Overview

This chapter describes the VPN acceleration module and contains the following sections:

VPN Acceleration Module Overview

The VPN Acceleration Module (VAM) is a single-width acceleration module supported on the Cisco 7200 series routers.

Note The Cisco 7100 series and the Cisco 7401ASR routers are no longer sold.

The VAM supports LAN/WAN media and full Layer 3 routing services. VAMs provide hardware-assisted tunneling and encryption services for virtual private network (VPN) remote access, site-to-site intranet and extranet applications, including security, quality of service (QoS), firewall and intrusion detection, and service-level validation and management. The VAM off-loads IPSec processing from the main processor to permit resources on the processor engines for other tasks.

The VAM provides 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

The VAM is available as a service adapter (SA-VAM), and as a service module (SM-VAM). The SA-VAM is supported on the Cisco 7100 series routers, the Cisco 7200 series routers, and the Cisco 7401ASR router. The SM-VAM is supported on the Cisco 7100 series router.

Data Encryption Overview

This section describes data encryption, including the IPSec, IKE, and Certification Authority (CA) interoperability features.

Note For additional information on these features, refer to the "IP Security and Encryption" chapter in the *Security Configuration Guide* and *Security Command Reference* publications.

IPSec is a network level open standards framework, developed by the Internet Engineering Task Force (IETF) that provides secure transmission of sensitive information over unprotected networks such as the Internet. IPSec includes data authentication, antireplay services and data confidentiality services.

Cisco follows these data encryption standards:

- IPSec—IPSec is an IP layer open standards framework that provides data confidentiality, data integrity, and data authentication between participating peers. IKE handles negotiation of protocols and algorithms based on local policy, and generates the encryption and authentication keys to be used by IPSec. IPSec protects one or more data flows between a pair of hosts, between a pair of security routers, or between a security router and a host.
- 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. IKE can be used with IPSec and other protocols. IKE authenticates the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. IPSec can be configured with or without IKE.
- CA—Certificate Authority (CA) interoperability supports the IPSec standard, using Simple Certificate Enrollment Protocol (SCEP) and Certificate Enrollment Protocol (CEP). CEP permits Cisco IOS devices and CAs to communicate to permit your Cisco IOS device to obtain and use digital certificates from the CA. IPSec can be configured with or without CA. The CA must be properly configured to issue certificates. For more information, see the "Configuring Certification Authority Interoperability" chapter of the *Security Configuration Guide* at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7b2.html

The component technologies implemented for IPSec include:

- DES and Triple DES—The Data Encryption Standard (DES) and Triple DES (3DES) encryption 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 to authenticate data.
- RSA signatures and RSA encrypted nonces—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman, hence RSA. RSA signatures provides non-repudiation while RSA encrypted nonces provide repudiation. For additional information, see the *Exporting and Importing RSA Keys* feature module at: http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541cf.html

IPSec with the 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 uses 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, a security protocol, provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected. The ESP protocol uses 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.
- IPPCP—When using Layer 3 encryption, lower layers (such as PPP at Layer 2) cannot provide compression. When compressing already encrypted packets, expansion usually results. IPPCP provides stateless compression for use with encryption services such as IPsec.

Features

This section describes the VAM features.

Feature	Description/Benefit
Throughput[1]	Up to 145 Mbps using 3DES
Number of IPSec protected tunnels[2]	Up to 5000 on Cisco 7401ASR routers[3] Up to 5000 on Cisco 7200 series routers Up to 3000 on Cisco 7100 series routers[3]
Hardware-based encryption	Data protection: IPsec DES and 3DES Authentication: RSA and Diffie-Hellman Data integrity: SHA-1 and Message Digest 5 (MD5)
VPN tunneling	IPsec tunnel mode; generic routing encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP) protected by IPsec
Hardware-based compression	Layer 3 IPPCP LZS
Standards supported	IPsec/IKE: RFCs 2401-2411, 2451 IPPCP: RFC 2393, 2395

1. As measured with IPSec 3DES HMAC-SHA1 on 1400 byte packets.
2. Number of tunnels supported varies based on the total system memory installed.
3. The Cisco 7100 series and the Cisco 7401ASR routers are no longer sold.

