debug dap through debug http-map Commands

debug dap

To enable logging of Dynamic Access Policy events, use the **debug dap** command in privileged EXEC mode. To disable the logging of DAP debugging messages, use the **no** form of this command.

debug dap {**errors** | **trace**}

no debug dap {**errors** | **trace**}

Syntax Description

errors	Specifies DAP processing errors.
trace	Specifies a DAP function trace.

Defaults

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to enable DAP trace debugging:

```
hostname # debug dap trace
hostname #
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.

debug ddns

To show debugging messages for DDNS, use the **debug ddns** command in privileged EXEC mode. To disable debugging messages, use the **no** form of this command.

debug ddns

no debug ddns

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **debug ddns** command displays detailed information about DDNS. The **undebug ddns** command and the **no debug ddns** command turn off DDNS debugging 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 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 shows an example of enabling DDNS debugging messages:

```
hostname# debug ddns
debug ddns enabled at level 1
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a DDNS update method with a ASA interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

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.
level	(Optional) Specifies the debugging level. Valid values range from 1 to 255.
packet	Displays packet information that is associated with the DHCP client.

Defaults

The default debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays DHCP client debugging 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 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 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.
level	(Optional) Specifies the debugging 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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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 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, statistical, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

debug dhcpd ddns

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

debug dhcpd ddns [*level*]

no debug dhcpd ddns [*level*]

Syntax Description

level	(Optional) Specifies the debugging level. Valid values range from 1 to 255.

Defaults

The default debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **debug dhcpd ddns** command displays detailed information about DHCP and DDNS. The **undebug dhcpd ddns** command and the **no debug dhcpd ddns** command turn off DHCP and DDNS debugging 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 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 shows DHCP DDNS debugging being enabled:

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

Related Commands

Command	Description
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
show running-config dhcpd	Displays the current DHCP server configuration.
show running-config ddns	Display the DDNS update methods of the running configuration.

debug dhcprelay

To enable debugging of the DHCP relay server, use the **debug dhcpreleay** 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.
level	(Optional) Specifies the debugging 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		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example 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 debugging information, use the **debug disk** command in privileged EXEC mode. To disable the display of debugging 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 debugging messages.
file-verbose	Enables verbose file-level disk debugging messages.
filesystem	Enables file system debugging messages.
level	(Optional) Sets the level to display debugging messages. The range of values is between 1 and 255. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
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 the current debugging configuration.

debug dns

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

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

no debug dns [**resolver** | **all**] [*level*]

Syntax Description

all	(Default) Shows all messages, including messages about the DNS cache.
level	(Optional) Sets the debugging message level to display, which can be either 1 or 2. 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 ASA shows all mesages.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables debugging messages for 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 eap

To enable logging of EAP events to debug NAC messaging, use the **debug eap** command in privileged EXEC mode. To disable the logging of EAP debugging messages, use the **no** form of this command.

debug eap {**all** | **errors** | **events** | **packets** | **sm**}

no debug eap {**all** | **errors** | **events** | **packets** | **sm**}

Syntax Description

all	Enables logging of debugging messages about all EAP information.
errors	Enables logging of EAP packet errors.
events	Enables logging of EAP session events.
packets	Enables logging of debugging messages about EAP packet information.
sm	Enables logging of debugging messages about EAP state machine information.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the ASA records EAP session state changes and EAP status query events, and generates a complete record of EAP and packet contents in hexadecimal format.

