



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, page 1](#)
- [Config Commands, page 51](#)
- [Clear Commands, page 287](#)
- [Debug Commands, page 290](#)
- [Test Commands, page 304](#)

Show Commands

This section lists the **show** commands to display information about your WLAN configuration settings.

Show Client Commands

This section lists the **show client** commands to display information about your client configuration settings.

show client ccx client-capability

To display the client's capability information, use the **show client ccx client-capability** command.

show client ccx client-capability *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Usage Guidelines

This command displays the client's available capabilities, not the current settings for the capabilities.

Examples

This example shows how to display the client's capability:

```
> show client ccx client-capability 00:40:96:a8:f7:98
Service Capability..... Voice, Streaming(uni-directional)
Video, Interactive(bi-directional) Video
Radio Type..... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)
Radio Type..... DSSS
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List(MB)..... 1.0 2.0
Radio Type..... HRDSSS(802.11b)
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List(MB)..... 5.5 11.0
Radio Type..... ERP(802.11g)
Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
Tx Power Mode..... Automatic
Rate List(MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Are you sure you want to start? (y/N)y Are you sure you want to start? (y/N)
```

Related Commands

config client ccx get-client-capability
config client ccx get-operating-parameters
config client ccx get-profiles
config client ccx stats-request
config client ccx operating-parameters
config client ccx profiles
config client ccx stats-report

show client ccx frame-data

To display the data frames sent from the client for the last test, use the **show client ccx frame-data** command.

```
show client ccx frame-data client_mac_address
```

Syntax Description

client_mac_address MAC address of the client.

Examples

This example shows how to display the data frame sent from the client for the last test:

```
> show client ccx frame-data  
xx:xx:xx:xx:xx:xx
```

show client ccx last-response-status

To display the status of the last test response, use the **show client ccx last-response-status** command.

show client ccx last-response-status *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to display the status of the last test response:

```
> show client ccx last-response-status
Test Status ..... Success
Response Dialog Token..... 87
Response Status..... Successful
Response Test Type..... 802.1x Authentication Test
Response Time..... 3476 seconds since system boot
```

Related Commands

config client ccx clear-reports
config client ccx clear-results
config client ccx default-gw-ping
config client ccx dhcp-test
config client ccx log-request
config client ccx last-response-status
config client ccx last-test-status

show client ccx last-test-status

To display the status of the last test, use the **show client ccx last-test-status** command.

```
show client ccx last-test-status client_mac_address
```

Syntax Description

client_mac_address MAC address of the client.

Examples

This example shows how to display the status of the last test of the client:

```
> show client ccx last-test-status

Test Type ..... Gateway Ping Test
Test Status ..... Pending/Success/Timeout
Dialog Token ..... 15
Timeout ..... 15000 ms
Request Time ..... 1329 seconds since system boot
```

Related Commands

config client ccx clear-reports

config client ccx clear-results

config client ccx default-gw-ping

config client ccx dhcp-test

config client ccx log-request

config client ccx last-response-status

show client ccx log-response

To display a log response, use the **show client ccx log-response** command.

show client ccx log-response {roam | rsna | syslog} *client_mac_address*

Syntax Description

roam	(Optional) Displays the CCX client roaming log response.
rsna	(Optional) Displays the CCX client RSNA log response.
syslog	(Optional) Displays the CCX client system log response.
<i>client_mac_address</i>	Inventory for the specified access point.

Command Default

None.

Examples

This example shows how to display the system log response:

```
> show client ccx log-response syslog 00:40:96:a8:f7:98
Tue Jun 26 18:07:48 2007      Syslog Response LogID=131: Status=Successful
    Event Timestamp=0d 00h 19m 42s 278987us
    Client SysLog = '<11> Jun 19 11:49:47 unravall3777 Mandatory elements missing in the
OID response'
    Event Timestamp=0d 00h 19m 42s 278990us
    Client SysLog = '<11> Jun 19 11:49:47 unravall3777 Mandatory elements missing in the
OID response'
Tue Jun 26 18:07:48 2007      Syslog Response LogID=131: Status=Successful
    Event Timestamp=0d 00h 19m 42s 278987us
    Client SysLog = '<11> Jun 19 11:49:47 unravall3777 Mandatory elements missing in the
OID response'
    Event Timestamp=0d 00h 19m 42s 278990us
    Client SysLog = '<11> Jun 19 11:49:47 unravall3777 Mandatory elements missing in the
OID response'
```

This example shows how to display the client roaming log response:

```
> show client ccx log-response roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2007      Roaming Response LogID=20: Status=Successful
Event Timestamp=0d 00h 00m 13s 322396us      Source BSSID=00:40:96:a8:f7:98
Target BSSID=00:0b:85:23:26:70,      Transition Time=100(ms)
Transition Reason: Normal roam, poor link      Transition Result: Success
Thu Jun 22 11:55:14 2007      Roaming Response LogID=133: Status=Successful
Event Timestamp=0d 00h 00m 16s 599006us      Source BSSID=00:0b:85:81:06:c2
Target BSSID=00:0b:85:81:06:c2,      Transition Time=3235(ms)
Transition Reason: Normal roam, poor link      Transition Result: Success
Thu Jun 22 18:28:48 2007      Roaming Response LogID=133: Status=Successful
Event Timestamp=0d 00h 00m 08s 815477us      Source BSSID=00:0b:85:81:06:c2
Target BSSID=00:0b:85:81:06:d2,      Transition Time=3281(ms)
Transition Reason: First association to WLAN      Transition Result: Success
```

Related Commands

config client ccx log-request

show client ccx manufacturer-info

To display the client manufacturing information, use the **show client ccx manufacturer-info** command.

show client ccx manufacturer-info *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Examples

This example shows how to display the client manufacturing information:

```
> show client ccx manufacturer-info 00:40:96:a8:f7:98
Manufacturer OUI ..... 00:40:96
Manufacturer ID ..... Cisco
Manufacturer Model ..... Cisco Aironet 802.11a/b/g Wireless Adapter
Manufacturer Serial ..... FOC1046N3SX
Mac Address ..... 00:40:96:b2:8d:5e
Radio Type ..... DSSS OFDM(802.11a) HRDSSS(802.11b)
  ERP(802.11g)
Antenna Type ..... Omni-directional diversity
Antenna Gain ..... 2 dBi
Rx Sensitivity:
Radio Type ..... DSSS
Rx Sensitivity ..... Rate:1.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:2.0 Mbps, MinRssi:-95, MaxRss1:-30
Radio Type ..... HRDSSS(802.11b)
Rx Sensitivity ..... Rate:5.5 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:11.0 Mbps, MinRssi:-95, MaxRss1:-30
Radio Type ..... ERP(802.11g)
Rx Sensitivity ..... Rate:6.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:9.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:12.0 Mbps, MinRssi:-95, MaxRss1:-30
Rx Sensitivity ..... Rate:18.0 Mbps, MinRss1:-95, MaxRss1:-30
```

Related Commands

config client ccx get-client-capability
config client ccx get-operating-parameters
config client ccx get-profiles
config client ccx get-manufacturer-info

show client ccx operating-parameters

To display the client operating-parameters, use the **show client ccx operating-parameters** command.

show client ccx operating-parameters *client_mac_address*

Syntax Description

<i>client_mac_address</i>	MAC address of the client.
---------------------------	----------------------------

Command Default

None.

Examples

This example shows how to display the client operating parameters:

```
> show client ccx operating-parameters 00:40:96:b2:8d:5e
Client Mac ..... 00:40:96:b2:8d:5e
Radio Type ..... OFDM(802.11a)
Radio Type ..... OFDM(802.11a)
Radio Channels ..... 36 40 44 48 52 56 60 64 100 104 108 112
116 120 124 128 132 136 140 149 153 157 161 165
Tx Power Mode ..... Automatic
Rate List(MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Power Save Mode ..... Normal Power Save
SSID ..... wifi
Security Parameters[EAP Method, Credential]..... None
Auth Method ..... None
Key Management..... None
Encryption ..... None
Device Name ..... Wireless Network Connection 15
Device Type ..... 0
OS Id ..... Windows XP
OS Version ..... 5.1.6.2600 Service Pack 2
IP Type ..... DHCP address
IPv4 Address ..... Available
IP Address ..... 70.0.4.66
Subnet Mask ..... 255.0.0.0
Default Gateway ..... 70.1.0.1
IPv6 Address ..... Not Available
IPv6 Address ..... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
IPv6 Subnet Mask ..... 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
DNS Servers ..... 103.0.48.0
WINS Servers .....
System Name ..... URAVAL3777
Firmware Version ..... 4.0.0.187
Driver Version ..... 4.0.0.187
```

Related Commands

config client ccx get-client-capability
config client ccx get-operating-parameters
config client ccx get-profiles
config client ccx get-manufacturer-info

show client ccx profiles

To display the client profiles, use the **show client ccx profiles** command.

show client ccx profiles *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to display the client profiles:

```
> show client ccx profiles 00:40:96:15:21:ac
Number of Profiles ..... 1
Current Profile ..... 1
Profile ID ..... 1
Profile Name ..... wifiEAP
SSID ..... wifiEAP
Security Parameters [EAP Method, Credential]..... EAP-TLS, Host OS Login Credentials
Auth Method ..... EAP
Key Management ..... WPA2+CCKM
Encryption ..... AES-CCMP
Power Save Mode ..... Constantly Awake
Radio Configuration:
Radio Type..... DSSS
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
  Data Retries..... 6
  Fragment Threshold..... 2342
  Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode..... Automatic
  Rate List (MB)..... 1.0 2.0
Radio Type..... HRDSSS(802.11b)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
  Data Retries..... 6
  Fragment Threshold..... 2342
  Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode..... Automatic
  Rate List (MB)..... 5.5 11.0
Radio Type..... ERP(802.11g)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
  Data Retries..... 6
  Fragment Threshold..... 2342
  Radio Channels..... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode..... Automatic
  Rate List (MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Radio Type..... OFDM(802.11a)
  Preamble Type..... Long preamble
  CCA Method..... Energy Detect + Carrier
Detect/Correlation
  Data Retries..... 6
  Fragment Threshold..... 2342
  Radio Channels..... 36 40 44 48 52 56 60 64 149 153 157 161
  165
```

```
Tx Power Mode..... Automatic
Rate List (MB)..... 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

Related Commands

config client ccx get-client-capability
config client ccx get-operating-parameters
config client ccx get-profiles
config client ccx get-manufacturer-info

show client ccx results

To display the results from the last successful diagnostic test, use the **show client ccx results** command.

show client ccx results *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to display the results from the last successful diagnostic test:

```
> show client ccx results xx.xx.xx.xx
dot1x Complete..... Success
EAP Method..... *1,Host OS Login Credentials
dot1x Status..... 255
```

Related Commands

config client ccx test-abort
config client ccx test-association
config client ccx test-dot1x
config client ccx clear-reports
config client ccx clear-results
config client ccx test-profile

show client ccx rm

To display Cisco Client eXtension (CCX) client radio management report information, use the **show client ccx rm** commands.

```
show client ccx rm client_MAC {status | {report {chan-load | noise-hist | frame | beacon | pathloss}}}
```

Syntax Description

<i>client_MAC</i>	Client MAC address.
status	Displays the client CCX radio management status information.
report	Displays the client CCX radio management report.
chan-load	Displays radio management channel load reports.
noise-hist	Displays radio management noise histogram reports.
beacon	Displays radio management beacon load reports.
frame	Displays radio management frame reports.
pathloss	Displays radio management path loss reports.

Command Default

None.

Examples

This example shows how to display the client radio management status information:

```
> show client ccx rm 00:40:96:15:21:ac status
Client Mac Address..... 00:40:96:15:21:ac
Channel Load Request..... Enabled
Noise Histogram Request..... Enabled
Beacon Request..... Enabled
Frame Request..... Enabled
Interval..... 30
Iteration..... 10
```

This example shows how to display the client radio management load reports:

```
> show client ccx rm 00:40:96:15:21:ac report chan-load
Channel Load Report
Client Mac Address..... 00:40:96:ae:53:bc
Timestamp..... 788751121
Incapable Flag..... On
Refused Flag..... On
Chan CCA Busy Fraction
-----
1 194
2 86
3 103
4 0
5 178
6 82
```

```
7 103
8 95
9 13
10 222
11 75
```

This example shows how to display the client radio management noise histogram reports:

```
> show client ccx rm 00:40:96:15:21:ac report noise-hist
Noise Histogram Report
Client Mac Address..... 00:40:96:15:21:ac
Timestamp..... 4294967295
Incapable Flag..... Off
Refused Flag..... Off
Chan RPI0 RPI1 RPI2 RPI3 RPI4 RPI5 RPI6 RPI7
```

Related Commands

config client ccx default-gw-ping

config client ccx dhcp-test

show client ccx stats-report

To display the Cisco Client eXtensions (CCX) statistics report from a specified client device, use the **show client ccx stats-report** command.

show client ccx stats-report *client_mac_address*

Syntax Description

client_mac_address Client MAC address.

Command Default

None.

Examples

This example shows how to displays the statistics report:

```
> show client ccx stats-report 00:0c:41:07:33:a6
Measurement duration = 1
dot11TransmittedFragmentCount = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount = 3
dot11RetryCount = 4
dot11MultipleRetryCount = 5
dot11FrameDuplicateCount = 6
dot11RTSSuccessCount = 7
dot11RTSFailureCount = 8
dot11ACKFailureCount = 9
dot11ReceivedFragmentCount = 10
dot11MulticastReceivedFrameCount = 11
dot11FCSErrorCount = 12
dot11TransmittedFrameCount = 13
```

Related Commands

config client ccx default-gw-ping
config client ccx dhcp-test
config client ccx dns-ping

show client detail

To display detailed information for a client on a Cisco lightweight access point, use the **show client detail** command.

show client detail *mac_address*

Syntax Description

<i>mac_address</i>	Client MAC address.
--------------------	---------------------

Command Default

None.

Usage Guidelines

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

Examples

This example shows how to display the client detailed information:

```
> show client detail 00:0c:41:07:33:a6
Policy Manager State.....POSTURE_REQD
Policy Manager Rule Created.....Yes
Client MAC Address..... 00:16:36:40:ac:58
Client Username..... N/A
Client State..... Associated
Client NAC OOB State..... QUARANTINE
Guest LAN Id..... 1
IP Address..... Unknown
Session Timeout..... 0
QoS Level..... Platinum
802.1P Priority Tag..... disabled
KTS CAC Capability..... Yes
WMM Support..... Enabled
Power Save..... ON
Diff Serv Code Point (DSCP)..... disabled
Mobility State..... Local
Internal Mobility State..... apFMsMmInitial
Security Policy Completed..... No
Policy Manager State..... WEBAUTH_REQD
Policy Manager Rule Created..... Yes
NPU Fast Fast Notified..... Yes
Last Policy Manager State..... WEBAUTH_REQD
Client Entry Create Time..... 460 seconds
Interface..... wired-guest
FlexConnect Authentication..... Local
FlexConnect Data Switching..... Local
VLAN..... 236
Quarantine VLAN..... 0
Client Statistics:
  Number of Bytes Received..... 66806
    Number of Data Bytes Received..... 160783
    Number of Realtime Bytes Received..... 160783
    Number of Data Bytes Sent..... 23436
    Number of Realtime Bytes Sent..... 23436
    Number of Data Packets Received..... 592
    Number of Realtime Packets Received..... 592
    Number of Data Packets Sent..... 131
    Number of Realtime Packets Sent..... 131
    Number of Interim-Update Sent..... 0
    Number of EAP Id Request Msg Timeouts..... 0
```

```
Number of EAP Request Msg Timeouts..... 0
Number of EAP Key Msg Timeouts..... 0
Number of Data Retries..... 0
Number of RTS Retries..... 0
Number of Duplicate Received Packets..... 3
Number of Decrypt Failed Packets..... 0
Number of Mic Failed Packets..... 0
Number of Mic Missing Packets..... 0
Number of RA Packets Dropped..... 6
Number of Policy Errors..... 0
Radio Signal Strength Indicator..... -50 dBm
Signal to Noise Ratio..... 43 dB
...
```

Related Commands **show client summary**

show client location-calibration summary

To display client location calibration summary information, use the **show client location-calibration summary** command.

show client location-calibration summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the location calibration summary information:

```
> show client location-calibration summary
MAC Address Interval
-----
10:10:10:10:10:10 60
21:21:21:21:21:21 45
```

Related Commands

- show client summary**
- show client summary guest-lan**

show client probing

To display the number of probing clients, use the **show client probing** command.

show client probing

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the number of probing clients:

```
> show client probing
Number of Probing Clients..... 0
```

Related Commands **show client summary**
show client summary guest-lan

show client roam-history

To display the roaming history of a specified client, use the **show client roam-history** command.

show client roam-history *mac_address*

Syntax Description

mac_address Client MAC address.

Command Default

None.

Examples

This example shows how to display the roaming history of a specified client:

```
> show client roam-history 00:14:6c:0a:57:77
```

show client summary

To display a summary of clients associated with a Cisco lightweight access point, use the **show client summary** command.

show client summary

Syntax Description This command has no arguments or keywords.

Command Default None.

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

Examples This example shows how to display a summary of the active clients:

```
> show client summary
Number of Clients..... 24
Number of PMIPv6 Clients..... 200
MAC Address      AP Name          Status          WLAN/GLAN/RLAN Auth Protocol      Port
Wired  PMIPv6
-----
-----
00:00:15:01:00:01 NMSP-TalwarSIM1-2 Associated      1              Yes  802.11a      13
  No      Yes
00:00:15:01:00:02 NMSP-TalwarSIM1-2 Associated      1              Yes  802.11a      13
  No      No
00:00:15:01:00:03 NMSP-TalwarSIM1-2 Associated      1              Yes  802.11a      13
  No      Yes
00:00:15:01:00:04 NMSP-TalwarSIM1-2 Associated      1              Yes  802.11a      13
  No      No
```

Related Commands **show client summary guest-lan**

Show IPv6 Commands

Use the **show ipv6** commands to display the IPv6 settings and information.

show ipv6 acl

To display the IPv6 access control lists (ACLs) that are configured on the controller, use the **show ipv6 acl** command.

show ipv6 acl detailed {*acl_name* | **summary**}

Syntax Description

<i>acl_name</i>	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
detailed	Displays detailed information about a specific ACL.

Command Default

None.

Examples

This example shows how to display the detailed information of the access control lists:

```
> show ipv6 acl detailed acl6
Rule Index..... 1
Direction..... Any
IPv6 source prefix..... ::/0
IPv6 destination prefix..... ::/0
Protocol..... Any
Source Port Range..... 0-65535
Destination Port Range..... 0-65535
DSCP..... Any
Flow label..... 0
Action..... Permit
Counter..... 0
Deny Counter..... 0
```

Related Commands

config ipv6 acl

show ipv6 neighbor-binding

To display the IPv6 Neighbor Binding data that are configured on the controller, use the **show ipv6 neighbor-binding** command.

show ipv6 neighbor-binding {**capture-policy** | **counters** | **detailed** {**mac** *mac_address* | **port** *port_number* | **vlan** *vlan_id*} | **features** | **policies** | **ra-throttle** {**statistics** *vlan_id* | **routers** *vlan_id*} | **summary**}

Syntax Description

capture-policy	Displays IPv6 next-hop message capture policies.
counters	Displays IPv6 next-hop counters.
detailed	Displays the IPv6 neighbor binding table.
mac	Displays the IPv6 binding table entries for a specific MAC address.
<i>mac_address</i>	Displays the IPv6 binding table entries for a specific MAC address.
port	Displays the IPv6 binding table entries for a specific port.
<i>port_number</i>	Port Number. You can enter ap for an access point or LAG for a LAG port.
vlan	Displays the IPv6 neighbor binding table entries for a specific VLAN.
<i>vlan_id</i>	VLAN identifier.
features	Displays IPv6 next-hop registered features.
policies	Displays IPv6 next-hop policies.
ra-throttle	Displays RA throttle information.
statistics	Displays RA throttle statistics.
routers	Displays RA throttle routers.
summary	Displays the IPv6 neighbor binding table.

Command Default

None.

Examples

This example shows how to display the IPv6 neighbor binding data summary:

```
> show ipv6 neighbor-binding summary
Binding Table has 6 entries, 5 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DDCP
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk      0004:Orig access
0008:Orig trusted access    0010:Orig trusted trunk  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
   IPv6 address                MAC Address          Port VLAN Type      prlvl age
   state      Time left
-----
ND fe80::216:46ff:fe43:eb01    00:16:46:43:eb01    1  980 wired          0005
  2 REACHABLE 157
ND fe80::9cf9:b009:b1b4:1ed9  70:f1:a1:dd:cb:d4   AP  980 wireless       0005
  2 REACHABLE 157
ND fe80::6233:4bff:fe05:25ef  60:33:4b:05:25:ef  AP  980 wireless       0005
  2 REACHABLE 203
ND fe80::250:56ff:fe8b:4a8f    00:50:56:8b:4a:8f  AP  980 wireless       0005
  2 REACHABLE 157
ND 2001:410:0:1:51be:2219:56c6:a8ad  70:f1:a1:dd:cb:d4   AP  980 wireless       0005
  5 REACHABLE 157
S  2001:410:0:1::9             00:00:00:00:00:08   AP  980 wireless       0100
  1 REACHABLE 205
```

Examples

This example shows how to display the detailed IPv6 neighbor binding data:

```
> show ipv6 neighbor-binding detailed mac 60:33:4b:05:25:ef
macDB has 3 entries for mac 60:33:4b:05:25:ef, 3 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DDCP
Preflevel flags (prlvl):
0001:MAC and LLA match      0002:Orig trunk      0004:Orig access
0008:Orig trusted access    0010:Orig trusted trunk  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated  0100:Statically assigned
   IPv6 address                MAC Address          Port VLAN Type      prlvl age
   state      Time left
-----
ND fe80::6233:4bff:fe05:25ef    60:33:4b:05:25:ef  AP  980 wireless       0009
  0 REACHABLE 303
ND 2001:420:0:1:6233:4bff:fe05:25ef  60:33:4b:05:25:ef  AP  980 wireless       0009
  0 REACHABLE 300
ND 2001:410:0:1:6233:4bff:fe05:25ef  60:33:4b:05:25:ef  AP  980 wireless       0009
  0 REACHABLE 301
```

Related Commands

config ipv6 neighbor-binding

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 ipv6 summary

To display the IPv6 configuration settings, use the **show ipv6 summary** command.

show ipv6 summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the IPv6 configuration settings:

```
> show ipv6 summary
Global Config..... Enabled
Reachable-lifetime value..... 300
Stale-lifetime value..... 86400
Down-lifetime value..... 86400
RA Throttling..... Enabled
RA Throttling allow at-least..... 1
RA Throttling allow at-most..... no-limit
RA Throttling max-through..... no-limit
RA Throttling throttle-period..... 60
RA Throttling interval-option..... throttle
NS Multicast CacheMiss Forwarding..... Disabled
```

Related Commands **show ipv6 acl**

Show RF-Profile Commands

Use the **show RF-Profile** commands to display RF profiles details.

show rf-profile summary

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

show rf-profile summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the summary of RF profile:

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

Related Commands

- show rf-profile details**
- config wlan band-select allow**
- config rf-profile client-trap-threshold**
- config rf-profile coverage**
- config rf-profile create**
- config rf-profile data-rates**
- config rf-profile delete**
- config rf-profile description**
- config rf-profile load-balancing**
- config rf-profile max-clients**
- config rf-profile multicast**
- config rf-profile out-of-box**
- config rf-profile tx-power-control-thresh-v1**
- config rf-profile tx-power-control-thresh-v2**
- config rf-profile tx-power-max**
- config rf-profile tx-power-min**

show rf-profile details

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

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

Syntax Description

<i>rf-profile-name</i>	Name of the RF profile.
------------------------	-------------------------

Command Default

None.

Examples

This example shows how to display the details of an RF profile:

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

Related Commands

show rf-profile summary
config wlan band-select allow
config rf-profile client-trap-threshold
config rf-profile coverage
config rf-profile create

`config rf-profile data-rates`
`config rf-profile delete`
`config rf-profile description`
`config rf-profile load-balancing`
`config rf-profile max-clients`
`config rf-profile multicast`
`config rf-profile out-of-box`
`config rf-profile tx-power-control-thresh-v1`
`config rf-profile tx-power-control-thresh-v2`
`config rf-profile tx-power-max`
`config rf-profile tx-power-min`

Other Show Commands

show advanced hotspot

To display the advanced HotSpot parameters, use the **show advanced hotspot** command.

show advanced hotspot

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the advanced HotSpot parameters:

```
> show advanced hotspot
ANQP 4-way state..... Disabled
GARP Broadcast state: ..... Enabled
GAS request rate limit ..... Disabled
ANQP comeback delay in TUs(TU=1024usec)..... 50
```

Related Commands

- show wlan
- debug hotspot events
- debug hotspot packets
- config wlan apgroup hotspot
- config wlan hotspot
- config ap hotspot venue
- config advanced hotspot
- config wlan security wpa gtk-random

show avc statistics wlan

To display the Application Visibility and Control (AVC) statistics of a WLAN, use the **show avc statistics wlan** command.

