



Config Commands: j to q

- [config known ap](#), on page 6
- [config lag](#), on page 7
- [config ldap](#), on page 8
- [config local-auth active-timeout](#), on page 10
- [config local-auth cipher-option](#), on page 11
- [config local-auth eap-profile](#), on page 12
- [config local-auth method fast](#), on page 14
- [config local-auth user-credentials](#), on page 16
- [config lync-sdn](#), on page 17
- [config license boot](#), on page 18
- [config load-balancing](#), on page 19
- [config location](#), on page 21
- [config location info rogue](#), on page 23
- [config logging buffered](#), on page 24
- [config logging console](#), on page 25
- [config logging debug](#), on page 26
- [config logging fileinfo](#), on page 27
- [config logging procinfo](#), on page 28
- [config logging traceinfo](#), on page 29
- [config logging syslog host](#), on page 30
- [config logging syslog facility](#), on page 33
- [config logging syslog facility client](#), on page 35
- [config logging syslog facility ap](#), on page 36
- [config logging syslog ipsec](#), on page 37
- [config logging syslog ipsec profile](#), on page 38
- [config logging syslog tls](#), on page 39
- [config logging syslog level](#), on page 40
- [config loginsession close](#), on page 41
- [config macfilter](#) , on page 42
- [config macfilter description](#), on page 43
- [config macfilter interface](#), on page 44
- [config macfilter ip-address](#), on page 45
- [config macfilter mac-delimiter](#), on page 46

- [config macfilter radius-compat](#), on page 47
- [config macfilter wlan-id](#), on page 48
- [config mdns ap](#), on page 49
- [config mdns profile](#), on page 50
- [config mdns query interval](#), on page 52
- [config mdns service](#) , on page 53
- [config mdns snooping](#) , on page 55
- [config mdns policy enable](#) , on page 56
- [config mdns policy service-group](#), on page 57
- [config mdns policy service-group parameters](#), on page 58
- [config mdns policy service-group user-name](#), on page 59
- [config mdns policy service-group user-role](#), on page 60
- [config media-stream multicast-direct](#), on page 61
- [config media-stream message](#), on page 62
- [config media-stream add](#), on page 63
- [config media-stream admit](#), on page 65
- [config media-stream deny](#), on page 66
- [config media-stream delete](#), on page 67
- [config memory monitor errors](#), on page 68
- [config memory monitor leaks](#), on page 69
- [config mesh alarm](#), on page 71
- [config mesh astools](#), on page 72
- [config mesh backhaul rate-adapt](#), on page 73
- [config mesh backhaul slot](#), on page 74
- [config mesh battery-state](#), on page 75
- [config mesh client-access](#), on page 76
- [config mesh convergence](#), on page 77
- [config mesh ethernet-bridging allow-bpdu](#), on page 78
- [config mesh ethernet-bridging vlan-transparent](#), on page 79
- [config mesh full-sector-dfs](#), on page 80
- [config mesh linkdata](#), on page 81
- [config mesh linktest](#), on page 83
- [config mesh lsc](#), on page 86
- [config mesh lsc advanced](#), on page 87
- [config mesh lsc advanced ap-provision](#), on page 88
- [config mesh multicast](#), on page 89
- [config mesh parent preferred](#), on page 91
- [config mesh public-safety](#), on page 92
- [config mesh radius-server](#), on page 93
- [config mesh range](#), on page 94
- [config mesh secondary-backhaul](#), on page 95
- [config mesh security](#), on page 96
- [config mesh slot-bias](#), on page 98
- [config mgmtuser add](#), on page 99
- [config mgmtuser delete](#), on page 100
- [config mgmtuser description](#), on page 101

- [config mgmtuser password](#), on page 102
- [config mgmtuser telnet](#), on page 103
- [config mobility dscp](#), on page 104
- [config mobility group anchor](#), on page 105
- [config mobility group domain](#), on page 106
- [config mobility group keepalive count](#), on page 107
- [config mobility group keepalive interval](#), on page 108
- [config mobility group member](#), on page 109
- [config mobility group multicast-address](#), on page 111
- [config mobility multicast-mode](#), on page 112
- [config mobility new-architecture](#), on page 113
- [config mobility oracle](#), on page 114
- [config mobility switchPeerGroup](#), on page 115
- [config mobility secure-mode](#), on page 116
- [config mobility statistics reset](#), on page 117
- [config netuser add](#) , on page 118
- [config netuser delete](#), on page 120
- [config netuser description](#), on page 121
- [config netuser guest-lan-id](#), on page 122
- [config netuser guest-role apply](#), on page 123
- [config netuser guest-role create](#), on page 124
- [config netuser guest-role delete](#), on page 125
- [config netuser guest-role qos data-rate average-data-rate](#), on page 126
- [config netuser guest-role qos data-rate average-realtime-rate](#), on page 127
- [config netuser guest-role qos data-rate burst-data-rate](#), on page 128
- [config netuser guest-role qos data-rate burst-realtime-rate](#), on page 129
- [config netuser lifetime](#), on page 130
- [config netuser maxUserLogin](#), on page 131
- [config netuser password](#), on page 132
- [config netuser wlan-id](#), on page 133
- [config network bridging-shared-secret](#), on page 134
- [config network web-auth captive-bypass](#), on page 135
- [config network web-auth port](#), on page 136
- [config network web-auth proxy-redirect](#), on page 137
- [config network web-auth secureweb](#), on page 138
- [config network webmode](#), on page 139
- [config network web-auth](#), on page 140
- [config network 802.3-bridging](#), on page 141
- [config network allow-old-bridge-aps](#), on page 142
- [config network ap-discovery](#), on page 143
- [config network ap-fallback](#), on page 144
- [config network ap-priority](#), on page 145
- [config network apple-talk](#), on page 146
- [config network arptimeout](#), on page 147
- [config assisted-roaming](#), on page 148
- [config network allow-old-bridge-aps](#), on page 149

- [config network ap-discovery](#), on page 150
- [config network ap-fallback](#), on page 151
- [config network ap-priority](#), on page 152
- [config network apple-talk](#), on page 153
- [config network bridging-shared-secret](#), on page 154
- [config network bridging-shared-secret](#), on page 155
- [config network broadcast](#), on page 156
- [config network fast-ssid-change](#), on page 157
- [config network ip-mac-binding](#), on page 158
- [config network link local bridging](#), on page 159
- [config network master-base](#), on page 160
- [config network mgmt-via-wireless](#), on page 161
- [config network multicast global](#), on page 162
- [config network multicast igmp query interval](#), on page 163
- [config network multicast igmp snooping](#), on page 164
- [config network multicast igmp timeout](#), on page 165
- [config network multicast l2mcast](#), on page 166
- [config network multicast mld](#), on page 167
- [config network multicast mode multicast](#), on page 168
- [config network multicast mode unicast](#), on page 169
- [config network oeap-600 dual-rlan-ports](#), on page 170
- [config network oeap-600 local-network](#), on page 171
- [config network otap-mode](#), on page 172
- [config network rf-network-name](#), on page 173
- [config network secureweb](#), on page 174
- [config network secureweb cipher-option](#), on page 175
- [config network ssh](#), on page 176
- [config network telnet](#), on page 177
- [config network usertimeout](#), on page 178
- [config network web-auth captive-bypass](#), on page 179
- [config network web-auth cmcc-support](#), on page 180
- [config network web-auth port](#), on page 181
- [config network web-auth proxy-redirect](#), on page 182
- [config network web-auth secureweb](#), on page 183
- [config network web-auth https-redirect](#), on page 184
- [config network webcolor](#), on page 185
- [config network webmode](#), on page 186
- [config network web-auth](#), on page 187
- [config network zero-config](#), on page 188
- [config network master-base](#), on page 189
- [config network oeap-600 dual-rlan-ports](#), on page 190
- [config network oeap-600 local-network](#), on page 191
- [config network otap-mode](#), on page 192
- [config network zero-config](#), on page 193
- [config nmsp notify-interval measurement](#), on page 194
- [config pmipv6 domain](#), on page 195

- [config pmipv6 add profile](#), on page 196
- [config pmipv6 delete](#), on page 197
- [config pmipv6 mag apn](#), on page 198
- [config pmipv6 mag binding init-retx-time](#), on page 199
- [config pmipv6 mag binding lifetime](#), on page 200
- [config pmipv6 mag binding max-retx-time](#), on page 201
- [config pmipv6 mag binding maximum](#), on page 202
- [config pmipv6 mag binding refresh-time](#), on page 203
- [config pmipv6 mag bri delay](#), on page 204
- [config pmipv6 mag bri retries](#), on page 205
- [config pmipv6 mag lma](#), on page 206
- [config pmipv6 mag replay-protection](#), on page 207
- [config port power](#), on page 208
- [config paging](#), on page 209
- [config passwd-cleartext](#), on page 210
- [config policy](#), on page 211
- [config port adminmode](#), on page 213
- [config port maxspeed](#), on page 214
- [config port linktrap](#), on page 215
- [config port multicast appliance](#), on page 216
- [config prompt](#), on page 217
- [config qos average-data-rate](#), on page 218
- [config qos average-realtime-rate](#), on page 219
- [config qos burst-data-rate](#), on page 220
- [config qos burst-realtime-rate](#), on page 221
- [config qos description](#), on page 222
- [config qos max-rf-usage](#), on page 223
- [config qos dot1p-tag](#), on page 224
- [config qos priority](#), on page 225
- [config qos protocol-type](#), on page 227
- [config qos queue_length](#), on page 228

config known ap

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

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

Syntax Description		
add	Adds a new known access point entry.	
alert	Generates a trap upon detection of the access point.	
delete	Deletes an existing known access point entry.	
<i>MAC</i>	MAC address of the known Cisco lightweight access point.	
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

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

```
(Cisco Controller) >config known ap add ac:10:02:72:2f:bf 12
```

config lag

To enable or disable link aggregation (LAG), use the **config lag** command.

config lag {enable | disable}

Syntax Description	enable	Enables the link aggregation (LAG) settings.
	disable	Disables the link aggregation (LAG) settings.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable LAG settings:

```
(Cisco Controller) > config lag enable
Enabling LAG will map your current interfaces setting to LAG interface,
All dynamic AP Manager interfaces and Untagged interfaces will be deleted
All WLANs will be disabled and mapped to Mgmt interface
Are you sure you want to continue? (y/n)
You must now reboot for the settings to take effect.
```

The following example shows how to disable LAG settings:

```
(Cisco Controller) > config lag disable
Disabling LAG will map all existing interfaces to port 1.
Are you sure you want to continue? (y/n)
You must now reboot for the settings to take effect.
```

config ldap

To configure the Lightweight Directory Access Protocol (LDAP) server settings, use the **config ldap** command.

config ldap {**add** | **delete** | **enable** | **disable** | **retransmit-timeout** | **retry** | **user** | **security-mode** | **simple-bind**} *index*

config ldap add *index server_ip_address port user_base user_attr user_type* [**secure**]

config ldap retransmit-timeout *index retransmit-timeout*

config ldap retry *attempts*

config ldap user {**attr** *index user-attr* | **base** *index user-base* | **type***index user-type*}

config ldap security-mode {**enable** | **disable**}*index*

config ldap simple-bind {**anonymous** *index* | **authenticated** *index username password*}

Syntax Description	
add	Specifies that an LDAP server is being added.
delete	Specifies that an LDAP server is being deleted.
enable	Specifies that an LDAP server is enabled.
disable	Specifies that an LDAP server is disabled.
retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
retry	Configures the retry attempts for an LDAP server.
user	Configures the user search parameters.
security-mode	Configures the security mode.
simple-bind	Configures the local authentication bind method.
anonymous	Allows anonymous access to the LDAP server.
authenticated	Specifies that a username and password be entered to secure access to the LDAP server.
<i>index</i>	LDAP server index. The range is from 1 to 17.
<i>server_ip_address</i>	IP address of the LDAP server.
<i>port</i>	Port number.
<i>user_base</i>	Distinguished name for the subtree that contains all of the users.

<i>user_attr</i>	Attribute that contains the username.
<i>user_type</i>	ObjectType that identifies the user.
secure	(Optional) Specifies that Transport Layer Security (TLS) is used.
<i>retransmit-timeout</i>	Retransmit timeout for an LDAP server. The range is from 2 to 30.
<i>attempts</i>	Number of attempts that each LDAP server is retried.
attr	Configures the attribute that contains the username.
base	Configures the distinguished name of the subtree that contains all the users.
type	Configures the user type.
<i>username</i>	Username for the authenticated bind method.
<i>password</i>	Password for the authenticated bind method.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
7.6	The secure keyword was added to support secure LDAP.

Usage Guidelines

When you enable secure LDAP, the controller does not validate the server certificate.

The following example shows how to enable LDAP server index 10:

```
(Cisco Controller) > config ldap enable 10
```

Related Commands

config ldap add
config ldap simple-bind
show ldap summary

config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local Extensible Authentication Protocol (EAP) after any pair of configured RADIUS servers fails, use the **config local-auth active-timeout** command.

config local-auth active-timeout *timeout*

Syntax Description	<i>timeout</i>	Timeout measured in seconds. The range is from 1 to 3600.
Command Default	The default timeout value is 100 seconds.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the active timeout to authenticate wireless clients using EAP to 500 seconds:

```
(Cisco Controller) > config local-auth active-timeout 500
```

Related Commands	clear stats local-auth config local-auth eap-profile config local-auth method fast config local-auth user-credentials debug aaa local-auth show local-auth certificates show local-auth config show local-auth statistics
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

config local-auth cipher-option

To configure the 3des-rc4 cipher option, use the **config local-auth cipher-option** command.

```
config local-auth cipher-option { enable | disable }
```

Syntax Description	cipher-option	Configures the cipher option.
	enable	Allows the 3des-rc4 cipher to be enabled.
	disable	Disables the 3des-rc4 cipher.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.

The following example shows how to disable the cipher-option on the WLC:

```
(Cisco Controller) > config local-auth cipher-option 3des-rc4 disable
```

config local-auth eap-profile

To configure local Extensible Authentication Protocol (EAP) authentication profiles, use the **config local-auth eap-profile** command.

```
config local-auth eap-profile {[add | delete] profile_name | cert-issuer {cisco | vendor} | method method local-cert {enable | disable} profile_name | method method client-cert {enable | disable} profile_name | method method peer-verify ca-issuer {enable | disable} | method method peer-verify cn-verify {enable | disable} | method method peer-verify date-valid {enable | disable}
```

Syntax Description	
add	(Optional) Specifies that an EAP profile or method is being added.
delete	(Optional) Specifies that an EAP profile or method is being deleted.
<i>profile_name</i>	EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
cisco	Specifies the Cisco certificate issuer.
vendor	Specifies the third-party vendor.
method	Configures an EAP profile method.
<i>method</i>	EAP profile method name. The supported methods are leap, fast, tls, and peap.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.

cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Command Default

None

Command History

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

The following example shows how to create a local EAP profile named FAST01:

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

The following example shows how to add the EAP-FAST method to a local EAP profile:

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

The following example shows how to specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile:

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

The following example shows how to specify that the incoming certificate from the client be validated against the CA certificates on the controller:

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

config local-auth active-timeout
config local-auth method fast
config local-auth user-credentials
debug aaa local-auth
show local-auth certificates
show local-auth config
show local-auth statistics

config local-auth method fast

To configure an EAP-FAST profile, use the **config local-auth method fast** command.

```
config local-auth method fast { anon-prov [enable | disable] | authority-id auth_id pac-ttl days
| server-key key_value }
```

Syntax Description		
anon-prov		Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during Protected Access Credentials (PAC) provisioning.
enable		(Optional) Specifies that the parameter is enabled.
disable		(Optional) Specifies that the parameter is disabled.
authority-id		Configures the authority identifier of the local EAP-FAST server.
<i>auth_id</i>		Authority identifier of the local EAP-FAST server (2 to 32 hexadecimal digits).
pac-ttl		Configures the number of days for the Protected Access Credentials (PAC) to remain viable (also known as the time-to-live [TTL] value).
<i>days</i>		Time-to-live value (TTL) value (1 to 1000 days).
server-key		Configures the server key to encrypt or decrypt PACs.
<i>key_value</i>		Encryption key value (2 to 32 hexadecimal digits).
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the controller to allows anonymous provisioning:

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

The following example shows how to configure the authority identifier 0125631177 of the local EAP-FAST server:

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

The following example shows how to configure the number of days to 10 for the PAC to remain viable:

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

Related Commands

clear stats local-auth
config local-auth eap-profile
config local-auth active-timeout
config local-auth user-credentials
debug aaa local-auth
show local-auth certificates
show local-auth config
show local-auth statistics

config local-auth user-credentials

To configure the local Extensible Authentication Protocol (EAP) authentication database search order for user credentials, use the **config local-auth user-credentials** command.

```
config local-auth user-credentials {local [ldap] | ldap [local] }
```

Syntax Description	local	Specifies that the local database is searched for the user credentials.
	ldap	(Optional) Specifies that the Lightweight Directory Access Protocol (LDAP) database is searched for the user credentials.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>The order of the specified database parameters indicate the database search order.</p> <p>The following example shows how to specify the order in which the local EAP authentication database is searched:</p> <pre>(Cisco Controller) > config local-auth user credentials local lda</pre> <p>In the above example, the local database is searched first and then the LDAP database.</p>	

Related Commands	clear stats local-auth
	config local-auth eap-profile
	config local-auth method fast
	config local-auth active-timeout
	debug aaa local-auth
	show local-auth certificates
	show local-auth config
show local-auth statistics	

config lync-sdn

To configure the Lync service, use the **config lync-sdn** command.

```
config lync-sdn {port port-number} | {enable | disable}
```

Syntax Description	port	Configures the Lync server port number.
	<i>port-number</i>	Port number of the server.
	enable	Enables Lync service globally.
	disable	Disables Lync service globally.
Command Default	None	
Command History	Release	Modification
	8.1	This command was introduced.

The following example shows how to enable Lync service globally:

```
(Cisco Controller) >config lync-sdn enable
```

config license boot

To specify the license level to be used on the next reboot of the Cisco 5500 Series Controller, use the **config license boot** command.

```
config license boot {base | wplus | auto}
```

Syntax Description	base	Specifies the base boot level.
	wplus	Specifies the wplus boot level.
	auto	Specifies the auto boot level.

Command Default None

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

Usage Guidelines If you enter **auto**, the licensing software automatically chooses the license level to use on the next reboot. It generally chooses permanent licenses over evaluation licenses and wplus licenses over base licenses.



Note If you are considering upgrading from a base license to a wplus license, you can try an evaluation wplus license before upgrading to a permanent wplus license. To activate the evaluation license, you need to set the image level to wplus in order for the controller to use the wplus evaluation license instead of the base permanent license.



Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

The following example shows how to set the license boot settings to wplus:

```
(Cisco Controller) > config license boot wplus
```

Related Commands

- license install
- show license in-use
- license modify priority

config load-balancing

To globally configure aggressive load balancing on the controller, use the **config load-balancing** command.

```
config load-balancing { window client_count | status { enable | disable } | denial denial_count }
```

```
config load-balancing uplink-threshold traffic_threshold
```

Syntax Description		
window		Specifies the aggressive load balancing client window.
<i>client_count</i>		Aggressive load balancing client window with the number of clients from 1 to 20.
status		Sets the load balancing status.
enable		Enables load balancing feature.
disable		Disables load balancing feature.
denial		Specifies the number of association denials during load balancing.
<i>denial_count</i>		Maximum number of association denials during load balancing. from 0 to 10.
uplink-threshold		Specifies the threshold traffic for an access point to deny new associations.
<i>traffic_threshold</i>		Threshold traffic for an access point to deny new associations. This value is a percentage of the WAN utilization measured over a 90 second interval. For example, the default threshold value of 50 triggers the load balancing upon detecting an utilization of 50% or more on an access point WAN interface.

Command Default By default, the aggressive load balancing is disabled.

