



database path through debug xml Commands

Cisco ASA 5580 Adaptive Security Appliance Command Reference

database path

To specify a path or location for the local CA server database, use the **database** command in CA server configuration mode. To reset the path to flash memory, the default setting, use the **no** form of this command.

[no] database path mount-name directory-path

Syntax Description	<i>directory-path</i> Specifies the path to a directory on the mount point where the CA files are stored.							
	mount-name	Specifies t	he mount na	ne.				
Defaults	By default, the CA server database is stored in flash memory.							
Command Modes	The following tabl	le shows the m	odes in whic	h you can enter	the comma	ind:		
			Firewall N	lode	Security (Context		
				- .		Multiple		
	Command Mode	instion	Kouted	Iransparent	Single	Context	System	
			•		•			
Command History	Release Modification							
	8.0(2) This command was introduced.							
Usage Guidelines	The local CA files PKCS12 files, and mount command	stored in the o the current C used to specify	latabase inclu RL file. The y a file syster	ide the certificat <i>mount-name</i> is t n for the security	e database, he same as y appliance	user database the <i>name</i> argu 2.	files, temporary ment for the	
Note	These CA files are	e internal store	d files and sh	ould not be mo	dified.			
Examples	The following exa database files dire hostname(config) hostname(config-	mple defines t ctory on the m # crypto ca -ca-server)# -ca-server)#	he mount poi nount point as server database pa	nt for the CA da ca_dir/files_dir th cifs_share	ntabase as c : ca_dir/fi:	cifs_share. It al les_dir/	so defines the	

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows the user to configure and manage a local CA.
crypto ca server user-db write	Writes the user information configured in the local CA database to disk.
debug crypto ca server	Shows debug messages when the user configures the local CA server.
mount	Makes Common Internet File System (CIFS) and/or File Transfer Protocol (FTPFS) file systems accessible to the security appliance
show crypto ca server	Displays the characteristics of the CA configuration on the security appliance.
show crypto ca server cert-db	Displays the certificates issued by the CA server.

ddns (DDNS-update-method)

To specify a DDNS update method type, use the **ddns** command in DDNS-update-method mode. To remove an update method type from the running configuration, use the **no** form of this command.

ddns [both]

no ddns [both]

Syntax Description	both(Optional) Specifies updating to both the DNS A and PTR resource records (RRs).							
Defaults	Update only A RRs.							
Command Modes	The following table show	s the modes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	DDNS-update-method	•		•	•			
Command History	Release Modification							
	7.2(1)	This command was	introduced.					
Usage Guidelines	Dynamic DNS (DDNS) updates the name to address and address to name mappings maintained by DNS. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the security appliance supports the IETF method in this release.							
	Name and address mapping	ngs are contained in	two types of rea	source reco	ords (RR):			
	• The A resource recor	d contains domain r	name to IP addre	ess mapping	gs.			
	• The PTR resource red	cord contains IP add	lress to domain	name mapp	ings.			
	DDNS updates can be use	ed to maintain consi	stent informatio	n between	the A and PTR	RR types.		
	When issued in DDNS-up update is just to A RR, or	odate-method config to both A RR and I	uration mode, th PTR RR.	he ddns co	mmand defines	whether the		
Examples	The following example contained ddns-2:	onfigures updating t	o both the A and	d PTR RRs	for the DDNS	update method		
	hostname(config)# ddns update method ddns-2 hostname(DDNS-update-method)# ddns both							

Related Commands	Command	Description			
	ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.			
	ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.			
	dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.			
	dhcpd update dns	Enables a DHCP server to perform DDNS updates.			
	interval maximum	Configures the maximum interval between update attempts by a DDNS update method.			

ddns update (interface configuration)

To associate a dynamic DNS (DDNS) update method with a security appliance interface or an update hostname, use the **ddns update** command in interface configuration mode. To remove the association between the DDNS update method and the interface or the hostname from the running configuration, use the **no** form of this command.

ddns update [method-name | **hostname** hostname]

no ddns update [method-name | **hostname** hostname]

Syntax Description	hostname Specifies that the next term in the command string is a hostname							
-,	hostname	Specifies a hostna	me to be used for	r updates.	g 10 u 1100u			
	method-name Specifies a method name for association with the interface being configured.							
Defaults	No default behavior or va	lues.						
Command Modes	The following table shows the modes in which you can enter the command:							
		Firewall	Mode	Security (Context			
			_		Multiple	Multiple		
	Command Mode	Routed	Transparent	Single	Context	System		
	Interface configuration	•		•	•			
Command History	Release Modification							
	7.2(1) This command was introduced.							
Usage Guidelines	After defining a DDNS update method, you must associate it with a security appliance interface to trigger DDNS updates.							
	A hostname could be a Fully Qualified Domain Name (FQDN) or just a hostname. If just a hostname, the security appliance appends a domain name to the hostname to create a FQDN.							
Examples	The following example associates the interface GigabitEthernet0/2 with the DDNS update method named ddns-2 and the hostname hostname1.example.com:							
	hostname(config)# interface GigabitEthernet0/2 hostname(config-if)# ddns update ddns-2 hostname(config-if)# ddns update hostname hostname1.example.com							

Related Commands

Command	Description
ddns (DDNS-update- method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update method (global configuration mode)

To create a method for dynamically updating a DNS resource records (RRs), use the **ddns update method** command in global configuration mode. To remove a dynamic DNS (DDNS) update method from the running configuration, use the **no** form of this command.

ddns update method *name*

no ddns update method name

Syntax Description	on <i>name</i> Specifies the name of a method for dynamically updating DNS records								
Defaults	No default behavior or value	s.							
Command Modes	The following table shows the	ne modes in whic	h you can enter	the comma	nd:				
		Firewall M	lode	Security C	ontext				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Global configuration	•		•	•				
Command History	Release Modification								
	7.2(1) This command was introduced.								
Usage Guidelines	DDNS updates the name to address and address to name mappings maintained by DNS. The update method configured by the ddns update method command determines what and how often dynamic DNS updates are performed. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the security appliance supports the IETF method in this release.								
	Name and address mappings are contained in two types of resource records (RR):								
	• The A resource record contains domain name to IP address mappings.								
	• The PTR resource record	d contains IP add	ress to domain i	name mapp	ings.				
•	DDNS updates can be used t	o maintain consi	stent informatio	n between t	the A and PTR	RR types.			
<u>Note</u>	Before ddns update method dns command with domain l	l will work, you ookup enabled o	must configure and the interface.	a reachable	default DNS s	erver using the			
Examples	The following example confi	gures the DDNS	update method	named ddn	s-2:				

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 dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.		
	dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.		
	dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.		
	interval maximum	Configures the maximum interval between update attempts by a DDNS update method.		

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 | common | internal | vpn [level]]

no debug aaa

Syntax Description	accounting (Ontional) Show debug messages for accounting only						
oyntax booonprion	authentication	(Optional) Show d	ebug messages f	or authenti	cation only.		
	authorization	(Optional) Show d	ebug messages f	or authoriz	ation only.		
	common	(Optional) Show debug messages for different states within the AAA feature.					
	internal	(Optional) Show d database only.	ebug messages f	or AAA fur	ictions support	ed by the local	
	level	(Optional) Specifie	es the debug leve	el. Valid wi	th the vpn key	word only.	
	vpn	(Optional) Show d	ebug messages f	for VPN-rel	ated AAA fund	ctions only.	
Defaults	The default <i>level</i> is 1.						
Command Modes	The following table sl	hows the modes in whic	ch you can enter	the comma	nd:		
		Firewall N	/lode	Security C	ontext		
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release	Modification					
	7.0(1)	This command wa	s modified to inc	clude new k	eywords.		
Usage Guidelines	The debug aaa comm undebug all comman	and displays detailed is ds turn off all enabled o	nformation abou debugs.	t AAA acti	vity. The no de	ebug all or	
Examples	The following examp	le enables debugging fo	or AAA function	s supported	by the local d	atabase:	
	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	Displays running configuration related to AAA.
	aaa	

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	(Option transfe	(Optional) Displays runtime information about processing of chunked transfer encoded packets.						
	event	(Option	nal) Display	s debug informa	tion about p	oacket inspecti	on events.		
	eventverb	(Option to an e	nal) Display vent	s the action take	n by the sec	curity applianc	e in response		
	regex	regex (Optional) Displays information about matching patterns with predefined signatures.							
Defaults	All options are ena	bled by defaul	lt.						
Command Modes	The following table	e shows the mo	odes in whic	h you can enter	the comma	nd:			
			Firewall N	lode	Security Context				
						Multiple	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 appfw debug all or undel	The debug appfw command displays detailed information about HTTP application inspection. The no debug all or undebug all commands turn off all enabled debug commands.							
Examples	The following example enables the display of detailed information about application inspection:								
	hostname # debug a	ıppfw							
Related Commands	Commands	Descri	ption						
	http-map	Define	s an HTTP r	nap for configur	ing enhance	ed HTTP inspe	ection.		
	inspect http	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:

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

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

Examples The following example enables debug messages for ARP: hostname# debug arp

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

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:

	Firewall M	ode	Security Co	ntext	
				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 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) Specifie	es the debug leve	el.		
Defaults	The default <i>level</i> is 1.					
Command Modes	The following table sh	nows the modes in which	ch you can enter	the comma	ind:	
		Firewall N	Node	Security (Context	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•	•	•
Command History	Release	Modification				
	7.0(1)	This command wa debug asdm histo	s changed from t ry command.	the debug J	odm history co	ommand to the
Usage Guidelines	Because debugging ou unusable. For this reas troubleshooting sessio during periods of lowe likelihood that increas	Itput is assigned high p son, use debug comma ns with Cisco technical er network traffic and f ed debug command pr	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	PU process, oleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problem is best to use d ng these perio ct system use.	he system s or during ebug commands ds decreases the
Examples	The following exampl	e enables level 1 debug n history	gging of ASDM:			
	debug asdm history (hostname#	enabled at level 1				
Related Commands	Command	Description				
	show asdm history	Displays the conte	nts of the ASDN	1 history bu	ıffer.	

debug auto-update

To display auto-update client and server debugging information, use the **debug auto-update** command in privileged EXEC mode. To disable the display of auto-update client and server debugging information, use the **no** form of this command.

debug auto-update client | server [level]

no debug auto-update client | server [level]

Syntax Description	client	The au	ito-update cli	ent.				
	level	<i>level</i> (Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set this parameter to a higher number.						
	server The Auto Update server.							
Defaults	The default value for	r <i>level</i> is 1.						
Command Modes	The following table	shows the m	odes in whic	h you can enter	the comma	ind:		
			Firewall M	lode	Security Context			
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•		•	
	<u> </u>							
Command History	Release Modification							
	8.0(2)		ommand was	introduced.				
Usage Guidelines	Because debugging ounusable. For this re	output is ass ason, use de	igned high p bug commar	riority in the CP ads only to troub	U process, leshoot sp	it can render the cific problems	he system s or during	
	troubleshooting sess during periods of lov likelihood that increa	ions with Cis wer network ased debug (sco technical traffic and fe command pro	support staff. M ewer users. Debu ocessing overhea	oreover, it ugging duri ad will affe	is best to use d ng these period ct system use.	ebug commands ds decreases the	
Examples	The following examp auto-update comma	ple enables a and indicates	uto-update c that auto-up	lient and server date client and s	debugging server debu	messages. The gging message	e show debug es are enabled.	
	hostname# debug au hostname# debug au hostname# show deb debug auto-update debug auto-update	to-update o to-update s ug auto-upd client enak server enak	client server date oled at leve	el 1 el 1				

Related Commands	Command	Description
	show debug auto	Displays the current auto-update debugging configuration.

debug boot-mem

To display boot memory debugging information, use the **debug boot-mem** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug boot-mem [*level*]

no debug boot-mem [level]

Syntax Description	<i>level</i> (Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set this parameter to a higher number.							
Defaults	The default value for <i>level</i>	is 1.						
Command Modes	The following table shows	the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•		•		
Command History	Release Modification							
	8.0(2)	This command was	s introduced.					
Usage Guidelines	Because debugging output unusable. For this reason, troubleshooting sessions w during periods of lower ne likelihood that increased d	is assigned high p use debug comman ith Cisco technical twork traffic and for ebug command pro-	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	U process, bleshoot sp foreover, it agging duri ad will affe	it can render the ecific problems is best to use d ing these period for system use.	he system s or during ebug commands ds decreases the		
Examples	The following example ena command indicates that be hostname# debug boot-me debug boot-mem enabled hostname# show debug bo debug boot-mem enabled	ables boot memory oot memory debugg m at level 1 ot-mem at level 1	debugging mes ing messages ar	sages. The e enabled.	show debug b	oot-mem		

Related Commands

Command	Description
show debug boot	Displays the current boot memory debugging configuration.

