



Software IPPCP (LZS) with Hardware Encryption

The Software IPPCP (LZS) with Hardware Encryption feature allows customers to use Lempel-Ziv-Stac (LZS) software compression with IP Security (IPSec) when a Virtual Private Network (VPN) module is in Cisco 2600 and Cisco 3600 series routers, allowing users to effectively increase the bandwidth on their interfaces.

Feature Specifications for the Software IPPCP (LZS) with Hardware Encryption feature

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Contents

- [Restrictions for Software IPPCP \(LZS\) with Hardware Encryption, page 2](#)
- [Information About Software IPPCP \(LZS\) with Hardware Encryption, page 2](#)
- [How to Use IPPCP Software with Hardware Encryption, page 3](#)
- [Configuration Examples for IPPCP Software Compression Verification, page 4](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 11](#)

Restrictions for Software IPPCP (LZS) with Hardware Encryption

- This feature is available only on platforms that support the Cisco 2600 and Cisco 3600 VPN hardware adapters.
- Compression will be running on the router main processor; thus, this feature is recommended only for low speed links with bandwidth less than 512 Kbps. For high speed links, second generation VPN advanced integration module (AIM) cards with hardware support of both encryption and compression is recommended.

Information About Software IPPCP (LZS) with Hardware Encryption

To use the Software IPPCP (LZS) with Hardware Encryption feature, you must understand the following concept:

- [Feature Description of IPPCP Software with Hardware Encryption, page 2](#)

Feature Description of IPPCP Software with Hardware Encryption

Before this feature was introduced, compression was not supported with the VPN encryption hardware AIM and network modules (NM); that is, a user had to remove the VPN module from the router and run software encryption with software compression. This feature enables all VPN modules to support LZS compression in software when the VPN module is in the router, thereby, allowing users to configure data compression and increase their bandwidth, which is useful for a low data link.

Without this feature, compression occurs at layer 2, and encryption occurs at layer 3. After a data stream is encrypted, it is passed on for compression services. When the compression engine receives the encrypted data streams, the data expands and does not compress. This feature enables both compression and encryption of the data to occur at layer 3 by selecting LZS with the IPsec transform set; that is, LZS compression occurs before encryption, and it is able to get better compression ratio.

Table 1 summarizes the functions used with this feature.

Table 1 *IPPCP Software with Hardware Encryption Feature Summary*

Function	Type
Data compression	LZS
Encryption and tunneling	<ul style="list-style-type: none"> • IPsec • generic routing encapsulation (GRE)
Encryption algorithm	<ul style="list-style-type: none"> • data encryption standard (DES) • 3DES
Encryption modes	<ul style="list-style-type: none"> • transport • tunnel
Hash	<ul style="list-style-type: none"> • Message Digest #5 (MD5) • standard hashing algorithm (SHA)
Authentication	<ul style="list-style-type: none"> • preshared • Rivest, Shamir, and Adelman (RSA-ENCR)

How to Use IPPCP Software with Hardware Encryption

This section contains the following procedures:

- [Configuring LZS Compression, page 3](#)
- [Verifying Compression Statistics, page 3](#)

Configuring LZS Compression

The necessary steps to configure this feature are identical to the steps used to configure the Cisco 2600 and Cisco 3600 hardware VPN modules. For information on completing these steps, refer to the document *Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*.

Verifying Compression Statistics

To verify software compression statistics, perform the following optional steps:

SUMMARY STEPS

1. `enable`
2. `show crypto engine accelerator statistic`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables higher privilege levels, such as privileged EXEC mode.
	Example: <code>Router> enable</code>	Enter your password if prompted.
Step 2	<code>show crypto engine accelerator statistic</code>	Displays the statistics and error counters for the router's onboard hardware accelerator for IP Security (IPSec) encryption.
	Example: <code>Router# show crypto engine accelerator statistic</code>	

Configuration Examples for IPPCP Software Compression Verification

This section provides the following configuration example:

- [LZS Compression Statistics Verification Example, page 4](#)

LZS Compression Statistics Verification Example

The following example displays LZS software compression statistics:

```
Router# show crypto engine accelerator statistic
```

```

Statistics for Hardware VPN Module:
      ds: 8235C3D8      idb: 82359A64
Statistics for Encryption Module:
      0 packets in                0 packets out
      0 packet overruns           0 output packets dropped
      0 packets decompressed       0 packets compressed
      0 compressed bytes in        0 encompassed bytes in
      0 packets bypass compression 0 packet abort compression
      0 packets fail compression
      4:1 compression ratio        2:1 overall compression ratio
      0 decompressed bytes out     0 compressed bytes out
      0 packets decrypted           0 packets encrypted
      0 bytes decrypted             0 bytes encrypted
      0 bytes before decrypt        0 bytes after encrypt
      0 paks/sec in                 0 paks/sec out
      0 Kbits/sec decrypted         0 Kbits/sec encrypted
      0 packet overruns
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_keys:          0    invalid_cmd:      0
dsp_coproc_err: 0  comp_unsupported:0  pak_too_big:      0
null packets: 0
pak_mp_length_spec_fault: 0
tx_lo_queue_size_max 0  cmd_unimplemented: 0
219 seconds since last clear of counters
Interrupts: 4      Immed: 3      HiPri ints: 0
LoPri ints: 0      POST Errs: 0  Alerts: 1
Unk Cmds: 0        UnexpCmds: 0
cgx_cmd_pending:0  packet_loop_max: 0  packet_loop_limit: 0

