PowerKEY Server for Encrypted VOD in an ISDP Network

Installation, Upgrade, and Operation Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing **or** later issued patent.

Copyright

Contents

Safety Precautions

Read, Retain, and Follow These Instructions

Carefully read all safety and operating instructions before operating this product. Follow all operating instructions that accompany this product. Retain the instructions for future use. Give particular attention to all safety precautions.

Warning and Caution Icons

WARNING:

Avoid personal injury and product damage! Do not proceed beyond any icon until you fully understand the indicated conditions.

The following icons alert you to important information about the safe operation of this product:

You will find this icon in the literature that accompanies this product. This icon indicates important operating or maintenance instructions.

You may find this icon affixed to this product and in this document to alert you of electrical safety hazards. On this product, this icon indicates a live terminal; the arrowhead points to the terminal device.

You may find this icon affixed to this product. This icon indicates a protective earth terminal.

You may find this icon affixed to this product. This icon indicates excessive or dangerous heat.

You may find this symbol affixed to this product and in this document. This symbol indicates an infrared laser that transmits intensity-modulated light and emits invisible laser radiation and an LED that transmits intensity-modulated light.

Heed All Warnings

Adhere to all warnings on the product and in the operating instructions.

Avoid Electric Shock

Follow the instructions in this warning.

WARNING:

To reduce risk of electric shock, perform only the instructions that are included in the operating instructions. Refer all servicing to qualified service personnel.

Servicing

WARNING:

Avoid electric shock! Opening or removing the cover may expose you to dangerous voltages.

Do not open the cover of this product and attempt service unless instructed to do so in the operating instructions. Refer all servicing to qualified personnel only.

Cleaning, Water, Moisture, Open Flame

To protect this product against damage from moisture and open flames, do the following:

- Before cleaning, unplug this product from the AC outlet. Do *not* use liquid or aerosol cleaners. Use a dry cloth for cleaning.
- Do not expose this product to moisture.
- Do not place this product on a wet surface or spill liquids on or near this product.
- Do not place or use candles or other open flames near or on this product.

Ventilation

To protect this product against damage from overheating, do the following:

- This product has openings for ventilation to protect it from overheating. To ensure product reliability, do not block or cover these openings.
- Do not open this product unless otherwise instructed to do so.
- Do not push objects through openings in the product or enclosure.

Placement

To protect this product against damage from breakage, do the following:

- Place this product close enough to a mains AC outlet to accommodate the length of the product power cord.
- Route all power supply cords so that people cannot walk on, or place objects on, or lean objects against them. This can pinch or damage the cords. Pay particular attention to cords at plugs, outlets, and the points where the cords exit the product.
- Make sure the mounting surface or rack is stable and can support the size and weight of this product.

WARNING:

Avoid personal injury and damage to this product! An unstable surface may cause this product to fall.

When moving a cart that contains this product, check for any of the following possible hazards:

- Move the cart slowly and carefully. If the cart does not move easily, this condition may indicate obstructions or cables that you may need to disconnect before moving this cart to another location.
- Avoid quick stops and starts when moving the cart.
- Check for uneven floor surfaces such as cracks or cables and cords.

WARNING:

Avoid personal injury and damage to this product! Move any appliance and cart combination with care. Quick stops, excessive force, and uneven surfaces may cause the appliance and cart to overturn.

Fuse

When replacing a fuse, heed the following warnings.

WARNING:

Avoid electric shock! Always disconnect all power cables before you change a fuse.

WARNING:

Avoid product damage! Always use a fuse that has the correct type and rating. The correct type and rating are indicated on this product.

Grounding This Product (U.S.A. and Canada Only)

Safety Plugs

If this product is equipped with either a three-prong (grounding pin) safety plug or a two-prong (polarized) safety plug, do not defeat the safety purpose of the polarized or grounding-type plug. Follow these safety guidelines to properly ground this product:

- For a 3-prong plug (consists of two blades and a third grounding prong), insert the plug into a grounded mains, 3-prong outlet.

  Note: This plug fits only one way. The grounding prong is provided for your safety. If you are unable to insert this plug fully into the outlet, contact your electrician to replace your obsolete outlet.
- For a 2-prong plug (consists of one wide blade and one narrow blade), insert the plug into a polarized mains, 2-prong outlet in which one socket is wider than the other.

Note: If you are unable to insert this plug fully into the outlet, try reversing the plug. The wide blade is provided for your safety. If the plug still fails to fit, contact an electrician to replace your obsolete outlet.

Grounding Terminal

If this product is equipped with an external grounding terminal, attach one end of an 18-gauge wire (or larger) to the grounding terminal; then, attach the other end of the wire to an earth ground, such as an equipment rack that is grounded.

20050727 Headend/Rack

About This Guide

Introduction

This guide describes the PowerKEY™ Encryption Server (PKES). Refer to this guide for installing, operating, and troubleshooting your PKES.

Audience

This document is written for system operators of the Digital Broadband Delivery System (DBDS) or the IPTV Broadband Delivery System (IBDS). Headend operators and support engineers may also find the contents of this document to be useful.

Document Version

This is the second formal release of this document.

1

PKES Hardware Installation

Introduction

This chapter describes the PowerKEY Encryption Server (PKES) and outlines the procedures required for installing the PKES hardware. After installing the server into the rack, see ***PKES Front Panel*** (on page 8) and ***PKES Back Panel*** **(on page 9)** to become familiar with the device.

If you are installing PKES software for the first time, complete the procedures in Chapters 1 through 4. If you are upgrading the PKES, complete the procedures in Chapter 5.

In This Chapter

Overview of the PowerKEY Encryption Server

The PowerKEY Encryption Server (PKES) is a computer server that "pre-encrypts" video-on-demand (VOD) content in a format that is compatible with the PowerKEY and SoftCAS Conditional Access Systems (CAS).

Note: Pre-encryption refers to the fact that the VOD "asset" is encrypted before it is stored on a VOD server. Previous solutions stored the asset in the clear and did not encrypt the VOD asset until ordered by a subscriber.

The PKES connects to an asset manager. When VOD content is ready to be processed, the asset manager sends a notification to the PKES which results in the initiation of an FTP transfer from the asset manager. The notification includes a setting that directs the PKES to either encrypt the content or leave it in the clear but apply copy protection. In both cases, the PKES inserts appropriate PowerKEY Entitlement Control Messages (ECMs) into the file. When the encryption setting is enabled, the PKES encrypts packets that have been previously marked for encryption. Once the processing of the file is complete, the PKES FTPs the file back to the asset manager for storage. Both the PKES and ISDS must be provisioned with a key generated by the Transaction Encryption Device (TED) before encryption can occur.

The PKES Hardware

We occasionally update the PKES hardware to take advantage of newer technologies as they become available. This guide presents examples based on a typical server configuration.

Refer to the hardware install guide provided with your PKES server for specifics on how to physically install the server and for safety recommendations regarding server placement and cooling requirements.

Before beginning your installation, read the ***Safety Precautions*** (on page vi) at the beginning of this document. Pay particular attention to the **Placement** topic in the *Safety Precautions* section.

Site Requirements

Your site must meet the following requirements before you proceed with the installation:

- The hardware must be installed in a standard four-post rack. See ***Rack Mounting*** (on page 4) in the next section for the rack requirements.
- Approved power sources: 90 to 120 V AC (continuous)
- Racking and environment temperature: Inside rack temperature must be maintained at between 0° and +50°C (32° and 122°F)

Note: A monitor and keyboard or a PC connected via the serial interface will be needed for initial setup of the PKES. These peripherals are not needed for normal operation or day to day troubleshooting.

