Multiprocessor WAN Application Module User Guide

for Mobile Wireless Applications
March 28, 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-7469-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Multiprocessor WAN Application Module User Guide

CONTENTS

Preface

This preface discusses the objectives, audience, organization, and conventions of this *user guide*.

Note Use this document along with the documents listed in the "Related Documentation" section on page xviii.

This preface contains the following sections:

Document Revision History

The Document Revision History table below records technical changes to this document. The table shows the document revision number for the change, the date of the change, and a brief summary of the change. Note that not all Cisco documents use a Document Revision History table.

Revision	Date	Change Summary
OL-7469-04	March 28, 2007	Updated the command clear logging slot, page 3
OL-7469-03	February 20, 2007	Updated Supported Applications, page 1-8. Added Configuring the MWAM Memory Allocation, page 6-17. Added the command memory-size iomem, page A-27
OL-7469-02	August 1, 2006	Added information to Memory, page 1-6 about allocating IO memory. Added note to AP and MP Upgrades, page 5-4 about AP and ROMMON images. Added new section: Recover from Session/Telnet Command after Reload, page 6-20.
OL-7469-01	October 25, 2005	Added new section: Feature Improvement, page 1-13. Added the following commands: • boot-mode • show boot-mode Modified the following command: • mwam config-mode Reorganized document for clarity. Retired part number OL-4858-xx.
OL-4858-07	June 24, 2004	Added new section: Recovering from Session Loss, page 6-21. Added the following commands: • show tech-support • show version
OL-4858-06	June 1, 2004	Added information to Remote Console Support for the Processor Control Complex, page 1-15.
OL-4858-05	May 21, 2004	Added description of Multicast MAC Addressing, page 6-10.
OL-4858-04	March 12, 2004	Updated document to include support for 1 GB memory per MWAM processor.

Revision	Date	Change Summary
OL-4858-03	February 26, 2004	Introduced the following features with Cisco IOS 12.3(5a)B: • Remote Console Support for the Processor Control Complex, page 1-15 • Inline IOS Image Upgrades from AP, page 1-18 • Persistent Log Files, page 1-18 Introduced the following feature with Cisco IOS 12.2(14)ZA7: • Assigning MWAM Traffic to VLAN QoS Policies, page 6-5 Added the following commands: • show images • restore ios • show mwam • mwam module vlan-based Added the following restriction on HSRP use with MWAMs: • Hot Standby Router Protocol Configuration, page 6-10
OL-4858-02	January 12, 2004	Most NTP/clock commands are now supported on MWAM; unsupported commands are listed in the Unsupported Commands, page 6-3. Introduced with Cisco IOS 12.3(3)B1.
OL-4858-01	April 3, 2003	First issue of this document.

Objectives

This guide provides an overview of the Multiprocessor WAN Application Module (MWAM) and its features. Included in this guide are instructions on how to install, remove, load, and configure the module.

Note This guide provides software configuration information, but it is not comprehensive. For detailed software configuration, refer to the Cisco IOS configuration guide and command reference publications (see the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page xx for more information).

Audience

If you are an installer, technician, or administrator, this guide contains information you can use to install, configure, and administer your MWAM.

This guide is also appropriate for managers or planners who are thinking about installing an MWAM in a Catalyst 6500/Cisco 7600 chassis, as well as people who are interested in the MWAM in general.

This guide is designed with the assumption that you are already familiar with networking products, concepts, and terminology, but may not be familiar with Cisco products or the Cisco nomenclature.

Organization

This guide is made up of this preface and six major chapters with supplementary information provided in Appendix A and B.

Chapter	Chapter Title	Description
1	Multiprocessor WAN Application Module	Discusses the MWAM, its architecture, software, features, and system requirements.
2	Preparing to Install the MWAM	Describes general safety recommendations, site preparations, required tools and equipment, and includes the installation checklist.
3	Installing the MWAM	Provides steps to install, remove, and verify the MWAM.
4	Command-Line Interface (CLI) Basics	Provides basic information about the command-line interfaces (CLIs) used in loading, upgrading, and configuring the MWAM.
5	Loading the MWAM	Describes the image loading process, loading procedures, and steps to boot the application.
6	Configuring the MWAM	Provides a configuration overview, a list of configuration tasks, and configuration procedures.
Appendix A	Command Reference	Includes syntax, usage guidelines, and examples of MWAM-related commands.
Appendix B	Troubleshooting	Discusses general and specific MWAM problem solving, and provides MWAM error messages, explanations of messages, and recommended actions.

Conventions

This guide uses the following conventions:

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example passwords, appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement. The safety warnings provide safety guidelines that you should follow when working with any equipment that connects to electrical power or telephone wiring. Included in the warnings are translations in several languages. (Refer to the *Cisco Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches and Cisco 7600 Series Routers* for detailed information about compliance guidelines and translated safety warnings.)

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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 de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal 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 vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告　重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의　중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso　**INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel　**VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير　**إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.
قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.3, the Catalyst 6500 Series Switch, and the Cisco 7600 Series Internet Router. These documents consist of release notes and platform related software and hardware installation guides, Cisco IOS configuration and command references, and other documents.

These documents are found in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following release notes are specific to MWAM and Release 12.3 and are located on the Documentation DVD at:

- *Release Notes for Catalyst 6500 and Cisco 7600 Multi-Processor WAN Application Module Software*
- *Release Notes for Cisco IOS Release 12.2(14)ZA4 on the Catalyst 6500 Series and Cisco 7600 Series Supervisor Engine and MSFC*

Note Cisco IOS Release 12.2(14)ZA5 is a Cisco early deployment release intended for customers deploying the MWAM (Multiprocessor Application Module).

- *Cross-Platform Release Notes and Caveats for Cisco IOS Release 12.3*

On Cisco.com (for MWAM), click:

Documentation>Routers>Cisco 7600 Series Routers>General Information>Release Notes>Release Notes for Cisco Multiprocessor WAN Application Module with Cisco IOS Release

On Cisco.com (for IOS), click:

Documentation>Cisco IOS Software>Cisco Software Releases 12.3 Mainline>General Information>Release Notes>Cisco IOS Release 12.3 Cross-Platform Release Notes and Caveats

Note If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

- For product bulletins, field notices, and other specific documents, on Cisco.con and click:

  Technical Documentation

  then, scroll down to “Other Resources” and select the desired item.

Platform-Specific Documents

The following is a list of platform-specific documents. These documents provide supplementary information for the *Multiprocessor WAN Application Module User Guide*. Copies of these manuals are available online at Cisco.com:

Note The list is not all inclusive. It is a representative sampling of the manuals that are available. Depending on your particular model number, refer to that manual for proper installation, configuration, and provisioning information.

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6000 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Module Installation and Configuration Documentation*
- *Catalyst Operating System Documentation for the Supervisor Engine and MSFC*

  (Includes Software Configuration Guides, Command References, and System Message Guides.)
- *Regulatory Compliance and Safety Information for the Cisco 7600 Routers*
- *Cisco 7600 Series Router Installation Guide*
- *Cisco 7609 Series Router Installation Guide (OSR-7609)*
- *Cisco 7600 Series Router Module Installation Guide*
- *Cisco 7600 Series Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Cisco IOS Command Reference*

- *Site Preparation and Safety Guide*
- *Cisco Packet Data Serving Note (PDSN) Release 1.2*
- *Cisco Mobile Wireless Home Agent*
- *Service Selection Gateway*
- *GGSN Configuration Guide*

Note If you plan to deploy IPSec services, please refer to the Documentation DVD or to these publications on Cisco.com for installation and configuration information:

http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800c4fe2.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Multiprocessor WAN Application Module

This chapter describes the Multiprocessor WAN Application Module (MWAM) and includes the following sections:

Product Overview

The MWAM is a Cisco IOS application module that you can install in the Cisco Catalyst 6500 Series switch or the Cisco 7600 Series Internet Router.

Each MWAM contains three processor complexes, with two CPUs each. Each CPU can be used to run an independent IOS image. Two CPUs in each processor complex share one Gigabit Ethernet interface to the switching fabric on the Catalyst 6500 switch or Cisco 7600 router. These Gigabit Ethernet interfaces perform as 802.1Q trunk ports, which carry virtual LAN (VLAN) encapsulated traffic to and from the network. Two processor complexes have access to 1 GB of memory and the third has access to 512 MB.

Features unique to the MWAM are:

- Provides up to 5 IOS images on one card
- Uses IPSec Acceleration Module for hardware support of IPSec
- Supports several Cisco mobile wireless applications to increase session density, improve management capabilities, and reduce complexity of configuration. These include:
  - Cisco Gateway GPRS Support (GGSN)—General Packet Radio Service (GPRS) Packet Gateway
  - Cisco Home Agent (HA)—Mobile IP Agent
  - Cisco Packet Data Serving Node (PDSN)—Code Division Multiple Access (CDMA) Packet Gateway
  - Cisco Service Selection Gateway (SSG)—Service Creation and Management Gateway

Note Each application on the MWAM has its own release schedule. For this reason, some MWAM features and commands documented in this publication may have changed for your application. Refer to the release notes for your application to determine the latest information about specific features and commands.

For release notes and feature module descriptions of mobile wireless applications that are supported on MWAM, see the "Supported Applications" section on page 1-8 of this user guide.

MWAM Ordering Information

The MWAM comes in two product types with the WS-SVC-MWAM-1 product having two options:

- WS-SVC-MWAM-1—Cisco Multiprocessor WAN Application Module (base card)
  - MEM-MWAM-512MB—Standard option for 512 MB memory per MWAM processor
  - MEM-MWAM-1GB—Option for 1 GB memory per MWAM processor
- SC-SVC-NAP-1.0—Cisco Multiprocessor WAN Application Module with No Application (NOAP)

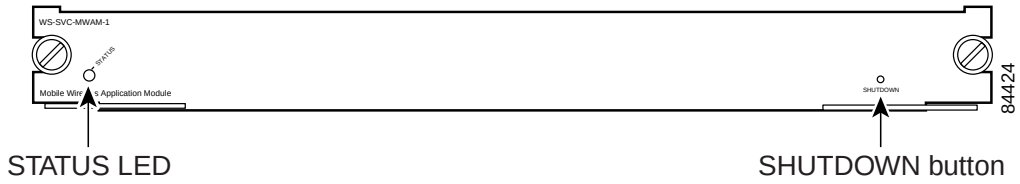
Hardware Description

Contained in a standard circuit card module, the MWAM weighs from 3-5 pounds (1.36-2.27 kg) and measures 1.18 in. high x 15.51 in. wide x 16.34 in. deep (3.0 cm x 39.4 cm x 41.5 cm). Each base MWAM contains six 700-MHz MIPs CPUs, one DIMM supporting up to 64 MB of Flash memory, and an SDRAM containing 5 DIMMs supporting 512 MB each, two processor complexes with 2 DIMMs each, and one processor complex with 1 DIMM (see the "Functional Description" section on page 1-4). Each module slides into a Catalyst 6500/Cisco 7600 chassis slot and connects directly to the backplane where each connects to power and communications located on the rear panel.

Front-Panel Features

On the MWAM front panel (see Figure 1-1), an LED (labeled STATUS) indicates the operating status of the MWAM and a recessed pushbutton (labeled SHUTDOWN) is used to manually shutdown (power off) the MWAM.

Figure 1-1 MWAM Front Panel



LED

Table 1-1 describes the MWAM LED.

Table 1-1 MWAM LED Description

LED	Color	State	Description
Status (labeled STATUS)	Green	On	All diagnostic tests pass. The MWAM is operational.
	Red	On	A diagnostic other than an individual port test failed.
	Orange	On	Indicates one of three conditions: • The MWAM is running through its boot and self-test diagnostic sequence. • The MWAM is disabled. • The MWAM is in the shutdown state.
		Off	The MWAM is powered off.

Shutdown Button

The SHUTDOWN button is used to manually shut down the MWAM. If the MWAM fails to respond to a **shutdown** command (see the following MWAM Shutdown section), you can shutdown the MWAM by using a small, pointed object (such as a paper clip) to access the recessed SHUTDOWN button on the front panel (see Figure 1-1 on page 1-3).

MWAM Shutdown

Caution The MWAM is *not* hot-swappable. Do *NOT* remove the MWAM from the chassis until the module has shut down completely and the STATUS LED is orange or off. You can damage the MWAM if you remove it from the chassis before it completely shuts down.

Shutting Down the MWAM

To shut down the MWAM, perform the following steps:

1. Enter the **show module** command and verify the MWAM status is `OK`.
2. Shut down the module with the **hw-module module** *mod* **shutdown** command in the privileged mode.
3. Enter the **show module** command and verify the MWAM status is `ShutDown` and the LED is orange.
4. Remove the MWAM as described in the "MWAM Removal" section on page 3-10.

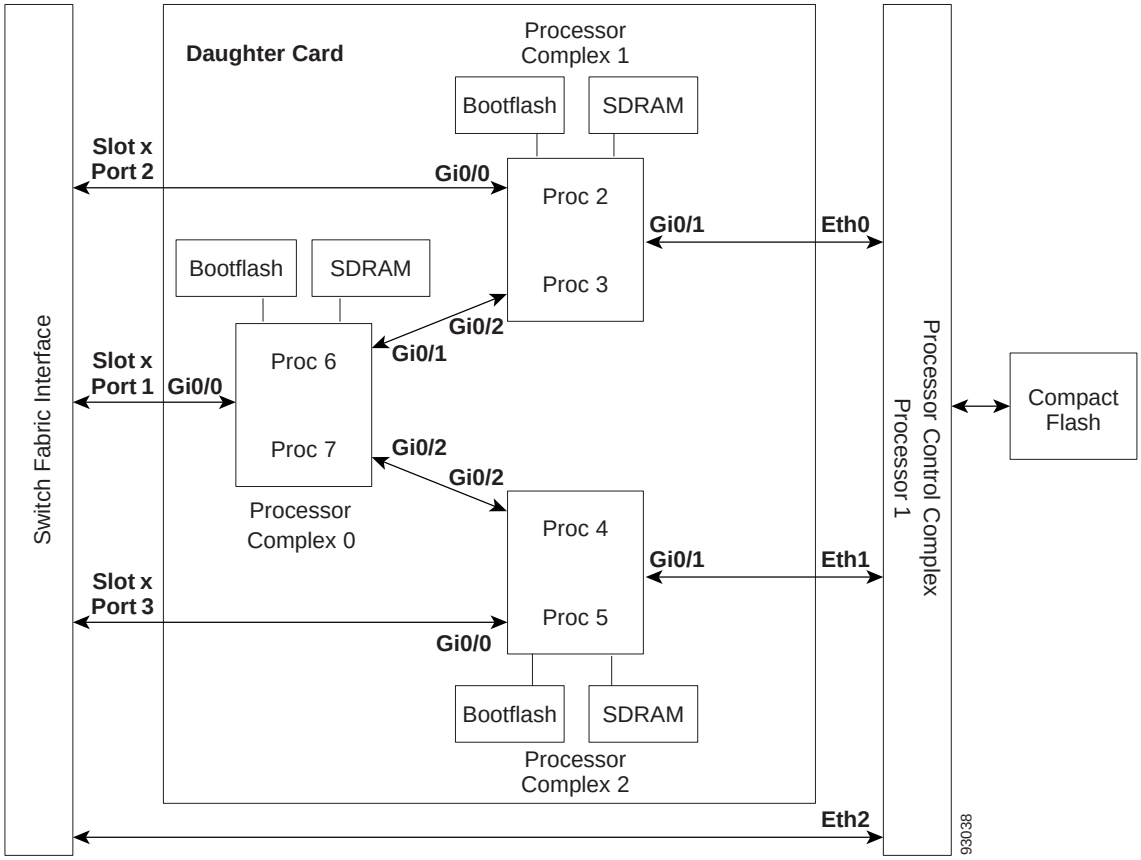
If the MWAM fails to respond to the **shutdown** command, a console message indicates `no response`. Issuing the **show module** command would reveal that the MWAM status is `Other`. In this case, shut down the module by using a small, pointed object (such as a paper clip) to access the SHUTDOWN button on the front panel (see Figure 1-1 on page 1-3).

Note The shutdown procedure may require several minutes. The STATUS LED turns off when power to the module is off.

Functional Description

The architecture of the MWAM uses a base module and daughter card arrangement to provide distributed functions. The daughter card contains three processor complexes with two processors on each complex (see Figure 1-2 on page 1-5). Two processor complexes have access to 1 GB of memory and the third has access to 512 MB. The processor complexes are controlled by a processor control complex on the base module. The processor control complex provides module initialization, control, and interface functions and two Gigabit Ethernet links to the daughter card.

Figure 1-2 MWAM Architecture



Processor Complexes

The daughter card has three dual-processor complexes. Each of the processors runs one Cisco IOS application image. Table 1-2 provides the specifications of the MWAM processors and complexes.

Table 1-2 MWAM Processor Matrix

Processor	Complex	Memory Option		Interface Mapping	
1	Processor Control	MEM-MWAM-512MB	MEM-MWAM-1GB[1]	From Processor	From Switch Fabric
2	1	1 Gigabyte	2 Gigabyte	Gi 0/0	Slot x, port 2
3					
4	2	1 Gigabyte	2 Gigabyte	Gi 0/0	Slot x, port 3
5					
6	0	512 Megabyte	1 Gigabyte	Gi 0/0	Slot x, port 1
7[2]					

1. This memory option was introduced with Cisco IOS 12.3(7)T1.
2. Processor 7 is disabled (not used by mobile wireless applications).

For mobile wireless applications, the MWAM runs five instances of the Cisco IOS software simultaneously. Each MWAM has one IOS application image—all processors on the MWAM are loaded with the same image. Mixed applications (for example, PDSN, GGSN, and SSG) on the same MWAM are *not* supported. The Catalyst 6500 chassis and Cisco 7600 chassis can accommodate multiple MWAMs. Therefore, multiple applications could run in the same chassis on different MWAMs.

Memory

As shown in Table 1-2 on page 1-5, each processor complex has a memory allocation that is based on the memory option purchased. Processor complex 0 has only one memory slot instead of two; therefore, processor 7 is disabled. This allows all MWAM processors (2-6) to have the same memory allocation, see "Configuring the MWAM Memory Allocation" section on page 6-17 for details on allocating IO memory.

Bootflash

Each processor complex has bootflash memory that it uses to store IOS configurations, crash information, Read Only Memory for Monitor (ROMMON) images, and variables for both processors. The 8 MB bootflash is partitioned as follows:

- IOS configuration—NVRAM 512 KB for each processor
- Backup configuration—NVRAM 512 KB for each processor (only for local mode operation)
- Crash information region—512 KB for each processor
- ROMMON Variables—64 KB for each processor
- Field-Upgradable ROMMON (FUR) 1 MB
- Standard ROMMON 1 MB

Caution The total disk space for bootflash memory cannot exceed 524,288 bytes. Also, no more than five files can be stored in bootflash memory. Ensure that enough disk space is available for a crash file by keeping no more than four files and using no more than approximately 300 KB of bootflash memory.

Both processors on a processor complex share the same physical bootflash memory. However, each processor has its own partition. If you list the directory of each processor, you observe that even though the processors share the same bootflash memory, the contents of each directory are unique. For example:

```
proc2#dir
Directory of bootflash:/

No files in directory

524288 bytes total (524288 bytes free)
proc2#


proc3#dir
Directory of bootflash:/

0  -rw-        1897   Jun 13 2003 22:25:41  running-config
1  -rw-        1897   Jun 14 2003 03:54:35  running-2

524288 bytes total (520110 bytes free)
```

Note Because the bootflash memory is shared by two processors, simultaneous read and write operations are not allowed. For example, if you issue the **copy running-config** command from MWAM processor 4 and then issue the **dir bootflash:** command from processor 5, the console returns a resource busy message because both processors share the same bootflash memory.

Compact Flash

The compact flash (cf) card is integrated with the processor control complex and is configured with the partitions listed in Table 1-3.

Table 1-3 Compact Flash Partitions[1]

Partition	Size	Description
1	16 MB	Maintenance Partition (boot partition)
2	1 MB	Maintenance Partition
3	7 MB	Maintenance Partition
4	100 MB	Application Partition (extended/boot partition)
5	16 MB	Application Partition (root partition)
6	48 MB	Application Partition (IOS image partition)
7	36 MB	Application Partition (logging/debugging partition)

1. Partitions, sizes, and descriptions listed here are introduced with IOS image 12.3(5a)B. Before this release, only six partitions were configured and sizes for the Application Partition were different from the values listed here.

Gigabit Ethernet Interfaces

Each processor complex shares one Gigabit Ethernet link to the switching fabric on the Catalyst 6500 switch or Cisco 7600 router. Gigabit Ethernet links to the switching fabric perform as 802.1Q trunks. Additional Gigabit Ethernet interfaces provide internal connections between the processor complexes and to the processor control complex.

Each of the three MWAM processor complexes has one Gigabit Ethernet interface (Gi0/0) that maps to the three Gigabit Ethernet interfaces known by the Supervisor module (see Figure 1-2 on page 1-5). Therefore two processors on each processor complex share a single Gigabit Ethernet interface. Each processor interface can be configured with multiple subinterfaces as required by the application.

Software Description

The MWAM requires two software components for its operation:

- Supervisor 2 Cisco IOS image—12.2(14)ZA or higher
- MWAM software

Supervisor 2 IOS Software Image

The first software component is the Cisco IOS image on the Catalyst 6500/Cisco 7600 Supervisor 2 Engine. This image on the Supervisor module recognizes and initializes the MWAM and its processors. You must use a Cisco IOS image that supports the MWAM—12.2(14)ZA or higher.

MWAM Software

The MWAM software resides in the compact flash (cf) card that is integrated with the processor control complex:

- Maintenance Partition (MP)—software required for base module initialization and daughter card control functions (identified as cf:1)
- Application Partition (AP)—the Cisco IOS image for the application (for example, GGSN, PDSN, or SSG) being installed (identified as cf:4)

The MWAM software on the compact flash card can be upgraded by the user through the Supervisor console. The upgrade process downloads the latest versions of the AP and MP images from the Cisco Software Center to the compact flash card.

The standard process involves booting the daughter card from the MP partition, copying the AP image to the compact flash card, then resetting the daughter card to the AP partition. Then, from the AP partition, you copy the MP image to the compact flash card. An inline IOS image upgrade procedure is also provided. See the "Standard Upgrade Procedures" section on page 5-4 of this guide for more information about these procedures.

The application processors (2-6) boot from processor 1. All processors run the same IOS application image.

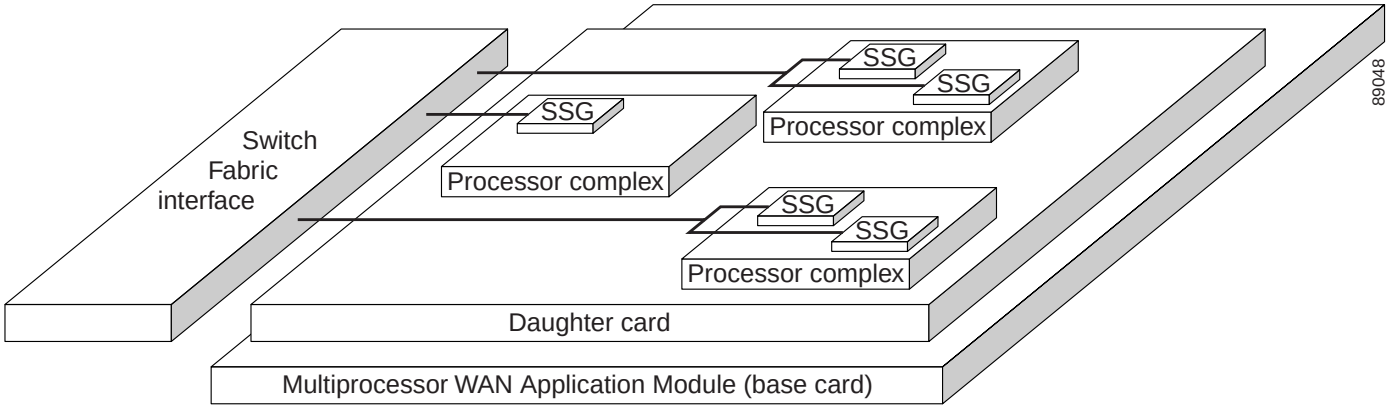
Supported Applications

The MWAM platform is not a generic platform and only the following application images are supported:

- GGSN - **c6svc5fmwam-g8is-mz**
- Home Agent - **c6svc5fmwam-h1is-mz**
- PDSN - **c6svc5fmwam-c6is-mz**
- SSG - **c6svc5fmwam-g4js-mz**

The MWAM architecture allows five mobile wireless applications to reside on a single MWAM. Figure 1-3 on page 1-9 shows an example of five SSGs on one module. Each Catalyst 6500/Cisco 7600 chassis can be populated with multiple MWAMs. Therefore, a chassis with three MWAMs can support 15 SSGs. The MWAM also supports the PDSN/HA and GGSN applications. Three MWAMs in a chassis can support, for example, five PDSNs, five SSGs, and five GGSNs.

