Debug Commands: j to q

debug l2age

To configure the debugging of Layer 2 age timeout messages, use the **debug l2age** command.

debug l2age {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of Layer2 age settings.
disable	Disables the debugging Layer2 age 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 the debugging of Layer2 age settings:

```
(Cisco Controller) > debug l2age enable
```

Related Commands

debug disable-all

debug mac

To configure the debugging of the client MAC address, use the **debug mac** command.

debug mac {**disable** | **addr** *MAC*}

Syntax Description

disable	Disables the debugging of the client using the MAC address.
addr	Configures the debugging of the client using the MAC address.
MAC	MAC address of the client.

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 debugging of the client using the MAC address:

```
(Cisco Controller) > debug mac addr 00.0c.41.07.33.a6
```

Related Commands

debug disable-all

debug mdns all

To debug all multicast DNS (mDNS) messages, details, and errors, use the **debug mdns all** command.

debug mdns all {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of all mDNS messages, details, and errors.
disable	Disables the debugging of all mDNS messages, details, and errors.

Command Default

By default, the debugging of all mDNS messages, details, and errors is disabled.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable debugging of all mDNS messages, details, and errors:

```
(Cisco Controller) > debug mdns all enable
```

Related Commands

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns error

debug mdns detail

debug mdns detail

To debug multicast DNS (mDNS) details, use the **debug mdns detail** command.

debug mdns detail {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS details.
disable	Disables the debugging of mDNS details.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS details:

```
(Cisco Controller) > debug mdns detail enable
```

Related Commands

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns error

To debug multicast DNS (mDNS) errors, use the **debug mdns error** command.

debug mdns error {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS errors.
disable	Disables the debugging of mDNS errors.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS errors.

```
(Cisco Controller) > debug mdns error enable
```

Related Commands

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns detail

debug mdns message

debug mdns message

To debug multicast DNS (mDNS) messages, use the **debug mdns message** command.

debug mdns message {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS messages.
disable	Disables the debugging of mDNS messages.

Command Default

Disabled.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS messages:

```
(Cisco Controller) > debug mdns message enable
```

Related Commands

config mdns profile

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns ha

To debug all the multicast Domain Name System (mDNS) High Availability (HA) messages, use the **debug mdns ha** command.

debug mdns ha {**enable** | **disable**}

Syntax Description

enable	Enables debugging of all the mDNS HA messages.
disable	Disables debugging of all the mDNS HA messages.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

This command is automatically enabled when the **debug mdns all** command is enabled.

The following example shows how to enable debugging of all the mDNS HA messages:

```
(Cisco Controller) > debug mdns ha enable
```

debug memory

To enable or disable the debugging of errors or events during the memory allocation of the controller, use the **debug memory** command.

debug memory { **errors** | **events** } { **enable** | **disable** }

Syntax Description

errors	Configures the debugging of memory leak errors.
events	Configures debugging of memory leak events.
enable	Enables the debugging of memory leak events.
disable	Disables the debugging of memory leak events.

Command Default

By default, the debugging of errors or events during the memory allocation of the controller 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 debugging of memory leak events:

```
(Cisco Controller) > debug memory events enable
```

Related Commands

config memory monitor errors

show memory monitor

config memory monitor leaks

debug mesh security

To configure the debugging of mesh security issues, use the **debug mesh security** command.

debug mesh security {**all** | **events** | **errors**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all mesh security messages.
events	Configures the debugging of mesh security event messages.
errors	Configures the debugging of mesh security error messages.
enable	Enables the debugging of mesh security error messages.
disable	Disables the debugging of mesh security error messages.

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 debugging of mesh security error messages:

```
(Cisco Controller) >debug mesh security errors enable
```

debug mobility

To configure the debugging of wireless mobility, use the **debug mobility** command.

debug mobility {**ap-list** | **config** | **directory** | **dtls** | **handoff** | **keep-alive** | **multicast** | **oracle** | **packet** | **peer-ip** *IP-address* | **pmk** | **pmtu-discovery** | **redha**} {**enable** | **disable**}

Syntax Description

ap-list	Configures the debugging of wireless mobility access point list.
config	Configures the debugging of wireless mobility configuration.
directory	Configures the debugging of wireless mobility error messages.
dtls	Configures the debugging of wireless mobility Datagram Transport Layer Security (DTLS) options.
handoff	Configures the debugging of wireless mobility handoff messages.
keep-alive	Configures the debugging of wireless mobility CAPWAP data DTLS keep-alive packets.
multicast	Configures the debugging of multicast mobility packets.
oracle	Starts the debugging of wireless mobility oracle options.
packet	Configures the debugging of wireless mobility packets.
peer-ip	Configures IP address of the mobility peer for which incoming and outgoing mobility messages should be displayed.
IP-address	IP address of the mobility peer for which incoming and outgoing mobility messages should be displayed.
pmk	Configures the debugging of wireless mobility pairwise master key (PMK).
pmtu-discovery	Configures the debugging of the wireless mobility path MTU discovery.
redha	Configures the debugging of the multicast mobility high availability.

enable	Enables the debugging of the wireless mobility feature.
disable	Disables the debugging of the wireless mobility feature.

