802.11 profile throughput

To set the Cisco lightweight access point data-rate throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11 profile throughput** command.

config advanced 802.11 {**a** | **b**} **profile throughput** {**global** | *cisco_ap*} *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
cisco_ap	Cisco lightweight access point name.
value	802.11a Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second.

Command Default

1,000,000 bytes per second.

Examples

This example shows how to set all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
> config advanced 802.11 profile throughput global 1000
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
> config advanced 802.11 profile throughput AP1 10000000
```

Related Commands

show advanced 802.11 profile

config advanced 802.11b profile data-rate

config advanced 802.11 profile utilization

To set the RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11 profile utilization** command. The operating system generates a trap when this threshold is exceeded.

config advanced 802.11 {**a** | **b**} **profile utilization** {**global** | *cisco_ap*} *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures a global Cisco lightweight access point specific profile.
cisco_ap	Cisco lightweight access point name.
percent	802.11a RF utilization threshold between 0 and 100 percent.

Command Default

80 percent.

Examples

This example shows how to set the RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
> config advanced 802.11 profile utilization global 0
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
> config advanced 802.11 profile utilization AP1 100
```

Related Commands

show advanced 802.11a profile

config advanced 802.11b profile utilization

Configure Network Commands

Use the **config network** commands to configure network settings.

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

config network allow-old-bridge-aps {**enable** | **disable**}

Syntax Description

enable	Enables the switch association.
disable	Disables the switch association.

Command Default Enabled.

Examples This example shows how to configure an old bridge access point to associate with the switch:

```
> config network allow-old-bridge-aps enable
```

Related Commands **show network summary**

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

config network ap-discovery nat-ip-only {**enable** | **disable**}

Syntax Description

enable	Enables use of NAT IP only in discovery response. This is the default.
disable	Enables use of both NAT IP and non NAT IP in discovery response.

Command Default

Enabled.

Usage Guidelines

If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.

If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.

If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.

Examples

This example shows how to enable NAT IP in an AP discovery response:

```
> config network ap-discovery nat-ip-only enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco lightweight access point fallback.
disable	Disables the Cisco lightweight access point fallback.

Command Default

Enabled.

Examples

This example shows how to enable the Cisco lightweight access point fallback:

```
> config network ap-fallback enable
```

Related Commands

show network summary

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {**enable** | **disable**}

Syntax Description

enable	Enables the lightweight access point priority reauthentication.
disable	Disables the lightweight access point priority reauthentication.

Command Default

Disabled.

Examples

This example shows how to enable the lightweight access point priority reauthorization:

```
> config network ap-priority enable
```

Related Commands

config ap priority

show ap summary

show network summary

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk {**enable** | **disable**}

Syntax Description

enable	Enables the AppleTalk bridging.
disable	Disables the AppleTalk bridging.

Command Default None.

Examples This example shows how to configure AppleTalk bridging:

```
> config network apple-talk enable
```

Related Commands **show network summary**

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

Enabled.

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

Examples

This example shows how to configure the bridging shared secret string “shhh1”:

```
> config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default master, use the **config network master-base** command.

config network master-base {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default master.
disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default master.

Command Default

None.

Usage Guidelines

This setting is only used upon network installation and should be disabled after the initial network configuration. Because the Master Cisco wireless LAN controller is normally not used in a deployed network, the Master Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

Examples

This example shows how to enable the Cisco wireless LAN controller as a default master:

```
> config network master-base enable
```

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

Syntax Description

enable	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.
disable	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.

Command Default

Disabled.

Examples

This example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
> config network oeap-600 dual-rlan-ports enable
```

Related Commands

show network summary

config network oeap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network oeap-600 local-network** command.

config network oeap-600 local-network {**enable** | **disable**}

Syntax Description

enable	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.
disable	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.

Command Default

Disabled.

Examples

This example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
> config network oeap-600 local-network enable
```

Related Commands

show network summary

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {**enable** | **disable**}

Syntax Description

enable	Enables the OTAP provisioning.
disable	Disables the OTAP provisioning.

Command Default Enabled.