Rack Mounting

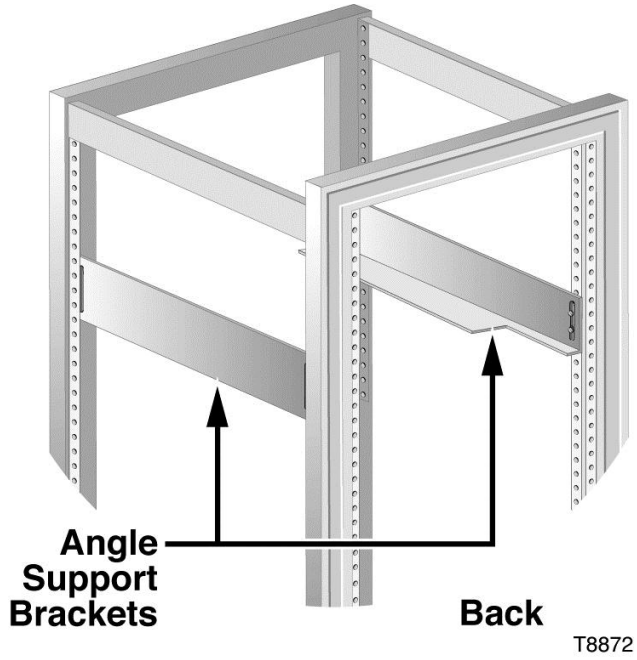
Installing the PKES in the Rack

Follow these steps to install the PKES in the rack using the angle support brackets.

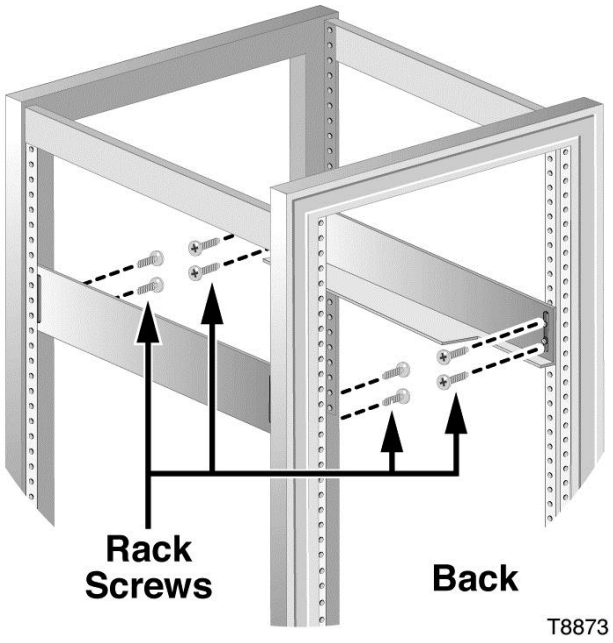
CAUTION:

Avoid personal injury and damage to this product! Be sure to support the server from underneath until it is securely positioned in the rack. Failure to do so could result in the server falling to the floor. The server could be damaged and you could be injured as a result.

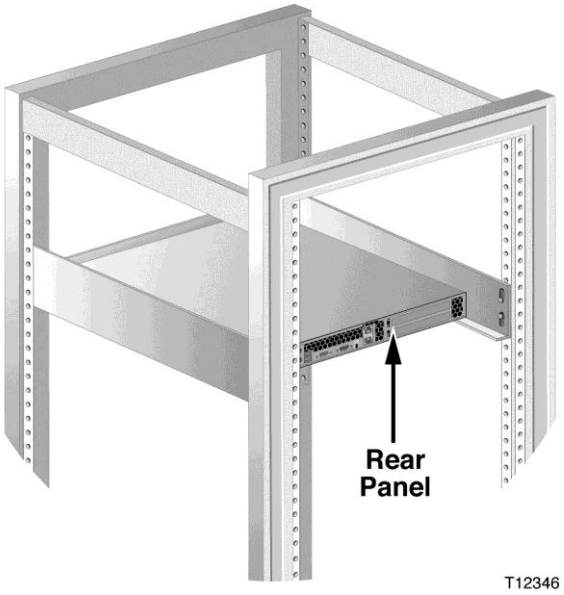
1. Make sure that the site requirements are met as outlined in the previous section.
2. Determine the approximate position in the equipment rack where you want the bottom of the PKES to be located. Then, position the angle support brackets in the rack. The cut-outs in the brackets must face toward the back of the rack as shown in the following illustration.



3 Attach the angle support brackets to the equipment rack using rack screws or other mounting hardware that came with your rack.



4 Slide the PKES into the equipment rack and onto the angle support brackets from the front of the rack until the front panel mounting flanges on the PKES are flush with the front mounting rails of the rack.



5 While holding the PKES in this position, make sure that the bottom of the unit is supported by the angle support brackets on both sides along the entire depth of the PKES chassis.

6 Check that the PKES front panel thumbscrews on both sides align with the proper mounting holes on the equipment rack.

If the thumbscrews...	THEN...
align with holes in the rack	carefully remove the PKES from the rack and go to step 7.
do not align with holes in the rack	carefully remove the PKES from the rack and repeat steps 4 and 5 until the thumbscrews align correctly, and the weight of the PKES is fully supported by the angle support brackets along both sides of the PKES.

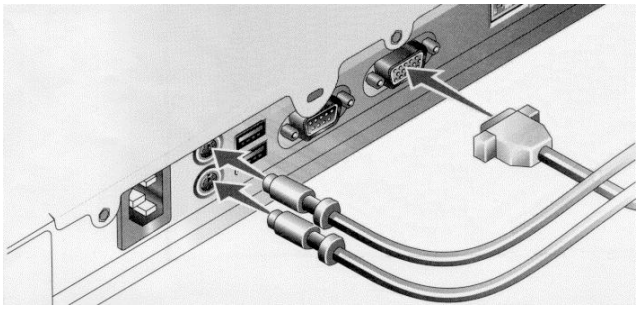
7 Securely tighten the rack screws (or other mounting hardware) that hold the angle support brackets in the rack.

8 Re-insert the PKES into the equipment rack and onto the angle support brackets from the front of the rack until the front panel mounting flanges of the PKES are flush with the front mounting rails of the rack.

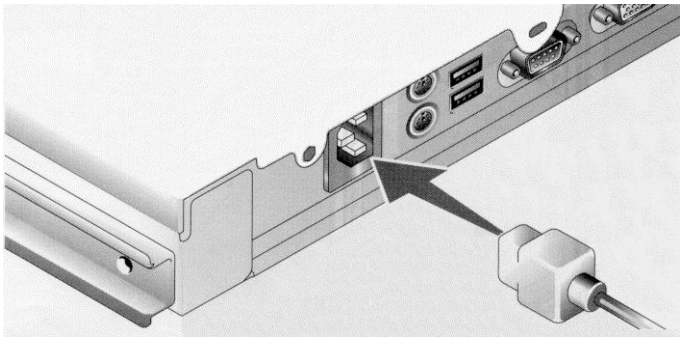
9 Tighten the two thumbscrews to secure the server in the rack.

Important: Verify that the weight of the server is still supported by the angle support brackets on both sides. If not, go back to step 5.

10 If you plan to use the keyboard, mouse, and monitor, attach them to their respective rear panel connectors.



11 Connect the input power cord to the rear panel.



12 Attach the front panel bezel if it is available and if you plan to use it.

Removing the PKES from the Rack

Follow these steps to remove the PKES from the rack.

CAUTION:

Avoid personal injury and damage to this product! Be sure to support the server from underneath while removing it from the rack. Failure to do so could result in the server falling to the floor. The server could be damaged and you could be injured as a result.

Note: You do not need to remove the optional front bezel to install or remove the system from the rack.

1. Turn off the system and attached peripherals.
2. Disconnect the system from the electrical power.
3. Disengage both thumbscrews from the front panel of the chassis.

