



CHAPTER

10

debug aaa through debug sip Commands

debug aaa

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

debug aaa [**accounting** | **authentication** | **authorization** | **internal** | **vpn** [*level*]]

no debug aaa

Syntax Description

accounting	(Optional) Show debug messages for accounting only.
authentication	(Optional) Show debug messages for authentication only.
authorization	(Optional) Show debug messages for authorization only.
internal	(Optional) Show debug messages for AAA functions supported by the local database only.
<i>level</i>	(Optional) Specifies the debug level. Valid with the vpn keyword only.
vpn	(Optional) Show debug messages for VPN-related AAA functions only.

Defaults

The default *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **debug aaa** command displays detailed information about AAA activity. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables debugging for AAA functions supported by the local database:

```
hostname(config)# debug aaa internal
debug aaa internal enabled at level 1
hostname(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

Related Commands

Command	Description
show running-config aaa	Displays running configuration related to AAA.

debug acl optimization

To show debug messages for access list optimization, use the **debug acl optimization** command in privileged EXEC mode. To stop showing access list optimization messages, use the **no** form of this command.

debug optimization

no debug optimization

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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **debug acl optimization** command displays detailed information about access list optimization activity. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables debugging for access list optimization functions:

```
hostname(config)# debug acl optimization
```

```
context 0 :: access-list test :: start time = 11:38:38, end time = 11:38:40, total time = 2.231 sec
```

Related Commands

Command	Description
access-list optimization enable	Enables access list optimization.
clear configure access-list	Clears an access list from the running configuration.
copy optimized-running-config	Copies the optimized running configuration to the designated location.

Command	Description
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

debug appfw

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

debug appfw [**chunk** | **event** | **eventverb** | **regex**]

no debug appfw [**chunk** | **event** | **eventverb** | **regex**]

Syntax Description

chunk	(Optional) Displays runtime information about processing of chunked transfer encoded packets.
event	(Optional) Displays debug information about packet inspection events.
eventverb	(Optional) Displays the action taken by the FWSM in response to an event.
regex	(Optional) Displays information about matching patterns with predefined signatures.

Defaults

All options are enabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **debug appfw** command displays detailed information about HTTP application inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

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

```
hostname# debug appfw
```

Related Commands

Commands	Description
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.

debug arp

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

debug arp

no debug arp

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:

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

Command History

Release	Modification
1.1(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 example enables debug messages for ARP:

```
hostname# debug arp
```

Related Commands

Command	Description
show debug	Shows all enabled debuggers.
arp	Adds a static ARP entry.
show arp statistics	Shows ARP statistics.

debug arp-inspection

To show debug messages for ARP inspection, use the **debug arp-inspection** command in privileged EXEC mode. To stop showing debug messages for ARP inspection, use the **no** form of this command.

debug arp-inspection

no debug arp-inspection

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:

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

Command History

Release	Modification
2.2(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 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 example enables debug messages for ARP inspection:

```
hostname# debug arp-inspection
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show debug	Shows all enabled debuggers.

debug asdm history

To view debug information for ASDM, use the **debug asdm history** command in privileged EXEC mode.

debug asdm history *level*

Syntax Description

level (Optional) Specifies the debug level.

Defaults

The default *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced (as debug pdm history).
3.1(1)	This command was changed from the debug pdm history command to the debug asdm history 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 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 example enables level 1 debugging of ASDM:

```
hostname# debug asdm history
debug asdm history enabled at level 1

hostname#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

debug context

To show debug messages when you add or delete a security context, use the **debug context** command in privileged EXEC mode. To stop showing debug messages for contexts, use the **no** form of this command.

debug context [*level*]

no debug context [*level*]

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.

Defaults

The default level is 1.

Command Modes

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

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

Command History

Release	Modification
2.2(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 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 example enables debug messages for context management:

```
hostname# debug context
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.

Command	Description
show context	Shows context information.
show debug	Shows all enabled debuggers.

debug control-plane

To show debug messages for the control plane, use the **debug control-plane** command in privileged EXEC mode. To stop showing debug messages for the control-plane, use the **no** form of this command.

debug control-plane {egress | gc | ingress | tcp | tlv | udp | xlate} [*level*]

no debug control-plane {egress | gc | ingress | tcp | tlv | udp | xlate} [*level*]

Syntax Description

egress	Shows debug messages related to packet egress processing.
gc	Shows garbage collection related debug messages.
ingress	Shows debug messages related to packet ingress processing.
<i>level</i>	(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.
tcp	Shows debug messages related to TCP connection, including SEQ and ACK numbers, window size, and TCP flags.
tlv	Shows debug messages related to TLV processing, and TLVs inserted into packets and their contents.
udp	Shows debug messages related to UDP, including the source and destination port numbers.
xlate	Shows debug messages related to NAT/PAT queries made to NPs, such as the type of query, parameters passed, and the values returned.

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
3.1(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 example enables debug messages for TCP packets:

```
hostname# debug control-plane tcp
```

Related Commands

Command	Description
show debug	Shows all enabled debuggers.

debug crypto ca

To show debug messages for PKI activity (used with CAs), use the **debug crypto ca** command in privileged EXEC mode. To stop showing debug messages for PKI, use the **no** form of this command.

debug crypto ca [messages | transactions] [*level*]

no debug crypto ca [messages | transactions] [*level*]

Syntax Description

<i>level</i>	(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. Level 1 (the default) shows messages only when errors occur. Level 2 shows warnings. Level 3 shows informational messages. Levels 4 and up show additional information for troubleshooting.
messages	(Optional) Shows only debug messages for PKI input and output messages.
transactions	(Optional) Shows only debug messages for PKI transactions.