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	<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 level is 1.								
Command Modes	The following table sh	nows the modes in whic	h you can enter	the comma	ind:				
		Firewall N	lode	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 comman	ids might slow down tra	ffic on busy net	works.					
Examples	The following example enables debug messages for context management:								
	nostname# debug con	text							
Related Commands	Command	Description							
	context	Creates a security of configuration mode	context in the sy	stem config	guration and er	iters context			
	show context	Shows context info	rmation.						
	show debug	Shows all enabled debuggers.							

debug boot-mem

To display boot memory debugging information, use the **debug boot-mem** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug boot-mem [level]

no debug boot-mem [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 this parameter to a higher number.							
Defaults	The default value for <i>lev</i>	vel is 1.							
Command Modes	The following table show	ws the modes in whic	ch you can enter	the comma	ind:				
		Firewall N	lode	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 outp unusable. For this reason troubleshooting sessions during periods of lower likelihood that increased	out is assigned high p n, use debug comman with Cisco technical network traffic and f l debug command pr	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	U process, bleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problems is best to use d ng these period ct system use.	he system s or during ebug commands ds decreases the			
Examples	The following example of command indicates that hostname# debug boot- debug boot-mem enable hostname# show debug debug boot-mem enable	enables boot memory boot memory debugg mem d at level 1 boot-mem d at level 1	debugging mes ging messages ar	sages. The e enabled.	show debug b	oot-mem			

Related Commands

Command	Description
show debug boot	Displays the current boot memory debugging configuration.

debug cplane

To show debug messages about the control plane that connects internally to an SSM, use the **debug cplane** command in privileged EXEC mode. To stop showing debug messages for the control plane, use the **no** form of this command.

debug cplane [level]

no debug cplane [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 sho	ows the modes in whic	h you can enter	the comma	and:				
		Firewall N	lode	Security Context					
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	_	•			
Command History	Release Modification								
Usage Guidelines	Using debug command	s might slow down tra	affic on busy net	works.					
Examples	The following example hostname# debug cpla	enables debug messa; ne	ges for the contr	ol plane:					
Related Commands	Command	Description							
	hw-module module recover	Recovers an intelli server.	gent SSM by loa	ading a reco	overy image fro	om a TFTP			
	hw-module module reset	Shuts down an SSM	A and performs	a hardware	reset.				
	hw-module module Reloads the intelligent SSM software. reload								

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

debug 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	messages	(Optional) Shows only debug messages for PKI input and output messages.								
	transactions	(Option	(Optional) Shows only debug messages for PKI transactions.							
	<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 highe	er number. L	evel 1 (the defau	ult) shows 1	nessages only	when errors			
		occur. Levels	Level 2 show 4 and up sh	ws warnings. Le	formation f	s informational	messages.			
			T und up sh		Iormation I		, , , , , , , , , , , , , , , , , , ,			
Defaults	By default, this com	nand shows	all debug m	essages. The def	ault level i	s 1.				
Command Modes	The following table s	shows the mo	odes in whic	h you can enter	the comma	nd:				
			Firewall N	lode	Security C	Context				
						Multiple				
	Command Mode		Routed Transpa	Transparent	Single	Context	System			
	Privileged EXEC		•	•	•	•	—			
Command History	Release Modification									
-	Preexisting	This co	ommand was	s preexisting.						
Usage Guidelines	Using debug comma	nds might sl	ow down tra	uffic on busy net	works.					
Examples	The following example enables debug messages for PKI:									
	hostname# debug grunto ca									
	· · · · · · · · · · · · · · · · · · ·	-								
Related Commands	Command	Descri	ption							
	debug crypto engin	e Shows	debug mess	ages for the cry	oto engine.					
	debug crypto ipsec	Shows	debug mess	ages for IPSec.						
	debug crypto isakmp Shows debug messages for ISAKMP.									

debug crypto ca server

To set the local CA server debug message level and begin listing associated debug messages, use the **debug crypto ca server** command in ca server configuration mode. To stop listing all debug messages, use the **no** form of the command.

debug crypto ca server [level]

no debug crypto ca server [level]

Syntax Description	<i>level</i> Sets the debug message level to display, the range of values is between 1 and 255.									
Defaults	The default debug level is 1.									
Command Modes	The following table shows the	ne modes in whic	ch you can enter	the comma	ind:					
		Firewall N	lode	Security (Context					
					Multiple					
	Command Mode	Routed	Transparent	Single	Context	System				
	CA server configuration	•		•						
	Global configuration	•		•						
	Privileged EXEC	•		•						
Command History	Release Modification									
	8.0(2) Th	is command was	s introduced.							
Usage Guidelines	Using debug commands mig raw data dumps and should b	ht slow down tra be avoided durin _i	ffic on busy netw g normal debugg	vorks. Leve jing becaus	ls 5 and higher e of excessive	are reserved for debug output.				
Examples	The following example sets	the debug level t	o 3:							
	hostname(config-ca-server hostname(config-ca-server	c)# debug crypt c)#	o ca server 3:							
	The following example turns off all debugging:									
	hostname(config-ca-server hostname(config-ca-server	c)# no debug cr c)#	ypto ca server							

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list (CRL) distribution point (CDP) to be include in the certificates issued by the CA.
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
database path	Specifies a path or location for the local CA server database.
show crypto ca server	Displays the characteristics of the certificate authority configuration on the security appliance in ASCII text format.
show crypto ca server certificate	Displays the local CA configuration in base64 format.
show crypto ca server crl	Displays the current CRL of the local CA.

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 sho	ows the modes in whic	h you can enter	the comma	and:				
		Firewall N	lode	Security (Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•				
Command History	ReleaseModification7.0This command was introduced.								
Usage Guidelines	Using debug command	ls might slow down tra	iffic on busy net	works.					
Examples	The following example enables debug messages for the crypto engine:								
	hostname# debug cryp	to engine							
Related Commands	Command	Description							
	debug crypto ca	Shows debug mess	ages for the CA						
	debug crypto ipsec	Shows debug mess	ages 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 default is 1. To dis a higher number.	e debug message splay additional r	level to dis nessages at	splay, between t higher levels,	1 and 255. The set the level to			
Defaults	The default level is 1.								
Command Modes	The following table sh	ows the modes in whi	ch you can enter	the comma	and:				
		Firewall I	Node	Security (Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•					
		·							
Command History	Release Modification								
	Preexisting This command was preexisting.								
Usage Guidelines	Using debug command	ds might slow down tr	affic on busy net	works.					
Examples	The following example enables debug messages for IPSec								
	hostname# debug crypto ipsec								
Related Commands	Command	Description							
	debug crypto ca	Shows debug mes	sages for the CA						
	debug crypto engine	Shows debug mes	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	timers	(Optional) Shows debug messages for ISAKMP timer expiration.							
Defaults	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. 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. The default level is 1.								
Command Modes	The following table sho	ws the modes in whic	ch you can enter	the comma	nd:				
		Firewall N	Node	Security C	ontext				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•					
Command History	Release Modification								
-	Preexisting This command was preexisting.								
Usage Guidelines	Using debug command	s might slow down tra	affic on busy net	works.					
Examples	The following example enables debug messages for ISAKMP:								
	hostname# debug crypt	co isakmp							
Related Commands	Command	Description							
	debug crypto ca	Shows debug mess	ages for the CA.						
	debug crypto engine	Shows debug mess	ages for the cryp	oto engine.					
	debug crypto ipsec	Shows debug mess	ages 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 s	shows the modes in whic	h you can enter	the comma	ind:				
		Firewall N	lode	Security (Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•				
Command History	Release Modification								
	Preexisting	This command was	s preexisting.						
Usage Guidelines	To see the current del enter the no debug co command.	bug command settings, e ommand. To stop all deb	nter the show do ug messages fro	e bug comm m being dis	ıand. To stop th splayed, enter t	ne debug output, he no debug all			
<u> </u>	Enabling the debug c	ctiqbe command may sl	ow down traffic	on busy ne	tworks.				
Examples	The following examp inspection:	The following example enables debug messages at the default level (1) for CTIQBE application inspection:							
	hostname# debug ct	hostname# debug ctigbe							
Related Commands									

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

service

debug ctl-provider

To show debug messages for Certificate Trust List providers, use the **debug ctl-provider** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug ctl-provider [errors | events | parser]

no debug ctl-provider [errors | events | parser]

Syntax Description	errors	Specifies CTL provider error debugging.						
	events	Specifies CTL provider event debugging.						
	parser	Specifies CTL pro	vider parser deb	ıgging.				
Defaults	No default behavior	r or values.						
Command Modes	The following table shows the modes in which you can enter the command:							
		Firewall N	/lode	Security Context				
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	—		
Command History	Release Modification							
	8.0(2) This command was introduced.							
Usage Guidelines	Using debug comm	ands might slow down tra	affic on busy net	works.				
Examples	The following example enables debug messages for CTL provider:							
	hostname# debug ctl-provider							
Related Commands	Command	Description						
	ctl	Parses the CTL file from the CTL client and install trustpoints.						
	ctl-provider	Configures a CTL	Configures a CTL provider instance in CTL provider mode.					
	export	Specifies the certificate to be exported to the client						

Specifies the port to which the CTL provider listens.

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 debug messages, use the **no** form of this command.

debug dap {errors | trace}

no debug dap [errors | trace]

Syntax Description	errors	errors Specifies DAP processing errors.					
	trace	Specifies a DA	AP function tr	ace.			
Defaults	No default va	lue or behaviors.					
Command Modes	The following	g table shows the r	nodes in whic	h you can enter	the comma	nd:	
			Firewall N	lode	Security C		
						Multiple	
	Command Mo	de	Routed	Transparent	Single	Context	System
	Privileged EX	KEC	•	•	•		
Command History	Release Modification						
	8.0(2)This command was introduced.						
Usage Guidelines	The high prio debug comma technical supp traffic and few command pro	rity assigned to de inds only to trouble port staff. Moreove wer users. Debugg cessing overhead	bugging outp eshoot specifi er, it is best to ing during the will affect sys	ut can render the c problems or de use debug com se periods decre tem use.	e system ur uring troub mands duri eases the lik	usable. For the leshooting sess ng periods of l celihood that in	is reason, use sions with Cisco lower network ncreased debug
Examples	The following	g example shows h	low to enable	DAP trace debug	gging:		
	hostname # d hostname #	ebug dap trace.					
Related Commands	Command		Desc	ription			
	dynamic-acc	ess-policy-record	l Crea	tes a DAP recor	l.		

debug ddns

L

To show debug messages for DDNS, use the **debug ddns** command in privileged EXEC mode. To disable debug 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 N	Firewall Mode		Security Context		
		Transparent	Single	Multiple		
Command Mode	Routed			Context	System	
Privileged EXEC	•		•	•		

Release Modification 7.2(1) This command was introduced.

Usage Guidelines The **debug ddns** command displays detailed information about DDNS. The **undebug ddns** turns off DDNS debugging information as does the **no debug ddns** command.

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 debug 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 security appliance 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.							
	<i>level</i> (Optional) Specifies the debug level. Valid values range from 1 to 255.								
	packet	Displa	ys packet inf	formation that is	associated	with the DHC	P client.		
Defaults	The default debug le	vel is 1.							
Command Modes	The following table a	shows the mo	odes in whic	h you can enter	the comma	nd:			
			Firewall M	ode	Security C	ontext			
						Multiple			
	Command Mode		Routed	Transparent	Single	Context	System		
	Privileged EXEC		•	<u> </u>	•	•			
Command History	Release Modification								
	Preexisting This command was preexisting.								
Usage Guidelines	Displays DHCP clier	nt debug info	ormation.						
	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 dh debug dhcpc detail	cpc detail enabled at	5 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 debug level. Valid values range from 1 to 255.								
	packet	Displa	iys packet in	formation that is	associated	with the DHC	P server.			
Defaults	The default debug lev	vel is 1.								
Command Modes	The following table s	shows the m	odes in whic	h you can enter	the comma	ind:				
			Firewall N	lode	Security (Context				
						Multiple				
	Command Mode		Routed	Transparent	Single	Context	System			
	Privileged EXEC		•	•	•	•	—			
Command History	Release Modification									
	Preexisting This command was preexisting.									
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 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, statistic, 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	<i>level</i> (Optional) Specifies the debug level. Valid values range from 1 to 255.									
Defaults	The default debug leve	el is 1.								
Command Modes	The following table sh	ows the mode	s in whic	h you can enter	the comma	nd:				
		F	irewall N	lode	Security C	ontext				
						Multiple				
	Command Mode	R	outed	Transparent	Single	Context	System			
	Privileged EXEC		•		•	•				
Command History	Palassa Madification									
oonnana motory	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 turns off DHCP and DDNS debugging information as does the no debug dhcpd ddns command.									
Because debugging output is assigned high priority in the CPU process, it can render the sy unusable. For this reason, use debug commands only to troubleshoot specific problems or o troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug during periods of lower network traffic and fewer users. Debugging during these periods de likelihood that increased debug command processing overhead will affect system use.										
Examples	The following example hostname# debug dhcg debug dhcpd ddns ena	e shows DHC od ddns abled at leve	P DDNS	debugging being	g enabled:					

Related Commands

Cisco ASA 5580 Adaptive Security Appliance Command Reference

Command	Description
dhcpd update dns	Enables a DHCP server to perform dynamic DNS 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 debug level. Valid values range from 1 to 255.							
	packet	Displa	iys packet inf	ormation that is	associated	with the DHC	P relay agent.		
Defaults	The default debug lo	evel is 1.							
Command Modes	The following table	shows the m	odes in whic	h you can enter	the comma	ind:			
			Firewall M	ode	Security C	Context			
						Multiple			
	Command Mode		Routed	Transparent	Single	Context	System		
	Privileged EXEC		•	—	•	•	—		
Command History	Release Modification								
	Preexisting	Preexisting This command was preexisting.							
Usage Guidelines Examples	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. 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 debug messages.							
	file-verbose	Enables verb	Enables verbose file-level disk debug messages						
	filesystem	filesystem Enables file system debug messages.							
	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 this parameter to a higher number.								
Defaults	The default value for	level is 1.							
Command Modes	The following table s	hows the modes ir	n which	you can enter	the comma	ind:			
		Fire	wall Mo	le	Security (Context			
	Command Mode					Multiple			
		Rout	ted	Transparent	Single	Context	System		
	Privileged EXEC	•		•	•		•		
Command History	Release Modification								
	7.0(1)	This comman	nd was in	ntroduced.					
Usage Guidelines	Because debugging o unusable. For this rea troubleshooting sessi during periods of low likelihood that increa	output is assigned h ason, use debug co ons with Cisco tech ver network traffic used debug comma	high pric ommand hnical su and few and proc	ority in the CP s only to troub upport staff. M er users. Debu essing overhea	U process, bleshoot sp oreover, it agging duri ad will affe	it can render t ecific problem is best to use d ng these perio ct system use.	he system s or during ebug commands ds decreases the		
Examples	The following examp that file-level disk de messages.	ole enables file-leve bugging messages	el disk d s are ena	ebugging mes bled. The dir	sages. The command o	show debug c causes several	ommand reveals debugging		
	hostname# debug di debug disk file en hostname# show deb u debug vpn-sessiondl	sk file abled at level 1 ug b enabled at le [.]	vel 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
       -rw- 5124096
                        14:42:27 Apr 04 2005 cdisk.binIFS: Opened: file flash:/ as fd 3
4
9
       -rw- 5919340
                        14:53:39 Apr 04 2005 ASDMIFS: Getdent: fd 3
                        15:18:56 Apr 21 2005 syslog
       drw- 0
11
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 debugging 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 [resolver | all] [level]