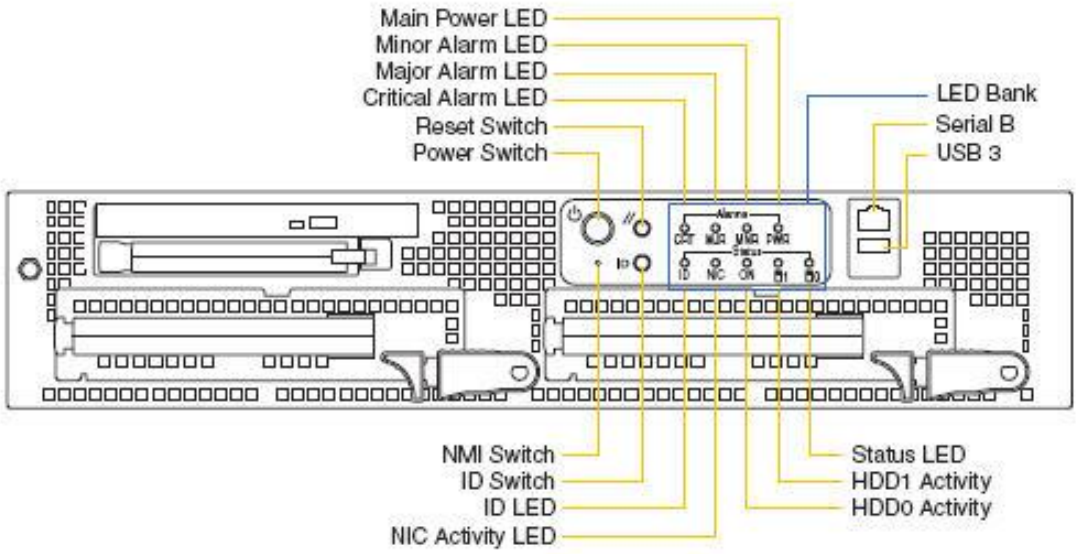
CAUTION:

This server is not supported by rack slides. Be sure to support the server from underneath while removing it from the rack.

4. Carefully pull the system forward and out of the rack.

PKES Front Panel Illustration

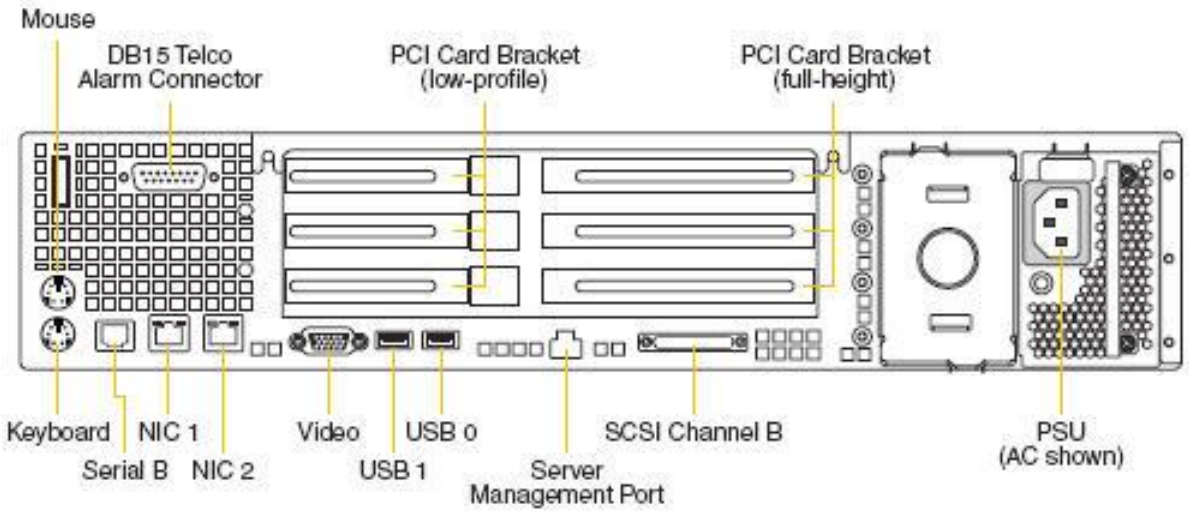
The PKES is a 2 RU rack-mount device. The front panel of the PKES is displayed in the following illustration. (Image may vary from actual product specification.)



PKES Back Panel Illustration

PKES Back Panel

The back panel of the PKES is displayed in the following illustration. (Image may vary from actual product specification.)



2

PKES Platform Installation

Introduction

The instructions in this chapter describe how to install the PKES platform software for the first time.

If you are upgrading the PKES, skip this chapter and complete the procedures in Chapter 5.

In This Chapter

Install the PKES Platform

Collect PKES Network Information

Network Information

Obtain the following network information from the network administrator for each PKES that will be installed. We recommend that you store this information with your documentation for this server.

Hostname: _____

Network Name	Network Interface	IP Address	Network Mask	Gateway IP
Headend Control	eth0			
Asset Ingest	eth1			

VOD Pass Phrase

When you create the VOD MSK on the TED, you are prompted to provide a VOD pass phrase that ranges from 10 to 64 characters long. If you do not know the pass phrase, contact your System Administrator. Your System Administrator creates the pass phrase and stores it in a secured location.

Installing the PKES Platform

Follow these instructions to install the PKES platform.

Important: A keyboard and a monitor need to be connected to the PKES before installing the platform software.

1. If the server is not powered on, press the power button on the front of the server. The server powers on.
2. Insert the PKES platform CD into the CD drive of the PKES. After a few minutes, the Cisco screen appears.
3. Type **platform** and then press **Enter**. The system runs an automated installation script and the following warning message appears:

   The partition table on the device sda was unreadable ... Would you like to initialize this drive, erasing ALL DATA?
4. Type **y** and then press **Enter**. The installation script continues.

   Note: The installation script should complete within 15 minutes.
5. When the PKES platform installation script has completed, log on to the **PKES** as root user.

Configuring the Management Network Interfaces

Follow these instructions to configure the management network interface for the PKES. This is the interface that is used to communicate with the ISDS and other management devices within the network.

1 On the PKES, type **cd /etc/sysconfig/network-scripts** and then press **Enter**. The /etc/sysconfig/network-scripts becomes the working directory.

2 Type **vi ifcfg-eth0** and then press **Enter**. The ifcfg-eth0 file opens for editing using the vi text editor.

3 Add the following information to the ifcfg-eth0 file:

DEVICE=eth0

BOOTPROTO=static

DHCPCLASS=

HWADDR=00:0E:0C:E5:F1:20

IPADDR=172.105.1.173

NETMASK=255.255.255.240

ONBOOT=yes

Important: The values used for IPADDR and NETMASK in the preceding example are for illustration, only. Use the actual IP address and netmask of the PKES in use on your system.

4 Save the file and close the vi editor.

Configuring the Asset Ingest Network Interface

Follow these instructions to configure the Asset Ingest network interface for the PKES. The Asset Ingest network interface is the interface that is used to communicate with video-on-demand (VOD) equipment, such as the AMS and NAS devices within the network.

1 On the PKES, type **cd /etc/sysconfig/network-scripts** and then press **Enter**. The /etc/sysconfig/network-scripts becomes the working directory.

2 Type **vi ifcfg-eth1** and then press **Enter**. The ifcfg-eth1 file opens for editing using the vi text editor.

3 Add the following data to the ifcfg-eth1 file:

DEVICE=eth1

BOOTPROTO=static

DHCPCLASS=

HWADDR=00:0E:0C:E5:F1:21

IPADDR=192.168.1.173

NETMASK=255.255.255.240

ONBOOT=yes

Important: The values used for IPADDR and NETMASK in the preceding example are for illustration, only. Use the actual IP address and netmask of the PKES in use on your system.

4 Save the file and close the vi editor.

Configuring the Routing Information

Follow these instructions to configure the routing information for the PKES.

1 At the PKES, type **cd /etc/sysconfig/network-scripts** and then press **Enter**. The /etc/sysconfig/network-scripts directory becomes the working directory.

2 Type **vi route-eth0** and then press **Enter**. The route-eth0 file opens for editing in the vi text editor.

3 Add the following lines to the route-eth0 file:

GATEWAY0=[the IP address of the management router]

NETMASK0=0.0.0.0

ADDRESS0=0.0.0.0

Example: When you are finished, the route-eth0 file should look similar to the following example:

GATEWAY0=172.105.1.174

NETMASK0=0.0.0.0

ADDRESS0=0.0.0.0

4 Save the file and close the vi editor.

5 Type **vi route-eth1** and then press **Enter**. The route-eth1 file opens for editing in the vi text editor.

6 Add the following lines to the route-eth1 file:

GATEWAY0=[The IP address of the Asset Ingest Interface router]

NETMASK0=255.255.255.255

ADDRESS0=[The IP address of the Tandberg AMS-PKES]

GATEWAY1=[The IP address of the Asset Ingest Interface router]

NETMASK1=255.255.255.255

ADDRESS1=[The IP address of the Tandberg NAS]

Example: When you are finished, the route-eth1 file should look similar to the following example:

GATEWAY0=192.106.1.174

NETMASK0=255.255.255.255

ADDRESS0=192.106.2.177

GATEWAY1=192.106.1.174

NETMASK1=255.255.255.255

ADDRESS1=192.106.2.178

7 Save the file and close the vi editor.

Configuring the PKES Hostname

Follow these instructions to configure the hostname on the PKES.