Defaults

By default, this command shows all debug messages. The default level is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(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 debug messages for PKI:

```
hostname# debug crypto ca
```

Related Commands

Command	Description
debug crypto engine	Shows debug messages for the crypto engine.
debug crypto ipsec	Shows debug messages for IPSec.
debug crypto isakmp	Shows debug messages for ISAKMP.

debug crypto engine

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

debug crypto engine [*level*]

no debug crypto engine [*level*]

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.

Defaults

The default level is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

Usage Guidelines

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

Examples

The following example enables debug messages for the crypto engine:

```
hostname# debug crypto engine
```

Related Commands

Command	Description
debug crypto ca	Shows debug messages for the CA.
debug crypto ipsec	Shows debug messages for IPSec.
debug crypto isakmp	Shows debug messages for ISAKMP.

debug crypto ipsec

To show debug messages for IPSec, use the **debug crypto ipsec** command in privileged EXEC mode. To stop showing debug messages for IPSec, use the **no** form of this command.

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

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.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables debug messages for IPSec:

```
hostname# debug crypto ipsec
```

Related Commands

Command	Description
debug crypto ca	Shows debug messages for the CA.
debug crypto engine	Shows debug messages for the crypto engine.
debug crypto isakmp	Shows debug messages for ISAKMP.

debug crypto isakmp

To show debug messages for ISAKMP, use the **debug crypto isakmp** command in privileged EXEC mode. To stop showing debug messages for ISAKMP, use the **no** form of this command.

debug crypto isakmp [**timers**] [*level*]

no debug crypto isakmp [**timers**] [*level*]

Syntax Description

<i>level</i>	(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. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted ISAKMP packets in a human readable format. Level 255 shows hexadecimal dumps of decrypted ISAKMP packets.
timers	(Optional) Shows debug messages for ISAKMP timer expiration.

Defaults

The default level is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables debug messages for ISAKMP:

```
hostname# debug crypto isakmp
```

Related Commands

Command	Description
debug crypto ca	Shows debug messages for the CA.
debug crypto engine	Shows debug messages for the crypto engine.
debug crypto ipsec	Shows debug messages for IPSec.

debug ctiqbe

To show debug messages for CTIQBE application inspection, use the **debug ctiqbe** command in privileged EXEC mode. To stop showing debug messages for CTIQBE application inspection, use the **no** form of this command.

debug ctiqbe [*level*]

no debug ctiqbe [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug ctiqbe
```

Related Commands

Command	Description
inspect ctique	Enables CTIQBE application inspection.
show ctique	Displays information about CTIQBE sessions established through the FWSM.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug dcerpc

To display detailed information about DCERPC traffic, use the **debug dcerpc** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug dcerpc [**packet** | **error** | **event**]

no debug dcerpc [**packet** | **error** | **event**]

Syntax Description

error	(Optional) Displays error messages that are associated with the DCERPC client.
event	(Optional) Displays debug information about packet inspection events.
packet	(Optional) Displays packet information that is associated with the DCERPC client.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.2	Support for this command was introduced.

Usage Guidelines

The **debug dcerpc** command displays detailed information about DCERPC traffic. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables the display of detailed information about DCERPC traffic:

```
hostname# debug dcerpc
```

Related Commands

Commands	Description
inspect dcerpc	Configures DCERPC inspection parameters.
dcerpc-map	Defines a DCERPC inspection map for DCERPC application inspection.

debug dhcpc

To enable debugging of the DHCP client, use the **debug dhcpc** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpc {**detail** | **packet** | **error**} [*level*]

no debug dhcpc {**detail** | **packet** | **error**} [*level*]

Syntax Description

detail	Displays detail event information that is associated with the DHCP client.
error	Displays error messages that are associated with the DHCP client.
<i>level</i>	(Optional) Specifies the debug level. Valid values range from 1 to 255.
packet	Displays packet information that is associated with the DHCP client.

Defaults

The default debug level is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

Usage Guidelines

Displays DHCP client debug information.

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 example shows how to enable debugging for the DHCP client:

```
hostname# debug dhcpc detail 5
debug dhcpc detail enabled at level 5
```


Related Commands

Command	Description
show ip address dhcp	Displays detailed information about the DHCP lease for an interface.
show running-config interface	Displays the running configuration of the specified interface.

debug dhcpd

To enable debugging of the DHCP server, use the **debug dhcpd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpd {event | packet} [*level*]

no debug dhcpd {event | packet} [*level*]

Syntax Description

event	Displays event information that is associated with the DHCP server.
<i>level</i>	(Optional) Specifies the debug level. Valid values range from 1 to 255.
packet	Displays packet information that is associated with the DHCP server.

Defaults

The default debug level is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

Usage Guidelines

The **debug dhcpd event** command displays event information about the DHCP server. The **debug dhcpd packet** command displays packet information about the DHCP server.

Use the **no** form of the **debug dhcpd** commands to disable debugging.

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 shows an example of enabling DHCP event debugging:

```
hostname# debug dhcpd event
debug dhcpd event enabled at level 1
```

Related Commands	Command	Description
	show dhcpd	Displays DHCP binding, statistic, or state information.
	show running-config dhcpd	Displays the current DHCP server configuration.

debug dhcprelay

To enable debugging of the DHCP relay server, use the **debug dhcprelay** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcprelay { **event** | **packet** | **error** } [*level*]

no debug dhcprelay { **event** | **packet** | **error** } [*level*]

Syntax Description

error	Displays error messages that are associated with the DHCP relay agent.
event	Displays event information that is associated with the DHCP relay agent.
<i>level</i>	(Optional) Specifies the debug level. Valid values range from 1 to 255.
packet	Displays packet information that is associated with the DHCP relay agent.

Defaults

The default debug level is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

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 example shows how to enable debugging for DHCP relay agent error messages:

```
hostname# debug dhcprelay error
debug dhcprelay error enabled at level 1
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

debug disk

To display file system debug information, use the **debug disk** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug disk { **file** | **file-verbose** | **filesystem** } [*level*]

no debug disk { **file** | **file-verbose** | **filesystem** }

Syntax Description

file	Enables file-level disk debug messages.
file-verbose	Enables verbose file-level disk debug messages
filesystem	Enables file system debug messages.
<i>level</i>	(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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 file-level disk debug messages. The **show debug** command reveals that file-level disk debug messages are enabled. The **dir** command causes several debug messages.

```
hostname# debug disk file
debug disk file enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname# dir
```

```
IFS: Opening: file flash:/, flags 1, mode 0
IFS: Opened: file flash:/ as fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3

Directory of flash:/
IFS: Close: fd 3
IFS: Opening: file flash:/, flags 1, mode 0

4      -rw-  5124096      14:42:27 Apr 04 2005  cdisk.binIFS: Opened: file flash:/ as fd 3

9      -rw-  5919340      14:53:39 Apr 04 2005  ASDMIFS: Getdent: fd 3

11     drw-   0          15:18:56 Apr 21 2005  syslog
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Close: fd 3

16128000 bytes total (5047296 bytes free)
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug dns

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

debug dns [**resolver** | **all**] [*level*]

no debug dns]

Syntax Description

all	(Default) Shows all messages, including messages about the DNS cache.
<i>level</i>	(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.
resolver	(Optional) Shows only DNS resolver messages.

Defaults

The default level is 1. If you do not specify any keywords, the FWSM shows all messages.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables debug messages for DNS:

```
hostname# debug dns
```

Related Commands

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

debug eigrp fsm

To display debug information the DUAL finite state machine, use the **debug eigrp fsm** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp fsm

no debug eigrp fsm

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:

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

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command lets you observe EIGRP feasible successor activity and to determine whether route updates are being installed and deleted by the routing process.

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 eigrp fsm** command:

```
hostname# debug eigrp fsm
```

```
DUAL: dual_rcvupdate(): 172.25.166.0 255.255.255.0 via 0.0.0.0 metric 750080/0
DUAL: Find FS for dest 172.25.166.0 255.255.255.0. FD is 4294967295, RD is 4294967295
found
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.0.0 metric 4294967295/4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL: 0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
```

```
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

In the first line, DUAL stands for diffusing update algorithm. It is the basic mechanism within EIGRP that makes the routing decisions. The next three fields are the Internet address and mask of the destination network and the address through which the update was received. The metric field shows the metric stored in the routing table and the metric advertised by the neighbor sending the information. If shown, the term “Metric... inaccessible” usually means that the neighbor router no longer has a route to the destination, or the destination is in a hold-down state.

In the following output, EIGRP is attempting to find a feasible successor for the destination. Feasible successors are part of the DUAL loop avoidance methods. The FD field contains more loop avoidance state information. The RD field is the reported distance, which is the metric used in update, query, or reply packets.

The indented line with the “not found” message means a feasible successor was not found for 192.168.4.0 and EIGRP must start a diffusing computation. This means it begins to actively probe (sends query packets about destination 192.168.4.0) the network looking for alternate paths to 192.164.4.0.

```
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL: 0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

The following output indicates the route DUAL successfully installed into the routing table:

```
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
```

The following output shows that no routes to the destination were discovered and that the route information is being removed from the topology table:

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp topology	Displays the EIGRP topology table.

debug eigrp neighbors

To display debug information for neighbors discovered by EIGRP, use the **debug eigrp neighbors** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp neighbors [siatimer | static]

no debug eigrp neighbors [siatimer | static]

Syntax Description

siatimer	(Optional) Displays EIGRP stuck in active messages.
static	(Optional) Displays EIGRP static neighbor messages.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
4.0(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 from the **debug eigrp neighbors static** command. The example shows a static neighbor being added, and then removed, and the corresponding debug messages.

```
hostname# debug eigrp neighbors static

EIGRP Static Neighbors debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Multicast Hello is disabled on Ethernet0/0!
```

```

EIGRP: Add new static nbr 10.86.194.3 to AS 100 Ethernet0/0

hostname(config-router)# no neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Static nbr 10.86.194.3 not in AS 100 Ethernet0/0 dynamic list
EIGRP: Delete static nbr 10.86.194.3 from AS 100 Ethernet0/0
EIGRP: Multicast Hello is enabled on Ethernet0/0!

hostname(config-router)# no debug eigrp neighbors static

EIGRP Static Neighbors debugging is off

```

Related Commands

Command	Description
neighbor	Defines an EIGRP neighbor.
show eigrp neighbors	Displays the EIGRP neighbor table.

debug eigrp packets

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

debug eigrp packets [SIAquery | SIAreply | ack | hello | probe | query | reply | request | retry | stub | terse | update | verbose]

no debug eigrp packets [SIAquery | SIAreply | ack | hello | probe | query | reply | request | retry | stub | terse | update | verbose]

Syntax Description

ack	(Optional) Limits the debug output to EIGRP ack packets.
hello	(Optional) Limits the debug output to EIGRP hello packets.
probe	(Optional) Limits the debug output to EIGRP probe packets.
query	(Optional) Limits the debug output to EIGRP query packets.
reply	(Optional) Limits the debug output to EIGRP reply packets.
request	(Optional) Limits the debug output to EIGRP request packets.
retry	(Optional) Limits the debug output to EIGRP retry packets.
SIAquery	(Optional) Limits the debug output to EIGRP stuck in active query packets.
SIAreply	(Optional) Limits the debug output to EIGRP stuck in active reply packets.
stub	(Optional) Limits the debug output to EIGRP stub routing packets.
terse	(Optional) Displays all EIGRP packets except hello packets.
update	(Optional) Limits the debug output to EIGRP update packets.
verbose	(Optional) Outputs all packet debug messages.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify more than one packet type in a single command, for example:

```
debug eigrp packets query reply
```

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 eigrp packets** command:

```
hostname# debug eigrp packets

EIGRP: Sending HELLO on Ethernet0/1
        AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
        AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
        AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
        AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
        AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
        AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
        AS 109, Flags 0x0, Seq 2, Ack 0
```

The output shows transmission and receipt of EIGRP packets. The sequence and acknowledgment numbers used by the EIGRP reliable transport algorithm are shown in the output. Where applicable, the network-layer address of the neighboring router is also included.

Related Commands

Command	Description
show eigrp traffic	Displays the number of EIGRP packets sent and received.

debug eigrp transmit

To display transmittal messages sent by EIGRP, use the **debug eigrp transmit** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

no debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

Syntax Description

ack	(Optional) Information for acknowledgment (ACK) messages sent by the system.
build	(Optional) Build information messages (messages that indicate that a topology table was either successfully built or could not be built).
detail	(Optional) Additional detail for debug output.
link	(Optional) Information regarding topology table linked-list management.
packetize	(Optional) Information regarding packetize events.
peerdown	(Optional) Information regarding the impact on packet generation when a peer is down.
sia	(Optional) Stuck-in-active messages.
startup	(Optional) Information regarding peer startup and initialization packets that have been transmitted.
strange	(Optional) Unusual events relating to packet processing.

Defaults

If at least one transmittal event is not specified, all transmittal events are shown in the debug output.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify more than one transmittal event in a single command. For example:

```
hostname# debug eigrp ack build link
```

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 eigrp transmit** command. The example shows a **network** command being entered and the transmittal event debug message that is generated.

```
hostname# debug eigrp transmit

EIGRP Transmission Events debugging is on

      (ACK, PACKETIZE, STARTUP, PEERDOWN, LINK, BUILD, STRANGE, SIA, DETAIL)

hostname# configure terminal
hostname(config)# router eigrp 100
hostname(config-router)# network 10.86.194.0 255.255.255.0

DNDB UPDATE 10.86.194.0 255.255.255.0, serno 0 to 1, refcount 0

hostname(config-router)# no debug eigrp transmit

EIGRP Transmission Events debugging is off
```

Related Commands

Command	Description
show eigrp traffic	Displays the number of EIGRP packets sent and received.

debug eigrp user-interface

To display debug information for EIGRP user events, use the **debug eigrp user-interface** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp user-interface

no debug eigrp user-interface

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:

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

Release	Modification
4.0(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 from the **debug eigrp user-interface** command. The output is caused by an administrator removing a **passive-interface** command from an EIGRP configuration.

```
hostname# debug eigrp user-interface

EIGRP UI Events debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# no passive-interface inside

CSB2AF: FOUND (AS=100, Name=, VRF=0, AFI=ipv4)

hostname(config-router)# no debug eigrp user-interface

EIGRP UI Events debugging is off
```

Related Commands	Command	Description
	router eigrp	Enables an EIGRP routing process and enters router configuration mode.
	show running-config eigrp	Displays the EIGRP commands in the running configuration.

debug entity

To display management information base (MIB) debug information, use the **debug entity** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug entity [*level*]

no debug entity

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for 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 MIB debug messages. The **show debug** command reveals that MIB debug messages are enabled.

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

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug fixup

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

debug fixup { **onat** | **tcp** | **udp** } [*level*]

no debug fixup

Syntax Description

<i>level</i>	(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.
onat	Enables application inspection messages related to outside NAT.
tcp	Enables TCP-related application inspection messages.
udp	Enables UDP-related application inspection messages.

Defaults

All options are enabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **debug fixup** command displays detailed information about application inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables the display of detailed TCP-related information:

```
hostname# debug fixup tcp
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.

Commands	Description
inspect <i>protocol</i>	Enables application inspection for specific protocols.
policy-map	Associates a class map with specific security actions.

debug fover

To display failover debug information, use the **debug fover** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug fover { **cable** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdump** | **rxip** | **switch** | **sync** | **tx** | **txdump** | **txip** | **verify** }

no debug fover { **cable** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdump** | **rxip** | **switch** | **sync** | **tx** | **txdump** | **txip** | **verify** }

Syntax Description

cable	Failover LAN status .
fail	Failover internal exception.
fmsg	Failover message.
ifc	Network interface status trace.
open	Failover device open.
rx	Failover message receive.
rxdump	Failover receive message dump (serial console only).
rxip	IP network failover packet receive.
switch	Failover switching status.
sync	Failover configuration/command replication.
tx	Failover message transmit.
txdump	Failover transmit message dump (serial console only).
txip	IP network failover packet transmit.
verify	Failover message verify.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified. It includes additional debug keywords.

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 example shows how to display debug information for failover command replication:

```
hostname# debug fover sync  
fover event trace on
```

Related Commands

Command	Description
show failover	Displays information about the failover configuration and operational statistics.

debug fsm

To display FSM debug information, use the **debug fsm** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug fsm [*level*]

no debug fsm

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables FSM debug messages. The **show debug** command reveals that FSM debug messages are enabled.

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

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug ftp client

To show debug messages for FTP, use the **debug ftp client** command in privileged EXEC mode. To stop showing debug messages for FTP, use the **no** form of this command.

debug ftp client [*level*]

no debug ftp client [*level*]

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.

Defaults

The default value for *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
1.1(1)	This command was introduced.

Usage Guidelines

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



Note

Enabling the **debug ftp client** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for FTP:

```
hostname# debug ftp client
```

Related Commands

Command	Description
copy	Uploads or downloads image files or configuration files to or from an FTP server.
ftp mode passive	Configures the mode for FTP sessions.
show running-config ftp mode	Displays FTP client configuration.

debug generic

To display miscellaneous debug information, use the **debug generic** command in privileged EXEC mode. To disable the display of miscellaneous debug information, use the **no** form of this command.

debug generic [*level*]

no debug generic

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables miscellaneous debug messages. The **show debug** command reveals that miscellaneous debug messages are enabled.