```
show avc statistics wlan wlan_id {application application_name | top-app-groups [upstream | downstream] | top-apps [upstream | downstream]}
```

Syntax Description

<i>wlan_id</i>	WLAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
<i>application_name</i>	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None.

Examples

This example shows how to display the AVC statistics of a WLAN:

```
> show avc statistics wlan 1
Application-Name      Packets   Bytes   Avg Pkt   Packets   Bytes
  (Up/Down)           (n secs) (n secs) Size      (Total)   (Total)
=====
unclassified          (U) 191464   208627    1       92208613  11138796586
                    (D) 63427   53440610  842     16295621  9657054635
ftp                   (U) 805      72880     90      172939    11206202
                    (D) 911      58143     63      190900    17418653
http                  (U) 264904   12508288  47      27493945  2837672192
                    (D) 319894   436915253 1365    29850934  36817587924
gre                   (U) 0         0         0       10158872  10402684928
                    (D) 0         0         0         0         0
icmp                  (U) 1         40        40      323       98476
                    (D) 7262     4034576   555     2888266   1605133372
ipinip                (U) 62565    64066560 1024    11992305  12280120320
                    (D) 0         0         0         0         0
imap                  (U) 1430     16798     11      305161    3795766
                    (D) 1555     576371    370     332290    125799465
irc                   (U) 9         74        8       1736     9133
                    (D) 11        371       33      1972     173381
nntp                  (U) 22        158       7       1705     9612
                    (D) 22        372       16      2047     214391
```

This example shows how to display the AVC statistics of an FTP application for a WLAN:

```
> show avc statistics wlan 1 application ftp
Description           Upstream   Downstream
=====

```

Number of Packtes(n secs)	0	0
Number of Bytes(n secs)	0	0
Average Packet size(n secs)	0	0
Total Number of Packtes	32459	64888
Total Number of Bytes	274	94673983

Related Commands

- config avc profile delete**
- config avc profile create**
- config avc profile rule**
- config wlan avc**
- show avc profile**
- show avc applications**
- show avc statistics client**
- show avc statistics applications**
- show avc statistics top-apps**
- show avc statistics guest-lan**
- show avc statistics remote-lan**
- debug avc error**
- debug avc events**

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.
<i>cisco_ap</i>	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 call-control client

To see call information for a call-aware client when Voice-over-IP (VoIP) snooping is enabled and the call is active, use the **show call-control client** command

show call-control client callInfo *client_MAC_address*

Syntax Description

callInfo Specifies the call-control information.

client_MAC_address Client MAC address.

Command Default

None.

Examples

This example shows how to display the call information such as the IP port for calls related to the client:

```
> show call-control client callInfo 10.10.10.10.10.10
Uplink IP/port..... 0.0.0.0 / 0
Downlink IP/port..... 9.47.96.107 / 5006
UP..... 6
Calling Party..... sip:1021
Called Party..... sip:1000
Call ID..... 38423970c3fca477
Call on hold: ..... FALSE
Number of calls for given client is..... 1
```

Related Commands

show call-control ap

show dhcp

To display the internal Dynamic Host Configuration Protocol (DHCP) server configuration, use the **show dhcp** command.

```
show dhcp {leases | summary | scope}
```

Syntax Description

leases	Displays allocated DHCP leases.
summary	Displays DHCP summary information.
<i>scope</i>	Name of a scope to display the DHCP information for that scope.

Command Default

None.

Examples

This example shows how to display the allocated DHCP leases:

```
> show dhcp leases
No leases allocated.
```

This example shows how to display the DHCP summary information:

```
> show dhcp summary
Scope Name      Enabled      Address Range
003              No           0.0.0.0 -> 0.0.0.0
```

This example shows how to display the DHCP information for the scope 003:

```
> show dhcp 003
Enabled..... No
Lease Time..... 0
Pool Start..... 0.0.0.0
Pool End..... 0.0.0.0
Network..... 0.0.0.0
Netmask..... 0.0.0.0
Default Routers..... 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain.....
DNS..... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers..... 0.0.0.0 0.0.0.0 0.0.0.0
```

Related Commands

```
config dhcp proxy
config dhcp timeout
config interface dhcp
config wlan dhcp server
debug dhcp
debug dhcp service-port
debug disable-all
```

```
config dhcp  
show dhcp proxy
```

show dhcp proxy

To display the status of DHCP proxy handling, use the **show dhcp proxy** command.

show dhcp proxy

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the status of DHCP proxy information:

```
> show dhcp proxy
DHCP Proxy Behavior: enabled
```

Related Commands

- config dhcp proxy
- config dhcp timeout
- config interface dhcp
- config wlan dhcp_server
- debug dhcp
- debug dhcp service-port
- debug disable-all
- show dhcp
- config dhcp

show dhcp timeout

To display the DHCP timeout value, use the **show dhcp timeout** command.

show dhcp timeout

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display the DHCP timeout value:

```
> show dhcp timeout
DHCP Timeout (seconds)..... 10
```

Related Commands

- config dhcp proxy**
- config dhcp**
- config interface dhcp**
- config wlan dhcp_server**
- debug dhcp**
- debug dhcp service-port**
- debug disable-all**
- show dhcp**
- show dhcp proxy**

show guest-lan

To display the configuration of a specific wired guest LAN, use the **show guest-lan** command.

show guest-lan *guest_lan_id*

Syntax Description

<i>guest_lan_id</i>	ID of selected wired guest LAN.
---------------------	---------------------------------

Command Default

None.

Usage Guidelines

To display all wired guest LANs configured on the controller, use the **show guest-lan summary** command.

Examples

This example shows how to display the guest LAN configuration:

```
> show guest-lan 2
Guest LAN Identifier..... 1
Profile Name..... guestlan
Network Name (SSID)..... guestlan
Status..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wired
Ingress Interface..... wired-guest
WLAN ACL..... unconfigured
DHCP Server..... 10.20.236.90
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
Security
  Web Based Authentication..... Enabled
  ACL..... Unconfigured
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Auto Anchor..... Disabled
Mobility Anchor List
GLAN ID IP Address Status
```

Related Commands

config guest-lan
config guest-lan custom-web ext-webauth-url
config guest-lan custom-web global disable
config guest-lan custom-web login_page
config guest-lan nac
config guest-lan security

show macfilter

To display the MAC filter parameters, use the **show macfilter** command.

show macfilter {**summary** | **detail** *MAC*}

Syntax Description

summary	Displays a summary of all MAC filter entries.
detail <i>MAC</i>	Displays details of a MAC filter entry.

Command Default

None.

Usage Guidelines

The MAC delimiter (none, colon, or hyphen) for MAC addresses sent to RADIUS servers is displayed. The MAC filter table lists the clients that are always allowed to associate with a wireless LAN.

Examples

This example shows how to display the detailed display of a MAC filter entry:

```
> show macfilter detail xx:xx:xx:xx:xx:xx
MAC Address..... xx:xx:xx:xx:xx:xx
WLAN Identifier..... Any
Interface Name..... management
Description..... RAP
```

This example shows how to display a summary of the MAC filter parameters:

```
> show macfilter summary
MAC Filter RADIUS Compatibility mode..... Cisco ACS
MAC Filter Delimiter..... None
Local Mac Filter Table
MAC Address          WLAN Id          Description
-----
xx:xx:xx:xx:xx:xx  Any             RAP
xx:xx:xx:xx:xx:xx  Any             PAP2 (2nd hop)
xx:xx:xx:xx:xx:xx  Any             PAP1 (1st hop)
```

Related Commands

config macfilter
config macfilter ip-address
config macfilter interface
config macfilter description
config macfilter mac-delimiter
config macfilter radius-compat
config macfilter wlan-id

show pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show pmk-cache** command.

show pmk-cache {all | *MAC*}

Syntax Description

all	Displays information about all entries in the PMK cache.
<i>MAC</i>	Information about a single entry in the PMK cache.

Command Default

None.

Examples

This example shows how to display information about a single entry in the PMK cache:

```
> show pmk-cache xx:xx:xx:xx:xx:xx
```

This example shows how to display information about all entries in the PMK cache:

```
> show pmk-cache all
PMK Cache
Station              Entry
                    Lifetime  VLAN Override  IP Override
-----
-----
```

Related Commands

config pmk-cache delete

show remote-lan

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

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

Syntax Description

summary	Displays a summary of all remote LANs.
<i>remote-lan-id</i>	Remote LAN identifier.

Command Default

None.

Examples

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

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

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

```
> show remote-lan 2
Remote LAN Identifier..... 2
Profile Name..... remote
Status..... Disabled
MAC Filtering..... Disabled
AAA Policy Override..... Disabled
Network Admission Control
  Radius-NAC State..... Disabled
  SNMP-NAC State..... Disabled
  Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Number of Active Clients..... 0
Exclusionlist..... Disabled
Session Timeout..... Infinity
CHD per Remote LAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Remote LAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Disabled
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Dynamic Interface..... Disabled
Security
  Web Based Authentication..... Enabled
  ACL..... Unconfigured
  Web Authentication server precedence:
  1..... local
  2..... radius
  3..... ldap
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
```

Related Commands

- config memory monitor errors
- config memory monitor leaks
- debug memory

show wlan

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

show wlan { **apgroups** | **summary** | *wlan_id* | **foreignAp** }

Syntax Description

apgroups	Displays access point group information.
summary	Displays a summary of all wireless LANs.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
foreignAp	Displays the configuration for support of foreign access points.

Command Default

None.

Examples

This example shows how to display a summary of wireless LANs for *wlan_id* 1:

```
> show wlan 1
WLAN Identifier..... 1
Profile Name..... aicha
Network Name (SSID)..... aicha
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control
  Client Profiling Status ..... Disabled
  DHCP ..... Disabled
  HTTP ..... Disabled
  Radius-NAC State..... Enabled
  SNMP-NAC State..... Enabled
Quarantine VLAN..... 0
Maximum number of Associated Clients..... 0
Maximum number of Clients per AP Radio..... 200
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
User Idle Timeout..... 300 seconds
User Idle Threshold..... 0 Bytes
NAS-identifier..... Talwar1
CHD per WLAN..... Enabled
Webauth DHCP exclusion..... Disabled
Interface..... management
Multicast Interface..... Not Configured
WLAN IPv4 ACL..... unconfigured
WLAN IPv6 ACL..... unconfigured
mDNS Status..... Disabled
mDNS Profile Name..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Enabled
PMIPv6 Mobility Type..... none
Quality of Service..... Silver (best effort)
Per-SSID Rate Limits..... Upstream      Downstream
Average Data Rate..... 0                0
```

```

Average Realtime Data Rate..... 0 0
Burst Data Rate..... 0 0
Burst Realtime Data Rate..... 0 0
Per-Client Rate Limits..... Upstream Downstream
Average Data Rate..... 0 0
Average Realtime Data Rate..... 0 0
Burst Data Rate..... 0 0
Burst Realtime Data Rate..... 0 0
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
WMM UAPSD Compliant Client Support..... Disabled
Media Stream Multicast-direct..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
Passive Client Feature..... Disabled
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Radius Servers
  Authentication..... Global Servers
  Accounting..... Global Servers
  Interim Update..... Disabled
  Dynamic Interface..... Disabled
Local EAP Authentication..... Enabled (Profile 'Controller_Local_EAP')
Security
  802.11 Authentication:..... Open System
  FT Support..... Disabled
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
    WPA2 (RSN IE)..... Enabled
      TKIP Cipher..... Disabled
      AES Cipher..... Enabled
Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Enabled
  FT(802.11r)..... Disabled
  FT-PSK(802.11r)..... Disabled
  PMF-1X(802.11w)..... Enabled
  PMF-PSK(802.11w)..... Disabled
FT Reassociation Timeout..... 20
FT Over-The-Air mode..... Enabled
FT Over-The-Ds mode..... Enabled
  GTK Randomization..... Disabled
  SKC Cache Support..... Disabled
  CCKM TSF Tolerance..... 1000
  Wi-Fi Direct policy configured..... Disabled
EAP-Passthrough..... Disabled
CKIP ..... Disabled
IP Security..... Disabled
IP Security Passthru..... Disabled
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
Auto Anchor..... Disabled
FlexConnect Local Switching..... Enabled
flexconnect Central Dhcp Flag..... Disabled
flexconnect nat-pat Flag..... Disabled
flexconnect Dns Override Flag..... Disabled
FlexConnect Vlan based Central Switching ..... Disabled
FlexConnect Local Authentication..... Disabled
FlexConnect Learn IP Address..... Enabled

```

```

Client MFP..... Optional
PMF..... Disabled
PMF Association Comeback Time..... 1
PMF SA Query RetryTimeout..... 200
Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Disabled
Roamed Call Re-Anchor Policy..... Disabled
SIP CAC Fail Send-486-Busy Policy..... Enabled
SIP CAC Fail Send Dis-Association Policy..... Disabled
KTS based CAC Policy..... Disabled
Band Select..... Disabled
Load Balancing..... Disabled
Mobility Anchor List
WLAN ID      IP Address      Status
-----
802.11u..... Enabled
Network Access type..... Chargeable Public Network
Internet service..... Enabled
Network Authentication type..... Not Applicable
HESSID..... 00:00:00:00:00:00
IP Address Type Configuration
IPv4 Address type..... Available
IPv6 Address type..... Not Known

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

Realm configuration summary
Realm index..... 1
Realm name..... jobin
EAP index..... 1
EAP method..... Unsupported
Index      Inner Authentication      Authentication Method
-----
1          Credential Type          SIM
2          Tunneled Eap Credential Type          SIM
3          Credential Type          SIM
4          Credential Type          USIM
5          Credential Type          Hardware Token
6          Credential Type          SoftToken

Domain name configuration summary
Index      Domain name
-----
1          rom3
2          ram
3          rom1

Hotspot 2.0..... Enabled

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

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

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

```

```
MSAP Services..... Disabled
```

This example shows how to display a summary of all WLANs:

```
> show wlan summary
Number of WLANs..... 1

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

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

```
> show wlan foreignap
Foreign AP support is not enabled.
This example shows how to display the AP groups:
```

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

Related Commands

- `config wlan`
- `config wlan 7920-support`
- `config wlan acl`
- `config wlan interface`
- `config wlan roamed-voice-client re-anchor`

Config Commands

This section lists the **config** commands to configure WLANs.

Configure Cisco Client Extension(CCX) Diagnostic Options

This section lists the **config client ccx** commands.

config client ccx clear-reports

To clear the client reporting information, use the **config client ccx clear-reports** command.

config client ccx clear-reports *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
> config client ccx clear-reports 00:1f:ca:cf:b6:60
```

Related Commands

config client ccx get-profiles
config client ccx get-operating-parameters
config client ccx get-client-capability
config client ccx get-manufacturer-info
config client ccx profiles
show client ccx operating-parameters
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-request
show client ccx stats-report

config client ccx clear-results

To clear the test results on the controller, use the **config client ccx clear-results** command.

config client ccx clear-results *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to clear the test results of the client MAC address 00:1f:ca:cf:b6:60:

```
> config client ccx clear-results 00:1f:ca:cf:b6:60
```

Related Commands

config client ccx default-gw-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx dns-ping
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx default-gw-ping

To send a request to the client to perform the default gateway ping test, use the **config client ccx default-gw-ping** command.

```
config client ccx default-gw-ping client_mac_address
```

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:0b:85:02:0d:20 to perform the default gateway ping test:

```
> config client ccx default-gw-ping 00:0b:85:02:0d:20
```

Related Commands

```
config client ccx dns-resolve  
config client ccx test-association  
config client ccx test-dot1x  
config client ccx test-profile  
config client ccx test-abort  
config client ccx clear-results  
config client ccx send-message  
show client ccx last-test-status  
show client ccx last-response-status  
show client ccx results  
show client ccx frame-data
```

config client ccx dhcp-test

To send a request to the client to perform the DHCP test, use the **config client ccx dhcp-test** command.

```
config client ccx dhcp-test client_mac_address
```

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DHCP test:

```
> config client ccx dhcp-test 00:E0:77:31:A3:55
```

Related Commands

```
config client ccx default-gw-ping
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data
```

config client ccx dns-ping

To send a request to the client to perform the Domain Name System (DNS) server IP address ping test, use the **config client ccx dns-ping** command.

config client ccx dns-ping *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DNS server IP address ping test:

```
> config client ccx dns-ping 00:E0:77:31:A3:55
```

Related Commands

config client ccx default-gw-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx dns-resolve

To send a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname, use the **config client ccx dns-resolve** command.

config client ccx dns-resolve *client_mac_address* *host_name*

Syntax Description

client_mac_address MAC address of the client.

host_name Hostname of the client.

Command Default

None.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

Examples

This example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DNS name resolution test to the specified hostname:

```
> config client ccx dns-resolve 00:E0:77:31:A3:55 host_name
```

Related Commands

config client ccx default-gw-ping
config client ccx dns-ping
config client ccx dhcp-test
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx get-client-capability

To send a request to the client to send its capability information, use the **config client ccx get-client-capability** command.

```
config client ccx get-client-capability client_mac_address
```

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send its capability information:

```
> config client ccx get-client-capability 172.19.28.40
```

Related Commands

```
config client ccx get-profiles  
config client ccx get-operating-parameters  
config client ccx get-manufacturer-info  
config client ccx clear-reports  
show client ccx profiles  
show client ccx operating-parameters  
show client ccx manufacturer-info  
show client ccx client-capability  
config client ccx stats-request  
show client ccx stats-report
```

config client ccx get-manufacturer-info

To send a request to the client to send the manufacturer's information, use the **config client ccx get-manufacturer-info** command.

config client ccx get-manufacturer-info *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send the manufacturer's information:

```
> config client ccx get-manufacturer-info 172.19.28.40
```

Related Commands

config client ccx get-profiles
config client ccx get-operating-parameters
config client ccx get-client-capability
config client ccx clear-reports
config client ccx profiles
show client ccx operating-parameters
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-request

config client ccx get-operating-parameters

To send a request to the client to send its current operating parameters, use the **config client ccx get-operating-parameters** command.

config client ccx get-operating-parameters *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send its current operating parameters:

```
> config client ccx get-operating-parameters 172.19.28.40
```

Related Commands

config client ccx get-profiles
config client ccx get-manufacturer-info
config client ccx get-client-capability
config client ccx clear-reports
config client ccx profiles
show client ccx stats-request
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-report

config client ccx get-profiles

To send a request to the client to send its profiles, use the **config client ccx get-profiles** command.

config client ccx get-profiles *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Examples

This example shows how to send a request to the client 172.19.28.40 to send its profile details:

```
> config client ccx get-profiles 172.19.28.40
```

Related Commands

config client ccx get-manufacturer-info
config client ccx get-operating-parameters
config client ccx get-client-capability
config client ccx clear-reports
config client ccx profiles
show client ccx operating-parameters
show client ccx manufacturer-info
show client ccx client-capability
config client ccx stats-request

config client ccx log-request

To configure a Cisco client eXtension (CCX) log request for a specified client device, use the **config client ccx log-request** command.

config client ccx log-request {roam | rsna | syslog} *client_mac_address*

Syntax Description

roam	(Optional) Specifies the request to specify the client CCX roaming log.
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.
<i>client_mac_address</i>	MAC address of the client.

Command Default

None.

Examples

This example shows how to specify the request to specify the client CCS system log:

```
> config client ccx log-request syslog 00:40:96:a8:f7:98
Tue Oct 05 13:05:21 2006
SysLog Response LogID=1: Status=Successful
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 2'
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 1'
Tue Oct 05 13:04:04 2006
SysLog Request LogID=1
```

This example shows how to specify the client CCX roaming log:

```
> config client ccx log-request roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2006
Roaming Response LogID=20: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:55:04 2006
Roaming Request LogID=20
Thu Jun 22 11:54:54 2006
Roaming Response LogID=19: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:54:33 2006 Roaming Request LogID=19
```

This example shows how to specify the client CCX RSNA log:

```
> config client ccx log-request rsna 00:40:96:a8:f7:98
Tue Oct 05 11:06:48 2006
```

```
RSNA Response LogID=2: Status=Successful
Event Timestamp=242424242424
Target BSSID=00:0b:85:23:26:70
RSNA Version=1
Group Cipher Suite=00-0f-ac-01
Pairwise Cipher Suite Count = 2
Pairwise Cipher Suite 0 = 00-0f-ac-02
Pairwise Cipher Suite 1 = 00-0f-ac-04
AKM Suite Count = 2
KM Suite 0 = 00-0f-ac-01
KM Suite 1 = 00-0f-ac-02
SN Capability = 0x1
PMKID Count = 2
PMKID 0 = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
PMKID 1 = 0a 0b 0c 0d 0e 0f 17 18 19 20 1a 1b 1c 1d 1e 1f
802.11i Auth Type: EAP_FAST
RSNA Result: Success
```

Related Commands **show client ccx log-response**

config client ccx send-message

To send a message to the client, use the **config client ccx send-message** command.

config client ccx send-message *client_mac_address* *message_id*

Syntax Description

client_mac_address MAC address of the client.

<i>message_id</i>	<p>Message type that involves one of the following:</p> <ul style="list-style-type: none">• 1—The SSID is invalid.• 2—The network settings are invalid.• 3—There is a WLAN credibility mismatch.• 4—The user credentials are incorrect.• 5—Please call support.• 6—The problem is resolved.• 7—The problem has not been resolved.• 8—Please try again later.• 9—Please correct the indicated problem.• 10—Troubleshooting is refused by the network.• 11—Retrieving client reports.• 12—Retrieving client logs.• 13—Retrieval complete.• 14—Beginning association test.• 15—Beginning DHCP test.• 16—Beginning network connectivity test.• 17—Beginning DNS ping test.• 18—Beginning name resolution test.• 19—Beginning 802.1X authentication test.• 20—Redirecting client to a specific profile.• 21—Test complete.• 22—Test passed.• 23—Test failed.• 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.• 25—Log retrieval refused by the client.• 26—Client report retrieval refused by the client.• 27—Test request refused by the client.• 28—Invalid network (IP) setting.• 29—There is a known outage or problem with the network.• 30—Scheduled maintenance period. <p>(continued on next page)</p>
-------------------	--

message_type (cont.)

- 31—The WLAN security method is not correct.
 - 32—The WLAN encryption method is not correct.
 - 33—The WLAN authentication method is not correct.
-

Examples

This example shows how to send a message to the client MAC address 172.19.28.40 with the message user-action-required:

```
> config client ccx send-message 172.19.28.40 user-action-required
```

Related Commands

```
config client ccx default-gw-ping
config client ccx dhcp
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx test-abort
config client ccx clear-results
config client ccx dns-ping
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data
```

config client ccx stats-request

To send a request for statistics, use the **config client ccx stats-request** command.

config client ccx stats-request *measurement_duration* [**dot11** | **security**] *client_mac_address*

Syntax Description

<i>measurement_duration</i>	Measurement duration in seconds.
dot11	(Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
<i>client_mac_address</i>	MAC address of the client.

Command Default

None.

Examples

This example shows how to specify dot11 counter settings:

```
> config client ccx stats-request 1 dot11 00:40:96:a8:f7:98
Measurement duration = 1
dot11TransmittedFragmentCount = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount = 3
dot11RetryCount = 4
dot11MultipleRetryCount = 5
dot11FrameDuplicateCount = 6
dot11RTSSuccessCount = 7
dot11RTSFailureCount = 8
dot11ACKFailureCount = 9
dot11ReceivedFragmentCount = 10
dot11MulticastReceivedFrameCount = 11
dot11FCSErrorCount = 12
dot11TransmittedFrameCount = 13
```

Related Commands

show client ccx stats-report

config client ccx test-abort

To send a request to the client to abort the current test, use the **config client ccx test-abort** command.

config client ccx test-abort *client_mac_address*

Syntax Description

client_mac_address MAC address of the client.

Command Default

None.

Usage Guidelines

Only one test can be pending at a time.

Examples

This example shows how to send a request to the client 11:11:11:11:11:11 to abort the correct test settings:

```
> config client ccx test-abort 11:11:11:11:11:11
```

Related Commands

config client ccx default-gw-ping
config client ccx dhcp
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx dns-ping
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx test-association

To send a request to the client to perform the association test, use the **config client ccx test-association** command.

config client ccx test-association *client_mac_address* *ssid* *bssid* **802.11**{**a** | **b** | **g**} *channel*

Syntax Description

client_mac_address MAC address of the client.

ssid Network name.

bssid Basic SSID.

802.11a Specifies the 802.11a network.

802.11b Specifies the 802.11b network.

802.11g Specifies the 802.11g network.

channel Channel number.

Command Default

None.

Examples

This example shows how to send a request to the client MAC address 00:0E:77:31:A3:55 to perform the basic SSID association test:

```
> config client ccx test-association 00:E0:77:31:A3:55 ssid bssid 802.11a
```

Related Commands

config client ccx default-gw-ping

config client ccx dns-resolve

config client ccx dhcp

config client ccx test-dot1x

config client ccx test-profile

config client ccx test-abort

config client ccx clear-results

config client ccx send-message

show client ccx last-test-status

show client ccx last-response-status

show client ccx results

show client ccx frame-data

config client ccx test-dot1x

To send a request to the client to perform the 802.1x test, use the **config client ccx test-dot1x** command.

config client ccx test-dot1x *client_mac_address* *profile_id* *bssid* **802.11** {**a** | **b** | **g**} *channel*

Syntax Description

<i>client_mac_address</i>	MAC address of the client.
<i>profile_id</i>	Test profile name.
<i>bssid</i>	Basic SSID.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
802.11g	Specifies the 802.11g network.
<i>channel</i>	Channel number.

Command Default

None.

Examples

This example shows how to send a request to the client to perform the 802.11b test with the profile name *profile_01*:

```
> config client ccx test-dot1x 172.19.28.40 profile_01 bssid 802.11b
```

Related Commands

config client ccx default-gw-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-profile
config client ccx dhcp
config client ccx clear-results
config client ccx send-message
show client ccx last-test-status
show client ccx last-response-status
show client ccx results
show client ccx frame-data

config client ccx test-profile

To send a request to the client to perform the profile redirect test, use the **config client ccx test-profile** command.

config client ccx test-profile *client_mac_address* *profile_id*

Syntax Description

<i>client_mac_address</i>	MAC address of the client.
<i>profile_id</i>	Test profile name.
Note	The <i>profile_id</i> should be from one of the client profiles for which client reporting is enabled.

Command Default

None.

Examples

This example shows how to send a request to the client to perform the profile redirect test with the profile name profile_01:

```
> config client ccx test-profile 11:11:11:11:11:11 profile_01
```

Related Commands

config client ccx default-gw-ping
config client ccx dhcp
config client ccx dns-ping
config client ccx dns-resolve
config client ccx test-association
config client ccx test-dot1x
config client ccx test-abort
config client ccx clear-results

config client deauthenticate

To disconnect a client, use the **config client deauthenticate** command.

config client deauthenticate *MAC*

Syntax Description

<i>MAC</i>	Client MAC address.
------------	---------------------

Command Default

None.

Examples

This example shows how to deauthenticate a client:

```
> config client deauthenticate 11:11:11:11:11
```

Related Commands

show client summary
show client detail

config client location-calibration

To configure link aggregation, use the **config client location-calibration** command.

config client location-calibration {**enable** *mac_address interval* | **disable** *mac_address*}

Syntax Description

enable	(Optional) Specifies that client location calibration is enabled.
<i>mac_address</i>	MAC address of the client.
<i>interval</i>	Measurement interval in seconds.
disable	(Optional) Specifies that client location calibration is disabled.

Command Default

None.

Examples

This example shows how to enable the client location calibration for the client 37:15:85:2a with a measurement interval of 45 seconds:

```
> config client location-calibration enable 37:15:86:2a:Bc:cf 45
```

Related Commands

show client location-calibration summary

Configure IPv6 Commands

Use the **config ipv6** commands to configure IPv6 settings.

config ipv6 disable

To disable IPv6 globally on the controller, use the **config ipv6 disable** command .

config ipv6 disable

Syntax Description This command has no arguments or keywords.

Command Default None.

Usage Guidelines When you use this command, the controller drops all IPv6 packets and the clients will not receive any IPv6 address.

Examples This example shows how to disable IPv6 on the controller:

```
> config ipv6 disable
```

Related Commands

- show ipv6 summary**
- config ipv6 acl**
- config ipv6 neighbor-binding**
- config ipv6 ns-mcast-fwd**
- config ipv6 ra-guard**
- config ipv6 enable**

config ipv6 enable

To enable IPv6 globally on the controller, use the **config ipv6 enable** command .

config ipv6 enable

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to enable IPv6 on the controller:

```
> config ipv6 enable
```

Related Commands

- show ipv6 summary
- config ipv6 acl
- config ipv6 neighbor-binding
- config ipv6 ns-mcast-fwd
- config ipv6 ra-guard
- config ipv6 disable

config ipv6 acl

To create or delete an IPv6 acl on the Cisco wireless LAN controller, use the **config ipv6 acl** command.

```
config ipv6 acl {apply ipv6_acl_name | create ipv6_acl_name | delete ipv6_acl_name | rule {action rule_name
rule_index {permit | deny} | add rule_name rule_index | change index rule_name old_index new_index |
delete rule_name rule_index | destination address rule_name rule_index ip_address netmask | destination
port range rule_name rule_index start_port end_port | direction rule_name rule_index {in | out | any} |
dscp rule_name rule_index dscp | protocol rule_name rule_index protocol | source address rule_name
rule_index ip_address netmask | source port range rule_name rule_index start_port end_port | swap index
rule_name index_1 index_2}
```

Syntax Description

apply	Applies an IPv6 ACL.
<i>ipv6_acl_name</i>	IPv6 ACL name that contains up to 32 alphanumeric characters.
create	Creates an IPv6 ACL.
delete	Deletes an IPv6 ACL.
rule	Configures the IPv6 ACL.
action	Configures whether to permit or deny access.
<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<i>rule_index</i>	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
<i>ip_address</i>	IP address of the rule.
<i>netmask</i>	Netmask of the rule.
<i>start_port</i>	Start port number (between 0 and 65535).
<i>end_port</i>	End port number (between 0 and 65535).

direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.
<i>dscp</i>	Number between 0 and 63, or any .
protocol	Configures a rule's DSCP.
<i>protocol</i>	Number between 0 and 255, or any .
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swap's two rules' indices.
destination port range	Configure a rule's destination port range.

Command Default None.

Usage Guidelines For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

Examples This example shows how to configure an IPv6 ACL to permit access:

```
> config ipv6 acl rule action lab1 4 permit
```

Related Commands `show ipv6 acl`

config ipv6 neighbor-binding

To configure the Neighbor Binding table on the Cisco wireless LAN controller, use the **config ipv6 neighbor-binding** command.

```
config ipv6 neighbor-binding {timers {down-lifetime down_time | reachable-lifetime reachable_time |
stale-lifetime stale_time } | { ra-throttle {allow at-least at_least_value} | enable | disable | interval-option
{ ignore | passthrough | throttle } | max-through {no_mcast_RA | no-limit} | throttle-period
throttle_period}}
```

Syntax Description

timers	Configures the neighbor binding table timeout timers.
down-lifetime	Configures the down lifetime.
<i>down_time</i>	Down lifetime in seconds. The range is from 0 to 86400. The default is 30 seconds.
reachable-lifetime	Configures the reachable lifetime.
<i>reachable_time</i>	Reachable lifetime in seconds. The range is from 0 to 86400. The default is 300 seconds.
stale-lifetime	Configures the stale lifetime.
<i>stale_time</i>	Stale lifetime in seconds. The range is from 0 to 86400. The default is 86400 seconds.
ra-throttle	Configures IPv6 RA throttling options.
allow	Specifies the number of multicast RAs per router per throttle period.
<i>at_least_value</i>	Number of multicast RAs from router before throttling. The range is from 0 to 32. The default is 1.
enable	Enables IPv6 RA throttling.
disable	Disables IPv6 RA throttling.
interval-option	Adjusts the behavior on RA with RFC3775 interval option.
ignore	Indicates interval option has no influence on throttling.
passthrough	Indicates all RAs with RFC3775 interval option will be forwarded (default).

throttle	Indicates all RAs with RFC3775 interval option will be throttled.
max-through	Specifies unthrottled multicast RAs per VLAN per throttle period.
<i>no_mcast_RA</i>	Number of multicast RAs on VLAN by which throttling is enforced. The default multicast RAs on vlan is 10.
no-limit	Configures no upper bound at the VLAN level.
throttle-period	Configures the throttle period.
<i>throttle_period</i>	Duration of the throttle period in seconds. The range is from 10 to 86400 seconds. The default is 600 seconds.

Command Default None.

Examples This example shows how to configure the Neighbor Binding table:

```
> config ipv6 neighbor-binding ra-throttle
```

Related Commands `show ipv6 neighbor-binding`

config ipv6 ns-mcast-fwd

To configure the NS multicast cachemiss forwarding, use the **config ipv6 ns-mcast-fwd** command.

config ipv6 ns-mcast-fwd {enable | disable}

Syntax Description

enable	Enables NS Multicast forwarding on CacheMiss.
disable	Disables NS Multicast forwarding on CacheMiss.

Command Default

None.

Examples

This example shows how to configure an NS multicast forwarding:

```
> config ipv6 ns-mcast-fwd enable
```

Related Commands

show ipv6 summary

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 Remote LAN Commands

Use the **config remote-lan** commands to configure remote LANs.

config remote-lan

To configure a remote LAN, use the **config remote-lan** command.

config remote-lan {**enable** | **disable**} {*remote-lan-id* | **all**}

Syntax Description

enable	Enables a remote LAN.
disable	Disables a remote LAN.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
all	Configures all wireless LANs.

Command Default

None.

Examples

This example shows how to enable a remote LAN with ID 2:

```
> config remote-lan enable 2
```

Related Commands

show remote-lan

config remote-lan aaa-override

To configure user policy override through AAA on a remote LAN, use the **config remote-lan aaa-override** command.

```
config remote-lan aaa-override {enable | disable} remote-lan-id
```

Syntax Description

enable	Enables user policy override through AAA on a remote LAN.
disable	Disables user policy override through AAA on a remote LAN.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

None.

Examples

This example shows how to enable user policy override through AAA on a remote LAN where the remote LAN ID is 2:

```
> config remote-lan aaa-override enable 2
```

Related Commands

show remote-lan

config remote-lan acl

To specify an access control list (ACL) for a remote LAN, use the **config remote-lan acl** command.

config remote-lan acl *remote-lan-id* *acl_name*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>acl_name</i>	ACL name.
Note	Use the show acl summary command to know the ACLs available.

Command Default

None.

Examples

This example shows how to specify ACL1 for a remote LAN whose ID is 2:

```
> config remote-lan acl 2 ACL1
```

Related Commands

show remote-lan

config remote-lan create

To configure a new remote LAN connection, use the **config remote-lan create** command.

config remote-lan create *remote-lan-id name*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>name</i>	Remote LAN name. Valid values are up to 32 alphanumeric characters.

Command Default

None.

Examples

This example shows how to configure a new remote LAN, MyRemoteLAN, with the LAN ID as 3:

```
> config remote-lan create 3 MyRemoteLAN
```

Related Commands

show remote-lan

config remote-lan custom-web

To configure web authentication for a remote LAN, use the **config remote-lan custom-web** command.

```
config remote-lan custom-web {ext-webauth-url URL } | global {enable | disable} | login-page page-name
| loginfailure-page {page-name | none} | logout-page {page-name | none} | webauth-type {internal
| customized | external} } remote-lan-id
```

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
<i>URL</i>	Web authentication URL for the Login page.
global	Configures the global status for the remote LAN.
enable	Enables the global status for the remote LAN.
disable	Disables the global status for the remote LAN.
login-page	Configures a login page.
<i>page-name</i>	Login page name.
none	Configures no login page.
logout-page	Configures a logout page.
none	Configures no logout page.
webauth-type	Configures the web authentication type for the remote LAN.
internal	Displays the default login page.
customized	Displays a downloaded login page.
external	Displays a login page that is on an external server.
<i>name</i>	Remote LAN name. Valid values are up to 32 alphanumeric characters.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are from 1 to 512.

Command Default

None.

Usage Guidelines

Follow these guidelines when you use the **config remote-lan custom-web** command:

- When you configure the external Web-Auth URL, do the following:

- Ensure that Web-Auth or Web-Passthrough Security is in enabled state. To enable Web-Auth, use the **config remote-lan security web-auth enable** command. To enable Web-Passthrough, use the **config remote-lan security web-passthrough enable** command.
 - Ensure that the global status of the remote LAN is in disabled state. To enable the global status of the remote LAN, use the **config remote-lan custom-web global disable** command.
 - Ensure that the remote LAN is in disabled state. To disable a remote LAN, use the **config remote-lan disable** command.
- When you configure the Web-Auth type for the remote LAN, do the following:
 - When you configure a customized login page, ensure that you have a login page configured. To configure a login page, use the **config remote-lan custom-web login-page** command.
 - When you configure an external login page, ensure that you have configured preauthentication ACL for external web authentication to function.

Examples

This example shows how to configure an external web authentication URL for a remote LAN with ID 3:

```
> config remote-lan custom-web ext-webauth-url http://www.AuthorizationURL.com/ 3
```

This example shows how to enable the global status of a remote LAN with ID 3:

```
> config remote-lan custom-web global enable 3
```

This example shows how to configure the login page for a remote LAN with ID 3:

```
> config remote-lan custom-web login-page custompage1 3
```

This example shows how to configure a web authentication type with the default login page for a remote LAN with ID 3:

```
> config remote-lan custom-web webauth-type internal 3
```

Related Commands

show remote-lan

config remote-lan delete

To delete a remote LAN connection, use the **config remote-lan delete** command.

config remote-lan delete *remote-lan-id*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
----------------------	--

Command Default

None.

Examples

This example shows how to delete a remote LAN with ID 3:

```
> config remote-lan delete 3
```

Related Commands

show remote-lan

config remote-lan dhcp_server

To configure a dynamic host configuration protocol (DHCP) server for a remote LAN, use the **config remote-lan dhcp_server** command.

```
config remote-lan dhcp_server remote-lan-id ip_address
```

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>ip_address</i>	IP address of the DHCP server.

Command Default

None.

Examples

This example shows how to configure a DHCP server for a remote LAN with ID 3:

```
> config remote-lan dhcp_server 3 209.165.200.225
```

Related Commands

show remote-lan

config remote-lan exclusionlist

To configure the exclusion list timeout on a remote LAN, use the **config remote-lan exclusionlist** command.

config remote-lan exclusionlist *remote-lan-id* {*seconds* | **disabled** | **enabled**}

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>seconds</i>	Exclusion list timeout in seconds. A value of 0 requires an administrator override.
disabled	Disables exclusion listing.
enabled	Enables exclusion listing.

Command Default

None.

Examples

This example shows how to configure the exclusion list timeout to 20 seconds on a remote LAN with ID 3:

```
> config remote-lan exclusionlist 3 20
```

Related Commands

show remote-lan

config remote-lan interface

To configure an interface for a remote LAN, use the **config remote-lan interface** command.

config remote-lan interface *remote-lan-id* *interface_name*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>interface_name</i>	Interface name. Note Interface name should not be in upper case characters.

Command Default

None.

Examples

This example shows how to configure an interface myinterface for a remote LAN with ID 3:

```
> config remote-lan interface 3 myinterface
```

Related Commands

show remote-lan

config remote-lan ldap

To configure a remote LAN's LDAP servers, use the **config remote-lan ldap** command.

config remote-lan ldap {**add** | **delete**} *remote-lan-id index*

Syntax Description

add	Adds a link to a configured LDAP server (maximum of three).
delete	Deletes a link to a configured LDAP server.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>index</i>	LDAP server index.

Command Default

None.

Examples

This example shows how to add an LDAP server with the index number 10 for a remote LAN with ID 3:

```
> config remote-lan ldap add 3 10
```

Related Commands

show remote-lan

config remote-lan mac-filtering

To configure MAC filtering on a remote LAN, use the **config remote-lan mac-filtering** command.

```
config remote-lan mac-filtering {enable | disable} remote-lan-id
```

Syntax Description

enable	Enables MAC filtering on a remote LAN.
disable	Disables MAC filtering on a remote LAN.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

Enabled.

Examples

This example shows how to disable MAC filtering on a remote LAN with ID 3:

```
> config remote-lan mac-filtering disable 3
```

Related Commands

show remote-lan

config remote-lan max-associated-clients

To configure the maximum number of client connections on a remote LAN, use the **config remote-lan max-associated-clients** command.

config remote-lan max-associated-clients *remote-lan-id max-clients*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>max-clients</i>	Configures the maximum number of client connections on a remote LAN.

Command Default

None.

Examples

This example shows how to configure 10 client connections on a remote LAN with ID 3:

```
> config remote-lan max-associated-clients 3 10
```

Related Commands

show remote-lan

config remote-lan radius_server

To configure the Remote Authentication Dial In User Service (RADIUS) servers on a remote LAN, use the `config remote-lan radius_server` command.

```
config remote-lan radius_server {acct {{add | delete} server-index | {enable | disable} | interim-update
{interval | enable | disable}} | auth {{add | delete} server-index | {enable | disable}} | overwrite-interface
{enable | disable}} remote-lan-id
```

Syntax Description

acct	Configures a RADIUS accounting server.
add	Adds a link to a configured RADIUS server.
delete	Deletes a link to a configured RADIUS server.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>server-index</i>	RADIUS server index.
enable	Enables RADIUS accounting for this remote LAN.
disable	Disables RADIUS accounting for this remote LAN.
interim-update	Enables RADIUS accounting for this remote LAN.
<i>interval</i>	Accounting interim interval. The range is from 180 to 3600 seconds.
enable	Enables accounting interim update.
disable	Disables accounting interim update.
auth	Configures a RADIUS authentication server.
enable	Enables RADIUS authentication for this remote LAN.
disable	Disables RADIUS authentication for this remote LAN.
overwrite-interface	Configures a RADIUS dynamic interface for the remote LAN.
enable	Enables a RADIUS dynamic interface for the remote LAN.
disable	Disables a RADIUS dynamic interface for the remote LAN.

Command Default

The default interim update interval is 600 seconds.

Examples

This example shows how to enable RADIUS accounting for a remote LAN with ID 3:

```
> config remote-lan radius_server acct enable 3
```

Related Commands

`show remote-lan`

config remote-lan security

To configure security policy for a remote LAN, use the **config remote-lan security** command.

```
config remote-lan security {{web-auth {enable | disable | acl | server-precedence} remote-lan-id |
{web-passthrough {enable | disable | acl | email-input} remote-lan-id}}
```

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
email-input	Configures the web captive portal using an e-mail address.
web-passthrough	Specifies the web captive portal with no authentication required.

Command Default

None.

Examples

This example shows how to configure the security web authentication policy for remote LAN ID 1:

```
> config remote-lan security web-auth enable 1
```

Related Commands

show remote-lan

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id* *seconds*

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None.

Examples

This example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
> config remote-lan session-timeout 1 6000
```

Related Commands

show remote-lan

config remote-lan webauth-exclude

To configure web authentication exclusion on a remote LAN, use the **config remote-lan webauth-exclude** command.

```
config remote-lan webauth-exclude remote-lan-id {enable | disable}
```

Syntax Description

<i>remote-lan-id</i>	Remote LAN identifier. Valid values are between 1 and 512.
enable	Enables web authentication exclusion on the remote LAN.
disable	Disables web authentication exclusion on the remote LAN.

Command Default

None.

Examples

This example shows how to enable web authentication exclusion on a remote LAN with ID 1:

```
> config remote-lan webauth-exclude 1 enable
```

Related Commands

show remote-lan

Configure RF-Profile commands

Use the **configure rf-profile** commands to configure RF profiles.

config rf-profile band-select

To configure the RF profile band selection parameters, use the **config rf-profile band-select** command.

config rf-profile band-select {**client-rssi** *rss* | **cycle-count** *cycles* | **cycle-threshold** *value* | **expire** {**dual-band** *value* | **suppression** *value*} | **probe-response** {**enable** | **disable**}} *profile_name*

Syntax Description

client-rssi	Configures the client Received Signal Strength Indicator (RSSI) threshold for the RF profile.
<i>rss</i>	Minimum RSSI for a client to respond to a probe. The range is from -20 to -90 dBm.
cycle-count	Configures the probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
<i>cycles</i>	Value of the cycle count. The range is from 1 to 10.
cycle-threshold	Configures the time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
<i>value</i>	Value of the cycle threshold for the RF profile. The range is from 1 to 1000 milliseconds.
expire	Configures the expiration time of clients for band select.
dual-band	Configures the expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
<i>value</i>	Value for a dual band. The range is from 10 to 300 seconds.
suppression	Configures the expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
<i>value</i>	Value for suppression. The range is from 10 to 200 seconds.
probe-response	Configures the probe response for a RF profile.
enable	Enables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
disable	Disables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
<i>profile name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The default value for client RSSI is -80 dBm.
The default cycle count is 2.
The default cycle threshold is 200 milliseconds.
The default value for dual-band expiration is 60 seconds.
The default value for suppression expiration is 20 seconds.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

Examples

This example shows how to configure the client RSSI:
> `config rf-profile band-select client-rssi -70`

Related Commands

`show rf-profile details`
`config wlan band-select allow`
`config rf-profile client-trap-threshold`
`config rf-profile coverage`
`config rf-profile create`
`config rf-profile data-rates`
`config rf-profile delete`
`config rf-profile description`
`config rf-profile load-balancing`
`config rf-profile max-clients`
`config rf-profile multicast`
`config rf-profile out-of-box`
`config rf-profile tx-power-control-thresh-v1`
`config rf-profile tx-power-control-thresh-v2`
`config rf-profile tx-power-max`
`config rf-profile tx-power-min`

config rf-profile client-trap-threshold

To configure the threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller, use the **config rf-profile client-trap-threshold** command.

config rf-profile client-trap-threshold *threshold profile_name*

Syntax Description

<i>threshold</i>	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller. The range is from 0 to 200. Traps are disabled if the threshold value is configured as zero.
<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None.

Examples

This example shows how to configure the threshold value of the number of clients that associate with an access point:

```
> config rf-profile client-trap-threshold 150
```

Related Commands

show rf-profile details
show rf-profile summary
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile multicast data-rate
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select

config rf-profile create

To create a RF profile, use the **config rf-profile create** command.

```
config rf-profile create {802.11a | 802.11b/g} profile-name
```

Syntax Description

802.11a	Configures the RF profile for the 2.4GHz band.
802.11b/g	Configures the RF profile for the 5GHz band.
<i>profile-name</i>	Name of the RF profile.

Command Default

None.

Examples

This example shows how to create a new RF profile:

```
> config rf-profile create 802.11a RFtestgroup1
```

Related Commands

- show rf-profile details
- show rf-profile summary
- config rf-profile coverage
- config rf-profile create
- config rf-profile data-rates
- config rf-profile delete
- config rf-profile description
- config rf-profile load-balancing
- config rf-profile max-clients
- config rf-profile multicast data-rate
- config rf-profile out-of-box
- config rf-profile tx-power-control-thresh-v1
- config rf-profile tx-power-control-thresh-v2
- config rf-profile tx-power-max
- config rf-profile tx-power-min
- config rf-profile band-select

config rf-profile coverage

To configure the RF profile coverage hole detection parameters, use the **config rf-profile coverage** command.

```
config rf-profile coverage {data coverage_level | exception clients | level value | voice coverage_level }
profile_name
```

Syntax Description

data	Configures the threshold value of the data RSSI.
<i>coverage_level</i>	Minimum receive signal strength indication (RSSI) value of data packets received by the access point. The value that you configure is used to identify coverage holes within the network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole is detected. The range is from –90 to –60 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
exception	Configures the coverage exception per access point.
<i>clients</i>	Minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold. The range is from 1 to 75. The default value is 3.
voice	Configures the threshold value of the voice RSSI.
<i>coverage_level</i>	Minimum receive signal strength indication (RSSI) value of voice packets received by the access point. The value that you configure is used to identify coverage holes within the network. If the access point receives a packet in the data queue with an RSSI value below the value that you enter here, a potential coverage hole is detected. The range is from –90 to –60 dBm. The access point takes voice RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.
level	Configures the coverage exception level per AP.
<i>value</i>	Coverage exception level per AP. Percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.
<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The default value of the data coverage level is –80 dBm.