Figure 1-3 Example of SSG Application on MWAM



Application Releases

Tip Some of the features and commands described in this publication are provided by the IOS image on the MWAM processors. The features and commands available to your application are dependent on the release level of this IOS image. See the "Features" section on page 1-10 of this chapter and the release notes for your application to determine the availability of specific features and commands.

For release notes and feature module descriptions of the mobile wireless applications that are supported on the MWAM, refer to the Cisco publications at the following URLs:

Cisco Gateway GPRS Support Node (GGSN)

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xb/123xb2/ggsn40/index.htm

Cisco Mobile Wireless Home Agent: (HA)

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zb8/ha12/index.htm

Cisco Packet Data Serving Node (PDSN)

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zb8/pdsn12/index.htm

Cisco Service Selection Gateway (SSG)

http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/prod_release_note09186a00801b43aa.html

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/wan_vcg.htm#1000988

http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guides_list.html

Supervisor Releases

Tip Some of the features and commands described in this publication are provided by the IOS image on the Supervisor 2 module. The features and commands available to your application are dependent on the release level of the Supervisor 2 IOS image. Refer to the "Features" section on page 1-10 of this chapter and the release notes for your application to determine the availability of specific features and commands.

For information about the Supervisor image that supports the mobile wireless applications on the MWAM, refer to the Cisco publication at the following URL:

Supervisor Image That Supports MWAM Applications

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_release_note09186a0080145494.html

Features

Table 1-4 lists the MWAM features:

Table 1-4 MWAM Features and IOS Image Requirements

Feature Description	IOS Image Requirement
Multiple processors on one MWAM running a Cisco IOS software image that supports an application (PDSN/HA, GGSN, or SSG).	Different for each application (check the release notes for the application).
Cisco IOS software image on the MSFC2 (daughter card on the Supervisor module) that supports the application image on the MWAM.	Cisco IOS 12.2(14)ZA or higher.
Bulk storage of MWAM configurations on Supervisor bootflash.	Cisco IOS 12.2(14)ZA5 or higher.
Remote console to MWAM processors 2-6 to: • Unify command operations (debug control, system information display, file listing, and pinging MWAM processors from a single console) • Display output of show and debug commands (through remote VTY) • Direct MWAM logs to console, buffer, or SysLog	Cisco IOS 12.2(14)ZA4 or higher.
Assignment of MWAM traffic to VLAN Quality of Service (QoS)	Cisco IOS 12.2(14)ZA7 or higher.
Remote console support for MWAM processor 1 (processor control).	Cisco IOS 12.3(5a)B or higher.
Persistent log files.	Cisco IOS 12.3(5a)B or higher.
Inline IOS image upgrades	Cisco IOS 12.3(5a)B or higher.
1 Gigabyte memory per processor	Cisco IOS 12.3(7)T1 or higher.
Supervisor mode feature improvement	Cisco IOS 12.3(11)T or higher.

Bulk Storage of MWAM Configurations on Supervisor Bootflash

Note This feature requires Cisco IOS 12.2(14)ZA5 (or higher) on the Supervisor module.

Configuration files for MWAM processors can be stored in either of the following locations:

- NVRAM of each MWAM processor (local mode)
- Supervisor bootflash (Supervisor mode)

Local Mode

The MWAM provides local storage of IOS configurations in NVRAM. However, if a fully configured MWAM requires replacement, you must perform the following tasks:

1. Log into the Supervisor module.
2. Session sequentially into each processor on the MWAM to copy its configurations to a TFTP server.
3. Replace the MWAM.
4. Session sequentially into each processor on the new MWAM to restore the configurations from the TFTP server.

This replacement scenario requires time-consuming intervention by an operator. To reduce operator intervention, you can configure the MWAM to provide Supervisor (bootflash) storage instead of local (NVRAM) storage of configuration files.

Supervisor Mode

Note Feature Improvement. The Supervisor storage mode behavior has been updated (see the "Feature Improvement" section on page 1-13 for details).

The Supervisor storage mode allows MWAM configuration files to be stored in the Supervisor bootflash. This mode allows centralized management of all MWAM configuration files. In the Supervisor mode, when an MWAM is replaced all processors on the MWAM automatically load their configuration files from the Supervisor bootflash. *No* configuration files are contained locally in NVRAM.

The Supervisor module verifies that its bootflash contains a properly named configuration file for each MWAM processor. The following naming convention is used:

`SLOTxPCy.cfg`

The variable *x* represents the MWAM slot number and *y* represents the processor number. For example, SLOT6PC3.cfg is the configuration file for processor 3 on the MWAM in slot 6.

The following example shows the display of MWAM configuration files on the Supervisor module:

```
ce-cat6k-1# dir bootflash:
Directory of bootflash:/

    1  -rw-     1733412   May 28 2002 18:59:10  c6msfc2-boot-mz.121-11b.E
    2  -rw-    11280364   May 28 2002 18:59:22  c6msfc2-psv-mz.121-11b.E.bin
   73  -rw-          42   Jun 24 2003 22:24:31  SLOT4PC7.cfg
   74  -rw-        2876   Jun 24 2003 22:24:32  SLOT6PC2.cfg
   75  -rw-          42   Jun 24 2003 22:24:32  SLOT6PC3.cfg
```

```
 79  -rw-         482   Jun 24 2003 22:24:34  SLOT6PC7.cfg
 85  -rw-        2747   Jul 01 2003 19:56:02  SLOT6PC6.cfg
 86  -rw-         450   Jul 01 2003 19:58:04  SLOT4PC2.cfg
 87  -rw-         450   Jul 01 2003 19:58:47  SLOT4PC3.cfg
 89  -rw-         450   Jul 01 2003 20:02:25  SLOT4PC4.cfg
 90  -rw-         450   Jul 01 2003 20:03:30  SLOT4PC5.cfg
 91  -rw-         450   Jul 01 2003 20:04:13  SLOT4PC6.cfg
107  -rw-         455   Jul 16 2003 11:31:50  SLOT6PC5.cfg
109  -rw-         505   Jul 25 2003 08:43:55  SLOT6PC4.cfg
```

If a standby (slave) Supervisor is installed, the slave bootflash stores backups of the MWAM configuration files that are on the master Supervisor. If a difference is detected between corresponding files on the active and standby Supervisor modules, the file on the bootflash is copied over from the file on the slave bootflash. This compare and copy operation occurs after MWAM replacement or when the active Supervisor module detects that a standby Supervisor module is installed.

When operating in Supervisor mode, the NVRAM on the MWAM does not keep a backup configuration file. Instead, the backup files for MWAM configurations are stored on the standby Supervisor. The following example shows the display of MWAM configuration files on the standby Supervisor module:

```
ce-cat6k-1# dir slavebootflash:
Directory of slavebootflash:/

  1  -rw-     1693168   May 08 2003 02:18:54  c6msfc2-boot-mz.121-8a.EX
  2  -rw-    27411228   May 28 2003 19:39:52  c6k222-jsv-mz.122-14.ZA1.bin
877  -rw-         450   Jul 25 2003 08:26:41  SLOT4PC2.cfg
878  -rw-         450   Jul 25 2003 08:26:42  SLOT4PC3.cfg
879  -rw-         450   Jul 25 2003 08:26:42  SLOT4PC4.cfg
880  -rw-         450   Jul 25 2003 08:26:43  SLOT4PC5.cfg
881  -rw-         450   Jul 25 2003 08:26:44  SLOT4PC6.cfg
882  -rw-          42   Jul 25 2003 08:26:44  SLOT4PC7.cfg
883  -rw-        2876   Jul 25 2003 08:26:45  SLOT6PC2.cfg
884  -rw-          42   Jul 25 2003 08:26:46  SLOT6PC3.cfg
886  -rw-         455   Jul 25 2003 08:26:47  SLOT6PC5.cfg
887  -rw-        2747   Jul 25 2003 08:26:48  SLOT6PC6.cfg
888  -rw-         482   Jul 25 2003 08:26:49  SLOT6PC7.cfg
889  -rw-         505   Jul 25 2003 08:43:36  SLOT6PC4.cfg
```

Caution If a standby Supervisor module is not equipped, copy all MWAM configuration files from the active Supervisor module to a TFTP server. Failure to take this precaution may result in the loss of all MWAM configuration files (if the Supervisor module fails).

Note The Supervisor mode is the default mode of operation for all new MWAMs. To convert an existing MWAM from local mode to Supervisor mode, session to the processor level and issue the **mwam config-mode supervisor** command.

The following commands are provided for storage mode configuration:

- **mwam bootflash access**
- **mwam config-mode** [**local** | **supervisor**]
- **show mwam config-mode**

  See Appendix A, "Command Reference" of this guide for syntax and usage guidelines.

Tip Best operating practice is to configure all MWAMs in a chassis for either local mode or Supervisor mode (no mixing of local-mode and Supervisor-mode MWAMs in the same chassis).

Feature Improvement

The following feature improvement introduces new behavior when operating in the Supervisor mode. This feature improvement is implemented in Cisco IOS 12.3(13)T and later releases.

New Behavior

When operating in the Supervisor mode, the running configuration is written to the following locations when the MWAM image is reloaded:

- Supervisor bootflash on the active Supervisor module
- Supervisor slave bootflash on the standby Supervisor module
- NVRAM on the MWAM (cached copy only)

Previously, the mode of operation (Supervisor or local) was determined by the contents of the configuration file in the NVRAM. If the file was empty (0 bytes long), the mode was set to Supervisor; if the file was not empty, the mode was set to local. With this feature improvement, the mode of operation is now determined by the setting of a persistent flag.

The previous behavior read the configuration file in the Supervisor directly into the running image. Now when a processor is reloaded and the MWAM initializes in Supervisor mode, the configuration file is copied from the Supervisor bootflash to the NVRAM.

Note If the configuration file is completely missing from the Supervisor at the time the processor is reloaded, the cached copy in the NVRAM will remain intact. If there is any configuration file on the Supervisor bootflash and **mwam bootflash access** is on (default), the configuration file will be loaded and will overwrite the cached configuration file in the NVRAM.

Another difference in the behavior of this feature concerns the CLI prompt. Previously, the CLI prompt was displayed before the configuration was downloaded from the Supervisor module. With the improved feature, no prompt is displayed until the configuration completes its download to the NVRAM. If there is a problem with configuration download, the attempt times out in 12 minutes.

See the "Converting to Supervisor Mode" section on page 6-15 for new behavior when converting to the Supervisor mode.

New CLI

On the MWAM console, a new optional keyword is added to the **mwam config-mode** command:

```
mwam config-mode {local|supervisor} [nowrite]
```

Use the **nowrite** option to change the mode without changing the contents of the configuration on the Supervisor (if Supervisor mode) or NVRAM (if local mode).

Note This feature improvement is implemented in Cisco IOS 12.3(13)T and later releases.

A new command is available at the PC console:

boot-mode {**supervisor**|**local**} [*complex*|**all**]

Note This feature improvement is implemented in AP version 2.1(2.0) and later releases.

For more information on these commands, see Appendix A, "Command Reference".

Remote Console for MWAMs

Note The Remote Console and Logging feature requires Cisco IOS 12.2(14)ZA4 (or higher) on the Supervisor module.

The remote console for MWAMs allows operators to use the existing Supervisor console as a single connection point to control debugging, display show commands, and view logging output for MWAM processors 2-6. The remote console has three related components:

- A mechanism for unified command operations from the Supervisor console to MWAM processors in the chassis
- A remote Virtual Terminal Line (VTY) to display the output of show and debug commands
- A remote logging utility to direct logging output from individual MWAM processors to any currently supported logging facility in the chassis (console, buffer, or SysLog)

The User Data Protocol (UDP) transports the remote console commands, VTY output, and logging information. Initially, the traffic flows through the processor control complex, which allows logging information to be relayed to the Supervisor module before the MWAM processors have been configured. When the MWAM processors are configured, the traffic can continue to be transmitted through the processor control complex, or it can be redirected to the switching fabric using a configuration command on the MWAM processor.

Unified Command Operations

The remote console provides a mechanism to execute supported commands on a specified MWAM processor in the chassis. The targeted processor receives the command through a registered UDP port, reassigns its VTY to the remote VTY, and executes the command. When the command operation completes, the VTY is restored.

The supported commands for unified operation from the remote console are listed alphabetically in Table 1-5.

Table 1-5 Unified Command Set

Command	Description
debug	Enables debugging functions
dir	Lists files in a file system
log dir	Logs the dir command to SysLog
log show	Logs the show command to SysLog
log systat	Logs the systat command to SysLog

Table 1-5 Unified Command Set (continued)

Command	Description
mwam	Allows remote execution of **mwam config-mode local** and **mwam config-mode supervisor** commands
ping *ip_address*	Executes a ping on a remote processor
show	Displays running system information
systat	Displays information about terminal lines
undebug	Disables debugging functions

The mechanism for unified command operation is provided in the following command:

execute-on *slot processor command*

The *slot* and *processor* variables represent the MWAM slot and processor numbers. The *command* variable can be any command in the unified command set listed in Table 1-5. Additional syntax and usage guidelines are provided in Appendix A, "Command Reference" of this guide.

Remote Console Support for the Processor Control Complex

This feature is introduced with Cisco IOS release 12.3(5a)B.

Remote console support for the processor control complex allows you to access the processor control complex using the **execute-on** command. With this feature, you can execute processor control commands from the Supervisor console (see the "Processor Control Commands" section on page A-16); you do not have to session down to the processor control complex. To enable remote console support for the processor control complex, configure UDP port 4000 on the Supervisor and the MWAM processor (see the "Configuring Remote Console and Logging" section on page 6-16 of this guide.).

The supported commands for processor control complex unified operation are listed alphabetically in Table 1-6.

Table 1-6 Processor Control Complex Unified Command Set

Command	Description
boot-mode	Set MWAM processors to boot Supervisor or Local configurations
clear	Clears logging information
logout	Logout of shell
normal-ios	Boot IOS with normal configuration
password	Set the password of the current user
recover-ios	Boots IOS with clean configuration
reload	Reloads MWAM processors or complexes
restore ios	Restores previous images following upgrade
show	Displays running system information

The mechanism for unified command operation is provided in the following command:

execute-on *slot processor command*

The *slot* variable represents the MWAM slot and the *processor* variable is always 1 for the processor control complex (see Table 1-2 on page 1-5). The *command* variable can be any command in the processor control complex unified command set listed in Table 1-6 on page 1-15. Additional syntax and usage guidelines are provided in Appendix A, "Command Reference" of this guide.

Show and Debug Display

The remote VTY function directs output from executive level commands to the appropriate console. Commands that are received and processed by the MWAM processor are directed to a remote VTY process on the Supervisor module. The remote VTY process directs the output to the Supervisor level for either:

- Remote display of command output during normal operation
- Logging of show output to capture failure information of an MWAM processor

MWAM Logging to Console, Buffer, or SysLog

The remote logging capability uses logging information from the MWAM logger process. When the MWAM attempts to log an event, the MWAM logger process invokes a list of destinations for the log. If the Supervisor logger is enabled on the MWAM processor, then the log flows through the remote VTY and is processed by the Supervisor. At the Supervisor, the log can be directed to one or more of several destinations including console, buffer, or SysLog.

Logs received by the Supervisor are prefixed with information that identifies which processor generated the log. Examples of log messages follow.

Processor 5 on the MWAM in slot 6 generated the following error message:

```
MWAM 06/5: 00:02:05: %SNMP-5-MODULETRAP: Module 6 [Up] Trap
```

Processor 4 on the MWAM in slot 2 generated the following debug message:

```
MWAM 02/4: 00:03:42: ICMP: echo reply sent, src 10.10.10.2, dst 10.10.10.1
```

Using the Log Option

When using the **execute-on** *slot processor* **log show** command, the volume of logging information can be large. Under these conditions, the console processing can load down the Supervisor CPU.

To prevent overloading the console, two options are available:

1. Configure the logging console feature as follows:

   ```
   no logging console guaranteed
   ```

   This configuration allows the output to be dropped when the console backs up.

2. Configure the logging console debug as follows:

   ```
   no logging console debug
   ```

   This configuration directs the output to other logging endpoints, such as buffer or SysLog.

Note These configurations are only necessary if command output is expected to be significant (for example, more than 100 lines of output).

Example Usage

The following examples illustrate ways you can use the Remote Console and Logging feature to manage MWAM processors from the Supervisor console.

Show Logs for All MWAM Processors

You can display logging information for all MWAM processors in a chassis with a single command from the Supervisor console. First, configure each MWAM processor to locally store logs (in each processor). You can set the buffer logging level on each processor to include the required level of information (the default setting is the debug level). Then you can display logs for all the processors in the chassis by entering the following command from the Supervisor console:

```
Sup-7600# execute-on all all show logging
```

Show Image Version of All MWAM Processors

You can display the software image versions running on all MWAM processors in a chassis with a single command from the Supervisor console. The following example illustrates this capability:

```
Sup-7600# execute-on all all show version

----------- Slot 3/CPU 2, show ver-------------
Cisco Internetwork Operating System Software
IOS (tm) MWAM Software (MWAM-G7IS-M), Experimental Version
12.3(20031015:202420) [GGSN_R3_R4_1015_1 103]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 15-Oct-03 15:53 by tester
Image text-base:0x20200D40, data-base:0x21168000

ROM:System Bootstrap, Version 12.2(11r)YS1, RELEASE SOFTWARE (fc1)

Router uptime is 2 days, 23 hours, 52 minutes
System returned to ROM by power-on
System restarted at 01:09:42 UTC Tue Oct 21 2003
System image file is "svcmwam-g7is-mz.r3_r4-1015"

Cisco MWAM (MWAM) processor with 473088K/32768K bytes of memory.
SB-1 CPU at 700Mhz, Implementation 1, Rev 0.2

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
1 Gigabit Ethernet/IEEE 802.3 interface(s)
511K bytes of non-volatile configuration memory.

Configuration register is 0x0


----------- Slot 3/CPU 3, show ver-------------
Cisco Internetwork Operating System Software
IOS (tm) MWAM Software (MWAM-G7IS-M), Experimental Version
12.3(20031015:202420) [howang-GGSN_R3_R4_1015_1 103]
Copyright (c) 1986-2003 by cisco Systems, Inc.
```

```
Compiled Wed 15-Oct-03 15:53 by howang
Image text-base:0x20200D40, data-base:0x21168000

ROM:System Bootstrap, Version 12.2(11r)YS1, RELEASE SOFTWARE (fc1)

Router uptime is 2 days, 23 hours, 52 minutes
System returned to ROM by power-on
System restarted at 01:10:19 UTC Tue Oct 21 2003
System image file is "svcmwam-g7is-mz.r3_r4-1015"

Cisco MWAM (MWAM) processor with 473088K/32768K bytes of memory.
SB-1 CPU at 700Mhz, Implementation 1, Rev 0.2

Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
1 Gigabit Ethernet/IEEE 802.3 interface(s)
511K bytes of non-volatile configuration memory.

Configuration register is 0x0
```

Tip To minimize the command output, you can use the pipe (|) support to include only lines of text that match the regular expression following the pipe. For example:

```
Sup-7600# execute-on all all show version | include image
```

Persistent Log Files

This feature was introduced with Cisco IOS release 12.3(5a)B.

Logs are stored on the processor control complex. These logs can be used to help diagnose system failures.

Inline IOS Image Upgrades from AP

This feature was introduced with Cisco IOS release 12.3(5a)B.

The "Inline IOS Image Upgrade Procedure" section on page 5-8 is similar to the AP upgrade in that both procedures upgrade the image used by the application. However, the inline IOS image upgrade is performed from the AP, not the MP; therefore, you do not have to reset the module. This significantly reduces the amount of down time associated with module resets.

Note After performing the inline IOS image upgrade, you must reload the MWAM processor(s).

AP 2.1(2.0) Unsolicted SCP Message

The latest version of AP 2.1(2.0) now sends an unsolicited SCP message to the Supervisor indicating that it supports SSO (stateful switchover). If you are running an older Supervisor image which does not recognize this message, then you will get the "unsolicited message" indicator. Ignore this message as it does not mean anything.

CHAPTER 2

Preparing to Install the MWAM

This chapter provides information about preparing your site for installation. It includes the following sections:

Safety Guidelines

Before you begin the installation of the MWAM, review the safety guidelines in this chapter to avoid injuring yourself or damaging the MWAM.

Follow the "Safety Recommendations" section on page 3-2 for specific safety information when installing the MWAM in a Catalyst 6500/Cisco 7600 chassis.

In addition, before replacing, configuring, or maintaining the MWAM, review the safety warnings listed in the document *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches and Cisco 7600 Series Routers* that you plan to install the MWAM into.

Caution The MWAM does *NOT* support hot swapping. The MWAM must be shutdown first before removal (see the "MWAM Shutdown" section on page 1-4). All other modules, including the Supervisor Engine 2 (if you have redundant Supervisor Engine 2 modules), support hot swapping. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down. For more information about hot-swapping modules, refer to the *Catalyst 6500 Series Module Installation and Configuration Documentation*.

Safety with Equipment

The following guidelines will help ensure your safety and protect the equipment. This list is not all-inclusive of all potentially hazardous situations, so be *alert*.

Warning **Read the installation instructions before connecting the system to the power source.** Statement 1004

- Always disconnect all power cords and interface cables before moving the system.
- Never assume that power is disconnected from a circuit; *always* check.
- Keep the chassis area clear and dust-free during, before, and after installation.
- Keep tools and assembly components away from walk areas where you or others could fall over them.
- Do not work alone if potentially hazardous conditions exist.
- 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.
- Do not wear loose clothing that may get caught in the chassis.
- Wear safety glasses when working under conditions that may be hazardous to your eyes.

Safety with Electricity

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit.** Statement 1003

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.** Statement 12

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Follow these guidelines when working on equipment powered by electricity:

- Locate the room's emergency power-off switch. Then, if an electrical accident occurs, you can quickly turn off the power.
- Before working on the system, turn off the DC main circuit breaker and disconnect the power terminal block cable.
- Disconnect all power before doing the following:
  - Working on or near power supplies
  - Installing or removing a router chassis or network processor module
  - Performing most hardware upgrades
- Never install equipment that appears damaged.
- Carefully examine your work area for possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Never assume that power is disconnected from a circuit; *always* check.
- Never perform any action that creates a potential hazard to people or makes the equipment unsafe.
- If an electrical accident occurs, proceed as follows:
  - Use caution, and do not become a victim yourself.
  - Turn off power to the router.
  - If possible, send another person to get medical aid. Otherwise, determine the condition of the victim, and then call for help.
  - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.

In addition, use the following guidelines when working with any equipment that is disconnected from a power source, but still connected to telephone wiring or network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for it.

- Never touch un-insulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. ESD can occur when electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow ESD prevention procedures when removing and replacing modules:

- Ensure that the router chassis is electrically connected to earth ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching a metal part of the chassis.

Caution For the safety of your equipment, periodically check the resistance value of the antistatic wrist strap. It should be between 1 and 10 Mohm.

Before You Begin

Before you install the MWAM:

- Determine the system requirements for the MWAM including hardware, software, and environmental
- Prepare the site (site requirements) and review the installation plans or method of procedures (MOPs)
- Unpack and inspect the MWAM
- Gather tools and test equipment required to properly install the MWAM

System Requirements

Before you install the MWAM into the Catalyst 6500/Cisco 7600 chassis, make sure that the switch meets the hardware, software, and environmental requirements.

Hardware Requirements

Before you can use the MWAM, you must have a Supervisor Engine 2 with a Multilayer Switch Feature Card 2 (MSFC2) and any module that has ports to connect server and client networks.

Software Requirements

To use the MWAM, you must have a Cisco IOS software image on the Supervisor Engine 2 that supports an application software image on the MWAM. You can use the Cisco Feature Navigator to assist you in selecting the appropriate Cisco IOS software. Cisco Feature Navigator is a web-based application that allows you to quickly match Cisco IOS Software releases to features to hardware.