Syntax Description	all	(Defaul	(Default) Shows all messages, including messages about the DNS cache.						
	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.							
	resolver	(Option	al) Shows c	only DNS resolv	er message	S.			
Defaults	The default level is	1. If you do no	ot specify a	ny keywords, the	e security a	ppliance show	s all mesages.		
Command Modes	The following table	e shows the mo	des in whic	h you can enter	the comma	nd:			
			Firewall M	ode	Security C	ontext			
						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 comm	nands might slo	ow down tra	ffic on busy net	works.				
Examples	The following example enables debug messages for DNS: hostname# debug dns								
Related Commands	Command	Descrip	tion						
	class-map	Defines	the traffic	class to which to	apply sec	urity actions.			
	inspect dns	Enables	s DNS appli	cation inspectio	n.				
	policy-map	Associa	ites a class i	nap with specifi	ic security a	actions.			
	service-policy	Applies	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 debug 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	all Enables logging of debug messages about all EAP information.								
	errors	Enables logging of EAP packet errors.								
	events	Enables logging of EAP session events.								
	packets	Enable	es logging of	debug messages	s about EAF	Packet inform	nation.			
	sm	Enable	es logging of	debug messages	s about EAF	state machine	e information.			
Defaults	No default behavio	or or values.								
Command Modes	The following table	e shows the mo	odes in whic	h you can enter	the comman	nd:				
			Firewall M	lode	Security C	ontext				
						Multiple				
	Command Mode		Routed	Transparent	Single	Context	System			
	Privileged EXEC		•	•	•		•			
Command History	Release Modification									
	7.2(1)	This co	ommand was	introduced.						
Usage Guidelines	When you use this	command, the	e security app	liance records I	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	mple enables th	he logging of	f all EAP sessio	n events:					
	hostname# debug eap events hostname#									

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

hostname**# debug eap all** hostname**#**

The following example disables the logging of all EAP debug 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 current debug configuration.

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:

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

```
        Release
        Modification

        8.0(2)
        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 0.0.00 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 0.0.00
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.00 metric 4294967295/4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL: 0.0.00 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

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 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 behavio	ors or values.						
Command Modes	The following table	e shows the m	odes in whic	h you can enter	the comma	nd:		
			Firewall N	lode	Security C	ontext		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	—	•			
Command History	Release	Modifi	cation					
-	8.0(2)	This c	ommand was	s introduced.				
Usage Guidelines	Because debugging	g output is ass	igned high p	riority in the CP	U process.	it can render t	he system	
	unusable. For this is troubleshooting set of lower network the increased debug co	reason, use de ssions with Ci raffic and fewo command proce	bug command sco TAC. Mo er users. Det essing overhe	nds only to troub preover, it is bes pugging during the ead will affect sy	bleshoot spe t to use deb hese period ystem use.	ecific problems oug commands s decreases the	s or during during periods e likelihood that	
Examples	The following is sa a static neighbor bo	ample output f eing added, an	from the deb nd then remo	ug eigrp neighb ved, and the corr	oors static of responding	command. The debug messag	e example shows es.	
	hostname# debug eigrp neighbors static							
	EIGRP Static Neighbors debugging is on							
	hostname# config hostname(config) hostname(config-1 hostname(config-1	ure terminal router eigr router)# neig router)#	9 100 ghbor 10.86	.194.3 interfac	ce outside			
	EIGRP: Multicast	Hello is dis	sabled on E	thernet0/0!				

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]

hello (Optional) Limits the debug output to EIGRP hello packets. probe (Optional) Limits the debug output to EIGRP query packets. query (Optional) Limits the debug output to EIGRP query packets. request (Optional) Limits the debug output to EIGRP request packets. retry (Optional) Limits the debug output to EIGRP request packets. retry (Optional) Limits the debug output to EIGRP request 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 query packets. stub (Optional) Limits the debug output to EIGRP stuck in active query packets. stub (Optional) Limits the debug output to EIGRP stuck in active query packets. stub (Optional) Limits the debug output to EIGRP stuck in active reply packets. stub (Optional) Displays all EIGRP packets except hello packets. update (Optional) Outputs all packet debug messages. Verbose (Optional) Outputs all packet debug messages. Command Modes Firewall Mode Security Context Command Mode Routed Transparent Single Context System Privileged EXEC • • • <					coug output to E		Jackets.		
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 repusets packets. retry (Optional) Limits the debug output to EIGRP repuset packets. retry (Optional) Limits the debug output to EIGRP repusets packets. SIAquery (Optional) Limits the debug output to EIGRP retry packets. SIAquery (Optional) Limits the debug output to EIGRP stuck in active query packets. SIAquery (Optional) Limits the debug output to EIGRP stuck in active query packets. stub (Optional) Limits the debug output to EIGRP stuck in active reply packets. stub (Optional) Limits the debug output to EIGRP update packets. update (Optional) Limits the debug output to EIGRP stuck in active reply packets. verbose (Optional) Limits the debug output to EIGRP update 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 Mode Firewall Mode Security Context Vou can specify more than one packet type in a single command, for example: Vou can specify more than one packet type in a single c		hello	(Optional)	Limits the de	ebug output to E	IGRP hello	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 represented to EIGRP stuck in active query packets. SIAreply (Optional) Limits the debug output to EIGRP stuck in active query packets. SIAreply (Optional) Limits the debug output to EIGRP stuck in active query packets. Stub (Optional) Limits the debug output to EIGRP stuck in active query packets. stub (Optional) Limits the debug output to EIGRP stuck in active query packets. terse (Optional) Limits the debug output to EIGRP stuck in active query packets. update (Optional) Limits the debug output to EIGRP stuck in active query packets. verse (Optional) Limits the debug output to EIGRP stuck in active query packets. update (Optional) Limits the debug output to EIGRP stuck in active query packets. verse (Optional) Limits the debug output to EIGRP stuck in active query packets. update (Optional) Limits the debug output to EIGRP stuck routing packets. verbose (Optional) Outputs all packet debug messages. Command Mode Firewall Mode Firewall		probe	(Optional)	Limits the de	ebug output to E	IGRP prob	e 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. SIAreply (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 stuck in active reply packets. terse (Optional) Limits the debug output to EIGRP stuck in active reply packets. update (Optional) Limits the debug output to EIGRP stuck in active reply packets. verbose (Optional) Displays all EIGRP packets except hello packets. update (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: Endemode Routed Transparent Single Context Privileged EXEC • - - - - Command History Release Modification 8.0(2) This command was introduced. Jage Guidelines		query (Optional) Limits the debug output to EIGRP query 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. 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 stuck in active reply packets. stub (Optional) Limits the debug output to EIGRP stuck in active reply packets. update (Optional) Displays all EIGRP packets except hello packets. update (Optional) Displays all EIGRP packets except hello packets. update (Optional) Displays all packet debug messages. Defaults No default behaviors or values. Security Context Multiple Command Mode Privileged EXEC Pri		reply	reply (Optional) Limits the debug output to EIGRP reply 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 stuck in active reply packets. terse (Optional) Displays all EIGRP packets except hello packets. update (Optional) Outputs all packet debug output to EIGRP update packets. verbose (Optional) Outputs all packet debug messages. Defaults No default behaviors or values. Firewall Mode Security Context Command Modes Firewall Mode Privileged EXEC • • Privileged EXEC • • 3.0(2) This command was introduced. Jaage Guidelines		request (Optional) Limits the debug output to EIGRP request 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 stuck in active reply 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. The following table shows the modes in which you can enter the command: Command Mode Firewall Mode Privileged EXEC • Privileged EXEC • 8.0(2) This command was introduced. Jsage Guidelines You can specify more than one packet type in a single command, for example:		retry	(Optional) Limits the debug output to EIGRP retry 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) Displays all EIGRP packets except hello packets. verbose (Optional) Outputs all packet debug messages. Defaults No default behaviors or values. The following table shows the modes in which you can enter the command: Example Firewall Mode Verbage Exec • Privileged EXEC • Store		SIAquery	(Optional)	Limits the de	ebug output to E	IGRP stuck	c in active que	ry 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. The following table shows the modes in which you can enter the command: <u>Firewall Mode</u> Security Context Command Mode Routed Transparent Single Privileged EXEC • - - Release Modification 8.0(2) This command was introduced. Jsage Guidelines You can specify more than one packet type in a single command, for example:		SIAreply	(Optional)	Limits the de	ebug output to E	IGRP stuck	c in active repl	y 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. The following table shows the modes in which you can enter the command: Firewall Mode Security Context Command Mode Routed Transparent Single Context System Privileged EXEC • – • – – Zommand History Release Modification 8.0(2) This command was introduced.		stub	(Optional)	Limits the de	ebug output to E	IGRP stub	routing packet	s.	
update (Optional) Limits the debug output to EIGRP update packets. verbose (Optional) Outputs all packet debug messages. Defaults No default behaviors or values. The following table shows the modes in which you can enter the command: Example Firewall Mode Security Context Command Modes Firewall Mode Single Multiple Command Mode Routed Transparent Single Context System Privileged EXEC • - • - - Command History Release Modification Store of the command was introduced. You can specify more than one packet type in a single command, for example:		terse	(Optional)	Displays all	EIGRP packets	except hell	o 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: Firewall Mode Security Context Command Mode Routed Transparent Single Ornext System Privileged EXEC • Vou can specify more than one packet type in a single command, for example:		update	(Optional)	Limits the de	ebug output to E	IGRP upda	te packets.		
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 Multiple Command Mode Routed Transparent Single Context System Privileged EXEC • - • - - - Command History Release Modification - - - - Jsage Guidelines You can specify more than one packet type in a single command, for example: You can specify more than one packet type in a single command, for example:		verbose	(Optional)	Outputs all p	acket debug me	ssages.			
Command Mode Routed Transparent Single Multiple Privileged EXEC • — • — — Command History Release Modification — — — — Release Modification 8.0(2) This command was introduced. — — — Isage Guidelines You can specify more than one packet type in a single command, for example: You can specify more than one packet type in a single command, for example: Image: Command was introduced.		The following tab.	ie snows the m	odes in whic	h you can enter	the comma	nd:		
Command Mode Routed Transparent Single Context System Privileged EXEC • - • - - - Command History Release Modification Single Single Single Single Jsage Guidelines You can specify more than one packet type in a single command, for example: You can specify more than one packet type in a single command, for example: Image: Context in the single command in the single command.				odes in whic	h you can enter	the comma	nd:		
Command Mode Routed Fraisparent Single Context System Privileged EXEC • - • - - Command History Release Modification 8.0(2) This command was introduced.				odes in whic	h you can enter	the comma	nd: Context		
Privileged EXEC • - • -		Commond Mode		Firewall N	h you can enter	the comma	nd: Context Multiple	Simtom	
Release Modification 8.0(2) This command was introduced. Jsage Guidelines You can specify more than one packet type in a single command, for example:		Command Mode		odes in whic Firewall N Routed	h you can enter lode Transparent	the comma Security C Single	nd: Context Multiple Context	System	
Base Guidelines You can specify more than one packet type in a single command, for example:		Command Mode Privileged EXEC		Firewall N Routed •	h you can enter lode Transparent —	the comma Security C Single •	nd: Context Multiple Context —	System —	
Jsage Guidelines You can specify more than one packet type in a single command, for example:	Command History	Command Mode Privileged EXEC Release	Modifi	Firewall N Routed • cation	h you can enter lode Transparent 	the comma Security C Single •	nd: Context Multiple Context —	System —	
under the stage of the stage o	Command History	Command Mode Privileged EXEC Release 8.0(2)	Modifi This co	Firewall N Routed • cation ommand was	h you can enter lode Transparent 	the comma Security C Single •	nd: Context Multiple Context —	System —	
	Command History	Command Mode Privileged EXEC Release 8.0(2)	Modifi This co	Firewall N Routed • cation ommand was	h you can enter lode Transparent 	the comma Security C Single •	nd: Context Context Context —	System —	
debug eigrp packets query reply	Command History Usage Guidelines	Command Mode Privileged EXEC Release 8.0(2) You can specify m	Modifi This co	Firewall N Routed • cation ommand was	h you can enter lode Transparent 	the comma Security C Single •	nd: Context Context — —	System —	

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							
	build	(Optional) I	Build inform	nation messages	(messages	that indicate th	at a topology	
	deteil (Ontional) Additional detail for debug output							
	link	(Optional)]	Information	regarding topolo	ory table li	nked-list mana	gement	
	nacketize	(Optional)]	Information	regarding packe	tize events	inced list mana	gement.	
	peerdown	(Optional) I is down.	Information	regarding the im	pact on pa	cket generatior	when a peer	
	sia	(Optional) S	Stuck-in-act	ive messages.				
	startup	(Optional) I been transm	nformation	regarding peer st	artup and ir	nitialization pao	ckets that have	
	strange	(Optional)	Unusual eve	nts relating to pa	cket proce	ssing.		
Command Modes	The following tal	ple shows the mo	odes in whic	ch you can enter	the comma	nd: Context		
					•	Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC	2	•	_	•	_	_	
Command History	Release	Modifi	cation					
	8.0(2)This command was introduced.							
Usage Guidelines	You can specify 1	nore than one tr	ansmittal ev	ent in a single co	ommand, F	or example:		
	hostname# debug	eigrp ack bui	ld 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 argumer	nts 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			ontext	
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	_	•	_	—

```
        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 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