Supported Standards, MIBs, and RFCs

This section describes the standards, Management Information Bases (MIBs), and Request for Comments (RFCs) supported on the VAM. Requests for Comments (RFCs) contain information about the supported Internet suite of protocols.

Standards

- IPPCP: RFC 2393, 2395
- IPsec/IKE: RFCs 2401-2411, 2451

MIBs

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

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

RFCs

- IPPCP: RFC 2393, 2395
- IPsec/IKE: RFCs 2401-2411, 2451

LEDs

This section describes the LEDs on the SA-VAM and the SM-VAM.

SA-VAM

The SA-VAM is supported on the Cisco 7200 series routers.

Note The Cisco 7100 series routers and the Cisco 7401ASR routers are no longer sold.

The SA-VAM has three LEDs, as shown in Figure 1-1. Table 1-1 lists the colors and functions of the SA-VAM LEDs.

Figure 1-1 SA-VAM LEDs

Table 1-1 SA-VAM LEDs

LED Label	Color	State	Function
ENABLE	Green	On	Indicates the VAM is powered up and enabled for operation.
BOOT	Amber	Pulses[1]	Indicates the VAM is operating.
		On	Indicates the VAM 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 VAM is operating. As crypto traffic increases, the nominal level of this LED increases in proportion to the traffic level.

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

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

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

SM-VAM

The SM-VAM is supported on the Cisco 7100 series router.

The SM-VAM has three LEDs, as shown in Figure 1-2. Table 1-2 lists the colors and functions of the LEDs.

Figure 1-2 SM-VAM LEDs

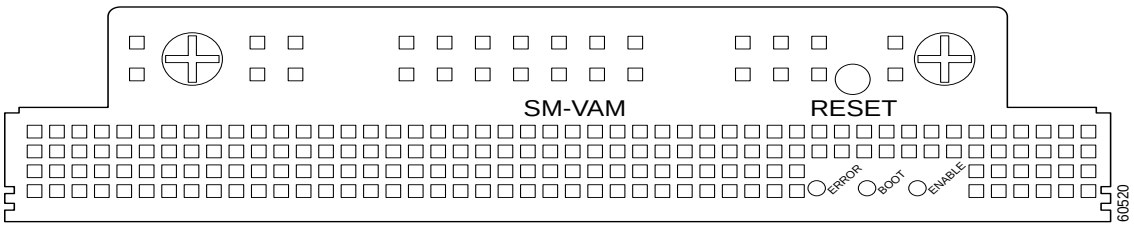


Table 1-2 SM-VAM LEDs

LED Label	Color	State	Function
ERROR	Amber	On	Indicates an encryption error has occurred. This LED is normally off.
BOOT	Amber	Pulses[1]	Indicates the SM-VAM is operating.
		On	Indicates the SM-VAM is booting or a packet is being encrypted or decrypted.
ENABLE	Green	On	Indicates the SM-VAM is powered up and enabled for operation.

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

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

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

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

Cables, Connectors, and Pinouts

There are no interfaces on the VAM, so there are no cables, connectors, or pinouts.

VAM Slot Locations

This section discusses VAM and port adapter slot locations on the supported platforms.

The VAM is available as a service adapter, (SA-VAM), and as a service module (SM-VAM). The SA-VAM installs in the port adapter slot on the Cisco 7100 series router, the Cisco 7200 series router, and the Cisco 7401ASR router. The SM-VAM installs in the service module slot on Cisco 7100 series router.

The illustrations that follow summarize slot location conventions on each platform:

- Cisco 7100 Series Routers Slot Numbering, page 1-7
- Cisco 7200 Series Router Slot Numbering, page 1-8
- Cisco 7401ASR Router Slot Numbering, page 1-9

Cisco 7100 Series Routers Slot Numbering

The SM-VAM is installed in service module slot 5 of the Cisco 7120 and the Cisco 7140 routers. (See Figure 1-3.) The SA-VAM is installed in port adapter slot 3 of the Cisco 7120 router and in port adapter slot 4 in the Cisco 7140 router. (See Figure 1-4).