The default value of the minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold is 3.

The default value of the percentage of clients on an access point that are experiencing a low signal level is 25%.

The default value of the voice coverage level is –80 dBm.

Examples

This example shows how to configure the threshold value of the data RSSI:

```
> config rf-profile coverage data -80
```

This example shows how to configure the minimum client coverage exception level:

```
> config rf-profile coverage exception 10
```

This example shows how to configure the coverage exception level per AP:

```
> config rf-profile coverage level 30
```

Related Commands

- show rf-profile details
- config rf-profile client-trap-threshold
- config rf-profile create
- config rf-profile data-rates
- config rf-profile delete
- config rf-profile description
- config rf-profile load-balancing
- config rf-profile max-clients
- config rf-profile multicast
- config rf-profile out-of-box
- config rf-profile tx-power-control-thresh-v1
- config rf-profile tx-power-control-thresh-v2
- config rf-profile tx-power-max
- config rf-profile tx-power-min
- config rf-profile band-select

config rf-profile data-rates

To configure the data rate on a RF profile, use the **config rf-profile data-rates** command.

config rf-profile data-rates {802.11a|802.11b} {disabled|mandatory|supported} *data-rate profile-name*

Syntax Description

802.11a	Specifies 802.11a as the radio policy of the RF profile.
802.11b	Specifies 802.11b as the radio policy of the RF profile.
disabled	Disables a rate.
mandatory	Sets a rate to mandatory.
supported	Sets a rate to supported.
<i>data-rate</i>	802.11 operational rates, which are 1*, 2*, 5.5*, 6, 9, 11*, 12, 18, 24, 36, 48 and 54, where * denotes 802.11b only rates.
<i>profile-name</i>	Name of the RF profile.

Command Default

Default data rates for RF profiles are derived from the controller system defaults, the global data rate configurations. For example, if the RF profile's radio policy is mapped to 802.11a then the global 802.11a data rates are copied into the RF profiles at the time of creation.

The data rates set with this command are negotiated between the client and the Cisco wireless LAN controller. If the data rate is set to mandatory, the client must support it in order to use the network. If a data rate is set as supported by the Cisco wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. It is not required that a client is able to use all the rates marked supported in order to associate.

Examples

This example shows how to set the 802.11b transmission of an RF profile at a mandatory rate at 12 Mbps:

```
> config rf-profile 802.11b data-rates mandatory 12 RFGGroup1
```

Related Commands

show rf-profile details
show rf-profile summary
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing

```
config rf-profile max-clients
config rf-profile multicast data-rate
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select
```

config rf-profile delete

To delete a RF profile, use the **config rf-profile delete** command.

```
config rf-profile delete profile-name
```

Syntax Description

<i>profile-name</i>	Name of the RF profile.
---------------------	-------------------------

Command Default

None.

Examples

This example shows how to delete a RF profile:

```
> config rf-profile delete RFGroup1
```

Related Commands

- show rf-profile details**
- show rf-profile summary**
- config rf-profile coverage**
- config rf-profile create**
- config rf-profile data-rates**
- config rf-profile description**
- config rf-profile load-balancing**
- config rf-profile max-clients**
- config rf-profile multicast data-rate**
- config rf-profile out-of-box**
- config rf-profile tx-power-control-thresh-v1**
- config rf-profile tx-power-control-thresh-v2**
- config rf-profile tx-power-max**
- config rf-profile tx-power-min**
- config rf-profile band-select**

config rf-profile description

To provide a description to a RF profile, use the **config rf-profile description** command.

config rf-profile description *description profile-name*

Syntax Description

<i>description</i>	Description of the RF profile.
<i>profile-name</i>	Name of the RF profile.

Command Default

None.

Examples

This example shows how to add a description to a RF profile:

```
> config rf-profile description This is a demo description RFGroup1
```

Related Commands

show rf-profile details
show rf-profile summary
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile multicast data-rate
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select

config rf-profile load-balancing

To configure load balancing on an RF profile, use the **config rf-profile load-balancing** command.

config rf-profile load-balancing {**window** *clients* | **denial** *value*} *profile_name*

Syntax Description

window	Configures the client window for load balancing of an RF profile.
<i>clients</i>	<p>Client window size that limits the number of client associations with an access point. The range is from 0 to 20. The default value is 5.</p> <p>The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:</p> $\text{load-balancing window} + \text{client associations on AP with lightest load} = \text{load-balancing threshold}$ <p>Access points with more client associations than this threshold are considered busy, and clients can associate only to access points with client counts lower than the threshold. This window also helps to disassociate sticky clients.</p>
denial	Configures the client denial count for load balancing of an RF profile.
<i>value</i>	<p>Maximum number of association denials during load balancing. The range is from 1 to 10. The default value is 3.</p> <p>When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again. After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association. The default is 3.</p>
<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None.

Examples

This example shows how to configure the client window size for an RF profile:

```
> config rf-profile load-balancing window 15
```

Related Commands

show rf-profile details
show load-balancing
config wlan load-balance allow
config rf-profile client-trap-threshold

config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile multicast
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select

config rf-profile max-clients

To configure the maximum number of client connections per access point of an RF profile, use the **config rf-profile max-clients** commands.

config rf-profile max-clients *clients*

Syntax Description

<i>clients</i>	Maximum number of client connections per access point of an RF profile. The range is from 1 to 200.
----------------	---

Command Default

None.

Usage Guidelines

You can use this command to configure the maximum number of clients on access points that are in client dense areas, or serving high bandwidth video or mission critical voice applications.

Examples

This example shows how to set the maximum number of clients at 50:

```
> config rf-profile max-clients 50
```

Related Commands

show rf-profile details
config wlan max-radio-clients
config wlan max-associated-clients
config rf-profile client-trap-threshold
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing
config rf-profile multicast
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select

config rf-profile multicast data-rate

To configure the minimum RF profile multicast data rate, use the **config rf-profile multicast data-rate** command.

config rf-profile multicast data-rate *value profile_name*

Syntax Description

<i>value</i>	Minimum RF profile multicast data rate. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that access points will dynamically adjust the data rate.
<i>profile_name</i>	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The default is 0.

Examples

This example shows how to set the multicast data rate for an RF profile:

```
> config rf-profile multicast data-rate 24
```

Related Commands

show rf-profile details
config 802.11 multicast data-rate
config rf-profile client-trap-threshold
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select

config rf-profile out-of-box

To create an out-of-box AP group consisting of newly installed access points, use the **config rf-profile out-of-box** command.

config rf-profile out-of-box {enable | disable}

Syntax Description

enable	Enables the creation of an out-of-box AP group. When you enable this command, the following occurs: <ul style="list-style-type: none"> • Newly installed access points that are part of the default AP group will be part of the out-of-box AP group and their radios will be switched off, which eliminates any RF instability caused by the new access points. • All access points that do not have a group name become part of the out-of-box AP group. • Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.
disable	Disables the out-of-box AP group. When you disable this feature, only the subscription of new APs to the out-of-box AP group stops. All APs that are subscribed to the out-of-box AP group remain in this AP group. You can move APs to the default group or a custom AP group upon network convergence.

Command Default

None.

Usage Guidelines

When an out-of-box AP associates with the controller for the first time, it will be redirected to a special AP group and the RF profiles applicable to this AP Group will control the radio admin state configuration of the AP. You can move APs to the default group or a custom group upon network convergence.

Examples

This example shows how to enable the creation of an out-of-box AP group:

```
> config rf-profile out-of-box enable
```

Related Commands

```
show rf-profile details
show rf-profile summary
config rf-profile client-trap-threshold
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
```

```
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile multicast data-rate
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile tx-power-min
config rf-profile band-select
```

config rf-profile tx-power-control-thresh-v1

To configure Transmit Power Control version1 (TPCv1) to an RF profile, use the **config rf-profile tx-power-control-thresh-v1** command.

```
config rf-profile tx-power-control-thresh-v1 tpc-threshold profile_name
```

Syntax Description

<i>tpc-threshold</i>	TPC threshold.
<i>profile-name</i>	Name of the RF profile.

Command Default

None.

Examples

This example shows how to configure TPCv1 on an RF profile:

```
> config rf-profile tx-power-control-thresh-v1 RFGroup1
```

Related Commands

- show rf-profile details
- show rf-profile summary
- config rf-profile coverage
- config rf-profile create
- config rf-profile data-rates
- config rf-profile delete
- config rf-profile description
- config rf-profile load-balancing
- config rf-profile max-clients
- config rf-profile multicast data-rate
- config rf-profile out-of-box
- config rf-profile tx-power-control-thresh-v2
- config rf-profile tx-power-max
- config rf-profile tx-power-min
- config rf-profile band-select

config rf-profile tx-power-control-thresh-v2

To configure Transmit Power Control version 2 (TPCv2) to an RF profile, use the **config rf-profile tx-power-control-thresh-v2** command.

config rf-profile tx-power-control-thresh-v2 *tpc-threshold profile-name*

Syntax Description

<i>tpc-threshold</i>	TPC threshold.
<i>profile-name</i>	Name of the RF profile.

Command Default

None.

Examples

This example shows how to configure TPCv2 on an RF profile:

```
> config rf-profile tx-power-control-thresh-v2 RFGGroup1
```

Related Commands

- show rf-profile details**
- show rf-profile summary**
- config rf-profile coverage**
- config rf-profile create**
- config rf-profile data-rates**
- config rf-profile delete**
- config rf-profile description**
- config rf-profile load-balancing**
- config rf-profile max-clients**
- config rf-profile multicast data-rate**
- config rf-profile out-of-box**
- config rf-profile tx-power-control-thresh-v1**
- config rf-profile tx-power-max**
- config rf-profile tx-power-min**
- config rf-profile band-select**

config rf-profile tx-power-max

To configure maximum auto-rf to an RF profile, use the **config rf-profile tx-power-max** command.

config rf-profile *tx-power-max profile-name*

Syntax Description

<i>tx-power-max</i>	Maximum auto-rf tx power.
<i>profile-name</i>	Name of the RF profile.

Command Default

None.

Examples

This example shows how to configure tx-power-max on an RF profile:

```
> config rf-profile tx-power-max RFGroup1
```

Related Commands

show rf-profile details
show rf-profile summary
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile multicast data-rate
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile client-trap-threshold
config rf-profile tx-power-min
config rf-profile band-select

config rf-profile tx-power-min

To configure minimum auto-rf to an RF profile, use the **config rf-profile tx-power-min** command.

config rf-profile tx-power-min *tx-power-min profile-name*

Syntax Description

<i>tx-power-min</i>	Minimum auto-rf tx power.
<i>profile-name</i>	Name of the RF profile.

Command Default

None.

Examples

This example shows how to configure tx-power-min on an RF profile:

```
> config rf-profile tx-power-min RFGroup1
```

Related Commands

show rf-profile details
config rf-profile coverage
config rf-profile create
config rf-profile data-rates
config rf-profile delete
config rf-profile description
config rf-profile load-balancing
config rf-profile max-clients
config rf-profile multicast data-rate
config rf-profile out-of-box
config rf-profile tx-power-control-thresh-v1
config rf-profile tx-power-control-thresh-v2
config rf-profile tx-power-max
config rf-profile client-trap-threshold
config rf-profile band-select

Configure Watchlist Commands

Use the **config watchlist** commands to configure watchlist settings.

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

```
config watchlist add {mac MAC | username username}
```

Syntax Description

mac <i>MAC</i>	Specifies the MAC address of the wireless LAN.
username <i>username</i>	Specifies the name of the user to watch.

Command Default

None.

Examples

This example shows how to add a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
> config watchlist add mac a5:6b:ac:10:01:6b
```

Related Commands

```
config watchlist delete  
config watchlist enable  
config watchlist disable  
show watchlist
```

config watchlist delete

To delete a watchlist entry for a wireless LAN, use the **config watchlist delete** command.

```
config watchlist delete {mac MAC | username username}
```

Syntax Description

mac <i>MAC</i>	Specifies the MAC address of the wireless LAN to delete from the list.
username <i>username</i>	Specifies the name of the user to delete from the list.

Command Default

None.

Examples

This example shows how to delete a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
> config watchlist delete mac a5:6b:ac:10:01:6b
```

Related Commands

```
config watchlist add  
config watchlist enable  
config watchlist disable  
show watchlist
```

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to disable the client watchlist:

```
> config watchlist disable
```

Related Commands

- config watchlist delete**
- config watchlist enable**
- config watchlist add**
- show watchlist**

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to enable a watchlist entry:

```
> config watchlist enable
```

Related Commands

- config watchlist add**
- config watchlist delete**
- show watchlist**

Configure Wireless LAN Commands

Use the **config wlan** commands to configure wireless LAN command settings.

config wlan

To create, delete, enable, or disable a wireless LAN, use the **config wlan** command.

config wlan {**enable** | **disable** | **create** | **delete**} *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

Syntax Description

enable	Enables a wireless LAN.
disable	Disables a wireless LAN.
create	Creates a wireless LAN.
delete	Deletes a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>name</i>	(Optional) WLAN profile name up to 32 alphanumeric characters.
foreignAp	(Optional) Specifies the third-party access point settings.
<i>ssid</i>	SSID (network name) up to 32 alphanumeric characters.
all	(Optional) Specifies all wireless LANs.

Command Default

None.

Usage Guidelines

When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

If you do not specify an SSID, the profile *name* parameter is used for both the profile name and the SSID.

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

Examples

This example shows how to enable wireless LAN identifier 16:

```
> config wlan enable 16
```

Related Commands

show ap wlan
show wlan

config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

config wlan 7920-support {**client-cac-limit** | **ap-cac-limit**} {**enable** | **disable**} *wlan_id*

Syntax Description

ap-cac-limit	Supports phones that require client-controlled Call Admission Control (CAC) that expect the Cisco vendor-specific information element (IE).
client-cac-limit	Supports phones that require access point-controlled CAC that expect the IEEE 802.11e Draft 6 QBSS-load.
enable	Enables phone support.
disable	Disables phone support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Examples

This example shows how to enable the phone support that requires client-controlled CAC with wireless LAN ID 8:

```
> config wlan 7920-support ap-cac-limit enable 8
```

Related Commands

show wlan

config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

```
config wlan 802.11e {allow | disable | require} wlan_id
```

Syntax Description

allow	Allows 802.11e-enabled clients on the wireless LAN.
disable	Disables 802.11e on the wireless LAN.
require	Requires 802.11e-enabled clients on the wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

802.11e provides quality of service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include a multimedia capability.

Examples

This example shows how to allow 802.11e on the wireless LAN with LAN ID 1:

```
> config wlan 802.11e allow 1
```

Related Commands

show trapflags

config wlan aaa-override

To configure a user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

```
config wlan aaa-override {enable | disable} {wlan_id | foreignAp}
```

Syntax Description

enable	Enables policy override.
disable	Disables policy override.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

Disabled.

Usage Guidelines

When AAA override is enabled, and a client has conflicting AAA and Cisco wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

If the corporate wireless LAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is performed by the AAA server if the controller wireless LAN does not contain any client-specific authentication parameters.

The AAA override values may come from a RADIUS server, for example.

Examples

This example shows how to configure user policy override via AAA on wireless LAN ID 1:

```
> config wlan aaa-override enable 1
```

Related Commands

show wlan

config wlan acl

To configure a wireless LAN access control list (ACL), use the **config wlan acl** command.

```
config wlan acl [acl_name | none]
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
<i>acl_name</i>	(Optional) ACL name.
none	(Optional) Clears the ACL settings for the specified wireless LAN.

Command Default

None.

Examples

This example shows how to configure a WLAN access control list with WLAN ID 1 and ACL named office_1:

```
> config wlan acl 1 office_1
```

Related Commands

show wlan

config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

config wlan assisted-roaming {neighbor-list | dual-list | prediction} {enable | disable} wlan_id

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
prediction	Configures assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

Examples

This example shows how to enable an 802.11k neighbor list for a WLAN:

```
> config wlan assisted-roaming neighbor-list enable 1
```

Related Commands

config assisted-roaming
show assisted-roaming
debug 11k

config wlan avc

To configure Application Visibility and Control (AVC) on a WLAN, use the **config wlan avc** command.

```
config wlan avc wlan_id {profile profile_name | visibility} {enable | disable}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
profile	Associates or removes an AVC profile from a WLAN.
<i>profile_name</i>	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
visibility	Configures application visibility on a WLAN.
enable	Enables application visibility on a WLAN. You can view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology. Use the show avc statistics client command to view the client AVC statistics.
disable	Disables application visibility on a WLAN.

Command Default

None.

Usage Guidelines

You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

Examples

This example shows how to associate an AVC profile with a WLAN:

```
> config wlan avc 5 profile profile1 enable
```

Related Commands

```
config avc profile delete  
config avc profile create  
config avc profile rule  
show avc statistics  
show avc profile applications  
show avc applications  
show avc statistics client
```

show avc statistics wlan

show avc statistics top-apps

show avc statistics guest-lan

show avc statistics remote-lan

debug avc error

debug avc events

config wlan apgroup

To manage access point group VLAN features, use the **config wlan apgroup** command.

```
config wlan apgroup {add apgroup_name [description] | delete apgroup_name | description apgroup_name
description | interface-mapping {add | delete} apgroup_name wlan_id interface_name | nac-snmp {enable
| disable} apgroup_name wlan_id | nasid NAS-ID apgroup_name | profile-mapping {add | delete}
apgroup_name profile_name | wlan-radio-policy apgroup_name wlan-id {802.11a-only | 802.11bg |
802.11g-only | all} | hotspot {venue {type apgroup_name group_codetype_code | name apgroup_name
language_codevenue_name } | operating-class {add | delete} apgroup_name operating_class_value}}
```

Syntax Description

add	Creates a new access point group (AP group).
<i>apgroup_name</i>	Access point group name.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
delete	Removes a wireless LAN from an AP group.
description	Describes an AP group.
<i>description</i>	Description of the AP group.
interface-mapping	(Optional) Assigns or removes a Wireless LAN from an AP group.
<i>interface_name</i>	(Optional) Interface to which you want to map an AP group.
nac-snmp	Configures NAC SNMP functionality on given AP group. Enables or disables Network Admission Control (NAC) out-of-band support on an access point group.
enable	Enables NAC out-of-band support on an AP group.
disable	Disables NAC out-of-band support on an AP group.
<i>NAS-ID</i>	Network Access Server identifier (NAS-ID) for the AP group. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters. Beginning in Release 7.4 and later releases, you can configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP group NAS-ID > WLAN NAS-ID > Interface NAS-ID.
none	Configures the controller system name as the NAS-ID.

profile-mapping	Configures RF profile mapping on an AP group.
<i>profile_name</i>	RF profile name for a specified AP group.
wlan-radio-policy	Configures WLAN radio policy on an AP group.
802.11a-only	Configures WLAN radio policy on an AP group.
802.11bg	Configures WLAN radio policy on an AP group.
802.11g-only	Configures WLAN radio policy on an AP group.
all	Configures WLAN radio policy on an AP group.
hotspot	Configures a HotSpot on an AP group.
venue	Configures venue information for an AP group.
type	Configures the type of venue for an AP group.
<i>group_code</i>	Venue group information for an AP group. The following options are available: <ul style="list-style-type: none"> • 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 an 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

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 following options are available:

- 0 : UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the following options are available:

- 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 an AP group.
<i>language_code</i>	An 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.
<i>venue_name</i>	Venue name for this AP group. 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 an operating class for an AP group.
delete	Deletes an operating class for an AP group.
<i>operating_class_value</i>	Operating class for an AP group. The available operating classes are 81, 83, 84, 112, 113, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127.

Command Default

Disabled.

Usage Guidelines

An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group in controller software release 6.0, move all APs in this group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the APs, enter the **show wlan apgroups** command. To move APs, enter the **config ap group-name groupname cisco_ap** command.

The NAS-ID configured on the controller for AP group or WLAN or interface is used for authentication. The NAS-ID is not propagated across controllers.

Examples

This example shows how to enable the NAC out-of-band support on access point group 4:

```
> config wlan apgroup nac enable apgroup 4
```

Related Commands

config guest-lan nac
config wlan nac
debug group
show ap stats
show ap summary
show ap wlan
show nac statistics
show nac summary
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advance hotspot gas-limit
config wlan security wpa gtk-random

```
config wlan hotspot dot11u
config wlan hotspot clear-all
config wlan hotspot msap
config wlan nasid
config interface nasid
```

config wlan band-select allow

To configure band selection on a WLAN, use the **config wlan band-select allow** command.

```
config wlan band-select allow {enable | disable} wlan_id
```

Syntax Description

enable	Enables band selection on a WLAN.
disable	Disables band selection on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

Examples

This example shows how to enable band selection on a WLAN:

```
> config wlan band-select allow enable 6
```

Related Commands

```
show band-select  
show load-balancing  
config band-select cycle-threshold  
config band-select expire  
config band-select cycle-count  
config band-select client-rssi
```

config wlan broadcast-ssid

To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

config wlan broadcast-ssid {enable | disable} *wlan_id*

Syntax Description

enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Disabled.

Examples

This example shows how to configure an SSID broadcast on wireless LAN ID 1:

```
> config wlan broadcast-ssid enable 1
```

Related Commands

show wlan

config wlan call-snoop

To enable or disable Voice-over-IP (VoIP) snooping for a particular WLAN, use the **config wlan call-snoop** command.

```
config wlan call-snoop {enable | disable} wlan_id
```

Syntax Description

enable	Enables VoIP snooping on a wireless LAN.
disable	Disables VoIP snooping on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

WLAN should be with Platinum QoS and it needs to be disabled while invoking this CLI

Examples

This example shows how to enable VoIP snooping for WLAN 3:

```
> config wlan call-snoop 3 enable
```

Related Commands

```
show wlan  
config wlan  
show call-control ap  
show call-control client
```

config wlan chd

To enable or disable Coverage Hole Detection (CHD) for a wireless LAN, use the **config wlan chd** command.

```
config wlan chd wlan_id {enable | disable}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.

Command Default

None.

Examples

This example shows how to enable CHD for WLAN 3:

```
> config wlan chd 3 enable
```

Related Commands

```
show wlan  
config wlan  
config ap wlan
```

config wlan ccx aironet-ie

To enable or disable Aironet information elements (IEs) for a WLAN, use the **config wlan ccx aironet-ie** command.

```
config wlan ccx aironet-ie {enable | disable}
```

Syntax Description

enable	Enables the Aironet information elements.
disable	Disables the Aironet information elements.

Command Default

None.

Examples

This example shows how to enable Aironet information elements for a WLAN:

```
> config wlan ccx aironet-ie enable
```

Related Commands

```
config wlan  
config wlan security ckip  
show client detail
```

config wlan channel-scan defer-priority

To configure the controller to defer priority markings for packets that can defer off channel scanning, use the **config wlan channel-scan defer-priority** command.

```
config wlan channel-scan defer-priority priority [enable | disable] wlan_id
```

Syntax Description

<i>priority</i>	User priority value (0 to 7).
enable	(Optional) Enables packet at given priority to defer off channel scanning.
disable	(Optional) Disables packet at given priority to defer off channel scanning.
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Command Default

None.

Usage Guidelines

The priority value should be set to 6 on the client and on the WLAN.

Examples

This example shows how to enable the controller to defer priority markings that can defer off channel scanning with user priority value 6 and WLAN id 30:

```
> config wlan channel-scan defer-priority 6 enable 30
```

Related Commands

```
config wlan  
show client detail  
config wlan channel-scan defer-time
```

config wlan channel-scan defer-time

To assign the channel scan defer time in milliseconds, use the **config wlan channel-scan defer-time** command.