Examples This example shows how to disable the OTAP provisioning:

```
> config network otap-mode disable
```

Related Commands **show network summary**

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {**enable** | **disable**}

Syntax Description

enable	Enables the bridge access point ZeroConfig support.
disable	Disables the bridge access point ZeroConfig support.

Command Default Enabled.

Examples This example shows how to enable the bridge access point ZeroConfig support:

```
> config network zero-config enable
```

Related Commands **show network summary**

Configure Redundancy Commands

Use the **config redundancy** commands to configure High Availability parameters on the Active and Standby controllers.

config redundancy interface address peer-service-port

To configure the service port IP and netmask of the peer or standby controller, use the **config redundancy interface address peer-service-port** command.

config redundancy interface address peer-service-port *ip_address netmask*

Syntax Description

ip_address	IP address of the peer service port.
netmask	Netmask of the peer service port.

Command Default

None.

Usage Guidelines

You can configure this command only from the Active controller. For the HA feature, the service port configurations are made per controller. You will loose these configurations if you change the mode from HA to non-HA and vice-versa.

Examples

This example shows how to configure the service port IP and netmask of the peer or standby controller:

```
> config redundancy interface address peer-service-port 11.22.44.55
```

Related Commands

config redundancy mode

config redundancy peer-route

config redundancy mobilitymac

config redundancy unit

config redundancy timer

config redundancy mobilitymac

To configure the HA mobility MAC address to be used as an identifier, use the **config redundancy mobilitymac** command.

config redundancy mobilitymac *mac_address*

Syntax Description

mac_address	MAC address that is an identifier for the active and standby controller pair.

Command Default

None.

Examples

This example shows how to configure the HA mobility MAC address:

```
> config redundancy mobilitymac ff:ff:ff:ff:ff:ff
```

Related Commands

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

debug rfac

debug rmgr

debug rsyncmgr

show redundancy mobilitymac

show redundancy summary

show redundancy peer-route

show redundancy statistics

show redundancy timers

config redundancy mode

To enable or disable redundancy or High Availability (HA), use the **config redundancy mode**command

config redundancy mode {**sso** | **none**}

Syntax Description

sso	Enables stateful switch over (SSO) or hot standby redundancy mode.
none	Disables redundancy mode.

Command Default None.

Usage Guidelines You must configure local and peer redundancy management IP addresses before you configure redundancy.

Examples This example shows how to enable redundancy:

```
> config redundancy mode sso
```

This example shows how to disable redundancy:

```
> config redundancy mode none
```

Related Commands

config redundancy mobilitymac
config redundancy interface address peer-service-port
config redundancy peer-route
config redundancy unit
config redundancy timer
show redundancy peer-route
show redundancy summary
debug rmgr
debug rsyncmgr

config redundancy peer-route

To configure the route configurations of the peer or standby controller, use the **config redundancy peer-route** command.

config redundancy peer-route {**add** | **delete**} *network_ip_address netmask gateway*

Syntax Description

add	Adds a network route.
delete	Deletes a network route specific to standby controller.
network_ip_address	Network IP address.
netmask	Subnet mask of the network.
gateway	IP address of the gateway for the route network.

Command Default

None.

Usage Guidelines

You can configure this command only from the Active controller. For the HA feature, the service port configurations are made per controller. You will loose these configurations if you change the mode from HA to non-HA and vice-versa.

Examples

This example shows how to configure route configurations of a peer or standby controller.

```
> config redundancy peer-route add 10.1.1.0 255.255.255.0 10.1.1.1
```

Related Commands

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy mode

config redundancy unit

config redundancy timer

show redundancy peer-route

show redundancy summary

debug rmgr

debug rsyncmgr

config redundancy timer keep-alive-timer

To configure the keep-alive timeout value, use the **config redundancy timer keep-alive-timer** command.

config redundancy timer keep-alive-timer *milliseconds*

Syntax Description

milliseconds	Keep-alive timeout value in milliseconds. The range is from 100 to 400 milliseconds.

Command Default

100 milliseconds.

