DES/3DES/AES VPN Encryption Module (AIM-VPN/EPII, AIM-VPN/HPII, AIM-VPN/BPII Family)

The DES/3DES/AES VPN Encryption Module (AIM-VPN/EPII, AIM-VPN/HPII, AIM-VPN/BPII Family) feature describes how to configure virtual private network (VPN) encryption hardware advanced integration modules (AIM) and network modules (NM) in Cisco IOS Release 12.3(7)T.

Feature Specifications for the VPN Encryption Module

Feature History	
Release	**Modification**
12.2(13)T	This feature was introduced on the Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This feature was introduced on the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.
12.3(5)	This feature was revised to include support for the AIM-VPN/EPII, AIM-VPN/HPII family of encryption modules and was integrated into Cisco IOS Release 12.3(5).
12.3(6)	This feature was revised to include support for the AIM-VPN/BPII-Plus on the 2600XM encryption modules and was integrated into Cisco IOS Release 12.3(6).
12.3(7)T	This feature was revised to include support for the AIM-VPN/BPII-Plus family of encryption modules and was integrated into Cisco IOS Release 12.3(7)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for DES/3DES/AES VPN Encryption Module

Installation Preconditions

- Cisco IOS Release 12.2(13)T or later.

Note See Table 1 for AIM/VPN Encryption Module support by Cisco IOS Release.

- A working IP network

For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*, Release 12.3.

Choice of Encryption Module

Determine which VPN encryption module to use, as described in Table 1.

Table 1 AIM/VPN Encryption Module Support by Cisco IOS Release

Platform	Encryption Module Support by Cisco IOS Release				
	12.2(13)T	12.3(4)T	12.3(5)	12.3(6)	12.3(7)T
Cisco 831	Software-based AES				
Cisco 1710 Cisco 1711 Cisco 1721 Cisco 1751 Cisco 1760	Software-based AES				
Cisco 2600 XM	—			AIM-VPN/BPII-Plus Hardware Encryption Module	
Cisco 2611 XM Cisco 2621 XM Cisco 2651 XM	—	AIM-VPN/BPII Hardware Encryption Module			AIM-VPN/BPII-Plus Hardware Encryption Module
Cisco 2691 XM	AIM-VPN/EPII Hardware Encryption Module				AIM-VPN/EPII-Plus Hardware Encryption Module

Table 1 AIM/VPN Encryption Module Support by Cisco IOS Release

Platform	Encryption Module Support by Cisco IOS Release				
	12.2(13)T	12.3(4)T	12.3(5)	12.3(6)	12.3(7)T
Cisco 3725	AIM-VPN/EPII Hardware Encryption Module		AIM-VPN/EPII-Plus Hardware Encryption Module		
Cisco 3660 Cisco 3745	AIM-VPN/HPII Hardware Encryption Module		AIM-VPN/HPII-Plus Hardware Encryption Module		

Restrictions for DES/3DES/AES VPN Encryption Module

- Rivest-Shamir-Adelman (RSA) manual keying is not supported.
- To achieve maximum benefit from hardware-assisted IP Payload Compression Protocol (IPPCP), it is suggested that prefragmentation be disabled if IP compression with the Limpel Zif Stac (LZS) algorithm is enabled on IP Security (IPSec) sessions.

How to Configure DES/3DES/AES VPN Encryption Module

There are no configuration tasks specific to the encryption hardware. Both software-based and hardware-based encryption are configured in the same way. The system automatically detects the presence of an encryption module at bootup and uses it to encrypt data. If no encryption hardware is detected, software is used to encrypt data.

Additional References

The following sections provide additional references pertaining to VPN Encryption Modules.

Related Documents

Related Topic	Document Title
Installation of VPN encryption modules	*Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*
ISDN configuration	Cisco IOS ISDN Voice Configuration Guide, Release 12.3
Cisco 2600 series	Cisco 2600 series routers documentation index on Cisco.com
Cisco IOS References	*Cisco IOS Security Configuration Guide*, Release 12.3 *Cisco IOS Security Command Reference*, Release 12.3

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
2401–2410	IPSec AH, ESP
2401–2411	IPsec/IKE
2401–2451	IPsec/IKE
AES (NIST)	Advanced Encryption Standard and The National Institute of Standards and Technology

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

- **clear crypto engine accelerator counter**
- **crypto engine accelerator**
- **show crypto engine**
- **show crypto engine accelerator statistic**
- **show crypto engine accelerator ring**
- **show diag**

clear crypto engine accelerator counter

To reset the statistical and error counters for a router's hardware accelerator to zero, use the **clear crypto engine accelerator counter** command in privileged EXEC mode.

clear crypto engine accelerator counter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII & AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example shows the router's statistical and error counters being cleared to zero:

```
Router# clear crypto engine accelerator counter
```

Related Commands

Command	Description
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.