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

Usage Guidelines Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

Clients can only be load balanced across access points joined to the same controller. The WAN utilization is calculated as a percentage using the following formula: (Transmitted Data Rate (per second) + Received Data Rate (per second))/(1000Mbps TX + 1000Mbps RX) * 100

The following example shows how to enable the aggressive load-balancing settings:

```
(Cisco Controller) > config load-balancing aggressive enable
```

Related Commands

show load-balancing

config wlan load-balance

config location

To configure a location-based system, use the **config location** command.

```
config location {algorithm {simple | rss-average} | {rss-half-life | expiry} [client |
calibrating-client | tags | rogue-aps] seconds | notify-threshold [client | tags | rogue-aps]
threshold | interface-mapping {add | delete} location wlan_id interface_name | plm {client
{enable | disable} burst_interval | calibrating {enable | disable} {uniband | multiband}}
```

Syntax Description		
algorithm	Note	We recommend that you do not use or modify the config location algorithm command. It is set to optimal default values.
		Configures the algorithm used to average RSSI and SNR values.
simple		Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
rss-average		Specifies a more accurate algorithm but requires more CPU overhead.
rss-half-life	Note	We recommend that you do not use or modify the config location rss-half-life command. It is set to optimal default values.
		Configures the half-life when averaging two RSSI readings.
expiry	Note	We recommend that you do not use or modify the config location expiry command. It is set to optimal default values.
		Configures the timeout for RSSI values.
client		(Optional) Specifies the parameter applies to client devices.
calibrating-client		(Optional) Specifies the parameter is used for calibrating client devices.
tags		(Optional) Specifies the parameter applies to radio frequency identification (RFID) tags.
rogue-aps		(Optional) Specifies the parameter applies to rogue access points.
<i>seconds</i>		Time value (0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, 300 seconds).
notify-threshold	Note	We recommend that you do not use or modify the config location notify-threshold command. It is set to optimal default values.
		Specifies the NMSP notification threshold for RSSI measurements.
<i>threshold</i>		Threshold parameter. The range is 0 to 10 dB, and the default value is 0 dB.
interface-mapping		Adds or deletes a new location, wireless LAN, or interface mapping element.
<i>wlan_id</i>		WLAN identification name.
<i>interface_name</i>		Name of interface to which mapping element applies.

plm	Specifies the path loss measurement (S60) request for normal clients or calibrating clients.
client	Specifies normal, noncalibrating clients.
<i>burst_interval</i>	Burst interval. The range is from 1 to 3600 seconds, and the default value is 60 seconds.
calibrating	Specifies calibrating clients.
uniband	Specifies the associated 802.11a or 802.11b/g radio (uniband).
multiband	Specifies the associated 802.11a/b/g radio (multiband).

Command Default See the “Syntax Description” section for default values of individual arguments and keywords.

Command History

Release Modification

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

The following example shows how to specify the simple algorithm for averaging RSSI and SNR values on a location-based controller:

```
(Cisco Controller) > config location algorithm simple
```

Related Commands

config location info rogue
clear location rfid
clear location statistics rfid
show location
show location statistics rfid

config location info rogue

To configure info-notification for rogue service, use the **config location info rogue** command.

config location info rogue { **basic** | **extended** }

Syntax Description

basic Configures basic rogue parameters such as mode, class, containmentlevel, numclients, firsttime, lasttime, ssid, and so on, for rogue info-notification service.

Note Configure the basic parameters if the version of Cisco MSE is older than the version of the Cisco WLC.

extended Configures extended rogue parameters, which is basic parameters plus security type, detecting LRAD type, and so on, for rogue info-notification service.

Command History

Release	Modification
---------	--------------

8.0	This command was introduced.
-----	------------------------------

config logging buffered

To set the severity level for logging messages to the controller buffer, use the **config logging buffered** command.

config logging buffered *security_level*

Syntax Description

security_level

Security level. Choose one of the following:

- emergencies—Severity level 0
 - alerts—Severity level 1
 - critical—Severity level 2
 - errors—Severity level 3
 - warnings—Severity level 4
 - notifications—Severity level 5
 - informational—Severity level 6
 - debugging—Severity level 7
-

Command Default

None

Command History

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

The following example shows how to set the controller buffer severity level for logging messages to 4:

```
(Cisco Controller) > config logging buffered 4
```

Related Commands

config logging syslog facility

config logging syslog level

show logging

config logging console

To set the severity level for logging messages to the controller console, use the **config logging console** command.

config logging console *security_level*

Syntax Description

security_level

Severity level. Choose one of the following:

- emergencies—Severity level 0
 - alerts—Severity level 1
 - critical—Severity level 2
 - errors—Severity level 3
 - warnings—Severity level 4
 - notifications—Severity level 5
 - informational—Severity level 6
 - debugging—Severity level 7
-

Command Default

None

Command History

Release Modification

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

The following example shows how to set the controller console severity level for logging messages to 3:

```
(Cisco Controller) > config logging console 3
```

Related Commands

config logging syslog facility

config logging syslog level

show logging

config logging debug

To save debug messages to the controller buffer, the controller console, or a syslog server, use the **config logging debug** command.

config logging debug { **buffered** | **console** | **syslog** } { **enable** | **disable** }

Syntax Description

buffered	Saves debug messages to the controller buffer.
console	Saves debug messages to the controller console.
syslog	Saves debug messages to the syslog server.
enable	Enables logging of debug messages.
disable	Disables logging of debug messages.

Command Default

The **console** command is enabled and the **buffered** and **syslog** commands are disabled by default.

Command History

Release Modification

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

The following example shows how to save the debug messages to the controller console:

```
(Cisco Controller) > config logging debug console enable
```

Related Commands

show logging

config logging fileinfo

To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, use the **config logging fileinfo** command.

config logging fileinfo { **enable** | **disable** }

Syntax Description	enable	disable
	Includes information about the source file in the message logs.	Prevents the controller from displaying information about the source file in the message logs.

Command Default None

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

The following example shows how to enable the controller to include information about the source file in the message logs:

```
(Cisco Controller) > config logging fileinfo enable
```

Related Commands `show logging`

config logging procinfo

To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, use the **config logging procinfo** command.

config logging procinfo { **enable** | **disable** }

Syntax Description	enable	disable
	Includes process information in the message logs.	Prevents the controller from displaying process information in the message logs.

Command Default None

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

The following example shows how to enable the controller to include the process information in the message logs:

```
(Cisco Controller) > config logging procinfo enable
```

Related Commands **show logging**

config logging traceinfo

To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, use the **config logging traceinfo** command.

config logging traceinfo { **enable** | **disable** }

Syntax Description	enable	Includes traceback information in the message logs.
	disable	Prevents the controller from displaying traceback information in the message logs.

Command Default None

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

The following example shows how to disable the controller to include the traceback information in the message logs:

```
(Cisco Controller) > config logging traceinfo disable
```

Related Commands `show logging`

config logging syslog host

To configure a remote host for sending syslog messages, use the **config logging syslog host** command.

config logging syslog host *ip_addr*

Syntax Description	<i>ip_addr</i>	IP address for the remote host.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports both IPv4 and IPv6 address formats.
Usage Guidelines	<ul style="list-style-type: none"> • To configure a remote host for sending syslog messages, use the config logging syslog host <i>ip_addr</i> command. • To remove a remote host that was configured for sending syslog messages, use the config logging syslog host <i>ip_addr delete</i> command. • To display the configured syslog servers on the controller, use the show logging command. 	

The following example shows how to configure two remote hosts 10.92.125.52 and 2001:9:6:40::623 for sending the syslog messages and displaying the configured syslog servers on the controller:

```
(Cisco Controller) > config logging syslog host 10.92.125.52
System logs will be sent to 10.92.125.52 from now on

(Cisco Controller) > config logging syslog host 2001:9:6:40::623
System logs will be sent to 2001:9:6:40::623 from now on

(Cisco Controller) > show logging
Logging to buffer :
- Logging of system messages to buffer :
  - Logging filter level..... errors
  - Number of system messages logged..... 1316
  - Number of system messages dropped..... 6892
- Logging of debug messages to buffer ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
- Cache of logging ..... Disabled
- Cache of logging time (mins) ..... 10080
- Number of over cache time log dropped ..... 0
Logging to console :
- Logging of system messages to console :
  - Logging filter level..... disabled
  - Number of system messages logged..... 0
  - Number of system messages dropped..... 8243
- Logging of debug messages to console ..... Enabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to syslog :
```

```

- Syslog facility..... local0
- Logging of system messages to console :
  - Logging filter level..... disabled
  - Number of system messages logged..... 0
  - Number of system messages dropped..... 8208
- Logging of debug messages to console ..... Enabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
- Logging of system messages to syslog :
  - Logging filter level..... errors
  - Number of system messages logged..... 1316
  - Number of system messages dropped..... 6892
- Logging of debug messages to syslog ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 2
- syslog over tls..... Disabled
  - Host 0..... 10.92.125.52
  - Host 1..... 2001:9:6:40::623
  - Host 2.....
Logging of RFC 5424..... Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
Logging of traceback..... Enabled

```

The following example shows how to remove two remote hosts 10.92.125.52 and 2001:9:6:40::623 that were configured for sending syslog messages and displaying that the configured syslog servers were removed from the controller:

```

(Cisco Controller) > config logging syslog host 10.92.125.52 delete
System logs will not be sent to 10.92.125.52 anymore

(Cisco Controller) > config logging syslog host 2001:9:6:40::623 delete
System logs will not be sent to 2001:9:6:40::623 anymore

(Cisco Controller) > show logging

```

```

Logging to buffer :
- Logging of system messages to buffer :
  - Logging filter level..... errors
  - Number of system messages logged..... 1316
  - Number of system messages dropped..... 6895
- Logging of debug messages to buffer ..... Disabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
- Cache of logging ..... Disabled
- Cache of logging time(mins) ..... 10080
- Number of over cache time log dropped ..... 0
Logging to console :
- Logging of system messages to console :
  - Logging filter level..... disabled
  - Number of system messages logged..... 0
  - Number of system messages dropped..... 8211
- Logging of debug messages to console ..... Enabled
  - Number of debug messages logged..... 0
  - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to syslog :
  - Logging filter level..... errors
  - Number of system messages logged..... 1316

```

```
- Number of system messages dropped..... 6895
- Logging of debug messages to syslog ..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 0
- syslog over tls..... Disabled
  - Host 0.....
  - Host 1.....
  - Host 2.....
Logging of RFC 5424..... Disabled
Logging of Debug messages to file :
- Logging of Debug messages to file..... Disabled
- Number of debug messages logged..... 0
- Number of debug messages dropped..... 0
Logging of traceback..... Enabled
- Traceback logging level..... errors
Logging of source file informational..... Enabled
Timestamping of messages.....
- Timestamping of system messages..... Enabled
  - Timestamp format..... Date and Time
```

config logging syslog facility

To set the facility for outgoing syslog messages to the remote host, use the **config logging syslog facility** command.

config logging syslog facility *facility_code*

Syntax Description	<i>facility_code</i>	Facility code. Choose one of the following:
		<ul style="list-style-type: none"> • authorization—Authorization system. Facility level—4. • auth-private—Authorization system (private). Facility level—10. • cron—Cron/at facility. Facility level—9. • daemon—System daemons. Facility level—3. • ftp—FTP daemon. Facility level—11. • kern—Kernel. Facility level—0. • local0—Local use. Facility level—16. • local1—Local use. Facility level—17. • local2—Local use. Facility level—18. • local3—Local use. Facility level—19. • local4—Local use. Facility level—20. • local5—Local use. Facility level—21. • local6—Local use. Facility level—22. • local7—Local use. Facility level—23. • lpr—Line printer system. Facility level—6. • mail—Mail system. Facility level—2. • news—USENET news. Facility level—7. • sys12—System use. Facility level—12. • sys13—System use. Facility level—13. • sys14—System use. Facility level—14. • sys15—System use. Facility level—15. • syslog—The syslog itself. Facility level—5. • user—User process. Facility level—1. • uucp—UNIX-to-UNIX copy system. Facility level—8.

Command Default None

Command History **Release** **Modification**

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

The following example shows how to set the facility for outgoing syslog messages to authorization:

```
(Cisco Controller) > config logging syslog facility authorization
```

Related Commands **config logging syslog host**
config logging syslog level
show logging

config logging syslog facility client

To configure the syslog facility to AP, use the **config logging syslog facility client** { **assocfail Dot11** | **associate Dot11** | **authentication** | **authfail Dot11** | **deauthenticate Dot11** | **disassociate Dot11** | **exclude** } { **enable** | **disable** } command.

config logging syslog facility *Client*

Syntax Description

Client

Facility Client. Has the following functions:

- **assocfail Dot11**—Association fail syslog for clients
- **associate Dot11**—Association syslog for clients
- **authentication**—Authentication success syslog for clients
- **authfail Dot11**—Authentication fail syslog for clients
- **deauthenticate Dot11**—Deauthentication syslog for clients
- **disassociate Dot11**—Disassociation syslog for clients
- **excluded**—Excluded syslog for clients

Command Default

None

Command History

Release Modification

7.5 This command was introduced in a release earlier than Release 7.5.

The following example shows how to set the facility syslog facility for client:

```
cisco controller config logging syslog facility client
```

Related Commands

show logging flags client

config logging syslog facility ap

To configure the syslog facility to AP, use the **config logging syslog facility ap** { **associate** | **disassociate** } { **enable** | **disable** } command.

config logging syslog facility *AP*

Syntax Description	<i>AP</i>	Facility AP. Has the following functions: <ul style="list-style-type: none"> • associate—Association syslog for AP • disassociate—Disassociation syslog for AP
---------------------------	-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

Command History	Release	Modification
	7.5	This command was introduced in a release earlier than Release 7.5.

The following example shows how to configure syslog facility for AP:

```
cisco controller config logging syslog facility ap
```

Related Commands	show logging flags ap
-------------------------	------------------------------

config logging syslog ipsec

To configure transmission of syslog messages over IPsec, use the **config logging syslog ipsec** command.

```
config logging syslog ipsec { enable | disable }
```

Syntax Description	enable	Disables transmission of syslog messages over IPsec.
	disable	Enables transmission of syslog messages over IPsec.

Command Default By default, transmission of syslog messages over IPsec is disabled.

Command History	Release	Modification
	8.0	This command was introduced.

Examples

The following example shows how to enable transmission of syslog messages over IPsec:

```
(Cisco Controller) > config logging syslog ipsec enable
```

config logging syslog ipsec profile

To configure an IPSec profile to define IPSec parameters for the connection, use the **config logging syslog ipsec profile** command.

config logging syslog ipsec profile *profile-name*

Syntax Description	<i>profile-name</i>	Name of the IPSec profile to use.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.

Examples

The following example shows how to configure an IPSec profile name to define IPSec parameters:

```
(Cisco Controller) > config logging syslog ipsec profile ipsec-profile-1
```

config logging syslog tls

To configure transmission of syslog messages over transport layer security (TLS), use the **config logging syslog tls** command.

config logging syslog tls { enable | disable }

Syntax Description	enable	disable
	Enables transmission of syslog messages over TLS. Enabling syslog over TLS on the controller enables the feature for all syslog hosts defined in the controller. You can define up to three syslog hosts per controller. The controller transmits messages concurrently to all the configured syslog hosts.	Disables transmission of syslog messages over TLS.

Command Default By default, transmission of syslog messages over TLS is disabled.

Command History	Release	Modification
	8.0	This command was introduced.

Examples

The following example shows how to enable transmission of syslog messages over TLS:

```
(Cisco Controller) > config logging syslog tls enable
```

Related Commands `show logging`

config logging syslog level

To set the severity level for filtering syslog messages to the remote host, use the **config logging syslog level** command.

config logging syslog level *severity_level*

Syntax Description

severity_level

Severity level. Choose one of the following:

- emergencies—Severity level 0
 - alerts—Severity level 1
 - critical—Severity level 2
 - errors—Severity level 3
 - warnings—Severity level 4
 - notifications—Severity level 5
 - informational—Severity level 6
 - debugging—Severity level 7
-

Command Default

None

Command History

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

The following example shows how to set the severity level for syslog messages to 3:

```
(Cisco Controller) > config logging syslog level 3
```

Related Commands

config logging syslog host

config logging syslog facility

show logging

config loginsession close

To close all active Telnet sessions, use the **config loginsession close** command.

```
config loginsession close {session_id | all}
```

Syntax Description

<i>session_id</i>	ID of the session to close.
-------------------	-----------------------------

all	Closes all Telnet sessions.
------------	-----------------------------

Command Default

None

Command History

Release Modification

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

The following example shows how to close all active Telnet sessions:

```
(Cisco Controller) > config loginsession close all
```

Related Commands

show loginsession

config macfilter

To create or delete a MAC filter entry on the Cisco wireless LAN controller, use the **config macfilter** { *add* | *delete* } command.

config macfilter { **add** *client_MAC wlan_id [interface_name] [description] [macfilter_IP]* | **delete** *client_MAC* }

Syntax Description

add	Adds a MAC filter entry on the controller.
delete	Deletes a MAC filter entry on the controller.
<i>MAC_addr</i>	Client MAC address.
<i>wlan_id</i>	Wireless LAN identifier with which the MAC filter entry should associate. A zero value associates the entry with any wireless LAN.
<i>interface_name</i>	(Optional) Name of the interface. Enter 0 to specify no interface.
<i>description</i>	(Optional) Short description of the interface (up to 32 characters) in double quotes. Note A description is mandatory if <i>macfilter_IP</i> is specified.
<i>IP Address</i>	(Optional) IPv4 address of the local MAC filter database.

Command Default

None

Command History

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

Usage Guidelines

Use the **config macfilter add** command to add a client locally to a wireless LAN on the Cisco wireless LAN controller. This filter bypasses the RADIUS authentication process.

As on release 7.6, the optional *macfilter_IP* supports only IPv4 address.

The following example shows how to add a MAC filter entry 00:E0:77:31:A3:55 with the wireless LAN ID 1, interface name labconnect, and MAC filter IP 10.92.125.51 on the controller:

```
(Cisco Controller) > config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

Related Commands

show macfilter
config macfilter ip-address

config macfilter description

To add a description to a MAC filter, use the **config macfilter description** command.

config macfilter description *MAC addr**description*

Syntax Description	<i>MAC addr</i>	Client MAC address.
	<i>description</i>	(Optional) Description within double quotes (up to 32 characters).

Command Default None

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

The following example shows how to configure the description MAC filter 01 to MAC address 11:11:11:11:11:11:

```
(Cisco Controller) > config macfilter description 11:11:11:11:11:11 "MAC Filter 01"
```

Related Commands `show macfilter`

config macfilter interface

To create a MAC filter client interface, use the **config macfilter interface** command.

config macfilter interface *MAC_addr interface*

Syntax Description		
	<i>MAC addr</i>	Client MAC address.
	<i>interface</i>	Interface name. A value of zero is equivalent to no name.

Command Default None

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

The following example shows how to configure a MAC filter interface Lab01 on client 11:11:11:11:11:11:

```
(Cisco Controller) > config macfilter interface 11:11:11:11:11:11 Lab01
```

Related Commands **show macfilter**

config macfilter ip-address

To enter passive client IP address , use the **config macfilter ip-address** command.

config macfilter ip-address *MAC_addr IP Address*

Syntax Description	<i>MAC_addr</i>	MAC address of the client.
	<i>IP Address</i>	Adds an IP address for passive clients.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4.

The following example shows how to add an IP address for a passive client:

```
(Cisco Controller) > config macfilter ip-address aa-bb-cc-dd-ee-ff 10.92.125.51
```

Related Commands **show macfilter**

config macfilter mac-delimiter

To set the MAC delimiter (colon, hyphen, none, and single-hyphen) for MAC addresses sent to RADIUS servers, use the **config macfilter mac-delimiter** command.

config macfilter mac-delimiter { **none** | **colon** | **hyphen** | **single-hyphen** }

Syntax Description	none	Disables the delimiters (for example, xxxxxxxxxx).
	colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
	hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
	single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
Command Default	The default delimiter is hyphen.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to have the operating system send MAC addresses to the RADIUS server in the form aa:bb:cc:dd:ee:ff:

```
(Cisco Controller) > config macfilter mac-delimiter colon
```

The following example shows how to have the operating system send MAC addresses to the RADIUS server in the form aa-bb-cc-dd-ee-ff:

```
(Cisco Controller) > config macfilter mac-delimiter hyphen
```

The following example shows how to have the operating system send MAC addresses to the RADIUS server in the form aabbccddeeff:

```
(Cisco Controller) > config macfilter mac-delimiter none
```

Related Commands **show macfilter**

config macfilter radius-compat

To configure the Cisco wireless LAN controller for compatibility with selected RADIUS servers, use the **config macfilter radius-compat** command.

