CHAPTER 15

debug icmp through debug ospfv3 Commands

debug icmp

To display detailed information about ICMP inspection, use the **debug icmp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug icmp trace [*level*]

no debug icmp trace [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
trace	Displays debugging information about ICMP trace activity.

Defaults

All options are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug icmp** command displays detailed information about ICMP inspection. The **no debug all** or **undebug all** command turns off all enabled debugs.

Examples

The following example enables the display of detailed information about ICMP inspection:

```
hostname# debug icmp
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
icmp	Configures access rules for ICMP traffic that terminates at a ASA interface.
show conn	Displays the state of connections through the ASA for different protocols and session types.

Commands	Description
show icmp	Displays the ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

debug idprom

To enable the display of IDPROM-related debugging information, use the **debug idprom** command in privileged EXEC mode. To disable the display of IDPROM-related debugging information, use the **no** form of this command.

debug idprom

no debug idprom

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.6(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables the display of debugging information for IDPROM-related errors:

```
hostname# debug idprom
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug igmp

To display IGMP debugging message information, use the **debug igmp** command in privileged EXEC mode. To disable the display of debugging message information, use the **no** form of this command.

debug igmp [**group** *group_id* | **interface** *if_name*]

no debug igmp [**group** *group_id* | **interface** *if_name*]

Syntax Description

group *group_id*	Displays IGMP debugging message information for the specified group.
interface *if_name*	Display IGMP debugging message information for the specified interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug igmp** command:

```
hostname# debug igmp

IGMP debugging is on
IGMP: Received v2 Query on outside from 192.168.3.2
IGMP: Send v2 general Query on dmz
IGMP: Received v2 Query on dmz from 192.168.4.1
IGMP: Send v2 general Query on outside
IGMP: Received v2 Query on outside from 192.168.3.1
IGMP: Send v2 general Query on inside
IGMP: Received v2 Query on inside from 192.168.1.1
IGMP: Received v2 Report on inside from 192.168.1.6 for 224.1.1.1
IGMP: Updating EXCLUDE group timer for 224.1.1.1
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the ASA and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

debug ils

To show debugging messages for ILS, use the **debug ils** command in privileged EXEC mode. To stop showing debugging messages for ILS, use the **no** form of this command.

debug ils [*level*]

no debug ils [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To see the current **debug** command settings, enter the **show debug** command. To stop the debugging output, enter the **no debug** command. To stop all debugging messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug ils** command may slow down traffic on busy networks.

Examples

The following example enables debugging messages at the default level (1) for ILS application inspection:

```
hostname# debug ils
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ils	Enables ILS application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

debug imagemgr

To display Image Manager debugging information, use the **debug imagemgr** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug imagemgr [*level*]

no debug imagemgr [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug imagemgr** and the **show debug** commands:

```
hostname# debug imagemgr
debug imagemgr  enabled at level 1
hostname# show debug
debug imagemgr  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug inspect tls-proxy

To show debugging messages for TLS proxy inspection, use the **debug inspect tls-proxy** command in privileged EXEC mode. To stop showing debugging messages, use the **no** form of this command.

debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

no debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

Syntax Description

all	Specifies all TLS proxy debugging.
errors	Specifies TLS proxy error debugging.
events	Specifies TLS proxy event debugging.
packets	Specifies TLS proxy packet debugging.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for TLS proxy:

```
hostname# debug inspect tls-proxy
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

debug ip eigrp

To display debugging message information EIGRP protocol packets, use the **debug ip eigrp** command in privileged EXEC mode. To disable the debugging message information display, use the **no** form of this command.

debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

no debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
ip-addr mask	(Optional) Limits debugging message output to messages that fall within the range defined by the IP address and network mask.
neighbor *nbr-addr*	(Optional) Limits debugging message output to the specified neighbor.
notifications	(Optional) Limits debugging message output to EIGRP protocol events and notifications.
summary	(Optional) Limits debugging message output to summary route processing.
user-interface	(Optional) Limits debugging message output to user events.