Command	Description
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

crypto engine accelerator

To enable a router's onboard hardware accelerator for IPSec encryption, use the **crypto engine accelerator** command in global configuration mode. To disable the use of the onboard hardware IPSec accelerator, and thereby perform IPSec encryption/decryption in software, use the **no** form of this command.

crypto engine accelerator

no crypto engine accelerator

Syntax Description

This command has no arguments or keywords.

Defaults

The hardware accelerator for IPSec encryption is enabled.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(3)T	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPSec encryption.
12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII & AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command is not normally needed for typical operations because the router's onboard hardware accelerator for IPSec encryption is enabled by default. The hardware accelerator should not be disabled except on instruction from Cisco TAC personnel.

Examples

The following example shows how to enable the router's onboard hardware accelerator for IPSec encryption. This operation is normally needed only after the accelerator has been disabled for testing or debugging purposes.

```
Router(config)# no crypto engine accel

Warning! all current connections will be torn down.
Do you want to continue? [yes/no]:
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto engine

To displays a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

show crypto engine [**brief** | **configuration**]

Syntax Description

brief	Displays a summary of the configuration information for the crypto engine.
configuration	Displays the version and configuration information for the crypto engine.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

Examples

The following example of **show crypto engine brief** shows typical crypto engine information:

```
Router# show crypto engine brief

crypto engine name: Virtual Private Network (VPN) Module
crypto engine type: hardware

VPN Module in slot: 1
Product Name: AIM-VPN/EPII
Software Serial #: 55AA
Device ID: 0014
Vendor ID: 13A3
VSK revision: 0
Boot version: 255
DPU version: 0
HSP version: 2.0(0x0) (PRODUCTION)

Time running: 0 Seconds

Compression: Yes
DES: Yes
3 DES: Yes
AES CBC: Yes (128,192,256)
AES CNTR: No
Maximum buffer length: 4096
```

```
Maximum DH index: 2000
Maximum SA index: 2000
Maximum Flow index: 4000
Maximum RSA key size: 2048
crypto engine in slot: 1

crypto engine name: unknown
crypto engine type: software
serial number: 0DDC7C0D
crypto engine state: installed
crypto engine in slot: N/A
```

Table 2 describes significant fields shown in the display.

Table 2 show diag Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the key-name argument in the crypto key generate dss command.
crypto engine type	If "software" is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2). If "crypto card" or "ESA" is listed, the crypto engine is associated with an Encryption Service Adapter (ESA).
crypto engine state	The state "installed" indicates that a crypto engine is located in the given slot, but is not configured for encryption. The state "dss key generated" indicates the crypto engine found in that slot has DSS keys already generated.
crypto firmware version	Version number of the crypto firmware running on the ESA.
crypto lib version	Version number of the crypto library running on the router.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the Route Switch Processor (RSP).

Related Commands

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.

show crypto engine accelerator statistic

To display the statistics and error counters for a router's onboard hardware accelerator for IPSec encryption, use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPSec encryption.
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII & AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples

The following example shows typical output of the current statistics and error counters for the router's hardware accelerator:

```
Router# show crypto engine accelerator statistics

Virtual Private Network (VPN) Module in slot :0
        Statistics for Hardware VPN Module since the last clear
         of counters 1379 seconds ago
            167874 packets in                167874 packets out
         201596210 bytes in                201596059 bytes out
               121 paks/sec in                   121 paks/sec out
              1169 Kbits/sec in                 1169 Kbits/sec out
                 0 packets decrypted               0 packets encrypted
                 0 bytes before decrypt            0 bytes encrypted
                 0 bytes decrypted                 0 bytes after encrypt
                 0 packets decompressed            0 packets compressed
                 0 bytes before decomp             0 bytes before comp
                 0 bytes after decomp              0 bytes after comp
                 0 packets bypass decompr          0 packets bypass compres
                 0 bytes bypass decompres          0 bytes bypass compressi
                 0 packets not decompress          0 packets not compressed
                 0 bytes not decompressed          0 bytes not compressed
             1.0:1 compression ratio           1.0:1 overall
                20 commands out                   20 commands acknowledged
        Last 5 minutes:
```