```
config macfilter radius-compat { cisco | free | other }
```

Syntax Description		
	cisco	Configures the Cisco ACS compatibility mode (password is the MAC address of the server).
	free	Configures the Free RADIUS server compatibility mode (password is secret).
	other	Configures for other server behaviors (no password is necessary).

Command Default	Other
-----------------	-------

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports only IPv4.

The following example shows how to configure the Cisco ACS compatibility mode to “other”:

```
(Cisco Controller) > config macfilter radius-compat other
```

Related Commands	show macfilter
------------------	----------------

config macfilter wlan-id

To modify a wireless LAN ID for a MAC filter, use the **config macfilter wlan-id** command.

config macfilter wlan-id *MAC_addr WLAN_id*

Syntax Description		
	<i>MAC_addr</i>	Client MAC address.
	<i>WLAN_id</i>	Wireless LAN identifier to associate with. A value of zero is not allowed.

Command Default None

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

The following example shows how to modify client wireless LAN ID 2 for a MAC filter 11:11:11:11:11:11:

```
(Cisco Controller) > config macfilter wlan-id 11:11:11:11:11:11 2
```

Related Commands

- show macfilter**
- show wlan**

config mdns ap

To configure multicast Domain Name System (mDNS) snooping on an access point, use the **config mdns ap** command.

```
config mdns ap {enable {ap_name | all} [vlan vlan_id] | disable {ap_name | all} | vlan
{add | delete} vlan ap_name}
```

Syntax Description	enable	ap_name	all	vlan	vlan_id	disable	add	delete
	Enables mDNS snooping on an access point.	Name of the access point on which mDNS snooping has to be configured.	Configures mDNS snooping on all access points.	(Optional) Configures the VLAN on which the access point snoops and forwards the mDNS packets.	VLAN identifier.	Disables mDNS snooping on an access point.	Adds a VLAN from which the access point snoops and forwards the mDNS packets to the Cisco Wireless LAN Controller (WLC). You can configure up to 10 VLANs for an mDNS access point.	Deletes a VLAN from which the access point snoops and forwards the mDNS packets to the Cisco WLC.

Command Default The mDNS-enabled access point snoops the access or native VLANs by default.

Command History	Release	Modification
	7.5	This command was introduced.

Usage Guidelines Enabling mDNS snooping on access points allows the access points to snoop the wired services on VLANs that are invisible to the Cisco WLC. mDNS snooping is supported only on local-mode and monitor-mode access points. The access point must be in the access mode or trunk mode. If the access point is in the trunk mode, you must configure the VLAN on the Cisco WLC on which the access point snoops and forwards the mDNS packets. You must also configure the native VLAN from the Cisco WLC for the access point to snoop and send mDNS queries on. The access point also tags the packets with the native VLAN.

Global mDNS snooping overrides mDNS access point snooping.

The following example shows how to enable mDNS snooping on an access point and the VLAN on which it must snoop for mDNS packets:

```
(Cisco Controller) > config mdns ap enable vlan 1
```

config mdns profile

To configure a multicast DNS (mDNS) profile and associate a service with the profile, use the **config mdns profile** command.

```
config mdns profile { create | delete | service { add | delete } service _name profile_name
```

Syntax Description

create	Creates an mDNS profile.
delete	Deletes an mDNS profile. If the profile is associated to an interface group, an interface, or a WLAN, an error appears.
service	Configures an mDNS service.
add	Adds an mDNS service to an mDNS profile.
delete	Deletes an mDNS service from an mDNS profile.
<i>service -name</i>	Name of the mDNS service.
<i>profile_name</i>	Name of the mDNS profile. You can create a maximum of 16 profiles.

Command Default

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. 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.

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

The following example shows how to add the Apple TV mDNS service to the mDNS profile1.

```
(Cisco Controller) > config mdns profile create profile1 Apple TV
```

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
clear mdns service-database
debug mdns all
debug mdns error
debug mdns detail
debug mdns message

config mdns query interval

To configure the query interval for multicast DNS (mDNS) services, use the **config mdns query interval** command.

config mdns query interval *interval_value*

Syntax Description	<i>interval_value</i> mDNS query interval, in minutes, that you can set. The query interval is the frequency at which the controller sends periodic queries to all the services defined in the Master Services database. The range is from 10 to 120.				
Command Default	The default query interval for an mDNS service is 15 minutes.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.4</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	7.4	This command was introduced.
Release	Modification				
7.4	This command was introduced.				
Usage Guidelines	<p>The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database. mDNS uses the multicast IP address 224.0.0.251 as the destination address and 5353 as UDP destination port.</p> <p>The following example shows how to configure the query interval for mDNS services as 20 minutes.</p> <pre>(Cisco Controller) > config mdns query interval 20</pre>				

Related Commands	<ul style="list-style-type: none"> config mdns profile 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 mdns message
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

config mdns service

To configure multicast DNS (mDNS) services in the master services database, use the **config mdns service** command.

The following command is valid in Release 7.5 and later releases:

```
config mdns service {create service_name service_string origin {Wireless | Wired | All} lss {enable
| disable} [query {enable | disable}] | lss {enable | disable} {service_name | all} |
priority-mac {add | delete} priority-mac service_name [ap-group ap-group-name] | origin
{Wireless | Wired | All} {service_name | all}}
```

Syntax Description

create	Adds a new mDNS service to the Master Services database.
<i>service_name</i>	Name of the mDNS service, for example, Air Tunes, iTunes Music Sharing, FTP, Apple File Sharing Protocol (AFP).
<i>service_string</i>	Unique string associated to an mDNS service, for example, <code>_airplay._tcp.local</code> . is the service string associated with Apple TV.
delete	Deletes an mDNS service from the Master Services database. Before deleting the service, the controller checks if any profile is using the service. Note You must delete the service from all profiles before deleting it.
query	Configures the query status for the mDNS service.
enable	Enables periodic query for an mDNS service by the controller.
disable	Disables periodic query for an mDNS service by the controller.
origin	Configures the origin of the mDNS service. You can restrict the origin of the service as wired or wireless.
Wireless	Configures the origin of the mDNS service as wireless.
Wired	Configures the origin of the mDNS service as wired.
All	Configures the origin of the mDNS service as wireless or wired.
lss	Configures Location Specific Services (LSS) for a service or all mDNS services. LSS is not applicable for registered service providers. The registered service providers are always included if the querying client corresponds to the user. You cannot configure LSS on the services configured as only wired.
all	Configures LSS for all mDNS services.
priority-mac	Configures the MAC address of a service provider device. This device gets a priority even if the service provider database is full.

add	Adds the MAC address of a service provider device for priority. You can configure up to 50 MAC addresses for a service.
delete	Deletes the MAC address of a service provider device from the priority list.
<i>priority-mac</i>	MAC address of a service provider device that needs priority. The MAC address must be unique for each service.
ap-group	Configures the access point group for wired service providers. These service providers get priority over others. When a client mDNS query originates from this AP group, the wired entries with priority MAC addresses and access point groups are listed first in the aggregated response.
<i>ap-group-name</i>	Name of the access point group to which the service provider belongs.

Command Default

By default, LSS is disabled, but it is enabled for all the discovered services.

Command History

Release	Modification
7.4	This command was introduced.
7.5	This command was modified. The origin , Wireless , Wired , All , lss , priority-mac , add , delete , ap-group keywords and <i>priority-mac ap-group-name</i> arguments were added.

Usage Guidelines

In Release 7.5 and later releases, the maximum number of service providers for different controller models are as follows:

- Cisco 5500 Series Controller and Cisco 2500 Series Controller—6400
- Cisco Wireless Services Module 2—6400
- Cisco 8500 Series Controller and Cisco 7500 Series Controller—16000

You cannot change the services with the origin set to Wireless to Wired if LSS is enabled for the service.

The following example shows how to add the HTTP mDNS service to the Master Services database, configure the origin as wireless, and enable LSS for the service:

```
(Cisco Controller) > config mdns service create http _http._tcp.local. origin wireless lss enable
```

The following example shows how to add a priority MAC address of a HTTP service provider device:

```
(Cisco Controller) > config mdns service priority-mac add 44:03:a7:a3:04:45 http
```

config mdns snooping

To enable or disable global multicast DNS (mDNS) snooping on the Cisco WLC, use the **config mdns snooping** command.

```
config mdns snooping {enable | disable}
```

Syntax Description

enable Enables mDNS snooping on the Cisco WLC.

disable Disables mDNS snooping on the Cisco WLC.

Command Default

By default, mDNS snooping is enabled on the Cisco WLC.

Command History

Release Modification

7.4 This command was introduced.

Usage Guidelines

mDNS service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast. mDNS supports zero configuration IP networking.

The following example shows how to enable mDNS snooping:

```
(Cisco Controller) > config mdns snooping enable
```

Related Commands

```
config mdns query interval
config mdns service
config mdns profile
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 mdns message
```

config mdns policy enable

To configure the mDNS policy use the **config mdns policy enable | disable** command.

config mdnspolicyenable | disable

Syntax Description	
policy	Name of the mDNS policy.
enable	Enables the policy for an mDNS service by the controller.
disable	Disables the policy for an mDNS service by the controller.

Command Default	
	None

Command History	Release	Modification
	8.0	This command was introduced.

Usage Guidelines	
	This command is valid for 8.0 release onwards.

Example

The following example show how to configure the mDNS policy.

```
(Cisco Controller) >config mdns
  policy enable
```

config mdns policy service-group

To create or delete mDNS policy service group use the **config mdns policy service-group** command.

```
config mdns policy service-group { create | delete } service-group-name
```

Syntax	Description
create	Creates the mDNS service group.
delete	Deletes the mDNS service group.
<i>service-group-name</i>	Name of the service group.

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

Command History	Release	Modification
	8.0	This command was introduced.

Example

The following example shows how to delete a mDNS service group.

```
(Cisco Controller) >config mdns policy service-group delete <service-group-name>
```

config mdns policy service-group parameters

To configure the parameters of a service group, use the **config mdns policy service-group** command.

config mdnspolicyservice-group device-mac add *service-group-name mac-addr device name* **location-type** *[AP_LOCATION | AP_NAME | AP_GROUP]* **device-location** *[location string | any | same]*

Syntax Description	device-mac	Configures MAC address of a service provider device.
	add	Adds the service group name of the service provider device.
	<i>service-group-name</i>	Name of a mDNS service group.
	<i>device-name</i>	Name of a device to which the service provider belongs.
	location type	Configures a location type of a service provider device.
	<i>[AP_LOCATION AP_NAME AP_GROUP]</i>	Name, location, group of the access point.
	device-location	Configures location of a device to which the service provider belongs.
	<i>[location string any same]</i>	location string of a device.
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.

Example

The following example shows how to configure a location type of a service provider device.

```
(Cisco Controller) >config mdns policy service-group location type [AP_LOCATION | AP_NAME
| AP_GROUP]
```

config mdns policy service-group user-name

To configure a user role for a mDNS service group, use the **config mdns policy service-group user-name add | delete <service-group-name> <user-role-name>** command

config mdnspolicy*service-group***user-name****add | delete***service-group-name user-name*

Syntax Description	user-name	Configures name of a user for mDNS service group.
	<i>service-group-name</i>	Name of a mDNS service group
	<i>user-name</i>	Name of the user role for mDNS service group

Command Default None

Command History	Release	Modification
	8.0	This command was introduced.

Example

The following example show how to add user name for a mDNS service group

```
(Cisco Controller) >config mdns policy service-group user-name add <service-group-name>
<user-role-name>
```

config mdns policy service-group user-role

To configure a user role for a mDNS service group, use the **config mdns policy service-group user-role add | delete <service-group-name> <user-role-name>** command.

config mdnspolicyservice-groupuser-roleadd | delete*service-group-name user-role-name*

Syntax Description	user-role	Configures a user role for mDNS service group.
	<i>service-group-name</i>	Name of a mDNS service group
	<i>user-role-name</i>	Name of the user role for mDNS service group
Command Default	None	
Command History	Release	Modification
	8.0	This command was introduced.

Example

The following example show how to add user role details for a mDNS service group

```
(Cisco Controller) >config mdns policy service-group user-role add <service-group-name>
<user-role-name>
```

config media-stream multicast-direct

To configure the media-stream multicast direct, use the **config media-stream multicast direct** command.

```
config media-stream multicast-direct { enable | disable }
```

Syntax Description

enable	Enables a media stream.
---------------	-------------------------

disable	Disables a media stream.
----------------	--------------------------

Command Default

None.

Usage Guidelines

Media-stream multicast-direct requires load based Call Admission Control (CAC) to run.

This example shows how to enable media-stream multicast-direct settings:

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

This example shows how to disable media-stream multicast-direct settings:

```
> config media-stream multicast-direct disable
```

Related Commands

config 802.11 media-stream video-redirect

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream message

To configure various parameters of message configuration, use the **config media-stream message** command.

```
config media-stream message {state [enable | disable] | url url | email email | phone
phone_number | note note }
```

Syntax Description		
state		Specifies the media stream message state.
enable		(Optional) Enables the session announcement message state.
disable		(Optional) Disables the session announcement message state.
url		Configures the URL.
<i>url</i>		Session announcement URL.
email		Configures the email ID.
<i>email</i>		Specifies the session announcement e-mail.
phone		Configures the phone number.
<i>phone_number</i>		Session announcement phone number.
note		Configures the notes.
<i>note</i>		Session announcement notes.

Command Default Disabled.

Usage Guidelines Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to enable the session announcement message state:

```
> config media-stream message state enable
```

This example shows how to configure the session announcement e-mail address:

```
> config media-stream message mail abc@co.com
```

Related Commands

- config media-stream**
- show 802.11a media-stream name**
- show media-stream group summary**
- show media-stream group detail**

config media-stream add

To configure the various global media-stream configurations, use the **config media-stream add** command.

```
config media-stream add multicast-direct media_stream_name start-IP end-IP [template {very coarse
| coarse | ordinary | low-resolution | med-resolution | high-resolution} | detail {bandwidth
packet-size {periodic | initial}}] qos priority {drop | fallback}
```

Syntax	Description
multicast-direct	Specifies the media stream for the multicast-direct setting.
<i>media_stream_name</i>	Media-stream name.
<i>start-IP</i>	IP multicast destination start address.
<i>end-IP</i>	IP multicast destination end address.
template	(Optional) Configures the media stream from templates.
very coarse	Applies a very-coarse template.
coarse	Applies a coarse template.
ordinary	Applies an ordinary template.
low-resolution	Applies a low-resolution template.
med-resolution	Applies a medium-resolution template.
high-resolution	Applies a high-resolution template.
detail	Configures the media stream with specific parameters.
<i>bandwidth</i>	Maximum expected stream bandwidth.
<i>packet-size</i>	Average packet size.
periodic	Specifies the periodic admission evaluation.
initial	Specifies the Initial admission evaluation.
<i>qos</i>	AIR QoS class (video only).
<i>priority</i>	Media-stream priority.
drop	Specifies that the stream is dropped on a periodic reevaluation.
fallback	Specifies if the stream is demoted to the best-effort class on a periodic reevaluation.

Command Default None

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

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to configure a new media stream:

```
> config media-stream add multicast-direct abc 227.8.8.8 227.9.9.9 detail 2 150 periodic
video 1 drop
```

Related Commands

show 802.11a media-stream name
show media-stream group summary
show media-stream group detail

config media-stream admit

To allow traffic for a media stream group, use the **config media-stream admit** command.

config media-stream admit *media_stream_name*

Syntax Description	<i>media_stream_name</i>	Media-stream group name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>When you try to allow traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.</p> <p>This example shows how to allow traffic for a media stream group:</p> <pre>(Cisco Controller) > config media-stream admit MymediaStream</pre>	
Related Commands	<p>show 802.11a media-stream name</p> <p>show media-stream group summary</p> <p>show media-stream group detail</p>	

config media-stream deny

To block traffic for a media stream group, use the **config media-stream deny** command.

Syntax Description	<i>media_stream_name</i> Media-stream group name.
---------------------------	---------------------------------------------------

config media-stream deny *media_stream_name*

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

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

Usage Guidelines	When you try to block traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

This example shows how to block traffic for a media stream group:

```
(Cisco Controller) > config media-stream deny MymediaStream
```

Related Commands	<p>show 802.11a media-stream name</p> <p>show media-stream group summary</p> <p>show media-stream group detail</p>
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------

config media-stream delete

To configure the various global media-stream configurations, use the **config media-stream delete** command.

config media-stream delete *media_stream_name*

Syntax Description	<i>media_stream_name</i>	Media-stream name.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.	
	This example shows how to delete the media stream named abc:	
	<pre>(Cisco Controller) > config media-stream delete abc</pre>	
Related Commands	show 802.11a media-stream name show media-stream group summary show media-stream group detail	

config memory monitor errors

To enable or disable monitoring for memory errors and leaks, use the **config memory monitor errors** command.

config memory monitor errors {enable | disable}



Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

enable Enables the monitoring for memory settings.

disable Disables the monitoring for memory settings.

Command Default

Monitoring for memory errors and leaks is disabled by default.

Command History

Release Modification

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

Usage Guidelines

Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

The following example shows how to enable monitoring for memory errors and leaks for a controller:

```
(Cisco Controller) > config memory monitor errors enable
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config memory monitor leaks

To configure the controller to perform an auto-leak analysis between two memory thresholds, use the **config memory monitor leaks** command.

config memory monitor leaks *low_thresh high_thresh*



Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description		
<i>low_thresh</i>		Value below which free memory cannot fall without crashing. This value cannot be set lower than 10000 KB.
<i>high_thresh</i>		Value below which the controller enters auto-leak-analysis mode. See the “Usage Guidelines” section.

Command Default The default value for *low_thresh* is 10000 KB; the default value for *high_thresh* is 30000 KB.

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

Usage Guidelines



Note Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Use this command if you suspect that a memory leak has occurred.

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 KB, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks.

The following example shows how to set the threshold values for auto-leak-analysis mode to 12000 KB for the low threshold and 35000 KB for the high threshold:

```
(Cisco Controller) > config memory monitor leaks 12000 35000
```

Related Commands

- config memory monitor leaks**
- debug memory**

show memory monitor

config mesh alarm

To configure alarm settings for outdoor mesh access points, use the **config mesh alarm** command.

```
config mesh alarm { max-hop | max-children | low-snr | high-snr | association | parent-change count } value
```

Syntax Description		
max-hop		Sets the maximum number of hops before triggering an alarm for traffic over the mesh network. The valid values are 1 to 16 (inclusive).
max-children		Sets the maximum number of mesh access points (MAPs) that can be assigned to a mesh router access point (RAP) before triggering an alarm. The valid values are 1 to 16 (inclusive).
low-snr		Sets the low-end signal-to-noise ratio (SNR) value before triggering an alarm. The valid values are 1 to 30 (inclusive).
high-snr		Sets the high-end SNR value before triggering an alarm. The valid values are 1 to 30 (inclusive).
association		Sets the mesh alarm association count value before triggering an alarm. The valid values are 1 to 30 (inclusive).
parent-change count		Sets the number of times a MAP can change its RAP association before triggering an alarm. The valid values are 1 to 30 (inclusive).
<i>value</i>		Value above or below which an alarm is generated. The valid values vary for each command.

Command Default See the “Syntax Description” section for command and argument value ranges.

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

The following example shows how to set the maximum hops threshold to 8:

```
(Cisco Controller) >config mesh alarm max-hop 8
```

The following example shows how to set the upper SNR threshold to 25:

```
(Cisco Controller) >config mesh alarm high-snr 25
```

config mesh astools

To globally enable or disable the anti-stranding feature for outdoor mesh access points, use the **config mesh astools** command.

config mesh astools {enable | disable}

Syntax Description	enable	Enables this feature for all outdoor mesh access points.
	disable	Disables this feature for all outdoor mesh access points.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable anti-stranding on all outdoor mesh access points:

```
(Cisco Controller) >config mesh astools enable
```

config mesh backhaul rate-adapt

To globally configure the backhaul Tx rate adaptation (universal access) settings for indoor and outdoor mesh access points, use the **config mesh backhaul rate-adapt** command.

config mesh backhaul rate-adapt [**all** | **bronze** | **silver** | **gold** | **platinum**] {**enable** | **disable**}

Syntax Description		
all	(Optional) Grants universal access privileges on mesh access points.	
bronze	(Optional) Grants background-level client access privileges on mesh access points.	
silver	(Optional) Grants best effort-level client access privileges on mesh access points.	
gold	(Optional) Grants video-level client access privileges on mesh access points.	
platinum	(Optional) Grants voice-level client access privileges on mesh access points.	
enable	Enables this backhaul access level for mesh access points.	
disable	Disables this backhaul access level for mesh access points.	

