Preparing for Installation

This chapter describes the general equipment, safety, and site preparation requirements for installing the Service Adapter VPN Acceleration Module 2 (SA-VAM2). This chapter contains the following sections:

Required Tools and Equipment

You need the following tools and parts to install a SA-VAM2. If you need additional equipment, contact a service representative for ordering information.

- SA-VAM2
- Number 2 Phillips screwdriver
- Your own electrostatic discharge (ESD)-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, field-replaceable units (FRUs), and spares
- Antistatic mat
- Antistatic container

Minimum Hardware and Software Requirements

This section describes the minimum software and hardware requirements for the SA-VAM2:

Hardware Requirements

Specific hardware prerequisites that ensure proper operation of the SA-VAM2 follow:

- The SA-VAM2 on the Cisco 7200 series routers requires a network processing engine 225 (NPE-225), 400 (NPE-400), G1 (NPE-G1), or the Network Services Engine (NSE-1) services accelerator.

- The Cisco 7200 series routers support up to two SA-VAM2s.

- The Cisco 7301 router supports a single SA-VAM2 in the port adapter slot.

Software Requirements

Table 2-1 lists the recommended minimum Cisco IOS software release required to use the SA-VAM2 in supported router or switch platforms. Use the **show version** command to display the system software version that is currently loaded and running.

Table 2-1   SA-VAM2 Software Requirements

Platform	Recommended Minimum Cisco IOS Release
Cisco 7200 series router	Cisco IOS Release 12.3(1)M or a later release of Cisco IOS Release 12.3M
	Cisco IOS Release 12.2(14)SU or a later release of Cisco IOS Release 12.2(14)SU
Cisco 7301 router	Cisco IOS Release 12.3(3) or a later release of Cisco IOS Release 12.3M
	Cisco IOS Release 12.3(2)T1 or a later release of Cisco IOS Release 12.3T1

Hardware and Software Compatibility

This section includes the following hardware and software compatibility requirements:

Hardware Compatibility

The Cisco 7301 router supports a single SA-VAM2 in the port adapter slot.

The Cisco 7200 series routers support up to two SA-VAM2 cards. SA-VAM2 cards can interoperate with port adapters supported on the Cisco 7200 chassis with the NPE-225, NPE-400, or NPE-G1 processor, or the NSE-1 services accelerator.

Note   The SA-VAM2 is compatible with the NPE-225, NPE-400, or NPE-G1 processor, or the NSE-1 services accelerator on the Cisco 7200 series routers.

Software Compatibility

To check the minimum software requirements of Cisco IOS software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com. Registered Cisco Direct users can access the Software Advisor at:http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl. This tool does not verify whether modules within a system are compatible, but it does provide the minimum Cisco IOS software requirements for individual hardware modules or components.

Note   Access to this tool is limited to users with Cisco.com login accounts.

Interoperability Between SA-VAM2, ISA, and SA-VAM

Note   The integrated services adapter (ISA) is the predecessor of the SA-VAM. The Cisco 7200 series routers supports both the ISA and the SA-VAM with the SA-VAM2.

Table 2-1 describes the interoperability between ISA, SA-VAM, and SA-VAM2. You can use SA-VAM2 with ISA or with SA-VAM, provided you observe the following conditions:

- The Cisco 7200 series routers support two SA-VAM2s in the same chassis. If one SA-VAM2 is enabled at system bootup, and a second SA-VAM2 is added later, the second SA-VAM2 becomes active immediately, and depending on the configuration, the system attempts to load-balance between the two SA-VAM2s.

- If SA-VAM and SA-VAM2 are in the chassis at system bootup, the Cisco 7200 series router supports the newer version, in this case, SA-VAM2, provided the Cisco IOS Release supports SA-VAM2; and the SA-VAM remains inactive.