Cisco ASA 5580 Adaptive Security Appliance Command Reference

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 The default is 1. To to a higher number	debugging mess display additior	sage level to al message	o display, betw s at higher leve	een 1 and 255. ls, set the level
Defaults	The default value for <i>level</i>	l is 1.				
Command Modes	The following table shows	the modes in whic	h you can enter	the comma	ınd:	
		Firewall N	lode	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 unusable. For this reason, troubleshooting sessions w during periods of lower ne likelihood that increased c	t is assigned high p use debug commany with Cisco technical etwork traffic and for lebug command pro-	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	U process, oleshoot spo oreover, it ugging duri ad will affe	it can render the cific problems is best to use d ng these period ct system use.	he system 3 or during ebug commands ds decreases the
Examples	The following example ena that e-mail debugging mes hostname# debug email debug email enabled at hostname# show debug em debug email enabled at	ables e-mail debugg ssages are enabled. level 1 vail level 1	ging messages. T	he show do	e bug email cor	nmand indicates

Related Commands

Command	Description
show debug	Displays the current debug configuration.

debug entity

To display 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	<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 <i>leve</i>	<i>l</i> is 1.				
Command Modes	The following table show	s the modes in whic	h you can enter	the comma	nd:	
		Firewall N	lode	Security C	ontext	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•	•	•
Command History	Release	Modification				
	7.0	This command was	s introduced.			
Usage Guidelines	Because debugging outpu unusable. For this reason, troubleshooting sessions v during periods of lower no likelihood that increased o	it is assigned high p use debug comman with Cisco technical etwork traffic and for debug command pro-	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	U process, bleshoot spe foreover, it i ugging duri ad will affe	it can render the cific problems is best to use d ong these period ct system use.	he system s or during ebug commands ds decreases the
Examples	The following example er debug messages are enabl hostname# debug entity debug entity enabled a hostname# show debug debug entity enabled a hostname#	nables MIB debug n led. at level 1 at level 1	nessages. The sh	ow debug	command reve	als that MIB

Related Commands

Command	Description
show debug	Displays current debug 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 debug 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	s logging of	debug messages	s about all l	EAPoUDP info	ormation.
	eap	Enables	s logging of	debug messages	s about EA	PoUDP packet	s.
	errors	Enables	s logging of	EAPoUDP pack	cet errors.		
	events	Enables	s logging of	EAPoUDP sess	ion events.		
	packets	Enables	s logging of	debug messages	s about EA	PoUDP packet	information.
	sm	sm Enables logging of debug messages about EAPoUDP state machine					
		informa	ation.				
Defaults	No default behavior	or values.					
Command Modes	The following table	shows the mo	odes in whic	h you can enter	the comma	nd:	
			Firewall M	ode	Security Context		
						Multiple	
	Command Mode		Routed	Transparent	Single	Context	System
	Privileged EXEC		•	•	•		•
Command History	Release	Modific	cation				
	7.2(1)	This co	mmand was	introduced.			
Usage Guidelines	When you use this c events, and generate The high priority as debug commands or	command, the s a complete r signed to debu	security app ecord of EA ugging outpo shoot specifi	liance records E PoUDP header a ut can render the c problems or du	APoUDP s and packet c e system un uring troub	ession state ch contents in hexa usable. For thi leshooting sess	anges and timer adecimal format. is reason, use sions with Cisco
Examples	technical support sta traffic and fewer use command processin The following exam	aff. Moreover, ers. Debuggin g overhead wi aple enables th	, it is best to g during the ill affect sys ne logging of	use debug com se periods decre tem use. f all EAPoUDP	mands durn eases the like session eve	ng periods of l celihood that ir	lower network acreased debug
	hostname# debug eou events						

hostname#

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

hostname# **debug eou all** hostname#

The following example disables the logging of all EAPoUDP debug 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 current debug configuration.

debug esmtp

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

debug esmtp [level]

no debug esmtp [level]

Defaults The default value for level is 1. Command Modes The following table shows the modes in which you can enter the command: Image: Command Mode Firewall Mode Security Context Command Mode Routed Transparent Multiple Command Mode Routed Transparent Single Multiple Command History Release Modification Prexisting This command was prexisting. Usage Guidelines To see the current debug command settings, enter the show debug command. To stop the debug our enter the no debug command. To stop all debug messages from being displayed, enter the no debu command. Note Enabling the debug esmtp command may slow down traffic on busy networks. Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applicat inspection: hostname# debug esmtp	Syntax Description	level	(Optional) Sets the default is 1. To dis a higher number.	e debug message play additional 1	level to dis messages at	splay, between t higher levels,	1 and 255. The set the level to
Command Modes The following table shows the modes in which you can enter the command: Firewall Mode Security Context Command Mode Routed Transparent Single Context System Privileged EXEC •	Defaults	The default value for	level is 1.				
Firewall Mode Security Context Command Mode Routed Transparent Single Multiple Context System Privileged EXEC • • • - Command History Release Modification	Command Modes	The following table s	hows the modes in whic	ch you can enter	the comma	ınd:	
Command Mode Routed Transparent Single Multiple Privileged EXEC •			Firewall N	Node	Security (Context	
Command Mode Routed Transparent Single Context System Privileged EXEC •<						Multiple	
Privileged EXEC •		Command Mode	Routed	Transparent	Single	Context	System
Command History Release Modification Preexisting This command was preexisting. Usage Guidelines To see the current debug command settings, enter the show debug command. To stop the debug or enter the no debug command. To stop all debug messages from being displayed, enter the no debu command. Note Enabling the debug esmtp command may slow down traffic on busy networks. Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applicatinspection: hostname# debug esmtp		Privileged EXEC	•	•	•	•	—
Preexisting This command was preexisting. Usage Guidelines To see the current debug command settings, enter the show debug command. To stop the debug or enter the no debug command. To stop all debug messages from being displayed, enter the no debu command. Note Enabling the debug esmtp command may slow down traffic on busy networks. Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applications: hostname# debug esmtp	Command History	Release	Modification				
Usage Guidelines To see the current debug command settings, enter the show debug command. To stop the debug or enter the no debug command. To stop all debug messages from being displayed, enter the no debu command. Note Enabling the debug esmtp command may slow down traffic on busy networks. Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applications: hostname# debug esmtp		Preexisting	This command wa	s preexisting.			
Note Enabling the debug esmtp command may slow down traffic on busy networks. Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applications: hostname# debug esmtp	Usage Guidelines	To see the current deb enter the no debug co command.	oug command settings, o ommand. To stop all deb	enter the show d oug messages fro	ebug comm m being dis	nand. To stop tl splayed, enter t	ne debug output, The no debug all
Note Enabling the debug esmtp command may slow down traffic on busy networks. Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applications hostname# debug esmtp							
Examples The following example enables debug messages at the default level (1) for SMTP/ESMTP applications hostname# debug esmtp	Note	Enabling the debug e	smtp command may sl	ow down traffic	on busy ne	tworks.	
hostname# debug esmtp	Examples	The following examp inspection:	le enables debug messa	ges at the defaul	t level (1) f	for SMTP/ESM	ITP application
		hostname# debug esm	ntp				

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 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	•	•	•	•	_

Release Modification Preexisting This command was preexisting.

Usage Guidelines The debug fixup command displays detailed information about application inspection. The no debug all or undebug all commands turn 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 messag	e.				
	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 o	r values.					
Command Modes	The following table s	hows the modes in w	hich you can enter	the comma	nd:		
		Firewall Mode		Security Context			
					Multiple	Multiple	
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release	Modification					
-	7.0(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 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 is shown after the debug output.				
	hostname(config)# debug fover cmd-exec				
	fover event trace on				
	hostname(config)# failover exec mate show running-config failover				
	<pre>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</pre>				
	<pre>failover failover lan interface failover GigabitEthernet0/3 failover polltime unit 1 holdtime 3 failover key ***** failover link failover GigabitEthernet0/3 failover interface ip failover 10.0.5.1 255.255.0 standby 10.0.5.2 ciscoasa(config)#</pre>				

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	<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.				1 and 255. The set the level to		
Defaults	The default value for <i>level</i> is 1.						
Command Modes	The following table sh	ows the modes in whic	ch you can enter	the comma	ind:		
		Firewall Mode		Security Context			
			Transparent	Single	Multiple		
	Command Mode	Routed			Context	System	
	Privileged EXEC	•	•	•	•	•	
Command History	Release Modification						
	7.0 This command was introduced.						
Usage Guidelines	Because debugging ou unusable. For this reas troubleshooting session during periods of lowe likelihood that increase	tput is assigned high p on, use debug comman ns with Cisco technical r network traffic and for ed debug command pro-	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	PU process, bleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problema is best to use d ing these perior ct system use.	he system s or during ebug commands ds decreases the	
Examples	The following example debug messages are en hostname# debug fsm debug fsm enabled a hostname# show debug debug fsm enabled a hostname#	enables FSM debug m abled. It level 1 It level 1 It level 1	nessages. The sh	10w debug	command reve	eals that FSM	

Related Commands

Command	Description
show debug	Displays current debug configuration.
debug ftp client

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

debug ftp client [*level*]

no debug ftp client [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 this parameter to a higher number.							
Defaults	The default value for <i>la</i>	evel is 1.							
Command Modes	The following table she	ows the modes in whic	ch you can enter	the comma	ınd:				
		Firewall N	Node	Security (Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•				
					L.				
Command History	Release Modification								
	Preexisting	This command wa	s preexisting.						
Usage Guidelines	To view the current del debugging output, ente enter the no debug all	bugging command sett r the no debug comma command.	ings, enter the s and. To stop all d	how debug ebugging n	command. To nessages from	stop the being displayed,			
Note	Enabling the debug ftp	o client command ma	y slow down traf	fic on busy	networks.				
Examples	The following example hostname# debug ftp	The following example enables debugging messages at the default level (1) for FTP clients: nostname# debug ftp client							

Related Commands

Command	Description
сору	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 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	icription 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 a higher number.								
Defaults	The default value for <i>leve</i>	<i>l</i> is 1.							
Command Modes	The following table show	s the modes in whic	h you can enter	the comma	ind:				
		Firewall N	lode	Security Context					
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•	•			
	.								
Command History	Release Modification								
	7.0(1)	I his command was	s introduced.						
Usage Guidelines	Because debugging outpu unusable. For this reason, troubleshooting sessions v during periods of lower no likelihood that increased o	t is assigned high p use debug comman with Cisco technical etwork traffic and for debug command pro-	riority in the CP ads only to troub support staff. M ewer users. Debu ocessing overhea	U process, bleshoot spe foreover, it igging duri ad will affe	it can render the cific problems is best to use d ng these period ct system use.	he system s or during ebug commands ds decreases the			
Examples The following example enables miscellaneous debug messages. The show debug command miscellaneous debug messages are enabled. hostname# debug generic debug generic debug generic enabled at level 1 hostname# show debug debug debug generic enabled at level 1 hostname# show debug debug generic enabled at level 1 hostname# hostname#						and reveals that			

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 Displays debug information on errors encountered while processing the GTP message.								
	event	Displa	ys debug inf	ormation on GT	P events.				
	ha option	Debug	s information	n on GTP HA ev	vents.				
	parser	parserDisplays debug information for parsing the GTP messages.							
Defaults	All options are enal	bled by defaul	lt.						
Command Modes	The following table	shows the m	odes in whic	h you can enter	the comma	ınd:			
			Firewall M	lode	Security C	Context			
						Multiple			
	Command Mode		Routed	Transparent	Single	Context	System		
	Privileged EXEC		•	•	•	•			
Command History	Release Modification								
	7.0(1)	This co	ommand was	introduced.					
Usage Guidelines	The debug gtp com undebug all comm	mand display ands turn off	vs detailed in all enabled d	formation about ebug commands	: GTP inspe s.	ection. The no	debug all or		
Note	GTP inspection requires a special license.								
Examples	The following example enables the display of detailed information about GTP inspection:								
•	hostname# debug g	tp	i i i i			- I I			
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 {h225 | h245 | ras} [asn | event]

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

Syntax Description	h225 Specifies H.225 signaling.									
	h245	Specifi	es H.245 sig	naling.						
	ras	Specifi	es the registi	ration, admissio	n, and statu	is protocol.				
	asn	asn (Optional) Displays the output of the decoded protocol data units (PDU)s.								
	event	event (Optional) Displays the signaling events or turns on both traces.								
Defaults	No default behavior	or values.								
Command Modes	The following table	shows the mo	odes in which	h you can enter	the comma	nd:				
			Firewall M	ode	Security C	ontext				
						Multiple				
	Command Mode		Routed	Transparent	Single	Context	System			
	Privileged EXEC		•	•	•	•				
					·					
Command History	Release	Modifie	cation							
	Preexisting This command was preexisting.									
Usage Guidelines	To see the current de enter the no debug o command.	ebug comman command. To	d settings, er stop all debu	nter the show de ng messages fro	e bug comm m being dis	aand. To stop th splayed, enter t	ne debug output, he no debug all			
<u>Note</u>	Enabling the debug	h323 comma	and may slov	v down traffic o	n busy netv	works.				
Examples	The following exam hostname# debug h :	iple enables d 323 h225	ebug messag	es at the defaul	t level (1) f	for H.225 signa	lling:			

OL-12173-03

Command	Description
inspect h323	Enables H.323 application inspection.
show h225	Displays information for H.225 sessions established across the security appliance.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 h323	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	tion <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 defafult for <i>leve</i>	<i>el</i> is 1.						
Command Modes	The following table	shows the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	7.0	This command was	introduced.					
Usage Guidelines Examples	The debug http com undebug all comma The following exam	nmand displays detailed i nds turn off all enabled d ple enables the display of	nformation abou ebug commands detailed inform	nt HTTP tra 5. nation abou	uffic. The no d t HTTP traffic	ebug all or		
	hostname# debug ht	tp						
Related Commands	Commands	Description						
	http Specifies hosts that can access the HTTP server internal to the security appliance.							
	http-proxy	Configures an HTT	P proxy server.					
	http redirect	ttp redirect Redirects HTTP traffic to HTTPS.						