```
config wlan channel-scan defer-time msecs wlan_id
```

Syntax Description

<i>msecs</i>	Deferral time in milliseconds (0 to 60000 milliseconds).
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Command Default

None.

Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on your wlan.

Examples

This example shows how to assign the scan defer time to 40 milliseconds for WLAN id 50:

```
> config wlan channel-scan defer-time 40 50
```

Related Commands

```
config wlan  
show client detail  
config wlan channel-scan defer-time
```

config wlan dhcp_server

To configure the internal DHCP server for a wireless LAN, use the **config wlan dhcp_server** command.

config wlan dhcp_server {*wlan_id* | **foreignAp**} *ip_address* [**required**]

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>ip_address</i>	IP address of the internal DHCP server (this parameter is required).
required	(Optional) Specifies whether DHCP address assignment is required.

Command Default

None.

Usage Guidelines

The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the **show wlan** command to verify that the DHCP server has been assigned to the WLAN.

Examples

This example shows how to configure an IP address 10.10.2.1 of the internal DHCP server for wireless LAN ID 16:

```
> config wlan dhcp_server 16 10.10.2.1
```

Related Commands

show dhcp
show dhcp proxy
config dhcp
config interface dhcp
debug dhcp
debug dhcp service-port
debug disable-all
show dhcp proxy

config wlan diag-channel

To enable the diagnostic channel troubleshooting on a particular WLAN, use the **config wlan diag-channel** command.

```
config wlan diag-channel [enable | disable] wlan_id
```

Syntax Description

enable	(Optional) Enables the wireless LAN diagnostic channel.
---------------	---

disable	(Optional) Disables the wireless LAN diagnostic channel.
----------------	--

<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
----------------	-------------------------------------

Command Default

None.

Examples

This example shows how to enable the wireless LAN diagnostic channel for WLAN ID 1:

```
> config wlan diag-channel enable 1
```

Related Commands

show wlan

show run-config

config wlan dtim

To configure a Delivery Traffic Indicator Message (DTIM) for 802.11 radio network **config wlan dtim** command.

```
config wlan dtim {802.11a | 802.11b} dtim wlan_id
```

Syntax Description

802.11a	Configures DTIM for the 802.11a radio network.
802.11b	Configures DTIM for the 802.11b radio network.
<i>dtim</i>	Value for DTIM (between 1 to 255 inclusive).
<i>wlan_id</i>	Number of the WLAN to be configured.

Command Default

The default is DTIM 1.

Examples

This example shows how to configure DTIM for 802.11a radio network with DTIM value 128 and WLAN ID 1:

```
> config wlan dtim 802.11a 128 1
```

Related Commands

show wlan

config wlan exclusionlist

To configure the wireless LAN exclusion list, use the **config wlan exclusionlist** command.

```
config wlan exclusionlist {wlan_id [enabled | disabled | time] | foreignAp [enabled | disabled | time]}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
enabled	(Optional) Enables the exclusion list for the specified wireless LAN or foreign access point.
disabled	(Optional) Disables the exclusion list for the specified wireless LAN or a foreign access point.
<i>time</i>	(Optional) Exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
foreignAp	Specifies a third-party access point.

Command Default

None.

Usage Guidelines

This command replaces the **config wlan blacklist** command.

Examples

This example shows how to enable the exclusion list for WLAN ID 1:

```
> config wlan exclusionlist 1 enabled
```

Related Commands

```
show wlan  
show wlan summary
```

config wlan flow

To associate a NetFlow monitor with a WLAN, use the **config wlan flow** command.

```
config wlan flow wlan_id monitor monitor_name {enable | disable}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier from 1 to 512 (inclusive).
monitor	Configures a NetFlow monitor.
<i>monitor_name</i>	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for a monitor name.
enable	Associates a NetFlow monitor with a WLAN.
disable	Dissociates a NetFlow monitor from a WLAN.

Command Default

None.

Usage Guidelines

You can use the **config flow** command to create a new NetFlow monitor.

Examples

This example shows how to associate a NetFlow monitor with a WLAN:

```
> config wlan flow 5 monitor monitor1 enable
```

Related Commands

```
show flow exporter  
show flow monitor  
config flow
```

config wlan flexconnect ap-auth

To configure local authentication of clients associated with FlexConnect on a locally switched WLAN, use the **config wlan flexconnect ap-auth** command.

```
config wlan flexconnect ap-auth wlan_id {enable | disable}
```

Syntax Description

ap-auth	Configures local authentication of clients associated with an FlexConnect on a locally switched WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables AP authentication on a WLAN.
disable	Disables AP authentication on a WLAN.

Command Default

None.

Usage Guidelines

Local switching must be enabled on the WLAN where you want to configure local authentication of clients associated with FlexConnect.

Examples

This example shows how to enable authentication of clients associated with FlexConnect on a specified WLAN:

```
> config wlan flexconnect ap-auth 6 enable
```

Related Commands

```
config wlan flexconnect local-switching  
show wlan
```

config wlan flexconnect learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan flexconnect learn-ipaddr** command.

```
config wlan flexconnect learn-ipaddr wlan_id {enable | disable}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables client IP address learning on a wireless LAN.
disable	Disables client IP address learning on a wireless LAN.

Command Default

Disabled when the **config wlan flexconnect local-switching** command is disabled. Enabled when the **config wlan flexconnect local-switching** command is enabled.

Usage Guidelines

If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.



Note

The ability to disable IP address learning is not supported with FlexConnect central switching.

Examples

This example shows how to disable client IP address learning for WLAN 6:

```
> config wlan flexconnect learn-ipaddr disable 6
```

Related Commands

```
config wlan flexconnect local-switching  
show wlan
```

config wlan flexconnect local-switching

To configure local switching, central DHCP, NAT-PAT, or, override DNS option on a FlexConnect WLAN, use the **config wlan flexconnect local switching** command.

```
config wlan flexconnect local switching wlan_id {enable | disable} { {central-dhcp {enable | disable}  
nat-pat {enable | disable} } | {override option dns { enable | disable} } }
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables local switching on a FlexConnect WLAN.
disable	Disables local switching on a FlexConnect WLAN.
central-dhcp	Configures central switching of DHCP packets on the local switching FlexConnect WLAN. When you enable this feature, the DHCP packets received from AP are centrally switched to the controller and forwarded to the corresponding VLAN based on the AP and the SSID.
enable	Enables central DHCP on a FlexConnect WLAN.
disable	Disables central DHCP on a FlexConnect WLAN.
nat-pat	Configures Network Address Translation (NAT) and Port Address Translation (PAT) on the local switching FlexConnect WLAN.
enable	Enables NAT-PAT on the FlexConnect WLAN.
disable	Disables NAT-PAT on the FlexConnect WLAN.
override	Specifies the DHCP override options on the FlexConnect WLAN.
option dns	Specifies the override DNS option on the FlexConnect WLAN. When you override this option, the clients get their DNS server IP address from the AP, not from the controller.
enable	Enables the override DNS option on the FlexConnect WLAN.
disable	Disables the override DNS option on the FlexConnect WLAN.

Command Default

Disabled.

Usage Guidelines

When you enable the **config wlan flexconnect local-switching** command, the **config wlan flexconnect learn-ipaddr** command is enabled by default.

**Note**

The ability to disable IP address learning is not supported with FlexConnect central switching.

Examples

This example shows how to enable WLAN 6 for local switching and enable central DHCP and NAT-PAT:

```
> config wlan flexconnect local-switching 6 enable central-dhcp enable nat-pat enable
```

This example shows how to enable the override DNS option on WLAN 6:

```
> config wlan flexconnect local-switching 6 override option dns enable
```

Related Commands

config wlan flexconnect learn-ipaddr

config wlan flexconnect vlan-central-switching

config wlan flexconnect ap-auth

show wlan

config wlan flexconnect vlan-central-switching

To configure central switching on a locally switched WLAN, use the **config wlan flexconnect vlan-central-switching** command.

```
config wlan flexconnect vlan-central-switching wlan_id { enable | disable }
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables central switching on a locally switched wireless LAN.
disable	Disables central switching on a locally switched wireless LAN.

Command Default

Disabled.

Usage Guidelines

You must enable Flexconnect local switching to enable VLAN central switching. When you enable WLAN central switching, the access point bridges the traffic locally if the WLAN is configured on the local IEEE 802.1q link. If the VLAN is not configured on the Access point, the AP will tunnel the traffic back to the controller and the controller bridges the traffic to the corresponding VLAN.

WLAN central switching does not support:

- FlexConnect Local Authentication.
- L3 roaming of local switching client.

Examples

This example shows how to enable WLAN 6 for central switching:

```
> config wlan flexconnect vlan-central-switching 6 enable
```

Related Commands

```
config wlan flexconnect local-switching  
show wlan
```

config wlan override-rate-limit

To override the bandwidth limits for upstream and downstream traffic per user and per service set identifier (SSID) defined in the QoS profile, use the **config wlan override-rate-limit** command.

config wlan override-rate-limit *wlan_id* { **average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate** } { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
average-data-rate	Specifies the average data rate for TCP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
average-realtime-rate	Specifies the average real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
burst-data-rate	Specifies the peak data rate for TCP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
burst-realtime-rate	Specifies the peak real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,200 Kbps.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
<i>rate</i>	Data rate for TCP or UDP traffic per user or per SSID. The range is from 0 to 51,200 Kbps. A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None.

Usage Guidelines

The rate limits are enforced by the controller and the AP. For central switching, the controller handles the downstream enforcement of per-client rate limit and the AP handles the enforcement of the upstream traffic and per-ssid rate limit for downstream traffic. When the AP enters standalone mode it handles the downstream enforcement of per-client rate limits too.

In FlexConnect local switching and standalone modes, per-client and per-ssid rate limiting is done by the AP for downstream and upstream traffic. However, in FlexConnect standalone mode, the configuration is not

saved on the AP, so when the AP reloads, the configuration is lost and rate limiting does not happen after reboot.

For roaming clients, if the client roams between the APs on the same controller, same rate limit parameters are applied on the client. However, if the client roams from an anchor to a foreign controller, the per-client downstream rate limiting uses the parameters configured on the anchor controller while upstream rate limiting uses the parameters of the foreign controller.

Examples

This example shows how to configure the burst real-time actual rate 2000 Kbps for the upstream traffic per SSID:

```
> config wlan override-rate-limit 2 burst-realtime-rate per-ssid upstream 2000
```

Related Commands

config qos average-realtime-rate

config qos average-data-rate

config qos burst-data-rate

config qos burst-realtime-rate

show qos

show wlan

show client details

show ap stats

config wlan interface

To configure a wireless LAN interface or an interface group, use the **config wlan interface** command.

config wlan interface {*wlan_id* | **foreignAp**} {*interface-name* | *interface-group-name*}

Syntax Description

<i>wlan_id</i>	(Optional) Wireless LAN identifier (1 to 512).
foreignAp	Specifies third-party access points.
<i>interface-name</i>	Interface name.
<i>interface-group-name</i>	Interface group name.

Command Default

None.

Examples

This example shows how to configure an interface named VLAN901:

```
> config wlan interface 16 VLAN901
```

Related Commands

show wlan

config wlan ipv6 acl

To configure IPv6 access control list (ACL) on a wireless LAN, use the **config wlan ipv6 acl** command.

```
config wlan ipv6 acl wlan_id acl_name
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>acl_name</i>	IPv6 ACL name.

Command Default

None.

Examples

This example shows how to configure an IPv6 ACL for local switching:

```
> config wlan ipv6 acl 22 acl_sample
```

Related Commands

show wlan

config wlan kts-cac

To configure the Key Telephone System-based CAC policy for a WLAN, use the **config wlan kts-cac** command.

config wlan kts-cac {enable | disable} *wlan_id*

Syntax Description

enable	Enables the KTS-based CAC policy.
disable	Disables the KTS-based CAC policy.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

To enable the KTS-based CAC policy for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:
config wlan qos *wlan-id* platinum
- Disable the WLAN by entering the following command:
config wlan disable *wlan-id*
- Disable FlexConnect local switching for the WLAN by entering the following command:
config wlan flexconnect local-switching *wlan-id* disable

Examples

This example shows how to enable the KTS-based CAC policy for a WLAN with the ID 4:

```
> config wlan kts-cac enable 4
```

Related Commands

config wlan
config wlan qos
config wlan flexconnect local-switching
config wlan wmm
config 802.11a cac voice

config wlan ldap

To add or delete a link to a configured Lightweight Directory Access Protocol (LDAP) server, use the **config wlan ldap** command.

```
config wlan ldap {add wlan_id server_id | delete wlan_id {all | server_id}}
```

Syntax Description

add	Adds a link to a configured LDAP server.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>server_id</i>	LDAP server index.
delete	Removes the link to a configured LDAP server.
all	Specifies all LDAP servers.

Command Default

None.

Usage Guidelines

Use this command to specify the LDAP server priority for the WLAN.

To specify the LDAP server priority, one of the following must be configured and enabled:

- 802.1X authentication and Local EAP
- Web authentication and LDAP



Note Local EAP was introduced in controller software release 4.1; LDAP support on Web authentication was introduced in controller software release 4.2.

Examples

This example shows how to add a link to a configured LDAP server with the WLAN ID 100 and server ID 4:

```
> config wlan ldap add 100 4
```

Related Commands

config ldap

config wlan load-balance

To override the global load balance configuration and enable or disable load balancing on a particular WLAN, use the **config wlan load-balance** command.

config wlan load-balance allow {enable | disable} *wlan_id*

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Examples

This example shows how to enable band selection on a wireless LAN with WLAN ID 3:

```
> config wlan load-balance allow enable 3
```

Related Commands

config load-balancing

config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the **config wlan mac-filtering** command.

```
config wlan mac-filtering {enable | disable} {wlan_id | foreignAp}
```

Syntax Description

enable	Enables MAC filtering on a wireless LAN.
disable	Disables MAC filtering on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to enable the MAC filtering on WLAN ID 1:

```
> config wlan mac-filtering enable 1
```

Related Commands

show wlan

config wlan max-associated-clients

To configure the maximum number of client connections on a wireless LAN, guest LAN, or remote LAN, use the **config wlan max-associated-clients** command.

config wlan max-associated-clients *max_clients* *wlan_id*

Syntax Description

<i>max_clients</i>	Maximum number of client connections to be accepted.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to specify the maximum number of client connections on WLAN ID 2:

```
> config wlan max-associated-clients 25 2
```

Related Commands

show wlan

config wlan max-radio-clients

To configure the maximum number of WLAN client per access point, use the **config wlan max-radio-clients** command.

```
config wlan max-radio-clients max_radio_clients wlan_id
```

Syntax Description

<i>max_radio_clients</i>	Maximum number of client connections to be accepted per access point radio. The valid range is from 1 to 200.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to specify the maximum number of client connections per access point radio on WLAN ID 2:

```
> config wlan max-radio-clients 25 2
```

Related Commands

show wlan

config wlan mdns

To configure an multicast DNS (mDNS) profile for a WLAN, use the **config wlan mdns** command.

config wlan mdns {enable | disable | profile {*profile-name* | none}} {*wlan_id* | all}

Syntax Description

enable	Enables mDNS snooping on a WLAN.
disable	Disables mDNS snooping on a WLAN.
profile	Configures an mDNS profile for a WLAN.
<i>profile-name</i>	Name of the mDNS profile to be associated with a WLAN.
none	Removes all existing mDNS profiles from the WLAN. You cannot configure mDNS profiles on the WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
all	Configures the mDNS profile for all WLANs.

Command Default

Enabled.

Usage Guidelines

You must disable the WLAN before you use this command. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

Examples

This example shows how to configure an mDNS profile for a WLAN:

```
> config wlan mdns profile profile1 1
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config mdns profile
show mdns profile
show mnds service
clear mdns service-database

debug mdns all
debug mdns error
debug mdns detail
debug mdns message

config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Syntax Description

multicast-direct	Configures multicast-direct for a wireless LAN media stream.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all media streams.
enable	Enables global multicast to unicast conversion.
disable	Disables global multicast to unicast conversion.

Command Default

None.

Usage Guidelines

Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

Examples

This example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
> config wlan media-stream multicast-direct 2 enable
```

Related Commands

config wlan
config wlan qos
show wlan

config wlan mfp

To configure management frame protection (MFP) options for the wireless LAN, use the **config wlan mfp** command.

```
config wlan mfp {client [enable | disable] wlan_id | infrastructure protection [enable | disable] wlan_id}
```

Syntax Description

client	Configures client MFP for the wireless LAN.
enable	(Optional) Enables the feature.
disable	(Optional) Disables the feature.
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
infrastructure protection	(Optional) Configures the infrastructure MFP for the wireless LAN.

Command Default

None.

Examples

This example shows how to configure client management frame protection for WLAN ID 1:

```
> config wlan mfp client enable 1
```

Related Commands

```
show wlan  
show run-config
```

config wlan mobility anchor

To change the state of MAC filtering on a wireless LAN, use the **config wlan mobility anchor** command.

config wlan mobility anchor {add | delete} *wlan_id ip_address*

Syntax Description

add	Enables MAC filtering on a wireless LAN.
delete	Disables MAC filtering on a wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>ip_address</i>	Member switch IP address for anchoring the wireless LAN.

Command Default

None.

Examples

This example shows how to configure the mobility wireless LAN anchor list with WLAN ID 4 and IP address 192.168.0.14:6:

```
> config wlan mobility anchor add 4 192.168.0.14
```

Related Commands

config guest-lan mobility anchor
config mobility group domain
config mobility group keepalive count
config mobility group keepalive interval
config mobility group member
config mobility group multicast-address
config mobility multicast-mode
config mobility secure-mode
config mobility statistics reset
debug mobility
show mobility anchor
show mobility statistics
show mobility summary
config wlan mobility foreign-map

config wlan mobility foreign-map

To configure interfaces or interface groups for foreign controllers, use the **config wlan mobility foreign-map** command.

config wlan mobility foreign-map {**add** | **delete**} *wlan_id* *foreign_mac_address* {*interface_name* | *interface_group_name*}

Syntax Description

add	Adds an interface or interface group to the map of foreign controllers.
delete	Deletes an interface or interface group from the map of foreign controllers.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>foreign_mac_address</i>	Foreign switch MAC address on WLAN.
<i>interface_name</i>	Interface name up to 32 alphanumeric characters.
<i>interface_group_name</i>	Interface group name up to 32 alphanumeric characters.

Command Default

None.

Examples

This example shows how to add an interface group for foreign controllers with WLAN ID 4 and a foreign switch MAC address on WLAN 00:21:1b:ea:36:60:

```
> config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```

Related Commands

config wlan mobility anchor
config mobility group member
debug mobility
show mobility anchor
show mobility summary

config wlan multicast buffer

To configure the radio multicast packet buffer size, use the **config wlan multicast buffer** command.

config wlan multicast buffer {enable | disable} *buffer-size*

Syntax Description

enable	Enables the multicast interface feature for a wireless LAN.
disable	Disables the multicast interface feature on a wireless LAN.
<i>buffer-size</i>	Radio multicast packet buffer size. The range is from 30 to 60. Enter 0 to indicate APs will dynamically adjust the number of buffers allocated for multicast.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

30.

Examples

This example shows how to configure radio multicast buffer settings:

```
> config wlan multicast buffer enable 45 222
```

Related Commands

config 802.11a multicast data-rate

config wlan multicast interface

To configure a multicast interface for a wireless LAN, use the **config wlan multicast interface** command.

```
config wlan multicast interface wlan_id {enable | disable} interface_name
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
enable	Enables multicast interface feature for a wireless LAN.
delete	Disables multicast interface feature on a wireless LAN.
<i>interface_name</i>	Interface name. Note The interface name can only be specified in lower case characters.

Command Default

Multicast is disabled.

Examples

This example shows how to enable the multicast interface feature for a wireless LAN with WLAN ID 4 and interface name myinterface1:

```
> config wlan multicast interface 4 enable myinterface1
```

Related Commands

```
config guest-lan mobility anchor  
config mobility group domain  
config mobility group keepalive count  
config mobility group keepalive interval  
config mobility group member  
config mobility group multicast-address  
config mobility multicast-mode  
config mobility secure-mode  
config mobility statistics reset  
debug mobility  
show mobility anchor  
show mobility statistics  
show mobility summary  
config wlan mobility foreign-map
```

config wlan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a WLAN, use the **config wlan nac** command.

```
config wlan nac {snmp | radius} {enable | disable} wlan_id
```

Syntax Description

snmp	Configures SNMP NAC support.
radius	Configures RADIUS NAC support
enable	Enables NAC for the WLAN.
disable	Disables NAC for the WLAN.
<i>wlan_id</i>	WLAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

You should enable AAA override before you enable the Radius NAC state. You also should disable FlexConnect local switching before you enable the Radius NAC state.

Examples

This example shows how to configure SNMP NAC support for WLAN 13:

```
> config wlan nac snmp enable 13
```

This example shows how to configure RADIUS NAC support for WLAN 34:

```
> config wlan nac radius enable 20
```

Related Commands

```
show nac statistics  
show nac summary  
config guest-lan nac  
debug nac
```

config wlan passive-client

To configure passive-client feature on a wireless LAN, use the **config wlan passive-client** command.

```
config wlan passive-client {enable | disable} wlan_id
```

Syntax Description

enable	Enables the passive-client feature on a WLAN.
disable	Disables the passive-client feature on a WLAN.
<i>wlan_id</i>	WLAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

You need to enable the global multicast mode and multicast-multicast mode by using the **config network multicast global** and **config network multicast mode multicast** commands before entering this command.



Note

You should configure the multicast in multicast-multicast mode only not in unicast mode. The passive client feature does not work with multicast-unicast mode in this release.

Examples

This example shows how to configure the passive client on wireless LAN ID 2:

```
> config wlan passive-client enable 2
```

Related Commands

```
config wlan
config network multicast global
config network multicast mode multicast
show wlan
```

config wlan peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **config wlan peer-blocking** command.

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

Syntax Description		
disable		Disables peer-to-peer blocking and bridge traffic locally within the controller whenever possible.
drop		Causes the controller to discard the packets.
forward-upstream		Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.
<i>wlan_id</i>		WLAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to disable the peer-to-peer blocking for WLAN ID 1:

```
> config wlan peer-blocking disable 1
```

Related Commands **show wlan**

config wlan profiling

To configure client profiling on a WLAN, use the **config wlan profiling** command.

config wlan profiling radius {all | dhcp | http} {enable | disable} wlan_id

Syntax Description

radius	Configures client profiling in RADIUS mode on a WLAN.
all	Configures DHCP and HTTP client profiling in a WLAN.
dhcp	Configures DHCP client profiling alone in a WLAN.
http	Configures HTTP client profiling in a WLAN.
enable	Enables the specific type of client profiling in a WLAN. When you enable HTTP profiling , the controller collects the HTTP attributes of clients for profiling. When you enable DHCP profiling , the controller collects the DHCP attributes of clients for profiling.
disable	Disables the specific type of client profiling in a WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Usage Guidelines

Ensure that you have disabled the WLAN before configuring client profiling on the WLAN.

Command Default

Disabled.

Usage Guidelines

Only clients connected to port 80 for HTTP can be profiled. IPv6 only clients will not be profiled.

If a session timeout is configured for a WLAN, clients must send the HTTP traffic before the configured timeout to get profiled.

This feature is not supported on the following:

- FlexConnect Standalone mode
- FlexConnect Local Authentication

Examples

This example shows how to enable both DHCP and HTTP profiling on a WLAN:

```
> config wlan profiling radius all enable 6
    HTTP Profiling successfully enabled.
    DHCP Profiling successfully enabled.
```

Related Commands `show wlan`

config wlan qos

To change the quality of service for a wireless LAN, use the **config wlan qos** command.

```
config wlan qos wlan_id {bronze | silver | gold | platinum}
```

```
config wlan qos foreignAp {bronze | silver | gold | platinum}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
bronze	Specifies the bronze QoS policy.
silver	Specifies the silver QoS policy.
gold	Specifies the gold QoS policy.
platinum	Specifies the platinum QoS policy.

Command Default

Silver.