1 At the PKES, type **cd /etc/sysconfig** and then press **Enter**. The /etc/sysconfig directory becomes the working directory.

2 Type **vi network** and then press **Enter**. The network file opens for editing in the vi text editor.

3 Add the following lines to the network file:

NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=[PKES Hostname]

Example: When you are finished, the network file should similar to the following example:

NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=PKES1

4 Save and close the network file.

Activate the PKES Platform Configuration

After installing the PKES platform software and editing the network interface and router files, follow these instructions to activate those changes, and to test the connection between the ISDS and the PKES.

1. Ensure that the network cables are connected to the PKES.
2. While logged into the PKES, type **shutdown -y -g0 -i6** and then press **Enter** to reboot the PKES server and activate the PKES platform configuration.
3. After the PKES has rebooted, from an xterm window on the ISDS, type **ping [IP Address of the PKES]** and then press **Enter** to verify connectivity.

3

VOD MSK Management

Introduction

After setting up the PKES platform, your next task is to create and configure the video-on-demand multi-session key (VOD MSK) for the PKES. The instructions in this chapter guide you through the necessary steps.

If you are upgrading the PKES, skip this chapter and complete the procedures in Chapter 5.

In This Chapter

Create and Configure the VOD MSK

Creating the VOD MSK on the TED

Follow these instructions to set up the VOD MSK on the TED.

1. If necessary, open an xterm window on the ISDS and log in as root.
2. Type **ssh root@dncsted** and then press **Enter** to remotely log on to the TED.
3. When presented with the **password** prompt, enter the password for the root user on the TED.
4. Type **cd /home/teduser/bin** and then press **Enter**. The /home/teduser/bin directory on the TED becomes the working directory.
5. Type **./GenMsk** and then press **Enter**. The GenMsk script runs and a menu appears.
6. Select menu option **1**, **Generate MSK with VOD passphrase**. A message appears, prompting you to enter a new pass phrase.
7. Type a VOD pass phrase that ranges from 10 to 64 characters long. A prompt to re-enter the pass phrase appears.

   Important: If you do not know the pass phrase, contact your System Administrator. Your System Administrator creates the pass phrase and stores it in a secured location.
8. Type your VOD pass phrase again. A message appears that prompts you to enter the location where the generated multi-session key (MSK) *should be* created.
9. Type **/home/teduser/bin/** and press **Enter**. The vodMskPkes file is written to the specified directory.
10. Select menu option **2**, **Generate MSK with EA Passphrase**. The system prompts you to enter the pass phrase.
11. Type the VOD pass phrase that you created in step 8. The system prompts you to enter the location where the generated VOD MSK was created.
12. Type **/home/teduser/bin/** and press **Enter**.
13. Type the location where the generated EA-wrapped VOD MSK *should be* created.
14. Type **/home/teduser/bin/** and press **Enter**. The file, which is titled vodMskIsds, is written to the specified directory.
15. Select menu option **3** to exit from the menu.
16. Type **exit** and then press **Enter** to close the remote login to the TED.

Configuring the VOD MSK on the ISDS

Follow these instructions to set up the VOD MSK on the ISDS.

1. If necessary, open an xterm window on the ISDS.
2. Type **su - dncs** and then press **Enter** to log on as the dncs role.
3. Type **mkdir /export/home/dncs/vodMsk** and press **Enter**.
4. Type **cd /export/home/dncs/vodMsk** and press **Enter**.
5. Type **scp root@dncsted:/home/teduser/bin/vodMsk* /export/home/dncs/vodMsk** and then press **Enter**. The system copies the VOD MSK files from the TED to the ISDS.

   Note: When prompted for the password, enter the password for the root user on the TED.
6. Type **exit** and then press **Enter** to log out the root user.
7. Type **camDncsTedInit** and then press **Enter**. A camDncsTedInit menu appears.
8. Select option **5**. A message appears that prompts you to enter the complete path and file name of where VOD MSK files are stored on the ISDS.
9. Type **/export/home/dncs/vodMsk/vodMskIsds** and press **Enter**.
10. Select option **2** to upload the TED with the updated MSK. Follow the prompts to enter both the EA and CAA pass phrases.
11. Select option **6** to exit from the camDncsTedInit menu.

4

PKES Software Installation and Configuration

Introduction

Use the procedures in this chapter to help you install and configure the PKES software.

If you are upgrading the PKES, skip this chapter and complete the procedures in Chapter 5.

In This Chapter

Overview of the PKES Application

Anyone who configures the PKES application is likely to benefit from understanding the structure of the PKES package. The following table describes the directories that comprise the PKES package.

Note: In the table that follows, <PKES pkg> represents a placeholder for the full path of the PKES software (for example, /usr/local/pkes).

Package Directories	Description
<PKES pkg>/bin	This directory holds the executable files for the PKES application.
<PKES pkg>/config	This directory contains configuration files used by the PKES application.
<PKES pkg>/content <PKES pkg>/content/current <PKES pkg>/content/current/clear <PKES pkg>/content/current/encrypted <PKES pkg>/content/error <PKES pkg>/content/error/clear <PKES pkg>/content/error/encrypted	These directories hold the in-process VOD content, as well as VOD files that are retained for debugging purposes when an error occurs.
<PKES pkg>/logs	This directory contains the PKES log file and asset status tables recorded by the PKES applications for use by SNMP.
<PKES pkg>/config/ /usr/share/snmp/ /usr/share/snmp/mibs/	These directories contain the PKES SNMP configuration and MIB files.

Install the PKES Software

1. If necessary, open an xterm window on the ISDS.
2. Type **ssh root@[PKES_IP]** to log on to the PKES from the ISDS.
3. Type the root password and then press **Enter** when prompted to do so.
4. Type **mkdir -p /media/cdrom** and then press **Enter** to create a directory for mounting the CD.
5. Insert the PKES application CD into the CD drive of the PKES.
6. Type **mount /dev/cdrom /media/cdrom** and then press **Enter** to mount the CD. The "/dev/cdrom is write-protected; mounting read-only" message appears.
7. Type **cd /media/cdrom** and then press **Enter**.
8. Type **./install** and then press **Enter**.
9. Type **cd /** and then press **Enter**.
10. Type **umount /media/cdrom** and then press **Enter** to unmount the CD.
11. Type **eject cdrom** and then press **Enter**.
12. Type **rpm -qi SAIpkes-lite** and then press **Enter** to obtain the current version of the PKES application software for ISDP networks.

    Example: The following example illustrates Version 1.1.0.4 of the PKES application software for ISDP networks:

```
Name        : SAIpkes-lite                 Relocations: (not relocatable)
Version     : 1.1.0.4                           Vendor: Cisco Systems,
Inc.
Release     : 1                             Build Date: Thu 28 Jan 2010
11:45:36 AM EST
Install Date: Wed 03 Feb 2010 04:46:08 PM EST      Build Host: happy
Group       : System Environment/Base       Source RPM: SAIpkes-lite-
1.1.0.4-1.src.rpm
Size        : 813368                           License: Proprietary
Signature   : (none)
Packager    : SPVTG
Summary     : SAI PKES Application
Description :
The PKES is responsible for taking clear VOD content in the form of an
MPEG file and producing an encrypted version of the file.  The PKES is
controlled through a web services interface that triggers the transfer of
the asset to the PKES, the encryption of the asset, and the transfer back
to the source machine.
```

13 Did the output display the expected PKES application version?

- If **yes**, continue with step 14.
- If **no**, contact Cisco Services for assistance.

14 Type **service pkesd start** and then press **Enter**.

Note: The "Unknown object identifier" message appears. You can ignore this message.