Figure 1-3 SM-VAM in Service Module Slot 5 of the Cisco 7120 Router

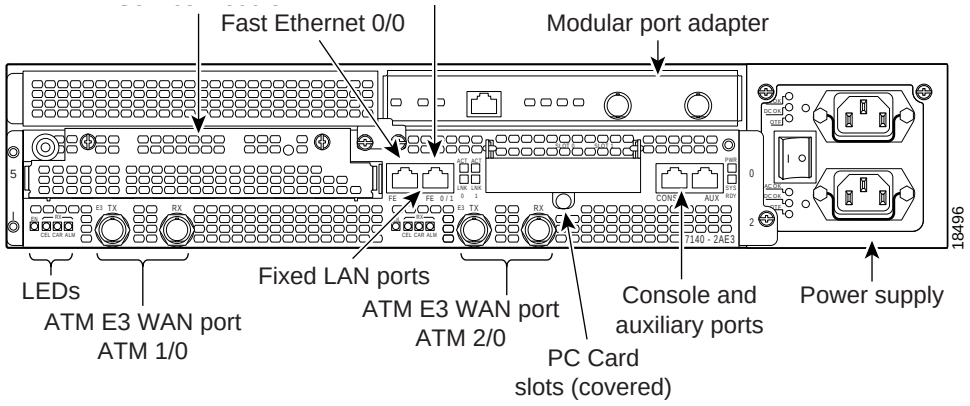
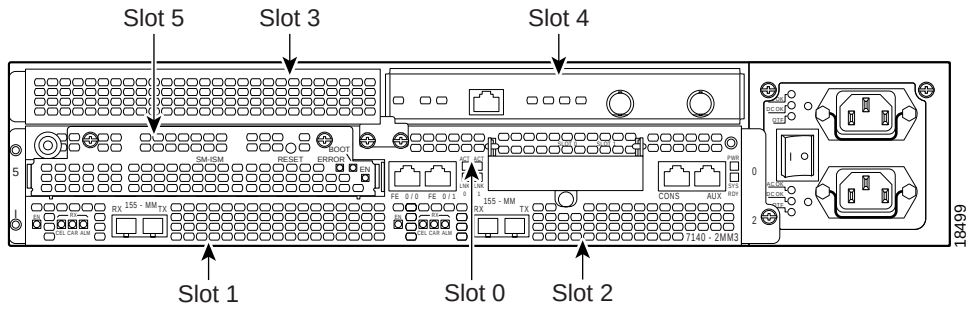


Figure 1-4 SA-VAM Available in Port Adapter Slot 4 in the Cisco 7140 Router



Cisco 7200 Series Router Slot Numbering

The SA-VAM can be installed in any single-width port adapter slot in the Cisco 7204 (see Figure 1-5) and the Cisco 7206 routers (see Figure 1-6).

Note In the Cisco 7200 series router with a PA-T3 or PA-FE installed in the odd-numbered slot, install the VAM in an even-numbered slot to help load-balance the bus.