Examples

This example shows how to set the highest level of service on wireless LAN 1:

```
> config wlan qos 1 gold
```

Related Commands

show wlan

config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

```
config wlan radio wlan_id {all | 802.11a | 802.11bg | 802.11g | 802.11ag}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all radio bands.
802.11a	Configures the wireless LAN on only 802.11a.
802.11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled).
802.11g	Configures the wireless LAN on 802.11g only.

Command Default

None.

Examples

This example shows how to configure the wireless LAN on all radio bands:

```
> config wlan radio 1 all
```

Related Commands

```
config 802.11a enable  
config 802.11a disable  
config 802.11b enable  
config 802.11b disable  
config 802.11b 11gSupport enable  
config 802.11b 11gSupport disable  
show wlan
```

config wlan radius_server acct

To configure RADIUS accounting servers of a WLAN, use the **config wlan radius_server acct** command.

```
config wlan radius_server acct {enable | disable} wlan_id | {add wlan_id server_id | delete wlan_id {all | server_id}}
```

Syntax Description

enable	Enables RADIUS accounting for the WLAN.
disable	Disables RADIUS accounting for the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
add	Adds a link to a configured RADIUS accounting server.
<i>server_id</i>	RADIUS server index.
delete	Deletes a link to a configured RADIUS accounting server.

Command Default

None.

Examples

This example shows how to enable RADIUS accounting for the WLAN 2:

```
> config wlan radius_server acct enable 2
```

This example shows how to add a link to a configured RADIUS accounting server:

```
> config wlan radius_server acct add 2 5
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

config wlan radius_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius_server acct interim-update** command.

```
config wlan radius_server acct interim-update {interval | enable | disable} wlan_id
```

Syntax Description

interim-update	Configures the interim update of the RADIUS accounting server.
<i>interval</i>	Interim update interval that you specify. The valid range is 180 seconds to 3600 seconds.
enable	Enables interim update of the RADIUS accounting server for the WLAN.
disable	Disables interim update of the RADIUS accounting server for the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Enabled at 600 seconds.

Examples

This example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
> config wlan radius_server acct interim-update 200 2
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

config wlan radius_server auth

To configure RADIUS authentication servers of a WLAN, use the **config wlan radius_server auth** command.

```
config wlan radius_serverauth {enable wlan_id | disable wlan_id} {add wlan_id server_id | delete wlan_id
{all | server_id}}
```

Syntax Description

auth	Configures a RADIUS authentication
enable	Enables RADIUS authentication for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
disable	Disables RADIUS authentication for this WLAN.
add	Adds a link to a configured RADIUS server.
<i>server_id</i>	RADIUS server index.
delete	Deletes a link to a configured RADIUS server.
all	Deletes all links to configured RADIUS servers.

Command Default

None.

Examples

This example shows how to add a link to a configured RADIUS authentication server with WLAN ID 1 and Server ID 1:

```
> config wlan radius_server auth add 1 1
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

config wlan radius_server acct interim-update

To configure a wireless LAN's RADIUS servers, use the **config wlan radius_server acct interim-update** command.

config wlan radius_server acct interim-update {enable *wlan_id* | disable *wlan_id*} {interval *wlan_id*}

Syntax Description

enable	Enables RADIUS authentication or accounting for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
disable	Disables RADIUS authentication or accounting for this WLAN.
<i>interval</i>	Accounting interim interval between 180 to 3600 seconds.

Command Default

None.

Usage Guidelines

This command helps to set some time as a default if the timeout interval is not specified.

Examples

This example shows how to force the 10 minutes as the default, if timeout interval is not specified:

```
> config wlan radius_server acct interim-update 600 1
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

config wlan radius_server overwrite-interface

To configure a wireless LAN's RADIUS dynamic interface, use the **config wlan radius_server overwrite-interface** command.

```
config wlan radius_server overwrite-interface {enable | disable} wlan_id
```

Syntax Description

enable	Enables RADIUS dynamic interface for this WLAN.
disable	Disables RADIUS dynamic interface for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

The controller uses the management interface as identity. If the RADIUS server is on a directly connected dynamic interface, the traffic is sourced from the dynamic interface. Otherwise, the management IP address is used.

If the feature is enabled, controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on the WLAN.

Examples

This example shows how to enable RADIUS dynamic interface for a WLAN with an ID 1:

```
> config wlan radius_server overwrite-interface enable 1
```

Related Commands

```
config 802.11a enable
config 802.11a disable
config 802.11b enable
config 802.11b disable
config 802.11b 11gSupport enable
config 802.11b 11gSupport disable
show wlan
```

config wlan roamed-voice-client re-anchor

To configure a roamed voice client's reanchor policy, use the **config wlan roamed-voice-client re-anchor** command.

config wlan roamed-voice-client re-anchor {enable | disable} *wlan_id*

Syntax Description

enable	Enables the roamed client's reanchor policy.
disable	Disables the roamed client's reanchor policy.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Disabled.

Examples

This example shows how to enable a roamed voice client's reanchor policy where WLAN ID is 1:

```
> config wlan roamed-voice-client re-anchor enable 1
```

Related Commands

show wlan

config wlan sip-cac disassoc-client

To enable client disassociation in case of session initiation protocol (SIP) call admission control (CAC) failure, use the **config wlan sip-cac disassoc-client** command.

```
config wlan sip-cac disassoc-client {enable | disable} wlan_id
```

Syntax Description

enable	Enables a client disassociation on a SIP CAC failure.
disable	Disables a client disassociation on a SIP CAC failure.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Disabled.

Examples

This example shows how to enable a client disassociation on a SIP CAC failure where the WLAN ID is 1:

```
> config wlan sip-cac disassoc-client enable 1
```

Related Commands

```
show wlan  
config wlan sip-cac send-486busy
```

config wlan sip-cac send-486busy

To configure sending session initiation protocol (SIP) 486 busy message if a SIP call admission control (CAC) failure occurs, use the **config wlan sip-cac send-486busy** command:

```
config wlan sip-cac send-486busy {enable | disable} wlan_id
```

Syntax Description

enable	Enables sending a SIP 486 busy message upon a SIP CAC failure.
disable	Disables sending a SIP 486 busy message upon a SIP CAC failure.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Examples

This example shows how to enable sending a SIP 486 busy message upon a SIP CAC failure where the WLAN ID is 1:

```
> config wlan sip-cac send-busy486 enable 1
```

Related Commands

show wlan
config wlan sip-cac disassoc-client

config wlan static-ip tunneling

To configure static IP client tunneling support on a WLAN, use the **config wlan static-ip tunneling** command.

```
config wlan static-ip tunneling {enable | disable} wlan_id
```

Syntax Description

tunneling	Configures static IP client tunneling support on a WLAN.
enable	Enables static IP client tunneling support on a WLAN.
disable	Disables static IP client tunneling support on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable static IP client tunneling support for WLAN ID 3:

```
> config wlan static-ip tunneling enable enable 34
```

Related Commands

```
config wlan  
show wlan
```

config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

config wlan timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>seconds</i>	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None.

Examples

This example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
> config wlan session-timeout 1 6000
```

Related Commands

show wlan

config wlan user-idle-threshold

To configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN, use the **config wlan user-idle-threshold** command.

config wlan user-idle-threshold *bytes wlan_id*

Syntax Description

<i>bytes</i>	Threshold data sent by the client during the idle timeout for the client session for a WLAN. If the client send traffic less than the defined threshold, the client is removed on timeout. The range is from 0 to 10000000 bytes.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

The default is 0 bytes.

Examples

This example shows how to configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN:

```
> config wlan user-idle-threshold 100 1
```

Related Commands

config network usertimeout
config wlan usertimeout

config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

config wlan usertimeout *timeout wlan_id*

Syntax Description

<i>timeout</i>	Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

300 seconds.

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

Examples

This example shows how to configure the idle client sessions for a WLAN:

```
> config wlan usertimeout 100 1
```

Related Commands

config network usertimeout

config wlan user-idle-threshold

config wlan webauth-exclude

To release the guest user IP address when the web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

```
config wlan webauth-exclude wlan_id {enable | disable}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier (1 to 512).
enable	Enables web authentication exclusion.
disable	Disables web authentication exclusion.

Command Default

Disabled.

Usage Guidelines

You can use this command for guest WLANs that are configured with web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

Examples

This example shows how to enable the web authentication exclusion for WLAN ID 5:

```
> config wlan webauth-exclude 5 enable
```

Related Commands

```
config dhcp  
show run-config  
show wlan
```

config wlan wmm

To configure Wi-Fi Multimedia (WMM) mode on a wireless LAN, use the **config wlan wmm** command.

```
config wlan wmm {allow | disable | require} wlan_id
```

Syntax Description

allow	Allows WMM on the wireless LAN.
disable	Disables WMM on the wireless LAN.
require	Specifies that clients use WMM on the specified wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier (1 to 512).

Command Default

None.

Usage Guidelines

When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

Examples

This example shows how to configure wireless LAN ID 1 to allow WMM:

```
> config wlan wmm allow 1
```

This example shows how to configure wireless LAN ID 1 to specify that clients use WMM:

```
> config wlan wmm require 1
```

Related Commands

show wlan

show run-config

Configure Wireless LAN HotSpot Commands

Use the **config wlan hotspot** commands to configure HotSpot and 802.11u parameters on a WLAN.

config advanced hotspot

To configure advanced HotSpot configurations, use the **config advanced hotspot** command.

```
config advanced hotspot {anqp-4way {disable | enable | threshold value } | cmbk-delay value | garp
{disable | enable } | gas-limit {disable | enable } }
```

Syntax Description

anqp-4way	Enables, disables, or, configures the Access Network Query Protocol (ANQP) four way fragment threshold.
disable	Disables the ANQP four way message.
enable	Enables the ANQP four way message.
threshold	Configures the ANQP fourway fragment threshold.
<i>value</i>	ANQP four way fragment threshold value in bytes. The range is from 10 to 1500. The default value is 1500.
cmbk-delay	Configures the ANQP comeback delay in TUs,
<i>value</i>	ANQP comeback delay in Time Units (TUs). 1 TU is defined by 802.11 as 1024 usec. The range is from 1 milliseconds to 30 seconds.
garp	Disables or enables the Gratuitous ARP (GARP) forwarding to wireless network.
disable	Disables the Gratuitous ARP (GARP) forwarding to wireless network.
enable	Enables the Gratuitous ARP (GARP) forwarding to wireless network.
gas-limit	Limits the number of Generic Advertisement Service (GAS) request action frames sent to the switch by an access point in a given interval.
disable	Disables the GAS request action frame limit on access points.
enable	Enables the GAS request action frame limit on access points.

Examples

This example shows how to configure the ANQP four way fragment threshold value:

```
> config advanced hotspot anqp-4way threshold 200
```

Related Commands

```
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
```

```
config wlan apgroup hotspot operating-class
config ap hotspot venue
config wlan security wpa gtk-random
config wlan hotspot dot11u
config wlan hotspot clear-all
config wlan hotspot msap
```

config wlan hotspot

To configure a HotSpot on a WLAN, use the **config wlan hotspot** command.

```
config wlan hotspot {clear-all wlan_id | dot11u | hs2 | msap}
```

Syntax Description

clear-all	Clears the HotSpot configurations on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
dot11u	Configures an 802.11u HotSpot on a WLAN.
hs2	Configures HotSpot2 on a WLAN.
msap	Configures the Mobility Services Advertisement Protocol (MSAP) on a WLAN.

Command Default

None.

Usage Guidelines

You can configure up to 32 HotSpot WLANs.

Examples

This example shows how to configure HotSpot2 for a WLAN:

```
> config wlan hotspot hs2 enable 2
```

Related Commands

```
show wlan  
debug hotspot events  
debug hotspot packets  
config wlan apgroup hotspot venue  
config wlan apgroup hotspot operating-class  
config ap hotspot venue  
config advanced hotspot  
show advanced hotspot  
config wlan security wpa gtk-random
```

config wlan hotspot dot11u

To configure an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u** command.

config wlan hotspot dot11u {**3gpp-info** | **auth-type** | **enable** | **disable** | **domain** | **hessid** | **ipaddr-type** | **nai-realm** | **network-type** | **roam-oi**}

Syntax Description

3gpp-info	Configures 3GPP cellular network information.
auth-type	Configures the network authentication type.
enable	Enables 802.11u on the HotSpot profile. IEEE 802.11u enables automatic WLAN offload for 802.1X devices at the HotSpot of mobile or roaming partners.
disable	Disables 802.11u on the HotSpot profile.
domain	Configures a domain.
hessid	Configures the Homogenous Extended Service Set Identifier (HESSID). The HESSID is a 6-octet MAC address that uniquely identifies the network.
ipaddr-type	Configures the IP address availability type.
nai-realm	Configures a realm for 802.11u enabled WLANs.
network-type	Configures the 802.11u network type and Internet access.
roam-oi	Configures the roaming consortium Organizational Identifier (OI) list.

Command Default

None.

Examples

This example shows how to enable 802.11u on a HotSpot profile:

```
> config wlan hotspot dot11u enable 6
```

Related Commands

show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot

```
show advanced hotspot
config wlan security wpa gtk-random
```

config wlan hotspot dot11u 3gpp-info

To configure 3GPP cellular network information on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u 3gpp-info** command.

config wlan hotspot dot11u 3gpp-info {**add** | **delete**} *index country_code network_code wlan_id*

Syntax Description

add	Adds mobile cellular network information.
delete	Deletes mobile cellular network information.
<i>index</i>	Cellular index. The range is from 1 to 32.
<i>country_code</i>	Mobile Country Code (MCC) in Binary Coded Decimal (BCD) format. The country code can be up to 3 characters. For example, the MCC for USA is 310.
<i>network_code</i>	Mobile Network Code (MNC) in BCD format. An MNC is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator or carrier. The network code can be up to 3 characters. For example, the MNC for T-Mobile is 026.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Usage Guidelines

Number of mobile network codes supported is 32 per WLAN.

Examples

This example shows how to configure 3GPP cellular network information on a WLAN:

```
> config wlan hotspot dot11u 3gpp-info add
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets

```
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random
```

config wlan hotspot dot11u auth-type

To configure the network authentication type on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u auth-type** command.

config wlan hotspot dot11u auth-type *network-auth wlan_id*

Syntax Description

<i>network-auth</i>	Network authentication that you would like to configure on the WLAN. The available values are as follows: <ul style="list-style-type: none"> • 0—Acceptance of terms and conditions • 1—On-line enrollment • 2—HTTP/HTTPS redirection • 3—DNS Redirection • 4—Not Applicable
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Usage Guidelines

The DNS redirection option is not supported in Release 7.3.

Examples

This example shows how to configure HTTP/HTTPS redirection as the network authentication type on an 802.11u HotSpot WLAN:

```
> config wlan hotspot dot11u auth-type 2 1
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue

```
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random
```

config wlan hotspot dot11u disable

To disable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u disable** command.

config wlan hotspot dot11u disable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
----------------	--

Examples

This example shows how to disable an 802.11u HotSpot on a WLAN:

```
> config wlan hotspot dot11u disable 6
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advance hotspot gas-limit
config wlan security wpa gtk-random

config wlan hotspot dot11u domain

To configure a domain operating in the 802.11 access network, use the **config wlan hotspot dot11u domain** command.

config wlan hotspot dot11u domain {**add** *wlan_id domain-index domain_name* | **delete** *wlan_id domain-index* | **modify** *wlan_id domain-index domain_name*}

Syntax Description

add	Adds a domain.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>domain-index</i>	Domain index in the range 1 to 32.
<i>domain_name</i>	Domain name. The domain name is case sensitive and can be up to 255 alphanumeric characters.
delete	Deletes a domain.
modify	Modifies a domain.

Examples

This example shows how to add a domain in the 802.11 access network:

```
> config wlan hotspot dot11u domain add 6 30 domain1
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue

```
config advanced hotspot
config wlan security wpa gtk-random
```

config wlan hotspot dot11u enable

To enable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u enable** command.

```
config wlan hotspot dot11u enable wlan_id
```

Syntax Description

wlan_id

Wireless LAN identifier between 1 and 512.

Examples

This example shows how to enable an 802.11u HotSpot on a WLAN:

```
> config wlan hotspot dot11u enable 6
```

Related Commands

```
config wlan hotspot dot11u disable  
config wlan hotspot dot11u 3gpp-info  
config wlan hotspot dot11u domain  
config wlan hotspot dot11u hessid  
config wlan hotspot dot11u auth-type  
config wlan hotspot dot11u ipaddr-type  
config wlan hotspot dot11u nai-realm  
config wlan hotspot dot11u network-type  
config wlan hotspot dot11u roam-oi  
show wlan  
debug hotspot events  
debug hotspot packets  
config wlan apgroup hotspot venue  
config wlan apgroup hotspot operating-class  
config ap hotspot venue  
config advance hotspot gas-limit  
config wlan security wpa gtk-random
```

config wlan hotspot dot11u hessid

To configure a Homogenous Extended Service Set Identifier (HESSID) on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u hessid** command.

config wlan hotspot dot11u hessid *hessid wlan_id*

Syntax Description

<i>hessid</i>	MAC address that can be configured as an HESSID. The HESSID is a 6-octet MAC address that uniquely identifies the network. For example, Basic Service Set Identification (BSSID) of the WLAN can be used as the HESSID.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Examples

This example shows how to configure an HESSID on an 802.11u HotSpot WLAN:

```
> config wlan hotspot dot11u hessid 00:21:1b:ea:36:60 6
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random

config wlan hotspot dot11u ipaddr-type

To configure the type of IP address available on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u ipaddr-type** command.

config wlan hotspot dot11u ipaddr-type *IPv4Type IPv6Type wlan_id*

Syntax Description

<i>IPv4Type</i>	IPv4 type address. Enter one of the following values: 0—IPv4 address not available. 1—Public IPv4 address available. 2—Port restricted IPv4 address available. 3—Single NAT enabled private IPv4 address available. 4—Double NAT enabled private IPv4 address available. 5—Port restricted IPv4 address and single NAT enabled IPv4 address available. 6—Port restricted IPv4 address and double NAT enabled IPv4 address available. 7— Availability of the IPv4 address is not known.
<i>IPv6Type</i>	IPv6 type address. Enter one of the following values: 0—IPv6 address not available. 1—IPv6 address available. 2—Availability of the IPv6 address is not known.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

The default values for IPv4 type address is 1 and for IPv6 type address is 2.

Examples

This example shows how to configure the IP address availability type on an 802.11u HotSpot WLAN:

```
> config wlan hotspot dot11u ipaddr-type 6 2 6
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type

```
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random
```

config wlan hotspot dot11u nai-realm

To configure realms for an 802.11u HotSpot WLANs, use the **config wlan hotspot dot11u nai-realm** command.

```
config wlan hotspot dot11u nai-realm {add | delete | modify} {auth-method wlan_id realm-index eap-index
auth-index auth-method auth-parameter | eap-method wlan_id realm-index eap-index eap-method |
realm-name wlan_id realm-index realm}
```

Syntax Description

add	Adds a realm.
delete	Deletes a realm.
modify	Modifies a realm.
auth-method	Specifies the authentication method used.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>realm-index</i>	Realm index. The range is from 1 to 32.
<i>eap-index</i>	EAP index. The range is from 1 to 4.
<i>auth-index</i>	Authentication index value. The range is from 1 to 10.
<i>auth-method</i>	Authentication method to be used. The range is from 1 to 4. The following options are available: <ul style="list-style-type: none"> • 1—Non-EAP Inner Auth Method • 2—Inner Auth Type • 3—Credential Type • 4—Tunneled EAP Method Credential Type
<i>auth-parameter</i>	Authentication parameter to use. This value depends on the authentication method used. See the following table for more details.
eap-method	Specifies the Extensible Authentication Protocol (EAP) method used.

<i>eap-method</i>	EAP Method. The range is from 0 to 7. The following options are available: <ul style="list-style-type: none"> • 0—Not Applicable • 1—Lightweight Extensible Authentication Protocol (LEAP) • 2—Protected EAP (PEAP) • 3—EAP-Transport Layer Security (EAP-TLS) • 4—EAP-FAST (Flexible Authentication via Secure Tunneling) • 5—EAP for GSM Subscriber Identity Module (EAP-SIM) • 6—EAP-Tunneled Transport Layer Security (EAP-TTLS) • 7—EAP for UMTS Authentication and Key Agreement (EAP-AKA)
realm-name	Specifies the name of the realm.
<i>realm</i>	Name of the realm. The realm name should be RFC 4282 compliant. For example, Cisco. The realm name is case-sensitive and can be up to 255 alphanumeric characters.

Usage Guidelines

The following table lists the Authentication Parameters:

Table 2: Authentication Parameters

Non-EAP Inner Method(1)	Inner Authentication EAP method type(2)	Credential Type(3)/Tunneled EAP Credential Type(4)
0—Reserved	1—LEAP	1—SIM
1—Password authentication protocol (PAP)	2—PEAP	2—USIM
2—Challenge-Handshake Authentication Protocol (CHAP)	3—EAP-TLS	3—NFC Secure Element
3—Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)	4—EAP-FAST	4—Hardware Token
4—MSCHAPV2	5—EAP-SIM	5—Soft Token
	6—EAP-TTLS	6—Certificate
	7—EAP-AKA	7—Username/Password
		8—Reserver
		9—Anonymous
		10—Vendor Specific

Examples

This example shows how to add the Tunneled EAP Method Credential authentication method on WLAN 4:

```
> config wlan hotspot dot11u nai-realm add auth-method 4 10 3 5 4 6
```

Related Commands

config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u network-type
config wlan hotspot dot11u roam-oi
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random

config wlan hotspot dot11u network-type

To configure the network type and internet availability on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u network-type** command.

config wlan hotspot dot11u network-type *wlan_id network-type internet-access*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.
<i>network-type</i>	Network type. The available options are as follows: <ul style="list-style-type: none"> • 0—Private Network • 1—Private Network with Guest Access • 2—Chargeable Public Network • 3—Free Public Network • 4—Personal Device Network • 5—Emergency Services Only Network • 14—Test or Experimental • 15—Wildcard
<i>internet-access</i>	Internet availability status. A value of zero indicates no Internet availability and 1 indicates Internet availability.

Examples

This example shows how to configure the network type and Internet availability on an 802.11u HotSpot WLAN:

```
> config wlan hotspot dot11u network-type 2 1
```

Related Commands

```
config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u roam-oi
show wlan
```

debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random

config wlan hotspot dot11u roam-oi

To configure a roaming consortium Organizational Identifier (OI) list on a 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u roam-oi** command.

```
config wlan hotspot dot11u roam-oi {add wlan_id oi-index oi is-beacon | modify wlan_id oi-index oi is-beacon | delete wlan_id oi-index}
```

Syntax Description

add	Adds an OI.
<i>wlan-id</i>	Wireless LAN identifier from 1 to 512.
<i>oi-index</i>	Index in the range 1 to 32.
<i>oi</i>	Number that must be a valid 6 digit hexadecimal number and 6 bytes in length. For example, 004096 or AABBDf.
<i>is-beacon</i>	Beacon flag used to add an OI to the beacon. 0 indicates disable and 1 indicates enable. You can add a maximum of 3 OIs for a WLAN with this flag set.
modify	Modifies an OI.
delete	Deletes an OI.

Examples

This example shows how to configure the roaming consortium OI list:

```
> config wlan hotspot dot11u roam-oi add 4 10 004096 1
```

Related Commands

```
config wlan hotspot dot11u enable
config wlan hotspot dot11u disable
config wlan hotspot dot11u 3gpp-info
config wlan hotspot dot11u domain
config wlan hotspot dot11u hessid
config wlan hotspot dot11u auth-type
config wlan hotspot dot11u ipaddr-type
config wlan hotspot dot11u nai-realm
config wlan hotspot dot11u network-type
show wlan
debug hotspot events
debug hotspot packets
config wlan apgroup hotspot venue
```

```
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random
```

config wlan hotspot hs2

To configure the HotSpot2 parameters, use the **config wlan hotspot hs2** command.

```
config wlan hotspot hs2 {disable wlan_id | enable wlan_id | operator-name {add wlan_id index
operator_name language-code | delete wlan_id index | modify wlan_id index operator-name language-code}
| port-config {add wlan_id port_config_index ip-protocol port-number status | delete wlan_id
port-config-index | modify wlan_id port-config-index ip-protocol port-number status} | wan-metrics wlan_id
link-status symet-link downlink-speed uplink-speed }
```

Syntax Description

disable	Disables HotSpot2.
<i>wlan-id</i>	Wireless LAN identifier from 1 to 512.
enable	Enables HotSpot2.
operator-name	Specifies the name of the 802.11 operator.
add	Adds the operator name, port configuration, or WAN metrics parameters to the WLAN configuration.
<i>index</i>	Index of the operator. The range is from 1 to 32.
<i>operator-name</i>	Name of the operator.
<i>language-code</i>	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.
delete	Deletes the operator name, port configuration, or WAN metrics parameters from the WLAN.
modify	Modifies the operator name, port configuration, or WAN metrics parameters of the WLAN.
port-config	Configures the port configuration values.
<i>port_config_index</i>	Port configuration index. The range is from 1 to 32. The default value is 1.