The software requirements for specific applications implemented on the MWAM are contained in application release notes. See the following URLs for available releases:

GGSN Requirements

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/cat6000/1232xb6k.htm

PDSN/HA Requirements

http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_release_note09186a00801245b3.html

SSG Requirements

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/mwam/index.htm

Environmental Requirements

Table 2-1 lists the environmental requirements for the MWAM.

Table 2-1 Environmental Requirements

Item	Specification
Temperature, ambient operating	0° to 40°C (32° to 104°F)
Temperature, ambient nonoperating	–40° to 70°C (–40° to 158°F)
Relative humidity, ambient (noncondensing) operating	10% to 90%
Relative humidity, ambient (noncondensing) nonoperating	5% to 95%

Site Requirements

Typically, you should have prepared the installation site beforehand. As described previously, part of your preparation includes reviewing installation plans or MOPs. An example of a MOP (pre-installation checklist of tasks and considerations that needs to be addressed and agreed upon before proceeding with the installation) is as follows:

Note The example assumes that you are installing the Catalyst 6500/Cisco 7600 chassis as well as the MWAM at the same time. However, the example MOP can be simplified to accommodate just the MWAM.

1. Assign personnel.
2. Determine protection requirements for personnel, equipment, and tools.
3. Evaluate potential hazards that may affect service (Catalyst 6500/Cisco 7600 chassis).
4. Schedule time for installation.
5. Determine any space requirements (Catalyst 6500/Cisco 7600 chassis).

6. Determine any power requirements (Catalyst 6500/Cisco 7600 chassis).
7. Identify any required procedures or tests.
8. On an equipment plan, make a preliminary decision that locates each MWAM that you plan to install.
9. Read this *user guide*.
10. Modify the preliminary plan, if necessary.
11. Verify the list of replaceable parts for installation (screws, bolts, washers, and so on) so that the parts are identified (Catalyst 6500/Cisco 7600 chassis).
12. Check the required tools list to make sure the necessary tools and test equipment are available (see the following Required Tools section).
13. Perform installation.

Unpacking and Checking the Contents of your Shipment

The shipping package for the MWAM is designed to reduce the possibility of product damage associated with routine material handling experienced during shipment. To reduce the potential damage to the product, transport the MWAM in its Cisco-specified packaging. Failure to do so may result in damage to the MWAM. Also do not remove the MWAM from its shipping container until you are ready to install it.

Note Do not discard the packaging materials used in shipping your MWAM. You will need the packaging materials in the future if you move or ship your MWAM.

Required Tools

This following tools are needed to install the MWAM.

Warning **Only trained and qualified personnel should install, replace, or service this equipment.** Statement 1030

Note Before installing the MWAM, you must install the Catalyst 6500/Cisco 7600 chassis and at least one Supervisor Engine 2. For information on installing the switch chassis (see the "Related Documentation" section on page xviii).

These tools are required to install the MWAM into the Catalyst 6500/Cisco 7600 chassis:

- Flat-blade screwdriver
- Phillips-head screwdriver
- Wrist strap or other grounding device
- Antistatic mat or antistatic foam

CHAPTER 3

Installing the MWAM

This chapter provides information about installing the MWAM in a Catalyst 6500/Cisco 7600 chassis and includes the following topics:

Safety Recommendations

As described in the "Safety Warnings" section on page xiii, safety warnings appear throughout this *user guide* in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each warning statement (see the "Safety Guidelines" section on page 2-2 for general safety information for installing your MWAM in a Catalyst 6500/Cisco 7600 chassis).

The following safety recommendations are specific to your MWAM installation.

Warning **Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.** Statement 200

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 181

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

MWAM Installation

This section describes how to install the MWAM into a Catalyst 6500/Cisco 7600 chassis.

Note The MWAM does *NOT* support hot swapping. The MWAM must be shutdown first before removal (see the "MWAM Shutdown" section on page 1-4). All other modules, including the Supervisor Engine 2 (if you have redundant Supervisor Engine 2 modules), support hot swapping. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down. For more information about hot-swapping modules, refer to the *Catalyst 6500 Series Module Installation and Configuration Documentation*.

Caution To prevent ESD damage, handle modules by the module edges only.

To install the MWAM into a Catalyst 6500/Cisco 7600 chassis, perform these steps:

Step 1 Choose a slot for the module.

Step 2 Verify that there is enough clearance to accommodate any interface equipment that you will connect directly to the module ports. If possible, place modules between empty slots that contain only module filler plates.

Step 3 Verify that the captive installation screws are tightened on all modules installed in the chassis.

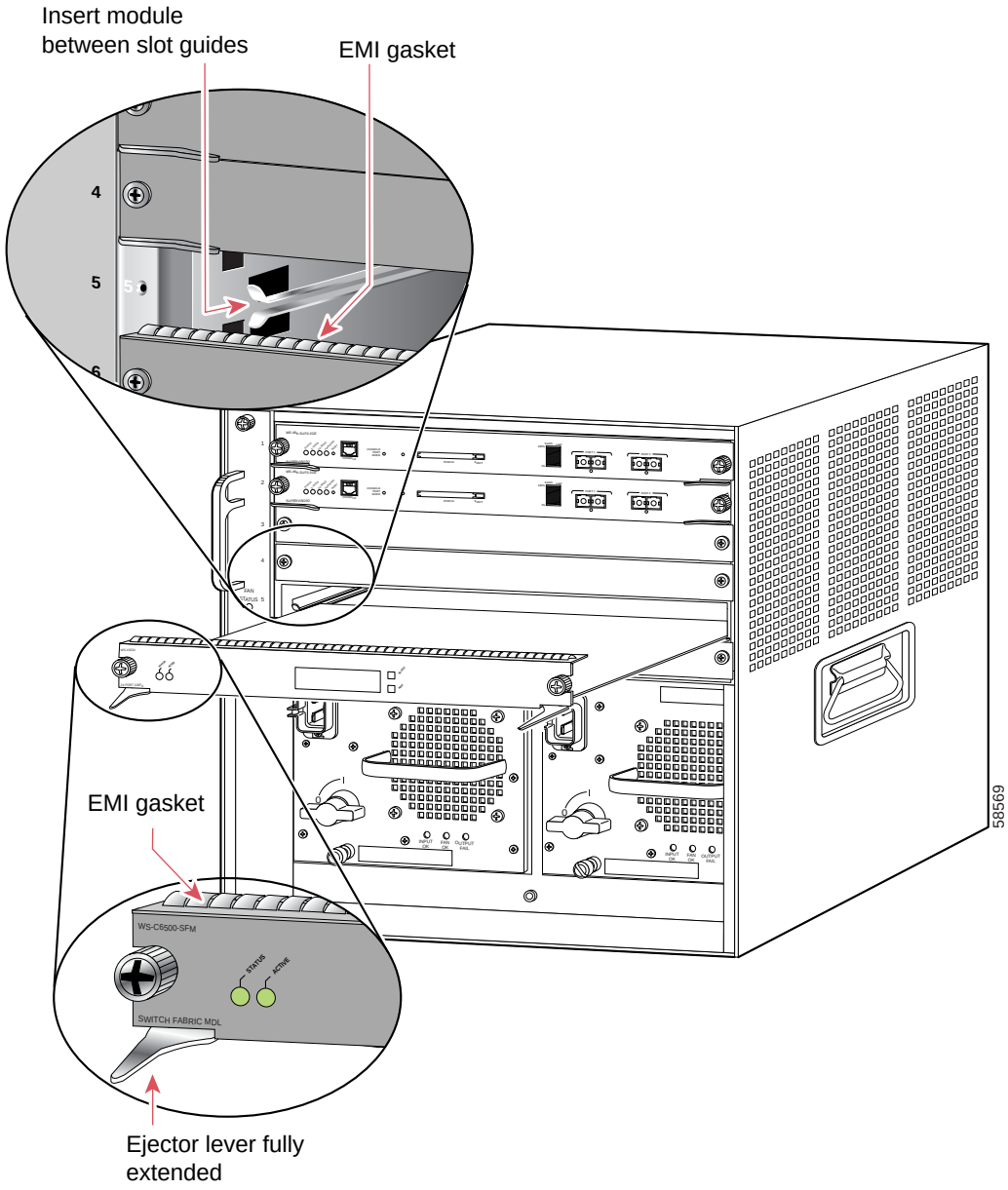
This action ensures that the EMI gaskets on all modules are fully compressed in order to maximize the opening space for the new module or the replacement module.

Note If the captive installation screws are loose, the EMI gaskets on the installed modules will push adjacent modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 4 Remove the module filler plate by removing the two screws from the filler plate. To remove a module, see the "MWAM Removal" section on page 3-10.

Step 5 Fully open both ejector levers on the new or replacement module (see Figure 3-1 on page 3-4).

Figure 3-1 Example of Positioning the Module in a Horizontal Slot Chassis



Step 6 Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of the following sets of substeps:

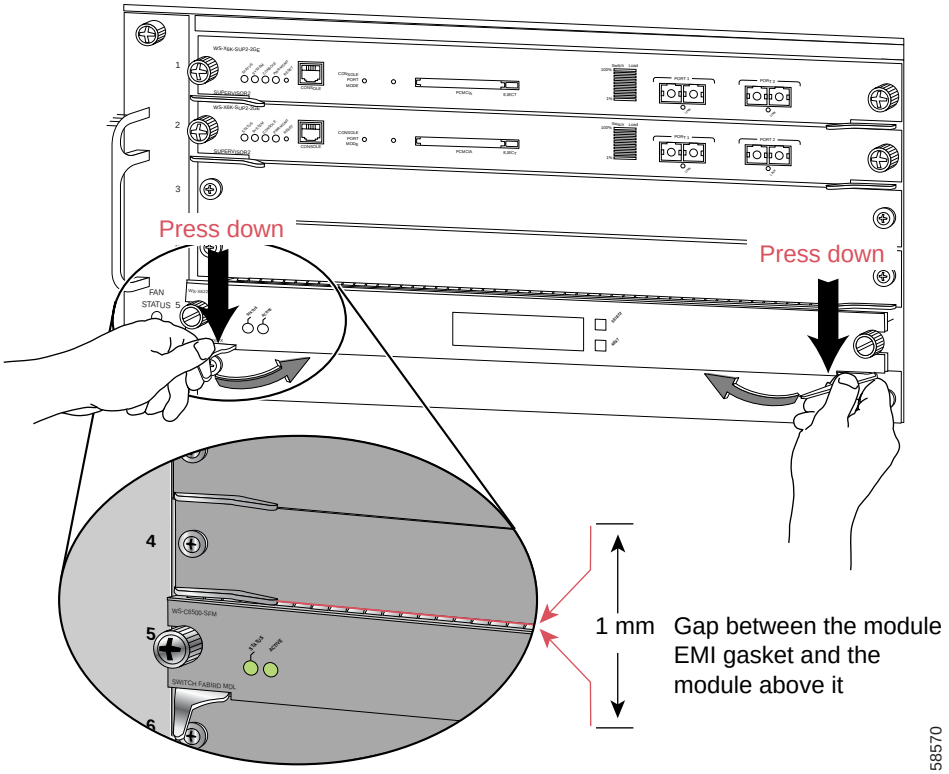
Caution Use grounding wrist straps connected to a captive installation screw on an installed module or power supply when inserting a module. At all other times (shipping, storage, and so on) keep the modules in their anti-static protective bags.

Horizontal slots

a. Position the module in the slot (see Figure 3-1). Make sure that you align the sides of the module carrier with the slot guides on each side of the slot.

b. Carefully slide the module into the slot until the EMI gasket along the top edge of the module makes contact with the module in the slot above it and both ejector levers have closed to approximately 45 degrees with respect to the module faceplate (see Figure 3-2).

Figure 3-2 Example of Clearing the EMI Gasket in a Horizontal Slot Chassis

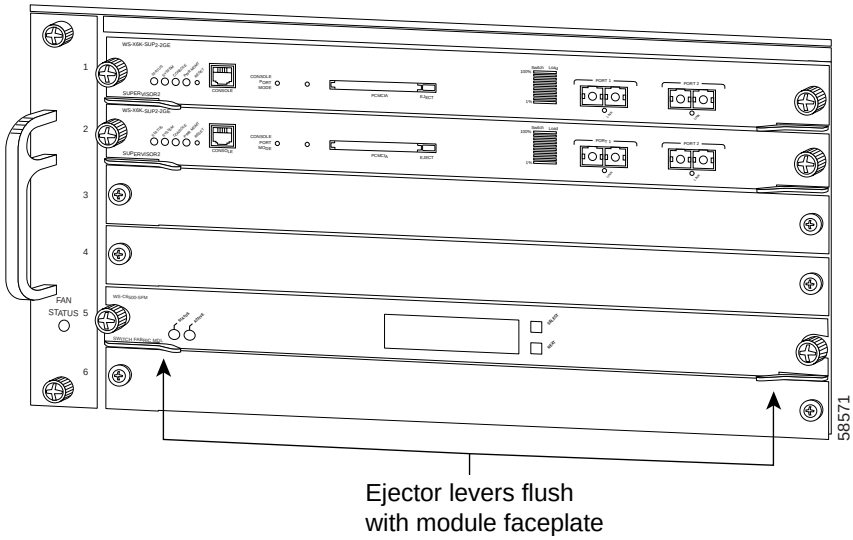


c. Using the thumb and forefinger of each hand, grasp the two ejector levers and press down to create a small (0.040 inch [1 mm]) gap between the module's EMI gasket and the module above it (see Figure 3-2).

Caution Do not press down too hard on the levers. They will bend and become damaged.

d. While pressing down, simultaneously close the left and right ejector levers to fully seat the module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate (see Figure 3-3 on page 3-6).

Figure 3-3 Example of Ejector Lever Closure in a Horizontal Slot Chassis



Note Failure to fully seat the module in the backplane connector can result in error messages.

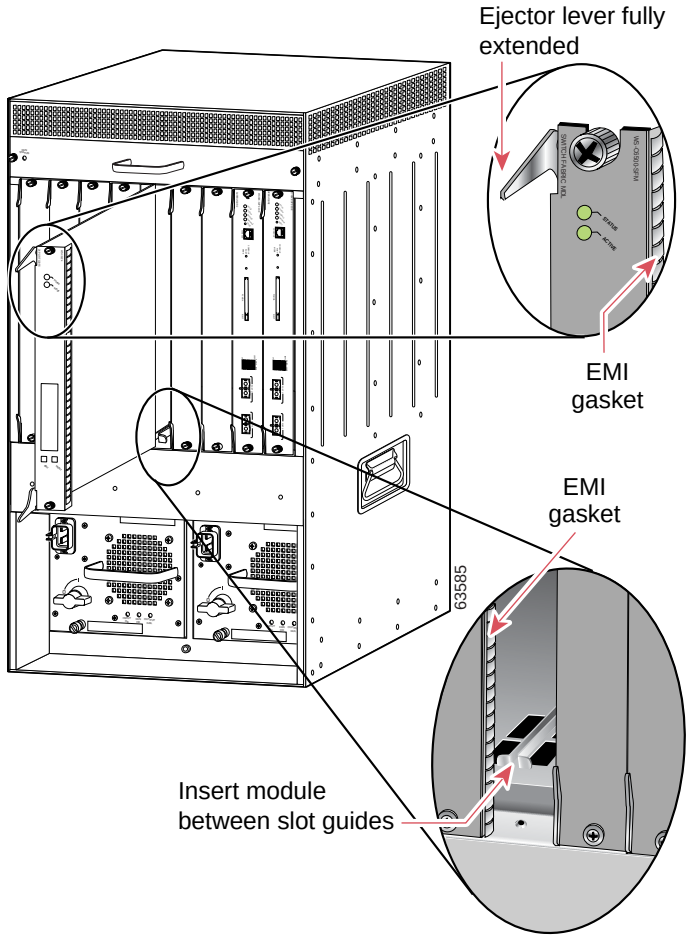
Caution Make sure the ejector levers are fully closed before tightening the captive installation screws.

e. Tighten the two captive installation screws on the module.

Vertical slots

a. Position the module in the slot (see Figure 3-4 on page 3-7). Make sure that you align the sides of the module carrier with the slot guides on the top and bottom of the slot.

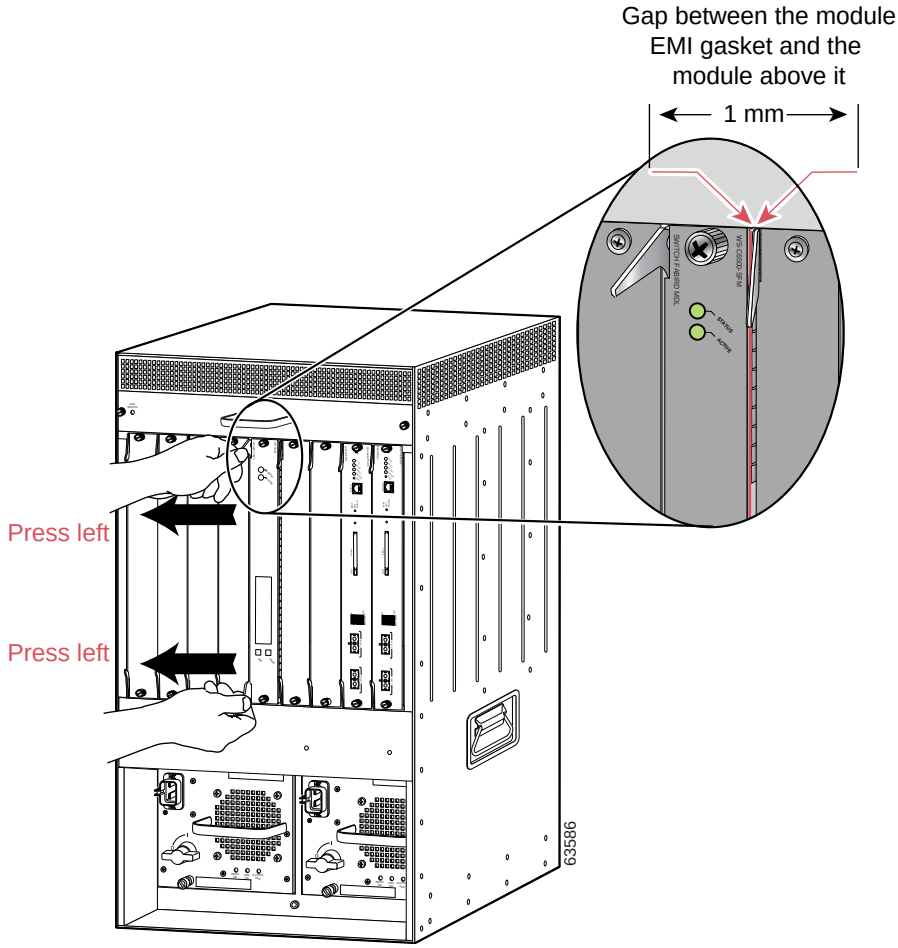
Figure 3-4 Example of Positioning the Module in a Vertical Slot Chassis



b. Carefully slide the module into the slot until the EMI gasket along the right edge of the module makes contact with the module in the slot adjacent to it and both ejector levers have closed to approximately 45 degrees with respect to the module faceplate (see Figure 3-5 on page 3-8).

c. Using the thumb and forefinger of each hand, grasp the two ejector levers and exert a slight amount of pressure to the left, deflecting the module approximately 0.040 inches (1 mm) to create a small gap between the module's EMI gasket and the module adjacent to it (see Figure 3-5 on page 3-8).

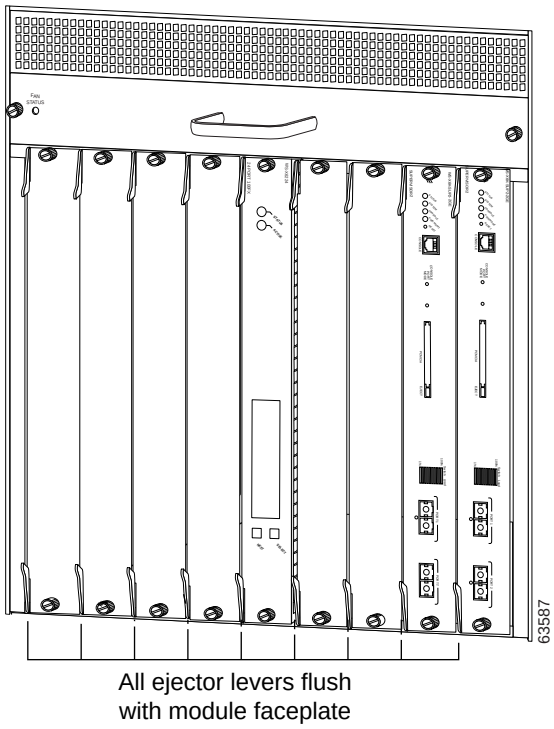
Figure 3-5 Example of Clearing the EMI Gasket in a Vertical Slot Chassis



Caution Do not exert too much pressure on the ejector levers. They will bend and become damaged.

d. While pressing on the ejector levers, simultaneously close them to fully seat the module in the backplane connector. The ejector levers are fully closed when they are flush with the module faceplate (see Figure 3-6 on page 3-9).

Figure 3-6 Example of Ejector Lever Closure in a Vertical Slot Chassis



Caution Make sure the ejector levers are fully closed before tightening the captive installation screws.

e. Tighten the two captive installation screws on the module.

This completes the MWAM installation procedure.

Verifying the Installation

When you install the MWAM into a Catalyst 6500/Cisco 7600 chassis, the module goes through a boot sequence that usually requires no intervention. At the successful conclusion of the boot sequence, the STATUS LED will show green and remain on. If the STATUS LED does not show green, or shows a different color, see Table 1-1 on page 1-3 to determine the module status.

Caution If the following message displays on the console after the boot sequence, you have installed an MWAM that does not have an application image. Go to the "Upgrading AP and MP Images" section on page 5-3, to bring the module on line.

```
*May  5 18:03:35.839:SP:oir_disable_notice:slot6:lcp failed to go online
```

MWAM Removal

This section describes how to remove the MWAM from a Catalyst 6500/Cisco 7600 chassis.

Caution The MWAM is *NOT* hot-swappable. Do *NOT* remove the MWAM from the chassis until the module has shut down completely and the STATUS LED is orange or off (see Table 1-1 on page 1-3 for description of the STATUS LED). You can damage the module if you remove it from the chassis before it completely shuts down (see the "MWAM Shutdown" section on page 1-4 for more information).

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the module. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 181

Warning **Before you install, operate, or service the system, read the *Site Preparation and Safety Guide*. This guide contains important safety information you should know before working with the system.** Statement 200

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

To remove the MWAM, perform these steps:

Step 1 Shut down the module using the following commands:

a. Enter the **show module** command and verify the MWAM status is `OK`.

b. Shut down the module with the **hw-module module** *mod* **shutdown** command in privileged mode. (If you enter this command to shut down the module, you can restart the module later by entering the **hw-module module** *mod* **reset** command.)

c. Enter the **show module** command and verify the MWAM status is `ShutDown` and the STATUS LED is orange.

d. If the module does not respond to any commands, use a small pointed object to access the SHUTDOWN button, which is located on the front panel of the module.

Note Shutdown may require several minutes.

Step 2 Verify that the MWAM shuts down. Do not remove the module from the switch until the STATUS LED is off or orange.

Step 3 Verify that the captive installation screws on all of the modules in the chassis are tight.

This step assures that the space created by the removed module is maintained.

Note If the captive installation screws are loose, the electromagnetic interference (EMI) gaskets on the installed modules will push the modules toward the open slot, reducing the opening size and making it difficult to install the replacement module.

Step 4 Loosen the two captive installation screws on the module.

Step 5 Depending on the orientation of the slots in the chassis (horizontal or vertical), perform one of the following set of substeps:

Caution Use grounding wrist straps connected to a captive installation screw on an installed module or power supply when removing a module. At all other times (shipping, storage, and so on) keep the modules in their static-shielding protective bags.

Horizontal slots

a. Place your thumbs on the left and right ejector levers, and simultaneously rotate the levers outward to unseat the module from the backplane connector.

b. Grasp the front edge of the module and slide the module part all the way out of the slot. Place your other hand under the module to support the weight of the module. Do not touch the module circuitry.

Vertical slots

a. Place your thumbs on the ejector levers located at the top and bottom of the module, and simultaneously rotate the levers outward to unseat the module from the backplane connector.

b. Grasp the edges of the module, and slide the module straight out of the slot. Do not touch the module circuitry.

Step 6 Place the module on an antistatic mat or antistatic foam, or immediately reinstall it in another slot.

Warning **Blank faceplates (filler panels) serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards and faceplates are in place.** Statement 1051

Step 7 If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the chassis.