Command Default Backhaul access level for mesh access points is disabled.

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

Usage Guidelines To use this command, mesh backhaul with client access must be enabled by using the **config mesh client-access** command.



Note After this feature is enabled, all mesh access points reboot.

The following example shows how to set the backhaul client access to the best-effort level:

```
(Cisco Controller) >config mesh backhaul rate-adapt silver
```

config mesh backhaul slot

To configure the slot radio as a downlink backhaul, use the **config mesh backhaul slot** command.

config mesh backhaul slot *slot_id* {**enable** | **disable**} *cisco_ap*

Syntax Description

<i>slot_id</i>	Slot number between 0 and 2.
enable	Enables the entered slot radio as a downlink backhaul.
disable	Disables the entered slot radio as a downlink backhaul.
<i>cisco_ap</i>	Name of the Root AP of the sector on which the backhaul needs to be enabled or disabled.

Command Default

The entered slot radio as a downlink backhaul is disabled.

Command History

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

Usage Guidelines

For 2.4 GHz, only slot 0 and 1 are valid. If slot 0 is enabled, slot 1 is automatically be disabled. If slot 0 is disabled, slot 1 is automatically enabled.

The following example shows how to enable slot 1 as the preferred backhaul for the root AP myrootap1:

```
(Cisco Controller) >config mesh backhaul slot 1 enable myrootap1
```

config mesh battery-state

To configure the battery state for Cisco mesh access points, use the **config mesh battery-state** command.

```
config mesh battery-state disable {all | cisco_ap}
```

Syntax Description	disable	Disables the battery-state for mesh access points.
	all	Applies this command to all mesh access points.
	cisco_ap	Specific mesh access point.

Command Default	Battery state is disabled.
-----------------	----------------------------

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

The following example shows how to disable battery state for all mesh APs:

```
(Cisco Controller) >config mesh battery-state disable all
```

config mesh client-access

To enable or disable client access to the mesh backhaul on indoor and outdoor mesh access points, use the **config mesh client-access** command.

config mesh client-access { **enable** [**extended**] | **disable** }

Syntax Description	enable	extended	disable
	Allows wireless client association over the mesh access point backhaul 802.11a radio.	(Optional) Enables client access over both the backhaul radios for backhaul access points.	Restricts the 802.11a radio to backhaul traffic, and allows client association only over the 802.11b/g radio.
Command Default	Client access is disabled.		
Command History	Release	Modification	
	7.6	This command was introduced in a release earlier than Release 7.6.	

Usage Guidelines

Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.

When this feature is enabled, the mesh access points allow wireless client association over the 802.11a radio, which implies that a 152x mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio.

When this feature is disabled, the mesh access points carry backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio.

The following example shows how to enable client access extended to allow a wireless client association over the 802.11a radio:

```
(Cisco Controller) >config mesh client-access enable extended
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh AP will be rebooted
Are you sure you want to start? (y/N)Y
```

The following example shows how to restrict a wireless client association to the 802.11b/g radio:

```
(Cisco Controller) >config mesh client-access disable
All Mesh AP will be rebooted
Are you sure you want to start? (Y/N) Y
Backhaul with client access is canceled.
```

config mesh convergence

To configure mesh convergence method on all mesh access points, use the **config mesh convergence** command.

```
config mesh convergence {fast [standard] | very-fast} all
```

Syntax Description

fast	Sets the fast convergence method.
standard	Sets the standard convergence method.
very-fast	Set very-fast convergence method.
<i>all</i>	Sets the selected mesh convergence method on all the mesh access points.

Command Default

The default mesh convergence method is standard.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

The standard convergence method is available on Release 7.6 onwards. The fast and very fast convergence methods are available from Release 8.0.

This table lists the different convergence methods.

Convergence method	Parent loss Timer (seconds)	Seek per channel Timer (seconds)
Standard	21	3
Fast	7	2
Very Fast	4	2

The following example shows how to set mesh convergence to standard:

```
(Cisco Controller) >config mesh convergence standard all
```

config mesh ethernet-bridging allow-bpdu

To configure STP BPDUs towards wired mesh uplink, use the **config mesh ethernet-bridging allow-bpdu** command.

config mesh ethernet-bridging allow-bpdu { **enable** | **disable** }

Syntax Description	enable	Enables STP BPDUs towards wired mesh uplink.
	disable	Disables STP BPDUs towards wired mesh uplink.
Command Default	Disabled	
Command History	Release	Modification
	8.0.110.0	This command was introduced.
Usage Guidelines	Cisco WLC does not allow you to use this command if VLAN transparency is enabled.	

config mesh ethernet-bridging vlan-transparent

To configure how a mesh access point handles VLAN tags for Ethernet bridged traffic, use the **config mesh ethernet-bridging vlan-transparent** command.

```
config mesh ethernet-bridging vlan-transparent {enable | disable}
```

Syntax Description	enable	Bridges packets as if they are untagged.
	disable	Drops all tagged packets.

Command Default	Bridges packets as if they are untagged.	
-----------------	------------------------------------------	--

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

The following example shows how to configure Ethernet packets as untagged:

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent enable
```

The following example shows how to drop tagged Ethernet packets:

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent disable
```

config mesh full-sector-dfs

To globally enable or disable full-sector Dynamic Frequency Selection (DFS) on mesh access points, use the **config mesh full-sector-dfs** command.

```
config mesh full-sector-dfs { enable | disable }
```

Syntax Description	enable Enables DFS for mesh access points.				
	disable Disables DFS for mesh access points.				
Command Default	None				
Command History	<table border="1"> <thead> <tr> <th data-bbox="342 709 565 743">Release</th> <th data-bbox="570 709 1490 743">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="342 758 565 791">7.6</td> <td data-bbox="570 758 1490 791">This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				

Usage Guidelines

This command instructs the mesh sector to make a coordinated channel change on the detection of a radar signal. For example, if a mesh access point (MAP) detects a radar signal, the MAP will notify the root access point (RAP), and the RAP will initiate a sector change.

All MAPs and the RAP that belong to that sector go to a new channel, which lowers the probability of MAPs stranding when radar is detected on the current backhaul channel, and no other valid parent is available as backup.

Each sector change causes the network to be silent for 60 seconds (as dictated by the DFS standard).

It is expected that after a half hour, the RAP will go back to the previously configured channel, which means that if radar is frequently observed on a RAP's channel, it is important that you configure a different channel for that RAP to exclude the radar affected channel at the controller.

This example shows to enable full-sector DFS on mesh access points:

```
(Cisco Controller) >config mesh full-sector-dfs enable
```



```

rx dup pkts:          0
rx out of order:     0
avgSNR: 30, high: 33, low: 3
SNR profile [0dB...60dB]
    0          6          0          0          0
    0          0          1          2          77
    2888       3          0          0          0
    0          0          0          0          0
(>60dB)           0
avgNf: -95, high: -67, low: -97
Noise Floor profile [-100dB...-40dB]
    0          2948       19          3          1
    0          0          0          0          0
    3          3          0          0          0
    0          0          0          0          0
(>-40dB)           0
avgRssi: 64, high: 68, low: 63
RSSI profile [-100dB...-40dB]
    0          0          0          0          0
    0          0          0          0          0
    0          0          0          0          0
    0          0          0          0          0
(>-40dB)           2977
Summary PktFailedRate (Total pkts sent/recvd):          0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%

```

This example shows how to enable external MAC filtering on access point AP001d.71d.e300:

```

(Cisco Controller) >config mesh linkdata AP001d.71d.e300
[SD:0,0,0(0,0,0), 0,0, 0,0]
[SD:1,105,0(0,0,0),30,704,95,707]
[SD:2,103,0(0,0,0),30,46,95,25]
[SD:3,105,0(0,0,0),30,73,95,29]
[SD:4,82,0(0,0,0),30,39,95,24]
[SD:5,82,0(0,0,0),30,60,95,26]
[SD:6,105,0(0,0,0),30,47,95,23]
[SD:7,103,0(0,0,0),30,51,95,24]
[SD:8,105,0(0,0,0),30,55,95,24]
[SD:9,103,0(0,0,0),30,740,95,749]
[SD:10,105,0(0,0,0),30,39,95,20]
[SD:11,104,0(0,0,0),30,58,95,23]
[SD:12,105,0(0,0,0),30,53,95,24]
[SD:13,103,0(0,0,0),30,64,95,43]
[SD:14,105,0(0,0,0),30,54,95,27]
[SD:15,103,0(0,0,0),31,51,95,24]
[SD:16,105,0(0,0,0),30,59,95,23]
[SD:17,104,0(0,0,0),30,53,95,25]
[SD:18,105,0(0,0,0),30,773,95,777]
[SD:19,103,0(0,0,0),30,745,95,736]
[SD:20,105,0(0,0,0),30,64,95,54]
[SD:21,103,0(0,0,0),30,747,95,751]
[SD:22,105,0(0,0,0),30,55,95,25]
[SD:23,104,0(0,0,0),30,52,95,35]
[SD:24,105,0(0,0,0),30,134,95,23]
[SD:25,103,0(0,0,0),30,110,95,76]
[SD:26,105,0(0,0,0),30,791,95,788]
[SD:27,103,0(0,0,0),30,53,95,23]
[SD:28,105,0(0,0,0),30,128,95,25]
[SD:29,104,0(0,0,0),30,49,95,24]
[SD:30,0,0(0,0,0), 0,0, 0,0]

```

config mesh linktest

To verify client access between mesh access points, use the **config mesh linktest** command.

config mesh linktest *source_ap* { *dest_ap* | *MAC addr* } *datarate* *packet_rate* *packet_size* *duration*

Syntax Description					
<i>source_ap</i>	Source access point.				
<i>dest_ap</i>	Destination access point.				
<i>MAC addr</i>	MAC address.				
<i>datarate</i>	<ul style="list-style-type: none"> Data rate for 802.11a radios. Valid values are 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps. Data rate for 802.11b radios. Valid values are 6, 12, 18, 24, 36, 54, or 100 Mbps. Data rate for 802.11n radios. Valid values are MCS rates between m0 to m15. 				
<i>packet_rate</i>	Number of packets per second. Valid range is 1 through 3000, but the recommended default is 100.				
<i>packet_size</i>	(Optional) Packet size in bytes. If not specified, packet size defaults to 1500 bytes.				
<i>duration</i>	(Optional) Duration of the test in seconds. Valid values are 10-300 seconds, inclusive. If not specified, duration defaults to 30 seconds.				
Command Default	100 packets per second, 1500 bytes, 30-second duration.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				

Usage Guidelines

The **config mesh linktest** and **config mesh linkdata** commands are designed to be used together to verify information between a source and a destination access point. To get this information, first enter the **config mesh linktest** command with the access point that you want link data from in the *dest_ap* argument. When the command completes, enter the **config mesh linkdata** command and list the same destination access point, to display the link data.

The following warning message appears when you run a linktest that might oversubscribe the link:

```
Warning! Data Rate (100 Mbps) is not enough to perform this link test on
packet size (2000bytes) and (1000) packets per second. This may cause AP
to disconnect or reboot. Are you sure you want to continue?
```

The following example shows how to verify client access between mesh access points *SB_MAP1* and *SB_RAP2* at 36 Mbps, 20 fps, 100 frame size, and 15-second duration:

```
(Cisco Controller) >config mesh linktest SB_MAP1 SB_RAP1 36 20 100 15
LinkTest started on source AP, test ID: 0
[00:1D:71:0E:85:00]->[00:1D:71:0E:D0:0F]
Test config: 100 byte packets at 20 pps for 15 seconds, a-link rate 36 Mb/s
In progress: | || || || || || |
LinkTest complete
Results
=====
txPkts:                290
txBuffAllocErr:        0
txQFullErrs:           0
Total rx pkts heard at destination:      290
rx pkts decoded correctly:
  err pkts: Total      0 (PHY 0 + CRC 0 + Unknown 0), TooBig 0, TooSmall 0
  rx lost packets:     0 (incr for each pkt seq missed or out of order)
  rx dup pkts:         0
  rx out of order:     0
avgSNR:   37, high: 40, low: 5
SNR profile [0dB...60dB]
   0          1          0          0          1
   3          0          1          0          2
   8         27         243         4          0
   0          0          0          0          0
(>60dB)      0
avgNf:   -89, high: -58, low: -90
Noise Floor profile [-100dB...-40dB]
   0          0          0          145         126
  11         2          0          1          0
   3          0          1          0          1
   0          0          0          0          0
(>-40dB)     0
avgRssi:  51, high: 53, low: 50
RSSI profile [-100dB...-40dB]
   0          0          0          0          0
   0          0          0          0          0
   0          0          0          0          0
   0          7         283         0          0
(>-40dB)     0
Summary PktFailedRate (Total pkts sent/recvd):                0.000%
Physical layer Error rate (Total pkts with errors/Total pkts heard): 0.000%
```

The following table lists the output flags displayed for the **config mesh linktest** command.

Table 1: Output Flags for the Config Mesh Linktest Command

Output Flag	Description
txPkts	Number of packets sent by the source.
txBuffAllocErr	Number of linktest buffer allocation errors at the source (expected to be zero).
txQFullErrs	Number of linktest queue full errors at the source (expected to be zero).
Total rx pkts heard at destination	Number of linktest packets received at the destination (expected to be same as or close to the txPkts).

Output Flag	Description
rx pkts decoded correctly	Number of linktest packets received and decoded correctly at the destination (expected to be same as close to txPkts).
err pkts: Total	Packet error statistics for linktest packets with errors.
rx lost packets	Total number of linktest packets not received at the destination.
rx dup pkts	Total number of duplicate linktest packets received at the destination.
rx out of order	Total number of linktest packets received out of order at the destination.
avgNF	Average noise floor.
Noise Floor profile	Noise floor profile in dB and are negative numbers.
avgSNR	Average SNR values.
SNR profile [odb...60dB]	Histogram samples received between 0 to 60 dB. The different columns in the SNR profile is the number of packets falling under the bucket 0-3, 3-6, 6-9, up to 57-60.
avgRSSI	Average RSSI values. The average high and low RSSI values are positive numbers.
RSSI profile [-100dB...-40dB]	The RSSI profile in dB and are negative numbers.

config mesh lsc

To configure a locally significant certificate (LSC) on mesh access points, use the **config mesh lsc** command.

config mesh lsc { **enable** | **disable** }

Syntax Description	enable	disable
	Enables an LSC on mesh access points.	Disables an LSC on mesh access points.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable LSC on mesh access points:

```
(Cisco Controller) >config mesh lsc enable
```

config mesh lsc advanced

To configure an advanced locally significant certificate (LSC) when a wildcard is used in an external authentication, authorization, and accounting (AAA) server for a mesh Access Point (AP), use the **config mesh lsc advanced** command.

```
config mesh lsc advanced {enable | disable}
```

Syntax Description	enable Enables advanced LSC for a mesh AP.
	disable Disables advanced LSC for a mesh AP.

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

Command History	Release Modification
	8.0 This command was introduced.

The following example shows how to enable advanced LSC for a mesh AP:

```
(Cisco Controller) >config mesh lsc advanced enable
```

config mesh lsc advanced ap-provision

To configure advanced mesh locally significant certificate (LSC) Access Point (AP) provision if a wildcard is used in an external authentication, authorization, and accounting (AAA) server for a mesh AP, use the **config mesh lsc advanced ap-provision** command.

config mesh lsc advanced ap-provision {enable | disable | open-window {enable | disable} | provision-controller {enable | disable}}

Syntax	Description
enable	Enables advanced mesh LSC AP provision if a wildcard is used in an external AAA server for a mesh AP.
disable	Disables advanced mesh LSC AP provision if a wildcard is used in an external AAA server for a mesh AP.
open-window	Configures mesh LSC provision for all mesh APs without MAC validation.
enable	Enables AP provision for all mesh APs without MAC validation.
disable	Disables AP provision for all mesh APs without MAC validation.
provision-controller	Configures the provision controller details for mesh APs to get an LSC.
enable	Enables the provision controller option to get an LSC.
disable	Disables the provision controller option to get an LSC.

Command Default None

Command History	Release	Modification
	8.0	This command was introduced.

The following example shows how to enable the advanced AP provision method:

```
(Cisco Controller) >config mesh lsc advanced ap-provision enable
```

config mesh multicast

To configure multicast mode settings to manage multicast transmissions within the mesh network, use the **config mesh multicast** command.

config mesh multicast { **regular** | **in** | **in-out** }

Syntax Description	regular	in	in-out
	Multicasts the video across the entire mesh network and all its segments by bridging-enabled root access points (RAPs) and mesh access points (MAPs).	Forwards the multicast video received from the Ethernet by a MAP to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-LWAPP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP-to-MAP multicasts do not occur because they are filtered out	Configures the RAP and MAP to multicast, but each in a different manner: If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP Ethernet networks, and the MAP-to-MAP packets are filtered out of the multicast. If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. See the Usage Guidelines section for more information.
Command Default	In-out mode		
Command History	Release	Modification	
	7.6	This command was introduced in a release earlier than Release 7.6.	

Usage Guidelines

Multicast for mesh networks cannot be enabled using the controller GUI.

Mesh multicast modes determine how bridging-enabled access points mesh access points (MAPs) and root access points (RAPs) send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-LWAPP multicast traffic only. LWAPP multicast traffic is governed by a different mechanism.

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

When using in-out mode, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.



Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (by using the **config network multicast global** command). If multicast does not need to extend to 802.11b clients beyond the mesh network, you should disable the global multicast parameter.

The following example shows how to multicast video across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs:

```
(Cisco Controller) >config mesh multicast regular
```

config mesh parent preferred

To configure a preferred parent for a mesh access point, use the **config mesh parent preferred** command.

```
config mesh parent preferred cisco_ap {mac_address | none}
```

Syntax Description

<i>cisco_ap</i>	Name of the child access point.
<i>mac_address</i>	MAC address of the preferred parent.
none	Clears the configured parent.

Command Default

None

Command History

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

Usage Guidelines

A child AP selects the preferred parent based on the following conditions:

- The preferred parent is the best parent.
- The preferred parent has a link SNR of at least 20 dB (other parents, however good, are ignored).
- The preferred parent has a link SNR in the range of 12 dB and 20 dB, but no other parent is significantly better (that is, the SNR is more than 20 percent better). For an SNR lower than 12 dB, the configuration is ignored.
- The preferred parent is not in a blocked list.
- The preferred parent is not in silent mode because of dynamic frequency selection (DFS).
- The preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child joins the parent AP using the default BGN.

The following example shows how to configure a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1:

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60
```

The following example shows how to clear a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1, by using the keyword none:

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60 none
```

config mesh public-safety

To enable or disable the 4.9-GHz public safety band for mesh access points, use the **config mesh public-safety** command.

config mesh public-safety {**enable** | **disable**} {**all** | *cisco_ap*}

Syntax Description

enable	Enables the 4.9-GHz public safety band.
disable	Disables the 4.9-GHz public safety band.
all	Applies the command to all mesh access points.
<i>cisco_ap</i>	Specific mesh access point.

Command Default

The 4.9-GHz public safety band is disabled.

Command History

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

Usage Guidelines

4.9 GHz is a licensed frequency band restricted to public-safety personnel.

The following example shows how to enable the 4.9-GHz public safety band for all mesh access points:

```
(Cisco Controller) >config mesh public-safety enable all
4.9GHz is a licensed frequency band in -A domain for public-safety usage
Are you sure you want to continue? (y/N) y
```

config mesh radius-server

To enable or disable external authentication for mesh access points, use the **config mesh radius-server** command.

config mesh radius-server *index* { **enable** | **disable** }

Syntax Description	<i>index</i>	RADIUS authentication method. Options are as follows:
		<ul style="list-style-type: none"> Enter eap to designate Extensible Authentication Protocol (EAP) for the mesh RADIUS server setting. Enter psk to designate Preshared Keys (PSKs) for the mesh RADIUS server setting.
	enable	Enables the external authentication for mesh access points.
	disable	Disables the external authentication for mesh access points.
Command Default	EAP is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable external authentication for mesh access points:

```
(Cisco Controller) >config mesh radius-server eap enable
```

config mesh range

To globally set the maximum range between outdoor root access points (RAPs) and mesh access points (MAPs), use the **config mesh range** command.

config mesh range [*distance*]

Syntax Description	<i>distance</i>	(Optional) Maximum operating range (150 to 132000 ft) of the mesh access point.
Command Default	12,000 feet.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	After this command is enabled, all outdoor mesh access points reboot. This command does not affect indoor access points.	