Examples

This example shows how to configure the keep-alive timeout value:

```
> config redundancy timer keep-alive-timer 200
```

Related Commands

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer peer-search-timer

show redundancy timers

show redundancy summary

debug rmgr

debug rsyncmgr

config redundancy timer peer-search-timer

To configure the peer search timer, use the **config redundancy timer peer-search-timer** command.

config redundancy timer peer-search-timer *seconds*

Syntax Description

seconds	Value of the peer search timer in seconds. The range is from 60 to 180 secs.

Command Default

120 seconds.

Usage Guidelines

You can use this command to configure the boot up role negotiation timeout value in seconds.

Examples

This example shows how to configure the redundancy peer search timer:

```
> config redundancy timer peer-search-timer 100
```

Related Commands

config redundancy mobilitymac
config redundancy interface address peer-service-port
config redundancy peer-route
config redundancy unit
config redundancy timer keep-alive-timer
show redundancy peer-route
show redundancy summary
debug rmgr
debug rsyncmgr

config redundancy unit

To configure a controller as a primary or secondary controller, use the **config redundancy unit** command.

config redundancy unit {**primary** | **secondary**}

Syntax Description

primary	Configures the controller as the primary controller.
secondary	Configures the controller as the secondary controller.

Command Default

Primary.

Usage Guidelines

When you configure a controller as the secondary controller, it becomes the HA Stakable Unit (SKU) without any valid AP licenses.

Examples

This example shows how to configure a controller as the primary controller:

```
> config redundancy unit primary
```

Related Commands

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

show redundancy peer-route

show redundancy summary

debug rmgr

debug rsyncmgr

redundancy force-switchover

To trigger a manual switch over on the active controller, use the **redundancy force-switchover** command.

redundancy force-switchover

Syntax Description This command has no arguments or keywords.

Command Default None.

Usage Guidelines When a manual switch over occurs, the active controller reboots and the standby controller takes over the network. Stateful switch over of access points (AP SSO) is supported. AP SSO ensures that the AP sessions are maintained after the standby controller takes over and the APs switch over to the standby controller. The clients on the active controller deauthenticate and join the new active controller.

Examples This example shows how to trigger a forceful switch over on the controller

```
> redundancy force-switchover
```

Related Commands

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

show redundancy peer-route

show redundancy summary

debug rmgr

debug rsyncmgr

config interface address redundancy-management

To configure the management interface IP addresses of the active and standby controllers, use the **config interface address redundancy-management** command.

config interface address redundancy-management *IP_address1* **peer-redundancy-management** *IP_address2*

Syntax Description

IP_address1	Management interface IP address of the active controller.
peer-redundancy-management	Specifies the management interface IP address of the peer controller.
IP_address2	Management interface IP address of the peer controller.

Command Default

None.

Usage Guidelines

You can use this command to check the Active-Standby reachability when the keep-alive fails and to configure an alias IP for the management port of the controller. Both the IP addresses must be in the same subnet.

Examples

This example shows how to configure the management IP addresses of the active and standby controllers:

```
> config interface address redundancy-management 209.165.201.30 peer-redundancy-management
 209.165.201.31
```

Related Commands

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

show redundancy timers

show redundancy summary

debug rmgr

debug rsyncmgr

Clear Access Point Commands

This section lists the **clear** commands to clear existing configurations, log files, and other functions for access points .

clear ap-config

To clear (reset to the default values) a lightweight access point's configuration settings, use the **clear ap-config** command.

clear ap-config *ap_name*

Syntax Description

ap_name	Access point name.

Command Default

None.

Usage Guidelines

Entering this command does not clear the static IP address of the access point.

Examples

This example shows how to clear the access point's configuration settings for the access point named ap1240_322115:

```
> clear ap-config ap1240_322115
Clear ap-config will clear ap config and reboot the AP. Are you sure you want continue?
(y/n)
```

Related Commands

show ap config

clear ap-eventlog

To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, use the **clear ap-eventlog** command.

clear ap-eventlog {**specific** *ap_name* | **all**}

Syntax Description

specific	Specifies a specific access point log file.
ap_name	Name of the access point for which the event log file will be emptied.
all	Deletes the event log for all access points joined to the controller.

Command Default

None.

