



## Overview

---

This chapter describes the ISA and the ISM and contains the following sections:

- [ISA and ISM Overview, page 1-1](#)
- [Data Encryption Overview, page 1-2](#)
- [Features, page 1-3](#)
- [Port Adapter Slot Locations on the Supported Platforms, page 1-4](#)
- [LEDs, page 1-6](#)



**Note**

---

The ISA and the ISM are the same board, but differ in their outside appearance.

---

## ISA and ISM Overview

The ISA is a single-width service adapter and the ISM is a single-width service module. Each provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access, site-to-site intranet, and extranet applications, as well as platform scalability and security while working with all services necessary for successful VPN deployments—security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management. The ISA and the ISM off-load IPsec and MPPE processing from the main processor of the Cisco 7200 series or Cisco 7100 series router, thus freeing resources on the processor engines (that is, the network processor engine [NPE] on the Cisco 7200 series, and the network processor [NP] on the Cisco 7100 series routers) for other tasks.

The ISA and the ISM provide hardware-accelerated support for multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5) hash algorithms
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

**Note**

The Cisco 7100 series VPN routers do not support ISM and ISA in the same chassis. The Cisco 7100 series routers do not support online insertion and removal of the ISM.

The Cisco 7200 series routers do not support the ISM. The Cisco 7200 series routers support online insertion and removal of the ISA.

## Data Encryption Overview

The ISA and the ISM support IPsec, IKE, Microsoft Point to Point Encryption (MPPE), and Certification Authority (CA) interoperability features, providing highly scalable remote access VPN capabilities to Microsoft Windows 95/98/NT systems.

MPPE in conjunction with Microsoft's Point-to-Point tunneling protocol (PPTP) provides security for remote Microsoft Windows users by providing a tunneling capability, user-level authentication, and data encryption.

**Note**

The ISA does not support MSCHAP-v2.

For more information on IPsec, IKE, MPPE, and CA interoperability, refer to the "IP Security and Encryption" chapter in the *Security Configuration Guide* and *Security Command Reference* publications.

IPsec acts at the network level and is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec services are similar to those provided by Cisco Encryption Technology (CET). However, IPsec provides a more robust security solution and is standards-based. IPsec also provides data authentication and antireplay services in addition to data confidentiality services, whereas CET provides data confidentiality services only.

Cisco implements the following standards with data encryption:

- IPsec—IPsec is 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; it 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.

IPsec is documented in a series of Internet Drafts. The overall IPsec implementation is documented in RFC 2401 through RFC 2412 and RFC 2451.

- IKE—Internet Key Exchange (IKE) is a hybrid security protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. Although IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard.
- Microsoft Point-to-Point Encryption (MPPE) protocol is an encryption technology that provides encryption across point-to-point links. These links may use Point-to-Point Protocol (PPP) or Point-to-Point Tunnel Protocol (PPTP).

The ISA and the ISM support MPPE when encapsulation is set to PPP or PPTP.

- CA—In addition, Certificate Authority (CA) interoperability is provided in support of the IPsec standard, using Certificate Enrollment Protocol (CEP). CEP permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPsec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPsec.

The component technologies implemented for IPsec include:

- DES and Triple DES—The Data Encryption Standard (DES) and Triple DES (3DES) are used to encrypt packet data. Cisco IOS implements the 3-key triple DES and DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet.
- MD5 (HMAC variant)—MD5 is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- SHA (HMAC variant)—SHA is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

IPsec as implemented in Cisco IOS software supports the following additional standards:

- AH—Authentication Header is a security protocol that provides data authentication and optional antireplay services.

The AH protocol allows for the use of various authentication algorithms; Cisco IOS has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The AH protocol provides antireplay services.

- ESP—Encapsulating Security Payload is a security protocol that provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected. The ESP protocol allows for the use of various cipher algorithms and (optionally) various authentication algorithms. Cisco IOS software implements the mandatory 56-bit DES-CBC with Explicit IV or Triple DES as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides antireplay services.

## Features

This section describes the ISA/ISM features, as listed in [Table 1-1](#).

**Table 1-1** Features

Feature	Description
Physical	Integrated Service Adapter (ISA) Integrated Service Module (ISM)
Platform Support	<b>Cisco 7100 series</b> <ul style="list-style-type: none"> <li>• Cisco 7120 series and Cisco 7140 series</li> </ul> <b>Cisco 7200 series and Cisco 7200VXR series (ISA only)<sup>1</sup></b> <ul style="list-style-type: none"> <li>• Cisco 7202, Cisco 7204, and Cisco 7206</li> <li>• Cisco 7204VXR and Cisco 7206VXR</li> </ul>
Hardware Prerequisites	None
Throughput	Up to full duplex DS3 (90 Mbps) using 3DES

Table 1-1 Features (continued)