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

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug gtp

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

debug gtp [**error** | **event** | **ha** | **parser**]

no debug gtp [**error** | **event** | **ha** | **parser**]

Syntax Description

error	(Optional) Displays debug information on errors encountered while processing the GTP message.
event	(Optional) Displays debug information on GTP events.
ha	(Optional) Debugs information on GTP HA events.
parser	(Optional) Displays debug information for parsing the GTP messages.

Defaults

All options are enabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **debug gtp** command displays detailed information about GTP inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.



Note

GTP inspection requires a special license.

Examples

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

```
hostname# debug gtp
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.
show running-config gtp-map	Shows the GTP maps that have been configured.

debug h323

To show debug messages for H.323, use the **debug h323** command in privileged EXEC mode. To stop showing debug messages for H.323, use the **no** form of this command.

debug h323 {gup | h225 | h245 | ras} [asn | event]

no debug h323 {gup | h225 | h245 | ras} [asn | event]

Syntax Description

asn	(Optional) Displays the output of the decoded PDUs.
event	(Optional) Displays the events of the H.245 signaling or turns on both traces.
gup	Specifies GUP signaling.
h225	Specifies H.225 signaling.
h245	Specifies H.245 signaling.
ras	Specifies the registration, admission, and status protocol.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	The keyword gup was added.

Usage Guidelines

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



Note

Enabling the **debug h323** command may slow down traffic on busy networks.

Examples

The following is sample output when debug messages are enabled at the default level (1) for H.225 signaling:

```
hostname# debug h323 h225
```

Related Commands	Command	Description
	inspect h323	Enables H.323 application inspection.
	show h225	Displays information for H.225 sessions established across the FWSM.
	show h245	Displays information for H.245 sessions established across the FWSM by endpoints using slow start.
	show h323-ras	Displays information for H.323 RAS sessions established across the FWSM.
	timeout (gtp-map)	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

debug http

To display detailed information about HTTP traffic, use the **debug http** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug http [*level*]

no debug http [*level*]

Syntax Description	<i>level</i>	(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.
--------------------	--------------	---

Defaults The default for *level* is 1.

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

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

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

Usage Guidelines The **debug http** command displays detailed information about HTTP traffic. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples The following example enables the display of detailed information about HTTP traffic:

```
hostname# debug http
```

Related Commands	Commands	Description
	http	Specifies hosts that can access the HTTP server internal to the FWSM.
	http-proxy	Configures an HTTP proxy server.
	http server enable	Enables the FWSM HTTP server.

debug http-map

To show debug messages for HTTP application inspection maps, use the **debug http-map** command in privileged EXEC mode. To stop showing debug messages for HTTP application inspection, use the **no** form of this command.

debug http-map

no debug http-map

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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



Note

Enabling the **debug http-map** command may slow down traffic on busy networks.

Examples

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

```
hostname# debug http-map
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

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	<i>level</i>	(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.
	trace	Displays debug 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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

The **debug icmp** command displays detailed information about ICMP inspection. The **no debug all** or **undebug all** commands turn 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 FWSM interface.
show conn	Displays the state of connections through the FWSM for different protocols and session types.

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

debug igmp

To display IGMP debug information, use the **debug igmp** command in privileged EXEC mode. To stop the display of debug 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 <i>group_id</i>	Displays IGMP debug information for the specified group.
interface <i>if_name</i>	Display IGMP debug 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:

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

Command History

Release	Modification
3.1(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 CiscoTAC. 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 FWSM and that were learned through IGMP.
	show igmp interface	Displays multicast information for an interface.

debug ils

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

debug ils [*level*]

no debug ils [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug 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 debug 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.

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

debug imagemgr [*level*]

no debug imagemgr

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for 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 Image Manager debug messages. The **show debug** command reveals that Image Manager debug messages are enabled.

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

Related Commands

 debug imagemgr

Command	Description
show debug	Displays current debug configuration.

debug ip bgp

To display debug information for the BGP routing processes, use the **debug ip bgp** command in privileged EXEC mode. To disable the display of debug information for the BGP routing processes, use the **no** form of this command.

debug ip bgp

no debug ip bgp

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context ¹	System
Privileged EXEC	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

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 bgp** command:

```
hostname# debug ip bgp
```

Related Commands

Command	Description
show ip bgp summary	Displays general information about the BGP routing process.

debug ipsec-over-tcp

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

debug ipsec-over-tcp [*level*]

no debug ipsec-over-tcp

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for 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 IPSec-over-TCP debug messages. The **show debug** command reveals that IPSec-over-TCP debug 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 current debug configuration.

debug ipv6

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

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

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

Syntax Description

icmp	Displays debug messages for IPv6 ICMP transactions, excluding ICMPv6 neighbor discovery transactions.
interface	Displays debug information for IPv6 interfaces.
nd	Displays debug messages for ICMPv6 neighbor discovery transactions.
packet	Displays debug messages for IPv6 packets.
routing	Displays debug 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:

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

Command History

Release	Modification
3.1(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 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 FWSM 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 iua-proxy

To display individual user authentication (IUA) proxy debug information, use the **debug iua-proxy** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug iua-proxy [*level*]

no debug iua-proxy

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.