Figure 1-5 Port Adapter Slots in the Cisco 7204 Router

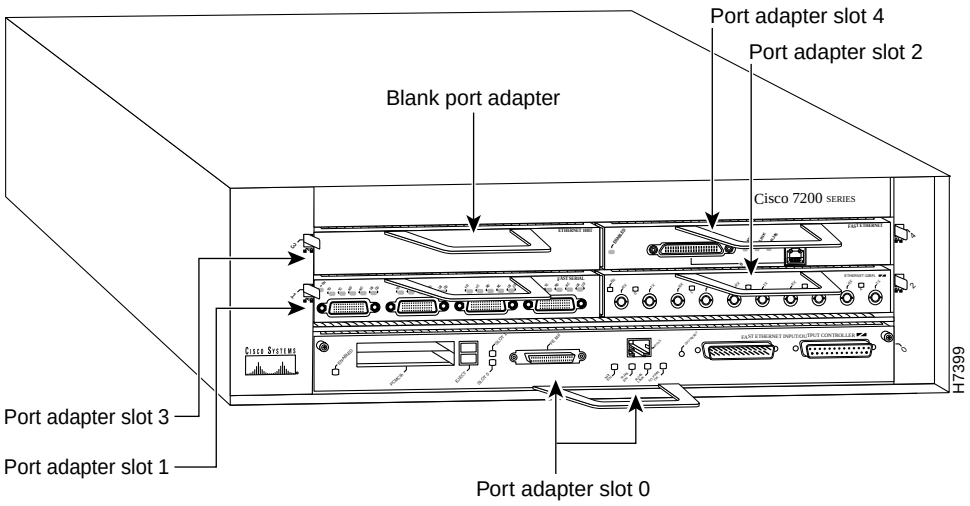
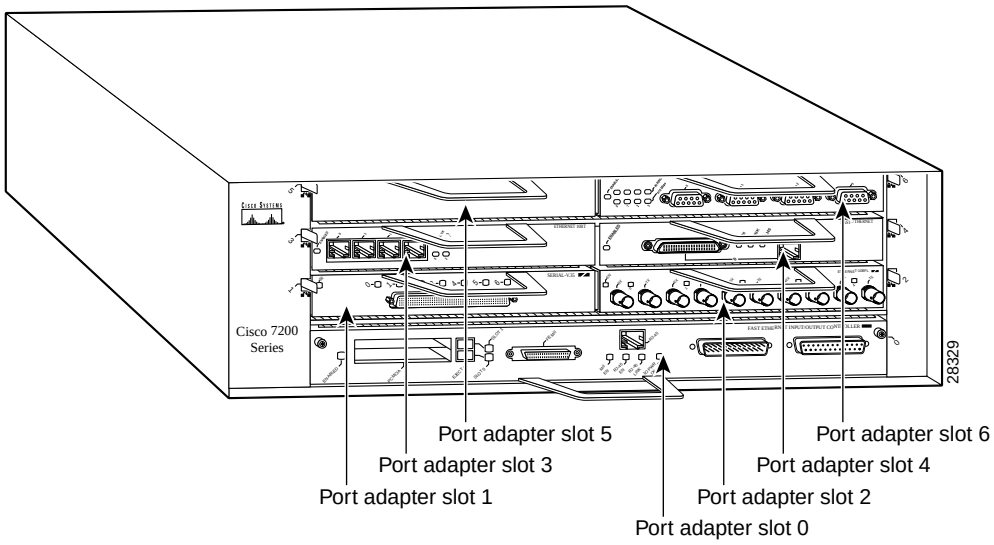


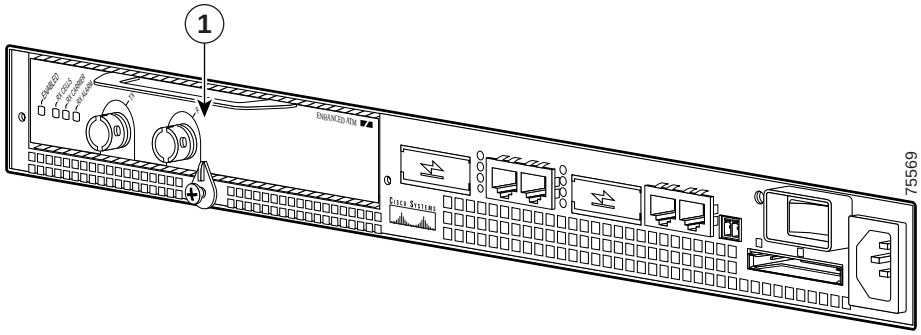
Figure 1-6 Port Adapter Slots in the Cisco 7206 Router



Cisco 7401ASR Router Slot Numbering

The SA-VAM can be installed in the only available slot in the Cisco 7401ASR router (see Figure 1-7).

Figure 1-7 Port Adapter Slot in the Cisco 7401ASR Router



1	Port adapter slot		

Note Interface ports are numbered from left to right starting with 0.