



# Operating System Conversion Procedure for Supervisor Engine 1A and Supervisor Engine 2

---

**Product numbers:**  
C6K-S1M1-HN-KIT=  
C6K-S1M2-HN-KIT=  
C6K-S2M2-HN-KIT=

This document provides the procedure for converting a Catalyst operating software image to a Cisco IOS image on a Supervisor Engine 1A and Supervisor Engine 2 using a removable media card.

## Converting from Catalyst Operating System to Cisco IOS for Dual Supervisor Engines and High Availability

This procedure is applicable for chassis with dual supervisor engines and operating in high availability mode. After you complete the installation of the replacement supervisor engine, follow the procedure to convert the system from the Catalyst operating system image to a Cisco IOS image.

### Installing the Replacement Supervisor Engine

To install the replacement supervisor engine, follow these steps:

- Step 1** Remove the defective supervisor engine from the Catalyst 6500 series switch.  
If you are unsure about the correct procedure for removing a supervisor engine from the switch chassis, refer to the removal and replacement procedures at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15767.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15767.htm)
- Step 2** Slide the replacement supervisor engine half way into the chassis.  
Refer to the module installation procedure in the module installation note located at the URL in Step 1.
- Step 3** Insert the PCMCIA card into the supervisor engine PCMCIA slot 0.



---

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

© 2004–2006 Cisco Systems, Inc. All rights reserved.



**Note** If your previous supervisor engine had a PCMCIA card installed that contained the correct Cisco IOS software release, you can use it for this step. If your supervisor engine does not have a PCMCIA card that contains the correct Cisco IOS release, use the PCMCIA card that comes with the software conversion kit.

**Step 4** Connect the console terminal cable to the replacement supervisor engine CONSOLE port.



**Note** Use an EIA/TIA-232 (RS-232) cable to connect the console terminal to the supervisor engine CONSOLE port.

**Step 5** Slide the supervisor engine the rest of the way into the chassis slot.

If you are unsure about the correct procedure for installing a supervisor engine in the switch chassis, refer to the module removal and replacement procedures at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15767.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15767.htm)

**Step 6** Press the **Ctrl** plus **Break** keys to enter the break sequence.

You might need to repeat this keystroke sequence several times before the supervisor engine enters the ROMMON mode.

## Changing ROMMON Configuration to Convert from the Catalyst Operating System to the Cisco IOS Operating System

This procedure is applicable for chassis with dual supervisor engines and operating in redundant mode with high availability. After you complete the installation of the removable media card as specified in the “Installing the Replacement Supervisor Engine” section on page 1, follow these steps to convert a system from a Catalyst operating software image to a Cisco IOS image:

	Command	Purpose
<b>Step 1</b>	rommon 1> <b>set</b> CONFIG_FILE=bootflash:switch.cfg BOOT=bootflash:cat6000-sup2k8.8-4-1.bin,1:	Displays the boot variables.
<b>Step 2</b>	rommon 2> <b>BOOT=</b> rommon 3> <b>CONFIG_FILE=</b>	Clears the boot variables.
<b>Step 3</b>	rommon 4> <b>BOOT=slot0:c6sup22-jsv-mz.121-26.E1.bin</b>  <b>Note</b> slot0: could also be disk0: if you are using an ATA flash disk.	Sets the boot variable to point to the Cisco IOS image on the PCMCIA card.
<b>Step 4</b>	rommon 5> <b>sync</b>	Causes the above changes to take effect.
<b>Step 5</b>	rommon 6> <b>reset</b> :: <output omitted> :: Router-sdby> Standby console disabled Router-sdby> Standby console disabled	Resets the supervisor engine from the ROMMON prompt.

	Command	Purpose
Step 6	<pre>Router&gt; Router&gt; en Router# sh bootvar BOOT variable = slot0:c6sup22-jsv-mz.121-26.E1.bin,1 CONFIG_FILE variable does not exist BOOTLDR variable= Configuration register is 0x2102 Standby is up</pre>	<p>Plug the console cable back into the active supervisor engine and verify the boot variables.</p>
Step 7	<pre>Router# format slavesup-bootflash:</pre>	<p>Formats the slave supervisor engine bootflash.</p> <p><b>Note</b> If the slave supervisor engine bootflash is not formatted, the standby supervisor engine will retain the Hybrid mode algorithm. The configuration changes will not be copied between the active and standby supervisor engines.</p>
Step 8	<pre>&gt;show mod</pre>	<p>Verifies that the replacement supervisor engine is recognized by the system.</p> <p><b>Note</b> Both supervisor engines should be recognized by the system; one supervisor engine shown as being active and the other supervisor engine as standby.</p>

After you have completed the operating system conversion task, finish the process by attaching the network interface cables to the interface ports.