Examples

This example shows how to delete the event log for all access points:

```
> clear ap-eventlog all
This will clear event log contents for all APs. Do you want continue? (y/n) :y
Any AP event log contents have been successfully cleared.
```

Related Commands

show ap eventlog

clear ap join stats

To clear the join statistics for all access points or for a specific access point, use the **clear ap join stats** command.

clear ap join stats {**all** | *ap_mac*}

Syntax Description

all	Specifies all access points.
ap_mac	Access point MAC address.

Command Default

None.

Examples

This example shows how to clear the join statistics of all the access points:

```
> clear ap join stats all
```

Related Commands

show ap config

clear ap tsm

To clear the Traffic Stream Metrics (TSM) statistics of clients associated to an access point, use the **clear ap tsm** command.

clear ap tsm {**802.11a** | **802.11b**} *cisco_ap* **all**

Syntax Description

802.11a	Clears 802.11a TSM statistics of clients associated to an access point.
802.11b	Clears 802.11b TSM statistics of clients associated to an access point.
cisco_ap	Cisco lightweight access point.
all	Clears TSM statistics of clients associated to the access point.

Command Default

None.

Examples

This example shows how to clear 802.11a TSM statistics for all clients of an access point:

```
> clear ap tsm 802.11a AP3600_1 all
```

clear lwapp private-config

To clear (reset to default values) an access point's current Lightweight Access Point Protocol (LWAPP) private configuration, which contains static IP addressing and controller IP address configurations, use the **clear lwapp private-config** command.

clear lwapp private-config

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

This command is executed from the access point console port.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

Examples

This example shows how to clear an access point's current LWAPP private configuration:

```
AP# clear lwapp private-config
removing the reap config file flash:/lwapp_reap.cfg
```

Related Commands

debug capwap

debug capwap reap

debug lwapp console cli

show capwap reap association

show capwap reap status

Debug Commands

This section lists the **debug** commands to manage debugging of access points managed by the controller.

Caution Debug commands are reserved for use only under the direction of Cisco personnel. Do not use these commands without direction from Cisco-certified staff.

debug ap

To enable or disable remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description

enable	Enables debugging on a lightweight access point. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables debugging on a lightweight access point. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

Disabled.

Examples

This example shows how to enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

This example shows how to execute the **config ap location** command on access point AP02:

```
> debug ap command "config ap location "Building 1" AP02"
```

This example shows how to execute the flash LED command on access point AP03:

```
> debug ap command "led flash 30" AP03
```

Related Commands

show sysinfo

config sysname

debug ap enable

To enable or disable remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap enable** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description

enable	Enables remote debugging. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables remote debugging.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
cisco_ap	Cisco lightweight access point name.

Command Default

None.

Examples

This example shows how to enable remote debugging on access point AP01:

```
> debug ap enable AP01
```

This example shows how to disable remote debugging on access point AP02:

```
> debug ap disable AP02
```

This example shows how to execute the flash LED command on access point AP03:

```
> debug ap command "led flash 30" AP03
```

Related Commands

show sysinfo

config sysname

debug ap packet-dump

To configure Packet Capture debug options, use the **debug ap packet-dump** command.

debug ap packet-dump {**enable** | **disable**}

Syntax Description

enable	Enables debugging of Packet Capture from an access point.
disable	Disables debugging of Packet Capture from an access point.

Command Default

Disabled.

Usage Guidelines

Packet Capture does not work during inter controller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as beacon or probe response. Only packets that flow through the radio driver in the Tx path will be captured.

Examples

This example shows how to enable debugging of Packet Capture from an access point:

```
> debug ap packet-dump enable
```

Related Commands

config ap packet-dump

show ap packet-dump status

debug ap show stats

To troubleshoot video messages and statistics of Cisco lightweight access points, use the **debug ap show stats** command.

debug ap show stats {**802.11a** | **802.11b**} *cisco_ap* {**tx-queue** | **packet** | **load** | **multicast** | **client** {*client_MAC* | **video** | **all**} | **video metrics**}

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_database_number* | **admission** | **bandwidth**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.
tx-queue	Displays the transmit queue traffic statistics of the AP.
packet	Displays the packet statistics of the AP.
load	Displays the QBSS and other statistics of the AP.
multicast	Displays the multicast supported rate statistics of the AP.
client	Displays the specified client metric statistics.
client_MAC	MAC address of the client.
video	Displays video statistics of all clients on the AP.
all	Displays statistics of all clients on the AP.
video metrics	Displays the video metric statistics.
mgid	Displays detailed multicast information for a single MGID.
mgid_database_number	L2 MGID database number.
admission	Displays video admission control on the AP.
bandwidth	Displays video bandwidth on the AP.