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 enable the debugging of wireless mobility packets.

```
(Cisco Controller) >debug mobility handoff enable
```

debug nac

To configure the debugging of Network Access Control (NAC), use the **debug nac** command.

debug nac {**events** | **packet**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of NAC events.
packet	Configures the debugging of NAC packets.
enable	Enables the NAC debugging.
disable	Disables the NAC debugging.

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 debugging of NAC settings:

```
(Cisco Controller) > debug nac events enable
```

Related Commands

show nac statistics

show nac summary

config guest-lan nac

config wlan nac

debug nmsp

To configure the debugging of the Network Mobility Services Protocol (NMSP), use the **debug nmsp** command.

debug nmsp {**all** | **connection** | **detail** | **error** | **event** | **message** | **packet**}

Syntax Description

all	Configures the debugging for all NMSP messages.
connection	Configures the debugging for NMSP connection events.
detail	Configures the debugging for NMSP events in detail.
error	Configures the debugging for NMSP error messages.
event	Configures the debugging for NMSP events.
message	Configures the debugging for NMSP transmit and receive messages.
packet	Configures the debugging for NMSP packet events.

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 debugging of NMSP connection events:

```
(Cisco Controller) > debug nmsp connection
```

Related Commands

clear nmsp statistics

debug disable-all

config nmsp notify-interval measurement

debug ntp

To configure the debugging of the Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of detailed NTP messages.
low	Configures the debugging of NTP messages.
packet	Configures the debugging of NTP packets.
enable	Enables the NTP debugging.
disable	Disables the NTP debugging.

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 debugging of NTP settings:

```
(Cisco Controller) > debug ntp packet enable
```

Related Commands

debug disable-all

debug packet error

To configure debugging of the packets sent to the controller CPU , use the **debug packet error** command.

debug packet error {**enable** | **disable**}

Syntax Description

enable	Enables debugging of the packets sent to the controller CPU.
disable	Disables debugging of the packets sent to the controller CPU.

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 debugging of the packets sent to the controller CPU:

```
(Cisco Controller) > debug packet error enable
```

debug packet logging

To configure logging of the packets sent to the controller CPU, use the **debug packet logging** command.

debug packet logging {**acl** | **disable** | **enable** {**rx** | **tx** | **all**} *packet_count display_size* | **format** {**hex2pcap** | **text2pcap**}}

debug packet logging acl {**clear-all** | **driver** *rule_index action npu_encap port* | **eoip-eth** *rule_index action dst src type vlan* | **eoip-ip** *rule_index action src dst proto src_port dst_port* | **eth** *rule_index action dst src type vlan* | **ip** *rule_index action src dst proto src_port dst_port* | **lwapp-dot11***rule_index action dst src bssid type* | **lwapp-ip** *rule_index action src dst proto src_port dst_port*}

Syntax Description

acl	Filters the displayed packets according to a rule.
disable	Disables logging of all the packets.
enable	Enables logging of all the packets.
rx	Displays all the received packets.
tx	Displays all the transmitted packets.
all	Displays both the transmitted and the received packets.
packet_count	Maximum number of packets to be logged. The range is from 1 to 65535. The default value is 25.
display_size	Number of bytes to be displayed when printing a packet. By default, the entire packet is displayed.
format	Configures the format of the debug output.
hex2pcap	Configures the output format to be compatible with the hex2pcap format. The standard format used by Cisco IOS supports the use of hex2pcap and can be decoded using an HTML front end.
text2pcap	Configures the output format to be compatible with the text2pcap format. In this format, the sequence of packets can be decoded from the same console log file. .
clear-all	Clears all the existing rules pertaining to the packets.
driver	Filters the packets based on an incoming port or a Network Processing Unit (NPU) encapsulation type.
rule_index	Index of the rule that is a value between 1 and 6 (inclusive).
action	Action for the rule, which can be **permit**, **deny**, or **disable**.