CHAPTER 4

Command-Line Interface (CLI) Basics

This chapter is intended as a quick reference, not as a step-by-step explanation of the Cisco IOS.

The chapter describes basic Cisco IOS software command-line interfaces that you may need to know before you load/upgrade the MWAM application image (see Chapter 5, "Loading the MWAM") and configure the MWAM (see Chapter 6, "Configuring the MWAM").

Note The MWAM configuration requires two command-line interface interactions: CLI on the Supervisor console and session CLI to each MWAM processor (see Chapter 6, "Configuring the MWAM").

This chapter includes the following topics:

If you have never used the Cisco IOS software or need a refresher, take a few minutes to read this chapter before you proceed to the next chapter. Understanding these concepts will save you time as you begin to use the CLI.

If you are already familiar with the Cisco IOS software, proceed to Chapter 5, "Loading the MWAM".

Note For specific Catalyst 6500/Cisco 7600 Cisco IOS CLI and Cisco IOS command modes, see Chapter 2, "Command Line Interfaces," in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*.

Getting Help

Use the question mark (?) and arrow keys to help you enter commands:

- For a list of available commands, enter a question mark:

```
Router> ?
```

- To complete a command (see the "Command-Line Completion" section on page 4-4), enter a few known characters followed by a question mark (with no space):

```
Router> s?
```

- For a list of command variables, enter the command followed by a space and a question mark:

```
Router> show ?
```

- To re-display a command you previously entered, press the up arrow key. You can continue to press the up arrow key for more commands.

Note The word "Router" is replaced with your router's hostname if the hostname is already configured.

Understanding Command Modes

There are two primary modes of operation within the Cisco IOS: user EXEC mode and privileged EXEC mode. When you first connect to the router, you are placed in the user EXEC mode.

The show commands in the user EXEC mode are limited to a few basic levels. You cannot edit or view configurations at this stage; you can only view the router status and other miscellaneous information.

Editing the router's configuration requires you to be in the privileged EXEC mode. Use the **enable** command to enter this mode (see Table 4-1 on page 4-3).

You can always tell whether you are in user EXEC mode or privileged EXEC mode by looking at the router prompt being displayed. The user EXEC mode has a > at the end; the privileged EXEC mode prompt always has a # at the end.

In the privileged EXEC mode, the user interface is further divided into different submodes. Each command mode permits you to configure different components on your router. The commands available at any given time depend on which mode you are currently in. Entering a question mark (**?**) at the prompt displays a list of commands available for each command mode (see Table 4-1 on page 4-3).

Tip If you are familiar with UNIX, you can equate privileged EXEC mode to "root" access. You could also equate it to the administer level in Windows 2000/NT. In this mode, you have permission to access everything inside the router, including configuration commands. However, you cannot type configuration commands directly. Before you can change the router's actual configuration, you must enter the global configuration mode of the privileged EXEC mode by giving the command **configure terminal** (see Table 4-1 on page 4-3).

Table 4-1 Common Command Modes

Command Mode	Access Method	Router Prompt Displayed	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Router#`	To exit to user EXEC mode, use the **disable**, **exit**, or **logout** command.
Global configuration	From the privileged EXEC mode, enter the **configure terminal** command.	`Router(config)#`	To exit to privileged EXEC mode, use the **exit** or **end** command, or press **Ctrl-z**.
Interface configuration	From the global configuration mode, enter the **interface** *type number* command, such as **interface serial 0/0**.	`Router(config-if)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, press **Ctrl-z**.

Timesaver Each command mode restricts you to a subset of commands. If you are having trouble entering a command, check the prompt, and enter the question mark (**?**) for a list of available commands. You might be in the wrong command mode or using the wrong syntax.

In the following example, notice how the prompt changes after each command to indicate a new command mode:

```
Router> enable
Password: <enable password>
Router# configure terminal
Enter configuration commands one per line. End with CNTL/Z.
Router (config)# interface gigabitEthernet 0/0
Router (config-if)# no shutdown
Router (config-if)# exit
Router (config)# exit
Router# DEC 24 07:16:15:079 %SYS-5-CONFIG_I: Configured from console by console
```

The last message is normal and does not indicate an error. Press **Return** to get the `Router#` prompt.

Note You can press **Ctrl-z** in any mode to immediately return to the privileged EXEC mode (`Router#`), instead of entering **exit**, which returns you to the previous mode.

Command-Line Completion

Command-line completion makes the Cisco IOS interface much more user-friendly. It saves you extra keystrokes and helps out when you cannot remember a command's syntax.

In the following example, notice how the command **configure terminal** is done:

```
Router> enable
Password: <enable password>
Router# config t
Router (config)#
```

The Cisco IOS expands the command **config t** to **configure terminal**.

Another form of command-line completion is the use of the Tab key. If you start a command by entering the first few characters, you can press the Tab key. As long as there is only one match, the Cisco IOS will complete the command: for example, if you key in **sh** and press Tab, the Cisco IOS completes the **sh** with **show**. If the Cisco IOS does not complete the command, you can enter a few more letters and try again.

Undoing a Command or Feature

If you want to undo a command you entered or disable a feature, enter the keyword **no** before most commands; for example, **no ip routing**.

Saving Configuration Changes

You need to enter the **copy running-config startup-config** command to save your configuration changes to nonvolatile random-access memory (NVRAM), so the changes are not lost if there is a system reload or power outage. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration to NVRAM. After the configuration has been saved, the following appears:

```
[OK]
Router#
```

Where to Go Next

Now that you have learned some Cisco IOS software basics, you can begin to configure the MWAM using the CLI.

Remember that:

- You can use the question mark (**?**) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you have difficulty entering a command, check the prompt and then enter the question mark (**?**) for a list of available commands. You might be in the wrong command mode or using the wrong syntax.
- To disable a feature, enter the keyword **no** before the command; for example, **no ip routing**.
- You need to save your configuration changes to NVRAM so the changes are not lost if there is a system reload or power outage.

Proceed to Chapter 5, "Loading the MWAM" to begin configuring the MWAM.

CHAPTER 5

Loading the MWAM

Note Typically, the MWAM is already pre-loaded with the necessary images.

This chapter describes the procedures required to load/upgrade the MWAM to the latest version of the MWAM image:

Supervisor Image Pre-requisite

The Supervisor Engine 2 must have a Cisco IOS image [Cisco IOS 12.2(14)ZA or higher] that supports the application image on the MWAM. The latest image is available from the Cisco Software Center at:

http://www.cisco.com/cgi-bin/tablebuild.pl/ssg

For more information on the Supervisor Engine 2 for the MWAM, refer to the following publications:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/

MWAM Images

As described earlier in the "MWAM Ordering Information" section on page 1-2, the MWAM comes from manufacturing in one of two product types:

- WS-SVC-MWAM-1—Pre-loaded with an application image (no loading is necessary unless you want to load a later version of the application software). Two options are available:
  - MEM-MWAM-512MB—Standard option for 512 MB memory per MWAM processor
  - MEM-MWAM-1GB—Option for 1 GB memory per MWAM processor
- SC-SVC-NAP-1.0—No application (NOAP) image (application image must be loaded)

Image Loading Process

Perform the following procedure if you have a NOAP MWAM or if you want to upgrade your MWAM images to a later version.

Note The NOAP MWAM is not operational until you download an AP image from the Cisco Software Center.

Note The pre-loaded MWAM already has the necessary images; therefore, the download procedure is required *only* when you want to upgrade the images to a later version.

The image loading process requires the following basic steps:

1. Boot the MWAM from the MP.
2. Copy the AP image to the compact flash (cf) card.
3. Reset the MWAM to the AP (to load the application image).
4. Copy the MP image to the compact flash card.

The image upgrade process loads the application image onto the three MWAM processor complexes.

Upgrading AP and MP Images

The compact flash on the MWAM has two bootable partitions: application partition (AP) and maintenance partition (MP). By default, the application partition boots every time. The application partition contains the binaries necessary to run the MWAM. The maintenance partition is booted if you need to upgrade the application partition.

You can upgrade both the application software and the maintenance software. However, you are not required to upgrade both images at the same time.

The entire application and maintenance partitions are stored on the FTP or TFTP server. The images are downloaded and extracted to the application partition or maintenance partition depending on which image is being upgraded.

To upgrade the application partition, change the boot sequence to boot the module from the maintenance partition. To upgrade the maintenance partition, change the boot sequence to boot the module from the application partition. Set the boot sequence for the module using the supervisor engine CLI commands. The maintenance partition downloads and installs the application image. The supervisor engine must be executing the run-time image to provide network access to the maintenance partition.

Before starting the upgrade process, you will need to download the application partition image or maintenance partition image from the TFTP server.

Note An AP upgrade will always upgrade an IOS image, whether it is a different version or not. However a ROMMON image will only be upgraded using **upgrade rom-monitor** command from the IOS login (**copy ... <slot>-fs:** command only updates the ROMMON image stored in the compactflash which is just an idle copy. It must be again copied to bootflash which is actually used by the processors using additional upgrade commands). For example: a GGSN MWAM image bundle like **c6svc6fmwam-g8is-mz.12.3(14)T** is made up of three components:

a.) Linux image running on processor 1. Version 2.1(2.0)

b.) IOS image running on processors 2 and above. Version 12.3(14)T

c.) ROMMON image for processors 2 and above. Version 12.2(11)YS2.

Whenever any of the 3 components change, the version of the image bundle will be different. When you copy an image bundle using **copy .. <slot>-fs:** it will overwrite all these 3 images on the compact flash of the MWAM. Both the Linux image and the IOS image are stored in compact flash and; so, the previous images are overwritten. After a following reset, the images from the new bundle will be used to boot the MWAM. However, the ROMMON is actually available in two places — compact flash and bootflash. The bootflash version is the one used by the processor and can be upgraded only by executing an explicit upgrade **rom-monitor** command. Even though we have a ROMMON image in every bundle, it is rarely changed. For example, the last ROMMON release was in 3/2004 along with AP-2.1(1.0). The same ROMMON has been used with all later image bundles.

NOAP MWAM Upgrade Procedure

The MWAM automatically attempts to boot to the AP when it is initially installed. However, if the card is a NOAP MWAM, it will fail the boot attempt because no application image is loaded. In this case, a message similar to the following is displayed on the console:

```
*May  5 18:03:35.839:SP:oir_disable_notice:slot6:lcp failed to go online
```

To bring the NOAP MWAM back on line, perform the following procedure.

	Command	Purpose
Step 1	`Router# configure terminal`	Enters the configuration mode.
Step 2	`Router(config)# no power enable module slot_number`	Disables power on the MWAM.
Step 3	`Router(config)# boot device module slot_number cf:1`	Forces the MWAM to boot to the maintenance partition (MP) at the next power on.
Step 4	`Router(config)# power enable module slot_number`	Enables power on the MWAM, which then boots to the MP.
Step 5	`Router(config)# no boot device module slot_number cf:1`	Enables the MWAM to boot to the default partition (AP) at the next boot cycle.

The NOAP MWAM can now be loaded using the "Standard Upgrade Procedures" that follow.

Standard Upgrade Procedures

The standard upgrade procedures available for the MWAM are listed in Table 5-1.

Table 5-1 Standard Upgrade Procedures

Upgrade Procedure	Description
AP Upgrade Procedure, page 5-5	Upgrades an application image to the latest available version. This procedure is performed from the MP and requires resetting the module.
MP Upgrade Procedure, page 5-7	Rarely used, this procedure upgrades the maintenance partition. Use this procedure only when instructed.
Inline IOS Image Upgrade Procedure, page 5-8	Uses an IOS-only image to upgrade an application. This procedure is performed from the AP and significantly reduces the down time associated with module resets. It is also called the fast upgrade procedure.

AP and MP Upgrades

The AP and MP upgrade procedures involve upgrading the AP and MP images on the compact flash of the MWAM. You upgrade one partition from the other partition. Usually, you upgrade the AP from the MP, then upgrade the MP from the AP. You upgrade the AP or MP to use new features or fixes.

Inline IOS Image Upgrade

The inline IOS image upgrade procedure, also called the fast upgrade procedure, is similar to the AP upgrade in that both procedures upgrade the image used by the application. However, because this procedure is performed from the AP, you are not required to reset the module. After the upgrade, you must reload each MWAM processor to activate the images. This procedure significantly reduces the amount of down time associated with module resets.

Upgrade Notes

Read the upgrade notes before performing these procedures. (For an explanation of the MP and AP software, see the "MWAM Software" section on page 1-8.)

- Use the **hw-module module** *slot_number* **reset cf:1** command to switch to the MP. In the MP mode, the processor complexes do not fully initialize and cannot run the IOS image. The main purpose for operating in the MP mode is to upgrade the AP image.
- Use the **hw-module module** *slot_number* **reset** command to switch to the AP. This is the normal operating mode.
- The **show module** command displays the software version of the partition image you are running. If you are running the AP image, **show module** displays the AP image version. If you are running the MP image, the MP image version displays.
- The MWAM images use the following formats:
  - The MP image: *mp.2-1-0-11.bin.gz* (example)
  - The AP image: *c6svc-5mwam-g4js-bf21_10.123-5a.B* (example)
  - The inline IOS image: *c6svc-mwam-g4js-bi21_10.123-5a.B* (example)

AP Upgrade Procedure

Note The total time to download an application image can be up to 30 minutes.

To upgrade an application image to the latest available version, first locate the image in the Software Center at Cisco.com:

http://www.cisco.com/cgi-bin/tablebuild.pl/ssg

Caution Cisco recommends that you globally configure the **logging console** command on the Supervisor module to display the output details of the upgrade procedure.

To upgrade the application image, perform the following tasks:

	Command	Purpose
Step 1	`Sup-7600# hw-module module slot_number reset cf:1`	Reset the MP on the MWAM (this takes about 3 minutes). **Note** Skip this step if you are already running the MP image.
Step 2	`Sup-7600# show module slot_number`	Verify that the MP has booted and MWAM status is OK.
Step 3	`Sup-7600# copy tftp://path/filename pclc#slot-fs:`	Copy the AP image to the compact flash. **Note** Copy operation could last several minutes.
Step 4	`Sup-7600# show module slot_number`	Monitor the copy process and verify that the module is on line (OK) before proceeding.

	Command	Purpose
Step 5	`Sup-7600# hw-module module slot_number reset`	Reset the MWAM to the AP. **Note** You must be running the AP image to perform the MP upgrade procedure.
Step 6	`Sup-7600# show module slot_number`	Verify that the AP image you copied is displayed in the output.

The following example shows how to upgrade the AP image:

AP Upgrade Example

```
Sup-7606# hw-module module 4 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified.<<<<<<<<<<<< This message is informational.

Proceed with reload of module? [confirm]

% reset issued for module 4

Sup-7606# show module 4
.
. Following output displays MP image version because MWAM is reset to MP (cf:1)
.
Mod MAC addresses                          Hw     Fw           Sw            Status
--- ---------------------------------- ------ ------------ ------------ -------
 4  0010.7b00.0c98 to 0010.7b00.0c9f   0.301 7.2(1)       2.1(0.11)m   Other
.
.
.
Sup-7606# copy tftp://mwamimages/ap/c6svc-5mwam-g4js-bf21_10.123-5a.B pclc#4-fs:
Upgrade has started
Do not reset the card till upgrade is complete
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK - 29048727/58096640 bytes]

29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
Sup-7606#
2d21h: %SVCLC-SP-5-STRRECVD: mod 4: <Application upgrade has started>
2d21h: %SVCLC-SP-5-STRRECVD: mod 4: <Do not reset the module till upgrade completes!!>
Sup-7606#

2d21h: %SVCLC-SP-5-STRRECVD: mod 4: <Application upgrade has succeeded>
2d21h: %SVCLC-SP-5-STRRECVD: mod 4: <You can now reset the module

Sup-7606# show module 4
.
.
.
Mod MAC addresses                          Hw     Fw           Sw            Status
--- ---------------------------------- ------ ------------ ------------ -------
 4  0010.7b00.0c98 to 0010.7b00.0c9f   0.301 7.2(1)       2.1(0.11)m   OK
.
.
.
Sup-7606# hw-module module 4 reset <<<<< Resets MWAM to AP
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
```

```
% reset issued for module 4
SP:The PC in slot 4 is shutting down. Please wait ...
SP:PC shutdown completed for module 4
%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
%C6KPWR-SP-STDBY-4-DISABLED:power to module in slot 4 set off (Reset)
%DIAG-SP-3-NO_TEST:Module 4:No test to run
%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

MP Upgrade Procedure

Caution Perform the MP upgrade procedure only when directed by Cisco TAC personnel.

The MP image rarely requires upgrading. If you are instructed to update the MP, perform the following tasks:

	Command	Purpose
Step 1	Router# **copy tftp://***path***/***filename* **pclc#***slot***-fs:**	Copy the MP image to the compact flash. **Note** You must be running the AP image to perform this step.
Step 2	Router# **show module** *slot_number*	Monitor the copy process and verify that the module is on line (OK) before proceeding.
Step 3	Router# **hw-module module** *slot_number* **reset cf:1**	Reset the MWAM to the MP.
Step 4	Router# **show module** *slot_number*	Verify that the MP image you copied is displayed in the output.
Step 5	Router# **hw-module module** *slot_number* **reset**	Reset the MWAM to the AP.

The following example shows how to upgrade the MP image:

MP Upgrade Example

```
Sup-7606# copy tftp://mwamimages/mp/mp.2-1-0-11.bin.gz pclc#4-fs:

Accessing tftp://mwamimages/mp/mp.2-1-0-11.bin.gz...
Loading mwamimages/mp/mp.2-1-0-11.bin.gz from 10.69.1.129 (via Vlan172):!
OOO!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


10300959 bytes copied in 124.360 secs (82832 bytes/sec)
Sup-7606#

3d19h:%SVCLC-SP-5-STRRECVD:mod 4:<Upgrade of MP was successful.>
3d19h:%SVCLC-SP-5-STRRECVD:mod 4:<You can now reset the module>

Sup-7606# show module 4
.
. Following output shows AP image version because MWAM is reset to AP (cf:4)
.
```

```
Mod Ports Card Type                                  Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  4     3  MWAM Module                              WS-SVC-MWAM-1      SAD063703NL

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  4  0010.7b00.0c98 to 0010.7b00.0c9f   0.301 7.2(1)       1.2(2.1)     Ok

Sup-7606# hw-module module 4 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified.<<<<<<<<<<<< This message is informational.

Proceed with reload of module? [confirm]

% reset issued for module 4

Sup-7606# show module 4
.
. Following output shows MP image version because MWAM is reset to MP (cf:1)
.
Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
 4  0010.7b00.0c98 to 0010.7b00.0c9f   0.301 7.2(1)       2.1(0.11)m   Other
.
.
.
Sup-7606# hw-module module 4 reset <<<<< Resets MWAM to AP (normal operation)
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]

% reset issued for module 4
SP:The PC in slot 4 is shutting down. Please wait ...
SP:PC shutdown completed for module 4
%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
%C6KPWR-SP-STDBY-4-DISABLED:power to module in slot 4 set off (Reset)
%DIAG-SP-3-NO_TEST:Module 4:No test to run
%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

Inline IOS Image Upgrade Procedure

This feature was introduced in IOS release 12.3(5a)B.

The "AP Upgrade Procedure" section on page 5-5 requires you to reset the MWAM, upgrade the image, then reset the module again. The inline IOS image upgrade, also called the fast upgrade, allows you to upgrade an IOS image without resetting the module. You must still reset each MWAM processor to load its image.

To upgrade an IOS image to the latest available version, first locate the image in the Software Center at Cisco.com:

http://www.cisco.com/cgi-bin/tablebuild.pl/ssg

Note The inline IOS image also includes a ROMMON image.

To upgrade the IOS image using this procedure, perform the following tasks:

	Command	Purpose
Step 1	`Sup-7606#` **`copy tftp://`***`path`***`/`***`filename`* **`pclc#`***`slot`***`-fs:`**	Copy the IOS-only image to the compact flash. **Note** You must be running the AP image to perform this step.
Step 2	`Sup-7606#` **`show module`** *`slot_number`*	Monitor the copy process and verify that the module is on line (OK) before proceeding.
Step 3	`root@mwam-5#` **`reload all`**	Session down to the PC and issue the **reload all** command. **Note** Alternatively, you can reset the MWAM using **hw-module module** *slot_number* **reset** command to load the new image on all the processors.
Step 4	`root@mwam-5#` **`show images`**	Show the images on the processor.
Step 5	`root@mwam-5#` **`show version`**	Show the image version.

The following example shows how to perform an inline IOS upgrade:

Inline IOS Upgrade Example

```
Sup-7606# copy tftp://mwamimages/ios/c6svc-5mwam-g4js-bi21_10.123-5a.B.bin pclc#5-fs:

Destination filename [svcmwam-js-mz.geo_t_040205.bin]?


Accessing tftp://mwamimages/ios/svcmwam-js-mz.geo_t_040205.bin...


Loading mwamimages/ios/svcmwam-js-mz.geo_t_040205.bin from 10.102.16.25 (via Vlan1):
!OOO!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


[OK - 11549631 bytes]


11549631 bytes copied in 107.552 secs (107386 bytes/sec)


Sup-7606#
2w1d: %SVCLC-SP-5-STRRECVD: mod 5: <Application upgrade has started>
2w1d: %SVCLC-SP-5-STRRECVD: mod 5: <Do not reset the module till upgrade completes!!>
2w1d: %SVCLC-SP-5-STRRECVD: mod 5: <Configuring svcmwam-js-mz.geo_t_040205>
2w1d: %SVCLC-SP-5-STRRECVD: mod 5: <Application upgrade has succeeded>
2w1d: %SVCLC-SP-5-STRRECVD: mod 5: <You can now reset the module>

Sup-7606#
Sup-7606# show module 5
.
```

```
.
Mod MAC addresses                         Hw    Fw           Sw           Status
--- ------------------------------------ ------ ------------ ------------ -------
 4  0010.7b00.0c98 to 0010.7b00.0c9f   0.301 7.2(1)       2.1(0.11)m   Other
.
.
.
Sup-7606#session slot 5 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open


SVCMWAM Image version 2.1(0.1b)
Tue Oct 14 11:04:43 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
Kernel 2.4.10.komodo on an i686
login: root
Password:

SVCMWAM Image version 2.1(0.1b)
Tue Oct 14 11:04:43 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.


SVCMWAM Image version 2.1(0.1b)
Tue Oct 14 11:04:43 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.


root@mwam-5# reload all

root@mwam-5# show images
Device name Partition#  Image name
----------- ----------  ----------
Compact flash(cf)6     SIMPSON_RAM.bin
Version Information:Compiled Tue 19-Aug-03 13:35 by dchih
Compact flash(cf)6
svcmwam-g4js-mz.123-7.3.T
Version Information:
Compiled Wed 11-Feb-04 21:26 by eaarmas$

AP software is c6svc-5mwam-g4js-bi21_10.123-5a.B

root@mwam-5# show version

SVCMWAM Image version 2.1(0.3b)
Thu Feb 19 05:30:06 EST 2004
Copyright (c) 2002-2003, 2004 by cisco Systems, Inc.
All rights reserved.

AP software is c6svc-5mwam-g4js-bi21_10.123-5a.B
AP software is based upon Maintenance image version:3.1(0.2)
IOS Software is svcmwam-g4js-mz.123-7.3.T
6 Processor Configuration

Line Card Number :WS-SVC-MWAM-1
Number of Pentium-class Processors :      1
BIOS Vendor:Phoenix Technologies Ltd.
BIOS Version:4.0-Rel 6.0.4
Total available memory:500 MB
```

```
Size of compact flash:122 MB

root@mwam-5#
```

Reverting to Previous IOS Image

If you decide to revert to the previous IOS image, establish a session to the processor control complex, log in as root, and run the following command:

```
root@mwam-5# restore ios
Restoring image
Restoring configuration files
Operation completed successfully
root@mwam-5#
```

This action restores the previous IOS image. You must then reload the MWAM processor(s) to activate the image.

Note You can revert to the previous image only if you have not reset or rebooted the MWAM. The previous IOS image is in temporary storage. If the MWAM has been reset/rebooted, the previous image is no longer available.

Upgrading the ROMMON Image

After downloading/upgrading the application image, you may need to upgrade the ROMMON images on each processor complex.

Note The ROMMON image is bundled with the application image. Upgrade the ROMMON image only when required. Refer to the release note for your application to determine if a ROMMON upgrade is required.