Configure the PKES Application

Configuring the PKES Software

Follow these instructions to configure the PKES application.

1 At the ISDS directory used in steps 3 and 4 of ***Configuring the VOD MSK on the ISDS*** (on page 19), type
scp vodMskPkes root@[pkes IP]:/usr/local/pkes/bin/vodMskPkes and then press **Enter**.

Note: The vodMskPkes file pertains to the file specified in step 9 of Creating the VOD MSK on the TED.

2 At the password prompt, type the root password.

3 Type **ssh root@[PKES_IP]** and then press **Enter**. The password prompt appears.

4 Type the root password and then press **Enter**.

5 Type **cd /usr/local/pkes/bin** and then press **Enter**. The /usr/local/pkes/bin directory becomes the working directory.

6 Type **./provisionMsk** and then press **Enter**. The system prompts for the path to the vodMskPkes file.

7 Type **/usr/local/pkes/bin/vodMskPkes** and then press **Enter**. The system prompts for the pass phrase you created in step 7 of ***Creating the VOD MSK on the TED*** (on page 18).

Note: The vodMskPkes file pertains to the file specified in step 9 of ***Creating the VOD MSK on the TED*** (on page 18).

8 Type the VOD pass phrase and then press **Enter**.

Editing the pkesConfiguration File

1 Type **cd [PKES pkg]/config** and then press **Enter**. The [PKES pkg]/config directory becomes the working directory.

Note: Substitute the directory in which the PKES package is located for [PKES pkg].

2 Type **vi pkesConfiguration** and then press **Enter** to open the pkesConfiguration file for editing.

3 Edit the pkesConfiguration file to set the following values.

Example: Refer to ***Sample pkesConfiguration File for ISDP Network*** (on page 26) for an example of what the file might look like.

- PKES IP address
- AMS IP address
- Encryption mode to be applied to VOD content
- Crypto period hint delay (in seconds)
- Crypto period ECM construction delay (in seconds)
- Crypto period control word activation delay (in seconds)
- AMS FTP user name to enable file transfers
- AMS FTP password to enable file transfers
- Encryption interrupt rate (determines the number of packets the PKES processes between checking for a query or a cancel command from the AMS)
- Assumed transfer rate in bytes per second (this number is used to estimate the time remaining for the current encryption)
- MSK parity (odd or even)
- Retain error file setting (determines whether or not VOD content should be retained following an error for debugging purposes)
- DRM override mode (enable or disable)
- DRM override setting
- PKES timeout value (determines the time that the PKES waits to timeout an incoming query or cancel command before generating an error)

4 Save the file and close the vi editor.

5 Type **service pkesd restart** and then press **Enter**.

Sample pkesConfiguration File for ISDP Network

An example of a pkesConfiguration file follows:

```
#
# PKES Configuration File
#


#
# IP Address of the PKES
#
PKES_IP_ADDRESS = 172.31.34.1


#
```

```
# IP Address of the AMS
#
AMS_IP_ADDRESS = 172.105.0.150

#
# Core Encryption Mode
#
# Encryption mode specified by following index values:
#
#     0 - PowerKEY native
#     6 - AES NSA 2
#     7 - ATIS_IIF_DSA
#     8 - AES_ECB2
#     9 - AES_ECB1
#
ENCRYPTION_MODE =  6

#
# Crypto period - length of delay in seconds after setting hint bit
#
# Default value: 2
# Minimum value: 1
#
CRYPTO_PERIOD_HINT_DELAY = 2

#
# Crypto period - length of delay in seconds after constructing the ECM
#
# Default value: 1
# Minimum value: 1
#
CRYPTO_PERIOD_CONSTRUCT_ECM_DELAY = 1

#
# Crypto period - length of delay in seconds after activating control word
#
```

```
# Default value: 5
# Minimum value: 2
#
CRYPTO_PERIOD_ACTIVATE_CW_DELAY = 5


#
# FTP account user name
#
FTP_ACCOUNT_NAME = CVC12


#
# FTP account password
#
FTP_ACCOUNT_PASSWORD = hb01231


#
# Encryption interrupt rate
#
# This is the number of packets at which the encryption process is
interrupted
# to check for a query or cancel command from the AMS
#
# Default value: 30000
#
INTERRUPT_RATE = 50000


#
# Encrypted packet threshold
#
# This is the threshold percentage of encrypted packets for an encryption to
# be successful.  In other words, if the encryption of an asset is requested
# and the resulting file has less than the specified percentage of encrypted
# packets, the encryption will be considered a failure
#
# Default value: 50
#
```

```
ENCRYPTION_PERCENTAGE_THRESHOLD = 50

#
# DRM Override value
#
# This value is applied to every asset regardless of the AMS setting as
# long as the override is enabled
#
# The following values are valid:
#    0 - copying is permitted
#    1 - no further copying is permitted
#    2 - one generation copy is permitted
#    3 - copying is prohibited
#
DRM_OVERRIDE_VALUE = 0

#
# DRM Override switch
#
# This switch enables/disables the DRM override setting.  When the override
# is enabled, the setting specified by DRM_OVERRIDE_VALUE will replace
# the DRM setting for each asset received from the AMS
#
#    Options include:
#       Yes
#       No
#
# Default value: No
#
ENABLE_DRM_OVERRIDE = No

#
# Assumed encryption rate
#
# This is the assumed number of packets processed in one second.  This rate
# is used to estimate the remaining number of seconds to encrypt the
```

```
# current asset
#
ESTIMATED_ENCRYPTION_RATE = 80000


#
# Assumed file transfer rate
#
# This is the assumed rate at which files are transferred via FTP in bytes
# per second.  This value is used to estimate the remaining time required
# to process an asset
#
ESTIMATED_TRANSFER_RATE = 35000000


#
# MSK switch
#
# This setting switches between the even/odd MSK
#    Options include:
#       Even
#       Odd
#
# Default value: Even
#
MSK_PARITY = Even


#
# Retain content file setting
#
# This setting enables/disables the saving of a content file when an
# error occurs during the encryption process.  The file is saved
# to a directory labeled with the eventSeqNum in the content/error area
#
#    Options include:
#       Yes
#       No
#
```

```
RETAIN_ERROR_FILE = Yes

#
# Indicates whether PKES Lite will mark packets for encryption
#
# This setting enables/disable the packet marking feature of PKES Lite.
#
#   Option include:
#       1- PKES Lite will mark packets for encryption
#       0- PKES Lite will not mark packets for encryption.
#
#  Default Value: 1
#
PACKET_MARKING = 1

#
#
# PKES timeout value
#
# This setting determines the number of seconds the PKES waits before
# timing out a query or cancel command from the AMS.  The timeout value
# is an integer that must be greater than zero.
#
PKES_TIMEOUT_VALUE = 300
```

Editing the trapDestinationTable File

Complete these instructions to edit the trapDestinationTable file.

1 At the PKES, type **cd <PKES pkg>/config** and then press **Enter**. The <PKES pkg>/config directory becomes the working directory.

Note: Substitute the directory in which the PKES package is located for <PKES pkg>.

2 Type **vi trapDestinationTable** and then press **Enter**. The trapDestinationTable file opens for editing in the vi text editor.

3 Edit the trapDestinationTable file so that the hostname and IP address of each NMS are included in the file, each on a separate line.

Example:

```
#
# SNMP Trap Destination Table
# This table defines the set of destinations for each trap created by
PKES.
# The entries in the table consist of:
#
#    NMS Hostname (string)
#    NMS IP address (string)
#
Nms1, 10.90.176.60
Nms2, 10.90.176.61
Nms3, 10.90.176.62
```

4 Save the file and close the vi text editor.

Set the SNMP Version for PKES Traps

The default SNMP version for PKES SNMP traps is 3. Complete these instructions if a version of SNMP other than SNMPv3 is desired for the SNMP traps.

1 Type the following command and press **Enter** to open the snmp.conf file with a text editor:

vi /usr/share/snmp/snmp.conf

2 Change the defversion value to the desired SNMP version for PKES traps.

Example:

```
defversion  2c
```

3 Save and close the snmp.conf file.

Editing the syslog.conf File

Complete these instructions to edit the syslog.conf file.