Defaults

The default value for *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
3.1(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 example enables IUA-proxy debug messages. The **show debug** command reveals that IUA-proxy debug 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#
```

■ debug iua-proxy

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug kerberos

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

debug kerberos [*level*]

no debug kerberos

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables Kerberos debug messages. The **show debug** command reveals that Kerberos debug 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 current debug configuration.

debug ldap

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

debug ldap [*level*]

no debug ldap

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables LDAP debug messages. The **show debug** command reveals that LDAP debug 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 current debug configuration.

debug mac-address-table

To show debug messages for the MAC address table, use the **debug mac-address-table** command in privileged EXEC mode. To stop showing debug 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 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.

Defaults

The default level is 1.

Command Modes

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

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

Command History

Release	Modification
2.2(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 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 example enables debug 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.
show debug	Shows all enabled debuggers.
show mac-address-table	Shows MAC address table entries.

debug menu

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

debug menu



Caution

The **debug menu** command should be used only under the supervision of Cisco technical support staff.

Syntax Description

This command should be used only under the supervision of Cisco technical support staff.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(1)	Support for 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

This command should be used only under the supervision of Cisco technical support staff.

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug mfib

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

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

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

Syntax Description

db	(Optional) Displays debug information for route database operations.
<i>group</i>	(Optional) IP address of the multicast group.
init	(Optional) Displays system initialization activity.
mrrib	(Optional) Displays debug information for communication with MRIB.
pak	(Optional) Displays debug information for packet forwarding operations.
ps	(Optional) Displays debug information for process switching operations.
signal	(Optional) Displays debug 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:

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

Command History

Release	Modification
3.1(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 displays MFIB database operation debug information:

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

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 }

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

Defaults

All options are enabled.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The **debug mgcp** command displays detailed information about mgcp inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.

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 FWSM.
show conn	Displays the connection state for different connection types.

debug mrib

To display MRIB debug information, use the **debug mrib** command in privileged EXEC mode. To stop the display of debug 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.
<i>group</i>	Enables debugging of MRIB routing entry activity for the specified group.
io	Enables debugging of MRIB I/O events.
route	Enables debugging of MRIB routing entry activity.
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:

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

Command History

Release	Modification
3.1(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 CiscoTAC. 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 shows how to enable debugging of MRIB I/O events:

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

Related Commands

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

debug ntdomain

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

debug ntdomain [*level*]

no debug ntdomain

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables NT domain debug messages. The **show debug** command reveals that NT domain debug messages are enabled.

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

 debug ntdomain**Related Commands**

Command	Description
show debug	Displays current debug configuration.

debug ospf

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

debug ospf [**adj** | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **spf** | **external** | **inter** | **intra**] | **tree**]

no debug ospf [**adj** | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **spf** | **external** | **inter** | **intra**] | **tree**]

Syntax Description

adj	(Optional) Enables the debugging of OSPF adjacency events.
database-timer	(Optional) Enables the debugging of OSPF 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.
inter	(Optional) Limits SPF debugging to inter-area events.
intra	(Optional) Limits SPF debugging to intra-area events.
lsa-generation	(Optional) Enables the debugging of OSPF summary LSA generation.
packet	(Optional) Enables the debugging of received OSPF packets.
retransmission	(Optional) Enables the debugging of OSPF retransmission events.
spf	(Optional) Enables the debugging of OSPF shortest path first calculations. You can limit the SPF debug information by using the external , inter , and intra keywords.
tree	(Optional) Enables the debugging of OSPF database events.

Defaults

Displays all OSPF debug 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
1.1(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 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 parser cache

To display CLI parser debug information, use the **debug parser cache** command in privileged EXEC mode. To disable the display of CLI parser debug information, use the **no** form of this command.

debug parser cache [*level*]

no debug parser cache

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables CLI parser debug messages. The **show debug** command reveals the current debug configuration. The CLI parser debug messages appear before and after the output of the **show debug** command.

```
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
parser cache: hit at index 8
hostname#
```

■ debug parser cache

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug pim

To display PIM debug information, use the **debug pim** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

debug pim [**df-election** [**interface** *if_name* | **rp** *rp*] | **group** *group* | **interface** *if_name* | **neighbor**]

no debug pim [**df-election** [**interface** *if_name* | **rp** *rp*] | **group** *group* | **interface** *if_name* | **neighbor**]

Syntax Description

df-election	(Optional) Displays debug messages for PIM bidirectional DF-election message processing.
group <i>group</i>	(Optional) Displays debug information for the specified group. The value for <i>group</i> can be one of the following: <ul style="list-style-type: none"> Name of the multicast group, as defined in the DNS hosts table or with the domain ipv4 host command. IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
interface <i>if_name</i>	(Optional) When used with the df-election keyword, it limits the DF election debug display to information for the specified interface. When used without the df-election keyword, displays PIM error messages for the specified interface. Note The debug pim interface command does not display PIM protocol activity messages; it only displays error messages. To see debug information for PIM protocol activity, use the debug pim command without the interface keyword. You can use the group keyword to limit the display to the specified multicast group.
neighbor	(Optional) Displays only the sent/received PIM hello messages.
rp <i>rp</i>	(Optional) Can be either one of the following: <ul style="list-style-type: none"> Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain ipv4 host command. IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Logs PIM packets received and transmitted and also PIM-related events.

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 pim** command:

```
hostname# debug pim
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received RP-Reachable on Vlan101 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Vlan101
PIM: Received Join/Prune on Vlan101 from 172.24.37.6
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16
PIM: Send Prune on Vlan101 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.24.84.16/28
PIM: Send periodic Join/Prune to RP via 172.24.37.6 (Vlan101)
```

Related Commands

Command	Description
show pim group-map	Displays group-to-protocol mapping table.
show pim interface	Displays interface-specific information for PIM.
show pim neighbor	Displays entries in the PIM neighbor table.

debug pix acl

To show pix acl debug messages, use the **debug pix acl** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix acl

no debug pix acl

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:

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

Command History

Release	Modification
1.1(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 example enables debug messages:

```
hostname# debug pix acl
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pix cls

To show pix cls debug messages, use the **debug pix cls** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix cls

no debug pix cls

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:

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

Command History

Release	Modification
1.1(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 example enables debug messages:

```
hostname# debug pix cls
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pix pkt2pc

To show debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path, use the **debug pix pkt2pc** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix pkt2pc

no debug pix pkt2pc

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:

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

Command History

Release	Modification
1.1(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 debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path:

```
hostname# debug pix pkt2pc
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pix process