Command Default None.

Examples This example shows how to troubleshoot the access point AP01's transmit queue traffic on an 802.11a network:

```
> debug ap show stats 802.11a AP01 tx-queue
```

This example shows how to troubleshoot the access point AP02's multicast supported rates on an 802.11b/g network:

```
> debug ap show stats 802.11b AP02 multicast
```

This example shows how to troubleshoot the metrics of a client identified by its MAC address, associated with the access point AP01 on an 802.11a network:

```
> debug ap show stats 802.11a AP01 client 00:40:96:a8:f7:98
```

This example shows how to troubleshoot the metrics of all clients associated with the access point AP01 on an 802.11a network:

```
> debug ap show stats 802.11a AP01 client all
```

Related Commands **debug ap show stats video**

debug ap show stats video

To troubleshoot video messages and statistics of Cisco lightweight access points, use the **debug ap show stats video** command.

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_value* | **admission** | **bandwidth**}

Syntax Description

cisco_ap	Cisco lightweight access point name.
multicast mgid	Displays multicast database related information for the specified MGID of an access point.
mgid_value	Layer 2 MGID database number between 1 to 4095.
admission	Displays the video admission control.
bandwidth	Displays the video bandwidth.

Command Default

None.

Examples

This example shows how to troubleshoot the access point AP01's multicast group that is identified by the group's Layer 2 MGID database number:

```
> debug ap show stats video AP01 multicast mgid 50
```

This example shows how to troubleshoot the access point AP01's video bandwidth:

```
> debug ap show stats video AP01 bandwidth
```

Related Commands

debug ap show stats

debug capwap

To obtain troubleshooting information about Control and Provisioning of Wireless Access Points (CAPWAP) settings, use the **debug capwap** command.

debug capwap {**detail** | **dtls-keepalive** | **errors** | **events** | **hexdump** | **info** | **packet** | **payload**} {**enable** | **disable**}

Syntax Description

detail	Configures debugging for CAPWAP detail settings.
dtls-keepalive	Configures debugging for CAPWAP DTLS data keepalive packets settings.
errors	Configures debugging for CAPWAP error settings.
events	Configures debugging for CAPWAP events settings.
hexdump	Configures debugging for CAPWAP hexadecimal dump settings.
info	Configures debugging for CAPWAP info settings.
packet	Configures debugging for CAPWAP packet settings.
payload	Configures debugging for CAPWAP payload settings.
enable	Enables debugging of the CAPWAP command.
disable	Disables debugging of the CAPWAP command.

Command Default

None.

Examples

This example shows how to enable debug CAPWAP detail settings:

```
> debug capwap detail enable
```

Related Commands

clear lwapp private-config

debug disable-all

show capwap reap association

show capwap reap status

debug group

To enable or disable debugging of access point groups, use the **debug group** command.

debug group {**enable** | **disable**}

Syntax Description

enable	Enables access point group debugging.
disable	Disables access point group debugging.

Command Default

None.

Examples

This example shows how to enable debugging of access point groups:

```
> debug group enable
```

Related Commands

config guest-lan nac

config wlan apgroup

config wlan nac

debug lwapp console cli

To begin debugging the access point console CLI, use the **debug lwapp console cli** command from the access point console port.

debug lwapp console cli

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

This access point CLI command must be entered from the access point console port.