1. At the PKES, type **cd /etc** and then press **Enter**. The /etc directory becomes the working directory.
2. Type **vi syslog.conf** and then press **Enter**. The syslog.conf file opens for editing using the vi text editor.
3. Append the following line, as shown, to the end of the syslog.conf file:

   # Saves pkes messages to pkes.log

   ***.debug;kern.none;mail.none;authpriv.none;cron.none /var/log/pkes.log**
4. Save the file and close the vi text editor.
5. Type **service syslog restart** and then press **Enter** to restart the syslog process.

Configure SNMP on the PKES

In this procedure, you will configure the Simple Network Management Protocol (SNMP) of the PKES.

1. Type **service snmpd start** and then press **Enter** to start the snmpd process.
2. Type **cd /usr/share/snmp/mibs** and then press **Enter**.
3. Type **snmpwalk localhost enterprises.1429 | more** and then press **Enter**. The system displays details of the management information base (MIB) tree using the default username, pass phrase, etc. that are stored in the /usr/share/snmp/snmp.conf file.
4. Contact your account representative to obtain the Engine ID, the User ID, and pass phrase information. Use the information you obtain from your account representative to configure your specific Network Management Server to receive the SNMP traps from the PKES.

Configure NTP on the PKES

Configure NTP on the PKES

Complete these instructions to configure NTP on the PKES.

1 At the PKES, type **cd /etc** and then press **Enter**. The /etc directory becomes the working directory.

2 Open the ntp.conf file with a text editor.

3 Within the ntp.conf file, comment out the following lines by placing a **#** at the beginning of each line:

#server 0.rhel.pool.ntp.org

#server 1.rhel.pool.ntp.org

#server 2.rhel.pool.ntp.org

4 After the last server entry, create a new entry containing the IP address for the NTP server to be used as the time source for the PKES.

Example: server 172.40.90.1

Note: The ISDS can be used as the time source for the PKES. If this is desired, use the ISDS dncsatm IP Address.

5 Save and close the file.

6 Type **service ntpd stop** and then press **Enter** to stop the NTP process.

7 Type **ntpdate [NTP Server IP]** and then press **Enter** to synchronize the time on the PKES to the time from the NTP server.

Example: ntpdate 172.40.90.1

8 Repeat step 7 three times.

9 Type **service ntpd start** and then press **Enter** to start the NTP process.

Note: Allow up to 10 minutes for the NTP to fully synchronize its time with the NTP server.

10 Type **ntpq -p** and then press **Enter** to check the synchronization status between the PKES NTP process and the NTP server.

Example: Output should be similar to the following example:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*172.40.90.1	192.133.225.100	5	u	177	1024	377	0.420	9.695	4.578
LOCAL (0)	.LOCL.	10	1	11	64	377	0.000	0.000	0.001

Note: When the PKES has synchronized with the NTP server, the NTP server will contain an asterisk at the beginning of the line, as displayed in the previous example.

Enable Support for Clear DRM VOD Assets (Optional)

Complete these instructions only if you require support for clear DRM VOD assets.

1. On the PKES, type **vi /etc/init.d/pkesd** and then press **Enter**. The pkesd file opens for editing in the vi text editor.
2. Add the following entry to the end of the list:

   export PKES_ENABLE_TSC_CLEAR=1

   Note: The top portion of the pkesd file should look similar to the following example when you are finished:

   ```
   RETVAL=0
   prog="pkes"
   PKES_DIR=/usr/local/pkes/bin
   PKES=pkes
   export PKES_LITE=1
   export PKES_ENABLE_TSC_CLEAR=1
   ```
3. Save and close the pkesd file.

Restart the PKES Application

To restart the PKES application, as root user, type **service pkesd restart** and then press **Enter**.

5

PKES Upgrade Procedures

Introduction

Use the procedures in this chapter to upgrade and configure the PKES platform and/or application software.

Important: If you are installing and configuring the PKES software for the first time, do not complete the procedures in this chapter. Complete the procedures in Chapters 1 through 4, instead.

In This Chapter

Upgrade the PKES Software

Complete the procedures in this section for each PKES server to be upgraded.

Important: Note these important points:

- A keyboard and monitor must be connected to the PKES server before beginning the upgrade of the PKES platform software.
- The PKES MSK file is required to complete the upgrade of the PKES platform software. This file should be onsite prior to beginning these upgrade procedures.

Determining the PKES Platform Software Version

Before you begin, obtain the expected platform version of the PKES from your Cisco account manager. Then, complete the following steps to determine the current PKES platform software version.

1 From an xterm window on the ISDS, type **ssh root@[PKES_IP]** and then press **Enter**.

Note: Substitute the IP address of the PKES server for [PKES_IP].

Important: The root password is not included in these procedures. If you need the root password, contact Cisco Services.

2 Type **rpm -qi SAIlxplat** and then press **Enter** to obtain the current version of the PKES platform software.

Example: The following example illustrates Version 1.0.4 of the PKES platform software.

```
Name        SAIxplat            Relocations:  (not
                                relocatable)
Version     1.0.4               Vendor:  Cisco Systems, Inc.
Release     1                   Build Date: Tue 12 May 2009
                                10:32:21 AM EDT
Install     Tue 16 Jun 2009     Build Host:
Date        04:30:53 AM EDT     sausatlpcg01.dvsg.sciatl.com
Group       System              Source RPM: SAIlxplat-1.0.4-
            Environment/Base    1.src.rpm
Size        0                   License: Proprietary
Signature   (none)
Packager    SPVTG
Summary     SAI Linux Platform Package (RHEL 5.1)
Descripti   The base platform for Linux based products.
on          This rpm is used to track the platform release
            version.
```

Backing Up the PKES Configuration

1. From an xterm window on the ISDS, type **su - dncs** and then press **Enter** to log on as the dncs role.
2. When prompted, type the password for the dncs role and then press **Enter**.
3. **Type mkdir /export/home/dncs/pkes-[PKES-Name or IP]-backup-[YYYYMMDD]** and then press **Enter** to create a directory which will be used to back up the current PKES server configuration.

   Note: Substitute the current date for [YYYMMDD].

   Example: `mkdir /export/home/dncs/pkes-172.105.1.173-backup-20090819`
4. Type **cd /export/home/dncs/pkes-backup-[YYYYMMDD]** and then press **Enter**.
5. Type the following commands to back up the current PKES server configuration.

   Important:

   - In each of the following commands, a space precedes a period at the end of the command.
   - For each of the following commands, when presented with the **password** prompt, type the password for the root user on the PKES.

   a. **scp root@[PKES_IP]:/etc/hosts .** and then press **Enter**.

   b. **scp root@[PKES_IP]:/etc/syslog.conf .** and then press **Enter**.

   c. **scp root@[PKES_IP]:/etc/sysconfig/network .** and then press **Enter**.

   d. **scp root@[PKES_IP]:/etc/sysconfig/network-scripts/ifcfg-eth0 .** and then press **Enter**.

   e. **scp root@[PKES_IP]:/etc/sysconfig/network-scripts/ifcfg-eth1 .** and then press **Enter**.

   f. **scp root@[PKES_IP]:/etc/sysconfig/network-scripts/route-eth0 .** and then press **Enter**.

   g. **scp root@[PKES_IP]:/etc/sysconfig/network-scripts/route-eth1 .** and then press **Enter**.

   h. **scp root@[PKES_IP]:/usr/local/pkes/config/pkesConfiguration .** and then press **Enter**.

   i. **scp root@[PKES_IP]:/usr/local/pkes/config/trapDestinationTable .** and then press **Enter**.

   j. **scp root@[PKES_IP]:/usr/share/snmp/snmpd.conf .** and then press **Enter**.

   k. **scp root@[PKES_IP]:/etc/ntp.conf .** and then press **Enter** to back up the NTP configuration file.

6 Record the following information for later use:

- PKES MGMT IP address: _____
- PKES MGMT Subnet Mask: _____
- PKES Default Gateway: _____

7 Did the PKES server have the desired platform software version, as determined in ***Determining the PKES Platform Software Version*** (on page 40)?