Defaults

If no keywords or arguments are specified, only debugging messages from the IPv4 ASDM appear.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

This command helps you analyze the packets that are sent and received on an interface.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug ip eigrp** command:

```
hostname# debug ip eigrp

IP-EIGRP Route Events debugging is on

EIGRP-IPv4(Default-IP-Routing-Table:1): Processing incoming UPDATE packet
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.0.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.43.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.43.0 255.255.255.0 metric 371200 -
256000 115200
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.246.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.246.0 255.255.255.0 metric 46310656 -
45714176 596480
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.40.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.40.0 255.255.255.0 metric 2272256 -
1657856 614400
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.245.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.245.0 255.255.255.0 metric 40622080 -
40000000 622080
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.244.0 255.255.255.0, - do advertise out
Ethernet0/1
```

Table 15-1describes the significant fields shown in the display.

Table 15-1 debug ip eigrp Field Descriptions

Field	Description
IP-EIGRP:	Indicates IP EIGRP messages.
Ext	Indicates that the following address is an external route rather than an internal route, which would be labeled as Int.
M	Displays the computed metric, which includes the value in the SM field and the cost between this router and the neighbor. The first number is the composite metric. The next two numbers are the inverse bandwidth and the delay, respectively.
SM	Displays the metric as reported by the neighbor.

Related Commands

Command	Description
debug eigrp packets	Displays debugging information for EIGRP packets.

debug ipsec-over-tcp

To display IPsec-over-TCP debugging information, use the **debug ipsec-over-tcp** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug ipsec-over-tcp [*level*]

no debug ipsec-over-tcp

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables IPsec-over-TCP debugging messages. The **show debug** command reveals that IPsec-over-TCP debugging messages are enabled.

```
hostname# debug ipsec-over-tcp
debug ipsec-over-tcp  enabled at level 1
hostname# show debug
debug ipsec-over-tcp  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug ipv6

To display IPv6 debugging messages, use the **debug ipv6** command in privileged EXEC mode. To stop the display of debugging messages, use the **no** form of this command.

debug ipv6 {**icmp** | **interface** | **mld** | **nd** | **packet** | **routing**}

no debug ipv6 {**icmp** | **interface** | **nd** | **packet** | **routing**}

Syntax Description

icmp	Displays debugging messages for IPv6 ICMP transactions, excluding ICMPv6 neighbor discovery transactions.
interface	Displays debugging information for IPv6 interfaces.
mld	Displays debugging messages for Multicast Listener Discovery (MLD).
nd	Displays debugging messages for ICMPv6 neighbor discovery transactions.
packet	Displays debugging messages for IPv6 packets.
routing	Displays debugging messages for IPv6 routing table updates and route cache updates.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output for the **debug ipv6 icmp** command:

```
hostname# debug ipv6 icmp
13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
```

```
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

Related Commands

Command	Description
ipv6 icmp	Defines access rules for ICMP messages that terminate on an ASA interface.
ipv6 address	Configures an interface with an IPv6 address or addresses.
ipv6 nd dad attempts	Defines the number of neighbor discovery attempts performed during duplicate address detection.
ipv6 route	Defines a static entry in the IPv6 routing table.

debug ipv6 dhcp

To enable and disable generic IPv6 DHCP debugging messages, use the **debug ipv6 dhcp** command in privileged EXEC mode. To stop the display of debugging messages, use the **no** form of this command.

debug ipv6 dhcp

no debug ipv6 dhcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output for the **debug ipv6 dhcp** command:

```
hostname# debug ipv6 dhcp
IPv6 DHCP: Received RELAY-REPLY from fe80::2a0:c9ff:fe5d:41ed on cnr

IPv6 DHCP: detailed packet contents
    src fe80::2a0:c9ff:fe5d:41ed (cnr)
    dst fe80::2e0:b6ff:fe00:3306
    type RELAY-REPLY(13), hop 0
    link 2002::1
    peer fe80::204:23ff:febb:b094
    option INTERFACE-ID(18), len 4
    0x00000003
    option RELAY-MSG(9), len 58
    type REPLY(7), xid 3718228
    option CLIENTID(1), len 14
```

```
  000100010f9a59d1000423bbb094
option SERVERID(2), len 14
  0001000147f28f15000cf1fcecac
option STATUS-CODE(13), len 14
  status code SUCCESS(0)
  status message: All on link!
```