The following example shows how to set the range between an outdoor mesh RAP and a MAP:

```
(Cisco Controller) >config mesh range 300
Command not applicable for indoor mesh. All outdoor Mesh APs will be rebooted
Are you sure you want to start? (y/N) y
```

config mesh secondary-backhaul

To configure a secondary backhaul on the mesh network, use the **config mesh secondary-backhaul** command.

```
config mesh secondary-backhaul { enable [force-same-secondary-channel] | disable [rll-retransmit
| rll-transmit] }
```

Syntax Description	enable	force-same-secondary-channel	disable	rll-transmit	rll-retransmit
	Enables the secondary backhaul configuration.	(Optional) Enables secondary-backhaul mesh capability. Forces all access points rooted at the first hop node to have the same secondary channel and ignores the automatic or manual channel assignments for the mesh access points (MAPs) at the second hop and beyond.	Specifies the secondary backhaul configuration is disabled.	(Optional) Uses reliable link layer (RLL) at the second hop and beyond.	(Optional) Extends the number of RLL retry attempts in an effort to improve reliability.

Command Default None

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

Usage Guidelines This command uses a secondary backhaul radio as a temporary path for traffic that cannot be sent on the primary backhaul due to intermittent interference.

The following example shows how to enable a secondary backhaul radio and force all access points rooted at the first hop node to have the same secondary channel:

```
(Cisco Controller) >config mesh secondary-backhaul enable force-same-secondary-channel
```

config mesh security

To configure the security settings for mesh networks, use the **config mesh security** command.

config mesh security {{**rad-mac-filter** | **force-ext-auth** } {**enable** | **disable**}} | {{**eap** | **psk provisioning** | **provisioning window**} | {**enable** | **disable**}} | {**delete_psk** | **key**}

Syntax Description

rad-mac-filter	Enables a Remote Authentication Dial-In User Service (RADIUS) MAC address filter for the mesh security setting.
force-ext-auth	Disables forced external authentication for the mesh security setting.
lsc-only-auth	Enables Locally Significant Certificate only authentication for the mesh security setting.
enable	Enables the mesh security setting.
disable	Disables the mesh security setting.
eap	Designates the Extensible Authentication Protocol (EAP) for the mesh security setting by default.
psk	Designates a preshared key(PSK) for the mesh security setting.
provisioning	Encrypts provisioning for the PSK in Cisco Wireless Controller (WLC).
provisioning window	Encrypts provisioning window for the PSK in Cisco WLC.
enable	Enables provisioning of the PSK.
disable	Disables provisioning of the PSK.
key	Specifies the key for the PSK.

Command Default

The EAP is designated as default for the mesh security.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2	This command was modified, the psk provisioning and psk provisioning keywords are added.

The following example shows how to configure EAP as the security option for all mesh access points:

```
(Cisco Controller) config mesh security eap
```

The following example shows how to configure PSK as the security option for all mesh access points:

```
(Cisco Controller) config mesh security psk
```

The following example shows how to enable PSK provisioning as the security option for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning enable
```

The following example shows how to configure a PSK provisioning key as the security option for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning key 5
```

The following example shows how to enable a PSK provisioning window as the security option for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning window enable
```

The following example shows how to delete the PSK provisioning for Cisco WLC :

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc
```

The following example shows how to delete the PSK provisioning for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning delete_psk ap
```

The following example shows how to delete PSK provisioning for all configurations in Cisco WLC :

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc all
```

config mesh slot-bias

To enable or disable slot bias for serial backhaul mesh access points, use the **config mesh slot-bias** command.

config mesh slot-bias { **enable** | **disable** }

Syntax Description

enable	Enables slot bias for serial backhaul mesh APs.
disable	Disables slot bias for serial backhaul mesh APs.

Command Default

By default, slot bias is in enabled state.

Command History

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

Usage Guidelines

Follow these guidelines when using this command:

- The **config mesh slot-bias** command is a global command and therefore applicable to all 1524SB APs associated with the same controller.
- Slot bias is applicable only when both slot 1 and slot 2 are available. If a slot radio does not have a channel that is available because of dynamic frequency selection (DFS), the other slot takes up both the uplink and downlink roles.
- If slot 2 is not available because of hardware issues, slot bias functions normally. Corrective action should be taken by disabling the slot bias or fixing the antenna.

The following example shows how to disable slot bias for serial backhaul mesh APs:

```
(Cisco Controller) >config mesh slot-bias disable
```

config mgmtuser add

To add a local management user to the controller, use the **config mgmtuser add** command.

```
config mgmtuser add username password {lobby-admin | read-write | read-only} [description]
```

Syntax Description		
<i>username</i>		Account username. The username can be up to 24 alphanumeric characters.
<i>password</i>		Account password. The password can be up to 24 alphanumeric characters.
read-write		Creates a management user with read-write access.
read-only		Creates a management user with read-only access.
<i>description</i>		(Optional) Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default None

Command History

Release Modification

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

The following example shows how to create a management user account with read-write access.

```
(Cisco Controller) > config mgmtuser add admin admin read-write "Main account"
```

Related Commands

show mgmtuser

config mgmtuser delete

To delete a management user from the controller, use the **config mgmtuser delete** command.

config mgmtuser delete *username*

Syntax Description	<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.
---------------------------	-----------------	-------------------------------------------------------------------------

Command Default	The management user is not deleted by default.	
------------------------	------------------------------------------------	--

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

The following example shows how to delete a management user account admin from the controller.

```
(Cisco Controller) > config mgmtuser delete admin
```

```
Deleted user admin
```

Related Commands	show mgmtuser
-------------------------	----------------------

config mgmtuser description

To add a description to an existing management user login to the controller, use the **config mgmtuser description** command.

config mgmtuser description *username description*

Syntax Description		
	<i>username</i>	Account username. The username can be up to 24 alphanumeric characters.
	<i>description</i>	Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default No description is added to the management user.

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

The following example shows how to add a description “primary-user” to the management user “admin”:

```
(Cisco Controller) > config mgmtuser description admin "primary-user"
```

Related Commands	
	config mgmtuser add
	config mgmtuser delete
	config mgmtuser password
	show mgmtuser

config mgmtuser password

To configure a management user password, use the **config mgmtuser password** command.

config mgmtuser password *username password*

Syntax Description		
<i>username</i>		Account username. The username can be up to 24 alphanumeric characters.
<i>password</i>		Account password. The password can be up to 24 alphanumeric characters.

Command Default None

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

The following example shows how to change the password of the management user “admin” with the new password 5rTfm:

```
(Cisco Controller) > config mgmtuser password admin 5rTfm
```

Related Commands `show mgmtuser`

config mgmtuser telnet

To enable local management users to use Telnet to connect to the Cisco Wireless LAN Controller, use the **config mgmtuser telnet** command.

```
config mgmtuser telnet user_name {enable | disable}
```

Syntax Description

user_name Username of a local management user.

enable Enables a local management user to use Telnet to connect to the Cisco WLC. You can enter up to 24 alphanumeric characters.

disable Disables a local management user from using Telnet to connect to the Cisco WLC.

Command Default

Local management users can use Telnet to connect to the Cisco WLC.

Command History

Release Modification

7.5 This command was introduced.

Usage Guidelines

You must enable global Telnet to enable this command. Secure Shell (SSH) connection is not affected when you enable this option.

The following example shows how to enable a local management user to use Telnet to connect to the Cisco WLC:

```
(Cisco Controller) > config mgmtuser telnet admin1 enable
```

config mobility dscp

To configure the mobility intercontroller DSCP value, use the **config mobility dscp** command.

config mobility dscp *dscp_value*

Syntax Description	<i>dscp_value</i>	DSCP value ranging from 0 to 63.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the mobility intercontroller DSCP value to 40:

```
(Cisco Controller) >config mobility dscp 40
```

config mobility group anchor

To create a new mobility anchor for the WLAN or wired guest LAN, enter, use the **config mobility group anchor** command.

```
config mobility group anchor { add | delete } { wlan wlan_id | guest-lan guest_lan_id } anchor_ip
```

Syntax Description	Parameter	Description
	add	Adds or changes a mobility anchor to a wireless LAN.
	delete	Deletes a mobility anchor from a wireless LAN.
	wlan	Specifies the wireless LAN anchor settings.
	<i>wlan_id</i>	Wireless LAN identifier between 1 and 512 (inclusive).
	guest-lan	Specifies the guest LAN anchor settings.
	<i>guest_lan_id</i>	Guest LAN identifier between 1 and 5 (inclusive).
	<i>anchor_ip</i>	IP address of the anchor controller.

Command Default None

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

Usage Guidelines The *wlan_id* or *guest_lan_id* must exist and be disabled.

Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor. Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

The following example shows how to add a mobility anchor with the IP address 192.12.1.5 to a wireless LAN ID 2:

```
(Cisco Controller) >config mobility group anchor add wlan 2 192.12.1.5
```

The following example shows how to delete a mobility anchor with the IP address 193.13.1.15 from a wireless LAN:

```
(Cisco Controller) >config mobility group anchor delete wlan 5 193.13.1.15
```

config mobility group domain

To configure the mobility domain name, use the **config mobility group domain** command.

config mobility group domain *domain_name*

Syntax Description	<i>domain_name</i>	Domain name. The domain name can be up to 31 case-sensitive characters.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a mobility domain name lab1:

```
(Cisco Controller) >config mobility group domain lab1
```

config mobility group keepalive count

To configure the Cisco WLC to detect failed mobility group members (including anchor Cisco WLCs), use the **config mobility group keepalive count** command.

config mobility group keepalive count *count*

Syntax Description	<i>count</i>	Number of times that a ping request is sent to a mobility group member before the member is considered unreachable. The range is from 3 to 20. The default is 3.
Command Default	The default number of times that a ping request is sent to a mobility group member is 3.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the number of times a ping request is sent to a mobility group member before the member is considered unreachable to three counts:

```
(Cisco Controller) >config mobility group keepalive count 3
```

config mobility group keepalive interval

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive** command.

config mobility group keepalive *interval*

Syntax Description	<i>interval</i>	Interval of time between each ping request sent to a mobility group member. The range is from 1 to 30 seconds. The default value is 10 seconds.
Command Default	The default interval of time between each ping request is 10 seconds.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:

```
(Cisco Controller) >config mobility group keepalive 10
```

config mobility group member

To add or delete users from the mobility group member list, use the **config mobility group member** command.

```
config mobility group member {add MAC-addr IP-addr [group_name] [encrypt{enable | disable} | [data-dtls mac-addr {enable | disable} | delete MAC-addr | hash IP-addr {key | none}}
```

Syntax Description		
add		Adds or changes a mobility group member to the list.
<i>MAC-addr</i>		Member switch MAC address.
<i>IP-addr</i>		Member switch IP address.
<i>group_name</i>		(Optional) Member switch group name (if different from the default group name).
delete		(Optional) Deletes a mobility group member from the list.
hash		Configures the hash key for authorization. You can configure the hash key only if the member is a virtual controller in the same domain.
<i>key</i>		Hash key of the virtual controller. For example, a819d479dcfeb3e0974421b6e8335582263d9169
none		Clears the previous hash key of the virtual controller.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports both IPv4 and IPv6 address formats.
	8.8.111.0	This command was updated by adding encrypt , data-dtls keywords to support IRCM functionality.

The following example shows how to add a mobility group member with an IPv4 address to the list:

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 209.165.200.225
```

The following example shows how to add a mobility group member with an IPv6 address to the list:

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 2001:DB8::1
```

The following example shows how to configure the hash key of a virtual controller in the same domain:



Note The IP address in this example can be in either IPv4 or IPv6 format.

```
(Cisco Controller) >config mobility group member hash 209.165.201.1  
a819d479dcfeb3e0974421b6e8335582263d9169
```

config mobility group multicast-address

To configure the multicast group IP address for nonlocal groups within the mobility list, use the **config mobility group multicast-address** command.

config mobility group multicast-address *group_name* *ip_address*

Syntax Description	<i>group_name</i>	Member switch group name (if different from the default group name).
	<i>ip_address</i>	Member switch IP address.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the multicast group IP address 10.10.10.1 for a group named test:

```
(Cisco Controller) >config mobility group multicast-address test 10.10.10.1
```

The following example shows how to configure the multicast group IP address 2001:DB8::1 for a group named test:

```
(Cisco Controller) >config mobility group multicast-address test 2001:DB8::1
```

config mobility multicast-mode

To enable or disable mobility multicast mode, use the **config mobility multicast-mode** command.

```
config mobility multicast-mode { enable | disable } local_group_multicast_address
```

Syntax Description		
enable		Enables the multicast mode; the controller uses to send Mobile Announce messages to the local
disable		Disables the multicast mode; the controller uses to send the Mobile Announce messages to the local
<i>local_group_multicast_address</i>		IP address for the local mobility group.

Command Default The mobility multicast mode is disabled.

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

The following example shows how to enable the multicast mobility mode for the local mobility group IP address 157.168.20.0:

```
(Cisco Controller) >config mobility multicast-mode enable 157.168.20.0
```

config mobility new-architecture

To enable new mobility on the Cisco Wireless LAN Controller (WLC), use the **config mobility new-architecture** command.

```
config mobility new-architecture {enable | disable}
```

Syntax Description

enable Configures the Cisco WLC to switch to the new mobility architecture.

disable Configures the Cisco WLC to switch to the old flat mobility architecture.

Command Default

By default, new mobility is disabled.

Command History

Release Modification

7.3.112.0 This command was introduced.

Usage Guidelines

New mobility is supported only on Cisco WiSM2, Cisco 2500 Series Wireless Controllers, Cisco 5500 Series Wireless Controllers, and Cisco 8500 Series Wireless Controllers. New mobility enables the Cisco WLC to be compatible with Converged Access controllers with Wireless Control Module (WCM), such as Cisco Catalyst 3850 Series and the Cisco 5760 Wireless LAN Controllers.

The following example shows how to enable new mobility on the Cisco WLC:

```
(Cisco Controller) >config mobility new-architecture enable
```

config mobility oracle

To configure the Mobility Oracle (MO), use the **config mobility oracle** command.

```
config mobility oracle { enable | disable | ip ip_address }
```

Syntax Description

enable	Enables the MO on startup.
disable	Disables the MO on startup.
ip	Specifies the IP address of the MO.
<i>ip_address</i>	IP address of the MO.

Command Default

None

Command History

Release	Modification
7.3.112.0	This command was introduced.
8.0	This command supports only IPv4 address format.

Usage Guidelines

The MO maintains the client database under one complete mobility domain. It consists of a station database, an interface to the mobility Cisco WLC, and an NTP server. There can be only one MO in the entire mobility domain.

The IPv6 address format for this command is not supported.

The following example shows how to configure the MO IP address:

```
(Cisco Controller) >config mobility oracle ip 27.0.0.1
```

config mobility switchPeerGroup

To configure a switch peer group (SPG) on the controller, use the **config mobility switchPeerGroup** command.

```
config mobility switchPeerGroup { bridge-domain-id peer-group-name bridge domain id | create
peer-group-name | delete peer-group-name | member { add | delete } IP_address [public_IP_address]
peer-group-name | multicast-address peer-group-name multicast_IP_address }
```

Syntax Description	Parameter	Description
	bridge-domain-id	Configures the bridge domain ID of the SPG.
	<i>peer-group-name</i>	Name of the SPG.
	<i>bridge domain id</i>	Bridge domain ID of the SPG.
	create	Creates an SPG.
	delete	Deletes an SPG.
	member	Configures a member switch for an SPG.
	add	Adds a member switch into an SPG.
	<i>IP_address</i>	IP address of the member switch.
	<i>public_IP_address</i>	(Optional) Public IP address of the SPG member.
	multicast-address	Configures the multicast address of the SPG.
	<i>multicast_IP_address</i>	Multicast address of the SPG.

Command Default None

Command History	Release	Modification
	7.3.112.0	This command was introduced.
	8.0	This command supports only IPv4 address format.

Usage Guidelines The IPv6 address format for this command is not supported.

The following example shows how to create an SPG.

```
(Cisco Controller) >config mobility switchPeerGroup create SPG1
```

config mobility secure-mode

To configure the secure mode for mobility messages between Cisco WLCs, use the **config mobility secure-mode** command.

config mobility secure-mode {enable | disable}

Syntax Description	enable	Enables the mobility group message security.
	disable	Disables mobility group message security.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the secure mode for mobility messages:

```
(Cisco Controller) >config mobility secure-mode enable
```

config mobility statistics reset

To reset the mobility statistics, use the **config mobility statistics reset** command.

config mobility statistics reset

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

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

This example shows how to reset the mobility group statistics:

```
(Cisco Controller) >config mobility statistics reset
```

config netuser add

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

config netuser add *username password* { **wlan** *wlan_id* | **guestlan** *guestlan_id* } **userType** **guest** **lifetime** *lifetime* **description** *description*

Syntax Description

<i>username</i>	Guest username. The username can be up to 50 alphanumeric characters.
<i>password</i>	User password. The password can be up to 24 alphanumeric characters.
wlan	Specifies the wireless LAN identifier to associate with or zero for any wireless LAN.
<i>wlan_id</i>	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
guestlan	Specifies the guest LAN identifier to associate with or zero for any wireless LAN.
<i>guestlan_id</i>	Guest LAN ID.
userType	Specifies the user type.
guest	Specifies the guest for the guest user.
lifetime	Specifies the lifetime.
<i>lifetime</i>	Lifetime value (60 to 259200 or 0) in seconds for the guest user. Note A value of 0 indicates an unlimited lifetime.
<i>description</i>	Short description of user. The description can be up to 32 characters enclosed in double-quotes.

Command Default

None

Command History

Release Modification

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

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to add a permanent username Jane to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

The following example shows how to add a guest username George to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

Related Commands

show netuser

config netuser delete

config netuser delete

To delete an existing user from the local network, use the **config netuser delete** command.

```
config netuser delete { username username | wlan-id wlan-id }
```

Syntax Description		
	<i>username</i>	Network username. The username can be up to 24 alphanumeric characters.
	<i>wlan-id</i>	WLAN identification number.

Command Default None

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

Usage Guidelines Local network usernames must be unique because they are stored in the same database.



Note When a WLAN associated with network users is deleted, the system prompts to delete all network users associated with the WLAN first. After deleting the network users, you can delete the WLAN.

The following example shows how to delete an existing username named able1 from the network:

```
(Cisco Controller) > config netuser delete able1
Deleted user able1
```

Related Commands **show netuser**

config netuser description

To add a description to an existing net user, use the **config netuser description** command.

config netuser description *username description*

Syntax Description	<i>username</i>	Network username. The username can contain up to 24 alphanumeric characters.
	<i>description</i>	(Optional) User description. The description can be up to 32 alphanumeric characters enclosed in double quotes.

Command Default None

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

The following example shows how to add a user description “HQ1 Contact” to an existing network user named able 1:

```
(Cisco Controller) > config netuser description able1 "HQ1 Contact"
```

Related Commands `show netuser`

config netuser guest-lan-id

To configure a wired guest LAN ID for a network user, use the **config netuser guest-lan-id** command.

config netuser guest-lan-id *username lan_id*

Syntax Description		
	<i>username</i>	Network username. The username can be 24 alphanumeric characters.
	<i>lan_id</i>	Wired guest LAN identifier to associate with the user. A zero value associates the user with any wired LAN.

Command Default None

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

The following example shows how to configure a wired LAN ID 2 to associate with the user named aire1:

```
(Cisco Controller) > config netuser guest-lan-id aire1 2
```

Related Commands

- show netuser
- show wlan summary

config netuser guest-role apply

To apply a quality of service (QoS) role to a guest user, use the **config netuser guest-role apply** command.

config netuser guest-role apply *username role_name*

Syntax Description

username Name of the user.

role_name QoS guest role name.