<i>ip-protocol</i>	<p>Protocol to use. This parameter provides information on the connection status of the most commonly used communication protocols and ports. The following options are available:</p> <ul style="list-style-type: none"> 1—ICMP 6—FTP/SSH/TLS/PPTP-VPN/VoIP 17—IKEv2 (IPSec-VPN/VoIP/ESP) 50—ESP (IPSec-VPN)
<i>port-number</i>	<p>Port number. The following options are available:</p> <ul style="list-style-type: none"> 0—ICMP/ESP (IPSec-VPN) 20—FTP 22—SSH 443—TLS-VPN 500—IKEv2 1723—PPTP-VPN 4500—IKEv2 5060—VoIP
<i>status</i>	<p>Status of the IP port. The following options are available:</p> <ul style="list-style-type: none"> 0—Closed 1—Open 2—Unknown
wan-metrics	Configures the WAN metrics.
<i>link-status</i>	<p>Link status. The following options are available:</p> <ul style="list-style-type: none"> • 0—Unknown • 1—Link up • 2—Link down • 3—Link in test state
<i>symet-link</i>	<p>Symmetric link status. The following options are available:</p> <ul style="list-style-type: none"> • 0—Link speed is different for uplink and downlink. For example: ADSL • 1—Link speed is the same for uplink and downlink. For example: DS1
<i>downlink-speed</i>	<p>Downlink speed of the WAN backhaul link in kbps. Maximum value is 4,194,304 kbps.</p>

*uplink-speed*Uplink speed of the WAN backhaul link in kbps. The maximum value is 4,194,304 kbps.

Examples

This example shows how to configure the WAN metrics parameters:

```
> config wlan hotspot hs2 wan-metrics add 345 1 0 3333
```

Related Commands

show wlan

debug hotspot events

debug hotspot packets

config wlan apgroup hotspot venue

config wlan apgroup hotspot operating-class

config ap hotspot venue

config advanced hotspot gas-limit

config wlan security wpa gtk-random

config wlan hotspot dot11u

config wlan hotspot clear-all

config wlan hotspot msap

config wlan hotspot msap

To configure the Mobility Service Advertisement Protocol (MSAP) parameters on a WLAN, use the **config wlan hotspot msap** command.

```
config wlan hotspot msap {enable | disable | server-id server_id} wlan_id
```

Syntax Description

enable	Enables MSAP on the WLAN.
disable	Disables MSAP on the WLAN.
server-id	Specifies the MSAP server id.
<i>server_id</i>	MSAP server ID. The range is from 1 to 10.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

Examples

This example shows how to enable MSAP on a WLAN:

```
> config wlan hotspot msap enable 4
```

Related Commands

```
show wlan  
debug hotspot events  
debug hotspot packets  
config wlan apgroup hotspot venue  
config wlan apgroup hotspot operating-class  
config ap hotspot venue  
config advanced hotspot  
config wlan security wpa gtk-random  
config wlan hotspot hs2  
config wlan hotspot clear-all  
config wlan hotspot msap
```

Configure Wireless LAN Security Commands

Use the `config wlan security` commands to configure wireless LAN security settings.

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

config wlan security 802.1X {enable {*wlan_id* | foreignAp} | disable {*wlan_id* | foreignAp} | encryption {*wlan_id* | foreignAp} {0 | 40 | 104} | on-macfilter-failure {enable | disable}}

Syntax Description

enable	Enables the 802.1X settings.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
disable	Disables the 802.1X settings.
encryption	Specifies the static WEP keys and indexes.
0	Specifies a WEP key size of 0 (no encryption) bits. The default value is 104. Note All keys within a wireless LAN must be the same size.
40	Specifies a WEP key size of 40 bits. The default value is 104. Note All keys within a wireless LAN must be the same size.
104	Specifies a WEP key size of 104 bits. The default value is 104. Note All keys within a wireless LAN must be the same size.
on-macfilter-failure	Configures 802.1X on MAC filter failure.
enable	Enables 802.1X authentication on MAC filter failure.
disable	Disables 802.1X authentication on MAC filter failure.

Command Default

None.

Usage Guidelines

To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.
- 104—104/128-bit encryption. (This is the default encryption setting.)

Examples

This example shows how to configure 802.1X security on WLAN ID 16:

```
> config wlan security 802.1X enable 16
```

Related Commands

`show wlan`

config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

```
config wlan security ckip {enable | disable} wlan_id [akm psk set-key {hex | ascii} {40 | 104} key key_index
wlan_id | mmh-mic {enable | disable} wlan_id | kp {enable | disable} wlan_id]
```

Syntax Description

enable	Enables CKIP security.
disable	Disables CKIP security.
<i>wlan_id</i>	WLAN to which you apply the command.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex	Specifies a hexadecimal encryption key.
ascii	Specifies an ASCII encryption key.
40	Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
104	Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	Specifies the CKIP WLAN key settings.
<i>key_index</i>	Configured PSK key index.
mmh-mic	(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
kp	(Optional) Configures key-permutation for the CKIP wireless LAN.

Command Default

None.

Examples

This example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
> config wlan security ckip akm psk set-key hex 104 key 2 03
```

Related Commands

```
config wlan ccx aironet-ie
show wlan
```

config wlan security cond-web-redir

To enable or disable conditional web redirect, use the **config wlan security cond-web-redir** command.

config wlan security cond-web-redir {enable | disable} *wlan_id*

Syntax Description

enable	Enables conditional web redirect.
disable	Disables conditional web redirect.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable the conditional web direct on WLAN ID 2:

```
> config wlan security cond-web-redir enable 2
```

Related Commands

show wlan

config wlan security eap-passthru

To configure the 802.1X frames pass through on to the external authenticator, use the **config wlan security eap-passthru** command.

```
config wlan security eap-passthru {enable | disable} wlan_id
```

Syntax Description

enable	Enables 802.1X frames pass through to external authenticator.
disable	Disables 802.1X frames pass through to external authenticator.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable the 802.1X frames pass through to external authenticator on WLAN ID 2:

```
> config wlan security eap-passthru enable 2
```

Related Commands

show wlan

config wlan security ft

To configure 802.11r fast transition parameters, use the **config wlan security ft** command.

config wlan security ft {**enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

enable	Enables 802.11r fast transition roaming support.
disable	Disables 802.11r fast transition roaming support.
reassociation-timeout	Configures reassociation deadline interval.
<i>timeout-in-seconds</i>	Reassociation timeout value in seconds. The valid range is 1 to 100 seconds.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Examples

This example shows how to enable 802.11r fast transition roaming support on WLAN 2:

```
> config wlan security ft enable 2
```

This example shows how to set the reassociation timeout value of 20 seconds for 802.11r fast transition roaming support on WLAN 2:

```
> config wlan security ft reassociation-timeout 20 2
```

Related Commands

show wlan

config wlan security ft over-the-ds

To configure 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** command.

```
config wlan security ft over-the-ds {enable | disable} wlan_id
```

Syntax Description

enable	Enables 802.11r fast transition roaming support over a distributed system.
disable	Disables 802.11r fast transition roaming support over a distributed system.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.
Ensure that 802.11r fast transition is enabled on the WLAN.

Examples

This example shows how to enable 802.11r fast transition roaming support over a distributed system on WLAN ID 2:

```
> config wlan security ft over-the-ds enable 2
```

Related Commands

show wlan

config wlan security IPsec disable

To disable IPsec security, use the **config wlan security IPsec disable** command.

config wlan security IPsec disable {*wlan_id* | **foreignAp**}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to disable the IPsec for WLAN ID 16:

```
> config wlan security IPsec disable 16
```

Related Commands

show wlan

config wlan security IPsec enable

To enable IPsec security, use the **config wlan security IPsec enable** command.

config wlan security IPsec enable {*wlan_id* | **foreignAp**}

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to enable the IPsec for WLAN ID 16:

```
> config wlan security IPsec enable 16
```

Related Commands

show wlan

config wlan security IPsec authentication

To modify the IPsec security authentication protocol used on the wireless LAN, use the **config wlan security IPsec authentication** command.

config wlan security IPsec authentication {**hmac-md5** | **hmac-sha-1**} {*wlan_id* | **foreignAp**}

Syntax Description

hmac-md5	Specifies the IPsec HMAC-MD5 authentication protocol.
hmac-sha-1	Specifies the IPsec HMAC-SHA-1 authentication protocol.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to configure the IPsec HMAC-SHA-1 security authentication parameter for WLAN ID 1:

```
> config wlan security IPsec authentication hmac-sha-1 1
```

Related Commands

show wlan

config wlan security IPsec encryption

To modify the IPsec security encryption protocol used on the wireless LAN, use the **config wlan security IPsec encryption** command.

```
config wlan security IPsec encryption {3des | aes | des} {wlan_id | foreignAp}
```

Syntax Description

3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES 128-bit encryption.
des	Enables IPsec DES encryption.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to configure the IPsec aes encryption:

```
> config wlan security IPsec encryption aes 1
```

Related Commands

show wlan

config wlan security IPsec config

To configure the proprietary Internet Key Exchange (IKE) CFG-Mode parameters used on the wireless LAN, use the **config wlan security IPsec config** command.

config wlan security IPsec config qotd *ip_address* {*wlan_id* | **foreignAp**}

Syntax Description

qotd	Configures the quote-of-the-day server IP for cfg-mode.
<i>ip_address</i>	Quote-of-the-day server IP for cfg-mode.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Usage Guidelines

IKE is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

Examples

This example shows how to configure the quote-of-the-day server IP 44.55.66.77 for cfg-mode for WLAN 1:

```
> config wlan security IPsec config qotd 44.55.66.77 1
```

Related Commands

show wlan

config wlan security IPsec ike authentication

To modify the IPsec Internet Key Exchange (IKE) authentication protocol used on the wireless LAN, use the **config wlan security IPsec ike authentication** command.

config wlan security IPsec ike authentication {**certificates** {*wlan_id* | **foreignAp**} | **pre-share-key** {*wlan_id* | **foreignAp**} *key* | **xauth-psk** {*wlan_id* | **foreignAp**} *key*}

Syntax Description

certificates	Enables the IKE certificate mode.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
pre-share-key	Enables the IKE Xauth with preshared keys.
xauth-psk	Enables the IKE preshared key.
<i>key</i>	Key required for preshare and xauth-psk.

Command Default

None.

Examples

This example shows how to configure the IKE certification mode:

```
> config wlan security IPsec ike authentication certificates 16
```

Related Commands

show wlan

config wlan security IPsec ike dh-group

To modify the IPsec Internet Key Exchange (IKE) Diffie Hellman group used on the wireless LAN, use the **config wlan security IPsec ike dh-group** command.

```
config wlan security IPsec ike dh-group {wlan_id | foreignAp} {group-1 | group-2 | group-5}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
group-1	Specifies DH group 1 (768 bits).
group-2	Specifies DH group 2 (1024 bits).
group-5	Specifies DH group 5 (1536 bits).

Command Default

None.

Examples

This example shows how to configure the Diffie Hellman group parameter for group-1:

```
> config wlan security IPsec ike dh-group 1 group-1
```

Related Commands

show wlan

config wlan security IPsec ike lifetime

To modify the IPsec Internet Key Exchange (IKE) lifetime used on the wireless LAN, use the **config wlan security IPsec ike lifetime** command.

```
config wlan security IPsec ike lifetime {wlan_id | foreignAp} seconds
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>seconds</i>	IKE lifetime in seconds, between 1800 and 345600.

Command Default

None.

Examples

This example shows how to configure the IPsec IKE lifetime use on the wireless LAN:

```
> config wlan security IPsec ike lifetime 1 1900
```

Related Commands

show wlan

config wlan security IPsec ike phase1

To modify IPsec Internet Key Exchange (IKE) Phase 1 used on the wireless LAN, use the **config wlan security IPsec ike phase1** command.

config wlan security IPsec ike phase1 {**aggressive** | **main**} {*wlan_id* | **foreignAp**}

Syntax Description

aggressive	Enables the IKE aggressive mode.
main	Enables the IKE main mode.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to modify IPsec IKE Phase 1:

```
> config wlan security IPsec ike phase1 aggressive 16
```

Related Commands

show wlan

config wlan security IPsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the **config wlan security IPsec ike contivity** command.

```
config wlan security IPsec ike contivity {enable | disable} {wlan_id | foreignAp}
```

Syntax Description

enable	Enables contivity support for this WLAN.
disable	Disables contivity support for this WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to modify Contivity VPN client support:

```
> config wlan security IPsec ike contivity enable 14
```

Related Commands

show wlan

config wlan security passthru

To modify the IPsec pass-through used on the wireless LAN, use the **config wlan security passthru** command.

config wlan security passthru {enable | disable} {wlan_id | foreignAp} [ip_address]

Syntax Description

enable	Enables IPsec pass-through.
disable	Disables IPsec pass-through.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>ip_address</i>	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None.

Examples

This example shows how to modify IPsec pass-through used on the wireless LAN:

```
> config wlan security passthru enable 3 192.12.1.1
```

Related Commands

show wlan

config wlan security pmf

To configure 802.11w Management Frame Protection (MFP) on a WLAN, use the **config wlan security pmf** command.

config wlan security pmf {**disable** | **optional** | **required** | **association-comeback** *association-comeback_timeout* | **saquery-retrytimeout** *saquery-retry_timeout*} *wlan_id*

Syntax Description

disable	Disables 802.11w MFP protection on a WLAN.
optional	Enables 802.11w MFP protection on a WLAN.
required	Requires clients to negotiate 802.11w MFP protection on a WLAN.
association-comeback	Configures the 802.11w association comeback time.
<i>association-comeback_timeout</i>	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later". The range is from 1 to 20 seconds.
saquery-retrytimeout	Configures the 802.11w Security Association (SA) query retry timeout.
<i>saquery-retry_timeout</i>	Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The range is from 100 to 500 ms.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

Command Default

Default SA query retry timeout is 200 milliseconds.

Default association comeback timeout is 1 second.

Usage Guidelines

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (controller) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four way handshake and is used only on WLANs that are configured with WPA or WPA2 security at Layer 2.

Examples

This example shows how to enable 802.11w MFP protection on a WLAN:

```
> config wlan security pmf optional 1
```

Examples

This example shows how to configure the SA query retry timeout on a WLAN:

```
> config wlan security pmf saquery-retrytimeout 300 1
```

Related Commands

show wlan

show client detail

config wlan security wpa akm pmf

debug 11w-pmf

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, use the **config wlan security splash-page-web-redir** command.

```
config wlan security splash-page-web-redir {enable | disable} wlan_id
```

Syntax Description

enable	Enables splash page web redirect.
disable	Disables splash page web redirect.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

Disabled.

Examples

This example shows how to enable splash page web redirect:

```
> config wlan security splash-page-web-redir enable 2
```

Related Commands

show wlan

config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

Syntax Description

shared-key	Enables shared key authentication.
open	Enables open system authentication.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable the static WEP shared key authentication for WLAN ID 1:

```
> config wlan security static-wep-key authentication shared-key 1
```

Related Commands

show wlan

config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

```
config wlan security static-wep-key disable wlan_id
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
----------------	--

Command Default

None.

Examples

This example shows how to disable the static WEP keys for WLAN ID 1:

```
> config wlan security static-wep-key disable 1
```

Related Commands

config wlan security wpa encryption

config wlan security static-wep-key enable

To enable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

```
config wlan security static-wep-key enable wlan_id
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
----------------	--

Command Default

None.

Examples

This example shows how to enable the use of static WEK keys for WLAN ID 1:

```
> config wlan security static-wep-key enable 1
```

Related Commands

config wlan security wpa encryption

config wlan security static-wep-key encryption

To configure the static Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

```
config wlan security static-wep-key encryption wlan_id {40 | 104} {hex | ascii} key key-index
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
40	Specifies the encryption level: 40.
104	Specifies the encryption level: 104.
hex	Specifies to use hexadecimal characters to enter key.
ascii	Specifies whether to use ASCII characters to enter key.
<i>key</i>	WEP key in ASCII.
<i>key-index</i>	Key index (1 to 4).

Command Default

None.

Usage Guidelines

One unique WEP key index can be applied to each wireless LAN. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

Examples

This example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
> config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

Related Commands

show wlan

config wlan security tkip

To configure the Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) countermeasure hold-down timer, use the **config wlan security tkip** command.

config wlan security tkip hold-down *time wlan_id*

Syntax Description

hold-down	Configures the TKIP MIC countermeasure hold-down timer.
<i>time</i>	TKIP MIC countermeasure hold-down time in seconds. The range is from 0 to 60 seconds.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

Command Default

60 seconds.

Usage Guidelines

TKIP countermeasure mode can occur if the access point receives 2 MIC errors within a 60 second period. When this situation occurs, the access point deauthenticates all TKIP clients that are associated to that 802.11 radio and hold offs any clients for the countermeasure holdoff time.

Examples

This example shows how to configure the TKIP MIC countermeasure hold-down timer:

```
> config wlan security tkip
```

Related Commands

show wlan

config wlan security web-auth

To change the status of web authentication used on wireless LAN, use the **config wlan security web-auth** command.

```
config wlan security web-auth {{acl | enable | disable} {wlan_id | foreignAp} [acl_name | none]} |
{on-macfilter-failure wlan_id} | {server-precedence wlan_id | local | ldap | radius} | {flexacl wlan_id
[ipv4_acl_name | none]} | {ipv6 acl wlan_id [ipv6_acl_name | none]}
```

Syntax Description

acl	Configures the access control list.
enable	Enables web authentication.
disable	Disables web authentication.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>acl_name</i>	(Optional) ACL name (up to 32 alphanumeric characters).
none	(Optional) Specifies no ACL name.
on-macfilter-failure	Enables web authentication on MAC filter failure.
server-precedence	Configures the authentication server precedence order for Web-Auth users.
local	Specifies the server type.
ldap	Specifies the server type.
radius	Specifies the server type.
flexacl	Specifies the IPv4 ACL name. You can enter up to 32 alphanumeric characters.
<i>ipv4_acl_name</i>	(Optional) IPv4 ACL name. You can enter up to 32 alphanumeric characters.
<i>ipv6_acl_name</i>	(Optional) IPv6 ACL name. You can enter up to 32 alphanumeric characters.

Command Default

None.

Examples

This example shows how to configure the security policy for WLAN ID 1 and an ACL named ACL03:

```
> config wlan security web-auth acl 1 ACL03
```

Related Commands

`show wlan`

config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

```
config wlan security web-passthrough acl {wlan_id | foreignAp} {acl_name | none}
```

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
<i>acl_name</i>	ACL name (up to 32 alphanumeric characters).
none	Specifies that there is no ACL.

Command Default

None.

Examples

This example shows how to add an ACL to the wireless LAN definition:

```
> config wlan security web-passthrough acl 1 ACL03
```

Related Commands

show wlan

config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

foreignAp Specifies third-party access points.

Command Default

None.

Examples

This example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
> config wlan security web-passthrough disable 1
```

Related Commands

show wlan

config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {enable | disable} {wlan_id | foreignAp}

Syntax Description

email-input	Configures a web captive portal using an e-mail address.
enable	Enables a web captive portal using an e-mail address.
disable	Disables a web captive portal using an e-mail address.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to configure a web captive portal using an e-mail address:

```
> config wlan security web-passthrough email-input enable 1
```

Related Commands

show wlan

config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

foreignAp Specifies third-party access points.

Command Default

None.

Examples

This example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
> config wlan security web-passthrough enable 1
```

Related Commands

show wlan

config wlan security wpa akm 802.1x

To configure authentication key-management using 802.1X, use the **config wlan security wpa akm 802.1x** command.

```
config wlan security wpa akm 802.1x {enable | disable} wlan_id
```

Syntax Description

enable	Enables the 802.1X support.
disable	Disables the 802.1X support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure authentication using 802.1X :

```
> config wlan security wpa akm 802.1x enable 1
```

Related Commands

show wlan

config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command.

```
config wlan security wpa akm cckm {enable wlan_id | disable wlan_id | timestamp-tolerance }
```

Syntax Description

enable	Enables CCKM support.
disable	Disables CCKM support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
<i>timestamp-tolerance</i>	CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; the default is 1000 milliseconds.

Command Default

None.

Examples

This example shows how to configure authentication key-management using CCKM:

```
> config wlan security wpa akm cckm 1500
```

Related Commands

show wlan

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

```
config wlan security wpa akm ft [over-the-air | over-the-ds | psk | [reassociation-timeout seconds]] {enable | disable} wlan_id
```

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
<i>seconds</i>	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure authentication key-management using 802.11r fast transition:

```
> config wlan security wpa akm ft reassociation-timeout 25 1
```

Related Commands

show wlan

config wlan security wpa akm pmf

To configure Authenticated Key Management (AKM) of management frames, use the **config wlan security wpa akm pmf** command.

```
config wlan security wpa akm pmf {802.1x | psk} {enable | disable} wlan_id
```

Syntax Description

802.1x	Configures 802.1X authentication for protection of management frames (PMF).
psk	Configures preshared keys (PSK) for PMF.
enable	Enables 802.1X authentication or PSK for PMF.
disable	Disables 802.1X authentication or PSK for PMF.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512.

Command Default

Disabled.

Usage Guidelines

802.11w has two new AKM suites: 00-0F-AC:5 or 00-0F-AC:6. You must enable WPA and then disable the WLAN to configure PMF on the WLAN.

Examples

This example shows how to enable 802.1X authentication for PMF in a WLAN:

```
> config wlan security wpa akm pmf 802.1x enable 1
```

Related Commands

```
show wlan
show client detail
config wlan security pmf
debug 11w-pmf
```

config wlan security wpa akm psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

```
config wlan security wpa akm psk {enable | disable | set-key key-format key} wlan_id
```

Syntax Description

enable	Enables WPA-PSK.
disable	Disables WPA-PSK.
set-key	Configures a preshared key.
<i>key-format</i>	Specifies key format. Either ASCII or hexadecimal.
<i>key</i>	WPA preshared key.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure the WPA preshared key mode:

```
> config wlan security wpa akm psk disable 1
```

Related Commands

show wlan

config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

config wlan security wpa disable *wlan_id*

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to disable WPA:

```
> config wlan security wpa disable 1
```

Related Commands

show wlan

config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

config wlan security wpa enable *wlan_id*

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure the WPA on WLAN ID 1:

```
> config wlan security wpa enable 1
```

Related Commands

show wlan

config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the **config wlan security wpa ciphers** command.

config wlan security wpa {wpa1 | wpa2} **ciphers** {aes | tkip} {enable | disable} *wlan_id*

Syntax Description

wpa1	Configures WPA1 support.
wpa2	Configures WPA2 support.
ciphers	Configures WPA ciphers.
aes	Configures AES encryption support.
tkip	Configures TKIP encryption support.
enable	Enables WPA AES/TKIP mode.
disable	Disables WPA AES/TKIP mode.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

If you are not specifying the WPA versions, it implies the following:

- If the cipher enabled is AES, you are configuring WPA2/AES.
- If the ciphers enabled is AES+TKIP, you are configuring WPA/TKIP, WPA2/AES, or WPA/TKIP.
- If the cipher enabled is TKIP, you are configuring WPA/TKIP or WPA2/TKIP.

Examples

This example shows how to encrypt the WPA:

```
> config wlan security wpa wpa1 ciphers aes enable 1
```

Related Commands

show wlan

config wlan security wpa gtk-random

To enable the randomization of group temporal keys (GTK) between access points and clients on a WLAN, use the **config wlan security wpa gtk-random** command.

config wlan security wpa gtk-random {enable | disable} *wlan_id*

Syntax Description		
enable		Enables the randomization of GTK keys between the access point and clients.
disable		Disables the randomization of GTK keys between the access point and clients.
<i>wlan_id</i>		WLAN identifier between 1 and 512.