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

Examples

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

```
hostname# debug eap events
hostname#
```

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

```
hostname# debug eap all
hostname#
```

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

```
hostname# no debug eap
hostname#
```

Related Commands

Command	Description
debug eou	Enables logging of EAPoUDP events to debug NAC messaging.
debug nac	Enables logging of NAC events.
eou initialize	Clears the resources assigned to one or more NAC sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC sessions.
show debug	Displays a current debugging configuration.

debug eigrp fsm

To display debugging information the DUAL finite state machine, use the **debug eigrp fsm** command in privileged EXEC mode. To disable the debugging 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:

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

Command History

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

Usage Guidelines

This command lets you observe EIGRP feasible successor activity and to determine whether or not 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 fist 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, 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 includes 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 debugging information for neighbors discovered by EIGRP, use the **debug eigrp neighbors** command in privileged EXEC mode. To disable the debugging 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 (SIA) 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:

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

Command History

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

Usage Guidelines

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 debugging 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 debugging information for EIGRP packets, use the **debug eigrp packets** command in privileged EXEC mode. To disable the debugging 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 debugging output to EIGRP ack packets.
hello	(Optional) Limits the debugging output to EIGRP hello packets.
probe	(Optional) Limits the debugging output to EIGRP probe packets.
query	(Optional) Limits the debugging output to EIGRP query packets.
reply	(Optional) Limits the debugging output to EIGRP reply packets.
request	(Optional) Limits the debugging output to EIGRP request packets.
retry	(Optional) Limits the debugging output to EIGRP retry packets.
SIAquery	(Optional) Limits the debugging output to EIGRP stuck in active query packets.
SIAreply	(Optional) Limits the debugging output to EIGRP stuck in active reply packets.
stub	(Optional) Limits the debugging output to EIGRP stub routing packets.
terse	(Optional) Displays all EIGRP packets except hello packets.
update	(Optional) Limits the debugging output to EIGRP update packets.
verbose	(Optional) Outputs all packet debugging messages.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

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

Usage Guidelines

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

```
hostname# 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 the 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 transmission messages sent by EIGRP, use the **debug eigrp transmit** command in privileged EXEC mode. To disable the debugging 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) Displays information for acknowledgment (ACK) messages sent by the system.
build	(Optional) Displays build information messages (messages that indicate that a topology table was either successfully built or could not be built).
detail	(Optional) Displays additional detail for debugging output.
link	(Optional) Displays information regarding topology table linked-list management.
packetize	(Optional) Displays information regarding packetized events.
peerdown	(Optional) Displays information regarding the effect on packet generation when a peer is down.
sia	(Optional) Displays stuck-in-active messages.
startup	(Optional) Displays information regarding peer startup and initialization packets that have been transmitted.
strange	(Optional) Displays unusual events relating to packet processing.

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

You can specify more than one transmission 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 transmission event debugging 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 debugging information for EIGRP user events, use the **debug eigrp user-interface** command in privileged EXEC mode. To disable the debugging 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:

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

Command History

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

Usage Guidelines

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 email

To display e-mail debugging information, use the **debug email** command in privileged EXEC mode. To disable the display of e-mail debugging information, use the **no** form of this command.

debug email [*level*]

no debug email [*level*]

Syntax Description

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

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	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 email** and the **show debug email** commands:

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

Related Commands

Command	Description
show debug	Displays the current debugging configuration.

debug entity

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

debug entity [*level*]

no debug entity

Syntax Description

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

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables MIB debugging messages. The **show debug** command indicates that MIB debugging 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 the current debugging configuration.

debug eou

To enable logging of EAPoUDP events to debug NAC messaging, use the **debug eou** command in privileged EXEC mode. To disable the logging of EAPoUDP debugging messages, use the **no** form of this command.

debug eou {**all** | **eap** | **errors** | **events** | **packets** | **sm**}

no debug eou [**all** | **eap** | **errors** | **events** | **packets** | **sm**]

Syntax Description

all	Enables logging of debugging messages about all EAPoUDP information.
eap	Enables logging of debugging messages about EAPoUDP packets.
errors	Enables logging of EAPoUDP packet errors.
events	Enables logging of EAPoUDP session events.
packets	Enables logging of debugging messages about EAPoUDP packet information.
sm	Enables logging of debugging messages about EAPoUDP state machine information.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the ASA records EAPoUDP session state changes and timer events, and generates a complete record of EAPoUDP header and packet contents in hexadecimal format.

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

Examples

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