```
     46121 packets in                  46121 packets out
       153 paks/sec in                   153 paks/sec out
   1667834 Kbits/sec in              1667836 Kbits/sec out
         0 bytes decrypted                 0 bytes encrypted
         0 Kbits/sec decrypted             0 Kbits/sec encrypted
     1.0:1 compression ratio           1.0:1 overall

Errors:
ppq full errors       :       0 ppq rx errors         :       0
cmdq full errors      :       0 cmdq rx errors        :       0
no buffer             :       0 replay errors         :       0
dest overflow         :       0 authentication errors :       0
Out of memory         :       0 Access denied         :       0
Out of handles        :       0 Bad function code     :       0
Invalid parameter     :       0 Bad handle value      :       0
Output buffer overrun :       0 Input Underrun        :       0
Input Overrun         :       0 Invalid Key           :       0
Invalid Packet        :       0 Decrypt Failure       :       0
Verification Fail     :       0 Bad Attribute         :       0
Invalid attrribute val:       0 Missing attribute     :       0
Unwrappable object    :       0 Hash Miscompare       :       0
DF Bit set            :       0 RNG self test fail    :       0
Other error           :       0
sessions              :       0

Warnings:
sessions_expired:0        packets_fragmented:0
general:         0
```

Note Command output for plus and non-plus VPN encryption modules is identical.

Table 3 describes significant fields shown in the display.

Table 3 show crypto engine accelerator statistic Field Descriptions

Counter	Description
packets in	Number of packets passed to the VPN module for either encryption or decryption.
packets out	Number of packets returned from the VPN module to IPSEC. This would include packets with errors.
bytes in	Number of payload bytes passed to the VPN Module. This does not include encryption header or trailer bytes.
bytes out	Number of payload bytes passed by the VPN Module. This does not include encryption header or trailer bytes.
packets decrypted	Number of packets passed to VPN module to be decrypted.
packets encrypted	Number of packets passed to VPN module to be encrypted.
bytes before decrypt	Number of payload bytes decrypted by the VPN Module, including encryption header and trailer bytes.
bytes encrypted	Number of payload bytes encrypted by the VPN Module. This does not include encryption header or trailer bytes.
bytes decrypted	Number of payload bytes decrypted by the VPN Module. This does not include encryption header or trailer bytes.

Table 3 show crypto engine accelerator statistic Field Descriptions

Counter	Description
bytes after encrypt	Number of payload bytes encrypted by the VPN Module, including encryption header and trailer bytes.
packets decompressed	Number of packets that were decompressed by the interface.
packets compressed	Number of packets that were compressed by the interface.
bytes before decomp	Number of payload bytes decompressed by the VPN Module, including encryption header and trailer bytes.
bytes before comp	Number of payload bytes decompressed by the VPN Module. Not including encryption header and trailer bytes.
bytes after decomp	Number of payload bytes compressed by the VPN Module. Not including encryption header and trailer bytes.
bytes after comp	Number of payload bytes compressed by the VPN Module, including encryption header and trailer bytes.
packets bypass decompr	Number of packets that were not decompressed by the compression algorithm on the originating router.
packets bypass compres	Number of packets that were not compressed by the compression algorithm because they were too short.
bytes bypass decompres	The Number of bytes in the payload that correspond to the number of bytes in packets bypass decompression.
bytes bypass compressi	Number of bytes in the packets that were not compressed by the originating router because they were too short.
packets not decompress	Number of bytes in the packets that were not decompressed by the compression algorithm on the originating router due to expansion.
packets not compressed	Number of packets that were not compressed because the packets were too short.
bytes not decompressed	The number of bytes in the packets that were counted in the bytes bypass decompresion counter.
bytes not compressed	The number of bytes in the packets that were counted in the packets not compressed counter.
compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm that were successfully compressed or decompressed. This statistic measures the efficiency of the algorithm for all packets that were compressed or decompressed.
overall	Ratio of compression and decompression of packets presented to the compression algorithm including those that were not compressed. This measures the compression efficiency of all packets on the tunnel.
commands out	The number of requests that have been made to the AIM-VPN card.
commands acknowledged	The number of responses that have been handled by the AIM-VPN card.

The following example shows typical output of the Cisco 2600 and Cisco 3600 VPN Modules. Note the current statistics, error counters, and associated error numbers that may be returned to the console:

```
Router# show crypto engine accelerator statistics

Hardware VPN0/2:
        ds: 0x81C96D98        idb:0x81C93C34
        Statistics for Encryption Module
                 0 packet overruns
                 0 packets in           0 packets out
                 0 paks/sec in          0 paks/sec out
                 0 packets decrypted    0 packets encrypted
                 0 bytes decrypted      0 bytes encrypted
                 0 bytes before decrypt 0 bytes after encrypt
                 0 Kbits/sec decrypted  0 Kbits/sec encrypted
        rx_no_endp:     0   rx_hi_discards:  0     fw_failure:         0
        invalid_sa:     0   invalid_flow:    0     cgx_errors          0
        fw_qs_filled:   0   fw_resource_lock:0     lotx_full_err:      0
        null_ip_error:  0   pad_size_error:  0     out_bound_dh_acc:   0
        esp_auth_fail:  0   ah_auth_failure: 0     crypto_pad_error:   0
        ah_prot_absent: 0   ah_seq_failure:  0     ah_spi_failure:     0
        esp_prot_absent:0   esp_seq_fail:    0     esp_spi_failure:    0
        obound_sa_acc:  0   invalid_sa:      0     out_bound_sa_flow:  0
        invalid_dh:     0   bad_keygroup:    0     out_of_memory:      0
        no_sh_secret:   0   no_skeys:        0     invalid_cmd:        0
        dsp_coproc_err: 0   comp_unsupported:0     pak_too_big:        0
        pak_mp_length_spec_fault: 0
        tx_lo_queue_size_max 0  cmd_unimplemented: 0
        858562 seconds since last clear of counters
        Interrupts: 142719745  Immed: 3         HiPri ints:  142696635
        LoPri ints: 27507     POST Errs: 0        Alerts: 1
        Unk Cmds: 0         UnexpCmds: 0
        cgx_cmd_pending:0   packet_loop_max: 0  packet_loop_limit: 0
```

Table 4 describes significant fields shown in the display.

Table 4 show crypto engine accelerator statistic Compression Statistics Descriptions for a Cisco 2600, Cisco 3600 or Cisco 3700 VPN module

Count Label	Significance	Associated Error Number
packet overruns	Number of packets passed to VPN module when VPN resources are all allocated. Packet is dropped.	—
packets in	Number of packets passed to VPN module for either encryption or decryption.	—
packets out	Number of packets returned from VPN module to IPSEC. This would include packets with errors.	—
paks/sec in	Total number of packets passed to VPN hardware/ number of seconds elapsed since last clear.	—
paks/sec out	Total number of packets returned to IPSEC from the VPN hardware/ number of seconds elapsed since last clear.	—
packets decrypted	Number of packets passed to VPN module to be decrypted.	—
packets encrypted	Number of packets passed to VPN module to be encrypted.	—
bytes decrypted	Number of payload bytes decrypted by the VPN Module. This does not include encryption header or trailer bytes.	—
bytes encrypted	Number of payload bytes encrypted by the VPN Module. This does not include encryption header or trailer bytes.	—

Table 4 show crypto engine accelerator statistic Compression Statistics Descriptions for a Cisco 2600, Cisco 3600 or Cisco 3700 VPN module

Count Label	Significance	Associated Error Number
bytes before decrypt	Total number of bytes in packets to be decrypted including encryption headers/trailers.	—
bytes after encrypt	Total number of bytes in encrypted packets including encryption headers/trailers.	—
Kbits/sec decrypted	Kilobits per second of payload bytes decrypted.	—
Kbits/sec encrypted	Kilobits per second of payload bytes encrypted.	—
rx_no_endp	Not used in Cisco 2600/3600 VPN.	—
rx_hi_discards	Number of packets discarded by the VPN Module. This can happen if a callback value is set, the output interface is NULL, or a packet has been received when the VPN Module is disabled.	1400 encryption not ready
fw_failure	—	4097 fatal firmware error
invalie_sa	—	4165 invalid sa
invalid_flow	Packet received for encryption decryption using an IPsec key that is invalid, for example, a session has expired or key is out of range.	4098 bad flow
cgx_errors	Not used in Cisco 2600/3600 VPN.	—
fw_qs_filled	Not used in Cisco 2600/3600 VPN.	4103 queue full
fw_resource_lock	Flow was deleted by IPSEC while VPN Module was processing the packet, or packet has a NULL Local Address, or packet does not have room for encapsulation headers	4104 resource swamp
lotx_full_err	Not used in Cisco 2600/3600 VPN.	4354 null ip
null_ip_error	Not used in Cisco 2600/3600 VPN.	—
pad_size_error	Unable to remove pad bytes in packet.	4612 pad size error