Enables the security appliance HTTP server.

http server enable

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:

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

Modification **Command History** Release 7.0(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

Relate

ed 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	level	evel (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 sho	ws the modes in whic	h you can enter	the comma	nd:				
		Firewall N	Firewall Mode		Context				
			-	o	Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•				
Command History	Release Modification								
	7.0This command was introduced.								
Usage Guidelines	The debug icmp comm undebug all commands	and displays detailed s turn off all enabled o	information abo lebugs.	out ICMP ir	spection. The	no debug all or			
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 c	onfiguration.						
	icmp	Configures access appliance interface	rules for ICMP	traffic that	terminates at a	security			
	show conn	show conn Displays the state of connections through the security appliance 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 group_id Displays IGMP debug information for the specified group.						
	interface <i>if_name</i>	Display IGMP deb	ug information f	for the spec	ified interface.		
Defaults	No default behavior or	values.					
Command Modes	The following table sh	ows the modes in whic	h you can enter	the comma	ind:		
		Firewall N	lode	Security Context			
					Multiple		
	Command Mode	Routed	Transparent	Single	Context	System	
	Privileged EXEC	•		•			
Command History	Release Modification						
	Preexisting This command was preexisting.						
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 samp	le output from the deb	ug igmp comma	und:			
	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: Undating 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 security appliance 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 default is 1. To disp a higher number.	debug message blay additional r	level to dis nessages a	splay, between t higher levels,	1 and 255. The set the level to		
Defaults	The default value for	level is 1.						
Command Modes	The following table s	shows the modes in whic	h you can enter	the comma	and:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
	Preexisting This command was preexisting.							
Usage Guidelines	To see the current del enter the no debug co command.	bug command settings, e ommand. To stop all deb	nter the show d o	e bug comn m being di	nand. To stop tl splayed, enter t	ne debug output, he no debug all		
Note	Enabling the debug i	ils command may slow o	lown traffic on b	ousy netwo	rks.			
Examples	The following examp hostname# debug il	ble enables debug messaş s	ges at the defaul	t level (1)	for ILS applica	tion inspection:		
Related Commands	Command	Description						
	class-map	Defines the traffic	class to which to	o apply sec	urity actions.			
	inspect ils	Enables ILS applic	ation inspection					

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

Related Commands

debug imagemgr

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

debug imagemgr [*level*]

no debug imagemgr

Syntax Description	level	(Optional) Sets the The default is 1. To parameter to a high	debugging mes o display additic ner number.	sage level t onal messag	o display, betw ges at higher le	veen 1 and 255. vels, set this
Defaults	The default value for <i>l</i>	evel is 1.				
Command Modes	The following table sh	ows the modes in whic	ch you can enter	the comma	and:	
		Firewall N	lode	Security (Context	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•	•	•
Command History	Release	Modification				
	7.0(1)	This command was	s introduced.			
Usage Guidelines	Because debugging ou unusable. For this reas troubleshooting session during periods of lowe likelihood that increase	tput is assigned high p on, use debug comman ns with Cisco technical r network traffic and for ed debug command pr	riority in the CF nds only to troul support staff. M ewer users. Deb ocessing overhe	PU process, oleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problem is best to use d ing these perio ect system use.	he system s or during ebug commands ds decreases the
Examples	The following example indicates that Image M hostname# debug imag debug imagemgr enak hostname# show debug debug imagemgr enak hostname#	e enables Image Manag lanager debugging mes pled at level 1 bled at level 1	ger debugging m ssages are enable	nessages. Ti ed.	he show debug	g command

Related Commands	Command	Description
	show debug	Displays the current debugging configuration.

debug inspect tls-proxy

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

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

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

Syntax Description	all	Specifi	es all TLS p	roxy debugging				
	errors	Specifi	es TLS prox	y error debuggi	ng.			
	events Specifies TLS proxy event debugging.							
	packets	Specifi	es TLS prox	y packet debugg	ging.			
							-	
Defaults	No default behavior	or values.						
Command Modes	The following table s	hows the mo	odes in whic	h you can enter	the comma	nd:		
			Firewall N	lode	Security C	Context		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•	•		
					1			
Command History	Release Modification							
	8.0(2)	This co	mmand was	introduced.				
Usage Guidelines	Using debug comma	nds might sl	ow down tra	ffic on busy net	works.			
Examples	The following example enables debug messages for TLS proxy:							
	hostname# debug in	spect tls-p	roxy					
	<u> </u>							
Related Commands	Command	Descrip					· · ·	
	client	Define	s a cipher su	ite and sets the lo	ocal dynam	ic certificate is	suer or keypair.	
	cti-provider	Define	s a CIL pro	vider instance ai	ia enters pi	rovider configu	iration mode.	
	show tis-proxy	Shows	the TLS pro	oxies.	1	· ·		
	tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.						

debug ip eigrp

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

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

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

Syntax Description	as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous						
	ip-addr mask	(Optional) I the IP addre	Limits debug	g output to messa ork mask.	iges that fal	l within the rat	nge defined by	
	neighbor nbr-addr	<i>r</i> (Optional) Limits debug output to the specified neighbor.						
	notifications	(Optional) Limits debug output to EIGRP protocol events and notifications.						
	summary	(Optional)	Limits debug	g output to summ	nary route p	processing.		
	user-interface	(Optional)	Limits debug	g output to user	events.			
Command Modes	The following table	shows the mo	odes in whic	h you can enter	the comma	nd:		
		Firewall Mode		Security C	Context			
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	—	•			
Command History	Release	Modifi	cation					
	8.0(2)	This co	ommand was	s introduced.				

Examples The following is sample output from the **debug ip eigrp** command: hostname# debug ip eigrp IP-EIGRP Route Events debugging is on EIGRP-IPv4(Default-IP-Routing-Table:1): Processing incoming UPDATE packet EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960 EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.0.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960 EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000 130560 SM 360960 - 256000 104960 EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.43.0 255.255.255.0, - do advertise out Ethernet0/1 EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.43.0 255.255.255.0 metric 371200 -256000 115200 EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.246.0 255.255.255.0, - do advertise out Ethernet0/1 EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.246.0 255.255.255.0 metric 46310656 -45714176 596480 EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.40.0 255.255.255.0, - do advertise out Ethernet0/1 EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.40.0 255.255.255.0 metric 2272256 -1657856 614400 EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.245.0 255.255.25.0, - do advertise out Ethernet0/1 EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.245.0 255.255.255.0 metric 40622080 -4000000 622080 EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.244.0 255.255.255.0, - do advertise out Ethernet0/1

Table 10-1 describes the significant fields shown in the display.

	Table 10-1	debua ip eiarp Field Descriptions
--	------------	-----------------------------------

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

Related Commands	Command	Description
	debug eigrp packets	Displays debug information for EIGRP packets.

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	<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 <i>level</i>	<i>l</i> is 1.						
Command Modes	The following table shows	s the modes in whic	ch you can enter	the comma	nd:			
		Firewall N	lode	Security C	ontext			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
	7.0 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 en that IPSec-over-TCP debu hostname# debug ipsec-o debug ipsec-over-tcp en hostname# show debug debug ipsec-over-tcp en hostname#	ables IPSec-over-T ng messages are ena over-tcp enabled at level i enabled at level i	°CP debug messa bled. 1	ages. The sl	now debug con	mmand reveals		

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 | mld | 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	Display	s debug inform	mation for IPv	6 interface	s.		
	mld	Display	s debug mess	ages for Multi	cast Listen	er Discovery (MLD).	
	nd	Display	s debug mess	ages for ICMI	v6 neighbo	or discovery tra	ansactions.	
	packetDisplays debug messages for IPv6 packets.							
	routing	Display updates	s debug mess.	ages for IPv6	routing tab	le updates and	route cache	
Defaults	No default behavio	or or values.						
Command Modes	The following table	e shows the mo	des in which	you can enter	the comma	nd:		
			Firewall Mod	le	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 unusable. For this troubleshooting ses during periods of 1 likelihood that incr	g output is assig reason, use deb ssions with Cisc ower network to reased debug co	gned high prio ug commands to technical su raffic and few ommand proce	rity in the CP s only to troub pport staff. M er users. Debu essing overhea	U process, leshoot spe oreover, it i ugging duri ad will affe	it can render the cific problems is best to use de ng these period ct system use.	ne system s or during e bug commands ds decreases the	
Examples	The following is sample output for the debug ipv6 icmp command:							
	amples Ine following is sample output for the debug ipvo 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 1 13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 1				.35 .36			

OL-12173-03

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

Command	Description
ipv6 icmp	Defines access rules for ICMP messages that terminate on a security appliance 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.
	Command ipv6 icmp ipv6 address ipv6 nd dad attempts ipv6 route

debug iua-proxy

To display 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 <i>level</i>	<i>l</i> is 1.						
Command Modes	The following table shows	s the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security C	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
	7.0 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 en IUA-proxy debug message hostname# debug iua-pro debug iua-proxy enable hostname# show debug debug iua-proxy enable hostname#	ables IUA-proxy de es are enabled. Ed at level 1 ed at level 1	ebug messages. '	The show d	lebug comman	d reveals that		

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 <i>leve</i>	<i>el</i> is 1.						
Command Modes	The following table show	rs the modes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security C	ontext			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
	7.0 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 e Kerberos debug message: hostname# debug kerber debug kerberos enable hostname# show debug debug kerberos enable hostname#	nables Kerberos deb s are enabled. o s d at level 1 d at level 1	ug messages. Th	ne show de	bug command	reveals that		

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug l2tp

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

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

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

Syntax Description	data displays data packet trace information.							
	error	Displa	ys error event	ts.				
	event	Displa	ys L2TP conr	nection events.				
	packet Displays packet trace information.							
	level	(Optio default a highe	nal) Sets the o t is 1. To disp er number.	debug message lay additional r	level to dis nessages at	play, between higher levels,	1 and 255. The set the level to	
Defaults	The default value fo	r <i>level</i> is 1.						
Command Modes	The following table	shows the m	odes in which	n you can enter	the comma	nd:		
			Firewall Mo	ode	Security C	ontext		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•	•	•	
Command History	Release Modification							
	7.2(1)	This co	ommand 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							
Examples	during periods of lower network traffic and fewer users. Debugging during these periods decrease likelihood that increased debug command processing overhead will affect system use. The following example enables L2TP debug messages for connection events. The show debug com- reveals that L2TP debug messages are enabled.					lebug command		
	hostname# debug hostname# show debug debug 12tp event enabled at level 1 hostname#							

Related Commands	Command	Description
	show debug	Displays current debug configuration.

debug Idap

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	<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 <i>le</i>	<i>vel</i> is 1.						
Command Modes	The following table sho	ws the modes in whic	h you can enter	the comma	nd:			
		Firewall N	lode	Security C	Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
	<u> </u>							
Command History	Release Modification							
	7.0(1) This command was introduced.							
Usage Guidelines	Because debugging outpunusable. For this reaso troubleshooting session during periods of lower likelihood that increase	put is assigned high p n, use debug comman s with Cisco technical network traffic and fo d debug command pro	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhea	PU process, bleshoot spe loreover, it ugging duri ad will affe	it can render the cific problems is best to use d ong these period ct system use.	he system s or during ebug commands ds decreases the		
Examples	The following example debug messages are ena hostname# debug ldap debug ldap enabled a hostname# show debug debug ldap enabled a hostname#	enables LDAP debug bled. at level 1 at level 1	messages. The s	show debu	g command rev	veals that LDAP		

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	<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 level is 1.								
Command Modes	The following table sh	nows the modes in whic	h you can enter	the comma	ind:				
		Firewall N	Firewall Mode			Security Context			
				Single	Multiple				
	Command Mode	Routed	Transparent		Context	System			
	Privileged EXEC		•	•	•				
Command History	Release Modification								
	7.0(1)This command was introduced.								
Usage Guidelines	Using debug command	ds might slow down tra	ffic on busy net	works.					
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.							

Command	Description
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 TAC.											
Syntax Description	This command should be used only under the supervision of Cisco TAC.										
Defaults	No default behavio	or or values.									
Command Modes	The following table	e shows the m ⁴	odes in which	n you can enter	the comma	nd:					
			Firewall Mode		Security Context						
						Multiple	Multiple				
	Command Mode		Routed	Transparent	Single	Context	System				
	Privileged EXEC		•	•	•	•	•				
Command History	Release Modification										
	7.0This 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	This command should be used only under the supervision of Cisco TAC.										
Related Commands	Command	Descri	Description								
	show debug	Displa	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** | **mrib** | **pak** | **ps** | **signal**} [group]

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

Syntax Description	db (Optional) Displays debug information for route database operations.								
_	group	(Option	nal) IP addre	ess of the multic	ast group.				
	init	(Option	nal) Display	s system initiali	zation activ	vity.			
	mrib	(Option	nal) Display	s debug informa	tion for con	mmunication v	vith MFIB.		
	pak	(Option	nal) Display	s debug informa	tion for pa	cket forwardin	g operations.		
	ps	(Optional) Displays debug information for process switching operations.							
	signal	(Option protoco	nal) Display ols.	s debug informa	tion for MI	FIB signaling t	to routing		
Defaults	No default behavio	or or values.							
Command Modes	The following tabl	e shows the mo	odes in whic	h you can enter	the comma	nd:			
			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 debuggin unusable. For this troubleshooting se during periods of I likelihood that inc	agging output is assigned high priority in the CPU process, it can render the system this reason, use debug commands only to troubleshoot specific problems or during ng sessions with Cisco technical support staff. Moreover, it is best to use debug commands is of lower network traffic and fewer users. Debugging during these periods decreases the at increased debug command processing overhead will affect system use.							
Examples	The following example displays MFIB dabase 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:

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

Release Modification 7.0(1) This command was introduced.

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

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

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 security appliance.
	show conn	Displays the connection state for different connection types.