Examples

This example shows how to begin debugging the access point console:

```
AP# debug lwapp console cli
LWAPP console CLI allow/disallow debugging is on
```

Related Commands

debug disable-all

debug ap

clear lwapp private-config

debug rfac

To configure debug options of the Redundancy Framework (RFAC), use the **debug rfac** command.

debug rfac {[**packet** | **events** | **errors** | **detail**] [**enable** | **disable**]}

Syntax Description

packet	Starts debugging Redundancy Framework packets.
events	Starts debugging Redundancy Framework events.
errors	Starts debugging Redundancy Framework errors.
detail	Starts debugging Redundancy Framework details.
enable	(Optional) Starts the debugging feature.
disable	(Optional) Stops the debugging feature.

Command Default

None.

Examples

This example shows how to enable debugging of Redundancy Framework packets:

```
> debug rfac packet enable
```

Related Commands

debug rmgr

debug rsyncmgr

config interface address redundancy-management

show redundancy summary

debug rmgr

To configure Redundancy Manager (RMGR) debug options, use the **debug rmgr** command.

debug rmgr {[**packet** | **events** | **errors** | **detail**] [**enable** | **disable**]}

Syntax Description

packet	Starts debugging Redundancy Manager packets.
events	Starts debugging Redundancy Manager events.
errors	Starts debugging Redundancy Manager errors.
detail	Starts debugging Redundancy Manager details.
enable	(Optional) Starts the debugging feature.
disable	(Optional) Stops the debugging feature.

Command Default

None.

Usage Guidelines

Redundancy Manager determines the role of the controllers, maintains the keepalive messages between the peers, and initiates the switchover.

Examples

This example shows how to enable debugging of Redundancy Manager packets:

```
> debug rmgr packet enable
```

Related Commands

debug rfac

debug rsyncmgr

config interface address redundancy-management

show redundancy summary

debug rsyncmgr

To configure the debug options of the Redundancy Sync Manager (RSYNCMGR), use the **debug rsyncmgr** command.

debug rsyncmgr {**packet** | **events** | **errors** | **detail**} {**enable** | **disable**}}

Syntax Description

packet	Starts debugging Redundancy Sync Manager packets.
events	Starts debugging Redundancy Sync Manager events.
errors	Starts debugging Redundancy Sync Manager errors.
detail	Starts debugging Redundancy Sync Manager details.
enable	Starts the debugging feature.
disable	Stops the debugging feature.

Command Default

None.

Usage Guidelines

Redundancy Synchronization Manager synchronizes the configurations of the active and standby controllers.

Examples

This example shows how to enable debugging of Redundancy Sync Manager packets:

```
> debug rsyncmgr packet enable
```

Related Commands

debug rfac

debug rmgr

config interface address redundancy-management

show redundancy summary

debug service ap-monitor

To debug the access point monitor service, use the **debug service ap-monitor** command.

debug service ap-monitor {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all access point status messages.
error	Configures debugging of access point monitor error events.
event	Configures debugging of access point monitor events.
nmsp	Configures debugging of access point monitor Network Mobility Services Protocol (NMSP) events.
packet	Configures debugging of access point monitor packets.
enable	Enables debugging for access point monitor service.
disable	Disables debugging for access point monitor service.

Command Default

None.

Examples

This example shows how to debug access point monitor NMSP events:

```
> debug service ap-monitor events
```

Related Commands

debug disable-all

show snmp status

transfer upload peer-start

To upload a file to the peer controller, use the **transfer upload peer-start** command.

transfer upload peer-start

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to start uploading a file to the peer controller:

```
> transfer upload peer-start
Mode..................................... FTP
FTP Server IP............................ 209.165.201.1
FTP Server Port.......................... 21
FTP Path................................. /builds/nimm/
FTP Filename............................. AS_5500_7_4_1_20.aes
FTP Username............................. wnbu
FTP Password............................. *********
Data Type................................ Error Log

Are you sure you want to start upload from standby? (y/N) n

Transfer Canceled
```

Related Commands

clear transfer

transfer upload filename

transfer upload mode

transfer upload pac

transfer upload password

transfer upload path

transfer upload port

transfer upload serverip

transfer upload datatype

transfer upload username

Resetting the System Reboot Time

Use the **reset** command to schedule a reboot of the controller and access points.

reset system at

To reset the system at a specified time, use the **reset system at** command.

reset system at YYYY-MM-DD HH:**MM**:**SS image** {**no-swap**|**swap**} **reset-aps** [**save-config**]

Syntax Description

YYYY-MM-DD	Specifies the date.
HH: MM: SS	Specifies the time in a 24-hour format.
image	Configures the image to be rebooted.
swap	Changes the active boot image.
no-swap	Boots from the active image.
reset-aps	Resets all access points during the system reset.
save-config	(Optional) Saves the configuration before the system reset.

