Data Encryption Service Adapter Installation and Configuration

Product Numbers: SA-Encrypt and SA-Encrypt=

This configuration note describes the installation and configuration of the data encryption service adapter, which is referred to throughout this publication collectively as *ESA* (Product Numbers SA-Encrypt and SA-Encrypt=).

The ESA is used in the Cisco 7204 and Cisco 7206 routers, and on the second-generation Versatile Interface Processor (VIP2-40 specifically) in all Cisco 7500 series routers, and on the VIP2-40 in Cisco 7000 series routers that have the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) installed.

Note For VIP2-40 users, use this configuration note in conjunction with the configuration note *Second-Generation Versatile Interface Processor (VIP2) Installation and Configuration* (Document Number 78-2658-xx), which shipped with your VIP2-40.

For Cisco 7200 series router users, use this configuration note in conjunction with the *Cisco 72xx Installation and Configuration Guide* that shipped with your Cisco 7200 series router.

For additional descriptions of interface subcommands and the configuration options available for VIP2-40-related interfaces, refer to the appropriate Cisco IOS software configuration and command reference publications listed in the section "Related Documentation" on page 2.

Caution To ensure compliance with U.S. export laws and regulations for 56-bit DES, and to prevent problems later on, refer to the section "Compliance with U.S. Export Laws and Regulations Regarding Encryption," on page 7, for specific and important information.

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

Document Contents

The following sections are included in this publication:

Caution To prevent system problems, do not remove service adapters from the VIP2-40 motherboard, or attempt to install other service adapters or port adapters on the VIP2-40 motherboard while the system is operating. To install or replace service adapters, first remove the VIP2-40 from its interface processor slot. The Cisco 7000 series and Cisco 7500 series chassis support online insertion and removal of the VIP2-40, but not of the ESA.

Note The Cisco 7200 series chassis support online insertion and removal of the ESA; however, you must observe special requirements. Before installing or removing an ESA from a Cisco 7200 series router, refer to the section "Enabling the ESA in the Cisco 7200 Series" on page 33.

Related Documentation

The documentation listed below is available online, on the Documentation CD-ROM, or as printed documents.

Your router, switch, or gateway and the Cisco IOS software running on it contain extensive features and functionality, which are documented in the following resources:

- Cisco IOS software:

- For configuration information and support, refer to the modular configuration and modular command reference publications in the Cisco IOS software configuration documentation set that corresponds to the software release installed on your Cisco hardware.
- 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: http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl. You must be a registered user on Cisco.com to access this tool.

Note You can access Cisco IOS software configuration and hardware installation and maintenance documentation on the World Wide Web at http://www.cisco.com/public/countries_languages.shtml.

- Cisco 7000 series routers:

  For hardware installation and maintenance information, refer to the following publications:
  - *Cisco 7000 Hardware Installation and Maintenance* that shipped with your router.
  - *Second-Generation Versatile Interface Processor (VIP2) Installation and Configuration*
  - *Fourth-Generation Versatile Interface Processor (VIP4) Installation and Configuration*
  - *Versatile Interface Processor (VIP6-80) Installation and Configuration*
- Cisco 7200 series routers:
  - For port adapter hardware and memory configuration guidelines, refer to the *Cisco 7200 Series Port Adapter Hardware Configuration Guidelines*.
  - For hardware installation and maintenance information (including the Cisco 7206 or Cisco 7206VXR as a router shelf in a Cisco AS5800 Universal Access Server), refer to the installation and configuration guide that shipped with your Cisco 7200 series router.
  - For information on network processing engines or network services engines, refer to the *Network Processing Engine and Network Services Engine Installation and Configuration* publication.
  - For information on the router boot images, refer to the *Cisco 7200 Series Routers Boot Images Information* publication.
- Cisco 7200 VXR routers:

  For hardware installation and maintenance information, refer to the *Cisco 7200 VXR Installation and Configuration Guide* or the *Cisco 7200 VXR Quick Start Guide*.
- Cisco uBR7200 series routers:

  For installation and maintenance information, refer to the *Cisco uBR7200 Series Hardware Installation Guide.*
- For international agency compliance, safety, and statutory information for WAN interfaces:
  - *Regulatory Compliance and Safety Information for the Cisco 7000 Series Routers*
  - *Regulatory Compliance and Safety Information for the Cisco 7200 Series Routers*
  - "Regulatory Compliance and Safety Information" appendix in the *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide*
  - *Site Preparation and Safety Guide*
- To view Cisco documentation or obtain general information about the documentation, refer to the following sections:

- Obtaining Documentation, page 60
- Obtaining Technical Assistance, page 61
- Customer service at 800 553-6387 or 408 526-7208. Customer service hours are 5:00 a.m. to 6:00 p.m. Pacific time, Monday through Friday (excluding Cisco-observed holidays). You can also send e-mail to cs-rep@cisco.com.

Data Encryption Overview

Network data encryption and router authentication together provide a means to safeguard network data that travels from one Cisco router to another, across unsecured networks. Safeguarding network data has become increasingly important to many organizations as they extend or replace private networks with public, unprotected networks. For example, many organizations are using the Internet as a economical way to replace leased line services.

Data that traverses unsecured network lines is open to many types of attacks. Data can be read, altered, or forged by anybody that has access to the route that your data takes. For example, a protocol analyzer can read packets and gain classified information. Or, a hostile party can tamper with packets and cause damage by hindering, reducing, or preventing effective communications within your organization. You can minimize the vulnerability of your network data by configuring your router for network data encryption with router authentication.

Data encryption is the process of transforming intelligible information, called *clear text*, into an unintelligible form, called *cipher text*, in order to provide secure data and information exchanges. Data encryption remains the best available data-security technique. The purpose of encryption is to convert data into meaningless data, which is converted in a manner that allows it to be reconverted into meaningful data. Further, date encryption assures that data sent over unsecure networks cannot be interrupted or intercepted in a readable form.

Encryption involves the use of an algorithm plus an encryption key. Different algorithms exist, each with its strengths and weaknesses, but each imposes restrictions on the minimum and maximum size of the encryption key. Encryption keys are simply large numbers used to convert the clear text into cipher text. Generally, the larger the encryption key, the more secure the data. Encryption can be applied at different levels of the protocol stack to protect against different forms of attack (for example, data protection or traffic analysis) and to allow passage through different types of networking equipment.

The act of encryption is to convert data such that recognizable patterns are removed. Take, for example, a simple electronic (e-mail) message. At least 70 percent of the message consists of white space. The encryption mechanism chosen must guarantee that all of the message is converted such that patterns of data cannot be interpreted. Successive white-space must be converted into different data. There can be no distinction between words or phrases that would give an attacker a clue as to the type of traffic being transmitted. Any hint of a pattern would greatly diminish the security of the data.

From the standpoint of data integrity, the secure network must allow for signatures that positively identify the parties involved. This signature must be irrevocable. No part should be able to emulate another and no party should be able to deny sending a message after the fact. No network is 100-percent secure. The encryption mechanism simply raises the cost of decrypting and acquiring the data.

Methods of Attack

Following are some of the methods of attack:

- Brute-force attack—an intruder tries all possible combinations of a key

- Intruder-in-the-middle attack—an intruder sits between two hosts and intercepts the traffic
- Denial-of-service attack—intruder attempts to hinder or reduce the amount of data going to and from the secure network; however, this is more detrimental to network productivity than security
- Replay attack—intruder attempts to reintroduce a decipher key time after time, hoping to hit on the repeated use of this key by the secure network
- Network address spoofing—an intruder looks for and finds the source and destination address pairs that are allowed into a particular secure network; this form of attack attempts to break access control restrictions.

In general, true data security should provide the following:

- Data encryption to deny access of the data to unauthorized sites or users
- A block to prevent the intruder-in-the-middle form of attack
- A block to prevent someone from masquerading as one of the trusted sites
- A signature to guarantee that the sender is real and authorized
- A signature to guarantee that the sender did in fact send the data and cannot later deny it
- Reduction and/or elimination of the denial-of-service attack
- Dynamic session key generation, which forces the intruder to periodically decipher the new key
- Access controls to deny access to unauthorized sites or users.

Levels of Encryption

Following are descriptions of the levels of data encryption, without positive or negative commentary on each method's efficacy:

- Link-level encryption (Layer 2 and 3)

  Link-level encryption provides extra protection by encrypting nearly all of the datagram. This includes the protocol header(s). The only portion of the datagram not encrypted is the link-level information. This method protects the protocol information as well as the data, and prevents a listener from obtaining information about an internal corporate network's structure. While link-level encryption allows no traffic analysis (a form of attack), it must encrypt/decrypt on every hop and every path.

- Protocol-level encryption (Layer 3 and 4)

  Protocol encryption forces the protocol data to be encrypted and leaves the protocol and link headers in the clear. In this method, it is assumed that the protocol data is sensitive, but no concern is given to the protocol headers' traffic analysis. While protocol-level encryption requires you to encrypt/decrypt data only once, and it encrypts/decrypts only those sessions that need it, headers are sent as clear text, which can allow for traffic analysis.

- Application encryption (Layer 5 and above)

  Application encryption is based on a particular application and requires that the application be modified to incorporate encryption.

Public-Key Technology

Public-Key (PK) technology operates on a pair of keys. One key is used for encryption and the other for decryption. Whichever key is used for encryption, only the other key can be used to decrypt the data. This is an asymmetric mechanism. Each key in the pair is a one-way encryption mechanism. The same key cannot be used to decrypt the message. Signing a document is key to PK technology.

A signature must have the following properties:

- Must be unforgettable.
- Must be authenticated such that it convinces the document's recipient that the signer deliberately signed the document.
- Not reusable, and should be part of the document so that another person cannot move it to a different document.
- A signed document must be unalterable.
- Cannot be repudiated, so that once signed and sent, the sender cannot later deny sending the message.

More often, this signature verification mechanism is used to establish a secure connection with a remote host for the purpose of sending encrypted traffic using a more efficient encryption mechanism.

Data Encryption Standard (DES) is a much more efficient mechanism for passing long strings of encrypted data. Unfortunately, this mechanism cannot be used to authenticate the participating stations. So the two mechanisms (PK and DES) are combined to create an encrypted and authenticated session between two hosts.

DES is a symmetric encryption mechanism. A single encryption key (called a *session key*) is used to both encrypt and decrypt the data. This key must be generated by the participating routers, without sending any meaningful data to each other, which might lead a third party (an intruder) into generating the same key value.

Securing Networks

Following are the essential parts to network security:

- Authenticating routers—a secure network must begin with trusted security devices. This means that each encryption device in the network must be authenticated to each other network device to which it will send encrypted data. This eliminates the intruder-in-the-middle attack.
- Setting encryption policies—including a declaration to networks that are to be encrypted and provision for time limits on encrypted sessions.
- Connection setup—provide secure connections that are as immune as possible to the effects of attackers listening in.
- Use of secure encryption keys—define the types of encryption to use over a secure network.

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

This product performs encryption and is regulated for export by the U.S. Government. Following is specific information regarding compliance with U.S. export laws and regulations for encryption products:

- This product is *not* authorized for use by persons located outside the United States and Canada that do not have export license authority from the U.S. Government.
- This product may *not* be exported outside the U.S. and Canada either by physical or electronic means without the *prior* written approval of the U.S. Government.
- Persons outside the U.S. and Canada may *not* reexport, resell, or transfer this product by either physical or electronic means without prior written approval of the U.S. Government.

What Is the Data Encryption Service Adapter?

The ESA (see) provides the hardware-based encryption mechanisms required to perform data encryption in Cisco 7000 family routers in which ESA is installed. The product number is SA-Encrypt(=), and the ESA uses a 40-bit or 56-bit Data Encryption Standard (DES), which is configurable via the Cisco IOS crypto engine (also called the *software* (*SW) crypto engine*).

The ESA provides data encryption mechanisms using PK technology based on the concept of the Protected Entity (PE), and employing the Data Encryption Standard (DES) and the Digital Signature Standard (DSS), to ensure secure data and information can be transferred between similarly equipped hosts on your network.

The ESA can be installed in the Cisco 7200 series routers; however, only one ESA can be installed in a Cisco 7200 series router. There are no slot restrictions and any chassis slot can be used; however, you must observe special requirements. Before installing or removing an ESA from a Cisco 7200 series router, refer to the section "Enabling the ESA in the Cisco 7200 Series" on page 33.

Figure 1 SA-Encrypt Service Adapter (Faceplate View)

Note The ESA can be installed on the VIP2-40 in adapter slot 0 or adapter slot 1; however, you *must* install a specific type of port adapter in the VIP2-40 port adapter slot *adjacent* to the ESA.

For specific information about the port adapters that can be used on the VIP2-40 with an ESA, and in Cisco 7200 series routers with an ESA, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.

The following additional sections discuss the ESA:

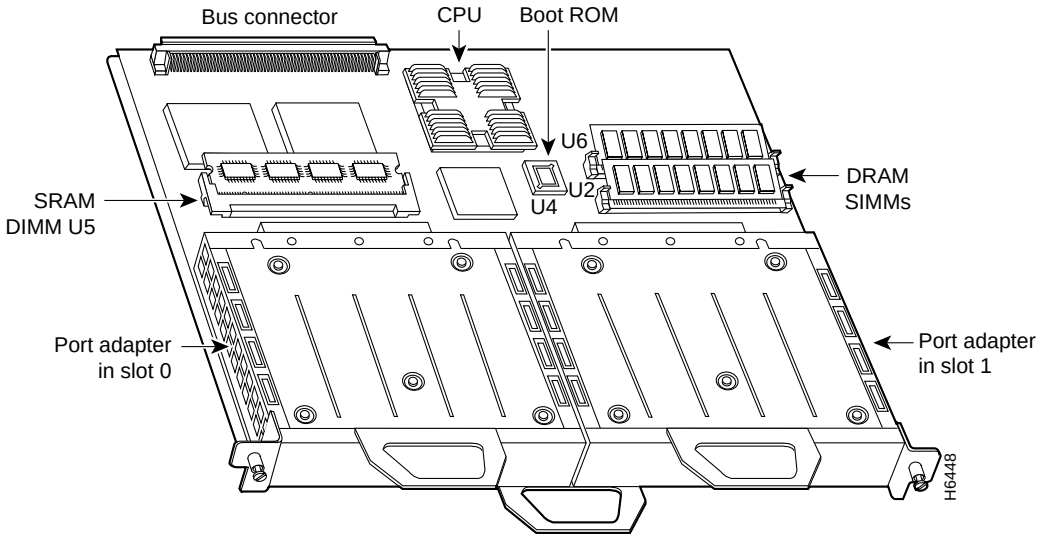
- Service Adapter Locations on the VIP2 and in the Cisco 7200 Series, page 8
- ESA LEDs, page 9

Service Adapter Locations on the VIP2 and in the Cisco 7200 Series

shows a VIP2-40 with installed port/service adapters. The VIP2-40 card and ESA have handles that allow for easy installation and removal. With the VIP2-40 oriented as shown in , the left adapter is in adapter slot 0 and the right adapter is in adapter slot 1.

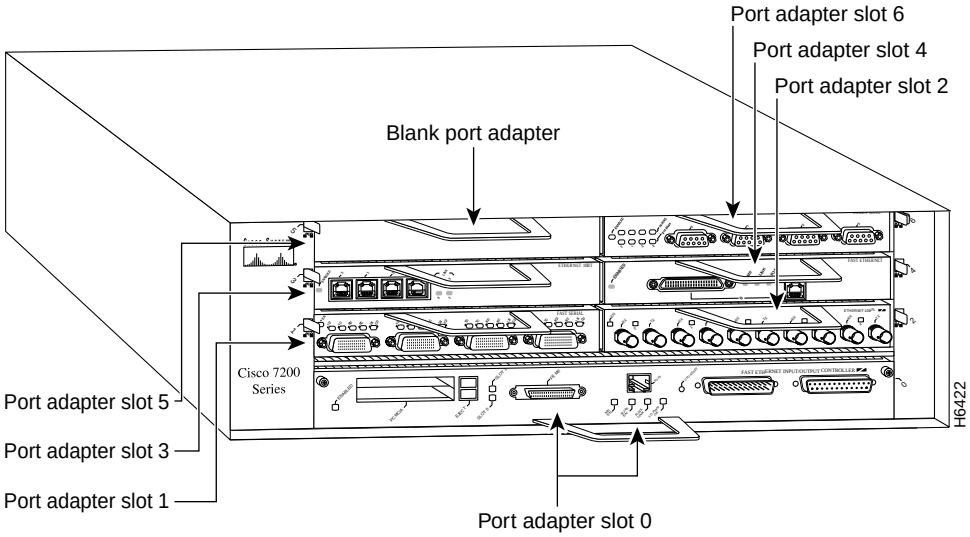
In the Cisco 7000, Cisco 7507, and Cisco 7513 chassis the VIP2-40 is installed vertically. In the Cisco 7010 and Cisco 7505 chassis, the VIP2-40 is installed horizontally. While the VIP2-40 supports online insertion and removal, individual adapters do not. To a replace service adapter, you must first remove the VIP2-40 from the chassis, then replace the service adapter.