Related Commands

Command	Description
debug ipv6 dhcprelay	Enables and disables IPv6 DHCP relay agent debugging.
show ipv6 dhcprelay binding	Displays the relay binding entries created by the relay agent.

debug ipv6 dhcprelay

To enable and disable IPv6 DHCP relay agent debugging messages, use the **debug ipv6 dhcprelay** command in privileged EXEC mode. To stop the display of debugging messages, use the **no** form of this command.

debug ipv6 dhcprelay

no debug ipv6 dhcprelay

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output for the **debug ipv6 dhcprelay** command:

```
hostname# debug ipv6 dhcprelay
IPv6 DHCP_RELAY: Relaying CONFIRM from fe80::204:23ff:febb:b094 on client
IPv6 DHCP_RELAY: Creating relay binding for fe80::204:23ff:febb:b094 at interface client
IPv6 DHCP_RELAY:   to fe80::2a0:c9ff:fe5d:41ed using cnr
IPv6 DHCP_RELAY:   to 2005::11 via 2005::11 using router
IPv6 DHCP_RELAY:   to fe80::204:23ff:febb:b094 using server
IPv6 DHCP_RELAY: Relaying RELAY-REPLY from fe80::2a0:c9ff:fe5d:41ed on cnr
IPv6 DHCP_RELAY:   relayed msg: REPLY
IPv6 DHCP_RELAY:   to fe80::204:23ff:febb:b094
IPv6 DHCP_RELAY: Deleting binding for fe80::204:23ff:febb:b094 at interface client
```

Related Commands

Command	Description
debug ipv6 dhcp	Enables and disables generic IPv6 DHCP debugging messages.
show ipv6 dhcprelay binding	Displays the relay binding entries created by the relay agent.

debug iua-proxy

To display IUA proxy debugging information, use the **debug iua-proxy** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug iua-proxy [*level*]

no debug iua-proxy

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables IUA-proxy debugging messages. The **show debug** command indicates that IUA-proxy debugging messages are enabled.

```
hostname# debug iua-proxy
debug iua-proxy  enabled at level 1
hostname# show debug
debug iua-proxy  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug kerberos

To display Kerberos authentication debugging information, use the **debug kerberos** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug kerberos [*level*]

no debug kerberos

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging lvel is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables Kerberos debugging messages. The **show debug** command reveals that Kerberos debugging messages are enabled.

```
hostname# debug kerberos
debug kerberos enabled at level 1
hostname# show debug
debug kerberos enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug l2tp

To display L2TP debugging information, use the **debug l2tp** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug l2tp {**data** | **error** | **event** | **packet**} *level*

no debug l2tp {**data** | **error** | **event** | **packet**} *level*

Syntax Description

data	Displays data packet trace information.
error	Displays error events.
event	Displays L2TP connection events.
level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
packet	Displays packet trace information.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables L2TP debugging messages for connection events. The **show debug** command indicates that L2TP debugging messages are enabled.

```
hostname# debug l2tp event 1
hostname# show debug
debug l2tp event enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug lacp

To display EtherChannel LACP debugging information, use the **debug lacp** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet** | **periodic**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet** | **periodic**]

Syntax Description

all	(Optional) Displays all LACP information.
event	(Optional) Displays LACP events.
fsm	(Optional) Displays LACP finite state machine eventd.
misc	(Optional) Displays LACP miscellaneous events.
packet	(Optional) Displays LACP packet activity.
periodic	(Optional) Displays periodic events.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables LACP debugging messages for events. The **show debug** command indicates that LACP debugging messages are enabled.