- If **yes**, skip to ***Upgrading the PKES Application Software*** (on page 42).
- If **no**, continue with ***Upgrading the PKES Platform Software*** (on page 42).

Upgrading the PKES Platform Software

1 From the attached keyboard and monitor, log on to the PKES server as **root** user.

2 Type **shutdown -y -g0 -i6** and then press **Enter** to reboot the PKES server.

3 Once the server has begun the reboot process, press the CD/DVD eject button to the drive on the server.

4 Insert the PKES platform CD into the drive tray and close the tray. After a few minutes, the Cisco screen appears.

5 Type **platform** and then press **Enter**. The PKES runs an automated installation script and the following warning message may appear:

The partition table on the device sda was unreadable … Would you like to initialize this drive, erasing ALL DATA?

6 Type **y** and then press **Enter**. The installation script continues.

Note: The installation script should complete within 15 minutes.

7 Go to Upgrading the PKES Application Software.

Upgrading the PKES Application Software

1 Did you just complete an upgrade of the PKES platform software?

- If **yes**, continue with step 2.
- If **no**, skip to step 4.

2 From the attached keyboard and monitor, login to the PKES server as **root** user.

3 Follow these directions to create a directory for mounting the PKES application CD.

a Type **mkdir -p /media/cdrom** and then press **Enter**.

b Skip to step 7.

4 Is the SSH connection to the PKES still established from step 1 of ***Determining the PKES Platform Software Version*** (on page 40)?

- If **yes**, continue with step 5.
- If **no**, from an xterm window on the ISDS, type **ssh root@[PKES_IP]** and then press **Enter**.

  Notes:

  – Substitute the IP address of the PKES server for [PKES_IP].

  – When presented with the **password** prompt, type the password for the **root** user of the PKES server.

5 Type **service pkesd stop** and then press **Enter** to stop the PKES application.

6 Type **service snmpd stop** and press **Enter** to stop SNMP.

7 Insert the PKES application CD into the CD drive of the PKES server.

8 Type **mount /dev/cdrom /media/cdrom** and then press **Enter** to mount the CD.

9 Type **cd /media/cdrom** and then press **Enter**.

10 Type **./install** and then press **Enter** to upgrade of the PKES application software.

Notes:

- The system displays the command prompt when the installation is complete.
- Check the log file for errors. The log file is /var/tmp/INST_R_SAIpkes.log.

  Note: Ignore the following message:

  # rpm -e SAIpkes
  error: package SAIpkes is not installed

11 When the PKES application software has finished installing, type **cd /** and then press **Enter**.

12 Type **umount /media/cdrom** and then press **Enter** to unmount the CD.

13 Type **eject cdrom** and then press **Enter** to eject the CD from the drive.

14 Type **rpm -qi SAIpkes-lite** and the press **Enter** to obtain the current version of the PKES application software.

Example: The following example illustrates Version 1.1.0.1 of the PKES application software for ISDP networks:

```
[root@platform ~]# rpm -qi SAIpkes-lite
Name        : SAIpkes-lite                  Relocations: (not
relocatable)
Version     : 1.1.0.1                           Vendor: Cisco
Systems, Inc.
Release     : 1                              Build Date: Mon 10
Aug 2009 08:01:54 AM EDT
Install Date: Wed 19 Aug 2009 12:32:17 AM EDT      Build Host:
happy
Group       : System Environment/Base       Source RPM:
SAIpkes-lite-1.1.0.1-1.src.rpm
Size        : 676350 Licenses: Proprietary
Signature   : (none)
Packager    : SPVTG
Summary     : SAI PKES Application
Description:
The PKES is responsible for taking clear VOD content in the
form of an MPEG file and producing an encrypted version of the
file.  The PKES is controlled through a web services interface
that triggers the transfer of the asset to the PKES, the
encryption of the asset, and the transfer back to the source
machine.
```

15 Did the output display the expected PKES application version?

- If **yes**, continue with step 16.
- If **no**, call Cisco Services for assistance.

16 Did you previously upgrade the PKES platform software (in ***Upgrading the PKES Platform Software*** (on page 42))?

- If **yes**, continue with ***Restoring the PKES Platform Configuration Files***.
- If **no**, skip to ***Restoring the PKES Application Configuration Files*** (on page 46).

Restoring the PKES Platform Configuration Files

1 Reference the information from step 8 of ***Backing Up the PKES Configuration*** (on page 41), to temporarily configure the PKES MGMT network interface to allow the PKES platform configuration files to be restored.

Note: You will temporarily configure the PKES MGMT network interface in the next few steps.

2 On the PKES, type **cd /etc/sysconfig/network-scripts** and then press **Enter**. The /etc/sysconfig/network-scripts becomes the working directory.

3 Type **vi ifcfg-eth0** and then press **Enter**. The ifcfg-eth0 file opens for editing using the vi text editor.

4 Update the ifcfg-eth0 file with the following information:

- **IPADDR=[PKES MGMT IP address]**
- **NETMASK=[PKES MGMT Subnet Mask]**

Note: For both of these values, reference the **PKES MGMT IP address** and the **PKES MGMT Subnet Mask** you recorded in step 8 of ***Backing Up the PKES Configuration*** (on page 41).

5 Save the file and close the vi editor.

6 Type **vi route-eth0** and then press **Enter**. The route-eth0 file opens for editing using the vi text editor.

7 Update the route-eth0 file with the following information:

- **GATEWAY0=[PKES Default Gateway]**
- **NETMASK0=0.0.0.0**
- **ADDRESS0=0.0.0.0**

Note: For the GATEWAY0 value, reference the **PKES Default Gateway** you recorded in step 8 of ***Backing Up the PKES Configuration*** (on page 41).

8 Save the file and close the vi editor.

9 Type **service network restart** and then press **Enter**.

10 From the PKES, type **ping [ISDS_IP]** and then press **Enter** to verify network communications.

11 Was the response from the ping command successful?

- If **yes**, continue with step 12.
- If **no**, contact Cisco Services for assistance.

12 From an xterm window on the ISDS, type **su - dncs** and then press **Enter** to log on in the dncs role.

13 Type **cd /export/home/dncs/pkes-backup-[YYYYMMDD]** and then press **Enter** to navigate to the directory in which you backed up the PKES configuration.

Note: This is the directory created in step 5 of ***Backing Up the PKES Configuration*** (on page 41).

14 Type the following commands to restore the platform configuration files.

Important: For each of the following commands, when presented with the **password** prompt, enter the password for the root user on the PKES.

a **scp hosts root@[PKES_IP]:/etc/hosts** and then press **Enter**.

b **scp syslog.conf root@[PKES_IP]:/etc/syslog.conf** and then press **Enter**.

c **scp network root@[PKES_IP]:/etc/sysconfig/network** and then press **Enter**.

d **scp ifcfg-eth0 root@[PKES_IP]:/etc/sysconfig/network-scripts/ifcfg-eth0** and then press **Enter**.

e **scp ifcfg-eth1 root@[PKES_IP]:/etc/sysconfig/network-scripts/ifcfg-eth1** and then press **Enter**.

f **scp route-eth0 root@[PKES_IP]:/etc/sysconfig/network-scripts/route-eth0** and then press **Enter**.

g **scp route-eth1 root@[PKES_IP]:/etc/sysconfig/network-scripts/route-eth1** and then press **Enter**.

h **scp ntp.conf root@[PKES_IP]:/etc/ntp.conf** and then press **Enter** to restore the NTP configuration file.

15 Go to Restoring the PKES Application Configuration Files.

Restoring the PKES Application Configuration Files

1 From an xterm window on the ISDS, type **su - dncs** and then press **Enter** to log on as the dncs role.

2 Type **cd /export/home/dncs/pkes-backup-[YYYYMMDD]** and then press **Enter** to navigate to the directory in which you backed up the PKES configuration.

Note: This is the directory created in step 5 of ***Backing Up the PKES Configuration*** (on page 41).

3 Type the following commands to restore the PKES application configuration files:

Important: For each of the following commands, when presented with the **password** prompt, enter the password for the root user on the PKES.

a **scp pkesConfiguration root@[PKES_IP]:/usr/local/pkes/config/pkesConfiguration** and then press **Enter**.

b **scp trapDestinationTable root@[PKES_IP]:/usr/local/pkes/config/trapDestinationTable.orig** and then press **Enter**.

c **scp snmpd.conf root@[PKES_IP]:/usr/share/snmp/snmpd.conf.orig** and then press **Enter**.