Figure 2 Port/Service Adapters on the VIP2-40 (Horizontal Orientation Shown)



shows a Cisco 7206 with port adapters installed. In the Cisco 7206, port adapter slot 1 is in the lower left position, and port adapter slot 6 is in the upper right position. (The Cisco 7204 is not shown, but has four port adapter slots.) The ESA can be installed in any of these slots.

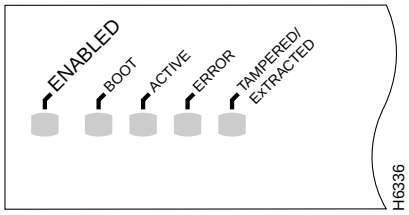
Figure 3 Port/Service Adapter Slots in the Cisco 7206



ESA LEDs

The ESA contains the enabled LED, standard on all service adapters, and a four status LEDs. After system initialization, the enabled LED goes on to indicate that the host has been enabled for operation. (The LEDs are shown in .)

Figure 4 LEDs on the ESA (Partial Faceplate View)



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

The data encryption interface is correctly connected to the backplane and receiving power.

The data-encryption-equipped VIP2-40 contains a valid microcode version that has been downloaded successfully and the bus recognizes the data-encryption-equipped VIP2-40.

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

In addition to the enabled LED, the ESA has the following four LEDs and indications:

- BOOT—this green LED is on to indicate the service adapter is booting itself, and remains on while the service adapter is in the boot process and goes off when the service adapter's boot process is complete. It is normally off.
- ACTIVE—this green LED is on to indicate the ESA is ready for operation, and goes on when the service adapter's boot process is complete and the boot LED goes off. It is normally on.
- ERROR—this amber LED goes on to indicate that an error was found, other than tampering, and if it remains on, it indicates the error might prevent accurate encryption. Error codes are generated by software. It is normally off.
- TAMPERED/EXTRACTED—this amber LED goes on to indicate that either the tamper switch or the extraction switch has been activated, which means that someone attempted to remove or has extracted and replaced the ESA or has removed the tamper shield. It is normally off.

Note The tampered/extracted LED goes on and stays on if the ESA is tampered with or extraction is attempted. After extracting the service adapter and replacing it, turn off the tampered/extracted LED by entering the appropriate password and the configuration command **crypto clear-latch** *slot*, where slot is the chassis slot in which the ESA is installed.

If the ESA was tampered with, the **crypto clear-latch** *slot* command will *not* turn off the tampered/extracted LED; use the **crypto zeroize** *slot* command instead, where slot is the chassis slot in which the ESA is installed.

If you do *not* know the password, you can enter the configuration command **crypto zeroize** *slot*, which removes the keys and turns off the tampered/extracted LED. You must then generate new keys for the ESA.

To determine the Cisco 7000 series, Cisco 7200 series, or Cisco 7500 series chassis slot in which an ESA is installed, use the **show crypto card** command as follows:

```
Router# show crypto card

Crypto card in slot: 2

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     No
FW version       0x5049702
```

Installation Prerequisites for the ESA

This section provides important hardware, software, and compliance prerequisites that we recommend you read and carefully observe, a list of parts and tools you will need to perform the installation, and safety and ESD-prevention guidelines to help you avoid injury and damage to the equipment.

Note The service adapter is designed to erase all internal information if it is tampered with. All encryption keys are stored in memory and backed up with a battery. If the card is tampered with, the memory is pulled to ground; therefore, erasing all memory and rendering the service adapter useless. Further, the battery that powers memory is external to the tamper-proof shielding. If the battery is removed, memory

is erased. If the service adapter is extracted from an installed system, an internal latch is set to indicate extraction. The service adapter is unusable, and the system administrator has to clear the latch with the appropriate password.

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. (For translated versions of this warning, refer to the section "Translated Battery Handling Warnings" on page 59.)**

Hardware, Software, and Compliance Prerequisites

The following list describes specific software and hardware prerequisites to ensure proper operation of the ESA:

- For Cisco 7200 series routers, the ESA requires Cisco IOS Release 11.2(7a)P or later.
- For Cisco 7000 and Cisco 7500 series routers with the VIP2-40, the ESA requires Cisco IOS Release 11.2(7)P or later.
- The ESA can be installed in Cisco 7200 series chassis: Cisco 7204 and Cisco 7206
- The ESA can be used in the second-generation Versatile Interface Processor (VIP2-40) in all Cisco 7500 series routers, and in Cisco 7000 series routers using the RSP7000 and RSP7000CI. The specific VIP2 model required for the ESA is VIP2-40(=), which has 2 MB of SRAM and 32 MB of DRAM.
- For VIP2-40 users: you *must* install the appropriate port adapter in the VIP2-40 port adapter slot *adjacent* to the ESA.
- For VIP2-40 users: most of the currently available port adapters, which are compatible with the VIP2-40, can be installed on a VIP2-40 alongside an ESA performing hardware encryption

  However, the following port adapters (and interface processor products) *cannot* be used with hardware encryption via the ESA, unless otherwise noted:

  – PA-4T—synchronous serial port adapter

  – PA-4T+—synchronous serial port adapter

    This port adapter is *not* compatible when X.25 or SMDS are configured

    This port adapter *is* compatible when PPP, HDLC, or Frame Relay are configured

  – PA-H—HSSI port adapter

    This port adapter is *not* compatible when X.25 or SMDS are configured

    This port adapter *is* compatible when PPP, HDLC, or Frame Relay are configured

  – PA-8B-ST, PA-4B-U—Basic Rate Interface port adapters

  – PA-2CE1/PRI-75, PA-2CE1/PRI-120, PA-2CT1/PRI—Channelized E1 and channelized T1 port adapters that can also be configured as Primary Rate Interface port adapters

    These port adapters are *not* compatible when in channelized mode and X.25 or SMDS is configured

    These port adapters are *not* compatible when in PRI mode and PPP or HDLC is configured

    These port adapters *are* compatible when in channelized mode and PPP, HDLC, or Frame Relay is configured

- CT3IP-20—Channelized T3 Interface Processor (in the same chassis as the ESA)
- For VIP2-40/Cisco 7500 series users: either the distributed switching (DSW) feature *or* NetFlow switching feature is required on the source and destination, encrypting/decrypting interfaces.

Note If distributed switching is on, every IP packet on the VIP2-40 goes through a crypto map check. If Netflow switching is on, the flow cache is used, and the only packets affected by the crypto map check are those for which no flow cache entry exists. For information on enabling and configuring the NetFlow switching feature, refer to the *Network Protocols Configuration Guide*, Part 1 (in the "Configuring IP" chapter) and in the *Network Protocols Command Reference* (in the "IP Commands" chapter). These publications are available on the Documentation CD-ROM and as printed copies.

- For Cisco 7200 series users: all of the currently available port adapters, which are compatible with the Cisco 7200 series, can be installed in a Cisco 7200 series router with an ESA

  There are no chassis slot restrictions on where the ESA can be installed; however, we recommend that you fully understand online insertion and removal functionality in the Cisco 7200 series routers *before* ESA installation; refer to the section "Enabling the ESA in the Cisco 7200 Series" on page 33.
- Cisco IOS software supports IP fragmentation for software (SW) and hardware (HW) encryption on all platforms except the VIP2-40.

List of Parts and Tools

You need some combination of the following tools and parts to install a service adapter on a VIP2-40 or in a Cisco 7200 series router. If you need additional equipment, contact a service representative for ordering information.

- SA-Encrypt(=), data encryption service adapter (ESA)
- Cisco IOS Release 11.2(7a)P or later, loaded on your Cisco 7200 series router
- Cisco IOS Release 11.2(7)P or later, loaded on your Cisco 7000 or Cisco 7500 series router with the VIP2-40
- For Cisco 7200 series users: a Cisco 7204 or Cisco 7206 in which to install the ESA

  For specific port adapter prerequisites for the Cisco 7200 series routers and ESA, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.
- For Cisco 7000 series and Cisco 7500 series users only:
  - VIP2-40(=) and one VIP2-40-compatible port adapter in the adjacent port adapter slot on the VIP2-40

    For specific port adapter prerequisites for the VIP2-40 and ESA, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.
- Number 1 Phillips and a 3/16-inch, flat-blade screwdriver
- Your own ESD-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, FRUs, and spares

Safety Guidelines

This section provides safety guidelines that you should follow.

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 **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het document *Regulatory Compliance and Safety Information* (Informatie over naleving van veiligheids- en andere voorschriften) raadplegen dat bij dit toestel is ingesloten.**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä julkaisussa esiintyvien varoitusten käännökset löydät laitteen mukana olevasta *Regulatory Compliance and Safety Information* -kirjasesta (määräysten noudattaminen ja tietoa turvallisuudesta).**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez le document *Regulatory Compliance and Safety Information* (Conformité aux règlements et consignes de sécurité) qui accompagne cet appareil.**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Dokument *Regulatory Compliance and Safety Information* (Informationen zu behördlichen Vorschriften und Sicherheit), das zusammen mit diesem Gerät geliefert wurde.**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nel documento *Regulatory Compliance and Safety Information* (Conformità alle norme e informazioni sulla sicurezza) che accompagna questo dispositivo.**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i dokumentet *Regulatory Compliance and Safety Information* (Overholdelse av forskrifter og sikkerhetsinformasjon) som ble levert med denne enheten.**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. Para ver as traduções dos avisos que constam desta publicação, consulte o documento *Regulatory Compliance and Safety Information* (Informação de Segurança e Disposições Reguladoras) que acompanha este dispositivo.**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Para ver una traducción de las advertencias que aparecen en esta publicación, consultar el documento titulado *Regulatory Compliance and Safety Information* (Información sobre seguridad y conformidad con las disposiciones reglamentarias) que se acompaña con este dispositivo.**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. Se förklaringar av de varningar som förkommer i denna publikation i dokumentet *Regulatory Compliance and Safety Information* (Efterrättelse av föreskrifter och säkerhetsinformation), vilket medföljer denna anordning.**

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.

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. (For translated versions of this warning, refer to the section "Translated Battery Handling Warnings" on page 59.)**

- 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.

Telephone Wiring Guidelines

Use the following guidelines when working with any equipment that is connected to telephone wiring or to other network cabling:

- Never install telephone wiring during a lightning storm or in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

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. A processor module comprises a printed circuit board that is fixed in a metal carrier. Electromagnetic interference (EMI) shielding, connectors, and a handle are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap whenever handling a processor module.

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 a captive installation screw on an installed power supply.
- When installing a processor module, use the ejector levers to properly seat the bus connectors in the backplane, then tighten both captive installation screws. These screws prevent accidental removal, provide proper grounding for the system, and help to ensure that the bus connectors are seated in the backplane.
- When removing a processor module, use the ejector levers to release the bus connectors from the backplane. Use the handle to pull the processor module out slowly while keeping your other hand underneath the carrier to guide it straight out of the slot.
- Handle carriers by the handles and carrier edges only; avoid touching the board or connectors.
- Place a removed processor module board-side-up on an antistatic surface or in a static shielding bag. If you plan to return the component to the factory, immediately place it in a static shielding bag.
- Avoid contact between the processor module and clothing. The wrist strap only protects the board 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 interface processor carrier.

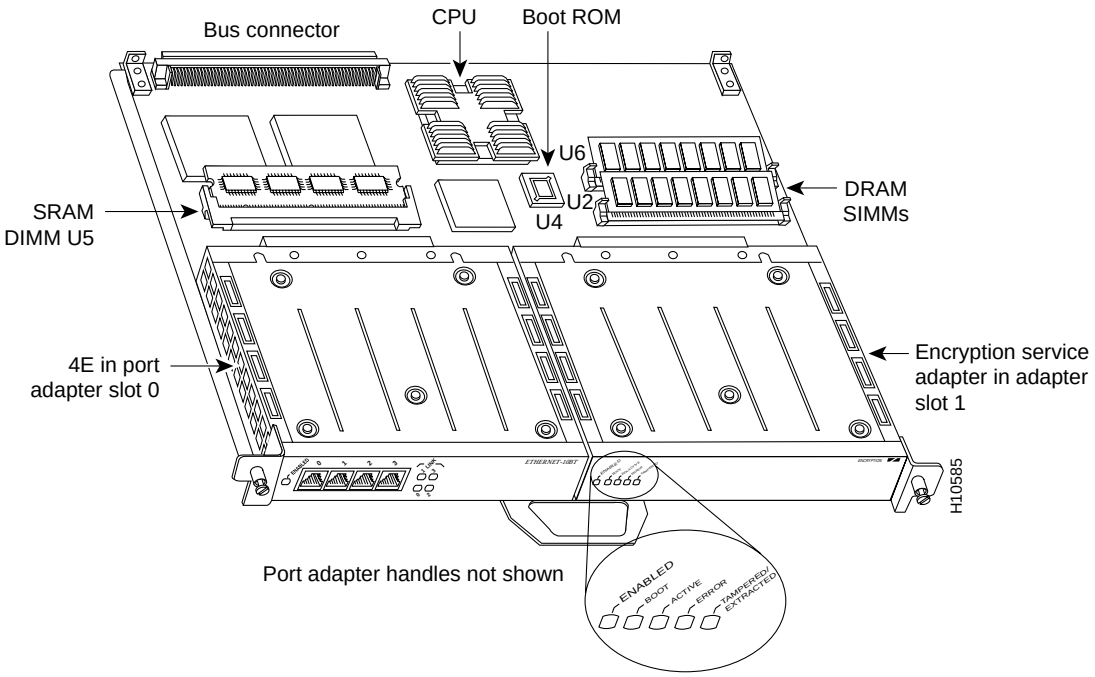
Caution For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohms.

Installing or Replacing a VIP2-40-Based Service Adapter

Depending on the circumstances you might need to install a new service adapter on a VIP2-40 motherboard or replace a failed service adapter in the field. In either case, you need a number 1 Phillips screwdriver, an antistatic mat onto which you can place the removed interface processor, and an antistatic container into which you can place a failed service adapter for shipment back to the factory. There are no chassis slot restrictions on where the VIP2--40-equipped ESA can be installed.

shows a VIP2-40 with an ESA in service adapter slot 1. Most of the currently available port adapters, which are compatible with the VIP2-40, can be installed on a VIP2-40 alongside the ESA. (For specific port adapter prerequisites for VIP2-40 and the Cisco 7200 series routers, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.)

Figure 5 VIP2-40 with a PA-4E and an ESA Installed (Horizontal Orientation Shown)



Caution To prevent system problems, do not remove service adapters from the VIP2-40 motherboard, or attempt to install other service adapters on the VIP2-40 motherboard while the system is operating. To install or replace service adapters, first remove the VIP2-40 from its interface processor slot.

Note Each service adapter circuit board is mounted to a metal carrier and is sensitive to ESD damage. The following procedures should be performed by a Cisco-certified service provider only. While the VIP2-40 supports online insertion and removal, individual service adapters do not. To replace service adapters, you must first remove the VIP2-40 from the chassis, then install or replace service adapters as required. If a blank port adapter is installed on the VIP2-40 in which you want to install a new service adapter, you must first remove the VIP2-40 from the chassis, then remove the blank port adapter. You must also have a port adapter in the adjacent port adapter slot.

Following is the standard procedure for removing and replacing any type of service adapter on the VIP2-40:

Step 1 Attach an ESD-preventive wrist strap between you and an unfinished chassis surface.

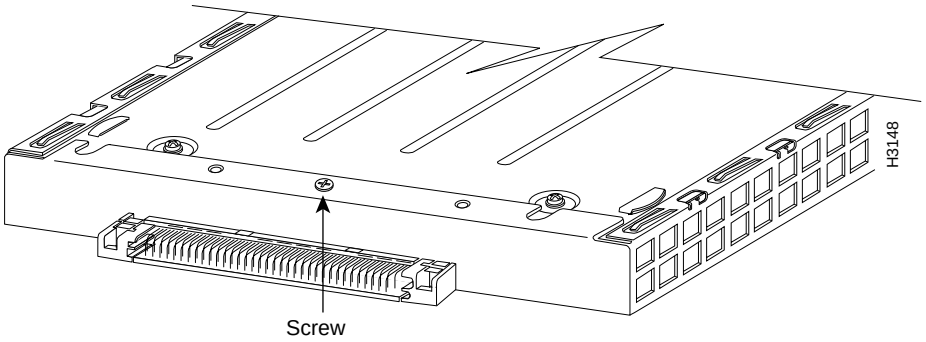
Step 2 For a new service adapter installation or a service adapter replacement, disconnect any interface cables from the ports on the front of the adjacent port adapter on the VIP2-40, although, this is not required. You can remove VIP2-40s with cables attached; however, we do not recommend it.