Cisco ASA 5580 Adaptive Security Appliance Command Reference

debug module-boot

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

debug module-boot [*level*]

no debug module-boot [level]

Syntax Description	level (Optional) Sets the debugging message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set this parameter to a higher number.								
Defaults	The default <i>level</i> is 1.								
Command Modes	The following table sho	ows the modes in whic	h you can enter	the comma	ind:				
		Firewall N	lode	Security (Context				
					Multiple	ł			
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•		•			
Command History	Release Modification								
	7.0(1)This command was introduced.								
Usage Guidelines	Enabling the debug concommand settings, enter command. To stop all d	mmands may slow dov er the show debug cor lebugging messages fr	vn traffic on bus nmand. To stop om being displa	y networks the debugg yed, enter	.To view the cu ing output, ent the no debug a	arrent debugging er the no debug I l command.			
Examples	The following example enables debugging messages for the SSM booting process:								
	hostname # debug modu	hostname# debug module-boot							
	<u> </u>	B							
Related Commands	Command	Description							
	hw-module module recover	Recovers an intelli server.	gent SSM by loa	ading a rec	overy image fr	om a TFTP			
	hw-module module reset	Shuts down an SSM and performs a hardware reset.							

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

debug mrib

To display MRIB 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	client Enables debugging for MRIB client management activity.							
	io	Enable	s debugging	of MRIB I/O e	vents.				
	routeEnables debugging of MRIB routing entry activity.								
	group	group Enables debugging of MRIB routing entry activity for the specified group.							
	table	Enable	s debugging	of MRIB table	manageme	nt activity.			
Defaults	No default behavior	or values.							
Command Modes	The following table	shows the mo	odes in whic	h you can enter	the comma	nd:			
			Firewall N	lode	Security (Context			
						Multiple			
	Command Mode		Routed	Transparent	Single	Context	System		
	Privileged EXEC		•		•		—		
Command History	Release Modification								
	7.0(1)	7.0(1) This command was introduced.							
Usage Guidelines	Because debugging of unusable. For this re troubleshooting sess during periods of low likelihood that increa	output is assi ason, use de l ions with Cis wer network ased debug c	igned high p bug comman sco technical traffic and fo command pro	riority in the CP nds only to trout support staff. M ewer users. Deb ocessing overhe	PU process, bleshoot spo loreover, it ugging duri ad will affe	it can render t ecific problem is best to use d ng these perio ct system use.	he system s or during ebug commands ds decreases the		
Examples	The following examp hostname# debug mr IPv4 MRIB io debug	ple shows ho Fib io Fging is on	w to enable	debugging of M	IRIB I/O ev	ents:			

Related Commands

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

debug nac

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

debug nac {all | auth | errors | events}

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

Syntax Description	all Enables logging of debug messages about all NAC information.							
	auth	Enables logging of	debug message	es about NAC au	thenticatio	n requests and	responses.	
	errors	Enables logging of	NAC session e	rrors.				
	events	Enables logging of	NAC session e	vents.				
Defaults	No defau	lt behavior or values.						
Command Modes	The follo	owing table shows the	e modes in whic	h you can enter	the comma	ind:		
			Firewall N	lode	Security (Context		
						Multiple		
	Command Mode	d Mode	Routed	Transparent	Single	Context	System	
	Privilege	ed EXEC	•	•	•		•	
Command History	Release	Mo	dification					
•	7.2(1)	Thi	s command was	introduced.				
Usage Guidelines	When you use this command, the security appliance logs the following types of NAC events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.							
	The high priority assigned to debugging output can render the system unusable. For this reason, a debug commands only to troubleshoot specific problems or during troubleshooting sessions with technical support staff. Moreover, it is best to use debug commands during periods of lower netw traffic and fewer users. Debugging during these periods decreases the likelihood that increased d command processing overhead will affect system use.							
Examples	The following example enables the logging of all NAC session events:							
	hostname# debug nac events hostname#							

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

hostname**# debug nac all** hostname**#**

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

hostname# **no debug nac** hostname#

Relatedommands

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

debug ntdomain

To display NT domain authentication 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 <i>le</i>	evel is 1.						
Command Modes	The following table sho	ows the modes in whic	ch you can enter	the comma	und:			
		Firewall N	lode	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 out unusable. For this reaso troubleshooting session during periods of lower likelihood that increase	put is assigned high p on, use debug comman as with Cisco technical r network traffic and for ed debug command pro-	riority in the CP nds only to troub support staff. M ewer users. Debu ocessing overhes	U process, bleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problems is best to use d ing these perior ect system use.	he system s or during ebug commands ds decreases the		
Examples	The following example domain debug message hostname# debug ntdo debug ntdomain enab hostname# show debug debug ntdomain enab hostname#	enables NT domain de s are enabled. main led at level 1 led at level 1	ebug messages. T	The show d	ebug command	l reveals that NT		

Related Commands	Command	Description
	show debug	Displays current debug configuration.

debug ntp

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

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

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

Syntax Description	adjust	Shows	messages a	bout NTP clock a	adjustment	s.		-
	authentication	Shows	messages a	bout NTP authen	tication.			
	events	Shows messages about NTP events.						
	loopfilter Shows messages about NTP loop filter.							
	packetsShows messages about NTP packets.							
	params	Shows	messages a	bout NTP clock	parameters			
	select	Shows	messages a	bout NTP clock	selection.			
	sync	Shows	messages a	bout NTP clock	synchroniz	ation.		
	validity	Shows	messages a	bout NTP peer c	lock validit	ty.		
Defaults	No default behavior	or values.						
Command Modes	The following table s	shows the mo	odes in whic	ch you can enter	the comma	ind:		
		Firewall Mode			Security Context			
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	—
	Privileged EXEC		•	•	•	•		
								—
Command History	Release	Modific	cation					
	Preexisting	This co	mmand was	s preexisting.				
Usage Guidelines	Using debug comma	nds might slo	ow down tra	affic on busy net	works.			
Examples	The following examp	ple enables de	ebug messa	ges for NTP:				
	hostname# debug ntp events							

Related Commands Co

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

debug ospf

To display debug information about the OSPF routing processes, use the **debug ospf** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this 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	s the debugging of	of OSPF ad	ljacency events	5.		
	database-timer	(Optional) Enables	s the debugging of	of OSPF tir	ner events.			
	events	(Optional) Enables the debugging of OSPF events.						
	external	(Optional) Limits	(Optional) Limits SPF debugging to external events.					
	flood	(Optional) Enables	s the debugging of	of OSPF flo	ooding.			
	inter	(Optional) Limits	SPF debugging t	o inter-area	a events.			
	intra	(Optional) Limits	SPF debugging t	o intra-area	a events.			
	lsa-generation	(Optional) Enables	s the debugging of	of OSPF su	immary LSA g	eneration.		
	packet	(Optional) Enables	s the debugging of	of received	OSPF packets			
	retransmission	(Optional) Enables	s the debugging of	of OSPF re	transmission e	vents.		
	spf	(Optional) Enables	s the debugging of	of OSPF sh	ortest path firs	t calculations.		
	You can limit the SPF debug information by using the external , inter , and intra keywords.							
	tree	cee (Optional) Enables the debugging of OSPF database events.						
Defaults	Displays all OSPF del	oug information if no k	eyword is provid	led.				
Command Modes	The following table sl	nows the modes in which	ch you can enter	the comma	ınd:			
		Firewall N	Node	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	—	•				
Command History	Release	Modification						
	Preexisting	This command wa	s preexisting.					

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

Examples	The following is sample output from the debug ospf events command:					
	hostname# debug ospf events ospf event debugging is on					
	OSPF: hello with invalid timers on interface Ethernet0					

hello interval received 10 configured 10 net mask received 255.255.255.0 configured 255.255.255.0 dead interval received 40 configured 30

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

debug 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	<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 <i>leve</i>	<i>el</i> is 1.						
Command Modes	The following table show	rs the modes in whic	h you can enter	the comma	ınd:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release Modification							
oominana mistory	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 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#							

Related Commands	Command	Description
	show debug	Displays current debug configuration.

debug pim

To display PI M 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 group	(Optional) Displays debug information for the specified group. The value for <i>group</i> can be one of the following:				
		• 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:				
		• 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:

	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	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 technical support staff. Moreover, it is best to use debug comman 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:					
Examples	<pre>hostname# debug pim PIM: Received Join/Prune on Ethernet1 from 172.24.37.33 PIM: Received RP-Reachable on Ethernet1 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 Ethernet1 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 Ethernet1 PIM: Received Join/Prune on Ethernet1 from 172.24.37.6 PIM: Received Join/Prune on Ethernet1 from 172.24.37.33 PIM: Received Join/Prune on Ethernet1 from 172.24.37.33 PIM: Received Join/Prune on Ethernet1 from 10.3.84.1 PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1 PIM: Received Join/Prune on Ethernet1 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), 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: Frune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16 PIM: For RP, Prune-list: 10.9.0.0/16 PIM: For RP, Prune-list: 10.9.0.0/16 PIM: For RP, Prune-list: 10.49.0.0/16 PIM: For RP, Prune-list: 10.49.0.0/16 PIM: For RP, Prune-list: 10.440.0.0/16 PIM: For RP, Prune-list: 10.46.0.0/16 PIM: Fo</pre>					

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:

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage GuidelinesBecause 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 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:

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage GuidelinesBecause 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 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:

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

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

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 l	has no arguments	or keywords
--------------------	----------------	------------------	-------------

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

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

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 showpix 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:

	Firewall M	ode	Security Co	ntext	
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage GuidelinesBecause 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	<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 sl	hows the modes in whic	ch you can enter	the comma	ınd:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
Command History	Release Modification							
-	Preexisting	This command wa	s preexisting.					
Usage Guidelines	To see the current deb enter the no debug co command.	oug command settings, e ommand. To stop all deb	enter the show d e ug messages fro	e bug comn m being dis	nand. To stop t splayed, enter t	he debug output, the no debug all		
Note	Enabling the debug p	ptp command may slo	w down traffic o	n busy net	works.			
Examples	The following exampl hostname# debug ppt	le enables debug messaş P	ges at the default	t level (1) fo	or PPTP applic	ation inspection		
Related Commands	Command	Description						
	class-map	Defines the traffic	class to which to	o apply sec	urity actions.			
	inspect pptp	Enables PPTP app	lication inspection	on.				

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) S	Show RA	DIUS debuggi	ng message	es for a specifi	c user.
	username	Specifies the keyword on	e user w ly.	hose messages	you want t	o see. Valid wi	th the user
Defaults	No default behavior	or values.					
Command Modes	The following table	shows the modes i	in which	you can enter	the comma	nd:	
		Firewall Mode			Security Context		
						Multiple	
	Command Mode	Rou	ıted	Transparent	Single	Context	System
	Privileged EXEC	•		•	•	•	•
Command History	Release	Modification	n				
	Preexisting This command was preexisting.						
Usage Guidelines	The debug radius c security appliance an enabled debugs.	ommand displays nd a RADIUS AA	detailed A server.	information ab The no debug	out RADIU all or und o	JS messaging e bug all comm	between the ands turn off all
Examples	The following example shows decoded RADIUS messages, which happen to be accounting packets:						
	hostname(config)# hostname(config)#	debug radius de RADIUS packet de	code ecode (a	accounting rea	quest)		

```
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 (0x0000009)
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 (0x0000009)
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 (0x0000009)
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
```

Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x0000009)
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 security appliance.

debug redundant-interface

To show debug messages about redundant interfaces, use the **debug redundant-interface** command in privileged EXEC mode. To stop showing debug messages for redundant interfaces, use the **no** form of this command.

debug redundant-interface [level]

no debug redundant-interfac [level]

Syntax Description	cription level (Optional) Sets the debug message level to display, b default is 1. To display additional messages at higher a higher number.							
Defaults	The default level is 1.							
Command Modes	The following table sho	ws the modes in whic	h you can enter	the comma	and:			
		Firewall N	lode	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•		•		
		i.				ľ		
Command History	Release Modification							
	8.0(2)	This command was	s introduced.					
Usage Guidelines	Using debug command	s might slow down tra	affic on busy net	works.				
Examples	The following example	enables debug messa	ges for redundan	t interfaces	s:			
·	hostname# debug redur	dant-interface	-					
Related Commands	Command	Description						
	interface redundant	Creates a redundar	t interface.					
	member-interface	Assigns a physical	interface to a re	dundant in	terface.			
	redundant-interface	Changes the active	interface in a re	dundant in	terface pair.			
	show debug	Shows all enabled	debuggers.					

debug rip

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

debug rip [database | events]

no debug rip [database | events]

Syntax Description	database Displays RIP database events.								
	events	Displays R	Displays RIP processing events.						
Defaults	All RIP events are shown in the debug output.								
Command Modes	The following table shows the modes in which you can enter the command:								
			Firewall N	Firewall Mode		Security Context			
						Multiple			
	Command Mode)	Routed	Transparent	Single	Context	System		
	Privileged EXE	C	•		•	—			
Command History	Release Modification								
	Preexisting This command was preexisting.								
	7.2(1)The database and events keywords were added.								
Usage Guidelines	Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.								
Examples	The following is sample output from the debug rip command:								
	hostname# debug rip								
	<pre>RIP: broadcasting general request on GigabitEthernet0/1 RIP: broadcasting general request on GigabitEthernet0/2 RIP: Received update from 10.89.80.28 on GigabitEthernet0/1 10.89.95.0 in 1 hops 10.89.81.0 in 1 hops 10.89.66.0 in 2 hops 172.31.0.0 in 16 hops (inaccessible) 0.0.0.0 in 7 hops RIP: Sending update to 255.255.255.255 via GigabitEthernet0/1 (10.89.64.31)</pre>								

```
subnet 10.89.94.0, metric 1
172.31.0.0 in 16 hops (inaccessible)
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/2 (10.89.94.31)
subnet 10.89.66.0, metric 1
subnet 10.89.66.0, metric 3
172.31.0.0 in 16 hops (inaccessible)
default 0.0.0.0, metric 8
RIP: bad version 128 from 192.168.80.43
```

Related Commands	Command	Description			
	router rip	Configures a RIP process.			
	show running-config	Displays the RIP commands in the running configuration.			
	rip				

OL-12173-03

debug rtp

To display debug information and error messages for RTP packets associated with H.323 and SIP inspection, use the **debug rtp** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug rtp [level]

no debug rtp [level]

Syntax Description	<i>level</i> (Optional) Specifies an optional level of debug.								
Defaults	The default <i>level</i> is 1	1.							
Command Modes	The following table shows the modes in which you can enter the command:								
		Firewall N	Firewall Mode		Security Context				
			Transparent	Single	Multiple				
	Command Mode	Routed			Context	System			
	Privileged EXEC	•	•	•	•	—			
Command History	Release Modification								
	7.2(1) This command was introduced.								
Usage Guidelines	Because debugging of unusable. For this re troubleshooting sess during periods of low likelihood that incre	output is assigned high p ason, use debug comman ions with Cisco technical wer network traffic and for ased debug command pro-	riority in the CP ads only to troub support staff. M ewer users. Debu ocessing overhea	U process, bleshoot sp loreover, it ugging duri ad will affe	it can render t ecific problems is best to use d ng these period ct system use.	he system s or during ebug commands ds decreases the			
Examples	The following example shows how to enable debugging for RTP packets using the debug rtp command: hostname# debug rtp 255 debug rtp enabled at level 255								
Related Commands	Command	Description							
	policy-map	Creates a Layer 3/4	policy map.						
Command	Description								
-----------------------------------	---								
rtp-conformance	Checks RTP packets flowing on the pinholes for protocol conformance in H.323 and SIP.								
show running-config policy-map	Displays all current policy map configurations.								