To upgrade the ROMMON image, perform the following tasks from the appropriate console:

	Command	Purpose
Step 1	`Sup-7606# enable`	Enters privileged EXEC mode.
Step 2	`Sup-7606# session slot slot_number processor processor_number (2-6)`	Establishes a session to an MWAM processor. **Note** When you session to one processor on a complex, both processors on the complex will be upgraded (see Table 1-2 on page 1-5 for processor-to-complex mapping.)
Step 3	`Proc-4-2# upgrade rom-monitor`	Gets the ROMMON image (from the compact flash card) for the processor complex.
Step 4	Repeat above steps for each processor complex.	Loads the ROMMON image on all complexes.
Step 5	`Sup-7606# hw-module module slot_number reset`	Resets the MWAM to upgrade the ROMMON images on the module.

The following example shows how to perform a ROMMON image upgrade:

ROMMON Image Upgrade Example

```
Sup-7606# enable
Sup-7606# session slot 4 processor 2
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.42 ... Open <<<<< last part of address indicates slot 4, processor 2

Proc-4-2#



Press RETURN to get started!

Proc-4-2#upgrade rom-monitor
MWAM: ROMMON image upgrade in progress.
Loading SIMPSON_RAM.bin from 128.0.1.1 (via GigabitEthernet0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 190592/380928 bytes]
MWAM: Erasing FUR Region.
MWAM: Programming Flash.
MWAM: Verifying new ROMMON image.
MWAM: ROMMON image upgrade complete.
MWAM: The card must be reset for this to take effect.

~Upgrade commands and output for processors 4 and 6 elided~

Sup-7606# hw-module module 4 reset
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]

% reset issued for module 4
SP:The PC in slot 4 is shutting down. Please wait ...
SP:PC shutdown completed for module 4
%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
%C6KPWR-SP-STDBY-4-DISABLED:power to module in slot 4 set off (Reset)
%DIAG-SP-3-NO_TEST:Module 4:No test to run
%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

Booting the Application Image

The Application Partition (AP) is specific to each MWAM and stores a Cisco IOS application image for the processors on the MWAM. By default, the MWAM boots to the application image when initially powered on.

To boot the application image manually, use the following command:

	Command	Purpose
Step 1	`Sup-7606# enable`	Enters privileged EXEC mode.
Step 2	`Sup-7606# hw-module module` *slot_number* **reset**	Reboots the MWAM.

For example, if you have an MWAM installed in slot 4, you would enter the following commands:

```
Sup-7606# enable
Sup-7606# hw-module module 4 reset
Device BOOT variable for reset = <cf:4>
```

```
Proceed with reload of module? [confirm]

% reset issued for module 4
SP:The PC in slot 4 is shutting down. Please wait ...
SP:PC shutdown completed for module 4
%C6KPWR-SP-4-DISABLED:power to module in slot 4 set off (Reset)
%C6KPWR-SP-STDBY-4-DISABLED:power to module in slot 4 set off (Reset)
%DIAG-SP-3-NO_TEST:Module 4:No test to run
%OIR-SP-6-INSCARD:Card inserted in slot 4, interfaces are now online
```

CHAPTER 6

Configuring the MWAM

This chapter discusses how to configure the MWAM. It includes the following sections:

For a complete description about the commands used in configuring the MWAM, see Appendix A, "Command Reference". To locate documentation about other commands that appear in this chapter, refer to the following books:

- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*—Chapter 2
- *Cisco 7600 Series Internet Router IOS Software Configuration Guide*—Chapter 2

Before You Begin

Before you configure the MWAM, read the following required sections:

- Release Notes
- Using the CLI
- Unsupported Commands
- Booting the Application Image

Release Notes

Refer to the latest release notes for your configuration. The release notes contain additional information that became available after the initial release of the product. These release notes describe the features, modifications, and caveats for the MWAM and its associated software and hardware platforms.

Note The most current version of these release notes can be found on Cisco.com (for MWAM), click:

Documentation>Routers>Cisco 7600 Series Routers>General Information>Release Notes>Release Notes for Cisco Multiprocessor WAN Application Module with Cisco IOS Release

On Cisco.com (for IOS), click:

Documentation>Cisco IOS Software>Cisco Software Releases 12.3 Mainline>General Information>Release Notes>Cisco IOS Release 12.3 Cross-Platform Release Notes and Caveats

Caution We strongly recommend that you read these release notes before using your MWAM or upgrading your MWAM software.

Each release note contains the following sections:

- System Requirements
- New and Changed Information
- Performance
- External Interfaces
- IP Address Management
- Reliability/Availability
- MWAM Installation and Configuration
- Limitations and Restrictions
- Caveats
- MIBs

Using the CLI

In configuring the MWAM, you use two command line interfaces:

- Main CLI on the Supervisor console to:
  - boot the device and load the application image
  - assign VLANs to the MWAM
  - configure MWAM VLANs on the Supervisor module
- Session CLI to each MWAM processor to:
  - configure subinterfaces on the VLANs
  - assign IP addresses to the subinterfaces
  - configure the application

On the Supervisor console, the main commands are:

- **mwam module** command—Configures connectivity between the switch fabric and the individual processors on the MWAM
- **show mwam module** command—Shows information about the individual MWAM processors. You must also configure any real external interfaces required by the application and VLANs to forward traffic to the switch fabric.

On the session CLI to the MWAM processor, you can access Cisco IOS commands to configure the application as required. This includes configuring the VLAN subinterfaces to connect to the switch fabric.

Note To get a basic understanding of the Cisco IOS CLI and Cisco IOS command modes (see Chapter 4, "Command-Line Interface (CLI) Basics" and refer to Chapter 2, "Command Line Interfaces", in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* and the *Cisco 7600 Series Router IOS Software Configuration Guide*).

Unsupported Commands

Note Support for NTP/Clock configuration on the MWAM was introduced in release 12.3(3)B1.

If NTP is configured on the MWAM, the processors synchronize with the NTP server clock. The Gi0/0 interface must be up and the NTP server must be reachable for synchronization to occur. If the MWAM is configured in Supervisor mode, the configuration must be downloaded before the Gi0/0 can come up.

If NTP is disabled (the default), the processors synchronize (once every minute) with the processor control complex.

The following NTP/Clock commands are not supported on the MWAM:

- `clock calendar-valid`
- `ntp master`
- `ntp update-calendar`

Booting the Application Image

As described in the "Booting the Application Image" section on page 5-12, the MWAM boots to the application image when initially powered on. Before "Assigning VLANs to the MWAM", ensure that the AP image has been downloaded to the MWAM. If it has not, follow the procedures described in Chapter 4, "Loading the MWAM".

VLAN Configuration Tasks

A virtual LAN (VLAN) configures switches and routers according to logical rather than physical topologies. Using VLANs, you can combine any collection of LAN segments within an internetwork into an autonomous user group, which appears as a single LAN. VLANs locally segment the network into different broadcast domains so that packets are switched only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

This section describes how to configure the VLANs for the MWAM.

The tasks discussed are:

Assigning VLANs to the MWAM

Note By default, the MWAM is in trunking mode and assigned to VLAN 1.

Assigning VLANs to the MWAM requires you to understand the mapping between the processors on the MWAM and the Ethernet port/VLAN that connects the processor to the switch fabric (see Table 1-2 on page 1-5 and Figure 1-2 on page 1-5 for this information).

To assign VLANs to the MWAM, enter this command for each of the three switch fabric interface ports (ports 1, 2, and 3) that connect the Supervisor module to the MWAM:

	Command	Purpose
Step 1	`Sup-7606> enable`	Enters privileged EXEC mode.
Step 2	`Sup-7606# configure terminal`	Enters the configuration mode.
Step 3	`Sup-7606(config)# mwam module` *slot_number* `port` *port_number* `allowed-vlan` *vlan_ID*	Configures the Ethernet connectivity from the backplane (that is, switch fabric) to the individual processors on the MWAM. **Note** One of the allowed VLANs must be the administrative VLAN.

This example assigns VLANs 1-1005 to ports 1-3 that connect to the MWAM in slot 5:

```
Sup-7606>
Sup-7606> enable

Sup-7606# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sup-7606(config)# mwam module 5 port 1 allowed-vlan 1-1005
Sup-7606(config)# mwam module 5 port 2 allowed-vlan 1-1005
Sup-7606(config)# mwam module 5 port 3 allowed-vlan 1-1005
```

Note You may need to wait up to 30 seconds for spanning tree to converge for connectivity.

Assigning MWAM Traffic to VLAN QoS Policies

Note This feature was introduced with Cisco IOS Release 12.2(14)ZA7.

Quality of Service (QoS) policies can be applied to differentiate levels of service to GGSN-based subscribers. A QoS policy is assigned to the same VLAN to which MWAM ports are assigned (see Assigning VLANs to the MWAM, page 6-4).

To assign MWAM traffic to the QoS policy, enter the following command for each of the three switch fabric interface ports (ports 1, 2, and 3) that connect the Supervisor module to the MWAM:

	Command	Purpose
Step 1	`Sup-7606> enable`	Enters privileged EXEC mode.
Step 2	`Sup-7606# configure terminal`	Enters the configuration mode.
Step 3	`Sup-7606(config)# mwam module` *slot_number* `port` *port_number* `vlan-based`	Assigns MWAM traffic on the specified port to VLAN-based QoS policies.

The following example assigns traffic to QoS policies for the switch fabric interface ports of the MWAM in slot 5:

```
Sup-7606>
Sup-7606> enable

Sup-7606# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Sup-7606(config)# mwam module 5 port 1 vlan-based
Sup-7606(config)# mwam module 5 port 2 vlan-based
Sup-7606(config)# mwam module 5 port 3 vlan-based
```

Configuring MWAM VLANs on the Supervisor Module

You must configure the VLANs on the Supervisor 2 module to forward traffic to the switch fabric. On the session CLI to the MWAM processor, you access the Cisco IOS commands to configure the VLANs. Two configuration modes are available for configuring Supervisor module VLANs:

- VLAN database mode
- Global configuration mode

Caution RPR+ redundancy does not support configurations entered in VLAN database mode. If you have a high-availability configuration with redundant Supervisor modules using RPR(+), configure the VLANs in global configuration mode and not in the VLAN database mode; otherwise, the VLAN information would not be synchronized to the redundant Supervisor module.

VLAN Database Mode

Note You cannot configure extended-range VLANs in VLAN database mode. You can configure extended-range VLANs only in global configuration mode.

To configure VLANs on the Supervisor 2 module in the VLAN database mode, perform this task:

	Command	Purpose
Step 1	`Sup-7606> enable`	Enters privileged EXEC mode.
Step 2	`Sup-7606# vlan database`	Enters VLAN database mode.
Step 3	`Sup-7606(vlan)# vlan` *vlan_ID*	Specifies a VLAN (1-1005) to configure.
Step 4	`Sup-7606(vlan)# exit`	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the Supervisor 2 module in the VLAN database mode:

```
Sup-7606> enable
Sup-7606# vlan database
Sup-7606(vlan)# vlan 100
VLAN 100 added:
     Name: VLAN100
Sup-7606(vlan)# exit
APPLY completed.
Exiting....
```

Global Configuration Mode

Note Release 12.1(11b)E or later supports VLAN configuration in global configuration mode.

To configure VLANs on the Supervisor 2 module in the global configuration mode, perform this task:

	Command	Purpose
Step 1	`Sup-7606# configure terminal`	Enters global configuration mode.
Step 2	`Sup-7606(config)# vlan vlan_ID {[-vlan_ID]|[,vlan_ID]}`	Enters VLAN configuration mode and creates an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs in a comma-separated list (do not enter space characters).
Step 3	`Sup-7606(config-vlan)# end`	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the Supervisor 2 module in global configuration mode:

```
Sup-7606# configure terminal
Sup-7606(config)# vlan 100-200
Sup-7606(config-vlan)# end
```

Configuring Layer 3 Interfaces on the VLANs

You can configure layer 3 interfaces on the MWAM VLANs if required by the application.

Note VLANs must exist before you can configure the layer 3 interfaces on them.

To configure the Layer 3 VLAN interface, perform this task:

	Command	Purpose
Step 1	`Sup-7606# configure terminal`	Enters global configuration mode.
Step 2	`Sup-7606(config)# interface vlan vlan_ID`	Selects an interface to configure.
Step 3	`Sup-7606(config-if)# ip address ip_address subnet_mask`	Configures the IP address and IP subnet.
Step 4	`Sup-7606(config-if)# no shutdown`	Enables the interface.
Step 5	`Sup-7606(config-if)# exit`	Exits configuration mode.

This example shows how to configure the Layer 3 VLAN interface:

```
Sup-7606# configure terminal
Sup-7606(config)# interface vlan 100

Sup-7606(config-if)# ip address 10.10.1.10 255.255.255.0

Sup-7606(config-if)# no shutdown
Sup-7606(config-if)# exit
```

MWAM Session Configuration Tasks

This section details the MWAM session configuration tasks that should be performed.

Configuring the Application to the MWAM

To configure the application on an MWAM processor, complete the following steps (see Cisco IOS Restrictions and Limitations on the MWAM, page 6-9 for information about Cisco IOS restrictions and limitations on the MWAM architecture):

	Command	Purpose
Step 1	`Sup-7600> enable`	Enters privileged EXEC mode.
Step 2	`Sup-7600# session slot slot_number processor processor_number (2-6)`	Establishes a session to the MWAM processor to allow Cisco IOS configuration. **Note** You can only configure interface Gi0/0.
Step 3	`mwam-6-4> enable`	Enters privileged EXEC mode.
Step 4	`mwam-6-4# dir bootflash:`	Displays the bootflash directory. **Note** If response is `0 bytes free`, format the bootflash file system.
Step 5	`mwam-6-4# format bootflash:`	Formats the bootflash file system to enable it to store files (see caution). **Caution** Use **format** command *only* if the response to **dir bootflash:** is 0 bytes free.
Step 6	Configure the application.	Refer to the configuration guide for the application.
Step 7	`mwam-6-4# copy running-config startup-config`	Copies the running configuration to NVRAM on the MWAM (if in local mode) or Supervisor bootflash (if in Supervisor mode).

This example shows how to establish a session to an MWAM processor:

```
Sup-7606> enable
Sup-7606# session slot 6 processor 4
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open <<<<< last part of address indicates slot 6, processor 4

mwam-6-4#

Press RETURN to get started!

mwam-6-4# dir bootflash:
Directory of bootflash:/
```

```
No files in directory
524288 bytes total (0 bytes free) <<<response indicates that bootflash requires formatting

mwam-6-4# format bootflash:

Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "bootflash:".  Continue? [confirm]
Format of bootflash complete
```

After configuring the application, make a backup of the configuration as follows:

```
mwam-6-4# copy running-config startup-config
Destination filename [startup-config]?
.
.
.
```

Cisco IOS Restrictions and Limitations on the MWAM

When you establish a session to an MWAM processor, you can access Cisco IOS commands to configure the application as required. This section describes Cisco IOS restrictions and limitations required by the MWAM architecture. The following topics are covered:

Reload Command

The Cisco IOS **reload** command reloads a Cisco router. However, at the MWAM processor level, use the Cisco IOS **reload** command with caution. Two MWAM processors reside on one processor complex. When the **reload** command is issued for one processor, *both* processors on the complex are reloaded. In the following example, reloading processor 4 also reloads processor 5 because they share a complex.

```
MWAM-7-4# reload
 !!!! WARNING !!!!!
 CPU 5 in this complex will also be reloaded. All the changed configs
 there will be lost unless saved before confirming the reload.
Proceed with reload? [confirm]
Mar 23 05:55:41.915: This processor is being reloaded, session connection from sup will be
reset
Mar 23 05:55:43.819:%SYS-5-RELOAD:Reload requested by console. Reload Reason:Reload
command.
```

Also, if you issue the reload command at the Supervisor level, the reload occurs for the entire chassis, which includes all modules in the chassis. If the chassis contains five MWAMs, and each MWAM contains five active processors, then 25 routers are reloaded by this operation.

Hot Standby Router Protocol Configuration

The MWAM architecture imposes some limitations on the configuration of the Hot Standby Router Protocol (HSRP). You must not configure HSRP groups for processors that are in the same processor complex. Because of the MWAM architecture, when one processors fails (crashes), both processors in the complex reload. For this reason, HSRP groups are not supported for processors in the same complex.

You can configure HSRP groups for processors on the same MWAM as long as they are not in the same complex. A preferable strategy is to configure HSRP groups to span processors on different MWAMs.

Multicast MAC Addressing

The Cisco IOS supports multicast Media Access Control (MAC) addressing in multiple ways. The MWAM supports some of these ways better than others. For applications, such as HSRP, where a single multicast MAC address is used, the MWAM can support the address in the same way as any other MAC address.

Each processor complex supports up to eight explicit MAC address entries. However, when exceeding this limit, the MWAM must use the multicast promiscuous mode. In this mode, all multicast addresses are received by the processor and must be validated in software rather than hardware. This restriction places additional load on the processor. Other types of multicast MAC addressing in the Cisco IOS (for example, IP multicast routing) require the multicast promiscuous mode at all times.

When the multicast promiscuous mode is enabled on both processors in a complex, each one processes *all* of the multicast packets. This condition leads to additional processing at the MAC layer. For this reason, Cisco recommends that IP multicast routing be configured on only one processor per complex.

You can determine the mode with the **show controller** command.

Copy Running Configuration Command

Note The following restrictions were introduced with release 12.2(14)ZA5.

Local Mode Operation

For MWAMs operating in local mode, the **copy running-config** command copies the running configuration to NVRAM on the MWAM. See the example that follows:

```
mwam-6-4# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

mwam-6-4# show startup
Using 505 out of 524280 bytes
!
!NVRAM config last updated at <time stamp>

<configuration>

end
```

Supervisor Mode Operation

For MWAMs operating in Supervisor mode, the **copy running-config** command copies the running configuration to the Supervisor module(s). See the example that follows:

```
mwam-6-4# copy running-config startup-config
Destination filename [startup-config]?
```

```
Writing bootflash:SLOT6PC4.cfg
Config uploaded to supervisor in slot 1

Writing bootflash:SLOT6PC4.cfg
Config uploaded to supervisor in slot 2

Config uploaded to 2 supervisor(s)
```

Note If redundant Supervisor modules are equipped and the **copy running-config startup-config** command succeeds for one Supervisor but fails for the other, you must manually correct the failure. If differences exist in an MWAM configuration file between the master and slave Supervisor modules, the file at the master Supervisor module is written over the file at the slave Supervisor module.

Copy TFTP Command

Note The following restriction was introduced with release 12.2(14)ZA5.

Caution The command **copy tftp:**//.../*filename* **startup-config** (issued at the MWAM processor level) copies the *filename* configuration to NVRAM on the MWAM. This action causes an MWAM that is configured in Supervisor mode to revert to local mode when the next reload operation occurs. Because a file exists in NVRAM, the MWAM processor gets its configuration locally and not from the Supervisor bootflash. To return to the Supervisor mode, perform the procedure provided in the "Converting to Supervisor Mode" section on page 6-15.

Erase Startup Configuration Command

Note The following restrictions were introduced with release 12.2(14)ZA5.

Local Mode

When operating in local mode, use the command **erase startup-config** (issued at the MWAM processor level) to erase the local NVRAM configuration file.

Supervisor Mode

When operating in Supervisor mode, erase the configuration file in the Supervisor bootflash with the following commands from the Supervisor console:

- **delete bootflash:SLOT***x***PC***y***.cfg** for the master Supervisor
- **delete slavebootflash:SLOT***x***PC***y***.cfg** for the slave Supervisor

Show Startup Configuration Command

Note The following restrictions were introduced with release 12.2(14)ZA5.

Local Mode

When operating in local mode, the command **show startup-config** (issued at the MWAM processor level) shows the contents of the NVRAM configuration file.

Supervisor Mode

When operating in Supervisor mode, show the startup configuration using the following commands from the Supervisor console:

- **more bootflash:SLOT*x*PC*y*.cfg** for the master Supervisor
- **more slavebootflash:SLOT*x*PC*y*.cfg** for the slave Supervisor

Note If you enter **show startup-config** from the MWAM console while in Supervisor mode, the system response is `startup-config is not present` because this command is reading the NVRAM on the MWAM.

Squeeze Bootflash Command

When operating in Supervisor mode, the operator must maintain adequate file space on the Supervisor bootflash. This includes periodically using the **squeeze bootflash** command to consolidate available space.

Configuring a LAN Port for Layer 2 Switching

To configure physical interfaces that connect to the servers or the clients in the corresponding VLAN, perform this task at the MWAM processor level:

	Command	Purpose
Step 1	`pro-6-2# configure terminal`	Enters configuration mode.
Step 2	`pro-6-2(config)# interface` *type*[1] *slot/port*	Selects the LAN port to configure.
Step 3	`pro-6-2(config-if)# switchport`	Configures the LAN port for Layer 2 switching. **Note** You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional **switchport** commands with keywords.
Step 4	`pro-6-2(config-if)# switchport mode access`	Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.
Step 5	`pro-6-2(config-if)# switchport access vlan` *vlan_ID*	Configures the default VLAN, which is used if the interface stops trunking.
Step 6	`pro-6-2(config-if)# no shutdown`	Activates the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure a physical interface as a Layer 2 interface and assign it to a VLAN:

```
pro-6-2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

pro-6-2(config)# interface gigabitethernet 1/1
```

```
pro-6-2(config-if)# switchport

pro-6-2(config-if)# switchport mode access

pro-6-2(config-if)# switchport access vlan 100

pro-6-2(config-if)# no shutdown

pro-6-2(config-if)# exit
```

Configuring Subinterfaces on MWAM Processor

The IEEE 802.1Q protocol is used to provide trunks between switches. The switches use the trunks to share VLANs and transfer data between VLANs on different switches. Create as many subinterfaces as needed to connect to different networks. You will configure 802.1Q encapsulation on each subinterface to the VLANs created on the Supervisor module.

To enable 802.1Q encapsulation on each of the processors on the MWAM, use the following commands in the interface configuration mode:

	Command	Purpose
Step 1	`pro-6-2# configure terminal`	Enters configuration mode.
Step 2	`pro-6-2(config)# interface gigabitethernet` *slot/port*	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 3	`pro-6-2(config-if)# encapsulation dot1Q` *vlan_id*	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 4	`pro-6-2(config-if)# ip address` *ip-address mask*	Sets a primary IP address for an interface.

This example shows how to enable IEEE 802.1Q on VLANs 310 and 401.