Step 3 To remove the VIP2-40 from the chassis, follow the steps in the section "Removing a VIP2" in the configuration note *Second-Generation Versatile Interface Processor (VIP2) Installation and Configuration* (Document Number 78-2658-xx), which shipped with your VIP2-40.

Step 4 Place the removed VIP2-40 on an antistatic mat.

Step 5 Locate the screw at the rear of the service adapter (or blank service adapter) to be replaced. (See .) This screw secures the service adapter (or blank service adapter) to its slot.

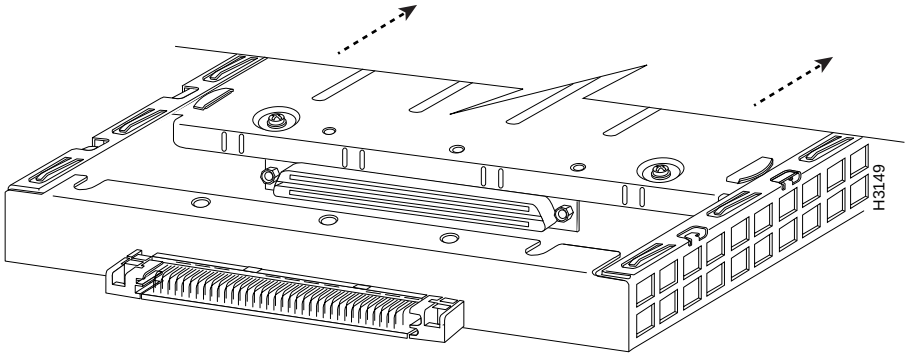
Figure 6 Location of Service Adapter Screw (Partial Service Adapter View)



Step 6 Remove the screw that secures the service adapter (or blank service adapter).

Step 7 With the screw removed, grasp the handle on the front of the service adapter (or blank service adapter) and carefully pull it out of its slot, away from the edge connector at the rear of the slot. (See .)

Figure 7 Pulling a Service Adapter Out of a Slot (Partial Service Adapter View)

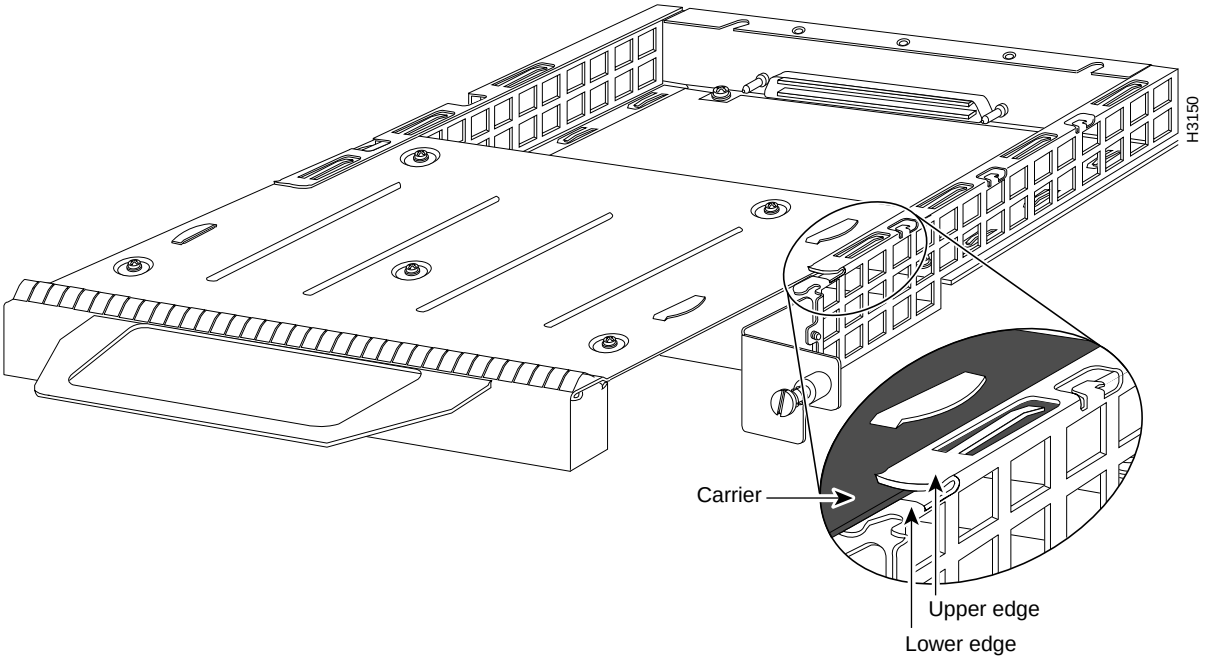


Step 8 If you removed a service adapter, place it in an antistatic container for safe storage or shipment back to the factory. If you removed a blank service adapter, no special handling is required; however, store the blank service adapter for potential future use.

Step 9 Remove the new service adapter from its antistatic container and position it at the opening of the slot. (See Figure 8.)

Caution To prevent jamming the carrier between the upper and lower edges of the service adapter slot, and to assure that the edge connector at the rear of the service adapter mates with the connector at the rear of the service adapter slot, make certain that the leading edges of the carrier are between the upper and lower slot edges, as shown in the cutaway in Figure 8.

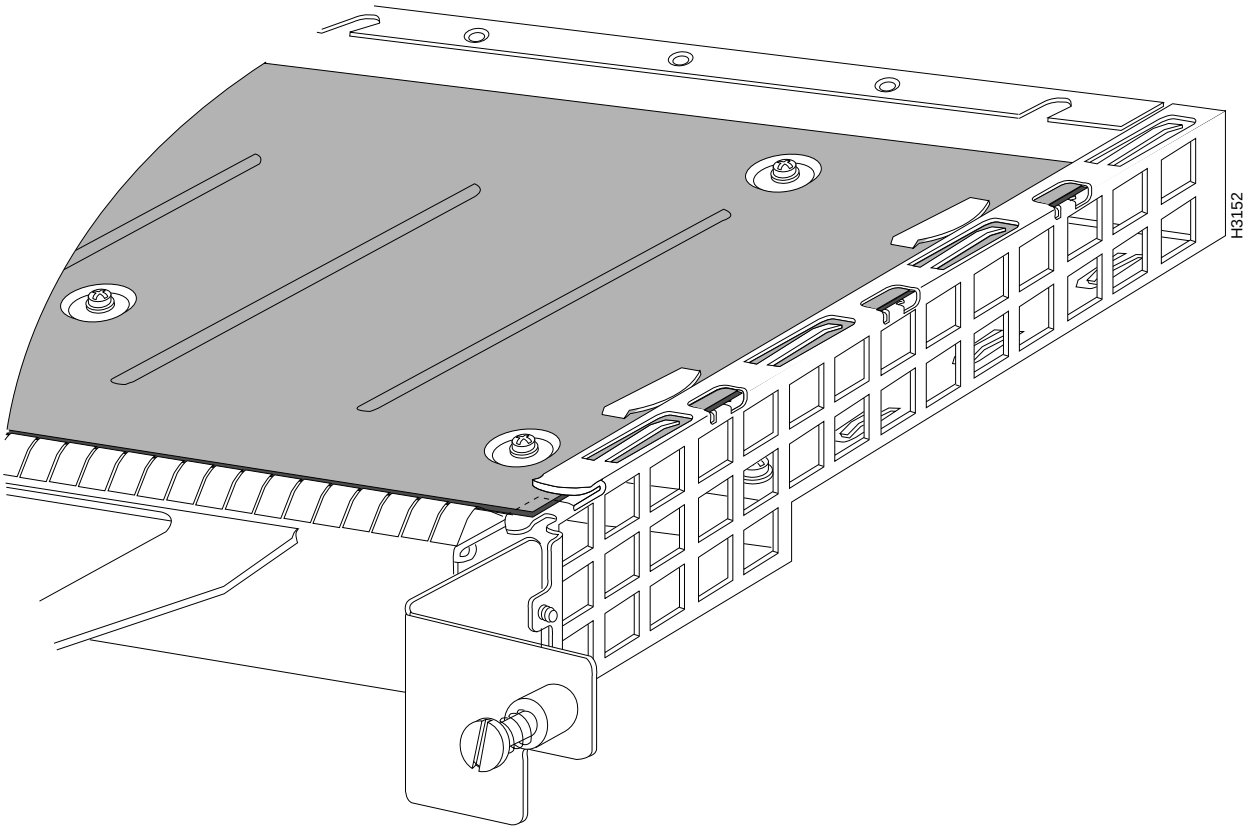
Figure 8 Inserting a Service Adapter



Caution To ensure a positive ground attachment between the service adapter carrier and the VIP2-40 motherboard and service adapter slot, and to ensure that the connectors at the rear of the service adapter and slot mate properly, the carrier must be between the upper and lower slot edges, as shown in .

Step 10 Carefully slide the new service adapter into the service adapter slot (see Figure 9) until the connector on the service adapter is completely mated with the connector at the rear of the service adapter slot.

Figure 9 Aligning the Carrier Edge with Upper and Lower Slot Edges (Partial View)



Step 11 Install the screw in the rear of the service adapter slot. (See for its location.) Do not overtighten this screw.

Step 12 To replace the VIP2-40, follow the steps in the section "Installing a VIP2" in the configuration note *Second-Generation Versatile Interface Processor (VIP2) Installation and Configuration* (Document Number 78-2658-xx), which shipped with your VIP2-40.

Step 13 If disconnected, reconnect the interface cables to the interface processor.

This completes the procedure for installing a new service adapter or replacing a service adapter on a VIP2-40.

Installing or Replacing a Service Adapter in Cisco 7200 Series Routers

Depending on your circumstances, you might need to install a new service adapter in a Cisco 7200 series router, replace a failed service adapter in the field, or replace a port adapter with a service adapter. In either case, no tools are necessary; all port and service adapters available for the Cisco 7200 series connect directly to the router midplane and are locked into position by a port adapter lever. When

removing and replacing a port or service adapter, you will need an antistatic mat onto which you can place a removed port or service adapter and an antistatic container into which you can place a failed service adapter for shipment back to the factory.

Note The procedures required to remove and replace a service adapter or a port adapter in a Cisco 7200 series router are identical. The Cisco 7200 series routers support OIR; therefore, you do not have to power down the Cisco 7200 series routers when removing and replacing a service adapter. There are no chassis slot restrictions on where the ESA can be installed; however, we recommend that you fully understand OIR functionality in the Cisco 7200 series routers *before* ESA installation; refer to the section "Enabling the ESA in the Cisco 7200 Series" on page 33.

When a chassis slot is not in use, a blank adapter must fill the slot to allow the router to conform to EMI emissions requirements and to allow proper air flow across the port and service adapters.To install a new service adapter in a slot that is not in use, you must first remove a blank adapter.

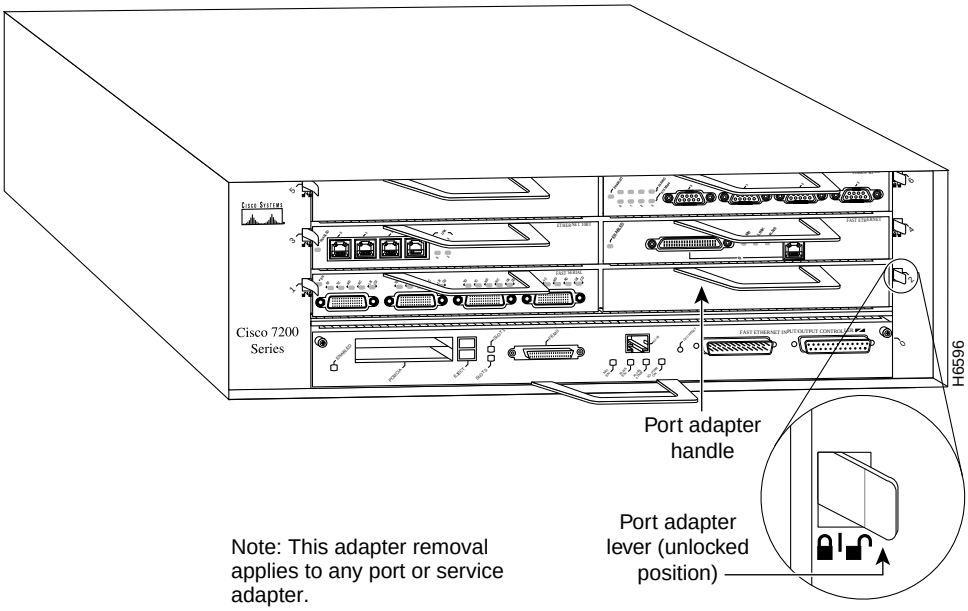
Removing a Port or Service Adapter

Following is the procedure for removing a port or service adapter from a Cisco 7200 series router:

Step 14 Attach an ESD-preventative wrist strap between you and an unfinished chassis surface.

Step 15 Place the port adapter lever for the desired adapter slot in the unlocked position. The port adapter lever remains in the unlocked position. (See Figure 10.)

Figure 10 Placing the Port Adapter Lever in the Unlocked Position (Cisco 7206 Shown)



Step 16 Grasp the handle on the port or service adapter and pull it from the midplane, about halfway out of its slot. If you are removing a blank adapter, pull the blank adapter from the chassis slot.

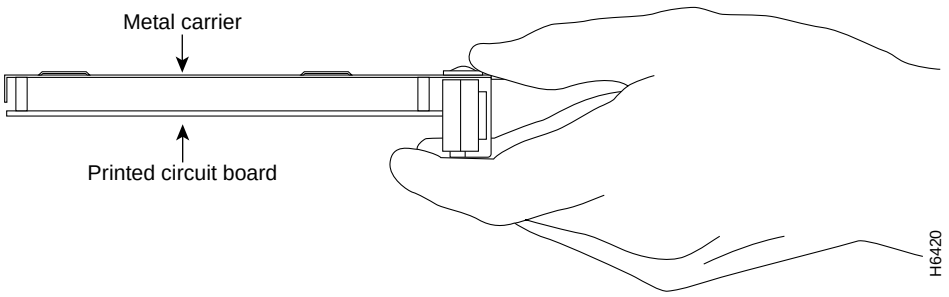
Note As you disengage a port adapter from the router midplane, OIR administratively shuts down all active interfaces on the port adapter. Service adapters do not have interfaces.

Step 17 With the port adapter halfway out of the slot, disconnect all cables from the port adapter. No cables attach to service adapters.

Step 18 After disconnecting the cables, pull the adapter from its chassis slot.

Caution Always handle the port or service adapter by the carrier edges and handle; never touch the port adapter's components or connector pins. (See Figure 11.)

Figure 11 Handling a Port or Service Adapter



Step 19 Place the adapter on an antistatic surface with its components facing upward, or in a static shielding bag. If the adapter will be returned to the factory, immediately place it in a static shielding bag.

This completes the procedure for removing a port or service adapter from a Cisco 7200 series router.

Replacing a Service Adapter

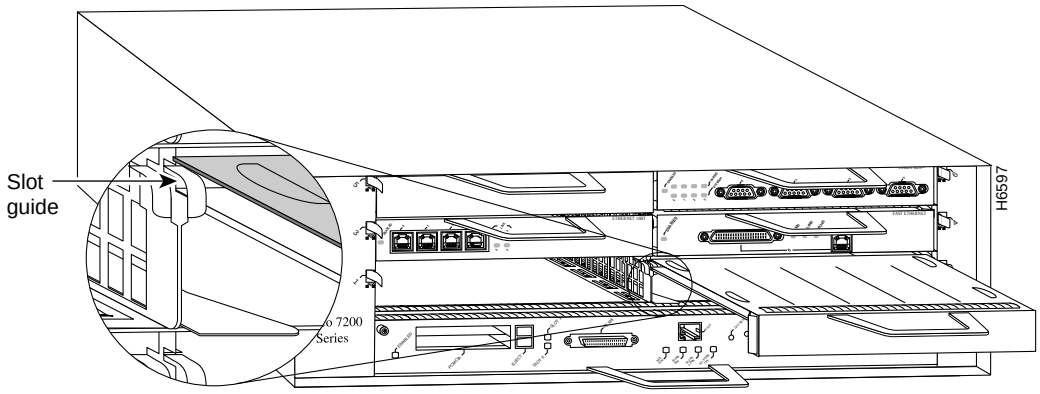
Following is the procedure for installing a new service adapter in a Cisco 7200 series router:

Step 1 Attach an ESD-preventative wrist strap between you and an unfinished chassis surface.