Command Default

None

Command History

Release Modification

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

Usage Guidelines

If you do not assign a QoS role to a guest user, the Role field in the User Details shows the role as default. The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

If you want to unassign a QoS role from a guest user, use the **config netuser guest-role apply** *username default*. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

The following example shows how to apply a QoS role to a guest user jsmith with the QoS guest role named Contractor:

```
(Cisco Controller) > config netuser guest-role apply jsmith Contractor
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role create

To create a quality of service (QoS) role for a guest user, use the **config netuser guest-role create** command.

config netuser guest-role create *role_name*

Syntax Description	<i>role name</i> QoS guest role name.				
Command Default	None				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
Usage Guidelines	<p>To delete a QoS role, use the config netuser guest-role delete <i>role-name</i> .</p> <p>The following example shows how to create a QoS role for the guest user named guestuser1:</p> <pre>(Cisco Controller) > config netuser guest-role create guestuser1</pre>				
Related Commands	config netuser guest-role delete				

config netuser guest-role delete

To delete a quality of service (QoS) role for a guest user, use the **config netuser guest-role delete** command.

```
config netuser guest-role delete role_name
```

Syntax Description

<i>role name</i>	Quality of service (QoS) guest role name.
------------------	-------------------------------------------

Command Default

None

Command History

Release Modification

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

The following example shows how to delete a quality of service (QoS) role for guestuser1:

```
(Cisco Controller) > config netuser guest-role delete guestuser1
```

Related Commands

config netuser guest-role create

config netuser guest-role qos data-rate average-data-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-data-rate** command.

config netuser guest-role qos data-rate average-data-rate *role_name* *rate*

Syntax Description

<i>role_name</i>	Quality of service (QoS) guest role name.
<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default

None

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure an average rate for the QoS guest named guestuser1:

```
(Cisco Controller) > config netuser guest-role qos data-rate average-data-rate guestuser1
0
```

Related Commands

config netuser guest-role create
config netuser guest-role delete
config netuser guest-role qos data-rate burst-data-rate

config netuser guest-role qos data-rate average-realtime-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-realtime-rate** command.

config netuser guest-role qos data-rate average-realtime-rate *role_name rate*

Syntax Description	<i>role_name</i>	Quality of service (QoS) guest role name.
	<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default None

Usage Guidelines For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure an average data rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate average-realtime-rate guestuser1
0
```

Related Commands **config netuser guest-role**
config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

To configure the peak data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-data-rate** command.

config netuser guest-role qos data-rate burst-data-rate *role_name* *rate*

Syntax Description	<i>role_name</i>	Quality of service (QoS) guest role name.
	<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default None

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

Usage Guidelines

The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure the peak data rate for the QoS guest named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-data-rate guestuser1 0
```

Related Commands

- config netuser guest-role create**
- config netuser guest-role delete**
- config netuser guest-role qos data-rate average-data-rate**

config netuser guest-role qos data-rate burst-realtime-rate

To configure the burst real-time data rate for UDP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-realtime-rate** command.

config netuser guest-role qos data-rate burst-realtime-rate *role_name* *rate*

Syntax Description	<i>role_name</i>	Quality of service (QoS) guest role name.
	<i>rate</i>	Rate for TCP traffic on a per user basis.

Command Default None

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

Usage Guidelines

The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the quality of service (QoS) policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure a burst real-time rate for the QoS guest user named `guestuser1` with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-realtime-rate guestuser1
0
```

Related Commands

- config netuser guest-role**
- config netuser guest-role qos data-rate average-data-rate**
- config netuser guest-role qos data-rate burst-data-rate**

config netuser lifetime

To configure the lifetime for a guest network user, use the **config netuser lifetime** command.

config netuser lifetime *username time*

Syntax Description		
<i>username</i>		Network username. The username can be up to 50 alphanumeric characters.
<i>time</i>		Lifetime between 60 to 31536000 seconds or 0 for no limit.

Command Default None

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

The following example shows how to configure lifetime for a guest network user:

```
(Cisco Controller) > config netuser lifetime guestuser1 22450
```

Related Commands

- show netuser**
- show wlan summary**

config netuser maxUserLogin

To configure the maximum number of login sessions allowed for a network user, use the **config netuser maxUserLogin** command.

config netuser maxUserLogin *count*

Syntax Description	<i>count</i>	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.
---------------------------	--------------	-----------------------------------------------------------------------------------------------------

Command Default	By default, the maximum number of login sessions for a single user is 0 (unlimited).
------------------------	--------------------------------------------------------------------------------------

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

The following example shows how to configure the maximum number of login sessions for a single user to 8:

```
(Cisco Controller) > config netuser maxUserLogin 8
```

Related Commands	show netuser
-------------------------	---------------------

config netuser password

To change a local network user password, use the **config netuser password** command.

config netuser password *username password*

Syntax Description		
<i>username</i>		Network username. The username can be up to 24 alphanumeric characters.
<i>password</i>		Network user password. The password can contain up to 24 alphanumeric characters.

Command Default None

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

The following example shows how to change the network user password from aire1 to aire2:

```
(Cisco Controller) > config netuser password aire1 aire2
```

Related Commands **show netuser**

config netuser wlan-id

To configure a wireless LAN ID for a network user, use the **config netuser wlan-id** command.

```
config netuser wlan-id username wlan_id
```

Syntax Description	<i>username</i>	Network username. The username can be 24 alphanumeric characters.
	<i>wlan_id</i>	Wireless LAN identifier to associate with the user. A zero value associates the user with any wireless LAN.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure a wireless LAN ID 2 to associate with the user named aire1:

```
(Cisco Controller) > config netuser wlan-id aire1 2
```

Related Commands	show netuser
	show wlan summary

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description	<i>shared_secret</i> Bridging shared secret string. The string can contain up to 10 bytes.				
Command Default	The bridging shared secret is enabled by default.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
Usage Guidelines	<p>This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.</p> <p>The zero-touch configuration must be enabled for this command to work.</p> <p>The following example shows how to configure the bridging shared secret string “shhh1”:</p> <pre>(Cisco Controller) > config network bridging-shared-secret shhh1</pre>				
Related Commands	show network summary				

config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

```
config network web-auth captive-bypass {enable | disable}
```

Syntax Description	enable	Allows the controller to support bypass of captive portals.
	disable	Disallows the controller to support bypass of captive portals.

Command Default None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

Related Commands

- show network summary**
- config network web-auth cmcc-support**

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description	<i>port</i>	Port number. The valid range is from 0 to 65535.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

Related Commands **show network summary**

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect { **enable** | **disable** }

Syntax Description	enable	Allows proxy redirect support for web authentication clients.
	disable	Disallows proxy redirect support for web authentication clients.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands **show network summary**

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb {enable | disable}

Syntax Description	enable	Allows secure web (https) authentication for clients.
	disable	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.
Command Default	The default secure web (https) authentication for clients is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>If you configure the secure web (https) authentication for clients using the config network web-auth secureweb disable command, then you must reboot the Cisco WLC to implement the change.</p> <p>The following example shows how to enable the secure web (https) authentication for clients:</p> <pre>(Cisco Controller) > config network web-auth secureweb enable</pre>	
Related Commands	show network summary	

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

```
config network webmode {enable | disable}
```

Syntax Description	enable	Disables the web interface.
	disable	Enables the web interface.

Command Default The default value for the web mode is **enable**.

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

The following example shows how to disable the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

Related Commands `show network summary`

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

```
config network web-auth {port port-number} | {proxy-redirect {enable | disable}}
```

Syntax Description

port	Configures additional ports for web authentication redirection.
<i>port-number</i>	Port number (between 0 and 65535).
proxy-redirect	Configures proxy redirect support for web authentication clients.
enable	Enables proxy redirect support for web authentication clients. Note Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
disable	Disables proxy redirect support for web authentication clients.

Command Default

The default network-level web authentication value is disabled.

Command History

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

Usage Guidelines

You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary
show run-config
config qos protocol-type

config network 802.3-bridging

To enable or disable 802.3 bridging on a controller, use the **config network 802.3-bridging** command.

```
config network 802.3-bridging {enable | disable}
```

Syntax Description

enable Enables the 802.3 bridging.

disable Disables the 802.3 bridging.

Command Default

By default, 802.3 bridging on the controller is disabled.

Command History

Release Modification

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

Usage Guidelines

In controller software release 5.2, the software-based forwarding architecture for Cisco 2100 Series Controllers is being replaced with a new forwarding plane architecture. As a result, Cisco 2100 Series Controllers and the Cisco wireless LAN controller Network Module for Cisco Integrated Services Routers bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

To determine the status of 802.3 bridging, enter the **show netuser guest-roles** command.

The following example shows how to enable the 802.3 bridging:

```
(Cisco Controller) > config network 802.3-bridging enable
```

Related Commands

show netuser guest-roles

show network

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

```
config network allow-old-bridge-aps {enable | disable}
```

Syntax Description	enable	Disables the switch association.
	enable	Enables the switch association.
	disable	Disables the switch association.

Command Default Switch association is enabled.

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

The following example shows how to configure an old bridge access point to associate with the switch:

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

```
config network ap-discovery nat-ip-only { enable | disable }
```

Syntax Description

enable	Enables use of NAT IP only in discovery response.
disable	Enables use of both NAT IP and non NAT IP in discovery response.

Command Default

The use of NAT IP only in discovery response is enabled.

Command History

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

Usage Guidelines

- If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.
- If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.
- If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.
- If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

The following example shows how to enable NAT IP in an AP discovery response:

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback { **enable** | **disable** }

Syntax Description	enable	enable
		Enables the Cisco lightweight access point fallback.
	disable	Disables the Cisco lightweight access point fallback.
Command Default	The Cisco lightweight access point fallback is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Cisco lightweight access point fallback:

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {enable | disable}

Syntax Description	enable	Disables the lightweight access point priority reauthentication.
	disable	Enables the lightweight access point priority reauthentication.

Command Default	The lightweight access point priority reauthentication is disabled.	
-----------------	---------------------------------------------------------------------	--

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

The following example shows how to enable the lightweight access point priority reauthorization:

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

```
config network apple-talk {enable | disable}
```

Syntax Description

enable	Enables the AppleTalk bridging.
disable	Disables the AppleTalk bridging.

Command Default

None

Command History

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

The following example shows how to configure AppleTalk bridging:

```
(Cisco Controller) > config network apple-talk enable
```

config network arptimeout

To set the Address Resolution Protocol (ARP) entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description	<i>seconds</i>	Timeout in seconds. The minimum value is 10 seconds. The default value is 300 seconds.
---------------------------	----------------	----------------------------------------------------------------------------------------

Command Default	The default ARP entry timeout value is 300 seconds.
------------------------	-----------------------------------------------------

Command History	Release Modification
------------------------	-----------------------------

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

This example shows how to set the ARP entry timeout value to 240 seconds:

```
(Cisco Controller) > config network arptimeout 240
```

Related Commands	show network summary
-------------------------	-----------------------------

config assisted-roaming

To configure assisted roaming parameters on the controller, use the **config assisted-roaming** command.

```
config assisted-roaming { denial-maximum count | floor-bias RSSI | prediction-minimum
number_of_APs }
```

Syntax Description	Parameter	Description
	denial-maximum	Configures the maximum number of counts for association denial.
	<i>count</i>	Maximum number of times that a client is denied for association when the association request that was sent to an access point does not match any access point on the prediction list. The range is from 1 to 10.
	floor-bias	Configures the RSSI bias for access points on the same floor.
	<i>RSSI</i>	RSSI bias for access points on the same floor. The range is from 5 to 25. Access points on the same floor have more preference.
	prediction-minimum	Configures the minimum number of optimized access points for the assisted roaming feature.
	<i>number_of_APs</i>	Minimum number of optimized access points for the assisted roaming feature. The range is from 1 to 6. If the number of access points in the prediction assigned to the client is smaller than this number, the assisted roaming feature does not work.

Command Default The default RSSI bias for access points on the same floor is 15 dBm.

Usage Guidelines 802.11k allows a client to request a neighbor report that contains information about known neighbor access points, which can be used for a service set transition. The neighbor list reduces the need for active and passive scanning.

This example shows how to configure the minimum number of optimized access points for the assisted roaming feature:

```
(Cisco Controller) >config assisted-roaming prediction-minimum 4
```

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

```
config network allow-old-bridge-aps {enable | disable}
```

Syntax Description	enable	Enables the switch association.
	disable	Disables the switch association.

Command Default Switch association is enabled.

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

The following example shows how to configure an old bridge access point to associate with the switch:

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

```
config network ap-discovery nat-ip-only {enable | disable}
```

Syntax Description	enable	Enables use of NAT IP only in discovery response.
	disable	Enables use of both NAT IP and non NAT IP in discovery response.
Command Default	The use of NAT IP only in discovery response is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

- If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.
- If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.
- If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.
- If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

The following example shows how to enable NAT IP in an AP discovery response:

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

```
config network ap-fallback {enable | disable}
```

Syntax Description	enable	Enables the Cisco lightweight access point fallback.
	disable	Disables the Cisco lightweight access point fallback.
Command Default	The Cisco lightweight access point fallback is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Cisco lightweight access point fallback:

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {enable | disable}

Syntax Description	enable	Disables the lightweight access point priority reauthentication.
	disable	Enables the lightweight access point priority reauthentication.
Command Default	The lightweight access point priority reauthentication is disabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the lightweight access point priority reauthorization:

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

```
config network apple-talk {enable | disable}
```

Syntax Description	enable	Enables the AppleTalk bridging.
	disable	Disables the AppleTalk bridging.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure AppleTalk bridging:

```
(Cisco Controller) > config network apple-talk enable
```

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

```
config network bridging-shared-secret shared_secret
```

Syntax Description	<i>shared_secret</i> Bridging shared secret string. The string can contain up to 10 bytes.				
Command Default	The bridging shared secret is enabled by default.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
Usage Guidelines	<p>This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.</p> <p>The zero-touch configuration must be enabled for this command to work.</p> <p>The following example shows how to configure the bridging shared secret string “shhh1”:</p> <pre>(Cisco Controller) > config network bridging-shared-secret shhh1</pre>				
Related Commands	show network summary				

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

```
config network bridging-shared-secret shared_secret
```

Syntax Description	<i>shared_secret</i> Bridging shared secret string. The string can contain up to 10 bytes.
Command Default	The bridging shared secret is enabled by default.
Command History	Release Modification 7.6 This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.</p> <p>The zero-touch configuration must be enabled for this command to work.</p> <p>The following example shows how to configure the bridging shared secret string “shhh1”:</p> <pre>(Cisco Controller) > config network bridging-shared-secret shhh1</pre>
Related Commands	show network summary

config network broadcast

To enable or disable broadcast packet forwarding, use the **config network broadcast** command.

config network broadcast {**enable** | **disable**}

Syntax Description

enable Enables the broadcast packet forwarding.

disable Disables the broadcast packet forwarding.

Command Default

The broadcast packet forwarding is disabled by default.

Command History

Release Modification

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

Usage Guidelines

This command allows you to enable or disable broadcasting. You must enable multicast mode before enabling broadcast forwarding. Use the **config network multicast mode command** to configure multicast mode on the controller.



Note The default multicast mode is unicast in case of all controllers except for Cisco 2106 Controllers. The broadcast packets and multicast packets can be independently controlled. If multicast is off and broadcast is on, broadcast packets still reach the access points, based on the configured multicast mode.

The following example shows how to enable broadcast packet forwarding:

```
(Cisco Controller) > config network broadcast enable
```

Related Commands

show network summary

config network multicast global

config network multicast mode

config network fast-ssid-change

To enable or disable fast Service Set Identifier (SSID) changing for mobile stations, use the **config network fast-ssid-change** command.

```
config network fast-ssid-change { enable | disable }
```

Syntax Description	enable	enable
		Enables the fast SSID changing for mobile stations
	disable	Disables the fast SSID changing for mobile stations.

Command Default None

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

Usage Guidelines When you enable the Fast SSID Change feature, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

When you disable the FastSSID Change feature, the controller enforces a delay before clients are allowed to move to a new SSID.

The following example shows how to enable the fast SSID changing for mobile stations:

```
(Cisco Controller) > config network fast-ssid-change enable
```

Related Commands show network summary

config network ip-mac-binding

To validate the source IP address and MAC address binding within client packets, use the **config network ip-mac-binding** command.

```
config network ip-network-binding {enable | disable}
```

Syntax Description	enable	Enables the validation of the source IP address to MAC address binding in clients packets.
	disable	Disables the validation of the source IP address to MAC address binding in clients packets.
Command Default	The validation of the source IP address to MAC address binding in clients packets is enabled by default.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

In controller software release 5.2, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.



Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

The following example shows how to validate the source IP and MAC address within client packets:

```
(Cisco Controller) > config network ip-mac-binding enable
```

config network link local bridging

To configure bridging of link local traffic at the local site, use the **config network link-local-bridging** command.

```
config network link-local-bridging {enable | disable}
```

Syntax Description	enable Enables bridging of link local traffic at the local site
	disable Disables bridging of link local traffic at the local site
Command Default	Disabled
Command History	Release Modification
	8.0 This command was introduced

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default primary, use the **config network master-base** command.

config network master-base {enable | disable}

Syntax Description	enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.
	disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	This setting is only used upon network installation and should be disabled after the initial network configuration. Because the primary Cisco wireless LAN controller is normally not used in a deployed network, the primary Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.	
	The following example shows how to enable the Cisco wireless LAN controller as a default primary:	

```
(Cisco Controller) > config network master-base enable
```

config network mgmt-via-wireless

To enable Cisco wireless LAN controller management from an associated wireless client, use the **config network mgmt-via-wireless** command.

```
config network mgmt-via-wireless {enable | disable}
```

Syntax Description	enable	Enables the switch management from a wireless interface.
	disable	Disables the switch management from a wireless interface.
Command Default	The switch management from a wireless interface is disabled by default.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	This feature allows wireless clients to manage only the Cisco wireless LAN controller associated with the client and the associated Cisco lightweight access point. That is, clients cannot manage another Cisco wireless LAN controller with which they are not associated.	
	This example shows how to configure switch management from a wireless interface:	
	<code>(Cisco Controller) > config network mgmt-via-wireless enable</code>	
Related Commands	<code>show network summary</code>	

config network multicast global

To enable or disable multicasting on the controller, use the **config network multicast global** command.

```
config network multicast global { enable | disable }
```

Syntax Description

enable	Enables the multicast global support.
disable	Disables the multicast global support.

Command Default

Multicasting on the controller is disabled by default.

Command History

Release Modification

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

Usage Guidelines

The **config network broadcast {enable | disable}** command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode configured on the controller (by using the **config network multicast mode command**) to operate.

The following example shows how to enable the global multicast support:

```
(Cisco Controller) > config network multicast global enable
```

Related Commands

- show network summary**
- config network broadcast**
- config network multicast mode**

config network multicast igmp query interval

To configure the IGMP query interval, use the **config network multicast igmp query interval** command.

config network multicast igmp query interval *value*

Syntax Description	<i>value</i>	Frequency at which controller sends IGMP query messages. The range is from 15 to 2400 seconds.
---------------------------	--------------	------------------------------------------------------------------------------------------------

Command Default	The default IGMP query interval is 20 seconds.
------------------------	------------------------------------------------

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

Usage Guidelines	To configure IGMP query interval, ensure that you do the following: <ul style="list-style-type: none">• Enable the global multicast by entering the config network multicast global enable command.• Enable IGMP snooping by entering the config network multicast igmp snooping enable command.
-------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The following example shows how to configure the IGMP query interval at 20 seconds:

```
(Cisco Controller) > config network multicast igmp query interval 20
```

Related Commands	config network multicast global config network multicast igmp snooping config network multicast igmp timeout
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------

config network multicast igmp snooping

To enable or disable IGMP snooping, use the **config network multicast igmp snooping** command.

```
config network multicast igmp snooping { enable | disable }
```

Syntax Description

enable	Enables IGMP snooping.
disable	Disables IGMP snooping.