Restoring the PKES SNMP Configuration

Complete these procedures to restore the PKES SNMP Configuration.

Checking the PKES Trap Destinations

1 From an xterm window on the ISDS, type **ssh root@[PKES_IP]** and press **Enter**. The password prompt appears.

Note: Substitute the IP address of the PKES for [PKES_IP].

2 Type the root password and press **Enter**.

3 Type **cd /usr/local/pkes/config** and press **Enter**.

4 Type **cat trapDestinationTable.orig** and press **Enter**. The system displays a list of trap destinations.

5 Does the list of original SNMP trap destinations include any entries that are not default values?

Note: The following is an example list of the default values:

Nms1, 10.90.176.60

Nms2, 10.90.176.61

Nms3, 10.90.176.62

- If **yes**, complete the following steps to update the trapDestinationTable file with the custom trap destinations that existed prior to the upgrade.
  - **a** Type **vi trapDestinationTable** and press **Enter**.
  - **b** Replace the existing default trap destination entries with the custom hostname and IP address of the custom trap destinations.

    Example: <NMS hostname>, <NMS IP address>

    Notes:

    - Replace <NMS hostname> with the hostname of the NMS.
    - Replace <NMS IP address> with the IP address of the NMS.
  - **c** Save and close the file when you are finished.
- If **no**, go to step 6.

6 Type **cd /usr/share/snmp** and press **Enter**.

7 Type **grep trapsess snmpd.conf.orig** and press **Enter**. The system displays the original platform trap destination entries.

Example:

trapsess -v 2c -c trapcomm 172.40.90.1:162

trapsess -e 0x80001f88800ed6913fdbb5774800000000 -v 3 -u myuser -a MD5 -A mypassword -l authNoPriv 172.40.90.1:162

8 Were any trap destinations displayed in the output from step 7?

- If **yes**, go to step 9.
- If **no**, you are finished with this procedure; go to ***Checking the SNMP Communities*** (on page 48).

9 Type **vi snmpd.conf** and press **Enter**.

10 Add all of the original trap destinations to the end of the snmpd.conf file.

11 Did any of the original trap destinations include **-v 3** which indicates the trap destination is SNMPv3?

- If **yes**, follow these instructions to verify the engine ID.
  - **a** As **root** user in another xterm window on the PKES, type **grep usmUser /var/net-snmp/snmpd.conf** and press **Enter**. SNMP configuration data, including the hexadecimal engine ID, appears.

    Note: The first hexadecimal number after **usmUser 1 3** in the second entry returned in the results from step a is the SNMPv3 engine ID.

Example: 0x80001f88800ed6913fdbb5774800000000

b Does the engine ID displayed in step 11 a match the engine ID of the original SNMPv3 trap destination?

- If **yes**, go to step 11 c.
- If **no**, then update the SNMPv3 trap destination engine ID with the engine ID found in step 11 a.

c Save and close the snmpd.conf file.

Checking the SNMP Communities

1 From the SSH session connected to the PKES, as root user, type **grep rocommunity snmpd.conf.orig** and press **Enter**. The system displays all of the original SNMPv2 communities configured on the PKES.

2 Did the system display any un-commented values other than the following:

rocommunity public localhost

rocommunity public 192.168.44.60

- If **yes**, go to step 3.
- If **no**, go to *Restarting the SNMP Daemon* (on page 48).

3 Complete the following steps to restore the SNMPv2 communities on the PKES.

a Type **vi snmpd.conf** and press **Enter**.

b Add all of the original SNMPv2 community entries to the end of the snmpd.conf file.

Important: Do not add the following entries:

rocommunity public localhost

rocommunity public 192.168.44.60

c Save and close the snmpd.conf file.

Restarting the SNMP Daemon

1 Did you make any changes to *either* the snmpd.conf file or the trapDestinationTable file?

- If **yes**, follow these steps to restart the Net-SNMP daemon.
  a Type **service snmpd stop** and press **Enter**.
  b Type **service snmpd start** and press **Enter**.
  c Type **service snmpd status** and press **Enter** to verify that the Net-SNMP daemon started.

  Example: Output should look similar to the following:

  snmpd (pid 6895) is running...
- If **no**, go to *Enable Support for Clear DRM VOD Assets (Optional)* (on page 49).

2 Type **exit** and then press **Enter** to log out of the PKES as root user.

Enable Support for Clear DRM VOD Assets (Optional)

Complete these instructions only if you require support for clear DRM VOD assets.

1 On the PKES, type **vi /etc/init.d/pkesd** and then press **Enter**. The pkesd file opens for editing in the vi text editor.

2 Add the following entry below the line that reads PKES=pkes

export PKES_ENABLE_TSC_CLEAR=1

Note: The top portion of the pkesd file should look similar to the following example when you are finished:

RETVAL=0
prog="pkes"
PKES_DIR=/usr/local/pkes/bin
PKES=pkes
export PKES_ENABLE_TSC_CLEAR=1

3 Save and close the pkesd file. Continue with *Initializing the PKES Upgrade* (on page 49).

Initializing the PKES Upgrade

1 From an xterm window on the ISDS, type **ssh root@[PKES_IP]** and press **Enter**. The password prompt appears.

2 Type the root password and press **Enter**.

3 Type **shutdown -y -g0 -i6** and then press **Enter** to reboot the PKES server and implement the restored configuration files.

4 Once the PKES server has rebooted, from the ISDS, type **ping [PKES_IP]** and then press **Enter** to verify communications between the ISDS and PKES server.

5 Was the response from the ping command successful?

- If **yes**, continue with Installing the PKES MSK.
- If **no**, contact Cisco Services for assistance.

Installing the PKES MSK

1 Did you previously upgrade the PKES platform software?

- If **yes**, continue with step 2.
- If **no**, skip to *Verifying the PKES Upgrade* (on page 50).

2 From an xterm window on the ISDS, type **scp /export/home/dncs/vodMsk/vodMskPkes root@<PKES_IP>:/usr/local/pkes/bin/vodMskPkes** and then press **Enter** to copy the PKES MSK file onto the PKES server.

3 At the password prompt, type the **root** password for the PKES server.

4 Type **ssh root@[PKES_IP]** and press **Enter**. The password prompt appears.

5 Type the **root** password and press **Enter**.

6 Type **cd /usr/local/pkes/bin** and press **Enter**.

7 Type **./provisionMsk** and then press **Enter**. The system prompts for the path to the vodMskPkes file.

8 Type **/usr/local/pkes/bin/vodMskPkes** and then press **Enter**. The system prompts for the pass phrase you created in step 8 of ***Creating the VOD MSK on the TED*** (on page 18).

9 Type the VOD pass phrase and then press **Enter**.

10 Type **service pkesd restart** and then press **Enter** to restart the PKES and to activate these changes.

11 Complete the ***Configure SNMP on the PKES*** (on page 34) procedure.

12 Continue with ***Verifying the PKES Upgrade*** (on page 50).

Verifying the PKES Upgrade

1 From an xterm window on the ISDS, type **ssh root@[PKES_IP]** and press **Enter**. The password prompt appears.

2 Type the root password and press **Enter**.

3 Type **ping [AMS_IP]** and press **Enter** to verify communications between the AMS and the PKES.

4 Was the response to the ping command successful?

- If **yes**, continue with step 5.
- If **no**, call Cisco Services.

5 From the AMS-PKES, navigate to the list of encryption delegates and verify that the upgraded PKES is in an online state. If not, set it online.

6 Take note of the total number of online PKES devices.

7 From the OpenETF Pre-Processor, export a series of packages to the AMS-PKES, one package for each online PKES.

8 Monitor the package ingest on the AMS-PKES.

9 Verify that the ingested packages display a state of **encrypting** while the PKES servers are encrypting the assets and a state of **encrypted** once the PKES servers have completed encrypting the assets.

6

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

Index

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

June 2012 Printed in USA

Part Number 4034718 Rev B