Feature	Description
Number of Tunnels	Up to 2000 IPSec protected tunnels Up to 2000 PPTP tunnels protected by MPPE
Encryption	Data protection: IPSec DES and 3 DES, 40 and 128-bit RC4 MPPE (stateful or stateless) Authentication: RSA and Diffie Hellman, MS Chap Data integrity: SHA-1 and MD5
VPN Tunneling	IPSec tunnel mode, GRE, LT2P, L2F protected by IPSec, PPTP protected by MPPE
Number of ISMs per Router	One ISM per chassis
Minimum Cisco IOS Release Supported <sup>2</sup>	
<b>Cisco 7100 series</b> <ul style="list-style-type: none"> <li>Cisco 7120 series and Cisco 7140 series</li> </ul>	Cisco IOS Release 12.0(5)XE or a later release of Cisco IOS Release 12.0 XE Cisco IOS Release 12.1(1)E or a later release of Cisco IOS Release 12.1 E Cisco IOS Release 12.2(2)T or later release of Cisco IOS Release 12.1T Cisco IOS Release 12.2M or later release of Cisco Release 12.2M.
<b>Cisco 7200 and Cisco 7200VXR series (for ISA only)</b> <ul style="list-style-type: none"> <li>Cisco 7202, Cisco 7204, and Cisco 7206</li> </ul>	Cisco IOS Release 12.0(5)XE or a later release of Cisco IOS Release 12.0 XE Cisco IOS Release 12.1(1)E or a later release of Cisco IOS Release 12.1 E Cisco IOS Release 12.2(2)T or a later release of Cisco IOS Release 12.1 T Cisco IOS Release 12.2M or a later release of Cisco IOS Release 12.2M Cisco IOS Release 12.2(4)B or a later release of Cisco IOS Release 12.2 B
Standards Supported	IPSec/IKE: RFCs 2401-2410, 2411, 2451 MPPE: draft-ietf-pppext-mppe-*

1. The Cisco 7200 series and Cisco 7200VXR series routers only support the ISA, not the ISM.

2. Cisco IOS Release 12.1 Mainline is not supported on ISA or ISM.

## Port Adapter Slot Locations on the Supported Platforms

This section discusses port adapter slot locations on the supported platforms. The illustrations that follow summarize the slot location conventions on the supported platforms:

- [Cisco 7100 Series Routers Slot Numbering](#)
- [Cisco 7200 Series Routers Slot Numbering](#)

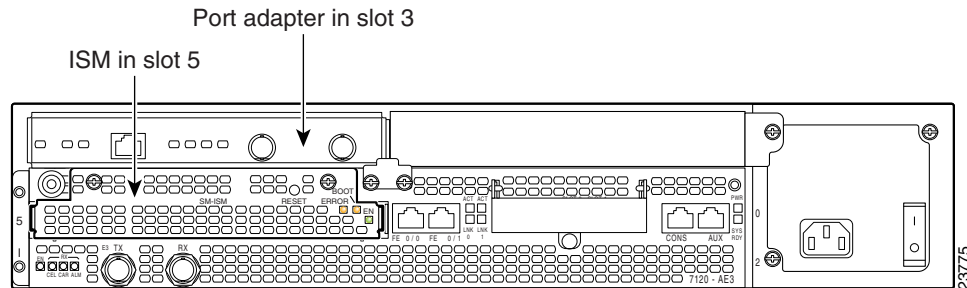
### Cisco 7100 Series Routers Slot Numbering

The ISM can be installed in service module slot 5 in Cisco 7120 series and Cisco 7140 series routers. [Figure 1-1](#) shows a Cisco 7120 with an ISM installed in slot 5. [Figure 1-2](#) shows a Cisco 7140 with an ISM installed in slot 5. A port adapter can be installed in slot 3 in the Cisco 7120 series routers and in slot 4 in the Cisco 7140 series routers.

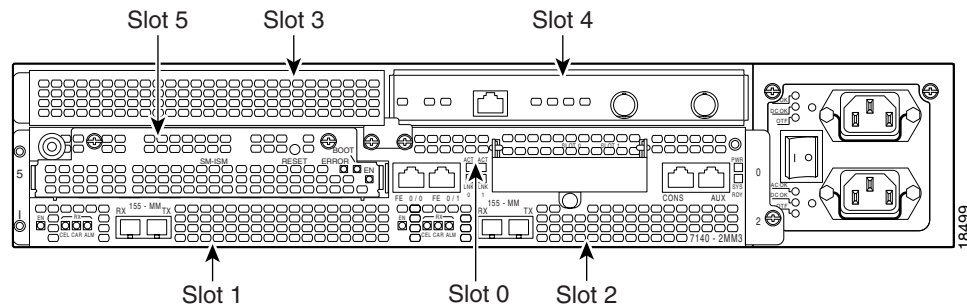
**Note**

The Cisco 7100 series VPN routers do not support an ISM and an ISA in the same chassis.