```
hostname# debug lacp event
hostname# show debug
debug lacp event enabled
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug lacp cluster

To display cluster Link Aggregation Control Protocol (cLACP) debug information, use the **debug lacp cluster** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug lacp cluster [**all** | **ccp** | **misc** | **protocol**] [*level*]

no debug lacp cluster [**all** | **ccp** | **misc** | **protocol**]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
ccp	(Optional) Displays debug messages for the cluster control process.
all	(Optional) Displays messages for all debug types.
misc	(Optional) Displays miscellaneous clustering debug messages.
protocol	(Optional) Displays debug messages for the protocol.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables debug messages for all types:

```
hostname# debug lacp cluster all
```

Related Commands

Command	Description
debug cluster	Enables debug messages for clustering.

debug ldap

To display LDAP debugging information, use the **debug ldap** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug ldap [*level*]

no debug ldap

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables LDAP debugging messages. The **show debug** command indicates that LDAP debugging messages are enabled.

```
hostname# debug ldap
debug ldap enabled at level 1
hostname# show debug
debug ldap enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug license

To show debugging messages for licenses, use the **debug license** command in privileged EXEC mode. To stop showing debugging messages for licenses, use the **no** form of this command.

debug license [*level*]

[no] debug license [*level*]

Syntax Description

level	Indicates the privilege level assigned to the specified user.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging for licenses:

```
hostname# debug lioense 255
debug license enabled at level 255
```

Related Commands

Command	Description
license server-enable	Identifies a unit as a shared licensing server.
show activation-key	Shows the current licenses installed.
show debug	Shows all enabled debuggers.

debug mac-address-table

To show debugging messages for the MAC address table, use the **debug mac-address-table** command in privileged EXEC mode. To stop showing debugging messages for the MAC address table, use the **no** form of this command.

debug mac-address-table [*level*]

no debug mac-address-table [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for the MAC address table:

```
hostname# debug mac-address-table
```

Related Commands

Command	Description
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.

Command	Description
show debug	Shows all enabled debuggers.
show mac-address-table	Shows MAC address table entries.

debug menu

To display detailed debugging information for specific features, use the **debug menu** command in privileged EXEC mode.

debug menu [**aaa** | **ak47** | **coredump** | **crashinfo** | **ctm** | **cts** | **dap** | **email** | **fw** | **ike-common** | **ikev1** | **ikev2** | **ipaddrutl** | **ipsec-over-tcp** | **ipv6** | **license** | **memory** | **nac** | **npshim** | **pki** | **ppp** | **qos** | **quota** | **regex** | **sessmgr** | **splitdns** | **ssl** | **syslog** | **vpnfo** | **vpnlib** | **webvpn**]

Syntax Description

aaa	(Optional) Specifies debugging information for the AAA feature.
ak47	(Optional) Specifies debugging information for the Application Kernel layer 4 to 7 framework feature.
coredump	(Optional) Specifies debugging information for the coredump feature.
crashinfo	(Optional) Specifies debugging information for the crashinfo feature.
ctm	(Optional) Specifies debugging information for the CTM feature.
cts	(Optional) Specifies debugging information for the CTS feature.
dap	(Optional) Specifies debugging information for the DAP feature.
email	(Optional) Specifies debugging information for the e-mail feature.
fw	(Optional) Specifies debugging information for the firewall feature.
ike-common	(Optional) Specifies debugging information for the IKE feature.
ikev1	(Optional) Specifies debugging information for the IKEv1 feature.
ikev2	(Optional) Specifies debugging information for the IKEv2 feature.
ipaddrutl	(Optional) Specifies debugging information for the IP address utilityfeature.
ipsec-over-tcp	(Optional) Specifies debugging information for the IPsec over TCP feature.
ipv6	(Optional) Specifies debugging information for the IPv6 feature.
license	(Optional) Specifies debugging information for the licensing feature.
memory	(Optional) Specifies debugging information for the memory feature.
nac	(Optional) Specifies debugging information for the NAC feature.
npshim	(Optional) Specifies debugging information for the NPSHIM feature.
pki	(Optional) Specifies debugging information for the PKI feature.
ppp	(Optional) Specifies debugging information for the PPP feature.
qos	(Optional) Specifies debugging information for the QoS feature.
quota	(Optional) Specifies debugging information for the quota feature.
regex	(Optional) Specifies debugging information for the registered expression feature.
sessmgr	(Optional) Specifies debugging information for the session manager feature.
splitdns	(Optional) Specifies debugging information for the split DNS feature.
ssl	(Optional) Specifies debugging information for the SSL feature.
syslog	(Optional) Specifies debugging information for the syslog feature.
vpnfo	(Optional) Specifies debugging information for the VPN failover feature.
vpnlib	(Optional) Specifies debugging information for the VPN library feature.
webvpn	(Optional) Specifies debugging information for the WebVPN feature.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
9.1(4)	The **ak47** option was added.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Caution The **debug menu** command should be used only under the supervision of Cisco TAC.

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug mfib

To display MFIB debugging information, use the **debug mfib** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug mfib {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [*group*] [**cluster**]

no debug mfib {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [*group*] [**cluster**]

Syntax Description

cluster	(Optional) Displays debugging information for the MFIB epoch number and the current timer value for the cluster.
group	(Optional) Displays the IP address of the multicast group.
init	(Optional) Displays system initialization activity.
mrib	(Optional) Displays debugging information for communication with MFIB.
pak	(Optional) Displays debugging information for packet forwarding operations.
ps	(Optional) Displays debugging information for process switching operations.
signal	(Optional) Displays debugging information for MFIB signaling to routing protocols.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	The **cluster** keyword was added.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug mfib db** command:

```
hostname# debug mfib db
MFIB IPv4 db debugging enabled
```

The following is sample output from the **debug mfib cluster** command:

```
hostname# debug mfib cluster

MFIB CLUSTER: MFIB CLUSTER: mfib_cluster_send_update_msg sync DB entry add:
s=172.23.57.98, g=229.111.112.12, mask_len=32, epoch=1, attr=0x20

MFIB CLUSTER: MFIB CLUSTER: mfib_cluster_send_update_msg sync DB entry add:
s=172.23.57.98, g=229.111.112.12, mask_len=32, epoch=1, attr=0x20

MFIB CLUSTER: MFIB CLUSTER: mfib_cluster_send_update_msg sync DB entry add:
s=172.23.57.98, g=229.111.112.12, mask_len=32, epoch=1, attr=0x20

MFIB CLUSTER: MFIB CLUSTER: mfib_cluster_send_update_msg sync DB entry add:
s=172.23.57.98, g=229.111.112.12, mask_len=32, epoch=1, attr=0x20
```

Related Commands

Command	Description
show mfib	Displays MFIB forwarding entries and interfaces.

debug mgcp

To display detailed information about MGCP application inspection, use the **debug mgcp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug mgcp {**messages** | **parser** | **sessions**}

no debug mgcp {**messages** | **parser** | **sessions**}

Syntax Description

messages	Displays debugging information about MGCP messages.
parser	Displays debugging information for parsing MGCP messages.
sessions	Displays debugging information about MGCP sessions.

Defaults

All options are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug mgcp** command displays detailed information about MGCP inspection. The **no debug all** or **undebug all** command turns off all enabled debugging.

Examples

The following example enables the display of detailed information about MGCP application inspection:

```
hostname# debug mgcp
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect mgcp	Enables MGCP application inspection.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays information about MGCP sessions established through the ASA.
show conn	Displays the connection state for different connection types.

debug mmp

To display inspect MMP events, use the **debug mmp** command in privileged EXEC mode. To stop the display of inspect MMP events, use the **no** form of this command.

