config Commands

config ap address

To configure the AP IPv4 or IPv6 address, use the **config ap address** command.

config ap address ipv4 { **dhcp** | **static** { *static-ip-addr static-netmask default-gateway-ip-addr* | **ipv6** { **auto-config** {**enable** | **disable**} | **dhcp** | **disable** | **link-local** *ipv6-addr* | **static** *ipv6-addr ipv6-prefix gateway-ipv6-addr*

Syntax Description

ipv4	Configure IPv4 address
ipv6	Configure IPv6 address
auto-config	Auto configure IPv6 address
dhcp	Configure IPv6 DHCP
auto-config	
auto-config	

Command Default None.

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Examples

Related Commands

Command	Description

config ap client-trace

To configure client trace on the access point, use the **config ap client-trace** command.

config ap client-trace {**address** {**add** | **clear-all** | **delete**} | **all-clients** {**enable** | **disable**} | **filter** {**all** {**enable** | **disable**} | **arp** {**enable** | **disable**} | **assoc** {**enable** | **disable**} | **auth** {**enable** | **disable**} | **dhcp** {**enable** | **disable**} | **eap** {**enable** | **disable**} | **icmp** {**enable** | **disable**} | **ndp** {**enable** | **disable**} | **probe** {**enable** | **disable**}} | **inline-mon** {**enable** | **disable**} | **output** *console-log* | **start** | **stop**}

Syntax Description

addresses	Configure clients to trace. Specify the MAC address of the client
add	Specifies a client to trace
clear-all	Delete all client traces on this access point
delete	Deletes client address to be traced. Takes a client MAC address
all-clients	Trace all clients
enable	Enables trace for all clients
disable	Disables trace for all clients
filter	Sets filters for cleint tracing
all	Traces all filters
arp	Traces ARP packets Use the **enable** or **disable** keyword to enable or disable this filter.
assoc	Traces ASSOC packets
auth	Traces auth packets
dhcp	Traces DHCP packets
eap	Traces EAP packets

icmp	Traces ICMP packets
ndp	Traces NDP packets
probe	Trace probe packets.
inline-mon	Enables or disables inline monitoring
output	Enables or disables logging to the console or log file
console-log	Specifies console log keyword
start	Starts client tracing
stop	Stops client tracking

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to start client tracing on the AP:

```
cisco-ap# config ap client-trace start
```

config ap client-trace filter

To set filters for client trace, use the **config ap client-trace filter** command.

config ap client-trace filter { **all** [**disable** | **enable**] | **arp** [**disable** | **enable**] | **assoc** [**disable** | **enable**] | **auth** [**disable** | **enable**] | **dhcp** [**disable** | **enable**] | **eap** [**disable** | **enable**] | **icmp** [**disable** | **enable**] | **ndp** [**disable** | **enable**] }

Syntax Description

all	Trace all filters
arp	Trace ARP packets
assoc	Trace ASSOC packets
auth	Trace auth packets
dhcp	Trace DHCP packets
eap	Trace EAP packets
icmp	Trace ICMP packets

ndp	Trace NDP Packets

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

To set filters for client trace, use this command:

```
cisco-ap# config ap client-trace filter
```

config ap client-trace output

To configure the trace output, use the **config ap client-trace output** command.

config ap client-trace output console-log {**disable** | **enable**}

Syntax Description

console-log	Displays trace output to console and log
disable	Disables trace output to console and log
enable	Enables trace output to console and log

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows you how to configure the trace output:

```
cisco-ap# config ap client-trace output
```

config boot baudrate

To set the baud rate, use the **config boot baudrate** command.

config boot baudrate {*115200* | *9600*}

Syntax Description

115200	Sets the baud rate to 115200
9600	Sets the baud rate to 9600

Command Default The default config boot baud rate is 9600.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to configure the baud rate to 9600:

```
cisco-ap# config boot baudrate 9600
```

config boot break

To enable break, use the **config boot break** command.