Command Default

None.

Examples

This example shows how to reset the system at 2010-03-29 and 12:01:01 time:

```
> reset system at 2010-03-29 12:01:01 image swap reset-aps save-config
```

Related Commands

reset system notify-time

reset system in

reset system in

To specify the amount of time delay before the devices reboot, use the **reset system in** command.

reset system in HH:**MM**:**SS image** {**swap** | **no-swap**} **reset-aps save-config**

Syntax Description

HH :MM :SS	Specifies a delay in duration.
image	Configures the image to be rebooted.
swap	Changes the active boot image.
no-swap	Boots from the active image.
reset-aps	Resets all access points during the system reset.
save-config	Saves the configuration before the system reset.

Command Default

None.

Examples

This example shows how to reset the system after a delay of 00:01:01:

```
> reset system in 00:01:01 image swap reset-aps save-config
```

Related Commands

reset system notify-time

reset system at

reset system cancel

To cancel a scheduled reset, use the **reset system cancel** command.

reset system cancel

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to cancel a scheduled reset:

```
> reset system cancel
```

Related Commands

reset system at

reset system in

reset system notify-time

reset system notify-time

To configure the trap generation prior to scheduled resets, use the **reset system notify-time** command.

reset system notify-time *minutes*

Syntax Description

minutes	Number of minutes before each scheduled reset at which to generate a trap.

Command Default

The default is 10 minutes.

Examples

This example shows how to configure the trap generation to 10 minutes before the scheduled resets:

```
> reset system notify-time 55
```

Related Commands

reset system in

reset system at

reset peer-system

To reset the peer controller, use the **reset peer-system** command.

reset peer-system

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to reset the peer controller:

```
> reset peer-system
```

Related Commands **reset system notify-time**

reset system in

Test Commands

This section lists the **test** commands for access points.

test ap pmtu

To enable or disable the Path Maximum Transmission Unit (PMTU) on the CAPWAP tunnel of a Cisco access point, use the **test ap** command.

test ap pmtu {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Disables PMTU on the CAPWAP tunnel of a Cisco access point.
disable	Enables PMTU on the CAPWAP tunnel of a Cisco access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None.

Examples

This example shows how to enable PMTU on the CAPWAP tunnel of a Cisco access point:

```
> test ap pmtu enable AP1600_1
```

Related Commands

test ap

test capwap

test ccx

test cleanair

test ftpstatus

test lic-agent

test license

test log

test make-space

test media

test reader

test redundancy

test rrm

test sip-cac-fail

test token-bucket

test wlan

test capwap

To configure an access point to send broadcast radio measurement requests to clients, or to enable the encryption of control packets that are sent between the access point and the controller, use the **test capwap** command.

test capwap {**message** *token cisco_ap* | **encr** *cisco_ap* {**enable** | **disable**}}

Syntax Description

message	Configures the access point to send a broadcast radio measurement requests to clients.
token	Time interval for the access point to send a broadcast radio measurement requests to clients.
cisco_ap	Name of the Cisco lightweight access point.
encr	Encrypts or decrypts the control packets that are sent between the access point and the controller.
enable	Enables the encryption or decryption of control packets that are sent between the access point and the controller.
disable	Disables the encryption or decryption of control packets that are sent between the access point and the controller.

Command Default

None.

Examples

This example shows how to enable encryption of control packets:

```
> test capwap encr A_1500_1 enable
```

Related Commands

test ap

test capwap

test ccx

test cleanair

test ftpstatus

test lic-agent

test license

test log

test make-space

test media

test reader

test redundancy

test rrm

test sip-cac-fail

test token-bucket

test wlan