Command Default

None

Command History

Release Modification

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

The following example shows how to enable internet IGMP snooping settings:

```
(Cisco Controller) > config network multicast igmp snooping enable
```

Related Commands

config network multicast global
config network multicast igmp query interval
config network multicast igmp timeout

config network multicast igmp timeout

To set the IGMP timeout value, use the **config network multicast igmp timeout** command.

config network multicast igmp timeout *value*

Syntax Description	<i>value</i> Timeout range from 30 to 7200 seconds.				
Command Default	None				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
Usage Guidelines	<p>You can enter a timeout value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of timeout/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.</p> <p>The following example shows how to configure the timeout value 50 for IGMP network settings:</p> <pre>(Cisco Controller) > config network multicast igmp timeout 50</pre>				
Related Commands	<p>config network multicast global</p> <p>config network igmp snooping</p> <p>config network multicast igmp query interval</p>				

config network multicast l2mcast

To configure the Layer 2 multicast on an interface or all interfaces, use the **config network multicast l2mcast** command.

```
config network multicast l2mcast { enable | disable { all | interface-name }
```

Syntax Description

enable	Enables Layer 2 multicast.
disable	Disables Layer 2 multicast.
all	Applies to all interfaces.
<i>interface-name</i>	Interface name for which the Layer 2 multicast is to enabled or disabled.

Command Default

None

Command History

Release Modification

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

The following example shows how to enable Layer 2 multicast for all interfaces:

```
(Cisco Controller) > config network multicast l2mcast enable all
```

Related Commands

config network multicast global
config network multicast igmp snooping
config network multicast igmp query interval
config network multicast mld

config network multicast mld

To configure the Multicast Listener Discovery (MLD) parameters, use the **config network multicast mld** command.

```
config network multicast mld { query interval interval-value | snooping { enable | disable } | timeout timeout-value }
```

Syntax Description		
query interval		Configures query interval to send MLD query messages.
<i>interval-value</i>		Query interval in seconds. The range is from 30 to 300.
snooping		Configures MLD snooping.
enable		Enables MLD snooping.
disable		Disables MLD snooping.
timeout		Configures MLD timeout.
<i>timeout-value</i>		Timeout value in seconds. The range is from 30 to 300.

Command Default None

Command History

Release Modification

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

The following example shows how to set a query interval of 20 seconds for MLD query messages:

```
(Cisco Controller) > config network multicast mld query interval 20
```

Related Commands

config network multicast global
config network multicast igmp snooping
config network multicast igmp query interval
config network multicast l2mcast

config network multicast mode multicast

To configure the controller to use the multicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode multicast** command.

config network multicast mode multicast

Syntax Description This command has no arguments or keywords.

Command Default None

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

The following example shows how to configure the multicast mode to send a single copy of data to multiple receivers:

```
(Cisco Controller) > config network multicast mode multicast
```

Related Commands

- config network multicast global**
- config network broadcast**
- config network multicast mode unicast**

config network multicast mode unicast

To configure the controller to use the unicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode unicast** command.

config network multicast mode unicast

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
---------	--------------

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

The following example shows how to configure the controller to use the unicast mode:

```
(Cisco Controller) > config network multicast mode unicast
```

Related Commands

- config network multicast global**
- config network broadcast**
- config network multicast mode multicast**

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports { **enable** | **disable** }

Syntax Description	enable	disable
	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.
Command Default	The Ethernet port 3 Cisco 600 Series OEAP is reset.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network ocap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network ocap-600 local-network** command.

```
config network ocap-600 local-network {enable | disable}
```

Syntax Description	enable	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.
	disable	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.

Command Default	Access to the local network for the Cisco 600 Series OEAPs is disabled.
-----------------	-------------------------------------------------------------------------

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

The following example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
(Cisco Controller) > config network ocap-600 local-network enable
```

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {enable | disable}

Syntax Description	enable	enable
		Enables the OTAP provisioning.
	disable	Disables the OTAP provisioning.

Command Default The OTAP provisioning is enabled.

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

The following example shows how to disable the OTAP provisioning:

```
(Cisco Controller) >config network otap-mode disable
```

config network rf-network-name

To set the RF-Network name, use the **config network rf-network-name** command.

config network rf-network-name *name*

Syntax Description	<i>name</i>	RF-Network name. The name can contain up to 19 characters.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the RF-network name to travelers:

```
(Cisco Controller) > config network rf-network-name travelers
```

Related Commands **show network summary**

config network secureweb

To change the state of the secure web (https is http and SSL) interface for management users, use the **config network secureweb** command.

config network secureweb { **enable** | **disable** }

Syntax Description

enable	Enables the secure web interface for management users.
disable	Disables the secure web interface for management users.

Command Default

The secure web interface for management users is enabled by default.

Command History

Release Modification

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

Usage Guidelines

This command allows management users to access the controller GUI using an http://ip-address. Web mode is not a secure connection.

The following example shows how to enable the secure web interface settings for management users:

```
(Cisco Controller) > config network secureweb enable
You must reboot for the change to take effect.
```

Related Commands

config network secureweb cipher-option
show network summary

config network secureweb cipher-option

To enable or disable secure web mode with increased security, or to enable or disable Secure Sockets Layer (SSL v2) for web administration and web authentication, use the **config network secureweb cipher-option** command.

config network secureweb cipher-option { **high** | **sslv2** | **rc4-preference** } { **enable** | **disable** }

Syntax Description		
high		Configures whether or not 128-bit ciphers are required for web administration and web authentication.
sslv2		Configures SSLv2 for both web administration and web authentication.
rc4-preference		Configures preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration.
enable		Enables the secure web interface.
disable		Disables the secure web interface.

Command Default The default is **disable** for secure web mode with increased security and **enable** for SSL v2.

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

Usage Guidelines



Note The **config network secureweb cipher-option** command allows users to access the controller GUI using an `http://ip-address` but only from browsers that support 128-bit (or larger) ciphers.

When cipher-option `sslv2` is disabled, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later.

In RC4-SHA based cipher suites, RC4 is used for encryption and SHA is used for message authentication.

The following example shows how to enable secure web mode with increased security:

```
(Cisco Controller) > config network secureweb cipher-option
```

The following example shows how to disable SSL v2:

```
(Cisco Controller) > config network secureweb cipher-option sslv2 disable
```

Related Commands

- `config network secureweb`
- `show network summary`

config network ssh

To allow or disallow new Secure Shell (SSH) sessions, use the **config network ssh** command.

```
config network ssh {enable | disable}
```

Syntax Description

enable	Allows the new SSH sessions.
disable	Disallows the new SSH sessions.

Command Default

The default value for the new SSH session is **disable**.

The following example shows how to enable the new SSH session:

```
(Cisco Controller) > config network ssh enable
```

Related Commands

show network summary

config network telnet

To allow or disallow new Telnet sessions, use the **config network telnet** command.

```
config network telnet {enable | disable}
```

Syntax Description	enable	Allows new Telnet sessions.
	disable	Disallows new Telnet sessions.

Command Default By default, the new Telnet session is disallowed and the value is **disable**.

Usage Guidelines Telnet is not supported on Cisco Aironet 1830 and 1850 Series Access Points.

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

The following example shows how to configure the new Telnet sessions:

```
(Cisco Controller) > config network telnet enable
```

Related Commands

- config ap telnet
- show network summary

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command.

config network usertimeout *seconds*

Syntax Description	<i>seconds</i>	Timeout duration in seconds. The minimum value is 90 seconds. The default value is 300 seconds.
---------------------------	----------------	-------------------------------------------------------------------------------------------------

Command Default	The default timeout value for idle client session is 300 seconds.	
------------------------	-------------------------------------------------------------------	--

Usage Guidelines	Use this command to set the idle client session duration on the Cisco wireless LAN controller. The minimum duration is 90 seconds.	
-------------------------	------------------------------------------------------------------------------------------------------------------------------------	--

The following example shows how to configure the idle session timeout to 1200 seconds:

```
(Cisco Controller) > config network usertimeout 1200
```

Related Commands	show network summary
-------------------------	-----------------------------

config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

```
config network web-auth captive-bypass {enable | disable}
```

Syntax Description

enable	Allows the controller to support bypass of captive portals.
disable	Disallows the controller to support bypass of captive portals.

Command Default

None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

Related Commands

show network summary
config network web-auth cmcc-support

config network web-auth cmcc-support

To configure eWalk on the controller, use the **config network web-auth cmcc-support** command.

```
config network web-auth cmcc-support { enable | disable }
```

Syntax Description

enable Enables eWalk on the controller.

disable Disables eWalk on the controller.

Command Default

None

The following example shows how to enable eWalk on the controller:

```
(Cisco Controller) > config network web-auth cmcc-support enable
```

Related Commands

show network summary

config network web-auth captive-bypass

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description	<i>port</i>	Port number. The valid range is from 0 to 65535.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

Related Commands **show network summary**

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect {enable | disable}

Syntax Description	enable	Allows proxy redirect support for web authentication clients.
	disable	Disallows proxy redirect support for web authentication clients.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands **show network summary**

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb { **enable** | **disable** }

Syntax Description	enable	Allows secure web (https) authentication for clients.
	disable	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.
Command Default	The default secure web (https) authentication for clients is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>If you configure the secure web (https) authentication for clients using the config network web-auth secureweb disable command, then you must reboot the Cisco WLC to implement the change.</p> <p>The following example shows how to enable the secure web (https) authentication for clients:</p> <pre>(Cisco Controller) > config network web-auth secureweb enable</pre>	
Related Commands	show network summary	

config network web-auth https-redirect

To configure https redirect support for web authentication clients, use the **config network web-auth https-redirect** command.

```
config network web-auth https-redirect {enable | disable}
```

Syntax Description	enable	Enables the secure redirection(https) for web-authentication clients.
	disable	Disables the secure redirection(https) for web-authentication clients.
Command Default	This command is by default disabled.	
Command History	Release	Modification
	8.0	This command was introduced in Release 8.0

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth https-redirect enable
```

Related Commands **show network summary**

config network webcolor

To configure the web color theme for the controller GUI, use the **config network webcolor** command.

```
config network webcolor { default | red }
```

Syntax Description	default	Specifies the default web color theme for the controller GUI.
	red	Specifies the web color theme as red for the controller GUI.

Command Default	Default
------------------------	---------

Command History	Release	Modification
	8.0	This command was introduced.

Usage Guidelines If you are changing the web color theme from the controller CLI, you need to reload the controller GUI to apply your changes.

The following example shows how to configure the web interface color as red for the controller GUI:

```
(Cisco Controller) > config network webcolor red
```

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

```
config network webmode {enable | disable}
```

Syntax Description

enable	Enables the web interface.
---------------	----------------------------

disable	Disables the web interface.
----------------	-----------------------------

Command Default

The default value for the web mode is **enable**.

Command History

Release	Modification
---------	--------------

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

The following example shows how to disable the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

Related Commands

show network summary

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

```
config network web-auth {port port-number} | {proxy-redirect {enable | disable}}
```

Syntax Description

port	Configures additional ports for web authentication redirection.
<i>port-number</i>	Port number (between 0 and 65535).
proxy-redirect	Configures proxy redirect support for web authentication clients.
enable	Enables proxy redirect support for web authentication clients. Note Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
disable	Disables proxy redirect support for web authentication clients.

Command Default

The default network-level web authentication value is disabled.

Command History

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

Usage Guidelines

You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary
show run-config
config qos protocol-type

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config { **enable** | **disable** }

Syntax Description	enable	Enables the bridge access point ZeroConfig support.
	disable	Disables the bridge access point ZeroConfig support.
Command Default	The bridge access point ZeroConfig support is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the bridge access point ZeroConfig support:

```
(Cisco Controller) >config network zero-config enable
```

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default primary, use the **config network master-base** command.

```
config network master-base {enable | disable}
```

Syntax Description	enable	disable
	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.

Command Default None

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

Usage Guidelines This setting is only used upon network installation and should be disabled after the initial network configuration. Because the primary Cisco wireless LAN controller is normally not used in a deployed network, the primary Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

The following example shows how to enable the Cisco wireless LAN controller as a default primary:

```
(Cisco Controller) > config network master-base enable
```

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports { **enable** | **disable** }

Syntax Description	enable	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.
	disable	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.
Command Default	The Ethernet port 3 Cisco 600 Series OEAP is reset.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network ocap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network ocap-600 local-network** command.

config network ocap-600 local-network { **enable** | **disable** }

Syntax Description	enable	disable
	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.
Command Default	Access to the local network for the Cisco 600 Series OEAPs is disabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
(Cisco Controller) > config network ocap-600 local-network enable
```

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {enable | disable}

Syntax Description	enable	enable
		Enables the OTAP provisioning.
	disable	Disables the OTAP provisioning.

Command Default The OTAP provisioning is enabled.

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

The following example shows how to disable the OTAP provisioning:

```
(Cisco Controller) >config network otap-mode disable
```

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

```
config network zero-config {enable | disable}
```

Syntax Description	enable	Enables the bridge access point ZeroConfig support.
	disable	Disables the bridge access point ZeroConfig support.
Command Default	The bridge access point ZeroConfig support is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the bridge access point ZeroConfig support:

```
(Cisco Controller) >config network zero-config enable
```

config nmsp notify-interval measurement

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **config nmsp notify-interval measurement** command.

```
config nmsp notify-interval measurement { client | rfid | rogue } interval
```

Syntax Description		
client		Modifies the interval for clients.
rfid		Modifies the interval for active radio frequency identification (RFID) tags.
rogue		Modifies the interval for rogue access points and rogue clients.
<i>interval</i>		Time interval. The range is from 1 to 30 seconds.

Command Default None

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

Usage Guidelines The TCP port (16113) that the controller and location appliance communicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for NMSP to function.

The following example shows how to modify the NMSP notification interval for the active RFID tags to 25 seconds:

```
(Cisco Controller) > config nmsp notify-interval measurement rfid 25
```

Related Commands

- clear loep statistics**
- clear nmsp statistics**
- show nmsp notify-interval summary**
- show nmsp statistics**
- show nmsp status**

config pmipv6 domain

To configure PMIPv6 and to enable Mobile Access Gateway (MAG) functionality on Cisco WLC, use the **config pmipv6 domain** command.

config pmipv6 domain *domain_name*

Syntax Description	<i>domain_name</i> Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive, alphanumeric characters.				
Command Default	None				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr></tbody></table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				

The following example shows how to configure a domain name for a PMIPv6 WLAN:

```
(Cisco Controller) >config pmipv6 domain floor1
```

config pmipv6 add profile

To create a Proxy Mobility IPv6 (PMIPv6) profile for the WLAN, use the **config pmipv6 add profile** command. You can configure PMIPv6 profiles based on a realm or a service set identifier (SSID).

config pmipv6 add profile *profile_name* **nai** { *user@realm* | *@realm* | * } **lma** *lma_name* **apn** *apn_name*

Syntax Description	
<i>profile_name</i>	Name of the profile. The profile name is case sensitive and can be up to 127 alphanumeric characters.
nai	Specifies the Network Access Identifier of the client.
<i>user@realm</i>	Network Access Identifier of the client in the format <i>user@realm</i> . The NAI name is case sensitive and can be up to 127 alphanumeric characters.
<i>@realm</i>	Network Access Identifier of the client in the format <i>@realm</i> .
*	All Network Access Identifiers. You can have profiles based on an SSID for all users.
lma	Specifies the Local Mobility Anchor (LMA).
<i>lma_name</i>	Name of LMA. The LMA name is case sensitive and can be up to 127 alphanumeric characters.
apn	Specifies the access point.
<i>ap_name</i>	Name of the access point. The access point name is case sensitive and can be up to 127 alphanumeric characters.

Command Default None

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

Usage Guidelines This command is a prerequisite for using PMIPv6 configuration commands if the controller uses open authentication.

The following example shows how to create a PMIPv6 profile:

```
(Cisco Controller) >config pmipv6 add profile profile1 nai @vodafone.com lma vodfonelma apn vodafoneapn
```

config pmipv6 delete

To delete a Proxy Mobility IPv6 (PMIPv6) profile, domain, or Local Mobility Anchor (LMA), use the **config pmipv6 delete** command.

```
config pmipv6 delete { profile profile_name nai { nai_id | all } | domain domain_name | lma lma_name }
```

Syntax Description

profile	Specifies the PMIPv6 profile.
<i>profile_name</i>	Name of the PMIPv6 profile. The profile name is case sensitive and can be up to 127 alphanumeric characters.
nai	Specifies the Network Access Identifier (NAI) of a mobile client.
<i>nai_id</i>	Network Access Identifier of a mobile client. The NAI is case sensitive and can be up to 127 alphanumeric characters.
all	Specifies all NAIs. When you delete all NAIs, the profile is deleted.
domain	Specifies the PMIPv6 domain.
<i>domain_name</i>	Name of the PMIPv6 domain. The domain name is case sensitive and can be up to 127 alphanumeric characters.
lma	Specifies the LMA.
<i>lma_name</i>	Name of the LMA. The LMA name is case sensitive and can be up to 127 alphanumeric characters.

Command Default

None

Command History

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

The following example shows how to delete a domain:

```
(Cisco Controller) >config pmipv6 delete lab1
```

config pmipv6 mag apn

To configure an Access Point Name (APN) for a mobile access gateway (MAG), use the **config pmipv6 mag apn** command.

config pmipv6 mag apn *apn-name*

Syntax Description	<i>apn-name</i> Access point name for the MAG.
---------------------------	------------------------------------------------

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

Command History	Release	Modification
	8.0	This command was introduced.

Usage Guidelines By default, the MAG role is WLAN. However, for the lightweight access points, MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.

To delete an APN for a MAG, use the **config pmipv6 delete mag apn** *apn-name* command.

The following example shows how to add an APN for a MAG:

```
(Cisco Controller) >config pmipv6 mag apn myCiscoAP
```

config pmipv6 mag binding init-retx-time

To configure the initial timeout between the proxy binding updates (PBUs) when the Mobile Access Gateway (MAG) does not receive the proxy binding acknowledgements (PBAs), use the **config pmipv6 mag binding init-retx-time** command.

config pmipv6 mag binding init-retx-time *units*

Syntax Description	<i>units</i> Initial timeout between the PBUs when the MAG does not receive the PBAs. The range is from 100 to 65535 seconds.				
Command Default	The default initial timeout is 1000 seconds.				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr></tbody></table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				

The following example shows how to configure the initial timeout between the PBUs when the MAG does not receive the PBAs:

```
(Cisco Controller) >config pmipv6 mag binding init-retx-time 500
```

config pmipv6 mag binding lifetime

To configure the lifetime of the binding entries in the Mobile Access Gateway (MAG), use the **config pmipv6 mag binding lifetime** command.

config pmipv6 mag binding lifetime *units*

Syntax Description

units Lifetime of the binding entries in the MAG. The binding lifetime must be a multiple of 4 seconds. The range is from 10 to 65535 seconds.

Command Default

The default lifetime of the binding entries is 65535 seconds.

Command History

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

Usage Guidelines

You must configure a Proxy Mobility IPv6 (PMIPv6) domain before you configure the lifetime of the binding entries in the controller.

The following example shows how to configure the lifetime of the binding entries in the controller:

```
(Cisco Controller) >config pmipv6 mag binding lifetime 5000
```

config pmipv6 mag binding max-retx-time

To configure the maximum timeout between the proxy binding updates (PBUs) when the Mobility Access Gateway (MAG) does not receive the proxy binding acknowledgments (PBAs), use the **config pmipv6 mag binding max-retx-time** command.

config pmipv6 mag binding max-retx-time *units*

Syntax Description	<i>units</i> Maximum timeout between the PBUs when the MAG does not receive the PBAs. The range is from 100 to 65535 seconds.				
Command Default	The default maximum timeout is 32000 seconds.				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>7.6</td><td>This command was introduced in a release earlier than Release 7.6.</td></tr></tbody></table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				

The following example shows how to configure the maximum timeout between the PBUs when the MAG does not receive the PBAs:

```
(Cisco Controller) >config pmipv6 mag binding max-retx-time 50
```

config pmipv6 mag binding maximum

To configure the maximum number of binding entries in the Mobile Access Gateway (MAG), use the **config pmipv6 mag binding maximum** command.

config pmipv6 mag binding maximum *units*

Syntax Description	<i>units</i> Maximum number of binding entries in the MAG. This number indicates the maximum number of users connected to the MAG. The range is from 0 to 40000.				
Command Default	The default maximum number of binding entries in the MAG is 10000.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
Usage Guidelines	<p>You must configure a Proxy Mobility IPv6 (PMIPv6) domain before you configure the maximum number of binding entries in the MAG.</p> <p>The following example shows how to configure the maximum number of binding entries in the MAG:</p> <pre>(Cisco Controller) >config pmipv6 mag binding maximum 20000</pre>				

config pmipv6 mag binding refresh-time

To configure the refresh time of the binding entries in the MAG, use the **config pmipv6 mag binding refresh-time** command.

config pmipv6 mag binding refresh-time *units*

Syntax Description

units Refresh time of the binding entries in the MAG. The binding refresh time must be a multiple of 4. The range is from 4 to 65535 seconds.

Command Default

The default refresh time of the binding entries in the MAG is 300 seconds.

Usage Guidelines

You must configure a PMIPv6 domain before you configure the refresh time of the binding entries in the MAG.

The following example shows how to configure the refresh time of the binding entries in the MAG:

```
(Cisco Controller) >config pmipv6 mag binding refresh-time 500
```

config pmipv6 mag bri delay

To configure the maximum or minimum amount of time that the MAG waits before retransmitting a Binding Revocation Indication (BRI) message, use the **config pmipv6 mag bri delay** command.

config pmipv6 mag bri delay { **min** | **max** } *time*

Syntax Description

min	Specifies the minimum amount of time that the MAG waits before retransmitting a BRI message.
max	Specifies the maximum amount of time that the MAG waits before retransmitting a BRI message.
<i>time</i>	Maximum or minimum amount of time that the Cisco WLC waits before retransmitting a BRI message. The range is from 500 to 65535 milliseconds.

Command Default

The default value of the maximum amount of time that the MAG waits before retransmitting a BRI message is 2 seconds.

The default value of the minimum amount of time that the MAG waits before retransmitting a BRI message is 1 second.

Command History

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

The following example shows how to configure the minimum amount of time that the MAG waits before retransmitting a BRI message:

```
(Cisco Controller) >config pmipv6 mag bri delay min 500
```

config pmipv6 mag bri retries

To configure the maximum number of times that the MAG retransmits the Binding Revocation Indication (BRI) message before receiving the Binding Revocation Acknowledgment (BRA) message, use the **config pmipv6 mag bri retries** command.

config pmipv6 mag bri retries *retries*

Syntax Description

retries Maximum number of times that the MAG retransmits the BRI message before receiving the BRA message. The range is from 1 to 10 retries.

Command Default

The default is 1 retry.

The following example shows how to configure the maximum number of times that the MAG retries:

```
(Cisco Controller) >config pmipv6 mag bri retries 5
```

config pmipv6 mag lma

To configure a local mobility anchor (LMA) with the mobile access gateway (MAG), use the **config pmipv6 mag lma** command.