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	<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	e level is 1.				
Command Modes	The following table s	shows the modes in whic	h you can enter	the comma	ınd:	
		Firewall N	lode	Security (Context	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•	•	
Command History	Release	Modification				
	Freexisting		s preexisting.			
Usage Guidelines	To see the current de enter the no debug co command.	bug command settings, e ommand. To stop all deb	nter the show d e ug messages fro	e bug comm m being dis	nand. To stop th splayed, enter t	ne debug output, he no debug all
Note	Enabling the dobug	rten command may slow	down traffic or	huev notu	orke	
NOLG		rtsp command may slov		I busy netw	/01K3.	
Examples	The following examp hostname# debug rt	ole enables debug messag sp	ges at the default	level (1) fo	or RTSP applic	ation inspection:
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 default is 1. To disp a higher number.	debug message play additional r	level to dis nessages at	play, between higher levels,	1 and 255. The set the level to
Defaults	The default value for <i>le</i>	<i>vel</i> is 1.				
Command Modes	The following table sho	ows the modes in whic	h you can enter	the comma	ınd:	
		Firewall N	lode	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 outpunusable. For this reaso troubleshooting session during periods of lower likelihood that increase	put is assigned high p on, use debug comman s with Cisco technical network traffic and fe d debug command pro	riority in the CP ads only to troub support staff. M ewer users. Debu ocessing overhes	U process, bleshoot sp foreover, it agging duri ad will affe	it can render the cific problems is best to use d ong these period ct system use.	he system s or during ebug commands ds decreases the
Examples	The following example messages are enabled. hostname# debug sdi debug sdi enabled at hostname# show debug debug sdi enabled at hostname#	enables SDI debug me = level 1 = level 1	ssages. The sho	w debug co	ommand reveal	s that SDI debug

Related Commands

Cisco ASA 5580 Adaptive Security Appliance Command Reference

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 default is 1. To disp a higher number.	debug message olay additional r	level to dis nessages at	splay, between t higher levels,	1 and 255. The set the level to
Defaults	The defaults are as fo • Debug message s	bllows: sequence numbers are dis	sabled.			
	• The default value	e for <i>level</i> is 1.				
Command Modes	The following table s	hows the modes in whic	h you can enter	the comma	and:	
		Firewall M	ode	Security (Context	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•	•	•
Command History	Release	Modification				
ooninana motory	7.0(1)	This command was	introduced.			
Usage Guidelines	Because debugging o unusable. For this rea troubleshooting sessio during periods of low likelihood that increa	utput is assigned high pr ason, use debug comman ons with Cisco technical er network traffic and fe sed debug command pro	iority in the CP ds only to troub support staff. M wer users. Debu ocessing overhea	U process, bleshoot sp loreover, it lgging duri ad will affe	it can render t ecific problems is best to use d ing these period ect system use.	he system s or during ebug commands ds decreases the
Examples	The following examp command enables CL configuration. The Cl hostname# debug seq debug sequence ena hostname# debug par debug parser cache	le enables sequence num I parser debug messages LI parser debug message guence abled at level 1 rser cache enabled at level 1	abers in debug n s. The show deb s shown include	nessages. T oug comma e sequence	The debug par s and reveals the numbers befor	ser cache current debug 'e each message.

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 session-command

To show debugging messages for a session to an SSM, use the **debug session-command** command in privileged EXEC mode. To stop showing debugging messages for a session to an SSM, use the **no** form of this command.

debug session-command [level]

no debug session-command [level]

Syntax Description	level	(Optional) Sets the The default is 1. To parameter to a high	debugging mes o display additio her number.	sage level t mal messag	o display, betw es at higher le	veen 1 and 255. vels, set this
Defaults	The default level i	is 1.				
Command Modes	The following tab	le shows the modes in whic	h you can enter	the comma	ind:	
		Firewall N	lode	Security (Context	
					Multiple	
	Command Mode	Routed	Transparent	Single	Context	System
	Privileged EXEC	•	•	•		•
Command History	Release	Modification				
	7.0(1)	This command was	s introduced.			
Usage Guidelines	Using debug com	mands might slow down tra	affic on busy net	works.		
Examples	The following exa	ample enables debugging m session-command	essages for a ses	ssion to an	SSM:	
Related Commands	Command	Description	-			
	session	Sessions to an SSM	1.			

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 [ha]

no debug sip [ha]

Syntax Description	ha	(Option	nal) Display	SIP Stateful Fai	ilover mess	sages.		
		When this keyword is used with the debug sip command on the active unit, debug messages are displayed when SIP state information is sent to the standby unit. When this keyword is used with the debug sip command on the standby unit, debug messages are displayed with state updates are received from the active unit.						
Defaults	No default behavio	r or values.						
Command Modes	The following table	e shows the mo	odes in whic	h you can enter	the comma	ind:		
			Firewall	lode	Security (Context		
						Multiple		
	Command Mode		Routed	Transparent	Single	Context	System	
	Privileged EXEC		•	•	•	•	—	
Command History	Release	Modifi	cation					
	Preexisting	This co	ommand was	s preexisting.				
	8.0(2)	The ha	i keyword w	as added.				
Usage Guidelines	To see the current of	lebug comman	ıd settings, e	nter the show d	e bug comm	nand. To stop th	ne debug output,	
-	enter the no debug command.	enter the no debug command. To stop all debug messages from being displayed, enter the no debug all command.						
	Because debugging unusable. For this r troubleshooting ses of lower network tr	output is assi eason, use del ssions with Cis raffic and fewe	igned high p bug comman sco TAC. Mo er users. Deb	riority in the CP nds only to troub preover, it is bes	U process, pleshoot spo t to use de l hese period	it can render the cific problems bug commands ls decreases the	he system s or during during periods e likelihood that	

increased debug command processing overhead will affect system use.

Examples The following is sample output from the **debug sip** command run on the active unit or failover group in a failover pair:

hostname# debug sip ha

SIP HA: Sending update SESSION message from faddr 10.132.80.120/5060 laddr 10.130.80.4/50295 Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From: sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120: State:1

SIP HA: msg sent to peer successful Version: 1 Action: update Object: session

SIP HA: Sending update TX message from faddr 10.132.80.120/5060laddr 10.130.80.4/50295CSeq 101 INVITEState Transaction Calling

The following is sample output from the **debug sip** command run on the standby unit or failover group in a failover pair:

hostname# **debug sip ha**

SIP HA: Message received from peer, Version: 1 Action: add Object: session

SIP HA: Created SIP session for faddr 10.132.80.120/5060 laddr 10.130.80.4/50295 Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From: sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120: 1 total

SIP HA: Message received from peer, Version: 1 Action: add Object: tx

SIP HA: Found an existing session faddr 10.132.80.120/5060 laddr 10.130.80.4/50295 Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From: sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:

SIP HA: Created SIP Transaction for faddr 10.132.80.120/5060 to laddr 10.130.80.4/50295CSeq 101 INVITEState Transaction Calling

Related Commands	Command	Description
	class-map	Defines the traffic class to which to apply security actions.
	inspect sip	Enables SIP application inspection.
	show conn	Displays the connection state for different connection types.
	show sip	Displays information about SIP sessions established through the security appliance.
	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	yntax Description level (Optional) Sets the debug message level to display, between 1 and 2 default is 1. To display additional messages at higher levels, set the a higher number.					1 and 255. The set the level to		
Defaults	The default value for <i>leve</i>	<i>l</i> is 1.						
Command Modes	The following table shows	s the modes in whic	h you can enter	the comma	ind:			
		Firewall N	lode	Security C	ontext			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•			
	.							
Command History	Release	Release Modification						
	Preexisting	This command was	s preexisting.					
Usage Guidelines	To see the current debug c enter the no debug comma command.	ommand settings, e and. To stop all deb	nter the show d e ug messages fro	ebug comm m being dis	and. To stop th splayed, enter t	ne debug output, he no debug all		
Note	Enabling the debug skinn	y command may s	low down traffic	c on busy ne	etworks.			
Examples	The following example en hostname# debug skinny	ables debug messag	es at the default	level (1) fo	r SCCP applic	ation inspection:		
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 security appliance.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug sla monitor

To display debug messages for the SLA monitor operation, use the **debug sla monitor** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sla monitor [error | trace] [sla-id]

no debug sla monitor [sla-id]

Syntax Description	error (Optional) Output IP SLA Monitor Error Messages.								
	sla-id	(Optional) The ID	of the SLA to de	ebug.					
	trace	(Optional) Output	IP SLA Monitor	Trace Mes	sages.				
Defaults	Both error and trace messages are shown by default.								
Command Modes	The following table show	ws the modes in whic	h you can enter	the comma	nd:				
		Firewall N	lode	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	Only 32 SLA operations can be debugged at one time.								
	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 SLA operation error debugging:								
	hostname(config)# deb	ug sla monitor erro	or						
	The following example shows how to display SLA operation trace messages for the specified SLA operation:								
	hostname(config)# debug sla monitor trace 123								

Related Commands	Command	Description	
	clear configure route	Removes statically of	
	clear route	Removes routes lear	

clear configure route	Removes statically configured route commands.
clear route	Removes routes learned through dynamic routing protocols such as RIP.
show route	Displays route information.
show running-config route	Displays configured routes.

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 s	shows the modes in whic	h you can enter	the comma	ınd:				
		Firewall N	lode	Security (Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•				
Command History	Release Modification								
	Preexisting	This command was	s preexisting.						
Usage Guidelines	To see the current del enter the no debug co command.	bug command settings, e ommand. To stop all deb	enter the show d o ug messages fro	e bug comm m being dis	nand. To stop th splayed, enter t	ne debug output, he no debug all			
Note	Enabling the debug sqlnet command may slow down traffic on busy networks.								
Examples	The following examp inspection: hostname# debug sq :	ile enables debug messa; Inet	ges at the defaul	t level (1) f	for SQL*Net a	pplication			
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	tion level (Optional) Specifies an optional level of debug. The default level is 1.						
Defaults							
Command Modes	The following table	e shows the mo	odes in whic	h you can enter	the comma	ind:	
			Firewall M	lode	Security C	Context	
						Multiple	
	Command Mode		Routed	Transparent	Single	Context	System
	Privileged EXEC		•	•	•	•	—
Command History	Release	Modifi	cation				
	Preexisting	This co	mmand was	preexisting.			
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.						he system s or during ebug commands ds decreases the
Examples	The following is sa	ample output fr	rom the deb	ug ssh 255 com	mand:		
	hostname# debug s debug ssh enable SSH2 0: send: ler SSH2 0: done calo SSH2 0: send: ler SSH2 0: done calo SSH2 0: done calo SSH2 0: done calo SSH2 0: done calo	ssh 255 ed at level 2 n 64 (include c MAC out #23 n 32 (include c MAC out #24 n 64 (include c MAC out #24 n 32 (include c MAC out #24 n 64 (include c MAC out #24 n 64 (include	55 s padlen 17 9 s padlen 7) 0 s padlen 16 2 s padlen 16 3 s padlen 18	7) 5) 5)			

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 #254SSH2 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 security appliance.
	ssh	Allows SSH connectivity to the security appliance from the specified client or network.

Cisco ASA 5580 Adaptive Security Appliance Command Reference

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	<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 <i>l</i>	evel is 1.							
Command Modes	The following table sh	ows the modes in whic	h you can enter	the comma	ind:				
		Firewall N	lode	Security C	Context				
					Multiple				
	Command Mode	Routed	Transparent	Single	Context	System			
	Privileged EXEC	•	•	•	•				
Command History	Release Modification								
commune motory	Preexisting This command was preexisting.								
Usage Guidelines	To see the current debu enter the no debug cor command.	ig command settings, e nmand. To stop all deb	nter the show d e ug messages fro	e bug comm m being dis	aand. To stop th splayed, enter t	ie debug output, ihe no debug all			
Note	Enabling the debug sunrpc command may slow down traffic on busy networks.								
Examples	The following example hostname# debug sunx	e enables debug messa; pe	ges at the defaul	t level (1) f	for RPC applic	ation inspection:			
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 switch ilpm

To show debug messages for models with a built-in switch, such as the ASA 5505 adaptive security appliance, show debug messages for PoE, use the **debug switch ilpm** command in privileged EXEC mode. To stop showing debug messages for PoE, use the **no** form of this command.

debug switch ilpm [events | errors] [level]

no debug switch ilpm [events | errors] [level]

Syntax Description	errors	(Optional) Shows troubleshooting information when there is an error.								
	events	(Optional) Shows PoE events.								
	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								
		a higher number.								
Defaults	By default, both events a	nd errors are shown	if you do not sp	ecify a key	word. The defa	ault level is 1.				
Command Modes	The following table shows the modes in which you can enter the command:									
		Firewall	Node	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	Using debug commands might slow down traffic on busy networks.									
Examples	The following example enables debug messages for PoE ports:									
	hostname# debug switch ilpm									
Related Commands	Command	Description								
	interface vlan	Adds a VLAN inte	erface.							
	debug switch manager	Shows debug mess	sages for VLAN	assignment	t and switchpo	ort				
		command-caused	events and errors							
	show debug	Shows all enabled debuggers.								