```
hostname# debug eou events
hostname#
```

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

```
hostname# debug eou all
hostname#
```

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

```
hostname# no debug eou
hostname#
```

Related Commands

Command	Description
debug eap	Enables logging of EAP events to debug NAC messaging.
debug nac	Enables logging of NAC events.
eou initialize	Clears the resources assigned to one or more NAC sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC sessions.
show debug	Displays the current debugging configuration.

debug esmtp

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

debug esmtp [*level*]

no debug esmtp [*level*]

Syntax Description

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

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
hostname# debug esmtp
```

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 etherchannel

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

debug etherchannel [**all** | **error** | **event**]

no debug etherchannel [**all** | **error** | **event**]

Syntax Description

all	(Optional) Displays all EtherChannel information.
event	(Optional) Displays major EtherChannel events.
error	(Optional) Displays EtherChannel errors.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# debug etherchannel event
hostname# show debug
debug etherchannel event enabled
hostname#
```

Related Commands

Command	Description
show debug	Displays the current debugging 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

no debug fixup

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# debug fixup
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect *protocol*	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** | **cmd-exec** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdmp** | **rxip** | **switch** | **sync** | **tx** | **txdmp** | **txip** | **verify**}

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

Syntax Description

cable	Failover LAN status or serial cable status.
cmd-exec	**failover exec** command execution trace.
fail	Failover internal exception.
fmsg	Failover message.
ifc	Network interface status trace.
open	Failover device open.
rx	Failover message receive.
rxdmp	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.
txdmp	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:

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

Command History

Release	Modification
7.0(1)	This command was modified to include additional debugging 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 is sample output from the **debug fover cmd-exec** command. After debugging is enabled, a **failover exec** command is entered. The results of the **failover exec** command are shown after the debugging output.

```
hostname(config)# debug fover cmd-exec

fover event trace on

hostname(config)# failover exec mate show running-config failover

ci/console: Sending cmd: show runn failovero to peer for execution, seq = 4
ci/console: frep_execv_cmd: replicating exec cmd: show runn failover...
fover_parse: Fover rexec response: seq=4, size=228, data="fail..."
ci/console: Fover rexec waiting at clock tick 2670960
fover_parse: Fover rexec ack: seq = 4, ret_val = 0
ci/console: Fover rexec conteinuer at clock tick: 2671040
ci/console: Fover exec succeeded, seq = 5

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover key *****
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

Related Commands

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

debug fsm

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

debug fsm [*level*]

no debug fsm

Syntax Description

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

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables FSM debugging messages. The **show debug** command indicates that FSM debugging 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 the current debugging configuration.

debug ftp client

To show debugging messages for FTP, use the **debug ftp client** command in privileged EXEC mode. To disable the display of debugging 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 level to display debugging messages. The range of values is between 1 and 255. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To see the current debugging command settings, enter the **show debug** command. To disable the debugging message output, enter the **no debug** command. To stop all debugging 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 debugging 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 the FTP client configuration.

debug generic

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

debug generic [*level*]

no debug generic

Syntax Description

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

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables miscellaneous debug messages. The **show debug** command indicates that miscellaneous debugging 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 the current debugging 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	Displays debugging information on errors encountered while processing the GTP message.
event	Displays debugging information on GTP events.
ha option	Debugs information on GTP HA events.
parser	Displays debugging 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		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example enables debugging messages 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 ASA.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the ASA.
timeout h225 | h323	Configures the 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

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

Defaults

The default for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug http** command displays detailed information about HTTP traffic. The **no debug all** or **undebug all** command turns off all enabled **debug** commands.

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 ASA.
http-proxy	Configures an HTTP proxy server.
http redirect	Redirects HTTP traffic to HTTPS.
http server enable	Enables the ASA HTTP server.

debug http-map

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

debug http-map

no debug http-map

Defaults

The default value for the debugging level is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example enables debugging 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.