```
config pmipv6 mag lma lma_name ipv4-address address
```

Syntax Description	<i>lma_name</i>	Name of the LMA. The LMA name can be a NAI or a string that uniquely identifies the LMA.
	ipv4-address	Specifies the IP address of the LMA.
	<i>address</i>	IP address of the LMA.
Command Default	None	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
Usage Guidelines	<p>This command is a prerequisite to configure PMIPv6 parameters on the MAG.</p> <p>The following example shows how to configure an LMA with the MAG:</p> <pre>(Cisco Controller) >config pmipv6 mag lma vodafonelma ipv4-address 209.165.200.254</pre>	

config pmipv6 mag replay-protection

To configure the maximum amount of time difference between the timestamp in the received proxy binding acknowledgment (PBA) and the current time of the day for replay protection, use the **config pmipv6 mag replay-protection** command.

```
config pmipv6 mag replay-protection { timestamp window time | sequence-no sequence |
mobile-node-timestamp mobile_node_timestamp }
```

Syntax Description		
timestamp		Specifies the time stamp of the PBA message.
window		Specifies the maximum time difference between the time stamp in the received PBA message and the current time of day.
<i>time</i>		Maximum time difference between the time stamp in the received PBA message and the current time of day. The range is from 1 to 300 milliseconds.
sequence-no		(Optional) Specifies the sequence number in a Proxy Binding Update message.
<i>sequence</i>		(Optional) Sequence number in the Proxy Binding Update message.
mobile_node_timestamp		(Optional) Specifies the time stamp of the mobile node.
<i>mobile_node_timestamp</i>		(Optional) Time stamp of the mobile node.

Command Default The default maximum time difference is 300 milliseconds.

Usage Guidelines Only the timestamp option is supported.

The following example shows how to configure the maximum amount of time difference in milliseconds between the time stamp in the received PBA message and the current time of day:

```
(Cisco Controller) >config pmipv6 mag replay-protection timestamp window 200
```

config port power

To enable or disable Power over Ethernet (PoE) for a specific controller port or for all ports, use the **config port power** command.

```
config port power {all | port} {enable | disable}
```

Syntax Description		
all	Configures all ports.	
<i>port</i>	Port number.	
enable	Enables the specified ports.	
disable	Disables the specified ports.	
Command Default	Enabled	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable PoE on all ports:

```
(Cisco Controller) > config port power all enable
```

The following example shows how to disable PoE on port 8:

```
(Cisco Controller) > config port power 8 disable
```

config paging

To enable or disable scrolling of the page, use the **config paging** command.

```
config paging {enable | disable}
```

Syntax Description

enable	Enables the scrolling of the page.
disable	Disables the scrolling of the page.

Command Default

By default, scrolling of the page is enabled.

Usage Guidelines

Commands that produce a huge number of lines of output with the scrolling of the page disabled might result in the termination of SSH/Telnet connection or user session on the console.

The following example shows how to enable scrolling of the page:

```
(Cisco Controller) > config paging enable
```

Related Commands

show run-config

config passwd-cleartext

To enable or disable temporary display of passwords in plain text, use the **config passwd-cleartext** command.

```
config passwd-cleartext {enable | disable}
```

Syntax Description	enable	Disables the display of passwords in plain text.
	disable	Enables the display of passwords in plain text.

Command Default By default, temporary display of passwords in plain text is disabled.

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

Usage Guidelines This command must be enabled if you want to see user-assigned passwords displayed in clear text when using the **show run-config** command.

To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

The following example shows how to enable display of passwords in plain text:

```
(Cisco Controller) > config passwd-cleartext enable
The way you see your passwds will be changed
You are being warned.
Enter admin password:
```

Related Commands **show run-config**

config policy

To configure a native profiling policy on the Cisco Wireless LAN Controller (WLC), use the **config policy** command.

```
config policy policy_name { action { acl { enable | disable } acl_name | { average-data-rate | average-realtime-rate | burst-data-rate | burst-realtime-rate | qos | session-timeout | sleeping-client-timeout | avc-profile-name { enable avc_profile_name | disable } | vlan } { enable | disable } } } | active { add hours start_time end_time days day | delete days day } | create | delete | match { device-type { add | delete } device-type | eap-type { add | delete } { eap-fast | eap-tls | leap | peap } | role { role_name | none } }
```

Syntax Description

<i>policy_name</i>	Name of a profiling policy.
action	Configures an action for the policy.
acl	Configures an ACL for the policy
enable	Enables an action for the policy.
disable	Disables an action for the policy.
<i>acl_name</i>	Name of an ACL.
average-data-rate	Configures the QoS average data rate.
average-realtime-rate	Configures the QoS average real-time rate.
burst-data-rate	Configures the QoS burst data rate.
burst-realtime-rate	Configures the QoS burst real-time rate.
qos	Configures a QoS action for the policy.
session-timeout	Configures a session timeout action for the policy.
sleeping-client-timeout	Configures a sleeping client timeout for the policy.
avc-profile-name	Configures AVC profile on a policy.
vlan	Configures a VLAN action for the policy.
active	Configures the active hours and days for the policy.
add	Adds active hours and days.
hours	Configures active hours for the policy.
<i>start_time</i>	Start time for the policy.
<i>end_time</i>	End time for the policy.
days	Configures the day on the policy must work.

<i>day</i>	Day of the week, such as mon, tue, wed, thu, fri, sat, sun . You can also specify daily or weekdays for the policy to occur daily or on all weekdays.
delete	Deletes active hours and days.
create	Creates a policy.
match	Configures a match criteria for the policy.
device-type	Configures a device type match.
<i>device-type</i>	Device type on which the policy must be applied. You can configure up to 16 devices types for a policy.
eap-type	Configures the Extensible Authentication Protocol (EAP) type as a match criteria.
eap-fast	Configures the EAP type as EAP Flexible Authentication via Secure Tunneling (FAST).
eap-tls	Configures the EAP type as EAP Transport Layer Security (TLS).
leap	Configures the EAP type as Lightweight EAP (LEAP).
peap	Configures the EAP type as Protected EAP (PEAP).
role	Configures the user type or user group for the user.
<i>role_name</i>	User type or user group of the user, for example, student, employee. You can configure only one role per policy.
none	Configures no user type or user group for the user.

Command Default There is no native profiling policy on the Cisco WLC.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines The maximum number of policies that you can configure is 64.

The following example shows how to configure a role for a policy:

```
(Cisco Controller) > config policy student_policy role student
```

config port adminmode

To enable or disable the administrative mode for a specific controller port or for all ports, use the **config port adminmode** command.

```
config port adminmode {all | port} {enable | disable}
```

Syntax Description	all	Configures all ports.
	<i>port</i>	Number of the port.
	enable	Enables the specified ports.
	disable	Disables the specified ports.
Command Default	Enabled	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable port 8:

```
(Cisco Controller) > config port adminmode 8 disable
```

The following example shows how to enable all ports:

```
(Cisco Controller) > config port adminmode all enable
```

config port maxspeed

To configure maximum speed for a port, use the **config port maxspeed** command.

```
config port maxspeed port { 1000 | 2500 | 5000 }
```

Syntax Description		
<i>port</i>	Port number	
1000	Configures 1 Gbps speed for the port	
2500	Configures 2.5 Gbps speed for the port	
5000	Configures 5 Gbps speed for the port	
Command Default	None	
Command History	Release	Modification
	8.0	The command was introduced.

Examples

The following example shows how to configure the maximum speed for port 4 to 5 Gbps:

```
(Cisco Controller) > config port maxspeed 4 5000
```

config port linktrap

To enable or disable the up and down link traps for a specific controller port or for all ports, use the **config port linktrap** command.

```
config port linktrap {all | port} {enable | disable}
```

Syntax Description	all	Configures all ports.
	<i>port</i>	Number of the port.
	enable	Enables the specified ports.
	disable	Disables the specified ports.
Command Default	The default value for down link traps for a specific controller port or for all ports is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable port 8 traps:

```
(Cisco Controller) > config port linktrap 8 disable
```

The following example shows how to enable all port traps:

```
(Cisco Controller) > config port linktrap all enable
```

config port multicast appliance

To enable or disable the multicast appliance service for a specific controller port or for all ports, use the **config port multicast appliance** commands.

config port multicast appliance {**all** | *port*} {**enable** | **disable**}

Syntax Description		
all	Configures all ports.	
<i>port</i>	Number of the port.	
enable	Enables the specified ports.	
disable	Disables the specified ports.	
Command Default	The default multicast appliance service for a specific controller port or for all ports is enabled.	
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable multicast appliance service on all ports:

```
(Cisco Controller) > config port multicast appliance all enable
```

The following example shows how to disable multicast appliance service on port 8:

```
(Cisco Controller) > config port multicast appliance 8 disable
```

config prompt

To change the CLI system prompt, use the **config prompt** command.

config prompt *prompt*

Syntax Description

prompt New CLI system prompt enclosed in double quotes. The prompt can be up to 31 alphanumeric characters and is case sensitive.

Command Default

The system prompt is configured using the startup wizard.

Command History

Release Modification

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

Usage Guidelines

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

The following example shows how to change the CLI system prompt to Cisco 4400:

```
(Cisco Controller) > config prompt "Cisco 4400"
```

config qos average-data-rate

To define the average data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos average-data-rate** command.

```
config qos average-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client}
{downstream | upstream} rate
```

Syntax Description		
	bronze	Specifies the average data rate for the queue bronze.
	silver	Specifies the average data rate for the queue silver.
	gold	Specifies the average data rate for the queue gold.
	platinum	Specifies the average data rate for the queue platinum.
	per-ssid	Configures the rate limit for an SSID per radio. The com
	per-client	Configures the rate limit for each client associated with t
	downstream	Configures the rate limit for downstream traffic.
	upstream	Configures the rate limit for upstream traffic.
	<i>rate</i>	Average data rate for TCP traffic per user. A value betwe no bandwidth restriction on the QoS profile.

Command Default None

Command History

Release Modification

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

The following example shows how to configure the average data rate 0 Kbps for the queue gold per SSID:

```
(Cisco Controller) > config qos average-data-rate gold per ssid downstream 0
```

Related Commands

config qos burst-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate
config wlan override-rate-limit

config qos average-realtime-rate

To define the average real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos average-realtime-rate** command.

```
config qos average-realtime-rate {bronze | silver | gold | platinum} {per-ssid | per-client}
{downstream | upstream} rate
```

Syntax Description		
	bronze	Specifies the average real-time data rate for the queue bronze.
	silver	Specifies the average real-time data rate for the queue silver.
	gold	Specifies the average real-time data rate for the queue gold.
	platinum	Specifies the average real-time data rate for the queue platinum.
	per-ssid	Configures the rate limit for an SSID per radio. The combined traffic rate is limited to the rate specified for the SSID.
	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>	Average real-time data rate for UDP traffic per user. A value between 1 and 1000000 Kbps. A restriction on the QoS profile.

Command Default None

Command History **Release** **Modification**

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

The following example shows how to configure the average real-time actual rate for queue gold:

```
(Cisco Controller) > config qos average-realtime-rate gold per ssid downstream 10
```

Related Commands

- config qos average-data-rate**
- config qos burst-data-rate**
- config qos burst-realtime-rate**
- config wlan override-rate-limit**

config qos burst-data-rate

To define the peak data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos burst-data-rate** command.

```
config qos burst-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client}
{downstream | upstream} rate
```

Syntax Description

bronze	Specifies the peak data rate for the queue bronze.
silver	Specifies the peak data rate for the queue silver.
gold	Specifies the peak data rate for the queue gold.
platinum	Specifies the peak data rate for the queue platinum.
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>	Peak data rate for TCP traffic per user. A value between 0 and 51,200 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

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

The following example shows how to configure the peak rate 30000 Kbps for the queue gold:

```
(Cisco Controller) > config qos burst-data-rate gold per ssid downstream 30000
```

Related Commands

config qos average-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate
config wlan override-rate-limit

config qos burst-realtime-rate

To define the burst real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos burst-realtime-rate** command.

```
config qos burst-realtime-rate {bronze | silver | gold | platinum} { per-ssid | per-client }
{ downstream | upstream } rate
```

Syntax Description		
	bronze	Specifies the burst real-time data rate for the queue bronze.
	silver	Specifies the burst real-time data rate for the queue silver.
	gold	Specifies the burst real-time data rate for the queue gold.
	platinum	Specifies the burst real-time data rate for the queue platinum.
	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>	Burst real-time data rate for UDP traffic per user. A value between 0 and 51,200 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default None

Command History

Release Modification

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

The following example shows how to configure the burst real-time actual rate 2000 Kbps for the queue gold:

```
(Cisco Controller) > config qos burst-realtime-rate gold per ssid downstream 2000
```

Related Commands

config qos average-data-rate
config qos burst-data-rate
config qos average-realtime-rate
config wlan override-rate-limit

config qos description

To change the profile description, use the **config qos description** command.

config qos description {**bronze** | **silver** | **gold** | **platinum**} *description*

Syntax Description

bronze	Specifies the QoS profile description for the queue bronze.
silver	Specifies the QoS profile description for the queue silver.
gold	Specifies the QoS profile description for the queue gold.
platinum	Specifies the QoS profile description for the queue platinum.
<i>description</i>	QoS profile description.

Command Default

None

Command History

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

The following example shows how to configure the QoS profile description “description” for the queue gold:

```
(Cisco Controller) > config qos description gold abc
```

Related Commands

show qos average-data-rate
config qos burst-data-rate
config qos average-realtime-rate
config qos burst-realtime-rate
config qos max-rf-usage

config qos max-rf-usage

To specify the maximum percentage of RF usage per access point, use the **config qos max-rf-usage** command.

```
config qos max-rf-usage {bronze | silver | gold | platinum} usage_percentage
```

Syntax Description		
bronze		Specifies the maximum percentage of RF usage for the queue bronze.
silver		Specifies the maximum percentage of RF usage for the queue silver.
gold		Specifies the maximum percentage of RF usage for the queue gold.
platinum		Specifies the maximum percentage of RF usage for the queue platinum.
<i>usage-percentage</i>		Maximum percentage of RF usage.

Command Default None

Command History

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

The following example shows how to specify the maximum percentage of RF usage for the queue gold:

```
(Cisco Controller) > config qos max-rf-usage gold 20
```

Related Commands

- show qos description
- config qos average-data-rate
- config qos burst-data-rate
- config qos average-realtime-rate
- config qos burst-realtime-rate

config qos dot1p-tag

To define the maximum value (0 to 7) for the priority tag associated with packets that fall within the profile, use the **config qos dot1p-tag** command.

```
config qos dot1p-tag {bronze | silver | gold | platinum} dot1p_tag
```

Syntax Description		
bronze		Specifies the QoS 802.1p tag for the queue bronze.
silver		Specifies the QoS 802.1p tag for the queue silver.
gold		Specifies the QoS 802.1p tag for the queue gold.
platinum		Specifies the QoS 802.1p tag for the queue platinum.
<i>dot1p_tag</i>		Dot1p tag value between 1 and 7.

Command Default None

Command History

Release Modification

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

The following example shows how to configure the a QoS 802.1p tag for the queue gold with the dot1p tag value of 5:

```
(Cisco Controller) > config qos dot1p-tag gold 5
```

Related Commands

show qos queue_length all

config qos protocol-type

config qos priority

To define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN, use the **config qos priority** command.

```
config qos priority {bronze | silver | gold | platinum} {maximum-priority | default-unicast-priority | default-multicast-priority}
```

Syntax Description	
bronze	Specifies a Bronze profile of the WLAN.
silver	Specifies a Silver profile of the WLAN.
gold	Specifies a Gold profile of the WLAN.
platinum	Specifies a Platinum profile of the WLAN.
<i>maximum-priority</i>	Maximum QoS priority as one of the following: <ul style="list-style-type: none"> • besteffort • background • video • voice
<i>default-unicast-priority</i>	Default unicast priority as one of the following: <ul style="list-style-type: none"> • besteffort • background • video • voice
<i>default-multicast-priority</i>	Default multicast priority as one of the following: <ul style="list-style-type: none"> • besteffort • background • video • voice

Command History

Release Modification

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

Usage Guidelines

The maximum priority level should not be lower than the default unicast and multicast priority levels.

The following example shows how to configure the QoS priority for a gold profile of the WLAN with voice as the maximum priority, video as the default unicast priority, and besteffort as the default multicast priority.

```
(Cisco Controller) > config qos priority gold voice video besteffort
```

Related Commands **config qos protocol-type**

config qos protocol-type

To define the maximum value (0 to 7) for the priority tag associated with packets that fall within the profile, use the **config qos protocol-type** command.

```
config qos protocol-type {bronze | silver | gold | platinum} {none | dot1p}
```

Syntax Description	Option	Description
	bronze	Specifies the QoS 802.1p tag for the queue bronze.
	silver	Specifies the QoS 802.1p tag for the queue silver.
	gold	Specifies the QoS 802.1p tag for the queue gold.
	platinum	Specifies the QoS 802.1p tag for the queue platinum.
	none	Specifies when no specific protocol is assigned.
	<i>dot1p</i>	Specifies when dot1p type protocol is assigned.

Command Default None

Command History **Release Modification**

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

The following example shows how to configure the QoS protocol type silver:

```
(Cisco Controller) > config qos protocol-type silver dot1p
```

Related Commands

- show qos queue_length all**
- config qos dot1p-tag**

config qos queue_length

To specify the maximum number of packets that access points keep in their queues, use the **config qos queue_length** command.

```
config qos queue_length {bronze | silver | gold | platinum} queue_length
```

Syntax Description

bronze	Specifies the QoS length for the queue bronze.
silver	Specifies the QoS length for the queue silver.
gold	Specifies the QoS length for the queue gold.
platinum	Specifies the QoS length for the queue platinum.
<i>queue_length</i>	Maximum queue length values (10 to 255).

Command Default

None

Command History

Release Modification

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

The following example shows how to configure the QoS length for the queue “gold” with the maximum queue length value as 12:

```
(Cisco Controller) > config qos queue_length gold 12
```

Related Commands

show qos