```
pro-6-2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
pro-6-2(config)# interface GigabitEthernet0/0
pro-6-2(config-if)# no ip address
!
pro-6-2(config-if)# interface GigabitEthernet0/0.310
pro-6-2(config-if)# encapsulation dot1Q 310
pro-6-2(config-if)# ip address 10.1.1.44 255.255.255.0
!
pro-6-2(config-if)# interface GigabitEthernet0/0.401
pro-6-2(config-if)# encapsulation dot1Q 401
pro-6-2(config-if)# ip address 10.121.68.44 255.255.255.0
```

Verifying the MWAM Configuration

To verify the configuration, enter these commands:

	Command	Purpose
Step 1	`Sup-7600# show spanning-tree vlan vlan_ID`	Displays the spanning tree state for the specified VLAN.
Step 2	`Sup-7600# show mwam mod slot_number port_number [state | traffic]`	Displays the trunk configuration.

Note In the following examples, the MWAM is installed in slot 3 (Gi3/1).

This example shows how to verify that the module is in the forwarding (FWD) state:

```
Sup-7606# show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0009.e9b2.b864
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768
             Address     0009.e9b2.b864
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi3/1            Desg FWD 4         128.129  P2p
Gi4/1            Desg FWD 4         128.193  P2p
Po261            Desg FWD 3         128.833  P2p
Router
```

This example shows how to verify that the VLAN information displayed matches the VLAN configuration:

```
Sup-7606#show mwam module 3 port 1 state
Mwam module 3 data-port 1:
 Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-1000
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1-1000
Vlans allowed and active in management domain:1-2,95,100
Vlans in spanning tree forwarding state and not pruned:
   1-2,95,100
Allowed-vlan : 1-1000

Sup-7606#show mwam module 3 port 1 traffic
Specified interface is up line protocol is up
  Hardware is C6k 1000Mb 802.3, address is 00e0.b0ff.3a18 (bia 00e0.b0ff.3a18)
```

```
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 77
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
   24598 packets input, 2138920 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   928697 packets output, 68993318 bytes, 0 underruns
   0 output errors, 0 collisions, 34 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers swapped out
```

Converting to Supervisor Mode

Note This feature requires Cisco IOS 12.2(14)ZA5 (or higher) on the Supervisor module and an MWAM image that supports Supervisor bootflash storage of MWAM configuration files. It also requires the ROMMON to be upgraded as described in the "Upgrading the ROMMON Image" section on page 5-11.

The default mode for the MWAM configuration file storage is Supervisor mode.

New Behavior

Cisco IOS 12.3(13)T introduces new behavior when converting to the Supervisor mode.

When an MWAM image boots on an MWAM processor, it queries a persistent flag to determine if the operating mode has ever been set. If the persistent flag is set to a mode (Supervisor or local), the MWAM boots up in that mode. If the flag has *never* been set, the MWAM determines the operating mode on the basis of the NVRAM contents. If the NVRAM startup-config file is 0 bytes long, the mode is set to Supervisor; if the NVRAM startup-config file is longer than 0 bytes, the mode is set to local.

Old Behavior

For MWAMs with earlier Cisco releases, the operating mode is determined solely by the contents of the NVRAM. If the NVRAM startup-config file is 0 bytes long, the mode is set to Supervisor; if the NVRAM startup-config file is longer than 0 bytes, the mode is set to local.

Currently deployed MWAMs that have pre-existing configuration files stored in NVRAM will continue to operate in local mode. If you choose to operate the MWAMs in local mode, you can use the **no mwam bootflash access** command in global configuration mode from the Supervisor console to ensure that MWAM access to TFTP/RCP services on the Supervisor is denied with appropriate error messages.

Steps to Convert to Supervisor Mode

To convert an MWAM processor from local mode to Supervisor mode, complete the following steps.

	Command	Purpose
Step 1	`Sup-7606> enable`	Enters privileged EXEC mode on the Supervisor.
Step 2	`Sup-7600# session slot slot_number processor processor_number (2-6)`	Establishes a session to the MWAM processor.
Step 3	`mwam-6-4> enable`	Enters privileged EXEC mode on the MWAM processor.
Step 4	`mwam-6-4# show mwam config-mode`	Shows the current configuration mode (local or Supervisor) of the MWAM processor.
Step 5	`mwam-6-4# mwam config-mode supervisor`	Changes the configuration mode to the Supervisor mode.

This example shows how to convert processor 4 on the MWAM in slot 6 to the Supervisor mode:

```
Sup-7606> enable
Sup-7606# session slot 6 processor 4

mwam-6-4> enable
mwam-6-4# show mwam config-mode
mwam config-mode local

mwam-6-4# mwam config-mode supervisor
Writing bootflash:SLOT6PC4.cfg
Config uploaded to supervisor in slot 1

Writing bootflash:SLOT6PC4.cfg
Config uploaded to supervisor in slot 2

Successfully changed mode: mwam config-mode supervisor
```

Caution If you are operating in the Supervisor mode in a chassis that does not have redundant Supervisor modules, back up both the *startup-config* file of the Supervisor module and all *SLOT*PC*.cfg* files on the bootflash device. Failure to take this precaution could result in the loss of all MWAM configurations, along with the Supervisor configuration.

Configuring Remote Console and Logging

Note The Remote Console and Logging feature requires Cisco IOS 12.2(14)ZA4 (or higher) on the Supervisor module. It also requires the ROMMON to be upgraded as described in the "Upgrading the ROMMON Image" section on page 5-11.

To configure the remote console and logging feature, complete the following steps:

	Command	Purpose
Step 1	`Sup-7606# configure terminal`	Enters configuration mode on the Supervisor console.
Step 2	`Sup-7606(config)# logging listen mwam udp_port`	Configures UDP port for MWAM logging input to the Supervisor module. **Note** If you are configuring "Remote Console Support for the Processor Control Complex" section on page 1-15, you must use UDP port 4000.
Step 3	`Sup-7606(config)# mwam module {slot_number | all} cpu {processor_number | all} logging log_level`	(Optional) Configures the severity level of MWAM logging information to send to the Supervisor module.
Step 4	`Sup-7606(config)# exit`	Exits configuration mode.
Step 5	`Sup-7606# session slot slot_number processor processor_number`	Establishes a Telnet session to the MWAM processor.
Step 6	`mwam-6-4# configure terminal`	Enters configuration mode on the MWAM processor console.
Step 7	`mwam-6-4(config)# logging main-cpu udp_port [log_level] [ip_address]`	Configures MWAM log redirection to the Supervisor module. **Note** You must specify the same UDP port number that you designated for the Supervisor module in Step 2.

When the Remote Console and Logging feature is configured, you can use the **execute-on** command to initiate a remote command request to an MWAM processor (see Appendix A, "Command Reference" for details).

Configuring the MWAM Memory Allocation

To reallocate the IO memory from the total available DRAM space on Cisco MWAM routers, use the **memory-size iomem** command in global configuration mode. To revert to the default memory allocation, use the **no** form of this command. By default, 32 MB is allocated for IO memory on each processor of a Cisco MWAM router.

The **iomem** configuration command is available on processors 2, 4, or 6, and it will be applied to the respective partner processors 3, 5, or 7 as well when configured. When 1 or 2 GB of total DRAM is available per MWAM processor complex, the permitted values for the IO memory are 32 MB, 64 MB, and 128 MB. When 512 MB of total DRAM is available per MWAM processor complex, only the default 32 MB IO memory option is available. After the IO memory is specified in the command line, the remaining DRAM memory will be used for the processor memory. After configuration, it must be saved and reloaded for the reallocation to occur.

The **memory-size iomem** command is applied in the global configuration mode as follows:

:

	Command	Purpose
Step 1	`Sup-7606> enable`	Enters privileged **EXEC** mode.
Step 2	`Sup-7606# session slot slot_number processor processor_number (2-6)`	Establishes a session to the MWAM processor. For example, Sup-7606 session slot 7 processor 2 **Note** The default escape character is **Ctrl-^**, then x.You can also type 'exit' at the remote prompt to end the session. Trying 127.0.0.72 ... Open
Step 3	`mwam-6-4>`	Press RETURN to get started.
Step 4	`mwam-6-4> enable`	
Step 5	`mwam-6-4# configure terminal`	Enters configuration mode. Enter configuration commands one per line. End with **Ctrl/Z**.
Step 6	`Router (config)# memory-size iomem 64`	This example allocates 64 MB of the DRAM memory to I/O memory and the remaining to processor memory.
Step 7	`Router# copy system:running-config nvram:startup-config`	The memory configuration will be saved to non volatile memory.
Step 8	`Router# reload`	

Clearing MWAM Session from Supervisor Console

To clear an MWAM session from the Supervisor console, complete the following steps:

	Command	Purpose
Step 1	`Sup-7606# show tcp brief`	Displays a concise description of TCP connection endpoints, including endpoints on the MWAM. **Tip** The command output displays the foreign address of the TCP connection between the processor control complex of the MWAM and the switch fabric interface. The address of this connection appears in the format 127.0.0.*xy*, where *x* is the MWAM slot number and *y* is the MWAM processor number. Correlate the foreign address to the TCB to perform the next step.
Step 2	`Sup-7606# clear tcp tcb tcb_addr`	Clears the Transmission Control Block (TCB) address of the TCP connection to the MWAM. The TCB address is an internal identifier for the endpoint.

This example shows how to clear an MWAM session on processor 2 of the MWAM in slot 7.

```
Sup-7606#show tcp brief
TCB        Local Address           Foreign Address        (state)
4345AC80  9.3.67.21.23            10.76.82.75.33713      ESTAB
509F0CD0  9.3.67.21.23            10.76.82.75.33777      ESTAB
43456D80  9.3.67.21.23            10.76.82.75.33712      ESTAB
43455A10  127.0.0.12.30211        127.0.0.72.23          ESTAB <<<< Connection to clear
4343BD18  9.3.67.21.23            9.3.66.4.11000         ESTAB
43449A0C  127.0.0.12.24068        127.0.0.71.23          ESTAB

Sup-7606#clear tcp tcb 43455A10

Sup-7606#
```

Recovering from MWAM Processor Lockout

Occasionally, you may discover that you are unable to log into an MWAM processor, either because of a configuration mistake or you have forgotten the password. On other Cisco routers the password recovery procedure involves setting the configuration register in ROMMON to ignore the startup-config. On MWAM processors you do not have access to the ROMMON. Instead, you issue the **recover-ios** command on the processor control complex. This forces the processor to ignore its configuration when it is reloaded.

To recover from the MWAM processor lockout condition, complete the following steps:

	Command	Purpose
Step 1	`Sup-7606# session slot` *slot_number* `processor 1`	Establishes a Telnet session to MWAM processor 1. **Note** User name is *root* and password is *cisco*.
Step 2	`root@mwam-5# recover-ios` *complex_number*	Sets the configuration register to boot with a clean configuration. **Note** The *complex_number* can be **0**, **1**, **2**, or **all**.
Step 3	`root@mwam-5# reload complex` *complex_number*	Reloads the processor complex. **Note** If the reload complex command is not recognized, contact the Cisco TAC Escalation Center to complete the recovery procedure.
Step 4	`root@mwam-5# normal-ios`	Sets the configuration register to boot with a normal configuration to ensure that processors do not ignore their startup configurations.

The following example shows how to recover from the lockout condition on processor complex 0 of the MWAM in slot 5:

```
Sup-7600# session slot 5 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.51 ... Open

SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct  3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
```

```
Kernel 2.4.10.komodo on an i686
login: root
Password:

SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct  3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.

root@mwam-5# recover-ios 0
processing -p
processing -c
Setting DHCP options for processor complex 0
Setting config-reg value to: 0x40
Base external MAC: "0005.9A3B.A180"
Internet Software Consortium DHCP Server V3.0.1rc6
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
Listening on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Sending on   LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Listening on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   Socket/fallback/fallback-net

root@mwam-5# reload complex 0

root@mwam-5# normal-ios
Base external MAC: "0005.9A3B.A180"
Internet Software Consortium DHCP Server V3.0.1rc6
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
Listening on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Sending on   LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Listening on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   Socket/fallback/fallback-net
```

Recover from Session/Telnet Command after Reload

If the session between a Supervisor module and an MWAM processor fails to recover from a reload after 10 minutes, Cisco recommends that you perform the following steps to recover.

Configure **ip rcmd rcp-enable** on the Supervisor module. For Supervisor release SXF4 and later, also configure **ip rcmd remote-host** <*localuser*> <*MWAM EOBC address*> <*remoteuser*> **enable** on the Supervisor module for each MWAM processor. For the supervisor **config-mode** to work, this remote IP address has to be, not just any IP, but the EOBC address(127.0.0.xy, where x = slot, y = processor). For example, for MWAM slot 10 processor 2, configure **ip rcmd remote-host 127.0.0.102 enable**.

Recovering from Session Loss

If the session between a Supervisor module and an MWAM processor fails, Cisco recommends that you perform the following steps to attempt a recovery and collect information. The collected information can be useful in determining the cause of the session loss.

An example of an error message indicating loss of session is shown below:

```
MWAM: No response from IOS complex 1, resetting complex
MWAM: No response from IOS complex 0, resetting complex
```

To attempt recovery and collect troubleshooting information, complete the following steps:

	Command	Purpose

Step 1	After stopping traffic, do the following:
	`Sup-7606> enable`
	`Sup-7606# session slot` *slot_number* `processor 1`
		Enters privileged EXEC mode and establishes a Telnet session to MWAM processor 1.
		Note User name is *root* and password is *cisco*.

Step 2	`root@mwam-4# show processor` *processor_number*	Displays information about the suspect MWAM processor.
Step 3	`root@mwam-4# show tech-support`	Displays information about the MWAM processors for technical support personnel.
Step 4	`root@mwam-4# reload processor` *processor_number*	Reloads the suspect MWAM processor.
Step 5	`Sup-7606# session slot` *slot_number* `processor` *processor_number (2-6)*	Establishes a session to the suspect MWAM processor.
Step 6	`mwam-4-2> enable`	Enters privileged EXEC mode of the MWAM processor.
Step 7	`mwam-4-2# show version`	Displays version information about the MWAM processor.
Step 8	`mwam-4-2# show tech-support`	Displays information about the MWAM processor for technical support personnel.
Step 9	`mwam-4-2# dir bootflash:`	Displays the bootflash directory of the MWAM processor.

The following example illustrates these steps:

```
Sup-7606# session slot 4 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.51 ... Open

SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct  3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
Kernel 2.4.10.komodo on an i686
login: root
Password:

SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct  3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
```

```
root@mwam-4# show processor 2
Processor 2, Complex 1, Core 0
  Complex Status is Online
  Information
  Health Monitoring
    0 User Resets, 0 IOS Reloads, 0 Unknown Resets
    0 Timeouts
    0 Consecutive heartbearts missed
    108878/108878 Heartbeats acked since last reset
    0% CPU Utilization
  Messages
    1831/1831 VRTC Update(s) acked by PC
    108878/108878 Heartbeats(s) acked from IOS
    0/0 ROMMON Config Msg(s) acked from ROMMON
    0/0 Supervisor Switchover Msg(s) acked from IOS
    0/0 Prepare Reload Msg(s) acked from IOS

root@mwam-4# show tech-support
-------------------------- show version --------------------------

SVCMWAM Image version 2.1(1.0)
Mon Feb 23 01:29:45 EST 2004
Copyright (c) 2002-2003, 2004 by cisco Systems, Inc.
All rights reserved.

~snipped~

root@mwam-4# reload processor 2
root@mwam-4#
Jun 16 01:55:22.575: %SVCLC-SP-5-STRRECVD: mod 4: <MWAM: Resetting complex 1 at
user request.>
~snipped~

Sup-7606# session slot 4 processor 2
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open

mwam-4-2#

Press RETURN to get started!

mwam-4-2> enable
mwam-4-2# show version
Cisco IOS Software, MWAM Software (MWAM-G4JS-M), Version 12.3(7)T1, RELEASE SOFT
WARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 22-Apr-04 06:59 by eaarmas

ROM: System Bootstrap, Version 12.2(11)YS RELEASE SOFTWARE

Router uptime is 1 day, 6 hours, 47 minutes
System returned to ROM by power-on
System restarted at 16:06:07 IST Mon Jun 14 2004
Running default software

Cisco MWAM (MWAM) processor with 473088K/32768K bytes of memory.
SB-1 CPU at 700MHz, Implementation 1, Rev 0.2

Last reset from power-on
1 Gigabit Ethernet interface
511K bytes of non-volatile configuration memory.
```

```
Configuration register is 0x0


mwam-4-2# show tech-support
-------------------------- show version --------------------------

~snipped~


mwam-4-2# dir bootflash:

Directory of bootflash:/

    0  -rw-        3107  Feb 25 2004 09:48:28 +05:30  running-config

524288 bytes total (520797 bytes free)
```

APPENDIX A

Command Reference

This appendix contains an alphabetical listing of new and revised commands specific to the MWAM configuration. The commands are categorized according to the console from which they are executed.

Note All other commands used with this product (those that already exist and have not been modified) are documented in the Cisco IOS 12.3 command reference publications.

Supervisor Console Commands

The following commands are available at the Supervisor console:

Processor Control Commands

The Processor Control (PC) commands are available when you session into MWAM processor 1 from the Supervisor console. The PC commands provide various functions for the MWAM processors.

To access the PC commands, use the **session slot** command to establish a connection to processor 1. Then log into the PC as *root* user with the password *cisco*.

- **boot-mode**
- **normal-ios**
- **recover-ios**
- **reload**
- **restore ios**
- **show boot-mode**
- **show images**
- **show log**
- **show processor**
- **show tech-support**
- **show version**

MWAM Console Commands

The following commands are available at the MWAM console:

- **memory-size iomem**
- **mwam config-mode**
- **show mwam**
- **show mwam config-mode**

Supervisor Console Commands

The following commands are available at the Supervisor console.

clear logging slot

To clear the following slave log options that are enabled on the MWAM:

- timeouts
- logevents
- sequence errors
- reset count
- KPA_missed counters

Use the **clear logging slot** command in privileged EXEC mode.

clear logging slot *slot_number* **counts**

Syntax Description

slot_number	Specifies the slot that the module is plugged into.

Defaults

There are no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.

Usage Guidelines

Use this command to clear the slave log options that are enabled.

Examples

The following example illustrates the **clear logging slot** command:

```
Router# clear logging slot 6 counts
```

execute-on

To initiate a remote command request on an MWAM processor from the Supervisor console, use the **execute-on** command in privileged EXEC mode.

execute-on {*slot_number* | **all**} {*processor_number* | **all**} *command* [*subcommand*]

Syntax Description

slot_number	Specifies the slot that the module is plugged into.
all	Specifies all the MWAMs in the chassis.[1]
processor_number	Specifies the processor number within the MWAM.
all	Specifies all the processors in the MWAM.[1]
command	Specifies the command to execute on the MWAM processor. The following commands are supported: • **debug** • **dir** • **show** • **systat** • **undebug** • **ping** *ip_addr* • **log** {**show** | **systat** | **dir**} The commands of the PC are also supported (see "Processor Control Commands" section on page A-2).
subcommand	(Optional) Additional parameters to be included with the command and executed by the remote processor. **Note** No Help is available for the *parameter* portion of the command.

1. When using the **all** option, the command is executed on all active processors but is not executed on processors that are inactive. The processor state can be shown using the **show logging** command.

Defaults

There are no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.
12.3(5a)B	Added remote console support for PC commands.

Usage Guidelines

The remote console and logging feature must be configured to use the **execute-on** command (see the "Configuring Remote Console and Logging" section on page 6-16).

When using the **all** options, the designated command is executed on all active processors. Inactive processors are ignored. Use the **show logging** command to determine if the processor is active.

To terminate a remote command that is in progress, the user can activate the escape sequence defined on the Supervisor console. For example, if a user initiates a **log show** command on a remote MWAM processor and the command execution is longer than expected, the user can terminate the command from the Supervisor console by entering **Ctrl-^**. To determine the escape sequence for your console/vty connection, use the **show line** *line_number* command.

Examples The following example executes the **log show running-config** command on processor 2 of the MWAM in slot 5.

```
Sup-7600# execute-on 5 2 log show running-config
```

logging listen mwam

To configure MWAM logging input to the Supervisor from an MWAM in the chassis, use the **logging listen mwam** command in global configuration mode. To remove this configuration, use the **no** form of the command.

logging listen mwam *udp_port*

no logging listen mwam *udp_port*

Syntax Description

udp_port	Specifies the UDP port on the Supervisor module for listening to logs from MWAM(s) in the chassis. This command is required to enable the remote console and logging feature. A UDP port must be defined at both the Supervisor and the MWAM, and the defined ports must match. The port range is 4000-10000. The port must be divisible by 100 (for MWAM processor identification).

Defaults There are no default behavior or values.

Command Modes Global configuration

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.

Usage Guidelines Use this command to specify the Supervisor UDP port for listening to MWAM logging. Use the **logging main-cpu** command from the MWAM console to enable slave log generation to the Supervisor. Ensure that the UDP ports defined at both the Supervisor and MWAM are the same.

When selecting the UDP port for an MWAM processor, you are defining a base UDP port used at the Supervisor. Two additional source ports, based on the selected port, are then automatically defined.

For example, on the Supervisor you have configured the following:

```
logging listen mwam 10000
```

On the MWAM, you have configured processor 2 as follows:

```
logging main-cpu 10000 emergencies 99.99.99.99
```

The Supervisor listens on port 10000 and uses this port as its base UDP port. Ports 10002 and 10012 are automatically defined for traffic streams. On MWAM processor 3, the defined ports would be 10003 and 10013. The port numbering pattern for the additional ports is shown here:

MWAM Processor:	2	3	4	5	6
Base UDP Port:[1]	<40-100>00	<40-100>00	<40-100>00	<40-100>00	<40-100>00
Additional UDP Port:	<40-100>02	<40-100>03	<40-100>04	<40-100>05	<40-100>06
Additional UDP Port:	<40-100>12	<40-100>13	<40-100>14	<40-100>15	<40-100>16

1. Must be in the range 4000-10000 and be a multiple of 100.

The port numbering pattern is important if you are configuring other UDP ports on either the Supervisor or the MWAM processor.

Examples

The following example illustrates the **logging listen mwam** command:

```
Router(config)# logging listen mwam 4100
```

mwam bootflash access

Note The MWAM bootflash access must be enabled if you want to operate in Supervisor mode.

To enable file transfer requests between the Supervisor bootflash and the individual processors on the MWAM, use the **mwam bootflash access** command in configuration mode. To remove this configuration, use the **no** form of the command.

mwam bootflash access

no mwam bootflash access

Syntax Description

mwam bootflash access	Configures bootflash access for MWAM file transfer requests.

Defaults

MWAM bootflash access is enabled by default. To disable access, issue **no mwam bootflash access**.

Command Modes

Supervisor configuration

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.

Usage Guidelines Use the **no** form of this command to disable MWAM access to the Supervisor bootflash.

Examples The following example illustrates the **mwam bootflash access** command:

```
Sup-7606(config)# mwam bootflash access
```

mwam module allowed-vlan

To configure the Ethernet connectivity from the backplane (that is, switch fabric) to the individual processors on the MWAM, use the **mwam module allowed-vlan** command in global configuration mode. To remove this configuration, use the **no** form of the command.

mwam module *slot_number* **port** *port_number* **allowed-vlan** *vlan-list*

no mwam module *slot_number* **port** *port_number* **allowed-vlan** *vlan-list*

Syntax Description

slot_number	Specifies the slot that the module is plugged into.
port *port_number*	Specifies the actual port number (1-3) used to connect to a processor complex within the MWAM (Figure 1-2 on page 1-5 shows the port layout).
allowed-vlan *vlan-list*	Configures the appropriate VLANs for this port.

Defaults There are no default behavior or values.

Command Modes Global configuration

Command History

Release	Modification
12.2(9)ZA	This command was introduced.

Usage Guidelines Each processor is connected to the backplane (that is, switch fabric) through an Ethernet port connection. When both processors within a complex are enabled, they are required to share the Ethernet port connection, thus their port configurations must be in common.

See Figure 1-2 on page 1-5 and Table 1-2 on page 1-5 to determine which port corresponds to each processor.

Examples The following example illustrates the **mwam module allowed-vlan** command:

```
Router(config)# mwam module 4 port 2 allowed-vlan 101
```

mwam module cpu logging

To configure the severity level of MWAM logging information to send to the Supervisor module, use the **mwam module cpu logging** command in global configuration mode. To remove this configuration, use the **no** form of the command.

mwam module {*slot_number* | **all**} **cpu** {*processor_number* | **all**} **logging** *log_level*

no mwam module {*slot_number* | **all**} **cpu** {*processor_number* | **all**} **logging** *log_level*

Syntax Description

slot_number | **all**	Specifies the slot that the module is plugged into or all MWAMs in the chassis
cpu_number | **all**	Specifies the processor on the MWAM or all processors on the MWAM.
log_level	Limits the logging of messages to be sent to the Supervisor to a specified level (for example, if *log_level* is **critical**, then emergencies, alerts, and critical events are sent). You can enter the level number or name. • **emergencies** (severity level 0)—system is unusable • **alerts** (severity level 1)— immediate action required • **critical** (severity level 2)—critical condition • **errors** (severity level 3)—error condition • **warnings** (severity level 4)—warning condition • **notifications** (severity level 5)—normal but significant condition • **informational** (severity level 6)—informational message • **debugging** (severity level 7)—debug messages

Defaults

The default configuration is logging enabled on all MWAM processors for emergencies.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.

Usage Guidelines

Logging methods may require additional configuration such as the destination IP address for the receiver of the log traffic. To configure the destination IP address, use the **logging main-cpu** command.

Examples

The following example sets the logging level for all MWAM processors in the chassis to the error logging level:

```
Sup-7600(config)# mwam module all cpu all logging error
```

The following example allows the Supervisor console to display debugging log messages received from processor 2 on the MWAM in slot 5:

```
Sup-7600(config)#mwam module 5 cpu 2 logging debug
```

mwam module vlan-based

To assign MWAM traffic to a VLAN QoS policy, use the **mwam module vlan-based** command in global configuration mode. To remove this configuration, use the **no** form of the command.

mwam module *slot_number* **port** *port_number* **vlan-based**

no mwam module *slot_number* **port** *port_number* **vlan-based**

Syntax Description

slot_number	Specifies the slot that the module is plugged into.
port_number	Specifies one of three switch fabric interface ports (1-3) that connect the Supervisor module to the MWAM.

Defaults

There are no default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)ZA7	This command was introduced.

Usage Guidelines

Use this command to assign MWAM traffic to a VLAN QoS policy.

See Figure 1-2 on page 1-5 and Table 1-2 on page 1-5 to determine which port corresponds to each processor.

Examples

The following example illustrates the **mwam module vlan-based** command:

```
Sup-7606(config)# mwam module 5 port 1 vlan-based
Sup-7606(config)# mwam module 5 port 2 vlan-based
Sup-7606(config)# mwam module 5 port 3 vlan-based
```

session slot

To establish a command session to a processor on an MWAM, use the **session slot** command in privileged EXEC mode.

session slot *slot_number* **processor** *processor_number*

Syntax Description

slot_number	Specifies the slot that the MWAM is plugged into.
processor *processor_number*	Specifies the MWAM processor (1-6) to connect to. **Note** Only MWAM processors 2-6 contain application images; MWAM processor 1 provides control commands for MWAM processors and complexes.

Defaults

There are no default behavior or values.

Command Modes

EXEC mode.

Command History

Release	Modification
12.2(9)ZA	This command was introduced.

Usage Guidelines

When you session into processor 1, you must enter the user name (*root*) and password (*cisco*).

Examples

The following example illustrates the **session slot** command for processor 2 on the MWAM in slot 9:

```
Sup-7606#session slot 9 processor 2
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.92 ... Open

proc2-9>


Press RETURN to get started!


proc2-9>
```

The following example illustrates the **session slot** command for processor 1 on the MWAM in slot 9:

```
Sup-7606#session slot 9 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open


SVCMWAM Image version 2.1(0.1b)
```

```
Tue Oct 14 11:04:43 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
Kernel 2.4.10.komodo on an i686
login: root
Password:

SVCMWAM Image version 2.1(0.1b)
Tue Oct 14 11:04:43 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.