Cisco ASA 5580 Adaptive Security Appliance Command Reference

debug switch manager

To show debug messages for switch port models with a built-in switch, such as the ASA 5505 adaptive security appliance, show debug messages for VLAN assignment, and **switchport** command-caused events and errors, use the **debug switch manager** command in privileged EXEC mode. To stop showing debug messages for switch ports, use the **no** form of this command.

debug switch manager [events | errors] [level]

no debug switch manager [events | errors] [level]

Syntax Description	errors (Optional) Shows troubleshooting information when there is an error.									
	events	(Option	(Optional) Shows the switch manager events.							
	<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	By default, both even	ts and errors	s are shown	if you do not sp	ecify a key	word. The defa	ult level is 1.			
Command Modes	The following table s	hows the mo	odes in whic	h you can enter	the comma	ind:				
			Firewall M	lode	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	Using debug comman	nds might sl	ow down tra	ffic on busy net	works.					
Examples	The following example enables debug messages for switch ports:									
	hostname# debug switch manager									
Related Commands	Command	Descrip	ption							
	interface vlan	Adds a	VLAN inte	rtace.						
	debug switch ilpm	Shows	debug mess	ages for PoE.						
	show debug Shows all enabled debuggers.									

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	sion Displays session-related TACACS+ debug messages.						
	user	Displays user-spec TACACS+ debug	cific TACACS+ c messages for onl	lebug mess y one user	ages. You can at a time.	display		
	<i>username</i> Specifies the user whose TACACS+ debug messages you want to view.							
Defaults	No default behavior of	r values.						
Command Modes	The following table shows the modes in which you can enter the command:							
		Firewall I	Vode	Security (Context			
			_		Multiple			
	Command Mode	Routed	Iransparent	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 exampl TACACS+ debug mes hostname# debug taca debug tacacs user ac hostname#	e enables TACACS+ d sages are enabled. acs user admin342 g dmin342	ebug messages. T	Гhe show d	lebug comman	d reveals that		

Cisco ASA 5580 Adaptive Security Appliance Command Reference

Related Commands	Command	Description
	show debug	Displays current debug configuration.

debug tcp-map

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

debug tcp-map

no debug tcp-map

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0(1)	This command was introduced.

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

Examples The following example enables debug messages for TCP application inspection maps. The **show debug** command reveals that debug messages for TCP application inspection maps are enabled.

hostname# debug tcp-map
debug tcp-map enabled at level 1.
hostname# show debug
debug tcp-map enabled at level 1.
hostname#

Related Commands

Command	Description
show debug	Displays current debug configuration.

Cisco ASA 5580 Adaptive Security Appliance Command Reference

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	<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 defaults are as fol • Debug timestamp	lows: information is disabled.						
	• The default value	for <i>level</i> is 1.						
Command Modes	The following table sh	ows the modes in which	you can enter	the comma	ind:			
		Firewall Mo	ode	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 ou unusable. For this reas troubleshooting sessio of lower network traffi increased debug comn	tput is assigned high pri on, use debug command ns with Cisco TAC. Mon ic and fewer users. Debu nand processing overhea	ority in the CP ds only to troub reover, it is bes agging during t ad will affect sy	U process, bleshoot spo t to use del hese period ystem use.	it can render t ecific problems bug commands ls decreases the	he system s or during during periods e likelihood that		
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**

Command 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

Description
Displays current debug configuration.

Related Commands

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	<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 s	hows the modes in whic	ch you can enter	the comma	and:			
		Firewall N	Node	Security (Context			
					Multiple			
	Command Mode	Routed	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•	•	•		
Command History	Release	Modification						
Usage Guidelines	Because debugging o unusable. For this rea troubleshooting sessi of lower network traf	utput is assigned high p ison, use debug comman ons with Cisco TAC. Ma fic and fewer users. Deb	priority in the CP nds only to troub oreover, it is bes pugging during t	U process, bleshoot sp t to use de hese period	it can render t ecific problems bug commands ls decreases the	he system s or during s during periods e likelihood that		
Examples	The following examp reveals that VPN-sess hostname# debug vpn debug vpn-sessiondh hostname# show debu debug vpn-sessiondh hostname#	le enables VPN-session sion database debug mes 1-sessiondb o enabled at level 1 1g o enabled at level 1	database debug ssages are enable	messages. ed.	The show deb	ug command		

Cisco ASA 5580 Adaptive Security Appliance Command Reference

Command	Description
show debug	Displays current debug configuration.

debug wccp

To enable logging of WCCP events, use the **debug wccp** command in privileged EXEC mode. To disable the logging of WCCP debug messages, use the **no** form of this command.

debug wccp {events | packets | subblocks}

no debug wccp {events | packets | subblocks}

Syntax Description	events Enables logging of WCCP session events.							
	packets	Enables log	ging of o	lebug messages	s about WC	CP packet info	ormation.	
	subblocksEnables logging of debug messages about WCCP subblocks.							
Defaults	No default behavior of	r values.						
Command Modes	The following table sh	nows the modes	in which	you can enter	the comma	nd:		
		Fire	ewall Mo	ode	Security C	ontext		
						Multiple		
	Command Mode	Rou	ıted	Transparent	Single	Context	System	
	Privileged EXEC	•		•	•		•	
Command History	Release Modification							
	7.2(1)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 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 the logging of all WCCP session events:							
	hostname# debug wccp events hostname#							
	The following exampl	e enables the log	gging of	WCCP packet	debug mes	sages:		
	hostname# debug wccj hostname#	p packets						
	The following exampl	e disables the lo	gging of	WCCP debug	messages:			
	hostname# no debug wccp							

hostname#

Related Commands

;	Command	Description
wccp Enables support of WCCF		Enables support of WCCP.
	show debug	Displays current debug configuration.

debug webvpn

To log WebVPN debug messages, use the **debug webvpn** command in privileged EXEC mode. To disable the logging of WebVPN debug messages, use the **no** form of this command.

debug webvpn [chunk | cifs | citrix | failover | html | javascript | request | response | svc | transformation | url | util | xml] [*level*]

no debug webvpn [chunk | cifs | citrix | failover | html | javascript | request | response | svc | transformation | url | util | xml] [*level*]

Syntax Description	chunk	Displays debug messages about memory blocks used to support WebVPN connections
	cifs	Displays debug messages about connections between CIFS)servers and WebVPN users.
	citrix	Displays debug messages about connections between Citrix Metaframe Servers and Citrix ICA clients over WebVPN.
	failover	Displays debug messages about equipment failovers affecting WebVPN connections.
	html	Displays debug messages about HTML pages sent over WebVPN connections.
	javascript	Displays debug messages about JavaScript sent over WebVPN connections.
	request	Displays debug messages about requests issued over WebVPN connections.
	response	Displays debug messages about responses issued over WebVPN connections.
	svc	Displays debug messages about connections to SSL VPN clients over WebVPN.
	transformation	Displays debug messages about WebVPN content transformation.
	url	Displays debug messages about website requests issued over WebVPN connections.
	util	Displays debug messages about CPU utilization dedicated to support connections to WebVPN remote users.
	xml	Displays debug messages about JavaScript sent over WebVPN connections.
	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.

		Firewa	III Mode	Security (Context			
		_			Multiple			
	Command Mode	Route	Transparent	Single	Context	System		
	Privileged EXEC	•	•	•		•		
Command History	Release	Modification						
	7.0(1)	This command	was introduced.					
-	debug commands of TAC. Moreover, it is users. Debugging d processing overhead	only to troubleshoot sp is best to use debug co luring these periods de d will affect system us	ecific problems or d ommands during per creases the likeliho e.	uring troub riods of low od that incr	leshooting sest ver network tra eased debug c	sions with Cisco ffic and fewer ommand		
Examples	The following example enables WebVPN debug messages, specifically for CIFS. The show debug command reveals that CIFS debug messages are enabled.							
	hostname # debug w INFO: debug webvp hostname # show de debug webvpn cifs hostname #	rebvpn cifs on cifs enabled at l b bug s enabled at level 1	evel 1.					
Related Commands	Command	Description						
	show debug	Displays curre	nt debug configurati	on.				

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

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 <i>level</i> is 1.						
Command Modes	The following table s	shows the modes in whic	h you can enter	the comma	ınd:		
		Firewall M	Firewall Mode		Security Context		
	Command Mode		Transparent	Single	Multiple		
		Routed			Context	System	
	Privileged EXEC	•	•	•	•		
Command History	Release Modification						
	Preexisting This command was preexisting.						
Usage Guidelines	To see the current del enter the no debug co command.	bug command settings, e ommand. To stop all deb	enter the show d o	e bug comn m being dis	1and. To stop th splayed, enter t	ne debug output, he no debug all	
Note	Enabling the debug xdmcp command may slow down traffic on busy networks.						
Examples	The following examp inspection: hostname# debug xdm	ole enables debug messa, mcp	ges at the defaul	t level (1) f	or XDMCP ap	plication	
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.	
debug xml

To display debugging information for the XML parser, use the **debug xml** command in privileged EXEC mode. To disable the display of debugging information, use the **no** form of this command.

debug xml [element | event]

no debug xml [element | event]

Syntax Description	element	(Optional) Displays debugging events that are related to processing individual XML elements.					
	event (Optional) Displays XML parsing or error events.						
Defaults	If no keywords are specified, all XML parser debugging messages are shown.						
Command Modes	The following table shows the modes in which you can enter the command:						
		Firewall Mode		Security Context			
			Transparent	Single	Multiple		
	Command Mode	Routed			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 samp	le output from the deb	ug xml element	command:			
	hostname# debug xml element debug xml element enabled at level 1						
	<pre>XML Executes cmd: hostname hostname XML Executes cmd: domain-name example.com XML Executes cmd: names XML Executes cmd: dns-guard XML Executes cmd: ! XML Executes cmd: interface Ethernet0 XML Executes cmd: nameif outside XML Executes cmd: security-level 0</pre>						

```
XML Executes cmd: ip address 192.168.5.151 255.255.255.0 standby 192.168.5.152
XML Executes cmd: interface Ethernet1
XML Executes cmd: nameif inside
XML Executes cmd: security-level 100
XML Executes cmd: ip address 192.168.0.151 255.255.255.0 standby 192.168.0.152
XML Executes cmd: !
XML Executes cmd: boot system flash:/f
XML Executes cmd: ftp mode passive
XML Executes cmd: clock timezone jst 9
XML Executes cmd: dns server-group DefaultDNS
XML Executes cmd: domain-name cisco.com
_tcp_listen: could not query index for interface 65535 port 23
XML Executes cmd: pager lines 24
XML Executes cmd: logging console debugging
XML Executes cmd: logging buffered debugging
XML Executes cmd: mtu outside 1500
XML Executes cmd: mtu inside 1500
XML Executes cmd: failover
XML Executes cmd: no asdm history enable
XML Executes cmd: arp timeout 14000
XML Executes cmd: route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
XML Executes cmd: timeout xlate 3:00:00
XML Executes cmd: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
XML Executes cmd: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
XML Executes cmd: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
XML Executes cmd: timeout uauth 0:05:00 absolute
XML Executes cmd: username user1 password mb02jYs13AX1IAGa encrypted
XML Executes cmd: username sugi password EB3OP7Hu2hSu6x/7 encrypted
XML Executes cmd: http server enable
XML Executes cmd: http 0.0.0.0 0.0.0.0 outside
XML Executes cmd: no snmp-server location
XML Executes cmd: no snmp-server contact
XML Executes cmd: snmp-server enable traps snmp authentication linkup linkdown coldstart
XML Executes cmd: telnet timeout 5
XML Executes cmd: ssh timeout 5
XML Executes cmd: console timeout 0
XML Executes cmd: !
XML Executes cmd: class-map inspection_default
XML Executes cmd: match default-inspection-traffic
XML Executes cmd: !
XML Executes cmd: !
XML Executes cmd: policy-map type inspect dns migrated_dns_map_1
XML Executes cmd: parameters
XML Executes cmd: message-length maximum 512
XML Executes cmd: policy-map global_policy
XML Executes cmd: class inspection_default
XML Executes cmd:
                  inspect ftp
XML Executes cmd: inspect h323 h225
XML Executes cmd: inspect h323 ras
XML Executes cmd: inspect netbios
XML Executes cmd: inspect rsh
XML Executes cmd: inspect rtsp
XML Executes cmd:
                   inspect skinny
XML Executes cmd:
                   inspect esmtp
XML Executes cmd:
                    inspect sqlnet
XML Executes cmd:
                    inspect sunrpc
XML Executes cmd:
                   inspect tftp
XML Executes cmd:
                   inspect sip
XML Executes cmd:
                   inspect xdmcp
XML Executes cmd: !
XML Executes cmd: service-policy global_policy global
XML error info: cmd-id 87 type info
```

XML Executes cmd: prompt hostname context XML Executes cmd: crashinfo save disable The following is sample output from the debug xml event command: hostname# debug xml event debug xml event enabled at level 1

```
XML parsing: data = <con... len = 3176
Exit XML parser, ret code = 0
```

Related Commands	Command	Description	
	show debug	Displays the debugging status for the various debug commands.	

Cisco ASA 5580 Adaptive Security Appliance Command Reference