out_bound_dh_acc	An out-of-bounds DH index was encountered during processing of the packet.	4161 bad dh index
esp_auth_fail	Digest in an ESP Encapsulated packet is incorrect.	4609 ESP authentication fail
ah_auth_failure	Digest in an AH Encapsulated packet is incorrect.	4610 AH authentication fail
crypto_pad_error	Encryption coprocessor found a padding error.	4611 crypto pad error
ah_prot_absent	The SPI in the ESP header of a packet does not match the SPI in the packet's flow.	4615 AH protocol absent
ah_seq_failure	The AH sequence check failed.	4612 AH Sequence fail
ah_spi_failure	The sequence number in the AH Header does not match the packets flow.	4613 AH SPI fail
esp_prot_absent	—	4617 ESP protocol absent

Table 4 show crypto engine accelerator statistic Compression Statistics Descriptions for a Cisco 2600, Cisco 3600 or Cisco 3700 VPN module

Count Label	Significance	Associated Error Number
esp_seq_fail	—	4614 ESP sequence fail
esp_spi_failure	—	4615 ESP SPI fail
obound_sa_acc	—	4162 bad sa index
invalid_sa	—	4165 invalid SA
out_bound_sa_flow	—	4163 bad flow index
invalid_dh	—	4166 invalid DH
bad_keygroup	—	4172 bad keygroup
out_of_memory	—	4177 out of memory
no_sh_secret	—	4195 no shared secret
no_skeys	—	4193 no SKEYS
invalid_cmd	An unknown command was either sent to the VPN Module from IPSEC or returned from the VPN Module to the VPN driver.	4351 unknown command
dsp_coproc_err	Packet was received for encryption or decryption when VPN hardware is disabled.	5120 Encryption not ready
comp_unsupported	Number of packets seen by the VPN module that request compression when the VPN Module does not support compression.	4111 compression unsupported
pak_too_big	The packet is too large to be handled. It has more particles than the VPN Module can physically handle.	6144 pak too large
pak_mp_length_spec_fault	Packet received for encryption/decryption that is larger than the VPN Module MTU size or a packet is smaller than its encapsulation.	4102 pkt spec fault
tx_lo_queue_size_max	Not used in Cisco 2600/3600 VPN.	
cmd_unimplemented	A command unsupported by the VPN hardware was passed to the VPN hardware.	4337 Unimplemented command
Interrupts	Total number of interrupts of all types received from the VPN Module.	—
Immed	—	—
HiPri ints	Number of data packet interrupts received by the CPU from the VPN Hardware Module.	—
LoPri ints	Number of cmd complete interrupts received by the CPU from the VPN Hardware Module.	—
POST Errs	Number of Power-on self test failures detected by VPN Module bring-up sequence.	—
Alerts	—	—
Unk Cmds	Not used in Cisco 2600/3600 VPN.	—
UnexpCmds	A command reply was received by IOS that it was not expecting.	None

Table 4 show crypto engine accelerator statistic Compression Statistics Descriptions for a Cisco 2600, Cisco 3600 or Cisco 3700 VPN module

Count Label	Significance	Associated Error Number
cgx_cmd_pending	Not used in Cisco 2600/3600 VPN.	—
packet_loop_max	Not used in Cisco 2600/3600 VPN.	—
packet_loop_limit	Not used in Cisco 2600/3600 VPN.	—

Tip In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to show commands that use the EXEC **prompt timestamp** command in line configuration mode.

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator sa-database	Displays the active entries in the crypto engine SA database.
show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto engine accelerator ring

To display the contents and status of the control command, transmit packet, and receive packet rings used by the hardware accelerator crypto engine, use the **show crypto engine accelerator ring** command in privileged EXEC mode.

show crypto engine accelerator ring [**control** | **packet** | **pool**]

Syntax Description

control	(Optional) Displays the number of control commands that are queued for execution by the hardware accelerator crypto engine.
packet	(Optional) Displays the contents and status information for the transmit packet rings that are used by the hardware accelerator crypto engine.
pool	(Optional) Displays the contents and status information for the receive packet rings that are used by the hardware accelerator crypto engine.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII & AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command displays the command ring information.

If there is valid data in any of the rings, the ring entry will be printed.

Examples

The following example shows the command ring information:

```
Router# show crypto engine accel ring packet

PPQ RING:

cmd ring:head = 10 tail =10

result ring:head = 10 tail =10

destination ring:head = 10 tail =10

source ring:head = 10 tail =10
```

```
free ring:head = 0 tail =255
        00000000  071A96C5
        00000000  071A96C5
        00000001  071A9465
        00000001  071A9465
        00000002  071A9205
        00000002  071A9205
              .
              .
              .
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec security associations and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator sa-database	Displays the active entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show diag

To display hardware information for a router, use the **show diag** command in privileged EXEC mode.

show diag [*slot*]

Syntax Description

slot	(Optional) Slot number of the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1 CA	This command was introduced.
11.2 P	This command was modified to update the example for PA-12E/2FE port adapter, PA-E3 port adapter, and PA-T3 port adapter.
11.3 XA	This command was made available for Cisco IOS Release 11.3 XA.
12.0(5)XQ	This command was enhanced and made available for the Cisco 1750 router.
12.0(7)T	This command was modified to add the example for the Cisco 1750 router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII & AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command displays information for the electronically erasable programmable read-only memory (EEPROM), the motherboard, and the WAN interface cards (WICs), voice interface cards (VICs), and, advanced integration modules (AIMs). Use this command to determine the type of port adapter installed on a Versatile Interface Processor (VIP2) in your router.

Examples

The following example show how to obtain hardware information about an installed AIM-VPN.

```
Router# show diag 0

Encryption AIM 1:
        Hardware Revision        :1.0
        Top Assy. Part Number    :800-03700-01
        Board Revision           :A0
        Deviation Number         :0-0
        Fab Version              :02
        PCB Serial Number        :JAB9801ABCD
        RMA Test History         :00
        RMA Number               :0-0-0-0
        RMA History              :00
        EEPROM format version 4
```

```
EEPROM contents (hex):
  0x00:04 FF 40 03 0B 41 01 00 C0 46 03 20 00 0E 74 01
  0x10:42 41 30 80 00 00 00 00 02 02 C1 8B 4A 41 42 39
  0x20:38 30 31 41 42 43 44 03 00 81 00 00 00 00 04 00
  0x30:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x40:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x50:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Table 5 describes significant fields shown in the display.

Table 5 show diag Field Descriptions

Counter	Description
Board Revision	Revision number (signifying a minor revision) of the Cisco uBR7200 series port adapter.
C2611 2E Mainboard Port adapter, 2 ports	Line card type; number of ports available.
Deviation Number	Revision number (signifying a minor deviation) of the port adapter.
EEPROM contents (hex)	Dumps of EEPROM programmed data.
EEPROM format version	Version number of the EEPROM format.
Hardware Revision	Version number of the Cisco 2611 series port adapter.
Part Number	Part number of the port adapter.
PCB Serial Number	Serial number of the printed circuit board.
Port adapter insertion time	Elapsed time since insertion.
Port adapter is analyzed	The system has identified the Cisco 2611 series port adapter.
RMA History	Counter that indicates how many times the port adapter has been returned and repaired.
RMA Number	Return material authorization number, which is an administrative number assigned if the port adapter needs to be returned for repair.

Glossary

AH—Authentication Header. A protocol for authentication of packets (header included).

AIM—advanced integration module. APCI-based card type used on C26*xx* and C36*xx* routers.

DES—Data Encryption Standard.

ESP—Encapsulating Security Payload. A protocol that specifies encryption or compression on the payload of a packet (not headers).

IPSec—IP Security. Protocol for encryption and authentication of IP packets.

IPPCP—IP Payload Compression Protocol. An IETF protocol used to encapsulate compressed payloads.

LZS—Limpel Zif Stac algorithm.

NM—network modules.

SA—security association. A negotiated relationship between two IPSec peers who have agreed on an encryption and authentication method for traffic between them.

VIP2—Versatile Interface Processor.

VPN—virtual private network.

Note Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.