To show debug messages for xlate and secondary connections processing, use the **debug pix process** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix process

no debug pix process

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:

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

Command History

Release	Modification
1.1(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 debug messages for xlate and secondary connections processing:

```
hostname# debug pix process
```

Related Commands

Command	Description
debug pix pkt2pc	Shows debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path.
show debug	Shows all enabled debuggers.

debug pix uauth

To show pix uauth debug messages, use the **debug pix uauth** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix uauth

no debug pix uauth

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:

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

Command History

Release	Modification
1.1(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 example enables debug messages that :

```
hostname# debug pix uauth
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pptp

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

debug pptp [*level*]

no debug pptp [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug pptp
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect pptp	Enables PPTP application inspection.

Command	Description
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

debug radius

To show debug messages for AAA, use the **debug radius** command in privileged EXEC mode. To stop showing RADIUS messages, use the **no** form of this command.

debug radius [**all** | **decode** | **session** | **user** *username*]]

no debug radius

Syntax Description

all	(Optional) Show RADIUS debugging messages for all users and sessions, including decoded RADIUS messages.
decode	(Optional) Show decoded content of RADIUS messages. Content of all RADIUS packets display, including hexadecimal values and the decoded, eye-readable versions of these values.
session	(Optional) Show session-related RADIUS messages. Packet types for sent and received RADIUS messages display but not the packet content.
user	(Optional) Show RADIUS debugging messages for a specific user.
<i>username</i>	Specifies the user whose messages you want to see. Valid with the user keyword only.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **debug radius** command displays detailed information about RADIUS messaging between the FWSM and a RADIUS AAA server. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example shows decoded RADIUS messages, which happen to be accounting packets:

```
hostname(config)# debug radius decode
hostname(config)# RADIUS packet decode (accounting request)
```

```

Raw packet data (length = 216).....
i
Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 105 (0x69)
Radius: Length = 216 (0x00D8)
Radius: Vector: 842E0E99F44C00C05A0A19AB88A81312
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.1.1.1 (0x0A010101)
Radius: Type = 14 (0x0E) Login-IP-Host
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.2.0.50 (0xD0FE1291)
Radius: Type = 16 (0x10) Login-TCP-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x50
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 12 (0x0C)
Radius: Value (String) =
30 78 31 33 30 31 32 39 66 65 | 0x130129fe
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
62 72 6f 77 73 65 72 | browser
Radius: Type = 46 (0x2E) Acct-Session-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 42 (0x2A) Acct-Input-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x256D
Radius: Type = 43 (0x2B) Acct-Output-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x3E1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=10.
31 2e 31 2e 31 30 | 1.1.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 27 (0x1B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 21 (0x15)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 70 6f 72 74 3d 33 | ip:source-port=3
34 31 33 | 413
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 40 (0x28)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 34 (0x22)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 69 | ip:destination-i
70 3d 32 30 38 2e 32 35 34 2e 31 38 2e 31 34 35 | p=10.2.0.50
Radius: Type = 26 (0x1A) Vendor-Specific

```

debug radius

```
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 70 | ip:destination-p
6f 72 74 3d 38 30                               | ort=80
```

Related Commands

Command	Description
show running-config	Displays the configuration that is running on the FWSM.

debug route-inject

To enable debugging of the route-injections that have been configured on FWSM, use the **debug route-inject** command in global configuration mode.

debug route-inject

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	•	—

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines The **debug route-inject** command allows you debug the route-injections that have been configured on FWSM.

Examples The following is sample output from the **debug route-inject** command:

```
hostname(config)# debug route-inject
hostname(config)# route-inject
hostname(config-route-inject)# redistribute connected interface blah31
route_inject_walk_routes_type: operation inject, context single_vf (0), type connected
checking: ip 10.94.180.0, mask 255.255.255.0, gw 10.94.180.35, proto 15, weight 1, vlan 31, SysIP 31.1.1.1
hostname(config-route-inject)# match 1, injected 0, send_update 1, advertise 1
add: ip 10.94.180.0, mask 255.255.255.0, gw 10.94.180.35, proto 15, weight 1, vlan 31, SysIP 31.1.1.1
checking: ip 20.1.1.0, mask 255.255.255.0, gw 20.1.1.1, proto 15, weight 1, vlan 31, SysIP 31.1.1.1
operation inject, match 1, injected 0, send_update 1, advertise 1
add: ip 20.1.1.0, mask 255.255.255.0, gw 20.1.1.1, proto 15, weight 1, vlan 31, SysIP 31.1.1.1
FWSM(config-route-inject)#
```

Related Commands

Command	Description
clear configure route-inject	Removes the routes/NAT pools that were injected into the MSFC routing tables. Additionally, removes the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if in single routed mode.
redistribute	Configures the type of route or NAT pools to inject.
route-inject	Injects the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.
show route-inject	Displays the routes and NAT pools that have been injected.
show running-config route-inject	Displays the route-injection running configuration.

debug rtsp

To show debug messages for RTSP application inspection, use the **debug rtsp** command in privileged EXEC mode. To stop showing debug messages for RTSP application inspection, use the **no** form of this command.

debug rtsp [*level*]

no debug rtsp [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug rtsp
```

Related Commands

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

debug sdi

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

debug sdi [*level*]

no debug sdi

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables SDI debug messages. The **show debug** command reveals that SDI debug messages are enabled.

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

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug sequence

To add a sequence number to the beginning of all debug messages, use the **debug sequence** command in privileged EXEC mode. To disable the use of debug sequence numbers, use the **no** form of this command.

debug sequence [*level*]

no debug sequence

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.