Step 2 Use both hands to grasp the service adapter by its metal carrier edges and position the service adapter so that its components are downward. (See).

Step 3 Align the left and right edge of the service adapter metal carrier between the guides in the service adapter slot. (See Figure 12.)

Figure 12 Aligning the Service Adapter Metal Carrier Between the Slot Guides (Cisco 7206 Shown)



Note: This adapter alignment applies to any port or service adapter.

Step 4 With the metal carrier aligned in the slot guides, gently slide the service adapter halfway into the slot.

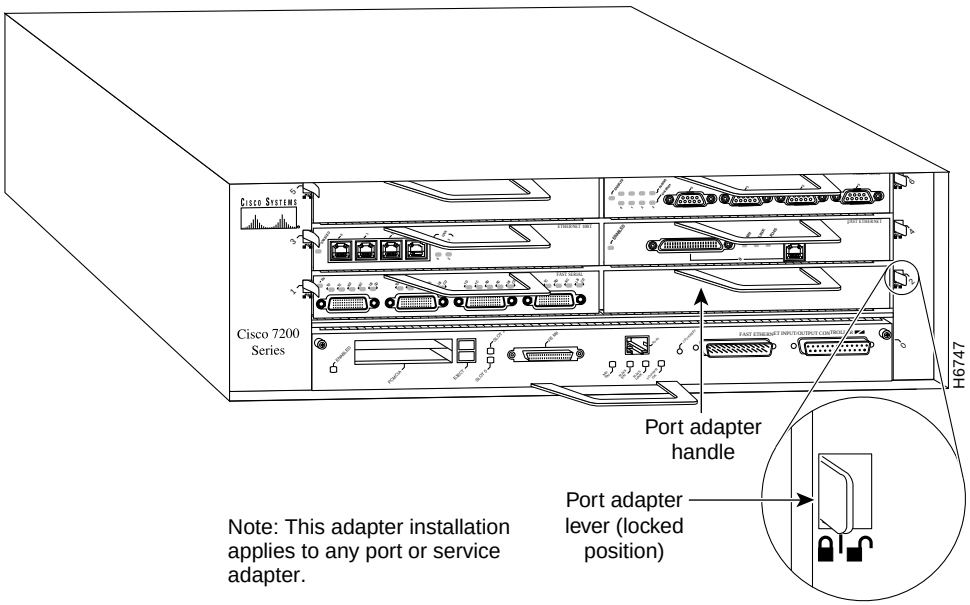
Caution Do not slide the service adapter all the way into the slot until you have connected all required cables. Trying to do so will disrupt normal operation of the router.

Step 5 Carefully slide the service adapter all the way into the slot until you feel the service adapter's connectors mate with the midplane.

Step 6 Move the port adapter lever to the locked position. shows the port adapter lever in the locked position.

Note If the port adapter lever does not move to the locked position, the adapter is not completely seated in the midplane. Carefully pull the adapter halfway out of the slot, reinsert it, and move the port adapter lever to the locked position.

Figure 13 Placing the Port Adapter Lever in the Locked Position (Cisco 7206 Shown)



This completes the procedure for installing a new service adapter in a Cisco 7200 series router.

Data Encryption Configuration Fundamentals and Sample Configurations

The remainder of this configuration note describes how to configure your Cisco 7000 family router for network data encryption with router authentication, and includes the following sections:

For a complete description of the commands mentioned in this configuration note, refer to the section "Network Data Encryption and Router Authentication Commands" in the *Security Command Reference* publication.

Cisco System's Network Data Encryption with Router Authentication

To safeguard your network data, Cisco provides network data encryption and router authentication services. Network data encryption is provided at the IP packet level. IP packet encryption prevents eavesdroppers from reading the data that is being transmitted. When IP packet encryption is used, IP packets can be seen during transmission, but the IP packet contents (payload) cannot be read. Specifically, the IP header and upper-layer protocol (TCP or UDP) headers are not encrypted, but all payload data within the TCP or UDP packet will be encrypted and therefore not readable during transmission.

The actual encryption and decryption of IP packets occurs only at routers that you configure for network data encryption with router authentication. Such routers are considered to be *peer encrypting routers* (or simply *peer routers*). Intermediate hops do not participate in encryption/decryption.

Note Encryption should not be enabled in the intermediate routers; otherwise, unnecessary encryption/decryption cycles might result in a subsequent reduction in overall system performance.

Typically, when an IP packet is initially generated at a host, it is unencrypted ("clear text"). This occurs on a secured (internal) portion of your network. Then when the transmitted IP packet passes through an encrypting router, the router determines if the packet should be encrypted. If the packet is encrypted, the encrypted packet will travel through the unsecured network portion (usually an external network such as the Internet) until it reaches the remote peer encrypting router. At this point, the encrypted IP packet is decrypted, and forwarded to the destination host as clear text.

Router authentication enables peer encrypting routers to positively identify the source of incoming encrypted data. This means that attackers cannot forge transmitted data or tamper with transmitted data without detection. Router authentication occurs between peer routers each time a new *encrypted session* is established.

An encrypted session will be established each time an encrypting router receives an IP packet that should be encrypted (unless an encrypted session is already occurring at that time).

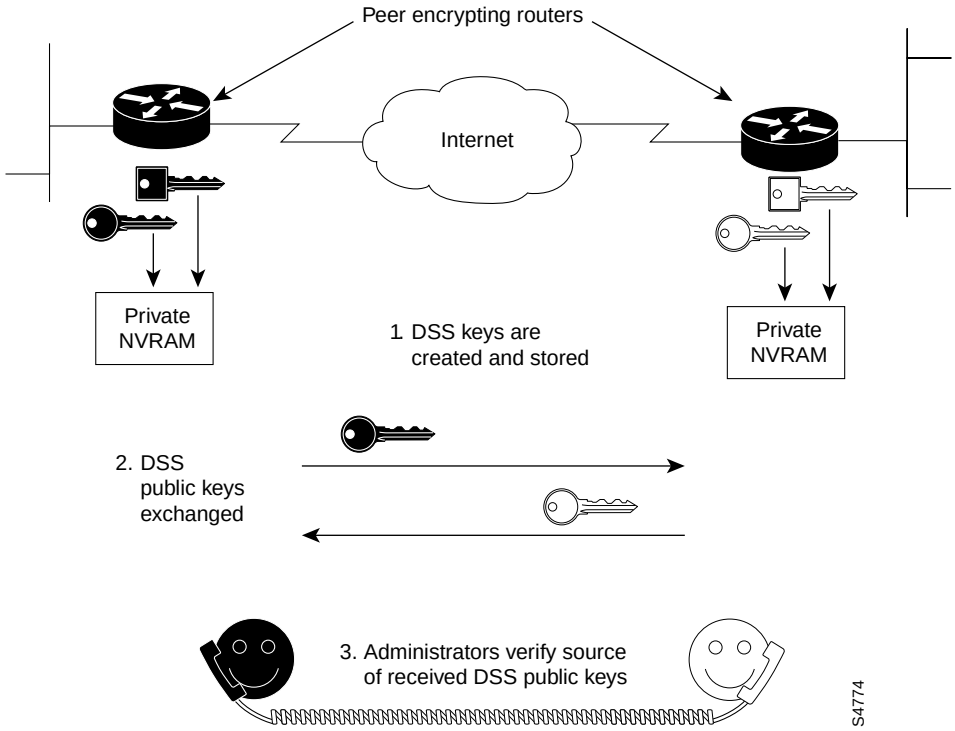
To provide IP packet encryption with router authentication, Cisco implements the following standards: Digital Signature Standard (DSS), the Diffie-Hellman (DH) public key algorithm, and Data Encryption Standard (DES). DSS is used in router authentication. The DH algorithm and DES are used to initiate and conduct encrypted communication sessions between participating routers.

The following sections provide an overview of Cisco's data encryption and router authentication.

Enabling Router Authentication (DSS Key Exchange)

Before encrypted communication or router authentication can occur between peer routers, DSS keys (public and private) must be generated. Also, the DSS public keys must be shared and verified (see Figure 14).

Figure 14 Exchanging DSS Keys (Overview)



This process occurs only once, and the DSS keys will be used each time an encrypted session occurs after that. The DSS keys are used at the beginning of encrypted sessions to authenticate the peer encrypting router (the source of encrypted data). Each peer router must generate and store two unique DSS keys: a DSS public key, and a DSS private key. DSS public and private keys are stored in a private portion of the router's NVRAM, which cannot be viewed with commands such as **show configuration**, **show running-config**, or **write terminal**. DSS keys are stored in the tamper-resistant memory of the ESA.

The DSS private key is not shared with any other device. However, the router's DSS public key is distributed to all other peer routers. After public keys are sent to peer routers, the routers' administrators must verbally verify to each other the public key's source router. (The verbal verification is sometimes referred to as "voice authentication.")

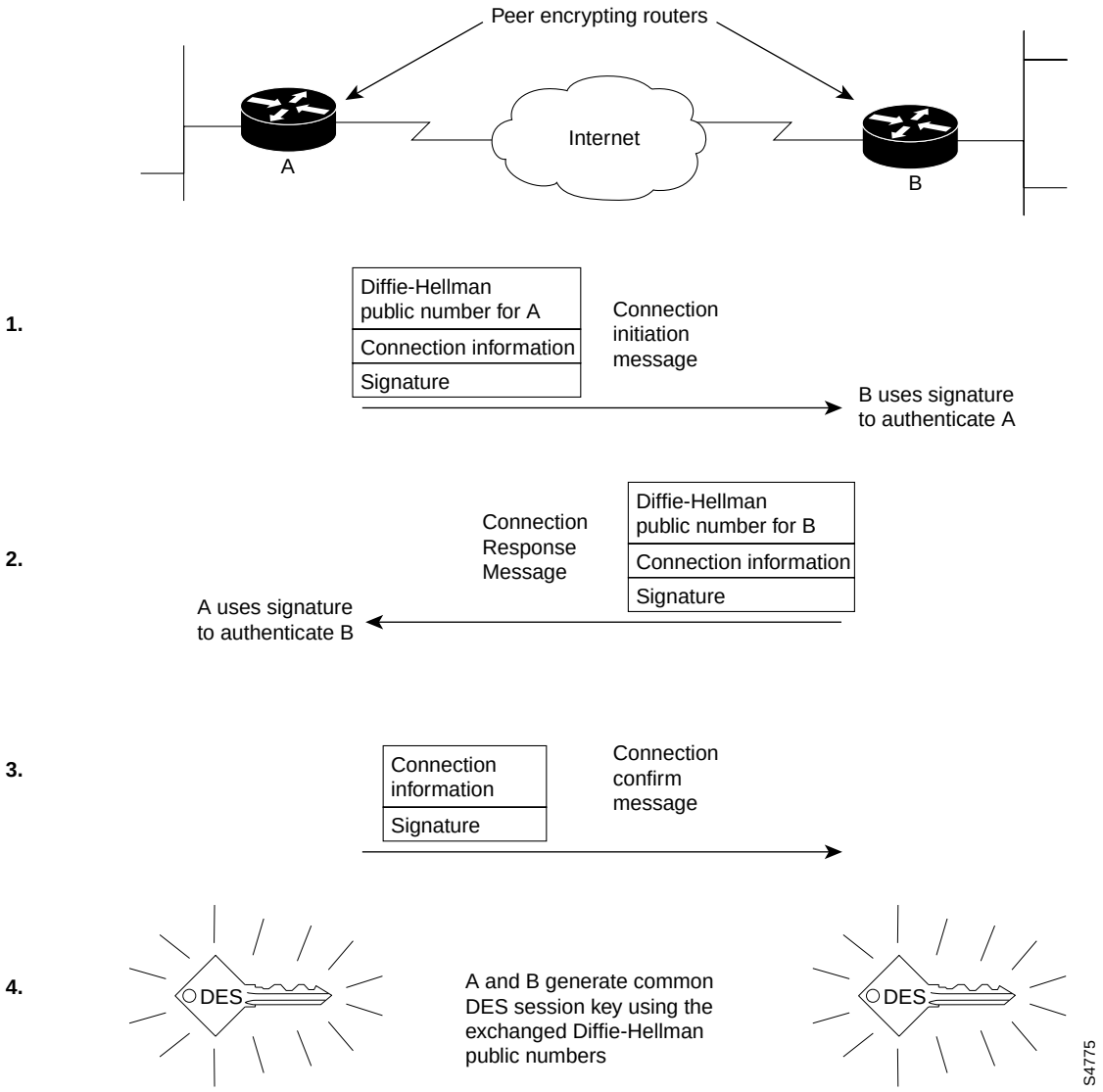
Establishing an Encrypted Session

When a Cisco router wants to send encrypted data to a peer router, it must first establish an encrypted session. (See Figure 15.)

To establish the session, the two peer routers exchange connection messages. These messages have two purposes. The first purpose is to authenticate each router to the other. This is accomplished by attaching "signatures" to the connection messages. A signature is a character string that is created by each router using its DSS private key and verified by the other router using the corresponding DSS public key. A signature is always unique to the sending router and cannot be forged by any other device. When a signature is verified, the sending router is authenticated.

The second purpose of the connection messages is to generate a temporary DES key (*session key*), which is the key that will be used to encrypt data during this encrypted session. To generate the DES key, DH numbers must be exchanged in the connection messages. Then, the DH numbers are used to compute a common DES session key that is shared by both routers.

Figure 15 Establishing an Encrypted Session



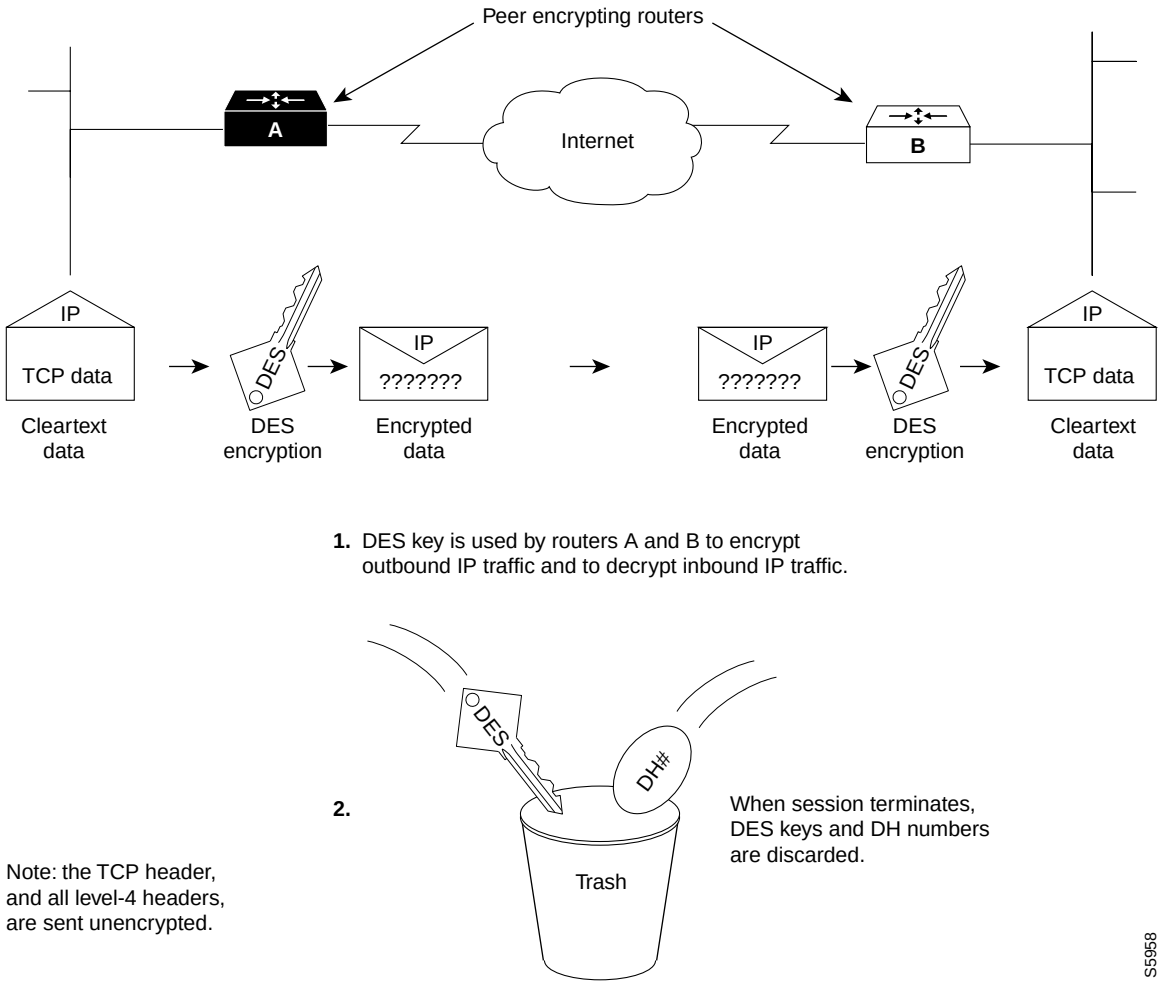
Encrypting Data During a Communication Session

When both routers are authenticated and the session key (DES key) has been generated, data can be encrypted and transmitted. A DES encryption algorithm is used with the DES key to encrypt and decrypt IP packets during the encrypted session. (See Figure 16.)