Command Default None.

Usage Guidelines When you enable this command, the clients in the Basic Service Set (BSS) get a unique GTK key. The clients do not receive multicast or broadcast traffic.

Examples This example shows how to enable the GTK randomization for each client associated on a WLAN:
 > **config wlan security wpa gtk-random enable 3**

Related Commands

- show wlan**
- debug hotspot events**
- debug hotspot packets**
- config wlan apgroup hotspot venue**
- config wlan apgroup hotspot operating-class**
- config ap hotspot venue**
- config advanced hotspot**
- config wlan hotspot dot11u**
- config wlan hotspot clear-all**
- config wlan hotspot msap**

config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

config wlan security wpa wpa1 disable *wlan_id*

Syntax Description

<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.
----------------	--

Command Default

None.

Examples

This example shows how to disable WPA1:

```
> config wlan security wpa wpa1 disable 1
```

Related Commands

show wlan

config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

config wlan security wpa wpa1 enable *wlan_id*

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable WPA1:

```
> config wlan security wpa wpa1 enable 1
```

Related Commands

show wlan

config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

config wlan security wpa wpa2 disable *wlan_id*

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to disable WPA2:

```
> config wlan security wpa wpa2 disable 1
```

Related Commands

show wlan

config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

config wlan security wpa wpa2 enable *wlan_id*

Syntax Description

wlan_id Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable WPA2:

```
> config wlan security wpa wpa2 enable 1
```

Related Commands

show wlan

config wlan security wpa wpa2 cache sticky

To configure Sticky PMKID Caching (SKC) on a WLAN, use the **config wlan security wpa wpa2 cache sticky** command.

config wlan security wpa wpa2 cache sticky {enable |disable} *wlan_id*

Syntax Description

enable	Enables SKC on a WLAN.
disable	Disables SKC on a WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

Disabled.

Usage Guidelines

Beginning in Release 7.2 and later releases, the controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client. In SKC also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

- You cannot use SKC for large scale deployments as the controller supports SKC only up to eight APs.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.
- SKC works only on local mode APs.

Examples

This example shows how to enable Sticky PMKID Caching on WLAN 5:

```
> config wlan security wpa wpa2 cache sticky enable 5
```

Related Commands

```
config wlan security wpa wpa2 enable
config wlan security wpa wpa2 disable
config wlan security wpa wpa2 ciphers
show wlan
```

Configure Wireless LAN Proxy Mobility IPv6 (PMIPv6) Commands

Use the `config wlan pmipv6` commands to configure PMIPv6 on WLANs.

config wlan pmipv6 default-realm

To configure a default realm for the PMIPv6 WLAN, use the **config wlan pmipv6 default-realm** command.

```
config wlan pmipv6 default-realm { default-realm-name | none } wlan_id
```

Syntax Description

<i>default-realm-name</i>	Default realm name for the WLAN.
none	Clears the realm name for the WLAN.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure a default realm name on a PMIPv6 WLAN:

```
> config wlan pmipv6 default-realm XYZ 6
```

Related Commands

```
config wlan pmipv6 profile-name  
config wlan pmipv6 mobility-type  
config pmipv6 domain  
show wlan summary  
show client summary
```

config wlan pmipv6 mobility-type

To configure the mobility type on a WLAN, use the **config wlan pmipv6 mobility-type** command.

```
config wlan pmipv6 mobility-type {none | pmipv6 | mixed} { wlan_id | all }
```

Syntax Description

none	Configures the WLAN with Simple IP mobility.
pmipv6	Configures the WLAN with PMIPv6 mobility.
mixed	Configures the WLAN with Simple IP and PMIPv6 mobility.
all	Enables the specified type of mobility for all WLANs.
<i>wlan_id</i>	WLAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

You must disable the WLAN when you configure the mobility type.

Examples

This example shows how to configure the mobility type as PMIPv6 on a WLAN:

```
> config wlan pmipv6 mobility-type pmipv6 16
```

Related Commands

```
config wlan pmipv6 profile-name  
config wlan pmipv6 default-realm  
config pmipv6 domain  
show wlan summary  
show client summary
```

config wlan pmipv6 profile_name

To configure a profile name for the PMIPv6 WLAN, use the **config wlan pmipv6 profile_name** command.

config wlan pmipv6 profile_name *profile_name* *wlan_id*

Syntax Description

<i>profile_name</i>	Profile name for the pmipv6 wlan.
<i>wlan_id</i>	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

This commands binds a profile name to the PMIPv6 WLAN or SSID. Everytime a mobile node associates with the controller, it uses the profile name and NAI in the trigger to the PMIPV6 module. PMIPV6 module extracts all the profile specific parameters like LMA IP, APN, NAI and sends the PBU to the ASR5K.

Examples

This example shows how to create a profile named ABC01 on a PMIPv6 WLAN:

```
> config wlan pmipv6 profile_name ABC01 16
```

Related Commands

config wlan pmipv6 mobility-type
config wlan pmipv6 default-realm
config pmipv6 domain
show wlan summary

Other Config Commands

This section lists the other **config** commands to configure WLANs.

config 802.11 dtpc

To enable or disable the Dynamic Transmit Power Control (DTPC) setting for an 802.11 network, use the **config 802.11 dtpc** command.

config 802.11 {a | b} dtpc {enable | disable}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the support for this command.
disable	Disables the support for this command.

Command Default

Enabled.

Examples

This example shows how to disable DTPC for an 802.11a network:

```
> config 802.11a dtpc disable
```

Related Commands

```
show 802.11a
config 802.11a beaconperiod
config 802.11a disable
config 802.11a enable
```

config auto-configure voice

To auto-configure voice deployment in WLANs, use the **config auto-configure voice** command.

config auto-configure voice cisco *wlan_id* **radio** {**802.11a** | **802.11b** | **all**}

Syntax Description

cisco	Auto-configure WLAN for voice deployment of Cisco end points.
<i>wlan_id</i>	Wireless LAN identifier from 1 to 512 (inclusive).
radio	Auto-configures voice deployment for a radio in a WLAN.
802.11a	Auto-configures voice deployment for 802.11a in a WLAN.
802.11b	Auto-configures voice deployment for 802.11b in a WLAN.
all	Auto-configures voice deployment for all radios in a WLAN.

Command Default

None.

Usage Guidelines

When you configure this command, all WLANs and radios are automatically disabled. After the completion of the configuration, the previous state of the WLANs and radios is restored.

Examples

This example shows how to auto-configure voice deployment for all radios in a WLAN:

```
> config auto-configure voice cisco 2 radio all
Warning! This command will automatically disable all WLAN's and Radio's.
It will be reverted to the previous state once configuration is complete.
Are you sure you want to continue? (y/N)y
```

```
Auto-Configuring these commands in WLAN for Voice..
wlan qos 2 platinum
- Success
wlan call-snoop enable 2
- Success
wlan wmm allow 2
- Success
wlan session-timeout 2 86400
- Success
wlan peer-blocking disable 2
- Success
wlan security tkip hold-down 0 2
- Success
wlan exclusionlist 2 disable
- Success
wlan mac-filtering disable 2
- Success
wlan dtim 802.11a 2 2
- Success
wlan dtim 802.11b 2 2
- Success
wlan ccx aironetIeSupport enabled 2
- Success
```

```

wlan channel-scan defer-priority 4 enable 2
- Success
wlan channel-scan defer-priority 5 enable 2
- Success
wlan channel-scan defer-priority 6 enable 2
- Success
wlan channel-scan defer-time 100 2
- Success
wlan load-balance allow disable 2
- Success
wlan mfp client enable 2
- Success
wlan security wpa akm cckm enable 2
- Success
wlan security wpa akm cckm timestamp-tolerance 5000 2
- Success
wlan band-select allow disable 2
- Success
*****

```

Auto-Configuring these commands for Voice - Radio 802.11a.

```

advanced 802.11a edca-parameter optimized-voice
- Success
802.11a cac voice acm enable
- Success
802.11a cac voice max-bandwidth 75
- Success
802.11a cac voice roam-bandwidth 6
- Success
802.11a cac voice cac-method load-based
- Success
802.11a cac voice sip disable
- Success
802.11a tsm enable
- Success
802.11a exp-bwreq enable
- Success
802.11a txPower global auto
- Success
802.11a channel global auto
- Success
advanced 802.11a channel dca interval 24
- Success
advanced 802.11a channel dca anchor-time 0
- Success
qos protocol-type platinum dot1p
- Success
qos dot1p-tag platinum 6
- Success
qos priority platinum voice voice besteffort
- Success
802.11a beacon period 100
- Success
802.11a dtpc enable
- Success
802.11a Coverage Voice RSSI Threshold -70
- Success
802.11a txPower global min 11
- Success
advanced eap eapol-key-timeout 250
- Success
advanced 802.11a voice-mac-optimization disable
- Success
802.11h channelswitch enable 1
- Success

```

Note: Data rate configurations are not changed.
It should be changed based on the recommended values after analysis.

Auto-Configuring these commands for Voice - Radio 802.11b.

```

advanced 802.11b edca-parameter optimized-voice
- Success

```

```
802.11b cac voice acm enable
- Success
802.11b cac voice max-bandwidth 75
- Success
802.11b cac voice roam-bandwidth 6
- Success
802.11b cac voice cac-method load-based
- Success
802.11b cac voice sip disable
- Success
802.11b tsm enable
- Success
802.11b exp-bwreq enable
- Success
802.11b txPower global auto
- Success
802.11b channel global auto - Success
advanced 802.11b channel dca interval 24
- Success
advanced 802.11b channel dca anchor-time 0
- Success
802.11b beacon period 100
- Success
802.11b dtpc enable
- Success
802.11b Coverage Voice RSSI Threshold -70
- Success
802.11b preamble short
- Success
advanced 802.11a voice-mac-optimization disable
- Success
Note: Data rate configurations are not changed.
It should be changed based on the recommended values after analysis.
```

config dhcp

To configure the internal DHCP, use the **config dhcp** command.

```
config dhcp {address-pool scope start end | create-scope scope | default-router scope router_1 [router_2] [router_3] | delete-scope scope | disable scope | dns-servers scope dns1 [dns2] [dns3] | domain scope domain | enable scope | lease scope lease_duration | netbios-name-server scope wins1 [wins2] [wins3] | networkscope network netmask}
```

```
config dhcpopt-82 remote-id {ap_mac | ap_mac:ssid | ap-ethmac | apname:ssid | ap-group-name | flex-group-name | ap-location | apmac-vlan_id | apname-vlan_id | ap-ethmac-ssid }
```

Syntax Description

address-pool <i>scope start end</i>	Configures an address range to allocate. You must specify the scope name and the first and last addresses of the address range.
create-scope <i>name</i>	Creates a new DHCP scope. You must specify the scope name.
default-router <i>scope router_1</i> [<i>router_2</i>] [<i>router_3</i>]	Configures the default routers for the specified scope and specify the IP address of a router. Optionally, you can specify the IP addresses of secondary and tertiary routers.
delete-scope <i>scope</i>	Deletes the specified DHCP scope.
disable <i>scope</i>	Disables the specified DHCP scope.
dns-servers <i>scope dns1</i> [<i>dns2</i>] [<i>dns3</i>]	Configures the name servers for the given scope. You must also specify at least one name server. Optionally, you can specify secondary and tertiary name servers.
domain <i>scope domain</i>	Configures the DNS domain name. You must specify the scope and domain names.
enable <i>scope</i>	Enables the specified dhcp scope.
lease <i>scope lease_duration</i>	Configures the lease duration (in seconds) for the specified scope.

netbios-name-server <i>scope wins1 [wins2] [wins3]</i>	Configures the netbios name servers. You must specify the scope name and the IP address of a name server. Optionally, you can specify the IP addresses of secondary and tertiary name servers.
network <i>scope network netmask</i>	Configures the network and netmask. You must specify the scope name, the network address, and the network mask.
opt-82 remote-id	Configures the DHCP option 82 remote ID field format. DHCP option 82 provides additional security when DHCP is used to allocate network addresses. The controller acts as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller adds option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.
<i>ap_mac</i>	MAC address of the access point to the DHCP option 82 payload.
<i>ap_mac:ssid</i>	MAC address and SSID of the access point to the DHCP option 82 payload.
<i>ap-ethmac</i>	Remote ID format as AP Ethernet MAC address.
<i>apname:ssid</i>	Remote ID format as AP name:SSID.
<i>ap-group-name</i>	Remote ID format as AP group name.
<i>flex-group-name</i>	Remote ID format as FlexConnect group name .
<i>ap-location</i>	Remote ID format as AP location.
<i>apmac-vlan_id</i>	Remote ID format as AP radio MAC address:VLAN_ID.
<i>apname-vlan_id</i>	Remote ID format as AP Name:VLAN_ID.
<i>ap-ethmac-ssid</i>	Remote ID format as AP Ethernet MAC:SSID address.

Command Default

The default values for ap-group-name is "default-group", and for ap-location is "default location".
If ap-group-name and flex-group-name are null, then the system MAC is sent as the remote ID field.

Usage Guidelines

Use the **show dhcp** command to display the internal DHCP configuration.

Examples

This example shows how to configure the DHCP lease for the scope 003:

```
> config dhcp lease 003
```

Related Commands

```
config dhcp proxy  
config dhcp timeout  
config interface dhcp  
config wlan dhcp_server  
debug dhcp  
debug dhcp service-port  
debug disable-all  
show dhcp  
show dhcp proxy
```

config dhcp proxy

To specify the level at which DHCP packets are modified, use the **config dhcp proxy** command.

```
config dhcp proxy {enable | disable {bootp-broadcast [enable | disable]}}
```

Syntax Description

enable	Allows the controller to modify the DHCP packets without a limit.
disable	Reduces the DHCP packet modification to the level of a relay.
bootp-broadcast	Configures DHCP BootP broadcast option.

Command Default

Enabled.

Usage Guidelines

Follow these guidelines when you use this command:

- Use the **show dhcp proxy** command to display the status of DHCP proxy handling.
- To enable third-party WGB support, you must enable the passive-client feature on the wireless LAN by entering the **config wlan passive-client enable** command.

Examples

This example shows how to disable the DHCP packet modification:

```
> config dhcp proxy disable
```

This example shows how to enable the DHCP BootP broadcast option:

```
> config dhcp proxy disable bootp-broadcast enable
```

Related Commands

```
config dhcp
config dhcp timeout
config interface dhcp
config wlan dhcp_server
debug dhcp
debug dhcp service-port
debug disable-all
show dhcp
show dhcp proxy
```

config dhcp timeout

To configure a DHCP timeout, use the **config dhcp timeout** command.

config dhcp timeout *timeout-value*

Syntax Description

<i>timeout-value</i>	Timeout value in the range of 5 to 120 seconds.
----------------------	---

Command Default

None.

Examples

This example shows how to set the DHCP timeout to 10 seconds:

```
> config dhcp timeout 10
```

Related Commands

- config dhcp proxy**
- config dhcp timeout**
- config interface dhcp**
- config wlan dhcp_server**
- debug dhcp**
- debug dhcp service-port**
- debug disable-all**
- show dhcp**
- show dhcp proxy**

Clear Commands

This section lists the **clear** commands to clear existing configurations, log files, and other functions for WLANs

clear avc statistics

To clear AVC statistics of a client, guest LAN, remote LAN, or a WLAN use the **clear avc statistics** command.

```
clear avc statistics {client {all | client-mac} | guest-lan {all | guest-lan-id} | remote-lan {all | remote-lan-id} | wlan {all | wlan-id}}
```

Syntax Description

client	Clears AVC statistics of a client.
all	Clears AVC statistics of all clients.
<i>client-mac</i>	MAC address of a client.
guest-lan	Clears AVC statistics of a guest LAN.
all	Clears AVC statistics of all guest LANs.
<i>guest-lan-id</i>	Guest LAN Identifier between 1 and 5.
remote-lan	Clears AVC statistics of a remote LAN.
all	Clears AVC statistics of all remote LANs.
<i>remote-lan-id</i>	Remote LAN Identifier between 1 and 512.
wlan	Clears AVC statistics of a WLAN.
all	Clears AVC statistics of all WLANs.
<i>wlan-id</i>	WLAN Identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to clear the AVC statistics of a client:

```
> clear avc statistics client 00:21:1b:ea:36:60
```

Related Commands

```
config avc profile create  
config avc profile delete  
config avc profile rule  
config wlan avc  
show avc profile  
show avc applications
```

show avc statistics

debug avc error

debug avc events

clear mdns service-database

To clear the mDNS service database, use the **clear mdns service-database** command.

clear mdns service-database {**all** | *service-name*}

Syntax Description

all	Clears the mDNS service database.
<i>service-name</i>	Name of the mDNS service. The controller clears the details of the mDNS service.

Command Default

None.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database.

Examples

This example shows how to clear the mDNS service database:

```
> clear mdns service-database all
```

Related Commands

config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
config mdns profile
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

Debug Commands

This section lists the **debug** commands to manage debugging of WLANs 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 11w-pmf

To configure 802.11w debug options, use the **debug 11w-pmf** command.

debug 11w-pmf {all | events| keys} {enable | disable}

Syntax Description

all	Configures debug of all 802.11w messages.
keys	Configures debug of 802.11w keys.
events	Configures debug of 802.11w events.
enable	Enables the 802.1w debug.
disable	Disables the 802.1w debug.

Command Default

None.

Examples

This example shows how to enable debug of 802.11w key generation:

```
> debug 11w-pmf keys enable
```

Related Commands

show wlan
show client detail
config wlan security pmf

debug call-control

To debug the SIP call control settings, use the **debug call-control** command.

```
debug call-control {all | event} {enable | disable}
```

Syntax Description

all	Configures debugging options for all SIP call control messages.
event	Configures debugging options for SIP call control events.
enable	Enables the SIP call control debugging settings.
disable	Disables the SIP call control debugging settings.

Command Default

Disabled.

Examples

This example shows how to enable debugging of all SIP call control messages:

```
> debug call-control all enable
```

debug client

To debug if the passive client is associated correctly with the access point and if the passive client has moved into the DHCP required state at the controller, use the **debug client** command.

debug client *mac_address*

Syntax Description

<i>mac_address</i>	MAC address of the client.
--------------------	----------------------------

Command Default

None.

Examples

This example shows how to debug a passive client with mac address 00:0d:28:f4:c0:45:

```
> debug client 00:0d:28:f4:c0:45
```

Related Commands

debug disable-all
show capwap reap association
show capwap reap status

debug dhcp

To configure DHCP debug options, use the **debug dhcp** command.

```
debug dhcp {message | packet} {enable | disable}
```

Syntax Description

message	Configures debugging of DHCP error messages.
packet	Configures debugging of DHCP packets.
enable	Enables the DHCP debugging.
disable	Disables the DHCP debugging.

Command Default

None.

Examples

This example shows how to enable DHCP debug settings:

```
> debug dhcp message enable
```

Related Commands

```
debug disable-all  
config dhcp  
config dhcp proxy  
config interface dhcp  
config wlan dhcp_server  
debug dhcp service-port  
show dhcp  
show dhcp proxy
```

debug dhcp service-port

To enable or disable debugging of Dynamic Host Configuration Protocol (DHCP) packets on the service port, use the **debug dhcp service-port** command.

debug dhcp service-port {enable | disable}

Syntax Description

enable	Enables the debugging of DHCP packets on the service port.
disable	Disables the debugging of DHCP packets on the service port.

Command Default

None.

Examples

This example shows how to enable debugging of DHCP packets on a service port:

```
> debug dhcp service-port enable
```

Related Commands

debug disable-all
config dhcp
config dhcp proxy
config interface dhcp
config wlan dhcp_server
debug dhcp service-port
show dhcp
show dhcp proxy

debug hotspot events

To debug HotSpot events, use the **debug hotspot events** command.

debug hotspot events {enable | disable}

Syntax Description

enable	Enables the debugging of HotSpot events.
disable	Disables the debugging of HotSpot events.

Command Default

None.

Examples

This example shows how to enable the debugging of HotSpot events:

```
> debug hotspot events enable
```

Related Commands

show wlan
debug hotspot packets
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random
config wlan hotspot dot11u
config wlan hotspot clear-all
config wlan hotspot msap

debug hotspot packets

To debug HotSpot packets, use the **debug hotspot packets** command.

debug hotspot packets {enable | disable}

Syntax Description

enable	Enables the debugging of HotSpot packets.
disable	Disables the debugging of HotSpot packets.

Command Default

None.

Examples

This example shows how to enable the debugging of HotSpot packets:

```
> debug hotspot packets enable
```

Related Commands

show wlan
debug hotspot events
config wlan apgroup hotspot venue
config wlan apgroup hotspot operating-class
config ap hotspot venue
config advanced hotspot
config wlan security wpa gtk-random
config wlan hotspot dot11u
config wlan hotspot clear-all
config wlan hotspot msap

debug mdns all

To debug all multicast DNS (mDNS) messages, details, and errors, use the **debug mdns all** command.

debug mdns all {enable | disable}

Syntax Description

enable	Enables the debug of all mDNS messages, details, and errors.
disable	Disables the debug of all mDNS messages, details, and errors.

Command Default

Disabled.

Examples

This example shows how to enable the debug of all mDNS messages, details, and errors:

```
> debug mdns all enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns error
debug mdns detail

debug mdns detail

To debug mDNS details, use the **debug mdns detail** command.

debug mdns detail {enable | disable}

Syntax Description

enable	Enables the debug of mDNS details.
disable	Disables the debug of mDNS details.

Command Default

Disabled.

Examples

This example shows how to enable the debug of mDNS details:

```
> debug mdns detail enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error

debug mdns error

To debug mDNS errors, use the **debug mdns error** command.

debug mdns error {enable | disable}

Syntax Description

enable	Enables the debug of mDNS errors.
disable	Disables the debug of mDNS errors.

Command Default

Disabled.

Examples

This example shows how to enable the debug of mDNS errors:

```
> debug mdns error enable
```

Related Commands

- config mdns profile**
- config mdns query interval**
- config mdns service**
- config mdns snooping**
- config interface mdns-profile**
- config interface group mdns-profile**
- config wlan mdns**
- show mdns profile**
- show mnds service**
- clear mdns service-database**
- debug mdns all**
- debug mdns detail**
- debug mdns message**

debug mdns message

To debug mDNS messages, use the **debug mdns message** command.

debug mdns message {enable | disable}

Syntax Description

enable	Enables the debug of mDNS messages.
disable	Disables the debug of mDNS messages.

Command Default

Disabled.

Examples

This example shows how to enable the debug of mDNS messages:

```
> debug mdns message enable
```

Related Commands

config mdns profile
config mdns query interval
config mdns service
config mdns snooping
config interface mdns-profile
config interface group mdns-profile
config wlan mdns
show mdns profile
show mnds service
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail

debug profiling

To configure the client profiling debug options, use the **debug profiling** command.

debug profiling {enable | disable}

Syntax Description

enable	Enables client profiling (HTTP and DHCP profiling) debugging.
disable	Disables client profiling (HTTP and DHCP profiling) debugging.

Command Default

Disabled.

Examples

This example shows how to enable client profiling debugging:

```
> debug profiling enable
```

Related Commands

config wlan profiling
show wlan

debug wcp

To configure WLAN Control Protocol (WCP) debug options, use the **debug wcp** command.

debug wcp {events | packet} {enable | disable}

Syntax Description

events	Configures debugging of WCP events.
packet	Configures debugging of WCP packets.
enable	Enables WCP debugging settings.
disable	Disables WCP debugging settings.

Command Default

None.

Examples

This example shows how to enable WCP debug settings:

```
> debug wcp packet enable
```

Related Commands

debug disable-all

Test Commands

This section lists the **test** commands for WLANs.

test pmk-cache delete

To delete an entry in the Pairwise Master Key (PMK) cache from all Cisco wireless LAN controllers in the mobility group, use the **test pmk-cache delete** command.

```
test pmk-cache delete {all | mac_address}
```

Syntax Description

all	Deletes PMK cache entries from all Cisco wireless LAN controllers.
<i>mac_address</i>	MAC address of the Cisco wireless LAN controller from which PMK cache entries have to be deleted.

Command Default

None.

Examples

This example shows how to delete all entries in the PMK cache:

```
> test pmk-cache delete all
```

Related Commands

show pmk-cache

test pmk-cache delete