npu_encap	NPU encapsulation type that determines how the packets are filtered. The possible values are *dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest,* or *any*.
port	Physical port for packet transmission or reception.
eoip-eth	Filters packets based on the Ethernet II header in the Ethernet over IP (EoIP) payload.
dst	Destination MAC address.
src	Source MAC address.
type	Two-byte type code, such as 0x800 for IP, 0x806 for Address Resolution Protocol (ARP). You can also enter a few common string values such as *ip* (for 0x800) or *arp* (for 0x806).
vlan	Two-byte VLAN identifier.
eoip-ip	Filters packets based on the IP header in the EoIP payload.
proto	Protocol. Valide values are: *ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, ddp, idpr-cmtp, rspf, vmtp, ospf, ipip,* and *encap*.
src_port	User Datagram Protocol or Transmission Control Protocol (UDP or TCP) two-byte source port, such as *telnet, 23* , or *any*. The controller supports the following strings: *tcpmux, echo, discard, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, bootpc, tftp, gopher, rje, finger, www, link, kerberos, supdup, hostnames, iso-tsap, csnet-ns, 3com-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, saft, npmp-local, npmp-gui,* and *hmmp-ind*.
dst_port	UDP or TCP two-byte destination port, such as *telnet, 23*, or *any*. The controller supports the same strings as those for the src_port.
eth	Filters packets based on the values in the Ethernet II header.
ip	Filters packets based on the values in the IP header.
lwapp-dot11	Filters packets based on the 802.11 header in the Lightweight Access Point Protocol (LWAPP) payload.
bssid	Basic Service Set Identifier of the VLAN.
lwapp-ip	Filters packets based on the IP header in the LWAPP payload.

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 logging of a packet:

```
(Cisco Controller) > debug packet logging enable
```

debug pem

To configure debugging of the access policy manager, use the **debug pem** command.

debug pem {**events** | **state**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of the policy manager events.
state	Configures the debugging of the policy manager state machine.
enable	Enables the debugging of the access policy manager.
disable	Disables the debugging of the access policy manager.

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 debugging of the access policy manager:

```
(Cisco Controller) >debug pem state enable
```

debug pm

To configure the debugging of the security policy manager module, use the **debug pm** command.

debug pm {**all disable** | {**config** | **hwcrypto** | **ikemsg** | **init** | **list** | **message** | **pki** | **rng** | **rules** | **sa-export** | **sa-import** | **ssh-l2tp** | **ssh-appgw** | **ssh-engine** | **ssh-int** | **ssh-pmgr** | **ssh-ppp** | **ssh-tcp**} {**enable** | **disable**}}

Syntax Description

all disable	Disables all debugging in the policy manager module.
config	Configures the debugging of the policy manager configuration.
hwcrypto	Configures the debugging of hardware offload events.
ikemsg	Configures the debugging of Internet Key Exchange (IKE) messages.
init	Configures the debugging of policy manager initialization events.
list	Configures the debugging of policy manager list mgmt.
message	Configures the debugging of policy manager message queue events.
pki	Configures the debugging of Public Key Infrastructure (PKI) related events.
rng	Configures the debugging of random number generation.
rules	Configures the debugging of Layer 3 policy events.
sa-export	Configures the debugging of SA export (mobility).
sa-import	Configures the debugging of SA import (mobility).
ssh-l2tp	Configures the debugging of policy manager Layer 2 Tunneling Protocol (l2TP) handling.
ssh-appgw	Configures the debugging of application gateways.
ssh-engine	Configures the debugging of the policy manager engine.
ssh-int	Configures the debugging of the policy manager intercepter.
ssh-pmgr	Configures the debugging of the policy manager.

ssh-ppp	Configures the debugging of policy manager Point To Point Protocol (PPP) handling.
ssh-tcp	Configures the debugging of policy manager TCP handling.
enable	Enables the debugging.
disable	Disables the debugging.

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 debugging of PKI-related events:

```
(Cisco Controller) > debug pm pki enable
```

Related Commands

debug disable-all

debug poe

To configure the debugging of Power over Ethernet (PoE), use the **debug poe** command.

debug poe {**detail** | **message** | **error**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of PoE detail logs.
error	Configures the debugging of PoE error logs.
message	Configures the debugging of PoE messages.
enable	Enables the debugging of PoE logs.
disable	Disables the debugging of PoE 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 PoE debugging:

```
(Cisco Controller) > debug poe message enable
```

Related Commands

debug disable-all

debug policy

To configure debugging of policy settings, use the **debug policy** command.

debug policy {**errors** | **events**} {**enable** | **disable**}

Syntax Description

errors	Configures debugging of policy errors.
events	Configures debugging of policy events.
enable	Enables debugging of policy events.
disable	Disables debugging of policy events.

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 debugging of policy errors:

```
(Cisco Controller) >  debug policy errors enable
```

debug profiling

To configure the debugging of client profiling, use the **debug profiling** command.

debug profiling {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of client profiling (HTTP and DHCP profiling).
disable	Disables the debugging of client profiling (HTTP and DHCP profiling).

Command Default

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 debugging of client profiling:

```
(Cisco Controller) >debug profiling enable
```