Note The TCP headers, and all level-4 headers, are sent unencrypted.

An encrypted communication session will terminate when the session times out. When the session terminates, both the DH numbers and the DES key are discarded. When another encrypted session is required, new DH numbers and DES keys will be generated.

Figure 16 Encrypting Data



Issues to Consider Before Configuring Encryption/Authentication

You should understand the issues explained in this section before attempting to configure your system for network data encryption with router authentication.

Implementation Issues

Please note the following issues:

- Cisco IOS software supports IP fragmentation for software (SW) and hardware (HW) encryption on all platforms except the VIP2-40.
- Using the Cisco IOS crypto engine, you can use any type of encapsulation with IP encryption. For example, if you want to encrypt AppleTalk traffic, you can encapsulate the AppleTalk traffic within an IP tunnel, and then encrypt the IP payload. The tunneling and encryption functions can be performed at the same router.
- If you have an ESA-equipped VIP2-40 with one of the currently available and supported wide-area network (WAN) port adapters installed, encryption will not work for traffic on these interfaces unless you use Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) protocol, or Frame Relay. This applies *only* to Cisco System's WAN port adapters on the VIP2-40. (This does not apply to the Cisco 7200 series routers.)
- Frame Relay does not support distributed switching on the VIP2-40. Incoming packets are decrypted or encrypted in the VIP2-40 and then sent to the RSP for switching.
- Generic routing encapsulation (GRE) is supported on the ESA; GRE allows you to encapsulate any protocols inside a GRE tunnel, and then encrypt the payload.
- Encrypted multicast is not supported.
- Each encrypting router can set up encrypted sessions with many other routers if these are peer encrypting routers. Encrypting routers can also set up multiple simultaneous encrypted sessions with multiple peer routers. Up to 299 concurrent encrypted sessions per router can be supported.
- Because of the high amount of processing required for encryption, if you use encryption heavily there will be performance impacts such as interface congestion or slowed CPU functionality. Using an ESA crypto engine rather than the Cisco IOS crypto engine can improve overall router performance because the Cisco IOS software will not be impacted by encryption/authentication processing.
- When an encrypted session is being set up, any packets that are intended to be encrypted will be dropped until the session setup is complete.
- If NVRAM fails, or if your ESA is tampered with or replaced, DSS public/private keys will no longer be valid. If this happens, you will need to regenerate and re-exchange DSS keys. Generating and exchanging DSS keys are described later in this configuration note in the section "Essential Encryption/Authentication Configuration Tasks."
- If you encrypt data over a serial link, and if encrypted session setup times are too long, the serial link might experience frequent drops during setup (this can be seen at the router console). This can be avoided by changing the link's keepalive value, or by enabling pregeneration of DH numbers (described later in this configuration note).
- Hosts might experience difficulty in establishing a Telnet session, if the session uses two encrypting peer routers to create the connection. This is more likely to occur if the peer routers are routers such as Cisco 2500 series routers. This occurs if the Telnet connection attempt times out before the encrypted session setup is complete.
- If this occurs, the host should wait a short time (a few seconds might be sufficient), and then attempt the Telnet connection again. By this time the encrypted session should be set up, and the Telnet session can be established. Enabling pregeneration of DH numbers (described later in this configuration note) might also help by speeding up encryption session connection setup times.
- After you configure your router for encryption/authentication, we recommend making a backup of your configuration. (Be careful to restrict unauthorized access of this backed-up configuration.)

Peer Router Identification

You must identify all peer routers which will be participating in IP packet encryption/router authentication. These are usually all routers within your administrative control that will be passing classified, confidential, or critical data using IP packets. Participating peer routers might also include routers not within your administrative control; however, this should only be the case if you share a trusted, cooperative relationship with the other router's administrator. This person should be known and trusted on a personal level by you, and known and trusted by your organization.

Network Topology

Take care in choosing a network topology between peer encrypting routers. Particularly, you should set up the network so that a stream of IP packets must use exactly one pair of encrypting routers at a time. Do not nest levels of encrypting routers. (That is, do not put encrypting routers in between two peer encrypting routers.)

Frequent route changes between pairs of peer encrypting routers, including for purposes of load balancing, will cause excessive numbers of connections to be set up and very few data packets to be delivered. Note that load balancing can still be used, but only if done transparently to the encrypting peer routers. That is, peer routers should *not* participate in the load balancing; *only* devices in between the peer routers should provide load balancing. A common network topology used for encryption is a hub-and-spoke arrangement between an enterprise router and branch routers. Also, Internet firewall routers are often designated as endpoint peer routers.

The Cisco IOS Crypto Engine

A software-controlled crypto engine resides in your router's encryption-capable Cisco IOS software (called a *crypto image*) and provides encryption/authentication services for all router ports that you specify during configuration. (The Cisco IOS crypto engine governs encryption/authentication for all router ports.)

All Cisco routers have only one Cisco IOS crypto engine that governs all ports, *except for* Cisco 7000 series routers and Cisco 7500 series routers, which can have more than one crypto engine when a VIP2-40 or ESA-equipped VIP2-40 is installed. For these routers, the Cisco IOS crypto engine resides in the Route Switch Processor (RSP) and any second-generation Versatile Interface Processors (VIP2-40s) that are installed.

Use the **show version** command to verify that you have a Cisco IOS crypto image loaded, as shown following for a Cisco 7200 series router and a Cisco 7500 series router:

```
Router# show version
Cisco Internetwork Operating System Software
--> IOS (tm) 7200 Software (C7200-IS56-M), Released Version 11.2(7a)P [biff 1145]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 19-Feb-97 10:17 by biff

Router# show version
Cisco Internetwork Operating System Software
--> IOS (tm) RSP Software (RSP-ISV56-M), Released Version 11.2(7)P [biff 722]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 19-Feb-97 16:47 by biff
```

The VIP2 Crypto Engine

Cisco 7500 series routers and Cisco 7000 series routers, with the RSP7000 installed, support the VIP2-40. The VIP2-40 has its own Cisco IOS crypto engine (if a Cisco IOS crypto image is running), which governs the ports on the port adapter that is installed adjacent to the ESA on the VIP2-40.

Therefore, if you have a VIP2-40 installed in your router, the VIP2 crypto engine will govern the adjacent port adapter's ports, and the Cisco IOS crypto engine on the RSP will govern all remaining router ports. If there is no VIP2-40, the Cisco IOS crypto engine on the RSP will govern all router ports.

If there is an ESA installed on a VIP2-40, the crypto engine will be a hardware (HW) crypto engine, and the encryption/decryption functions will be executed by the ESA. In this case, the **show process** command will reveal three processes related to the crypto engine.

Following is an example of the **show process** command in this case:

```
Router# show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID  QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process

      (additional displayed text omitted from this example)

  21 Hwe 604E8C0C            0          1       0 5608/6000   0 Crypto HW Proc
  22 Mwe 604BDD20            0      12168       011596/12000  0 Crypto SM
  23 Hwe 607C3A38            0          1       0 5628/6000   0 Encrypt Proc

  (additional displayed text omitted from this example)

Router#
```

Conversely, if no ESA and VIP2-40 is installed, the crypto engine will be the Cisco IOS crypto engine, and the encryption/decryption functions will be executed by the RSP and the Cisco IOS crypto image. Further, the **show process** command will reveal the existence of only two processes related to the Cisco IOS crypto engine.

Following is an example of the **show process** command in this case:

```
Router# show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID  QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process

      (additional displayed text omitted from this example)

  21 Hwe 604E8C0C            0          1       0 5608/6000   0 Crypto HW Proc
  22 Mwe 604BDD20            0      12168       011596/12000  0 Crypto SM
```

The Cisco 7200 Series Crypto Engine

In the Cisco 7200 series routers, there can only be one functioning crypto engine, as follows:

- The Cisco IOS (software) crypto engine, which governs all router ports used for encryption/decryption

  or

- The hardware crypto engine on the ESA, if one is installed, which governs all router ports used for encryption/decryption

Note Only a single ESA can be installed in the Cisco 7200 series routers.

If there is no ESA installed in the Cisco 7200 series router, and a Cisco IOS crypto image is loaded into the Cisco 7200 series router, then there will be a Cisco IOS crypto engine running on the router. (In other words, encryption, decryption, key generation, and so forth, will be performed by the router's CPU in software.)

If there is an ESA installed in the Cisco 7200 series router, the crypto engine will be a HW crypto engine, and the encryption/decryption functions will be executed by the ESA. In this case, the **show process** command will reveal three processes related to the crypto engine and one process related to online insertion and removal (OIR), with respect to the ESA in the Cisco 7200 series router.

Following is an example of the **show process** command in this case:

```
Router# show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID  QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process

      (additional displayed text omitted from this example)

  21 Hwe 604E8C0C            0          1       0 5608/6000   0 Crypto HW Proc
  22 Mwe 604BDD20            0      12168       011596/12000  0 Crypto SM
  23 Hwe 607C3A38            0          1       0 5628/6000   0 Encrypt Proc
  24 Hwe 607C4328            0          3       0 5148/6000   0 Key Proc

  (additional displayed text omitted from this example)
```

Conversely, if no ESA is installed in the Cisco 7200 series router, the crypto engine will be the Cisco IOS crypto engine, and the encryption/decryption functions will be executed by the Cisco 7200 series router's CPU. Further, the **show process** command will reveal only two processes related to the Cisco IOS crypto engine.

Following is an example of the **show process** command in this case:

```
Router# show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID  QTy       PC Runtime (ms)    Invoked   uSecs    Stacks TTY Process

      (additional displayed text omitted from this example)

  21 Hwe 604E8C0C            0          1       0 5608/6000   0 Crypto HW Proc
  22 Mwe 604BDD20            0      12168       011596/12000  0 Crypto SM

  (additional displayed text omitted from this example)
```

The Data Encryption Service Adapter Crypto Engine

If you have a Cisco 7000 series or Cisco 7500 series router with an ESA, your router will have an additional crypto engine associated with the ESA, called the *hardware (HW) crypto engine*.

If you have a Cisco 7200 series router, your router will have either the Cisco IOS crypto engine, or the HW crypto engine associated with the ESA.

In the Cisco 7000 and Cisco 7500 series routers, the ESA and a compatible port adapter are attached to a VIP2-40, and the ESA's HW crypto engine provides encryption/authentication services *only* for ports on the adjoining VIP2-40 port adapter. Most of the currently available port adapters, which are

compatible with the VIP2-40, can be installed on a VIP2-40, or in a Cisco 7200 series router with an ESA. (For specific, additional port adapter limitations for VIP2-40 and the Cisco 7200 series, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.)

The Cisco IOS crypto engine will provide encryption/authentication for all remaining ports of your router. In other words, the ESA's HW crypto engine can govern the adjoining VIP2-40 port adapter's ports, and the Cisco IOS crypto engine governs all remaining ports in the router. This is also true if distributed switching is not enabled. (During configuration, you must specify which ports will participate in encryption/authentication.)

For Cisco 7200 series routers *without* an ESA installed, the Cisco IOS crypto engine will govern any port adapter's ports. For Cisco 7200 series routers *with* an ESA installed, the ESA's HW crypto engine will govern any port adapter's ports.

Configuration Guidelines for the Crypto Engine

For Cisco 7000 series, Cisco 7200 series, or Cisco 7500 series router with an ESA, you need to complete certain configuration tasks for each crypto engine of your router if you want that crypto engine to provide encryption/authentication for the ports it governs. These tasks are: generate DSS keys and exchange DSS keys. (These two tasks are described later in this configuration note, in the section "Essential Encryption/Authentication Configuration Tasks" on page 45.)

In Cisco 7000 series or 7500 series routers with one or more VIP2-40 and ESA, your router will have multiple crypto engines. When you configure these crypto engines, you must identify them by a chassis slot number. The HW crypto engines are identified by the chassis slot number in which the VIP2-40 and ESA is installed.

A VIP2-40 and RSP will perform encryption/decryption via software (the Cisco IOS crypto engine) if no ESA is installed on the VIP2-40. After you configure a Cisco IOS crypto engine, you can configure any port governed by that SW crypto engine to perform encryption/authentication. Most of the currently available port adapters, which are compatible with the VIP2-40, can be installed on a VIP2-40 alongside an ESA. (For specific, additional port adapter limitations for VIP2-40, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.)

The ESA can be installed in either port adapter slot 0 or 1 on the VIP2-40; however, you *must* install the appropriate port adapter in the VIP2-40 port adapter slot *adjacent* to the ESA.

In the Cisco 7200 series, the router has only one active crypto engine. If an ESA is installed, you must identify it by a chassis slot number, when you configure the crypto engine. You must also identify the ports that you want to use for encryption/decryption; these ports are identified by the chassis slot number(s) in which the port adapter is installed. After you configure the crypto engine, you can configure any port, which is governed by the crypto engine, to perform encryption/authentication.

Most of the currently available port adapters, which are compatible with the Cisco 7200 series, can be installed in a Cisco 7200 series router with an ESA. (For specific, additional port adapter limitations for the Cisco 7200 series, refer to the section "Hardware, Software, and Compliance Prerequisites" on page 11.)

Enabling the ESA in the Cisco 7200 Series

For Cisco 7200 series routers with an ESA, the tasks in this section must be used to enable or shutdown an ESA.

If the Cisco 7200 series router is booted with an ESA installed in it, or if you install the ESA after the router is operational, the ESA will not be put into service (that is, the router will not switch to the hardware crypto engine) until the extraction latch has been cleared, there are DSS keys stored on the ESA card, and the card is enabled.

The extraction latch is a hardware latch that is set when an ESA is removed and reinstalled in the chassis. When the extraction latch is set, the Tampered LED is on. You can clear the extraction latch on the ESA by using the **crypto clear-latch** global configuration command.

If the extraction latch is set or there are no DSS keys stored on the ESA, the router displays a message similar to the one below which shows that it switched to the software crypto engine.

```
SETUP: new interface ESA-Key2/1 placed in "shutdown" state
There are no keys on the ESA in slot 2- ESA not enabled

...switching to SW crypto engine
```

To determine if there are DSS keys stored on the ESA card, use the **show crypto card** command and look at the "DSS Key set" field in the output. If the field contains "Yes," the keys are stored.

If the crypto system on the Cisco 7200 series router is a software crypto engine and you install an ESA, the extraction latch is set, and the ESA enters a "pending" state. After the extraction latch is cleared, the crypto system checks to see if there are any keys on the ESA card. If there are no keys, the ESA card remains in a pending state. While the ESA is in a pending state, attempts to generate keys apply to the ESA and not the existing software crypto engine. However, the crypto system is still a fully functional software crypto engine and can sustain crypto connections in this state. To determine the ESA state, use the **show crypto engine brief** command and look at the "crypto engine state" field in the output.

To change the ESA's pending state, you must perform one of the following actions:

- Enable the ESA with the **crypto esa enable** global configuration command. You must also clear the extraction latch and generate keys for the ESA card before the ESA card is successfully enabled.
- Shutdown the ESA with the **crypto esa shutdown** global configuration command. After shutdown, the crypto engine reverts to the software crypto engine.

As mentioned above, after installing an ESA in a Cisco 7200 series router, you must enable the ESA before the hardware crypto engine becomes available. Until the ESA is enabled, the software crypto engine functions as the crypto engine. While the ESA hardware crypto engine is being enabled, crypto traffic will not pass through the hardware crypto engine. After the ESA is enabled, crypto traffic will pass through the hardware crypto engine and all preexisting software connections are closed and reestablished on the hardware crypto engine.

When an ESA is installed in a Cisco 7200 series router and the router already has crypto connections, the keys to maintain these connections do not disappear, but the keys on the ESA are used instead. However, the ESA cannot be used until, at a minimum, the extraction latch has been cleared. Keys might also need to be generated and if so, they keys must be exchanged between the peer routers before crypto connections can be established using the ESA. These tasks involving the ESA can take an indeterminate amount of time.