SVCMWAM Image version 2.1(0.1b)
Tue Oct 14 11:04:43 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.


root@mwam-9#
```

show logging

To display the slave log options that are enabled on the MWAM, use the **show logging** command in privileged EXEC mode.

show logging {**slot** *slot_number* | **summary**}

Syntax Description

slot_number	Specifies the slot that the module is plugged into.
summary	Displays logging information for all MWAMs in the chassis.

Defaults

There are no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.
12.2(14)ZA5	The output of this command was modified to incorporate improvements in the display of information.

Usage Guidelines

Use this command to display the slave log options that are enabled.

Examples

The following example illustrates the **show logging** command:

```
Router# show logging slot 5
  CPU: 05/2      State: ACTIVE         Command Active: No
  ttynum: -1                 Logging Level: debugging
  timeouts:                1 logevents:             0
  sequence errors:         0 reset count:       16001 KPA_missed: 4294967201
  send seq:                5 tty recv seq:          0 log recv seq: 0
  Current queue count:     0 IP addr: 172.18.48.94
.
.
.
```

Note Each processor (CPU) on the MWAM in slot 5 is displayed in the output.

Field descriptions for the output of this command are listed below:

Active	Processor is operational and remote console/logging is active.
Online	Processor is operational but remote console/logging is not active. **Note** This state commonly occurs when a processor is not enabled by the application running on the MWAM.
Inactive	Processor is rest or resetting, and remote console/logging is inactive.
Proving	The remote console connection is testing the IP path between the Supervisor and MWAM processor before moving to the ACTIVE state. If there is a configuration problem or VLAN mismatch, the connection may stay in Proving state until the configuration issue is resolved.
ttynum	Line number of the user with an active command on the processor. A value of -1 indicates no user.
Logging Level	Indicates the maximum severity level at which the Supervisor displays logger messages from an MWAM.
timeouts	Number of occurrences of remote command execution time-out.
logevents	Number of logging events.
sequence errors	Protocol sequence errors caused by overrun or time-out.
reset count	Number of times the connection reset because of connection time-out or MWAM processor reload.
KPA_missed	Number of keepalives missed.
send seq	Sequence number of remote commands sent.
tty recv seq	Sequence number of remote command response messages received from the MWAM processor.
log recv seq	Sequence number of remote logging messages received from the MWAM processor.
Current queue count	Number of messages received at the Supervisor and queued to be processed (logged/displayed).
IP addr	IP address of the MWAM processor. **Note** Typically, this is an internal address, but it can be a defined address, such as the one shown in processor 6 (06/6) in the example. Use the **logging main-cpu** command on the MWAM processor to define a different IP address, if required.

show mwam module

To display connectivity information about the individual processors on the MWAM, use the **show mwam module** command in privileged EXEC mode.

show mwam module *slot_number* **port** *port_number* {**state** | **traffic**}

Syntax Description

slot_number	Displays the slot that the module is plugged into.
port *port_number*	Displays the actual port number (1-3) used to connect to a processor complex within an MWAM (see Figure 1-2 on page 1-5).
state	Displays the interface status.
traffic	Displays the interface statistics.

Defaults

There are no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(9)ZA	This command was introduced.

Examples

The following example illustrates the **show mwam module** command:

```
Sup-7606#sho mwam mod 7 port 1 state
Mwam module 7 data-port 1:
 Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-999
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1-999
Vlans allowed and active in management domain:1,3,11-12,17,60
Vlans in spanning tree forwarding state and not pruned:
   1,3,11-12,17,60
Allowed-vlan : 1-999

Sup-7606#sho mwam mod 7 port 1 traffic
Specified interface is up line protocol is up
  Hardware is C6k 1000Mb 802.3, address is 0010.7b00.0cb0 (bia 0010.7b00.0cb0)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  Last input never, output never, output hang never
```

```
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 67
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 3 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     46504312 packets output, 2501255885 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

Sup-7606#sho mwam mod 7 port 2 state
Mwam module 7 data-port 2:
 Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-999
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1-999
Vlans allowed and active in management domain:1,3,11-12,17,60
Vlans in spanning tree forwarding state and not pruned:
   1,3,11-12,17,60
Allowed-vlan : 1-999

Sup-7606#sho mwam mod 7 port 2 traffic
Specified interface is up line protocol is up
  Hardware is C6k 1000Mb 802.3, address is 0010.7b00.0cb1 (bia 0010.7b00.0cb1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  Last input 00:00:09, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 68
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     24922473 packets input, 430882532 bytes, 0 no buffer
     Received 93145 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     26261319 packets output, 4263983434 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

Sup-7606#sho mwam mod 7 port 3 state
Mwam module 7 data-port 3:
 Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
```

```
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-999
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1-999
Vlans allowed and active in management domain:1,3,11-12,17,60
Vlans in spanning tree forwarding state and not pruned:
   1,3,11-12,17,60
Allowed-vlan : 1-999

Sup-7606#sho mwam mod 7 port 3 traffic
Specified interface is up line protocol is up
  Hardware is C6k 1000Mb 802.3, address is 0010.7b00.0cb2 (bia 0010.7b00.0cb2)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  Last input 00:00:11, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 22
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
     35270 packets input, 5189978 bytes, 0 no buffer
     Received 4444 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     46510270 packets output, 2501832096 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Processor Control Commands

The following PC commands are available when you session into the MWAM processor.

boot-mode

To set the MWAM configuration file storage mode when debugging problems, use the **boot-mode** command available at the PC complex (processor 1 on the MWAM).

boot-mode {**local** | **supervisor**} [*complex_number* | **all]**

Syntax Description

boot-mode	Sets the MWAM configuration file storage mode.
local	Stores configuration files locally in NVRAM of the MWAM processor.
supervisor	Stores configuration files in the Supervisor bootflash.
complex_number | **all**	Changes the mode on the processors in complex 0, 1, or 2 or on all the complexes. Use the **show map** command to see the processor-to-complex mapping. Optional. If not entered, all complexes are affected.

Defaults

Default setting is Supervisor mode.

Command Modes

PC command

Command History

Release	Modification
12.3(11)T	This command is introduced.

Usage Guidelines

Use this command when you are experiencing problems with the MWAM configuration download. For example, if there is a problem with loading the configuration in the current mode, you can use this command to interrupt the download and change the mode. To use this command, first enable MWAM access to the Supervisor bootflash with the **mwam bootflash access** command from the Supervisor console.

For normal operation, set the configuration mode with the **show mwam config-mode** command from the MWAM console.

Examples

The following examples illustrate the **boot-mode** command.

This example sets the **boot-mode** for local when the next reboot is performed.

```
root@mwam-9#boot-mode local
Complex(s) 0, 1, 2 in slot 9 must be reloaded for changes to take effect.
If the MWAM in slot 9 is shutdown/reset before the complexes are
reloaded then these changes will be lost.
root@mwam-9#show boot-mode
Complex 0 : Local config mode upon next complex reload
Complex 1 : Local config mode upon next complex reload
Complex 2 : Local config mode upon next complex reload
root@mwam-9#
```

This example sets the **boot-mode** for supervisor when the next reboot is performed.

```
root@mwam-9#boot-mode sup
Complex(s) 0, 1, 2 in slot 9 must be reloaded for changes to take effect.
If the MWAM in slot 9 is shutdown/reset before the complexes are
reloaded then these changes will be lost.
root@mwam-9#show boot-mode
Complex 0 : Supervisor config mode upon next complex reload
Complex 1 : Supervisor config mode upon next complex reload
Complex 2 : Supervisor config mode upon next complex reload
root@mwam-9#
```

normal-ios

To set the configuration register to boot with a normal configuration, use the **normal-ios** command available at the PC complex (processor 1 on the MWAM).

normal-ios

Syntax Description

normal-ios	Sets the configuration register to boot with a normal configuration.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.(9)ZA	This command was introduced.

Usage Guidelines

Use this command to set the configuration register to boot using the normal startup configuration. This command resets the effects of the **recover-ios** command. It is used in the "Recovering from MWAM Processor Lockout" section on page 6-19.

Note You must first establish a session to processor 1 (session slot command).

Examples The following example illustrates the **normal-ios** command:

```
root@mwam-9#normal-ios
Base external MAC: "0003.FEAB.9FB6"
Internet Software Consortium DHCP Server V3.0.1rc6
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
Listening on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Sending on   LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Listening on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   Socket/fallback/fallback-net
root@mwam-9#
```

recover-ios

To set the configuration register to boot with a clean configuration, use the **recover-ios** command available at the PC complex (processor 1 on the MWAM).

recover-ios *complex_number*

Syntax Description

complex_number	Specifies a complex (0, 1, 2, or all) on the MWAM.

Defaults There are no default behavior or values.

Command Modes PC command

Command History

Release	Modification
12.2(9)ZA	This command was introduced.

Usage Guidelines Use this command when you want to recover from a lockout condition on an MWAM processor as described in the "Recovering from MWAM Processor Lockout" section on page 6-19.

Note You must first establish a session to processor 1 (session slot command).

Examples The following example illustrates the **recover-ios** command on processor complex 2 of the MWAM in slot 9:

```
root@mwam-9#recover-ios 2
processing -p
processing -c
```

```
Setting DHCP options for processor complex 2
Setting config-reg value to: 0x40
Base external MAC: "0003.FEAB.9FB6"
Internet Software Consortium DHCP Server V3.0.1rc6
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
Listening on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Sending on   LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Listening on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on   Socket/fallback/fallback-net
```

reload

To reload processors on an MWAM, use the **reload** command available at the PC complex (processor 1 on the MWAM).

reload {**processor** *processor_number* | **complex** *complex_number* | **all**}

Syntax Description

processor *processor_number*	Specifies a processor (2-6) on the MWAM. **Note** Even though only one processor is specified, both processors on the complex will reload.
complex *complex_number*	Specifies a complex (0, 1, 2, or all) on the MWAM.
all	Specifies all processors on the MWAM.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.3(3)B1	This command was introduced.

Usage Guidelines

Use this command when you want to reload MWAM processors or complexes. When you reload a single processor, the other processor on the complex will also reload. See Table 1-2 on page 1-5 for processor-to-complex mapping.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following examples illustrate the **reload** command.

This example reloads processors 4 and 5 on complex 2 of the MWAM in slot 9:

```
root@mwam-9#reload complex 2
```

This example also reloads processors 4 and 5 on complex 2 of the MWAM in slot 9:

```
root@mwam-9#reload processor 4
```

This example reloads processors 2-6 of the MWAM in slot 9:

```
root@mwam-9#reload all
```

restore ios

To restore the previously loaded IOS image and ROM-Monitor image, use the **restore** command available at the PC complex (processor 1 on the MWAM).

restore ios

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.3(5a)B	This command was introduced.

Usage Guidelines

Use this command to restore the previously loaded IOS image on the MWAM. You must then reload the MWAM or the individual processors to activate the image. You can revert to the previous image only if you have not rebooted/recycled the MWAM.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following example illustrates the **restore** command:

```
root@mwam-9#restore ios
Restoring image
Restoring configuration files
Operation completed successfully
root@mwam-9#
```

show boot-mode

To show the processor complexes that will be configured in either local or Supervisor mode stored on the MWAM, use the **show boot-mode** command available at the PC complex (processor 1 on the MWAM).

show boot-mode

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.3(11)T	This command is introduced.

Usage Guidelines

Use this command to show the processor complexes that will be configured in either Local or Supervisor mode when the next complex is reloaded on the MWAM.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following examples illustrate the **show boot-mode** command:

This example shows the **boot-mode** for local when the next reboot is performed.

```
root@mwam-9#boot-mode local
Complex(s) 0, 1, 2 in slot 9 must be reloaded for changes to take effect.
If the MWAM in slot 9 is shutdown/reset before the complexes are
reloaded then these changes will be lost.
root@mwam-9#show boot-mode
Complex 0 : Local config mode upon next complex reload
Complex 1 : Local config mode upon next complex reload
Complex 2 : Local config mode upon next complex reload
root@mwam-9#
```

This example shows the **boot-mode** for Supervisor when the next reboot is performed.

```
root@mwam-9#boot-mode sup
Complex(s) 0, 1, 2 in slot 9 must be reloaded for changes to take effect.
If the MWAM in slot 9 is shutdown/reset before the complexes are
reloaded then these changes will be lost.
root@mwam-9#show boot-mode
Complex 0 : Supervisor config mode upon next complex reload
Complex 1 : Supervisor config mode upon next complex reload
Complex 2 : Supervisor config mode upon next complex reload
root@mwam-9#
```

show images

To list the images stored on the MWAM, use the **show images** command available at the PC complex (processor 1 on the MWAM).

show images

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.(9)ZA	This command was introduced.

Usage Guidelines

Use this command to list the image names on the MWAM.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following example illustrates the **show images** command:

```
root@mwam-9#show images
Device name          Partition#         Image name
-----------          ----------         ----------
Compact flash(cf)    6                  SIMPSON_RAM.bin
Version Information:
Compiled Tue 19-Aug-03 13:35 by dchih
Compact flash(cf)    6                  svcmwam-js-mz.geo_t_040121
Version Information:
Compiled Wed 21-Jan-04 02:34 by $

AP software is c6svcmwam-js-mz.geo_t_040121.2-1-0-3b.6cpu.bin
root@mwam-9#
```

show log

To show the upgrade or restart logs, use the **show log** command available at the PC complex (processor 1 on the MWAM).

show log {**upgrade** | **restart**}

Syntax Description

upgrade	Shows the upgrade log.
restart	Shows the MWAM and process restart log.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.3(3)B1	This command was introduced.

Usage Guidelines

Use this command when you want to display the contents of the upgrade log.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following examples illustrate the **show log** command:

```
root@mwam-4#show log upgrade
Log 'upgrade' is not available.
root@mwam-4

root@mwam-4# show log restart

MWAM started on Fri Jan  1 00:02:20 UTC 1988

Restarting rcal on Fri Jan  1 00:02:24 UTC 1988

MWAM started on Fri Jan  1 00:02:20 UTC 1988
MWAM shutdown on Mon Jun 14 15:29:47 UTC 2004

MWAM started on Fri Jan  1 00:02:22 UTC 1988
root@mwam-4#
```

show processor

To show status information about an MWAM processor, use the **show processor** command available at the PC complex (processor 1 on the MWAM).

show processor {*processor_number* | **all**}

Syntax Description

show processor	Shows status information for the MWAM processor.
processor_number	Specifies the MWAM processor number (2-6).
all	Specifies all processors on the MWAM.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.3(3)B1	This command was introduced.

Usage Guidelines

Use this command when you want to show the status of one or more MWAM processors.

Note You must first establish a session to processor 1 (session slot command).

The output of this command provides the following counter information:

Counter	Description
User Resets	Number of times the user manually reloaded the processor
IOS Reloads	Number of times the user issued the **reload** command on the processor itself
Unknown Resets	Number of times the processor reset without a known cause (for example, IOS crash)
Timeouts	Number of times the processor complex stopped responding to heartbeats

Examples

The following example illustrates the **show processor** command for processor 2 in slot 9:

```
root@mwam-9#show processor 2

Processor 2, Complex 1, Core 0
  Complex Status is Online
  Information
  Health Monitoring
    0 User Resets, 0 IOS Reloads, 0 Unknown Resets
    0 Timeouts
```

```
    0 Consecutive heartbeats missed
    244528/244528 Heartbeats acked since last reset
    0% CPU Utilization
  Messages
    4115/4115 VRTC Update(s) acked by PC
    244528/244528 Heartbeats(s) acked from IOS
    1/1 ROMMON Config Msg(s) acked from ROMMON
    0/0 Supervisor Switchover Msg(s) acked from IOS
    0/0 Prepare Reload Msg(s) acked from IOS
root@mwam-9#
```

show tech-support

To display general information about the MWAM and its processors when it reports a problem, use the **show tech-support** command available at the PC complex (processor 1 on the MWAM).

show tech-support

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.(9)ZA	This command was introduced.

Usage Guidelines

The **show tech-support** command from the PC displays the output of a number of show commands. The **show tech-support** command is useful for collecting a lot of information for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following example illustrates the **show tech-support** command:

```
root@mwam-4# show tech-support
-------------------------- show version --------------------------

SVCMWAM Image version 2.1(1.0)
Mon Feb 23 01:29:45 EST 2004
Copyright (c) 2002-2003, 2004 by cisco Systems, Inc.
All rights reserved.

~snipped~
```

show version

To display information about the currently loaded software version along with hardware and device information, use the **show version** command available at the PC complex (processor 1 on the MWAM).

show version

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default behavior or values.

Command Modes

PC command

Command History

Release	Modification
12.(9)ZA	This command was introduced.

Usage Guidelines

The **show version** command from the PC displays information about the software version currently running on the MWAM.

Note You must first establish a session to processor 1 (session slot command).

Examples

The following example illustrates the **show version** command:

```
root@mwam-4# show version

SVCMWAM Image version 2.1(1.0)
Mon Feb 23 01:29:45 EST 2004
Copyright (c) 2002-2003, 2004 by cisco Systems, Inc.
All rights reserved.

AP software is c6svc-5mwam-g4js-bf21_10.123-7.T1
AP software is based upon Maintenance image version: 3.1(0.2)
IOS Software is svcmwam-g4js-mz.123-7.T1
5 Processor Configuration

Line Card Number :WS-SVC-MWAM-1
Number of Pentium-class Processors :       1
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.4
Total available memory: 500 MB
Size of compact flash: 122 MB

root@mwam-4#
```

MWAM Console Commands

The following commands are available at the MWAM console.

memory-size iomem

By default, 32 MB is allocated for the IO memory on each processor of a Cisco MWAM router. However, the **memory-size iomem** command can be used to reallocate the IO memory from the total available DRAM space. The **no** form of the **iomem** command is used to revert to the default memory allocation.

The **iomem** configuration command is available on processors 2, 4, or 6, and when configured, it will be applied to the respective partner processors 3, 5, or 7. When 1 or 2 GB of total DRAM is available per MWAM processor complex, the permitted values for the IO memory are 32 MB, 64 MB, and 128 MB. When 512 MB of total DRAM is available per MWAM processor complex, only the default 32 MB IO memory option is available. After the IO memory is specified in the command line, the remaining DRAM memory will be used for processor memory. After configuration, it must be saved and reloaded for the reallocation to occur.

memory-size iomem [32 64 128]

Syntax Description

32, 64, or 128	Specifies the size of the DRAM allocated to the I/O memory. When an MWAM processor complex has 1 or 2 GB of DRAM memory, the values permitted are 32 MB, 64 MB, and 128 MB. When an MWAM processor complex has 512 MB of DRAM memory, the value permitted is 32 MB.

Defaults

Default value is 32 MB for I/O memory on each processor.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(12)	This command was introduced.

Usage Guidelines

When you specify the amount of IO memory in the command line, the processor memory automatically acquires the remaining DRAM memory.

Examples

The following example allocates 64 MB of DRAM memory to the I/O memory and the remaining memory to the processor memory:

```
Supervisor# session slot 7 processor 2
The default escape character i is Ctrl-^, then x. You can also type exit at the remote
prompt to end the session.
Typing 127.0.0.72 . . . open
mwmam-sibyte2>
Press Enter to get started.
```

```
mwmam-sibyte2> enable
mwmam-sibyte2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# memory-size iomem 64
Router(config)# exit
Router# copy system:running-config nvram:startup-config
Building configuration...
[OK]
Router# reload
```

logging main-cpu

To configure MWAM log redirection to the Supervisor for all events up to a maximum specified log level, use the **logging main-cpu** command in global configuration mode. To remove this configuration, use the **no** form of the command.

logging main-cpu *udp_port* [*log_level*] [*ip_addr*]

no logging main-cpu *udp_port* [*log_level*] [*ip_addr*]

Syntax Description

udp_port	Specifies the UDP port on the MWAM for sending logs to the Supervisor. A UDP port must be defined at both the Supervisor and the MWAM, and the ports must match. The port range is 4000-10000. The port must be divisible by 100.
log_level	(Optional) Limits the logging of messages displayed on the console terminal to a specified level (for example, if *log_level* is **critical**, then emergencies, alerts, and critical events are sent). You can enter the level number or name. • **emergencies** (severity level 0)—system is unusable • **alerts** (severity level 1)— immediate action required • **critical** (severity level 2)—critical condition • **errors** (severity level 3)—error condition • **warnings** (severity level 4)—warning condition • **notifications** (severity level 5)—normal but significant condition • **informational** (severity level 6)—informational message • **debugging** (severity level 7)—debug messages
ip_addr	(Optional) Specifies an IP address for traffic flow through the switching fabric instead of the EOBC. You can use this option to direct traffic on a dedicated management VLAN.

Defaults

Default value for the log level is **errors** (3).

Command Modes

Global configuration

Command History

Release	Modification
12.3(1a)BW	This command was introduced.

Usage Guidelines

Use this command to specify the MWAM UDP port for sending MWAM logs to the Supervisor. Use the **logging listen mwam** command from the Supervisor console to enable MWAM log input to the Supervisor. Ensure that the UDP ports defined at both the Supervisor and MWAM are the same.

When selecting the UDP port for an MWAM processor, you are defining a base UDP port used at the Supervisor. Two additional source ports, based on the selected port, are then automatically defined.

For example, on the Supervisor you have configured the following:

```
logging listen mwam 10000
```

On the MWAM, you have configured processor 2 as follows:

```
logging main-cpu 10000 emergencies 99.99.99.99
```

The Supervisor listens on port 10000 and uses this port as its base UDP port. Ports 10002 and 10012 are automatically defined for traffic streams. On MWAM processor 3, the defined ports would be 10003 and 10013. The port numbering pattern for the additional ports is shown here:

MWAM Processor:	2	3	4	5	6
Base UDP Port:[1]	<40-100>00	<40-100>00	<40-100>00	<40-100>00	<40-100>00
Additional UDP Port:	<40-100>02	<40-100>03	<40-100>04	<40-100>05	<40-100>06
Additional UDP Port:	<40-100>12	<40-100>13	<40-100>14	<40-100>15	<40-100>16

1. Must be in the range 4000-10000 and be a multiple of 100.

The port numbering pattern is important if you are configuring other UDP ports on either the Supervisor or the MWAM processor.

Examples

The following example enables the remote console and logging feature for an MWAM processor and specifies UDP port 10000 to match the port designated on the Supervisor. There is no logging default value; therefore, this command only enables the console portion of the feature.

```
mwam-6-4(config)#logging main-cpu 10000
```

The following example enables logging messages up to level 7 (debug) to be sent to the Supervisor module. Specifying the logging level is required to direct the logging messages to the Supervisor.

```
mwam-6-4(config)#logging main-cpu 10000 debug
```

The following example includes the IP address to direct logging and console messages to the Catalyst switching fabric. This can be used by service providers that define a management VLAN between the Supervisor and each MWAM processor.

```
mwam-6-4(config)#logging main-cpu 10000 debug 172.18.48.84
```

mwam config-mode

To set the MWAM configuration file storage mode, use the **mwam config-mode** command in privileged EXEC mode from the MWAM console.

mwam config-mode {**supervisor**} **nowrite**

Syntax Description

mwam config-mode	Sets the MWAM configuration file storage mode.
supervisor	Stores configuration files in the NVRAM of the MWAM processor and the Supervisor bootflash at the same time.
nowrite	Changes the mode without changing the contents of the configuration on the Supervisor or NVRAM.