**Figure 1-1 Service Module Slot 5 in the Cisco 7100 Series Router—Cisco 7120 Series**



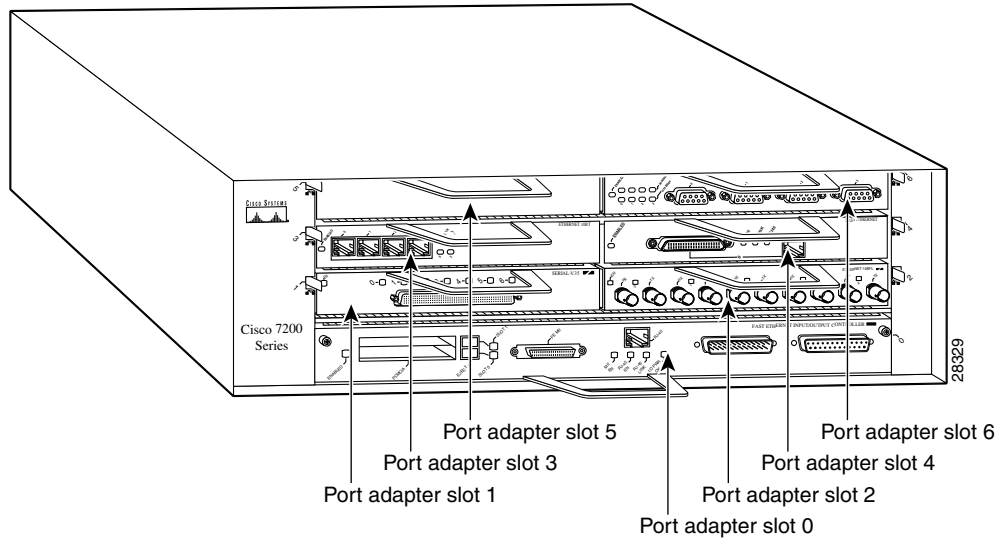
**Figure 1-2 Service Module Slot 5 in the Cisco 7100 Series Router—Cisco 7140 Series**



## Cisco 7200 Series Routers Slot Numbering

The ISA can be installed in the Cisco 7200 series routers in any available port adapter slot. [Figure 1-3](#) shows a Cisco 7206 with port adapters installed, and a port adapter filler installed in slot 5. (The Cisco 7202 and Cisco 7204 are not shown; however, the ISA can be installed in any available port adapter slot.)

**Figure 1-3** Port Adapter Slots in the Cisco 7206



## LEDs

The ISA has three LEDs, as shown in [Figure 1-4](#). [Table 1-2](#) lists the colors and functions of the ISA LEDs.



### Note

The Boot LED remains lit when the ISA/ISM is configured for MPPE, and it starts to pulsate after booting when the ISA/ISM is configured for IPsec. The ISA/ISM functions normally whether the Boot LED is pulsating or is solid. See [Chapter 4, “Configuring the ISA and ISM”](#) for more information on configuring the ISA/ISM.

**Figure 1-4 ISA Front Panel LEDs (SA-ISA shown)****Table 1-2 ISA LEDs**

LED Label	Color	State	Function
ENABLE	Green	On	Indicates the ISA is powered up and enabled for operation.
BOOT	Amber	Pulses <sup>1</sup>	Indicates the ISA is operating.
		On	Indicates the ISA is booting or a packet is being encrypted or decrypted.
ERROR	Amber	On	Indicates an encryption error has occurred. This LED is normally off.

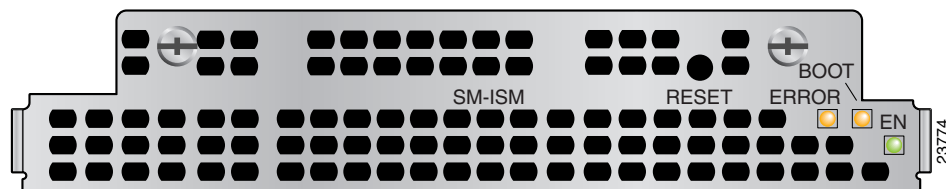
1. After successfully booting, the boot LED pulses in a “heartbeat” pattern to indicate that the ISA is operating. As crypto traffic increases, the nominal level of this LED increases in proportion to the traffic level.

The following conditions must all be met before the enabled LED goes on:

- The ISA is correctly connected to the backplane and receiving power.
- The system bus recognizes the ISA.

If either of these conditions is not met, or if the router initialization fails, the enabled LED does not go on.

The ISM has three LEDs, as shown in [Figure 1-5](#). [Table 1-3](#) lists the colors and functions of the LEDs.

**Figure 1-5 ISM LEDs****Note**

The physical orientation of the ISM LEDs is reversed from that of the ISA (see [Figure 1-5](#)).

**Table 1-3 ISM LEDs**

LED Label	Color	State	Function
EN	Green	On	Indicates the ISM is powered up and enabled for operation.
BOOT	Amber	Pulses <sup>1</sup> On	Indicates the ISM is operating. Indicates the ISM is booting or a packet is being encrypted or decrypted.
ERROR	Amber	On	Indicates an encryption error has occurred. This LED is normally off.

1. After successfully booting, the boot LED pulses in a “heartbeat” pattern to indicate that the ISM is operating. As crypto traffic increases, the nominal level of this LED increases in proportion to the traffic level.

The following conditions must all be met before the enabled LED goes on:

- The ISM is correctly connected to the backplane and receiving power.
- The system bus recognizes the ISM.

If either of these conditions is not met, or if the router initialization fails for other reasons, the enabled LED does not go on.