To enable the ESA on a Cisco 7200 series router when the ESA does not have keys, perform the following tasks beginning in global configuration mode:

Task	Command
Clear the extraction latch on the ESA.	crypto clear-latch *slot*
When prompted, enter the crypto card password.	password
Generate and exchange software keys between peer routers.	**crypto gen-signature-keys** *key-name* [*slot*][1]
When prompted, enter the crypto card password.	password
When prompted, reenter the crypto card password.	password
Specify the ESA to enable on the Cisco 7200 series router.	crypto esa enable *slot*
Exit global configuration mode.	exit

1.For more information, refer to the "Generate DSS Public/Private Keys" and the "Exchange DSS Public Keys" sections in the "Configuring Network Data Encryption with Router Authentication" chapter of the *Security Configuration Guide*.

To enable the ESA on a Cisco 7200 series router when the ESA already has keys, perform the following tasks beginning in global configuration mode:

Task	Command
Clear the extraction latch on the ESA.	crypto clear-latch *slot*
When prompted, enter the crypto card password.	password
When prompted, enter yes. If existing keys were found on the ESA, you are prompted to enable the ESA.	yes
Exit global configuration mode.	exit

To enable the ESA on a Cisco 7200 series router when the ESA already has keys but you want to generate new keys, perform the following tasks beginning in global configuration mode:

Task	Command
Clear the extraction latch on the ESA.	crypto clear-latch *slot*
When prompted, enter the crypto card password.	password
When prompted, enter no. If existing keys were found on the ESA, you are prompted to enable the ESA.	no
Generate and exchange software keys between peer routers.	**crypto gen-signature-keys** *key-name* [*slot*][1]
When prompted, enter yes to generate new DSS keys.	yes
When prompted, enter the crypto card password.	password
When prompted, reenter the crypto card password.	password
Specify the ESA to enable on the Cisco 7200 series router.	crypto esa enable *slot*
Exit global configuration mode.	exit

1.For more information, refer to the "Generate DSS Public/Private Keys" and the "Exchange DSS Public Keys" sections in the "Configuring Network Data Encryption with Router Authentication" chapter of the *Security Configuration Guide*.

Note With the **crypto esa enable** command, there is minimal crypto down time when an ESA is installed in a Cisco 7200 series router and there are already software crypto connections. This is because the crypto subsystem can continue to function as a software crypto engine while the hardware keys are being created and exchanged, or at least until the extraction latch has been cleared (if the ESA already had previously exchanged keys in its NVRAM).

For an example of enabling the ESA, refer to the "Configuration Example" section.

Shutting Down the ESA in the Cisco 7200 Series

On Cisco 7200 series routers, you can switch from the hardware crypto engine to the software crypto engine without manually removing the ESA from the slot by using the **crypto esa shutdown** global command. When an ESA is shutdown, there is crypto downtime if there are no preexisting software keys

that were exchanged before the ESA was shutdown. The crypto connections that existed before the extraction are closed—they cannot continue because their session keys were in the removed ESA's NVRAM.

The **crypto esa shutdown** global command allows you to minimize crypto engine unavailability and to generate and exchange software session keys.

To switch from the hardware crypto engine to the software crypto engine by shutting down the ESA (as if it were extracted), perform the following task in global configuration mode:

Task	Command
Specify the ESA to shutdown on the Cisco 7200 series router.	crypto esa shutdown *slot*

To reinstall the ESA using the **crypto esa enable** command, refer to the "Enabling the ESA" section.

Removing Keys In the Cisco 7200 Series

On Cisco 7200 series routers it is possible to have two sets of keys associated with one crypto engine slot (that is, keys can be exchanged with peers when there is a software crypto engine and also a hardware crypto engine). If there are two sets of keys, they will not be the same. Each set of keys has a serial number that is associated with the crypto engine. The **crypto zeroize** global configuration command only deletes keys that match the serial number of the current crypto engine. It is not possible to delete the ESA's keys until the crypto system switches to the hardware crypto engine. When using the hardware crypto engine, the slot of the ESA must be supplied in the **crypto zeroize** command.

To remove keys from the crypto engine on Cisco 7200 series routers when there are two sets of keys, perform the following tasks beginning in EXEC mode:

Task	Command
Determine if there are two sets of keys.	show crypto mypubkey
Determine the current crypto engine.	show crypto engine configuration
If the current crypto engine is the one you want to remove the keys from, delete the keys. or If the current crypto engine is not the one you want to remove keys from, go to step 5 or step 6.	**crypto zeroize** (for the software crypto engine) **crypto zeroize** *slot* (for the hardware crypto engine)
Switch to the hardware crypto engine. or Switch to the software crypto engine.	crypto esa enable *slot* or crypto esa shutdown *slot*

Task	Command
Verify that the crypto engine you want is now the current crypto engine.	show crypto engine configuration
Delete the keys from the current crypto engine.	**crypto zeroize** (for the software crypto engine) **crypto zeroize** *slot* (for the hardware crypto engine)

Cisco 7200 Series OIR Functionality for the ESA

For the Cisco 7200 series routers, online insertion and extraction of the ESA has special requirements for the crypto subsystem. Whether the crypto engine in the system is a hardware or software crypto engine is dependent on the presence of the ESA. If the ESA is extracted from the system, the crypto engine will reconfigure itself from a hardware crypto engine to a software engine. Conversely, if an ESA is inserted, the software crypto engine will reconfigure itself as a hardware engine; however, this reconfiguration is somewhat time dependent, which will be explained later.

Whenever the crypto engine is in the process of reconfiguring itself, all traffic flowing through the crypto engine is stopped and all crypto connections, which were established before the OIR event occurred, are halted and removed. This is done because the session keys for that connection might have disappeared as a result of the OIR event. When the crypto engine is fully reconfigured, traffic is allowed through the crypto engine. Since the crypto connections were previously closed, the initial packets sent will trigger the crypto connection setup.

At this point several potential issues arise. Consider first the case where the ESA is extracted. Since the crypto engine was a hardware crypto engine before ESA removal, the session keys used for the crypto connections were on the ESA, in nonvolatile random-access memory (NVRAM). Once the ESA is extracted, the private keys used to generate session keys must be present in NVRAM for the connection setup to occur without an interruption in the flow of packets through the crypto engine. If there are no software engine keys on the system at the time of the removal of the ESA, then crypto service will be interrupted until new keys are generated and exchanged with the peer routers.

The opposite scenario has a different set of issues. When an ESA is inserted into the Cisco 7200 series router, and the router already has crypto connections, the keys to maintain these connections have not disappeared, but the keys on the ESA are used instead. However, the ESA cannot be used until, at a minimum, the extraction latch has been cleared. Keys might also need to be generated and, if so, exchanged between the peer routers *before* crypto connections can be established using the ESA. These tasks involving the ESA can take an indeterminate amount of time.

For this reason, the **crypto esa enable** *slot* command is available to direct the crypto system to enable the ESA as the hardware crypto engine. Until this command is issued, the crypto engine will continue to function as a software crypto engine. When the **crypto esa enable** *slot* command is issued, crypto traffic will not pass through the crypto engine while the crypto engine is being reconfigured as a hardware crypto engine. When the reconfiguration is complete, crypto traffic will be allowed; however, at this point, all preexisting software connections are closed. Therefore, any packets that resume from the preexisting software connections will trigger the new crypto connection. After that, the crypto traffic will resume.

Note that with the **crypto esa enable** *slot* command, there is minimal crypto down time when an ESA is inserted, and there are already software crypto connections. This is because the crypto subsystem can continue to function as a software engine while hardware keys are being created and exchanged, or at least until the extraction latch has been cleared, if the ESA already has previously exchanged keys in its NVRAM.

When an ESA is extracted there is crypto downtime if there are no preexisting software keys that were exchanged before the ESA was extracted. The crypto connections that existed before the extraction are closed—they cannot continue because their session keys were in the extracted ESA's NVRAM.

To minimize crypto engine unavailability in this scenario, the **crypto esa shutdown** *slot* command is provided to shut down the ESA (as if it were extracted), and to generate and exchange software session keys. Then, the ESA can be reenabled, using the **crypto esa enable** *slot* command, and the crypto engine restarted.

The following example scenarios describe the operations required to provide your system with the least amount of downtime during crypto engine reconfiguration as a result of ESA OIR.

Scenario 1: ESA Extraction—Software Session Keys Not Pregenerated and Preexchanged

Following is the order of operations required if the ESA is extracted, but if software session keys are *not* first generated and exchanged.

Note Scenario 1 is not recommended due to its effects on system and crypto connection downtime, and is provided as an example only.

Step 1 Before crypto connections are set, generate and exchange hardware keys between peer routers: Router 1 and Router 2.

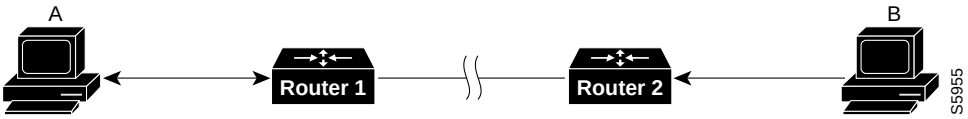
Step 2 A crypto connection exists between Router 1 and Router 2; encrypted traffic is flowing between Points A and B (a hardware crypto engine is configured on Router 1; ignore Router 2). (See .)

Figure 17 HW Crypto Engine Configured on Router 1—Crypto Connection between Router 1 and Router 2

Note: Router 1 is a HW crypto engine.

Step 3 Extract ESA from Router 1. There is no crypto connection while Router 1 is reconfigured as a software (SW) crypto engine. Packets sent between Points A and B get dropped while this occurs. (See .)

Figure 18 ESA Extracted—No Crypto Connection between Router 1 and Router 2



Note: SW crypto engine configuration is in progress.

Step 4 Generate software keys; packets sent between Points A and B are still being dropped.

Software keys are exchanged between peer routers (indeterminate duration). Packets between Points A and B get dropped while this occurs. (See .)

Step 5 Traffic between Points A and B triggers a crypto connection setup using generated and exchanged software keys; traffic can now continue to flow. Router1 is now configured as a software crypto engine. (See .)

Figure 19 SW Crypto Engine Configured on Router 1—Crypto Connection Exists between Router 1 and Router 2

Note: Router 1 is a SW crypto engine.

This completes the nonpreferred set of operations required for ESA extraction.

Scenario 2: ESA Extraction—Software Keys Pregenerated and Preexchanged

The following order of operations is required if the ESA is extracted, and software session keys *are* first generated and exchanged.

Note Scenario 2 is recommended over Scenario 1, due its clearly reduced effects on system and crypto connection downtime.

Step 1 Crypto connections are not yet set up; the ESA is still installed. In configuration mode, enter the following command to halt crypto sessions (slot 1 is used in the examples):

```
Router(config)# crypto esa shutdown 1

...switching to SW crypto engine

Router(config)#
```

Step 2 Generate software keys; exchange software keys between peer routers. In configuration mode, enter the following command to enable the ESA's HW crypto engine

```
Router(config)# crypto esa enable 1

...switching to HW crypto engine

Router(config)#
```

Step 3 Before crypto connections are set up, generate and exchange hardware keys between peer routers.

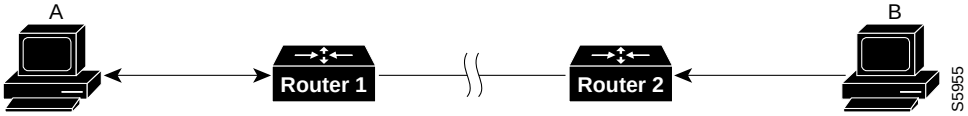
A crypto connection exists between Router 1 and Router 2; crypto traffic is flowing between Points A and B. The hardware crypto engine is configured on Router1; ignore Router 2. (See .)

Figure 20 HW Crypto Engine Configured on Router 1—Crypto Connection between Router 1 and Router 2

Note: Router 1 is a HW crypto engine.

Step 4 Extract ESA from Router1. There is no crypto connection while Router 1 is reconfigured as a software (SW) crypto engine. Packets sent between Points A and B get dropped while this occurs. (See .)

Figure 21 ESA Extracted—No Crypto Connection between Router 1 and Router 2



Note: SW crypto engine configuration is in progress.

Traffic between Points A and B will trigger the crypto-connection setup using software keys, and traffic continues to flow between Points A and B. Router 1 is now configured as a software engine. (See .)

Figure 22 SW Crypto Engine Configured on Router 1—Crypto Connection between Router 1 and Router 2

Note: Router 1 is a SW crypto engine.

This completes the preferred set of operations required for ESA online extraction.

Scenario 3: ESA Insertion

The following order of operations is required when the ESA is inserted:

Step 1 Generate and exchange software keys between peer routers.

Traffic between A and B will trigger the crypto connection setup using software keys, and traffic can continue to flow. (See .)

Figure 23 SW Crypto Engine Configured on Router 1—Crypto Connection between Router 1 and Router 2

Note: Router 1 is a SW crypto engine.

Step 2 Insert the ESA. The crypto engine on Router 1 is still a software crypto engine; traffic is still flowing between Points A and B. (See .)

Step 3 In configuration mode, use the **crypto clear-latch** *slot* command to clear the extraction latch on the ESA. Traffic is still flowing between Points A and B. (See .) When you clear the extraction latch on the ESA, the system will try to find keys associated with the ESA. If no associated keys exist, a console message indicating that the ESA is not enabled will appear.

If keys are found, a prompt will appear asking you to enable the ESA. If you enter “yes,” the ESA will be enabled; if you enter “no,” the ESA will not be enabled. Following are examples of these two choices.

Enable the ESA after clearing the extraction latch, as follows:

```
Router# show crypto card
```

```
Crypto card in slot: 2

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702

Router# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto clear-latch 2
% Enter the crypto card password.
Password:
Keys were found for this ESA- enable ESA now? [yes/no]: y
...switching to HW crypto engine

[OK]
Router(config)# exit
Router#
```

Do *not* enable the ESA card after clearing the extraction latch, as follows:

```
Router# show crypto card

Crypto card in slot: 2

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702

Router# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# crypto clear-latch 2
% Enter the crypto card password.
Password:
Keys were found for this ESA- enable ESA now? [yes/no]: n
ESA in slot 2 not enabled
[OK]

Router(config)# exit
Router#
```

Step 4 If necessary, generate and exchange hardware keys between peer routers. Router 1 is still configured as a software crypto engine; traffic still flowing between Points A and B. (See .).

SW Crypto Engine Configured on Router 1—Crypto Connection between Router 1 and Router 2

Note: Router 1 is a SW crypto engine.

Step 5 In configuration mode, enable the ESA using the **crypto esa enable** *slot* command:

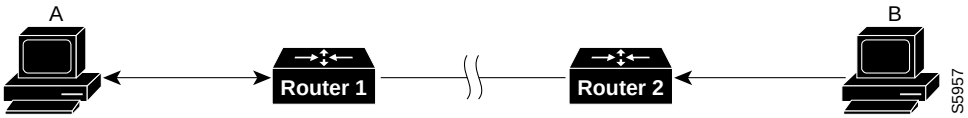
```
Router(config)# crypto esa enable 1

...switching to HW crypto engine

Router(config)#
```

Traffic now stops flowing between Points A and B while Router 1 reconfigures as a hardware crypto engine. (See .)

Figure 24 ESA Installed—No Crypto Connection between Router 1 and Router 2



Note: Router 1 HW crypto engine configuration is in progress.

A crypto connection between Router 1 and Router 2 is now established; traffic is flowing between Points A and B. The installed ESA's hardware crypto engine is now configured in Router 1. (See .)

Figure 25 ESA's HW Crypto Engine Configured on Router 1—Crypto Connection between Router 1 and Router 2

Note: Router 1 is a HW crypto engine.

This completes the operations required for ESA online insertion.

Configuration Example

The following example shows how to enable the ESA in slot 2 when there are no keys on the ESA card. This example shows that you must clear the extraction latch before the ESA can be enabled.

```
Apricot# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Apricot(config)# crypto esa enable 2
The extraction latch is set on the ESA in slot 2- ESA not enabled
Apricot(config)# crypto clear-latch 2
% Enter the crypto card password.
Password:
ESA in slot 2 not enabled
[OK]
Apricot(config)# crypto gen-signature-keys apricot
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.
Password:
Re-enter password:
Generating DSS keys....
 [OK]
Apricot(config)# crypto esa enable 2
...switching to HW crypto engine
Apricot(config)# exit

The following example shows how to enable the ESA when keys already exist on the ESA card.
Apricot# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Apricot(config)# crypto clear-latch 2
% Enter the crypto card password.
Password:
Keys were found for this ESA- enable ESA now? [yes/no]: yes
...switching to HW crypto engine
[OK]
Apricot(config)# exit
```

The following example shows how to enable the ESA when keys already exist on the ESA card but you want to generate new keys.

```
Apricot# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Apricot(config)# crypto clear-latch 2
% Enter the crypto card password.
Password:
Keys were found for this ESA- enable ESA now? [yes/no]: no
ESA in slot 2 not enabled
[OK]
Apricot(config)# crypto gen-signature-keys newkeys
% Generating new DSS keys will require re-exchanging
   public keys with peers who already have the public key
   named apricot!
Generate new DSS keys? [yes/no]: yes
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.
Password:
Re-enter password:
Generating DSS keys....
[OK]
Apricot(config)#
... Exchange new keys here...
Apricot(config)# crypto esa enable 2
...switching to HW crypto engine
Apricot(config)# exit
```

Note For additional examples of configuring the crypto engine on the ESA, refer to the chapter "Configuring Network Data Encryption with Router Authentication" in the *Security Configuration Guide*.