- If ISA and SA-VAM2 are in the chassis at system bootup, and the **encryption mppe** command is in the router's running configuration, then both ISA/ISM and SA-VAM2 are enabled at system bootup. The ISA/ISM card supports MPPE, and the SA-VAM2 supports ISAKMP/IPSec. You can enable **encryption mppe** by following the steps in "Configuring IPSec" section on page 4-46. To disable MPPE on an ISA card, use the **no encryption mppe** command. This disables the ISA.

- To disable a card, use the **no crypto engine accelerator** *type slot/port* (port-adapter-slot-number/ interface-port-number) command.

Table 2-2   Interoperability Between ISA, SA-VAM, and SA-VAM2

SA-VAM2 with ISA	SA-VAM2 with SA-VAM	SA-VAM2 with SA-VAM2
• Supports MPPE	• Does not support MPPE	• Does not support MPPE
• Supports ISAKMP/IPSec	• Supports ISAKMP/IPSec	• Supports ISAKMP/IPSec
• If ISA and SA-VAM2 are enabled in the chassis at power up, ISA is used for MPPE, and SA-VAM2 is used for ISAKMP/IPSec, provided the router's running configuration includes the **encryption mppe** command	• If SA-VAM2 and SA-VAM are in the chassis at power up, the router supports SA-VAM2, and SA-VAM remains inactive	• If SA-VAM2 and SA-VAM2 are enabled in the chassis at power up, the router supports both
• If ISA is enabled in the chassis at bootup, and SA-VAM2 is added later, the SA-VAM2 remains inactive until the next reboot, or until the configuration is changed to enable the SA-VAM2	• If SA-VAM is enabled in the chassis at bootup, and SA-VAM2 is added later, the SA-VAM2 remains inactive until the next reboot, or until the configuration is changed to enable the SA-VAM2	• If SA-VAM2 is enabled in the chassis at bootup, and another SA-VAM2 is added later, the second SA-VAM2 immediately becomes active and depending on the configuration, the system attempts to load-balance between the two SA-VAM2s

Safety Guidelines

This section provides safety guidelines that you should follow when working with any equipment that connects to electrical power or telephone wiring. This section includes the following topics:

- Safety Warnings, page 2-28
- Electrical Equipment Guidelines, page 2-29
- Preventing Electrostatic Discharge Damage, page 2-29

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement.

Warning   **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Warning   **Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.**

Warning   **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

Electrical Equipment Guidelines

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedures requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.
- Disconnect all power and external cables before moving a chassis; do not work alone when potentially hazardous conditions exist.
- Never assume that power has been disconnected from a circuit; always check.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe; carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Port adapters and processor modules comprise printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap during handling.

Following are guidelines for preventing ESD damage:

- Always use an ESD wrist or ankle strap and ensure that it makes good skin contact.
- Connect the equipment end of the strap to an unfinished chassis surface.
- When installing a component, use any available ejector levers or captive installation screws to properly seat the bus connectors in the backplane or midplane. These devices prevent accidental removal, provide proper grounding for the system, and help to ensure that bus connectors are properly seated.
- When removing a component, use any available ejector levers or captive installation screws to release the bus connectors from the backplane or midplane.
- Handle carriers by available handles or edges only; avoid touching the printed circuit boards or connectors.
- Place a removed board component-side-up on an antistatic surface or in a static shielding container. If you plan to return the component to the factory, immediately place it in a static shielding container.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- Never attempt to remove the printed circuit board from the metal carrier.
- For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 Mohm.

Compliance with U.S. Export Laws and Regulations Regarding Encryption

This product performs encryption and is regulated for export by the U.S. government. Persons exporting any item out of the United States by either physical or electronic means must comply with the Export Administration Regulations as administered by the U.S. Department of Commerce, Bureau of Export Administration. See http://www.bxa.doc.gov/ for more information.

Certain "strong" encryption items can be exported outside the United States depending upon the destination, end user, and end use. See http://www.cisco.com/wwl/export/encrypt.html for more information about Cisco-eligible products, destinations, end users, and end uses.

Check local country laws prior to export to determine import and usage requirements as necessary. See http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm as one possible, unofficial source of international encryption laws.