



Multi-ISA

This feature module describes the Multi-ISA feature and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 5](#)
- [Verifying Multi-ISA, page 5](#)
- [Monitoring and Maintaining Multi-ISA, page 5](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 8](#)
- [Glossary, page 9](#)

Feature Overview

The Multi-ISA feature allows a Cisco IOS router to accommodate more than one hardware crypto engine at a time. This feature allows users to increase the capacity of their routers with multiple Integrated Services Adapters (ISAs) and Integrated Services Module (ISMs).



Note

ISAs are used on Cisco 7200 routers and ISMs are used on Cisco 7100 routers. Hereafter, for purposes of this document and unless otherwise noted, the term ISA will denote both Integrated Services Adapters and Integrated Services Modules.

The multi-ISA layer provides a single interface, which Cisco IOS software can use to send commands to different hardware crypto engines. The multi-ISA layer accepts all commands and packets on behalf of all underlying hardware crypto engines; it distributes all commands and packets in a predefined manner. That is, when you request an Internet Key Exchange-security association (IKE-SA) session, the multi-ISA layer determines which of the two hardware crypto engine contains fewer IKE-SAs, and it assigns the next session to the hardware crypto engine that has fewer IKE-SAs.



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

© 2007 Cisco Systems, Inc. All rights reserved.

How Multi-ISA Works

When your router has only one ISA in an active state, all IKE and IP Security-SA sessions go to this one ISA. Once you have inserted the second ISA into your router and it becomes active, subsequent IKE-SAs will flow to the second ISA until the first and second ISAs have an equal number of IKE-SA sessions. For example, if ISA-1 has 10 IKE sessions, and then ISA-2 becomes active, the router will send the following 11 through 20 IKE sessions to ISA-2. Thereafter, the multi-ISA layer will maintain a balance of IKE-SA sessions on both ISAs.


Note

The second ISA becomes active through online insertion and removal (OIR) or micro reload.

Benefits

The Multi-ISA feature provides the following benefits:

- Load-sharing of IKE-SAs
- Increased IPSec traffic throughput of your router
- OIR support

Restrictions

System Requirements

Your system should contain at least 128 megabytes of memory to run a single ISA and 256 megabytes of memory to run two ISAs. You need more than 128 megabytes of memory to cross 2,000 bidirectional IPSec tunnels.


Note

All tunnels referenced to in this document are defined as bidirectional IPSec tunnels.

Crypto Capabilities

All ISAs supported by the multi-ISA layer must have the same crypto capabilities. For example, if one ISA supports 3DES, another ISA that does not support 3DES cannot be in the same router under the multi-ISA layer.

Failover Limitations

Keepalives are needed to achieve failover in your router. If you turn on keepalives, you cannot exceed 500 tunnels because of current IKE keepalive limitations in the Cisco IOS software.


Note

This restriction will be lifted in a future release.

MPPE

Multiple Microsoft Point-to-Point Encryption (MPPE) ISA support is not available.

Related Documents

The following documents provide information related to the Multi-ISA feature:

- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1
- ISA and ISM Installation and Configuration
- The chapter “Basic System Management” in *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.1
- The chapter “Performing Basic System Management” in *Cisco IOS Configuration Fundamentals Configuration Guide*

Supported Platforms

The following platforms support the Multi-ISA feature:

- Cisco 7140
- Cisco 7200 with NP300 service module

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.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported 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://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

No new or modified RFCs are supported by this feature.

Prerequisites

IPSec Encryption

To use the Multi-ISA feature, you must configure your ISAs to provide IPSec encryption services by performing the following tasks:

- Configure IKE policies.
- Configure IPSec.
- Create crypto map entries.
- Apply a crypto map set to each interface through which IPSec traffic flows.

For information on completing these tasks, refer to *ISA and ISM Installation and Configuration*.

Manual Buffer Tuning

In the 7200 platform, it is recommended that you manually finetune packet buffers to establish more IKE-SA or IPSec tunnels.

To manually configure buffer tuning, enter the following global configuration command:

Command	Purpose
Router# (config) buffers { small middle big verybig large huge <i>type number</i> } { permanent max-free min-free initial } <i>number</i>	Makes adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed.

For buffer tuning examples, see the “[Configuration Examples](#)” section later in this document.

Configuration Tasks

None

Verifying Multi-ISA

To verify how many active IKE and IPSec sessions are on each hardware crypto engine, how many Diffie-Hellman (DH) keys are in use, and how far your ISA is from reaching its maximum limit, use the **show crypto eli** command in EXEC mode.

Monitoring and Maintaining Multi-ISA

To obtain a snapshot of how many IKE-SAs and IPSec sessions are active and how many DH keys are in use, use the following command in EXEC mode:

Command	Purpose
Router# show crypto eli	Displays a snapshot of how many IKE-SAs and IPSec sessions are active and how many DH keys are in use for each hardware crypto engine.