Using the show diagbus Command to Verify ESA Installation

Use the **show diagbus** command to determine whether or not your installed ESA is recognized by your system.

Following is sample output of the **show diagbus** command from a Cisco 7200 series router:

```
7200Router# show diagbus

(Additional display text omitted from this example)

Slot 2:
        Encryption engine port adapter, 2 ports
        Port adapter is analyzed
        Port adapter insertion time 01:47:00 ago
        Hardware revision 1.0           Board revision A0
        Serial number     8             Part number    73-1557-07
        Test history      0x17          RMA number     00-00-00
        EEPROM format version 1
        EEPROM contents (hex):
```

```
  0x20: 01 08 01 00 00 00 00 08 49 06 15 07 17 00 00 00
  0x30: 50 00 00 00 97 01 03 00 FF FF FF FF FF FF FF FF
```

Following is sample output of the **show diagbu**s command from a Cisco 7500 router with an ESA installed on a VIP2-40:

```
7500Router# show diagbus

(Additional displayed text omitted from this example)

Slot 0:
        Physical slot 0, ~physical slot 0xF, logical slot 0, CBus 0
        Microcode Status 0x4
        Master Enable, LED, WCS Loaded
        Board is analyzed
        Pending I/O Status: None
        EEPROM format version 1
        VIP2 controller, HW rev 2.2, board revision UNKNOWN
        Serial number: 03341454  Part number: 73-1684-02
        Test history: 0x00        RMA number: 00-00-00
        Flags: cisco 7000 board; 7500 compatible

        EEPROM contents (hex):
          0x20: 01 15 02 02 00 32 FC 8E 49 06 94 02 00 00 00 00
          0x30: 07 2E 00 2A 1A 00 00 00 00 00 00 00 00 00 00 00

        Slot database information:
        Flags: 0x4      Insertion time: 0x1470 (16:44:07 ago)

        Controller Memory Size: 32 MBytes DRAM, 2048 KBytes SRAM

       (Additional display text omitted from this example)

        PA Bay 1 Information:
                Encryption SA
                EEPROM format version 1
                HW rev 1.0, Board revision UNKNOWN
                Serial number: 00000444  Part number: 73-1557-07
```

Note The chassis slot locations will vary in the Cisco 7000 series, Cisco 7200 series, and Cisco 7500 series router models. There are no chassis slot restrictions on where the ESA can be installed.

Other Sources of Information

The following reading material can provide additional background information about authentication and data encryption, including theory, standards, and legal requirements:

- *Applied Cryptography*, Bruce Schneier. John Wiley & Sons, Inc. ISBN 0-471-11709-9
- *Network Security: Private Communication in a Public World*, Charlie Kaufman, Radia Perlman, and Mike Specinen. Prentice-Hall, Inc. ISBN 0-13-061466-1
- *Actually Useful Internet Security Techniques*, Larry J. Hughes, Jr. New Riders Publishing
- *FIPS140*, Federal Information Processing Standard
- Defense Trade Regulations (Parts 120 through 126)
- *Information Security and Privacy in Network Environments*, Office of Technology Assessment (OTA)—Congress of the United States

Essential Encryption/Authentication Configuration Tasks

To enable your Cisco router to establish and conduct encrypted communication sessions and to authenticate peer routers, the following essential configuration tasks must be performed on all participating peer routers:

- Task 1—Generate DSS Public/Private Keys: you must perform task 1 one time *only* for *each* crypto engine of your router that you plan to use. (For a description of crypto engines, refer to the sections "The Cisco IOS Crypto Engine," "The VIP2 Crypto Engine," and "The Data Encryption Service Adapter Crypto Engine" on page 29.) The DSS key pair generated in task 1 will be used with every peer encrypting router to which you connect.
- Task 2—Exchange DSS Public Keys: task 2 must be accomplished for each peer encrypting router that your router will connect to for encrypted sessions. If the network contains several peer encrypting routers that you will be using for encrypted communication, you will need to exchange DSS keys multiple times (once for each peer router). If you ever add an encrypting peer router to your network topology, you will then need to exchange DSS keys with the new router to enable encryption to occur with that new router.

  Task 2 involves making a phone call to the administrator of the peer encrypting router. You need to be in voice contact with the other administrator during task 2 to voice authenticate the source of exchanged DSS public keys. It is likely that you will confer with the peer router administrator prior to task 2, to plan your encryption strategy. When you discuss this strategy you need to decide (among other things) what DES algorithm both your routers will be using because you must both configure the same DES algorithm for encryption to work.
- Task 3—Enable DES Encryption Algorithms: perform task 3 at any time prior to encrypted communication. You might choose to perform this step in conjunction with (or even before) task 2; however, we recommend that you enable DES encryption algorithms *before* performing task 4.
- Task 4—Define Crypto Maps and Assign them to Interfaces: task 4 is typically performed last. You must complete task 4 to allow specific router interfaces to perform encryption/authentication.

These four essential tasks are each described in the following sections.

Generate DSS Public/Private Keys

You must generate DSS keys so that peer routers can authenticate each other before each encrypted session. You must generate DSS keys for each crypto engine that governs ports you will use to provide encryption/authentication services. To generate DSS keys for a crypto engine, perform at least the first of the following global configuration tasks:

Task	Command
Generate DSS public and private keys.	**crypto gen-signature-keys** *key-name* [*slot*]
View your DSS public key (private key not viewable).	**show crypto mypubkey** [*slot*]
Save DSS keys to private NVRAM (only for Cisco IOS crypto engines).	copy running-config startup-config

Note You must perform the **copy running-config startup-config** (previously **write memory**) command to save Cisco IOS crypto engine DSS keys to a private portion of NVRAM. DSS keys are *not* saved with your configuration when you perform a **copy running-config rcp** or **copy running-config tftp** (previously **write network**) command. If you are using an ESA, DSS keys generated for the ESA crypto engine are automatically saved to the tamper resistant memory of the ESA upon DSS key generation. You will be prompted to create a password the first time you generate DSS keys for the ESA crypto engine. If you ever need to regenerate DSS keys for the ESA, you will be required to use this same password to complete the DSS key regeneration.

Exchange DSS Public Keys

You must exchange DSS public keys with all participating peer routers. This will allow peer routers to authenticate each other at the start of encrypted communication sessions.

You must exchange the DSS public keys of each crypto engine that you will be using.

To successfully exchange DSS public keys, you must cooperate with a trusted administrator of the other peer router. You and the administrator of the peer router must complete the following steps in the order given:

Step 1 You and the other administrator decide which of you will be called “PASSIVE,” and which will be called “ACTIVE.”

Phone the other person to verbally assign the PASSIVE and ACTIVE roles. You will remain on the phone with this person until you complete all the steps in this list.

Step 2 PASSIVE enables a DSS exchange connection.

The person who is assigned “PASSIVE” should perform the following global configuration task:

Task	Command
Enable a DSS exchange connection.	**crypto key-exchange passive** [*TCP-port*]

Step 3 ACTIVE creates a DSS exchange connection and sends a DSS public key.

The person who is assigned “ACTIVE” should perform the following global configuration task:

Task	Command
Initiate connection and send DSS public key.	**crypto key-exchange** *ip-address key-name* [*TCP-port*]

Step 4 You both observe the serial number and fingerprint of ACTIVE’s DSS public key. The DSS key’s serial number and fingerprint are numeric values that will be displayed on both screens at this time.

Step 5 You both read to each other the DSS key serial number and fingerprint displayed on your screens. The two numbers on both screens should be identical. ACTIVE asks PASSIVE to accept the DSS key. If the numbers matched, PASSIVE should agree to accept ACTIVE’s DSS key.

Step 6 PASSIVE sends ACTIVE a DSS public key.

PASSIVE's screen will display a prompt to send a DSS public key in return. PASSIVE should press **Return** to continue. PASSIVE will be prompted to confirm a public key name. When PASSIVE accepts a name by pressing **Return**, the DSS public key will be sent to ACTIVE.

Step 7 PASSIVE's DSS serial number and fingerprint display on both of your screens.

Step 8 As before, you both verbally verify that the PASSIVE's DSS serial number and fingerprint match on your two screens.

Step 9 ACTIVE agrees to accept PASSIVE's DSS public key.

DSS public keys have now been exchanged, so both of you can now hang up the phone.

Note The previous nine steps (illustrated in Figure 27) must be accomplished between your router and a peer router, for every peer router with which you will conduct encrypted sessions.

Enable DES Encryption Algorithms

Cisco routers use DES encryption algorithms and DES keys to encrypt and decrypt data. You must globally enable (turn on) all the DES encryption algorithms that your router will use during encrypted sessions. If a DES algorithm is not enabled globally, you will not be able to use it. (Enabling a DES algorithm once allows it to be used by all crypto engines of a router.)

To conduct an encrypted session with a peer router, you must enable at least one DES algorithm that the peer router also has enabled.

Cisco (and the ESA) supports the following four types of DES encryption algorithms:

- DES with 8-bit Cipher Feedback (CFB)
- DES with 64-bit CFB
- 40-bit variation of DES with 8-bit CFB
- 40-bit variation of DES with 64-bit CFB

The 40-bit variations use a 40-bit DES key, which is easier for attackers to "crack" than basic DES, which uses a 56-bit DES key. However, some international applications might require you to use 40-bit DES, because of export laws. Also, 8-bit CFB is more commonly used than 64-bit CFB, but requires more CPU time to process. Other conditions might also exist that will require you to use one or another type of DES.

Note If you are running an exportable image, you can only enable and use 40-bit variations of DES. You cannot enable or use the basic DES algorithms, which are not available with exportable images.

One DES algorithm is enabled for your router by default. If you do not plan to use the default DES algorithm, you may choose to disable it. If you are running a nonexportable image, the DES default algorithm will be DES with 64-bit CFB. If you are running an exportable image, the DES default algorithm will be 40-bit variation of DES with 64-bit CFB.

If you don't know if your image is exportable or nonexportable, you can perform the **show crypto algorithms** command (shown in the table below) to determine which DES algorithms are currently enabled.

To globally enable one or more DES algorithms, perform one or more of the following global configuration tasks:

Task	Command
Enable DES with 8-bit or 64-bit CFB.	**crypto algorithm des** [**cfb-8** | **cfb-64**]
Enable 40-bit DES with 8-bit or 64-bit CFB.	**crypto algorithm 40-bit-des** [**cfb-8** | **cfb-64**]
View all enabled DES algorigthms.	show crypto algorithms

Define Crypto Maps and Assign Them to Interfaces

The purpose of this task is to tell your router which IP packets to encrypt or decrypt, and also which DES encryption algorithm to use when encrypting/decrypting the packets.

There are actually three parts to this task:

- Set Up Encryption Access Lists, page 49
- Define Crypto Maps, page 49
- Apply Crypto Maps to Interfaces, page 50

Set Up Encryption Access Lists

Encryption access lists are used in this step to define which IP packets will be encrypted and which IP packets will not be encrypted. Encryption access lists are defined using extended IP access lists, but are not used in the same way that IP access lists are typically used.

To set up encryption access lists for IP packet encryption, perform the following global configuration task:

Task	Command
Enable or disable encryption for a network.	**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**log**]

Using the **permit** keyword will cause all traffic that is passed between the specified source and destination addresses to be encrypted/decrypted by peer routers. Using the **deny** keyword prevents that traffic from being encrypted/decrypted by peer routers.

Caution When creating encryption access lists, it is *not* recommended to use the **any** keyword to specify source or destination addresses. Using the **any** keyword could cause extreme problems if a packet enters your router and is destined for a router that is not configured for encryption/authentication. This would cause your router to attempt to set up an encryption session with a nonencrypting router.

If you perform the **show extended IP access-lists** command, the router will show all extended IP access lists that have been defined, including those that are used for traffic filtering purposes as well as those that are used for encryption. The show command output does not differentiate between the two uses of the extended access lists.

Define Crypto Maps

Crypto maps are used to specify which DES encryption algorithm(s) will be used in conjunction with each access list defined in the previous step. Crypto maps are also used to identify which peer routers will provide the remote end encryption/authentication services. You must define one crypto map for each interface that will send encrypted data to a peer encrypting router.

To define a crypto map, perform the following tasks. The first task is performed in global configuration mode; the other tasks are performed in crypto map configuration mode.

Task	Command
Name the crypto map and enter the crypto map configuration mode.	**crypto map** *map-name* [*seq-no*]
Specify the remote peer router's name.	**set peer** *key-name*

Task	Command
Specify the encryption access list.	**match address** *access-list*
Specify the DES encryption algorithm to be used.	**set algorithm des** [**cfb-8** | **cfb-64**] or **set algorithm 40-bit-des** [**cfb-8** | **cfb-64**]

Note If you are running an exportable image, you can only specify 40-bit variations of DES. You cannot enable or use the basic DES algorithms, which are not available with exportable images.

Apply Crypto Maps to Interfaces

This step puts into effect the crypto maps just defined. You must apply exactly one crypto map to each interface that will encrypt outbound data and decrypt inbound data. This interface provides the encrypted connection to a peer encrypting router. An interface will not encrypt/decrypt data until you apply a crypto map to the interface.

To apply a crypto map to an interface, perform the following interface configuration task:

Task	Command
Apply a crypto map to an interface.	**crypto map** *map-name*

Optional Encryption/Authentication Configuration Tasks

The following optional tasks are described below:

- Define Time Duration of Encrypted Sessions, page 50
- Pregenerate DH Numbers, page 51
- Remove all DSS Keys, page 51

Define Time Duration of Encrypted Sessions

The default time duration of an encrypted session is 30 minutes. After the default time duration expires, an encrypted session must be renegotiated if encrypted communication is to continue. You can change this default to extend or limit the time of encrypted sessions.

To change the time duration of encrypted sessions, perform at least the first of the following global configuration tasks:

Task	Command
Define maximum time duration of encrypted sessions.	**crypto key-timeout** *minutes*
View defined time duration of encrypted sessions.	show crypto key-timeout

Pregenerate DH Numbers

Diffie-Hellman (DH) numbers are generated in pairs during the setup of each encrypted session. (DH numbers are used during encrypted session setup to compute the DES session key.) Generating these numbers is a CPU-intensive activity, which can make session setup slow—especially for low-end routers. To speed up session setup time, you can choose to pregenerate DH numbers.

To pregenerate DH numbers, perform the following global configuration task:

Task	Command
Pregenerate DH numbers.	**crypto pregen-dh-pairs** *number* [*slot*]

Remove all DSS Keys

If you choose to stop using encryption on a router, you can delete its public/private DSS key pair(s).

Caution DSS keys cannot be recovered after they have been removed. Use this function *only* after careful consideration.

To remove your DSS public/private keys (for all crypto engines) from your router, perform the following global configuration task:

Task	command
Remove DSS keys from your router.	crypto zeroize

Testing and Troubleshooting Encryption/Authentication

This section discusses how you can verify your configuration and the correct operation of encryption/authentication. This section also discusses diagnosing connection problems.

You should complete all the essential configuration tasks (as described earlier in the section "Essential Encryption/Authentication Configuration Tasks") *before* trying to test or troubleshoot your encryption configuration.

Test the Encryption/Authentication Configuration

If you want to test the packet encryption setup between peers, you can manually attempt to establish a session by specifying the IP address of a local host and a remote host that have been specified in an encryption access list.

To test the encryption setup, perform the following tasks in privileged EXEC mode:

Task	Command
Set up a test encryption session.	**test crypto initiate-session** *src-IP-addr dst-IP-addr map-name seq-num*
View the connection status.	show crypto connections

An example at the end of this configuration note explains how to interpret the **show crypto connections** command output.

Diagnose Connection Problems

If you need to verify the state of a connection, you can perform the following tasks in privileged EXEC mode:

Task	Command
Check status of connection setup.	show crypto connections
Check status of a crypto map.	show crypto map
Check that connection is established and that packets are being encrypted.	show crypto crypto-engine connections active

Debug commands are also available to assist in problem-solving. These commands are documented in the *Debug Command Reference*.