```

Additional References

The following sections provide additional references related to Software IPPCP (LZS) with Hardware Encryption:

- [Related Documents, page 5](#)
- [Standards, page 5](#)
- [MIBs, page 5](#)
- [RFCs, page 6](#)
- [Technical Assistance, page 6](#)

Related Documents

Related Topic	Document Title
AIM installation information	<i>Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers</i>
IKE configuration information	The chapter “Configuring Internet Key Exchange Security Protocol” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2
IPSec configuration information	The chapter “Configuring IPSec Network Security” in the <i>Cisco IOS Security Configuration Guide</i> , Release 12.2

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
FRC 2393	<i>IP Payload Compression Protocol (IPComp)</i>
RFC 2395	<i>IP Payload Compression Using LZS</i>

1. Not all supported RFCs are listed.

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 a modified command. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [show crypto engine accelerator statistic](#)

show crypto engine accelerator statistic

To display the statistics and error counters for the router's onboard hardware accelerator for IP Security (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 implemented on the Cisco uBR905 cable access router.
	12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
	12.2(13)T	The show output for this command was enhanced to display compression statistics.

Examples The following example displays compression statistics:

```
Router# show crypto engine accelerator statistic
```

```

Statistics for Hardware VPN Module:
  ds: 8235C3D8      idb: 82359A64
Statistics for Encryption Module:
  0 packets in                0 packets out
  0 packet overruns          0 output packets dropped
  0 packets decompressed     0 packets compressed
  0 compressed bytes in      0 encompassed bytes in
  0 packets bypass compression 0 packet abort compression
  0 packets fail compression
  4:1 compression ratio      2:1 overall compression ratio
  0 decompressed bytes out   0 compressed bytes out
  0 packets decrypted        0 packets encrypted
  0 bytes decrypted          0 bytes encrypted
  0 bytes before decrypt     0 bytes after encrypt
  0 paks/sec in              0 paks/sec out
  0 Kbits/sec decrypted      0 Kbits/sec encrypted
  0 packet overruns
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

```

```
show crypto engine accelerator statistic
```

```

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
null packets:  0
pak_mp_length_spec_fault: 0
tx_lo_queue_size_max 0   cmd_unimplemented: 0
219 seconds since last clear of counters
Interrupts: 4           Immed: 3           HiPri ints: 0
LoPri ints: 0          POST Errs: 0       Alerts: 1
Unk Cmds: 0            UnexpCmds: 0
cgx_cmd_pending:0     packet_loop_max: 0   packet_loop_limit: 0

```

Table 2 describes significant fields shown in the display.

Table 2 *show crypto engine accelerator statistic Compression Statistics Descriptions*

Counter	Description
packets decompressed	Number of packets that were decompressed by the interface.
packets compressed	Number of packets that were compressed by the interface.
compressed bytes in	Number of compressed bytes that were presented to the compression algorithm from the input interface on decrypt.
encompassed bytes in	Number of uncompressed bytes (payload) that were presented to the compression algorithm from Cisco IOS on encrypt.
packet bypass compression	Number of packets that were not compressed because they were too small (<128 bytes).
packets abort compression	Number of packets that were not compressed because the packets are expanded rather than compressed.
packets fail compression	Number of packets that were not compressed because of problems in the compression algorithm.
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 compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm, including those that were not compressed due to expansion, too small. This ratio indicates whether the data traffic on this interface is suitable for compression. A ratio of 1:1 would imply that no successful compression is being performed on this data traffic.
decompressed bytes out	Number of decompressed bytes that were sent to Cisco IOS by the compression algorithm on decrypt.
compressed bytes out	Number of compressed bytes that were forwarded to Cisco IOS by the algorithm on encrypt.

The following sample output displays a typical output of the current statistics and error counters for the router's hardware accelerator:

```
Router# show crypto engine accelerator statistic

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
```



Tip

In Cisco IOS Release 12.2(8)T and later releases, you can add a timestamp to show commands using 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 engine accelerator	Enables the use of the Cisco uBR905 and Cisco uBR925 router's onboard hardware accelerator for IPsec encryption.
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 transmit rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine security association (SA) database.

Glossary

AIM—advanced integration module. A PCI-based card type that is used on Cisco 2600 and Cisco 3600 series routers to provide hardware-based encryption.

DES—Data Encryption Standard. An algorithm that is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Cisco IOS software also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers, particularly in the finance industry, to utilize network-layer encryption.

GRE—generic routing encapsulation. Tunnels that provide a specific pathway across the shared WAN and encapsulate traffic with new packet headers to ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. Tunnels do not provide true confidentiality (encryption does) but can carry encrypted traffic.

GRE tunneling can also be used to encapsulate non-IP traffic into IP and send it over the Internet or IP network. The Internet Package Exchange (IPX) and AppleTalk protocols are examples of non-IP traffic.

IKE—Internet Key Exchange. A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPSec. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

IPSec—IP Security. A framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”), such as Cisco routers.

IPPCP—IP Payload Compression Protocol. A protocol that reduces the size of IP datagrams.

MD5 (HMAC variant)—Message Digest 5. A hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.

SHA (HMAC variant)—Secure Hash Algorithm. A hash algorithm used to authenticate packet data. HMAC is a variant that provides an additional level of hashing.

transport mode—Encapsulates the upper layer payload of the original IP datagram, leaving the original IP header intact. The outer IP header contains the IP address of the source and destination IPSec endpoints.

tunnel mode—Encapsulates the complete original IP datagram. The outer IP header contains the IP address of the source and destination IPSec endpoints.

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