Configuration Examples

This section provides the following configuration examples:

- [Single ISA Scenario Example](#)
- [Load-Balancing with Multi-ISA Example](#)
- [Manual Buffer Tuning Examples](#)

Single ISA Scenario Example

The following example is sample output from the **show crypto eli** command. In this example, a router has established 1246 IKE sessions; however, all IKE sessions flow to a single ISA because only one ISA is in an active state.

```
P0# show crypto eli

Encryption Layer :  ACTIVE
Number of crypto engines = 1 .

Slot-3 crypto engine details.
Capability-IPSec :No-IPPCP, 3DES, NoRSA

IKE-Session   : 1246 active,  2029 max, 0 failed
DH-Key        :      0 active,  1014 max, 0 failed
IPSec-Session : 2712 active,  4059 max, 0 failed
```

Load-Balancing with Multi-ISA Example

The following example is sample output from the **show crypto eli** command. In this example, a router has established 2492 IKE sessions; the IKE sessions are equally distributed between two ISAs (each ISA contains 1246 IKE sessions), allowing you to increase the capacity of your router.

```
P0# show crypto eli

Encryption Layer :  ACTIVE
Number of crypto engines = 2 .

Slot-3 crypto engine details.
Capability-IPSec :No-IPPCP, 3DES, NoRSA

IKE-Session   : 1246 active,  2029 max, 0 failed
DH-Key        :      0 active,  1014 max, 0 failed
IPSec-Session : 2676 active,  4059 max, 0 failed

Slot-5 crypto engine details.
Capability-IPSec :No-IPPCP, 3DES, NoRSA

IKE-Session   : 1246 active,  2029 max, 0 failed
DH-Key        :      0 active,  1014 max, 0 failed
IPSec-Session : 2678 active,  4059 max, 0 failed
```

[Table 1](#) describes significant fields shown in the display.

Table 1 *show crypto eli summary Field Descriptions*

Field	Description
active	The number of sessions that are active on a given hardware crypto engine.
max	The maximum number of sessions allowed for any given IKE, DH, or IPSec entry.
failed	The number of times that Cisco IOS software attempted to create more sessions than the number specified in “max.”

Manual Buffer Tuning Examples

The following example shows recommended numbers to use, based on available memory, when manually configuring packet buffers on the 7200 platform using the **buffers** command:

Memory (MB)	Non-HUGE Buffers		
	Min-free	Permanent	Max-free
32	64	256	1280
64	128	512	2560
96	192	768	3840
128	256	1024	5120
160	320	1280	6400
192	384	1536	7680
224	448	1792	8960
256	512	2048	10240

Memory (MB)	HUGE Buffers		
	Min-free	Permanent	Max-free
32	4	16	64
64	8	32	128
96	12	48	192
128	16	64	256
160	20	80	320
192	24	96	384
224	28	112	448
256	32	128	512

[Table 2](#) describes significant fields shown in the display.

Table 2 Manual Buffer Tuning Example Descriptions

Field	Description
Memory (MB)	Available memory on your 7200 platform.
Min-free	Minimum number of free or unallocated buffers in a buffer pool.
Permanent	Number of permanent buffers that the system tries to create and keep.
Max-free	Maximum number of free or unallocated buffers in a buffer pool.

The following example shows sample output from the **show buffers** command:

P0# **show buffers**

Buffer elements:

500 in free list (500 max allowed)
12666974 hits, 0 misses, 0 created

Public buffer pools:

Small buffers, 104 bytes (total 2048, permanent 2048):

2039 in free list (512 min, 10240 max allowed)
293 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Middle buffers, 600 bytes (total 2048, permanent 2048, peak 5000 @ 16:34:14):

2048 in free list (512 min, 10240 max allowed)
849 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

Big buffers, 1524 bytes (total 2048, permanent 2048):

2048 in free list (512 min, 10240 max allowed)
84 hits, 0 misses, 0 trims, 0 created

```
0 failures (0 no memory)
VeryBig buffers, 4520 bytes (total 2048, permanent 2048):
  2048 in free list (512 min, 10240 max allowed)
  0 hits, 0 misses, 0 trims, 0 created
  0 failures (0 no memory)
Large buffers, 5024 bytes (total 2048, permanent 2048, peak 5000 @ 16:34:25):
  2047 in free list (512 min, 10240 max allowed)
  18 hits, 0 misses, 0 trims, 0 created
  0 failures (0 no memory)
Huge buffers, 18024 bytes (total 128, permanent 128):
  128 in free list (32 min, 512 max allowed)
  0 hits, 0 misses, 0 trims, 0 created
  0 failures (0 no memory)
```

Command Reference

The following commands are introduced or modified in the feature or features

- **show crypto eli**

For information about these commands, see the Cisco IOS Security Command Reference at

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html.

For information about all Cisco IOS commands, see the Command Lookup Tool at

<http://tools.cisco.com/Support/CLILookup> or the Master Command List.

Glossary

crypto map—A Cisco IOS software configuration entity that performs two primary functions: (1) selecting data flows that need security processing and (2) defining the policy for these flows and the crypto peer to which traffic needs to go. A crypto map is applied to an interface. The concept of a crypto map was introduced in classic crypto but was expanded for IPSec.

DH—See Diffie-Hellman.

Diffie-Hellman—A public-key cryptography protocol that allows two parties to establish a shared secret over an insecure communications channel. Diffie-Hellman is used within IKE to establish session keys and is a component of Oakley.

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

IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router, firewall, or host must be able to verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a certification authority (CA) service.

Integrated Services Adapter—See ISA.

Internet Key Exchange—See IKE.

IPSec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IP Security—See IPSec.

ISA—Integrated Services Adapter. Provides high-performance, hardware-assisted tunneling and encryption services suitable for private WAN and virtual private network (VPN) applications. Within this feature module, ISA includes ISM.

ISM—Integrated Services Module.

OIR—online insertion and removal. A feature that allows you to add, replace, or remove a card from your router without interrupting the system power, entering console commands, or causing other software or interfaces to shut down. This feature is sometimes referred to as “hot swapping” or “power-on servicing.”

online insertion and removal—See OIR.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.