Defaults

The defaults are as follows:

- Debug message sequence numbers are disabled.
- The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables sequence numbers in debug messages. The **debug parser cache** command enables CLI parser debug messages. The **show debug** command reveals the current debug configuration. The CLI parser debug messages shown include sequence numbers before each message.

```
hostname# debug sequence
debug sequence enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
```

debug sequence

```
hostname# show debug
0: parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
debug sequence  enabled at level 1
1: parser cache: hit at index 8
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug sip

To show debug messages for SIP application inspection, use the **debug sip** command in privileged EXEC mode. To stop showing debug messages for SIP application inspection, use the **no** form of this command.

debug sip [*level*]

no debug sip [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug sip
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sip	Enables SIP application inspection.

Command	Description
show conn	Displays the connection state for different connection types.
show sip	Displays information about SIP sessions established through the FWSM.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug skinny

To show debug messages for SCCP (Skinny) application inspection, use the **debug skinny** command in privileged EXEC mode. To stop showing debug messages for SCCP application inspection, use the **no** form of this command.

debug skinny [*level*]

no debug skinny [*level*]

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.

Defaults

The default value for *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
1.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug skinny
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect skinny	Enables SCCP application inspection.
show skinny	Displays information about SCCP sessions established through the FWSM.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug smtp

To show debug messages for SMTP/ESMTP application inspection, use the **debug smtp** command in privileged EXEC mode. To stop showing debug messages for SMTP/ESMTP application inspection, use the **no** form of this command.

debug smtp [*level*]

no debug smtp [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

The following example enables debug messages at the default level (1) for SMTP/ESMTP application inspection:

```
hostname# debug smtp
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect esmtp	Enables ESMTP application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SMTP.

debug sqlnet

To show debug messages for SQL*Net application inspection, use the **debug sqlnet** command in privileged EXEC mode. To stop showing debug messages for SQL*Net application inspection, use the **no** form of this command.

debug sqlnet [*level*]

no debug sqlnet [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

The following example enables debug messages at the default level (1) for SQL*Net application inspection:

```
hostname# debug sqlnet
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sqlnet	Enables SQL*Net application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SQL*Net.

debug ssh

To display debug information and error messages associated with SSH, use the **debug ssh** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ssh [*level*]

no debug ssh [*level*]

Syntax Description

level (Optional) Specifies an optional level of debug.

Defaults

The default *level* is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(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 ssh 255** command:

```
hostname# debug ssh 255
debug ssh enabled at level 255
SSH2 0: send: len 64 (includes padlen 17)
SSH2 0: done calc MAC out #239
SSH2 0: send: len 32 (includes padlen 7)
SSH2 0: done calc MAC out #240
SSH2 0: send: len 64 (includes padlen 15)
SSH2 0: done calc MAC out #241
SSH2 0: send: len 32 (includes padlen 16)
SSH2 0: done calc MAC out #242
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #243
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #244
```

```

SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #245
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #246
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #247
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #248
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #249
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #250
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #251
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #252
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #253
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #254
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #255
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #256
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #257
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #258

```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.
show ssh sessions	Displays information about active SSH sessions to the FWSM.
ssh	Allows SSH connectivity to the FWSM from the specified client or network.

debug sunrpc

To show debug messages for RPC application inspection, use the **debug sunrpc** command in privileged EXEC mode. To stop showing debug messages for RPC application inspection, use the **no** form of this command.

debug sunrpc [*level*]

no debug sunrpc [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug sunrpc
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sunrpc	Enables Sun RPC application inspection.
policy-map	Associates a class map with specific security actions.
show conn	Displays the connection state for different connection types, including RPC.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug tacacs

To display TACACS+ debug information, use the **debug tacacs** command in privileged EXEC mode. To disable the display of TACACS+ debug information, use the **no** form of this command.

debug tacacs [**session** | **user** *username*]

no debug tacacs [**session** | **user** *username*]

Syntax Description

session	Displays session-related TACACS+ debug messages.
user	Displays user-specific TACACS+ debug messages. You can display TACACS+ debug messages for only one user at a time.
<i>username</i>	Specifies the user whose TACACS+ debug messages you want to view.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(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 example enables TACACS+ debug messages. The **show debug** command reveals that TACACS+ debug messages are enabled.

```
hostname# debug tacacs user admin342
hostname# show debug
debug tacacs user admin342
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug timestamps

To add timestamp information to the beginning of all debug messages, use the **debug timestamps** command in privileged EXEC mode. To disable the use of debug timestamps, use the **no** form of this command.

debug timestamps [*level*]

no debug timestamps

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.

Defaults

The defaults are as follows:

- Debug timestamp information is disabled.
- The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(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 example enables timestamps in debug messages. The **debug parser cache** command enables CLI parser debug messages. The **show debug** command reveals the current debug configuration. The CLI parser debug messages shown include timestamps before each message.

```
hostname# debug timestamps
debug timestamps enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
```

```
hostname# show debug
1982769.770000000: parser cache: try to match 'show debug' in exec mode
1982769.770000000: parser cache: hit at index 8
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug vpn-sessiondb

To display VPN-session database debug information, use the **debug vpn-sessiondb** command in privileged EXEC mode. To disable the display of VPN-session database debug information, use the **no** form of this command.

debug vpn-sessiondb [*level*]

no debug vpn-sessiondb

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for 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 VPN-session database debug messages. The **show debug** command reveals that VPN-session database debug messages are enabled.

```
hostname# debug vpn-sessiondb
debug vpn-sessiondb enabled at level 1
hostname# show debug
debug vpn-sessiondb enabled at level 1
hostname#
```

Related Commands

 debug vpn-sessiondb

Command	Description
show debug	Displays current debug configuration.

debug xdmcp

To show debug messages for XDMCP application inspection, use the **debug xdmcp** command in privileged EXEC mode. To stop showing debug messages for XDMCP application inspection, use the **no** form of this command.

debug xdmcp [*level*]

no debug xdmcp [*level*]

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.

Defaults

The default value for *level* is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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



Note

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

Examples

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

```
hostname# debug xdmcp
```

Related Commands

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