# Converting from Catalyst Operating System to Cisco IOS for a Single Supervisor Engine

This procedure is applicable for chassis equipped with a single supervisor engine. After you complete the installation of the replacement supervisor engine, follow the procedure to convert the system from the Catalyst operating system image to a Cisco IOS image.

## Installing the Replacement Supervisor Engine

To install the replacement supervisor engine, follow these steps:

**Step 1** Obtain and save the current the switch configuration.



**Note** You might need to consult with the system administrator to see if they have a copy of the current system configuration. If you do not have a copy of the configuration, obtain the enable password and save a copy of the current configuration to your computer or by contacting the NOC, the customer, a site representative, or by using the configuration from a PCMCIA card.

**Step 2** Power down the chassis by turning the power supply power switch to the 0 position. If there is a second power supply in the chassis, turn its power switch to the 0 position.



**Note** You must power down the switch in chassis equipped with only one supervisor engine. Network traffic will be lost during the period of time the system is shut down.

**Step 3** Remove the defective supervisor engine from the Catalyst 6500 series switch.

If you are unsure about the correct procedure for removing a supervisor engine from the switch chassis, refer to the removal and replacement procedures at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15767.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15767.htm)

**Step 4** Slide the replacement supervisor engine half way into the chassis.

Refer to the module installation procedure in the module installation note located at the URL in Step 3.

**Step 5** Insert the PCMCIA card into the supervisor engine PCMCIA slot 0.



**Note** If your previous supervisor engine had a PCMCIA card installed that contained the correct Cisco IOS software release, you can use it for this step. If your supervisor engine does not have a PCMCIA card that contains the correct Cisco IOS release, use the PCMCIA card that comes with the software conversion kit.

**Step 6** Connect the console terminal cable to the replacement supervisor engine CONSOLE port.



**Note** Use an EIA/TIA-232 (RS-232) cable to connect the console terminal to the supervisor engine CONSOLE port.

**Step 7** Finish installing the supervisor engine in the chassis slot. If you are unsure about the correct procedure for installing a supervisor engine in the switch chassis, refer to the module removal and replacement procedures at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78\\_15767.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/78_15767.htm)

**Step 8** Power up the switch chassis by turning the power supply power switch to the I position. If the chassis is equipped with a second power supply, power it up by turning the power switch to the I position.

**Step 9** Press the Ctrl plus Break keys to enter the break sequence. You might need to repeat this keystroke sequence several times before the supervisor engine enters the ROMMON mode.

## Changing ROMMON Configuration to Convert from Catalyst Operating System to Cisco IOS on Chassis with One Supervisor Engine

This procedure is applicable for chassis with one supervisor engine. After you complete the installation of the replacement supervisor engine, follow these steps to convert a system from the Catalyst operating system image to a Cisco IOS image:

	Command	Purpose
<b>Step 1</b>	rommon 1> <b>set</b> CONFIG_FILE=bootflash:switch.cfg BOOT=bootflash:cat6000-sup2k8.8-4-1.bin,1:	Displays the boot variables.
<b>Step 2</b>	rommon 2> <b>BOOT=</b> rommon 3> CONFIG_FILE=	Clears the boot variables
<b>Step 3</b>	<b>rommon 4&gt; BOOT=slot0:c6sup22-jsv-mz.121-26.E1.bin</b> <b>Note</b> slot0: could also be disk0: if you are using an ATA flash disk.	Sets the boot variable to point to the Cisco IOS image on the PCMCIA card.
<b>Step 4</b>	rommon 5> <b>sync</b>	Forces the previous changes to take effect.
<b>Step 5</b>	rommon 6> <b>reset</b> :: <output omitted> ::	Resets the supervisor engine from the ROMMON prompt.
	<b>Note</b> The supervisor engine reloads normally.	

## Related Documentation

For additional information on the operating system conversion process, refer to the following URLs:

- <http://www.cisco.com/warp/customer/473/80.shtml>
- <http://www.cisco.com/warp/customer/473/81.html>

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents shipped with your product.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

© 2004–2006 Cisco Systems, Inc. All rights reserved.