debug mmp

no debug mmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows how to display inspect MMP events:

```
hostname# debug mmp
ciscoasa5520-tfw-cuma/admin(config-pmap)# MMP:: received 28 bytes from outside:1
72.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: version OLWP-2.0
MMP status: 0
MMP:: forward 28/28 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: version OLWP-2.0
MMP:: session-id: 41A3D410-8B10-4DEB-B15C-B2B4B0D22055
MMP status: 201
MMP:: forward 85/85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 196
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 200/196
MMP:: forward 265/265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 198
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 202/198
MMP:: forward 267/267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 67
```

```
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 71/67
MMP:: forward 135/135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: content-length: 32
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 36/32
MMP:: forward 100/100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 151
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 155/151
MMP:: forward 220/220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
```

Related Commands

Command	Description
inspect mmp	Configures the MMP inspection engine.
show debug mmp	Displays the current debugging settings for the MMP inspection module.
show mmp	Displays information about existing MMP sessions.

debug module-boot

To show debugging messages about the SSM booting process, use the **debug module-boot** command in privileged EXEC mode. To disable the display of debugging messages for the SSM booting process, use the **no** form of this command.

debug module-boot [*level*]

no debug module-boot [*level*]

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for the SSM booting process:

```
hostname# debug module-boot
```

Related Commands

Command	Description
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.

Command	Description
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

debug mrib

To display MRIB debugging information, use the **debug mrib** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug mrib {**client** | **io** | **route** [*group*] | **table**}

no debug mrib {**client** | **io** | **route** [*group*] | **table**}

Syntax Description

client	Enables debugging for MRIB client management activity.
io	Enables debugging of MRIB I/O events.
route	Enables debugging of MRIB routing entry activity.
group	Enables debugging of MRIB routing entry activity for the specified group.
table	Enables debugging of MRIB table management activity.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug mrib** io command:

```
hostname# debug mrib io
IPv4 MRIB io debugging is on
```

Related Commands

Command	Description
show mrib client	Displays information about the MRIB client connections.
show mrib route	Displays MRIB table entries.

debug nac

To enable logging of NAC Framework events, use the **debug nac** command in privileged EXEC mode. To disable the logging of NAC debugging messages, use the **no** form of this command.

debug nac {**all** | **auth** | **errors** | **events**}

no debug nac {**all** | **auth** | **errors** | **events**}

Syntax Description

all	Enables logging of debugging messages about all NAC information.
auth	Enables logging of debugging messages about NAC authentication requests and responses.
errors	Enables logging of NAC session errors.
events	Enables logging of NAC session events.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the ASA logs the following types of NAC events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.

The high priority assigned to debugging output can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables the logging of all NAC session events:

```
hostname# debug nac events
hostname#
```

The following example enables the logging of all NAC debugging messages:

```
hostname# debug nac all
```

```
hostname#
```

The following example disables the logging of all NAC debugging messages:

```
hostname# no debug nac
hostname#
```

Related Commands

Command	Description
debug eap	Enables logging of Extensible Authentication Protocol events to debug NAC Framework messaging.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
show vpn-session_summary.db	Displays the number of IPsec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

debug ntdomain

To display NT domain authentication debugging information, use the **debug ntdomain** command in privileged EXEC mode. To disable the display of NT domain debugging information, use the **no** form of this command.

debug ntdomain [*level*]

no debug ntdomain

Syntax Description

level	(Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables NT domain debugging messages. The **show debug** command indicates that NT domain debugging messages are enabled.

```
hostname# debug ntdomain
debug ntdomain enabled at level 1
hostname# show debug
debug ntdomain enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug ntp

To show debugging messages for NTP, use the **debug ntp** command in privileged EXEC mode. To stop showing debugging messages for NTP, use the **no** form of this command.

debug ntp {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **select** | **sync** | **validity**}

no debug ntp {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **select** | **sync** | **validity**}

Syntax Description

adjust	Shows messages about NTP clock adjustments.
authentication	Shows messages about NTP authentication.
events	Shows messages about NTP events.
loopfilter	Shows messages about NTP loop filter.
packets	Shows messages about NTP packets.
params	Shows messages about NTP clock parameters.
select	Shows messages about NTP clock selection.
sync	Shows messages about NTP clock synchronization.
validity	Shows messages about NTP peer clock validity.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debugging messages for NTP:

```
hostname# debug ntp events
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp server	Identifies an NTP server.
show debug	Shows all enabled debuggers.
show ntp associations	Shows the NTP servers with which the ASA is associated.
show ntp status	Shows the status of the NTP association.

debug ospf

To display debugging information about the OSPF routing processes, use the **debug ospf** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug ospf [**adj** | **database-timer** | **events** | **flood** | **hello** | **ipsec** | **lsa** | **lsa-generation** | **lsa-maxage** | **lsdb** | **packet** | **rate-limit** | **retransmission** | **spf** | **tree**] [**external**]

no debug ospf [**adj** | **database-timer** | **events** | **flood** | **hello** | **ipsec** | **lsa** | **lsa-generation** | **lsa-maxage** | **lsdb** | **packet** | **rate-limit** | **retransmission** | **spf** | **tree**] [**external**]

Syntax Description

adj	(Optional) Enables the debugging of OSPF adjacency events.
database-timer	(Optional) Enables the debugging of OSPF database timer events.
events	(Optional) Enables the debugging of OSPF events.
external	(Optional) Limits SPF debugging to external events.
flood	(Optional) Enables the debugging of OSPF flooding events.
hello	(Optional) Enables the debugging of OSPF hello events.
ipsec	(Optional) Enables the debugging of OSPF IPsec events.
lsa	(Optional) Enables SPF debugging of LSA events.
lsa-generation	(Optional) Enables the debugging of OSPF summary LSA generation events.
lsa-maxage	(Optional) Enables the debugging of OSPF summary LSA maximum age events.
lsdb	(Optional) Enables the debugging of OSPF summary LSA database events.
packet	(Optional) Enables the debugging of received OSPF packets.
rate-limit	(Optional) Enables the debugging of received OSPF rate limits.
retransmission	(Optional) Enables the debugging of OSPF retransmission events.
spf	(Optional) Enables the debugging of OSPF shortest path first calculations.
tree	(Optional) Enables the debugging of OSPF database events.

Defaults

Displays all OSPF debugging information if no keyword is provided.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	The following keywords have been added: **hello, ipsec, lsa, lsa-maxage, lsdb,** and **rate-limit.**

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug ospf events** command:

```
hostname# debug ospf events
ospf event debugging is on

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

Related Commands

Command	Description
show ospf	Displays general information about the OSPF routing process.

debug ospfv3

To display debugging information about the OSPFv3 routing processes, use the **debug ospfv3** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug ospfv3 [**adj** | **database-timer** | **events** | **flood** | **hello** | **lsa-generation** | **packet** | **retransmission** | **spf**]

no debug ospfv3 [**adj** | **database-timer** | **events** | **flood** | **hello** | **lsa-generation** | **packet** | **retransmission** | **spf**]

Syntax Description

adj	(Optional) Enables the debugging of OSPFv3 adjacency events.
database-timer	(Optional) Enables the debugging of OSPFv3 timer events.
events	(Optional) Enables the debugging of OSPFv3 events.
flood	(Optional) Enables the debugging of OSPFv3 flooding.
hello	(Optional) Enables the debugging of OSPFv3 hello events.
lsa-generation	(Optional) Enables the debugging of OSPFv3 summary LSA generation.
packet	(Optional) Enables the debugging of received OSPv3F packets.
retransmission	(Optional) Enables the debugging of OSPFv3 retransmission events.
spf	(Optional) Enables the debugging of OSPFv3 SPF calculations.

Defaults

Displays all OSPFv3 debugging information if no keyword is provided.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug ospf events** command:

```
hostname# debug ospfv3 events
ospfv3 event debugging is on

OSPFv3:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

Related Commands

Command	Description
show ipv6 ospf	Displays general information about the OSPFv3 routing process.