config boot break {**enable** | **disable**}

Syntax Description

enable	Enables boot break
disable	Disables boot break

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to enable boot break:

```
cisco-ap# config boot break enable
```

config boot crashkernel

To enable or disable kernel crash, use the **config boot crashkernel** command.

config boot crashkernel {**enable** | **disable**}

Syntax Description

enable	Enables kernel crash

disable	Disables kernel crash

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to enable kernel crash:

```
cisco-ap# config boot crashkernel enable
```

config boot debug-memory

To enable memory debug, use the **config boot debug-memory** command.

config boot debug-memory {**enable** | **disable**}

Syntax Description

enable	Enables memory debug
disable	Disables memory debug

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

This example shows you how to enable memory debug:

```
cisco-ap# config boot debug-memory enable
```

config boot manual

To enable manual boot of the AP, use the **config boot manual** command.

config boot manual {**enable** | **disable**}

Syntax Description

enable	Enables manual boot

disable	Disables manual boot

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to enable manual boot:

```
cisco-ap# config boot manual enable
```

config boot path

To configure the boot path, use the **config boot path** command.

config boot path {*1* | *2*}

Syntax Description

{*1* | *2*}	Path to be specified as Part 1 or Part 2

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to configure the booth path as 1:

```
cisco-ap# config boot path 1
```

config cts debug enforcement host_ip

To filter the SGACL enforcement debugs based on the host IP, use the **config cts debug enforcement host_ip** command.

config cts debug enforcement host_ip {**ipv4** *dst-ip* [*src-ip*] | **ipv6** *dst-ip* [*src-ip*]}

Syntax Description		
	ipv4 *dst-ip* [*src-ip*]	Displays only the IPv4 SGACL enforcement debugs based on the destination and, optionally, source IP addresses
	ipv6 *dst-ip* [*src-ip*]	Displays only the IPv6 SGACL enforcement debugs based on the destination and, optionally, source IP addresses

Command Modes Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows you how to filter the IPv4 SGACL enforcement debugs based on the host IP:

```
cisco-ap# config cts debug enforcement host_ip ipv4 209.165.200.224 209.165.200.227
```

config cts debug enforcement rate

To configure the rate of printing of debug logs, use the **config cts debug enforcement rate** command.

config cts debug enforcement rate {*X Y* }

Command Modes Privileged EXEC (#)

Syntax Description		
	rate	Configure the rate of printing debug logs
	X	Number of packets whose debugs are to be displayed for every *Y* number of packets processed; valid range is between 0 to 10000
	Y	Number of packets to be processed; valid range is between 0 to 10000

Command History

Release	Modification
8.1.111.0	This command was introduced.

Examples

The following example shows how to configure the rate of printing of debug logs such that debugs of 100 packets are displayed for every 500 packets processed:

```
cisco-ap# config cts debug enforcement rate 100 500
```

config cts debug enforcement permissions

To filter SGACL enforcement debugs based on source group tag (SGT) and destination group tag (DGT), use the **config cts debug enforcement permissions** command.

config cts debug enforcement permissions {**dgt** | **sgt**} *tag-id*

Syntax Description

dgt	Destination group tag
sgt	Source group tag
tag-id	Tag identifier; valid values are beteween 0 to 65535

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows you how to filter SGACL enforcement debugs for a destination group tag whose ID is 600:

```
cisco-ap# config cts debug enforcement permissions dgt 600
```

config cts debug enforcement protocol

To filter SGACL enforcement debugs based on protocol, use the **config cts debug enforcement protocol** command.

config cts debug enforcement protocol {*protocol-id* | **icmp** | **tcp** | **udp**}

Syntax Description

protocol-id	Protocol ID; valid values are between 0 to 65535
icmp	Filter SGACL enforcement for ICMP traffic
tcp	Filter SGACL enforcement for TCP traffic
udp	Filter SGACL enforcement for UDP traffic

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.1.111.0	This command was introduced.

The following example shows you how to filter SGACL enforcement debugs based on protocol for UDP traffic:

```
cisco-ap# config cts debug enforcement protocol udp
```