Encryption/Authentication Configuration Examples

The following sections provide examples of configuring and testing your router for network data encryption with router authentication:

Generate DSS Public/Private Keys

The following example illustrates two encrypting peer routers (named Apricot and Banana) generating their respective DSS public/private keys. Apricot is a Cisco 2500 series router. Banana is a Cisco 7500 series router with an RSP in chassis slot 4 and an ESA/VIP2-40 in chassis slot 2.

Apricot

```
Apricot(config)# crypto gen-signature-keys Apricot
Generating DSS keys .... [OK]
Apricot(config)#
```

Banana

```
Banana(config)# crypto gen-signature-keys BananaIOS 4
Generating DSS keys .... [OK]
Banana(config)# crypto gen-signature-keys BananaESA 2
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password: <passwd>

Re-enter password: <passwd>

Generating DSS keys .... [OK]
Banana(config)#
```

The password entered in the preceding example is a new password that you create when you generate DSS keys for an ESA crypto engine for the first time. If you ever generate DSS keys a second time for the same ESA crypto engine, you must use the same password to complete the key regeneration.

Exchange DSS Public Keys

The following is an example of a DSS public key exchange between two peer encrypting routers (Apricot and Banana). Apricot is a Cisco 2500 series router, and Banana is a Cisco 7500 series router with an ESA. In this example, Apricot sends its DSS public key, and Banana sends its ESA DSS public key. DSS keys have already been generated as shown in the previous example. Before any commands are entered, one administrator must call the other administrator. After the phone call is established, the two administrators decide which router is “PASSIVE” and which is “ACTIVE” (an arbitrary choice). In this example, router Apricot is ACTIVE and router Banana is PASSIVE. To start, PASSIVE enables a connection as follows:

Banana (PASSIVE)

```
Banana(config)# crypto key-exchange passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]<Return>
Waiting ....
```

PASSIVE must wait while ACTIVE initiates the connection and sends a DSS public key.

Apricot (ACTIVE)

```
Apricot(config)# crypto key-exchange 192.168.114.68 Apricot
Public key for Apricot:
   Serial Number 01461300
0F1D 373F 2FC1 872C D5D7
Wait for peer to send a key[confirm]<Return>
Waiting ....
```

After ACTIVE sends a DSS public key, the key's serial number and fingerprint display on both terminals, as shown previously and as follows:

Banana (PASSIVE)

```
Public key for Apricot:
   Serial Number 01461300
   Fingerprint   0F1D 373F 2FC1 872C D5D7
Add this public key to the configuration? [yes/no]: y
```

Now you both must verbally verify that your two screens show the same serial number and fingerprint. If they do, PASSIVE will accept the DSS key as shown previously by typing **y**, and continue by sending ACTIVE a DSS public key:

```
Send peer a key in return[confirm]<Return>
Which one?
BananaIOS? [yes]: n
BananaESA? [yes]: <Return>
Public key for BananaESA:
   Serial Number 01579312
   Fingerprint   BF1F 9EAC B17E F2A1 BA77
```

You both observe Banana's serial number and fingerprint on your screens. Again, they verbally verify that the two screens show the same numbers.

Apricot (ACTIVE):

```
Public key for BananaESA:
   Serial Number 01579312
   Fingerprint   BF1F 9EAC B17E F2A1 BA77

Add this public key to the configuration? [yes/no]: y
Apricot(config)#
```

ACTIVE accepts Apricot's DSS public key. Both administrators hang up the phone and the key exchange is complete.

Enable DES Encryption Algorithms

In this example, a router (Apricot) globally enables two DES algorithms: the basic DES algorithm with 8-bit Cipher Feedback (CFB), and the 40-bit DES algorithm with 8-bit CFB. Another router (Banana) globally enables three DES algorithms: the basic DES algorithm with 8-bit CFB, the basic DES algorithm with 64-bit CFB, and the 40-bit DES algorithm with 8-bit CFB.

The following commands are entered from the global configuration mode.

Apricot

```
crypto algorithm des cfb-8
crypto algorithm 40-bit-des cfb-8
```

Banana

```
crypto algorithm des cfb-8
crypto algorithm des cfb-64
crypto algorithm 40-bit-des cfb-8
```

Set Up Encryption Access Lists, Define Crypto Maps, and Assign Crypto Maps to Interfaces

The following two examples show how to set up interfaces for encrypted transmission. Participating routers will be configured as encrypting peers for IP packet encryption.

Example 1

In the first example, a team of researchers at a remote site communicate with a research coordinator at headquarters. Company-confidential information is exchanged by IP traffic that consists only of TCP data. Figure 29 shows the network topology.

In the first example, Apricot is a Cisco 2500 series router, and Banana is a Cisco 7500 series router with an ESA/VIP2-40 in chassis slot 4.

Apricot

```
Apricot(config)# access-list 101 permit tcp 192.168.3.0 255.255.255.240 host 192.168.15.6
Apricot(config)# crypto map Research 10
Apricot(config-crypto-map)# set peer BananaESA
Apricot(config-crypto-map)# set algorithm des cfb-8
Apricot(config-crypto-map)# match address 101
Apricot(config-crypto-map)# exit
Apricot(config)# interface s0
Apricot(config-if)# crypto map Research
Apricot(config-if)# exit
Apricot(config)#
```

Banana

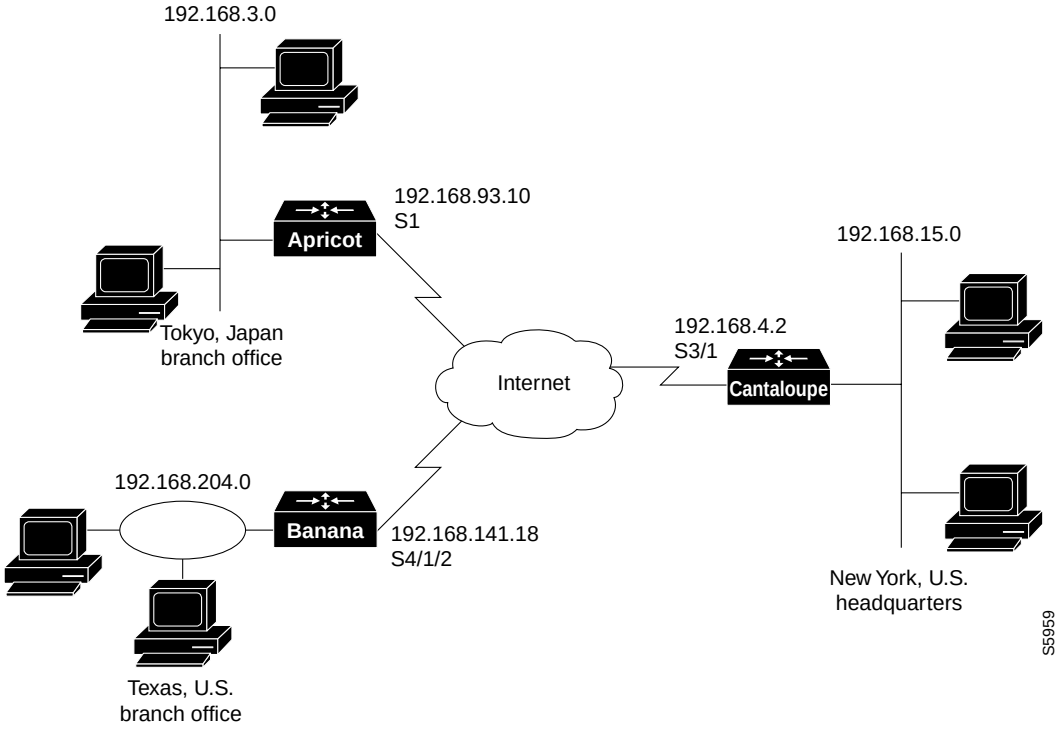
```
Banana(config)# access-list 110 permit tcp host 192.168.15.6 192.168.3.0 255.255.255.240
Banana(config)# crypto map Rsrch 10
Banana(config-crypto-map)# set peer Apricot
Banana(config-crypto-map)# set algorithm des cfb-8
Banana(config-crypto-map)# set algorithm des cfb-64
Banana(config-crypto-map)# match address 110
Banana(config-crypto-map)# exit
Banana(config)# interface s4/0/2
Banana(config-if)# crypto map Rsrch
Banana(config-if)# exit
Banana(config)#
```

Because Banana set two DES algorithms for crypto map Rsrch, Banana could use either algorithm with traffic on the S4/0/2 interface. However, because Apricot only set one DES algorithm (CFB-8 DES) for the crypto map Research, that is the only DES algorithm which will be used for all encrypted traffic between Apricot and Banana.

Example 2

In this example, employees at two branch offices and at headquarters must communicate sensitive information. A mix of TCP and UDP traffic is transmitted by IP packets. Figure 26 shows the network topology used in this example.

Figure 26 Example Network Topology



Apricot is a Cisco 2500 series router and connects to the Internet through port S1. Both Banana and Cantaloupe are Cisco 7500 series routers with ESAs. Banana connects to the Internet using the ESA-governed VIP2-40 interface S4/1/2. Cantaloupe is already using every VIP2-40 port (governed by the ESA) to connect to several off-site financial services, and so must connect to the Internet using a serial interface (S3/1) in slot 3. (Cantaloupe's interface S3/1 is governed by the Cisco IOS crypto engine.)

Apricot will be using one interface to communicate with both Banana and Cantaloupe. Because only one crypto map can be applied to this interface, Apricot creates a crypto map that has two distinct definition sets by using the *seq-no* argument with the **crypto map** command. By using *seq-no* values of 10 and 20, Apricot creates a single crypto map named "TXandNY" that contains a subset of definitions for encrypted sessions with Banana, and a second distinct subset for definitions for encrypted sessions with Cantaloupe.

Banana and Cantaloupe also use a single interface to communicate with the other two routers and therefore, will use the same strategy as Apricot does for creating crypto maps.

In this example, we assume that Apricot has generated DSS keys with the *key-name* "Apricot.TokyoBranch," Banana has generated DSS keys with the *key-name* "BananaESA.TXbranch," and Cantaloupe has generated DSS keys with the *key-name* CantaloupeIOS.NY." We also assume that each router has exchanged DSS public keys with the other two routers, and that each router has enabled each DES algorithm that is specified in the crypto maps.

Apricot

```
Apricot(config)# access-list 105 permit tcp 192.168.3.0 255.255.255.240 192.168.204.0
255.255.255.0
Apricot(config)# access-list 105 permit udp 192.168.3.0 255.255.255.240 192.168.204.0
255.255.255.0
Apricot(config)# access-list 106 permit tcp 192.168.3.0 255.255.255.240 192.168.15.0
255.255.255.0
Apricot(config)# access-list 106 permit udp 192.168.3.0 255.255.255.240 192.168.15.0
255.255.255.0
Apricot(config)# crypto map TXandNY 10
Apricot(config-crypto-map)# set peer BananaESA.TXbranch
Apricot(config-crypto-map)# set algorithm 40-bit-des cfb-8
Apricot(config-crypto-map)# match address 105
Apricot(config-crypto-map)# exit
Apricot(config)# crypto map TXandNY 20
Apricot(config-crypto-map)# set peer CantaloupeIOS.NY
Apricot(config-crypto-map)# set algorithm 40-bit-des cfb-64
Apricot(config-crypto-map)# match address 106
Apricot(config-crypto-map)# exit
Apricot(config)# interface s1
Apricot(config-if)# crypto map TXandNY
Apricot(config-if)# exit
```

Banana

```
Banana(config)# access-list 110 permit tcp 192.168.204.0 255.255.255.0 192.168.3.0
255.255.255.240
Banana(config)# access-list 110 permit udp 192.168.204.0 255.255.255.0 192.168.3.0
255.255.255.240
Banana(config)# access-list 120 permit tcp 192.168.204.0 255.255.255.0 192.168.15.0
255.255.255.0
Banana(config)# access-list 120 permit udp 192.168.204.0 255.255.255.0 192.168.15.0
255.255.255.0
Banana(config)# crypto map USA 10
Banana(config-crypto-map)# set peer Apricot.TokyoBranch
Banana(config-crypto-map)# set algorithm 40-bit-des cfb-8
Banana(config-crypto-map)# match address 110
Banana(config-crypto-map)# exit
Banana(config)# crypto map USA 20
Banana(config-crypto-map)# set peer CantaloupeIOS.NY
Banana(config-crypto-map)# set algorithm des cfb-64
Banana(config-crypto-map)# match address 120
Banana(config-crypto-map)# exit
Banana(config)# interface s4/1/2
Banana(config-if)# crypto map USA
Banana(config-if)# exit
```

Cantaloupe

```
Cantaloupe(config)# access-list 101 permit tcp 192.168.15.0 255.255.255.0 192.168.3.0
255.255.255.240
Cantaloupe(config)# access-list 101 permit udp 192.168.15.0 255.255.255.0 192.168.3.0
255.255.255.240
```

```
Cantaloupe(config)# access-list 102 permit tcp 192.168.15.0 255.255.255.0 192.168.204.0
255.255.255.0
Cantaloupe(config)# access-list 102 permit udp 192.168.15.0 255.255.255.0 192.168.204.0
255.255.255.0
Cantaloupe(config)# crypto map satellites 10
Cantaloupe(config-crypto-map)# set peer Apricot.TokyoBranch
Cantaloupe(config-crypto-map)# set algorithm 40-bit-des cfb-64
Cantaloupe(config-crypto-map)# match address 101
Cantaloupe(config-crypto-map)# exit
Cantaloupe(config)# crypto map satellites 20
Cantaloupe(config-crypto-map)# set peer BananaESA.TXbranch
Cantaloupe(config-crypto-map)# set algorithm des cfb-64
Cantaloupe(config-crypto-map)# match address 102
Cantaloupe(config-crypto-map)# exit
Cantaloupe(config)# interface s3/1
Cantaloupe(config-if)# crypto map satellites
Cantaloupe(config-if)# exit
```

The previous configurations will result in DES encryption algorithms being applied to encrypted IP traffic as shown in Figure 31.

Test the Encryption Connection

The following example sets up and verifies a test encryption session.

Assume the same network topology and configuration as in the previous example and shown in Figure 26 on page 56.

Router Apricot sets up a test encryption session with router Banana, and then views the connection status to verify a successful encrypted session connection.

Step 1 Router Apricot sets up a test encryption connection with router Banana.

```
Apricot# test crypto initiate-session 192.168.3.12 192.168.204.110 BananaESA.TXbranch 10
Sending CIM to: 192.168.204.110 from: 192.168.3.12.
Connection id: -1
```

Notice the Connection id value is -1. A negative value indicates that the connection is being set up.

Step 2 Router Apricot issues the **show crypto connections** command.

```
Apricot# show crypto connections
Pending Connection Table
PE              UPE             Timestamp       Conn_id
192.168.3.10    192.168.204.100 730944064       -1

Connection Table
PE              UPE             Conn_id New_id  Alg     Time
192.168.3.10    192.168.204.100 -1      1       0       0
                flags:USED_NODE PEND_CONN
```

Look in the Pending Connection Table for an entry with a Conn_id value equal to the previously shown Connection id value—in this case, look for an entry with a Conn_id value of -1. If this is the first time an encrypted connection has been attempted, there will only be one entry (as shown).

Note the PE and UPE addresses for this entry.

Step 3 Now, look in the Connection Table for an entry with the same PE and UPE addresses. In this case, there is only one entry in both tables, so finding the right Connection Table entry is easy!

Step 4 At the Connection Table entry, note the Conn_id and New_id values. In this case, Conn_id equals -1, and New_id equals 1. The New_id value of 1 will be assigned to the test connection when setup is complete. (Positive numbers are assigned to established, active connections.)

Step 5 Apricot waits a moment for the test connection to set up and then reissues the **show crypto connections** command.

```
Apricot# show crypto connections
Pending Connection Table
PE              UPE             Timestamp       Conn_id
192.168.3.10    192.168.204.100 730944064       -1

Connection Table
PE              UPE             Conn_id New_id  Alg     Time
192.168.3.10    192.168.204.100 1       1       0       0
                flags:USED_NODE PEND_CONN
```

Again, look for the Connection Table entry with the same PE and UPE addresses as shown before. In this entry, notice that the Conn_id value has changed to 1. This indicates that the test connection has been successfully established because the Conn_id value changed to match the New_id value of Step 4. (Also, New_id has been reset to 0 at this point.)

The **show crypto connections** command is explained in greater detail in the chapter "Network Data Encryption and Router Authentication Commands" in the *Security Command Reference*. It includes a description of how connection ids are assigned during and following connection setup.

Translated Battery Handling Warnings

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.**

Waarschuwing **Er is ontploffingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggeworpen te worden.**

Varoitus **Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.**

Attention **Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.**

Warnung **Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.**

Avvertenza **Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.**

Advarsel **Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.**

Aviso **Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.**

¡Advertencia! Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

Varning! Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.