Defaults

Default setting is Supervisor mode.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1a)BW	This command was introduced.
12.3(13)T	The **nowrite** option is added.

Usage Guidelines

Use this command when you want to set the MWAM configuration file storage mode. You must first enable MWAM access to the Supervisor bootflash with the **mwam bootflash access** command from the Supervisor console.

Caution If you are operating in the Supervisor mode in a chassis that does not have redundant Supervisor modules, back up both the *startup-config* file of the Supervisor module and all *SLOT*PC*.cfg* files on the bootflash device. Failure to take this precaution could result in the loss of all MWAM configurations, along with the Supervisor configuration.

Examples

The following examples illustrate the **mwam config-mode** command:

```
mwam-6-4# mwam config-mode local
Successfully changed mode: mwam config-mode local

Building configuration...

Jul 27 12:02:51.723: %C6K_MWAM_CENTRALIZED_CONFIG-6-MODE_CHANGED: mwam config-mode changed
to mwam config-mode local[OK]
 Successfully wrote configuration to nvram.

mwam-6-4# mwam config-mode supervisor
Successfully changed mode: mwam config-mode supervisor

Writing bootflash:SLOT6PC4.cfg
Writing slavebootflash:SLOT6PC4.cfg
Building configuration...

Jul 27 12:05:12.239: %C6K_MWAM_CENTRALIZED_CONFIG-6-MODE_CHANGED: mwam config-mode changed
to mwam config-mode supervisor
Jul 27 12:05:12.319: %C6K_MWAM_CENTRALIZED_CONFIG-6-UPLD_SUCCESS: Success: config uploaded
to supervisor bootflash:
Jul 27 12:05:12.319: %C6K_MWAM_CENTRALIZED_CONFIG-6-UPLD_SUCCESS: Success: config uploaded
to supervisor slavebootflash:[OK]
 Successfully wrote configuration to supervisor(s).

mwam-6-4#mwam config-mode local nowrite
 Successfully changed mode: mwam config-mode local

mwam-6-4#
Jul 27 12:09:41.739: %C6K_MWAM_CENTRALIZED_CONFIG-6-MODE_CHANGED: mwam config-mode changed
to mwam config-mode local
mwam-6-4#
```

show mwam

To show MWAM Translation Look-aside Buffers (TLBs) and cache errors, use the **show mwam** command in privileged EXEC mode.

show mwam

Syntax Description

show mwam	Displays MWAM TLBs and cache errors.

Defaults

There are no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(5a)B	This command was introduced.

Usage Guidelines

This command can be used to provide information about TLBs and cache errors.

Examples

The following examples illustrate the **show mwam** command:

```
mwam-7-2#show mwam
Slot Number: 7, Complex Number: 1, Global Session Number: 2
  2 active cpu(s) in complex

Gi0/0 IDB: 0x235D978C, MAC address: 0005.9a38.3820
Gi0/1 IDB: 0x235F0BF8, MAC address: 0200.0000.0110, IP address: 128.0.1.2
Gi0/2 IDB: 0x23606778, MAC address: 0200.0000.0120

Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=0
 netint usec=4000, netint mask usec=200


 512k of L2 cache shared between CPU 0 and 1


TLB entries (49/64 used):
Virt Address range      Phy Address range         Attributes
0x10000000:0x101FFFFF   0x020000000:0x0201FFFFF   CacheMode=2, RW, Valid
0x10200000:0x103FFFFF   0x020200000:0x0203FFFFF   CacheMode=2, RW, Valid
0x20200000:0x203FFFFF   0x000200000:0x0003FFFFF   CacheMode=5, RO, Valid
0x20400000:0x205FFFFF   0x000400000:0x0005FFFFF   CacheMode=5, RO, Valid
0x20600000:0x207FFFFF   0x000600000:0x0007FFFFF   CacheMode=5, RO, Valid
0x20800000:0x20FFFFFF   0x000800000:0x000FFFFFF   CacheMode=5, RO, Valid
0x21000000:0x211FFFFF   0x001000000:0x0011FFFFF   CacheMode=5, RO, Valid
0x21200000:0x213FFFFF   0x001200000:0x0013FFFFF   CacheMode=5, RO, Valid
0x21400000:0x2147FFFF   0x001400000:0x00147FFFF   CacheMode=5, RO, Valid
```

```
0x21480000:0x214FFFFF   0x001480000:0x0014FFFFF   CacheMode=5, RO, Valid
0x21500000:0x2151FFFF   0x001500000:0x00151FFFF   CacheMode=5, RO, Valid
0x21520000:0x21527FFF   0x001520000:0x001527FFF   CacheMode=5, RO, Valid
0x21528000:0x2152FFFF   0x001528000:0x00152FFFF   CacheMode=5, RW, Valid
0x21530000:0x21537FFF   0x001530000:0x001537FFF   CacheMode=5, RW, Valid
0x21538000:0x2153FFFF   0x001538000:0x00153FFFF   CacheMode=5, RW, Valid
0x21540000:0x2155FFFF   0x001540000:0x00155FFFF   CacheMode=5, RW, Valid
0x21560000:0x2157FFFF   0x001560000:0x00157FFFF   CacheMode=5, RW, Valid
0x21580000:0x215FFFFF   0x001580000:0x0015FFFFF   CacheMode=5, RW, Valid
0x21600000:0x217FFFFF   0x001600000:0x0017FFFFF   CacheMode=5, RW, Valid
0x21800000:0x21FFFFFF   0x001800000:0x001FFFFFF   CacheMode=5, RW, Valid
0x22000000:0x221FFFFF   0x002000000:0x0021FFFFF   CacheMode=5, RW, Valid
0x22200000:0x2227FFFF   0x002200000:0x00227FFFF   CacheMode=5, RW, Valid
0x22280000:0x2229FFFF   0x002280000:0x00229FFFF   CacheMode=5, RW, Valid
0x222A0000:0x222BFFFF   0x0022A0000:0x0022BFFFF   CacheMode=5, RW, Valid
0x222C0000:0x222DFFFF   0x0022C0000:0x0022DFFFF   CacheMode=5, RW, Valid
0x222E0000:0x222FFFFF   0x0022E0000:0x0022FFFFF   CacheMode=5, RW, Valid
0x22300000:0x2237FFFF   0x002300000:0x00237FFFF   CacheMode=5, RW, Valid
0x22380000:0x223FFFFF   0x002380000:0x0023FFFFF   CacheMode=5, RW, Valid
0x22400000:0x225FFFFF   0x002400000:0x0025FFFFF   CacheMode=5, RW, Valid
0x22600000:0x227FFFFF   0x002600000:0x0027FFFFF   CacheMode=5, RW, Valid
0x22800000:0x22FFFFFF   0x002800000:0x002FFFFFF   CacheMode=5, RW, Valid
0x23000000:0x237FFFFF   0x003000000:0x0037FFFFF   CacheMode=5, RW, Valid
0x23800000:0x23FFFFFF   0x003800000:0x003FFFFFF   CacheMode=5, RW, Valid
0x24000000:0x25FFFFFF   0x080000000:0x081FFFFFF   CacheMode=5, RW, Valid
0x26000000:0x27FFFFFF   0x082000000:0x083FFFFFF   CacheMode=5, RW, Valid
0x28000000:0x29FFFFFF   0x084000000:0x085FFFFFF   CacheMode=5, RW, Valid
0x2A000000:0x2BFFFFFF   0x086000000:0x087FFFFFF   CacheMode=5, RW, Valid
0x2C000000:0x2DFFFFFF   0x090000000:0x091FFFFFF   CacheMode=5, RW, Valid
0x2E000000:0x2FFFFFFF   0x092000000:0x093FFFFFF   CacheMode=5, RW, Valid
0x30000000:0x31FFFFFF   0x094000000:0x095FFFFFF   CacheMode=5, RW, Valid
0x32000000:0x33FFFFFF   0x096000000:0x097FFFFFF   CacheMode=5, RW, Valid
0x34000000:0x35FFFFFF   0x0C0000000:0x0C1FFFFFF   CacheMode=5, RW, Valid
0x36000000:0x37FFFFFF   0x0C2000000:0x0C3FFFFFF   CacheMode=5, RW, Valid
0x38000000:0x39FFFFFF   0x0C4000000:0x0C5FFFFFF   CacheMode=5, RW, Valid
0x3A000000:0x3BFFFFFF   0x0C6000000:0x0C7FFFFFF   CacheMode=5, RW, Valid
0x3C000000:0x3C7FFFFF   0x008000000:0x0087FFFFF   CacheMode=5, RW, Valid
0x3C800000:0x3CFFFFFF   0x008800000:0x008FFFFFF   CacheMode=5, RW, Valid
0x1A000000:0x1BFFFFFF   0x00A000000:0x00BFFFFFF   CacheMode=5, RW, Valid
0x1E000000:0x1FFFFFFF   0x00E000000:0x00FFFFFFF   CacheMode=5, RW, Valid

0 spurious cache errors detected.
0 correctable ECC errors have occurred, A_BUS_L2_ERRORS: 0x0, A_BUS_MEMIO_ERRORS: 0x0
```

show mwam config-mode

To show the MWAM configuration file storage mode, use the **show mwam config-mode** command in privileged EXEC mode.

show mwam config-mode

Syntax Description

show mwam config-mode	Displays the MWAM configuration file storage mode.

Defaults

There are no default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1a)BW	This command was introduced.

Usage Guidelines

Use this command when you want to display the current file storage mode for MWAM configuration files.

Examples

The following examples illustrate the **show mwam config-mode** command:

```
mwam-6-4# show mwam config-mode
mwam config-mode local
```

```
mwam-6-6# show mwam config-mode
mwam config-mode supervisor
```

APPENDIX B

Troubleshooting

During power up, your Cisco Catalyst 6500 Series switch or Cisco 7600 Series Internet Router goes through a system check. This system check also includes all the modules (for example, the MWAM) that are installed.

If your MWAM is not powering up properly, begin troubleshooting using the procedures in this appendix. This appendix guides you through some initial checks and procedures that can solve some basic MWAM problems. It can also direct you to the appropriate document for detailed troubleshooting information and procedures to solve more complex problems.

This appendix contains general problem solving information about your Catalyst 6500 switch or Cisco 7600 router and specific problem solving information about your MWAM module in the following sections:

Tip If you cannot locate the source of the problem, contact a customer service representative for information on how to proceed. For technical support information, see the *Cisco Information Packet* publication that shipped with your product. Before you call, have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the new chassis
- Brief description of the problem
- Brief explanation of the steps you have taken to isolate the problem

For specific troubleshooting details about the Catalyst 6500 switch or Cisco 7600 router, refer to the *Troubleshooting* chapters in the following books:

- *Catalyst 6500 Series Switch Installation Guide*—Appendix E
- *Cisco 7600 Series Router Installation Guide*—Chapter 4

General Problem Solving

As you start your problem solving, you first look at the way your Catalyst 6500 switch or Cisco 7600 router is responding during power up. The key to problem solving is to isolate the problem to a specific subsystem by comparing what your switch or router is doing to what it should be doing.

The LEDs on the front panel of the switch or router enable you to determine the switch or router performance and operation. For a description of these LEDs, refer to the following books:

- *Catalyst 6500 Series Switch Installation Guide*—Appendix E
- *Cisco 7600 Series Router Installation Guide*—Chapter 4

When problem solving, consider the following:

- Power and cooling systems—Power LEDs, external power source, power cable, power supply and circuit breaker, and blower and fan. Also consider inadequate ventilation or air circulation.
- Modules—LEDs on the modules help identify a failure (see the "Front-Panel Features" section on page 1-3 for details about the MWAM STATUS LED).
- Cables—External cables that connect the router to the network.

Troubleshooting the Power and Cooling Systems

In your Catalyst 6500 switch or Cisco 7600 router, both the power LED and the fans can help you troubleshoot a power problem. The following items will help you isolate the problem (refer to the "Troubleshooting the Power Supply" section in Appendix E, "Troubleshooting" of the *Catalyst 6500 Series Switch Installation Guide* or the "Troubleshooting the Power Supply" section in Chapter 4, "Troubleshooting" of the *Cisco 7600 Series Router Installation Guide* for details*)*:

Check the following items to help isolate problems with the power supply installation:

- With the Catalyst 6500 switch or Cisco 7600 router connected to the power source, is the power LED on the front panel on?
  - If not, check the DC input, DC source, and the power supply wiring.
  - Check the power supply connection to the motherboard.
  - If the power LED is still off, the problem might be a power supply failure.
- Does the Catalyst 6500 switch or Cisco 7600 router shut down after being on a short time?
  - Check the fans. If the fans are not working, the switch or router will overheat and shut itself down.
  - If the fans are not working, check the power supply connections to the fans.
  - Ensure that the chassis intake and exhaust vents are clear.

  Check the environmental site requirements in the:
  - *Catalyst 6500 Series Switch Installation Guide*—Chapter 2
  - *Cisco 7600 Series Router Installation Guide*—Chapter 2
- Does the switch or router partially boot, but the LEDs do not go on?
  - Check for a power supply failure by inspecting the power LED on the front panel of the switch or router. If the power LED is on, the power supply is functional.
  - If the power LED is not on, refer to the *Cisco Information Packet* for warranty information or contact customer service.

Environmental Monitoring

The Catalyst 6500 switch and the Cisco 7600 router both provide environmental monitoring of their chassis components for over temperature conditions. This environmental monitoring provides an early warning indication of possible component failure to ensure safe and reliable system operation and to avoid network interruptions.

Some causes of abnormally high switch or router temperatures are:

- Fan failure
- Air conditioner failure in the room
- Air blockage to cooling vents

Take steps to correct the problem. For information about environmental operating conditions, refer to the following books:

- *Catalyst 6500 Series Switch Installation Guide*—Chapter 2
- *Cisco 7600 Series Router Installation Guide*—Chapter 2

Troubleshooting Modules

Typical module problems can be caused by the module itself, cables, or cable connections. As a rule, just verifying the status LEDs of a particular module will help you to determine any faults.

Check for the following general symptoms to help isolate a problem:

- Module is not recognized by the switch or router.
  - Make sure the module is firmly seated in its slot.
  - Check the LEDs on the module. Each module has its own set of LEDs.
  - Make sure you have a version of Cisco IOS software that supports the module.
- Module is recognized, but interface ports do not initialize.
  - Make sure the module is firmly seated in its slot.
  - Check external cable connections.
  - Make sure you have a version of Cisco IOS software that supports the module.
- Switch or router does not boot properly, or constantly or intermittently reboots.
  - Make sure the module is firmly seated in its slot.
  - Check the switch or router chassis or software. Refer to the *Cisco Information Packet* publication that shipped with your switch or router for warranty information, or contact customer service.
- Switch or router powers on and boots only when a particular module is removed.
  - Check the module. Refer to the *Cisco Information Packet* publication that accompanied your order for warranty information, or contact customer service.
- Switch or router powers on and boots only when a particular cable is disconnected.
  - There may be a problem with the module or cable. Refer to the *Cisco Information Packet* publication for warranty information, or contact customer service.

MWAM Problem Solving

In a typical MWAM problem solving situation, you would first check the following:

- The module is firmly seated in its slot.
- The installation is verified.
- The STATUS LED is on.
- The version of Cisco IOS software that supports the MWAM is installed.
- The MWAM configuration is verified.

This section also contains information that can be useful for some common problems that may affect the proper operation of the MWAM, such as:

- DIMM Issue
- Performance Tuning
- Buffer Allocation for Complex 0 CPUs

Module Seating

Note All Catalyst 6500 series switches and Cisco 7600 series internet routers support hot swapping, which lets you install, remove, replace, and rearrange the modules without turning off the system power. When the system detects that a module has been installed or removed, it runs diagnostic and discovery tests automatically, acknowledges the presence or absence of the module, and resumes system operation with no operator intervention. However, DO NOT remove the MWAM until it has shut down (see the "Front-Panel Features" section on page 1-3 and the "MWAM Shutdown" section on page 1-4 for details).

To ensure the MWAM is securely seated, see the "MWAM Installation" section on page 3-3.

Verify the installation

Note As a rule, right after installing the MWAM, you verify the installation of the MWAM.

To verify the installation of the MWAM, see the "Verifying the Installation" section on page 3-9.

STATUS LED

Verify that the MWAM STATUS LED is on. Periodically, check the STATUS LED. If the STATUS LED changes to orange or red, the MWAM has not successfully completed the boot process or may have encountered an error. For more information about the orange or red STATUS LED states, see Table 1-1 on page 1-3.

Determining the MWAM Cisco IOS Image Name

To determine the MWAM Cisco IOS image name, execute the following command at the Cisco Supervisor 2 (see the "Software Description" section on page 1-7 for more details):

```
show cdp entry *
```

You can also execute the following command at the Supervisor to determine the MWAM Cisco IOS image name:

```
session slot x processor [2-6]
```

Then issue the following command:

```
show version
```

You can also enter the following command from the privileged EXEC mode (also available through **show images** at the processor complex):

```
show version
```

Verifying the MWAM Configuration

To determine the MWAM configuration, see the "Verifying the MWAM Configuration" section on page 6-14.

DIMM Issue

The following shows a possible DIMM issue (CSCin29212) that may be solved by re-inserting the DIMM memory:

```
*** Cache Error Exception***
Cache Err Reg = 0x14001f20
instruction reference, primary cache, , tag field error, error on internal request on
SysAD Bus,
PC = 0x800fb5d4, Cause Reg = 0x20008068, Status Reg = 0x400005

%MWAM-0-CORRECTABLE_ECC_ERR: A correctable ECC error has occurred,
A_BUS-L2_ERRORS: 0x0, A_BU
A-MEMIO-ERRORS: 0xFF, A_SCD_BUS_ERR_STATUS: 0x80DC0000
RRECTABLE_ECC_ERR: A correctable ECC error has occurred.
```

MWAM Performance Tuning

You can improve system performance (by 6 to 12 percent depending on the traffic type) by turning off VLAN accounting:

```
Router# configure terminal
Router(config)# no vlan accounting
Router#
```

Maximum Buffer Allocation for Complex 0 CPUs

When upgrading processor complex images, it may be necessary to set the maximum allowable small buffer allocation for processor complex 0 to 7000 and the maximum allowable middle sized buffer allocation to 3500.

MWAM System Error Messages

Error messages may be received and reported in the system log (SysLog). This section lists these messages from the MWAM SysLog Files.

Processor Complex Resetting

When upgrading MWAM software, you may see an error message similar to the following:

```
%SVCLC-SP-5-STRRECVD: mod 5: MWAM: No response from IOS complex <complex>, resetting
complex.
```

If this occurs, you must upgrade the ROMMON image (see the "Upgrading the ROMMON Image" section on page 5-11.

Note After receiving the error message, proceed immediately to the procedure named Upgrading the ROMMON Image, page 5-11 before the error occurs again. If you are unable to perform this procedure immediately, the processor complex continues to reset at three minute intervals until the ROMMON image upgrade process is completed. The ROMMON image upgrade process should take approximately 30 seconds to complete.

Crashinfo/Crashdump

Error Message `%MWAM_FILESYSTEM-3-FC_CANNOT_FORMAT: Insufficient memory to format bootflash file system.`

Explanation The router does not have enough working storage available in heap memory to format a file system for crashinfo data. The router will function normally without a bootflash file system, however, the router cannot save information for problem analysis if it crashes.

Recommended Action Try to format the file system again at a later time or shortly after a re-boot.

Error Message `%MWAM_FILESYSTEM-3-FC_FLASH_WRITE_ERROR: Cannot write to bootflash file system:`

Explanation The router cannot write to the bootflash.

Recommended Action If the problem occurred while executing a CLI command, try the command again. If problems persist, contact Cisco technical support.

Error Message `%MWAM_FILESYSTEM-3-FC_INVALID_DIR_REQ: Cannot read or write complete %s file system.`

Explanation A CLI command attempted to copy or overwrite the full file system.

Recommended Action Copy from or to an individual file.

Error Message `%MWAM_FILESYSTEM-3-FC_DIR_IS_FULL: Cannot add %s to file system, directory is full.`

Explanation The file system directory holds a limited number of entries, and an attempt was made to add a new file when the directory was already full. This can happen even when the file system still contains free space.

Recommended Action Delete an existing file or FORMAT the file system.

Error Message `%MWAM_FILESYSTEM-6-BOOTFLASH_BUSY: Cannot access bootflash, filesystem is busy`

Explanation The MWAM bootflash does not support reading and writing at the same time. The message means that bootflash is being accessed by some other operation, like copy, dir, format or squeeze.

Recommended Action Try the bootflash operation again after other operations have completed.

Flash Error Messages

Error Message `%MWAM_FLASH-3-ERR: "%s"`

Explanation An error occurred while programming/erasing the BootFlash

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter "OUTPUT_INTERPRETER." Also perform a search of the Bug Toolkit "BUG_TOOLKIT." If you still require assistance, open a case with the Technical Assistance Center via the Internet "TAC_CASE_OPEN," or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message `%MWAM_FLASH-3-OTHER_CPU_RELOAD: "%s"`

Explanation The other CPU within this complex is reloading, flash programming operation can not proceed.

Recommended Action Wait for the system to complete the reload operation.

Error Message `MWAM_FLASH-3-FLASH_LOCKED_BY_OTHER_CPU: "%s"`

Explanation The other CPU within this complex is programming the shared flash, flash programming must complete before proceeding with reload

Recommended Action Wait for the other CPU to complete its flash programming operation, then reenter the CLI command.

NVRAM Error Messages

Error Message `%MWAM_NVRAM-3-ERR: "%s"`

Explanation An error occurred while saving/erasing the configuration from flash.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `MWAM_NVRAM-5-INFO: "%s"`

Explanation Information showing the state of the NVRAM configuration in the BootFlash.

Recommended Action If this message recurs, copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter "OUTPUT_INTERPRETER." Also perform a search of the Bug Toolkit "BUG_TOOLKIT." If you still require assistance, open a case with the Technical Assistance Center via the Internet "TAC_CASE_OPEN," or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message `%MWAM_NVRAM-5-KRUSTY_NVRAM_NOT_FOUND: "%s"`

Explanation Information indicating there is no NVRAM pointer.

Recommended Action This indicates either NVRAM has not initialized properly, or it is corrupted.

FUR Error Messages

Error Message `%MWAM_FUR-3-ERR: "%s\n"`

Explanation An error occurred while upgrading or invalidating the Field-Upgradeable ROMMON.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `%MWAM_FUR-1-INFO: "%s\n"`

Explanation Information about the Field-Upgradable ROMMON.

Recommended Action If this message recurs, copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter "OUTPUT_INTERPRETER." Also perform a search of the Bug Toolkit "BUG_TOOLKIT." If you still require assistance, open a case with the Technical Assistance Center via the Internet "TAC_CASE_OPEN," or contact your Cisco technical support representative and provide the representative with the collected information.

System Error Messages

Error Message `%MWAM-0-ADDRESS_TRAP: "Address trap: %d occurred on physical address: 0x%llx at EPC: 0x%x, ERR_EPC: 0x%x"`

Explanation A previously defined address trap has occurred.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `%MWAM-0-UNCORRECTABLE_ECC_ERR: "An uncorrectable ECC error has occurred, A_BUS_L2_ERRORS: 0x%llx, A_BUS_MEMIO_ERRORS: 0x%llx, A_SCD_BUS_ERR_STATUS: 0x%llx"`

Explanation An uncorrectable ECC error has occurred.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `%MWAM-0-CORRECTABLE_ECC_ERR: "A correctable ECC error has occurred, A_BUS_L2_ERRORS: 0x%llx, A_BUS_MEMIO_ERRORS: 0x%llx, A_SCD_BUS_ERR_STATUS: 0x%llx"`

Explanation A correctable ECC error has occurred.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

Error Message `%MWAM-0-MISDIRECTED_INTERRUPT: "A misdirected interrupt occurred with int_mask: 0x%x"`

Explanation A misdirected interrupt occurred.

Recommended Action Copy the error message exactly as it appears, and report it to your technical support representative.

GLOSSARY

A

AAA Authentication, Authorization, and Accounting. Network security services that provide the primary framework to set up access control on a router or access server. AAA is an architectural framework and modular means of configuring three independent, but closely related security functions in a consistent manner. It is flexible, scalable, and supports multiple authentication methods.

C

CCIE Cisco Certified Internetwork Expert. The CCIE program offers various CCIE certification in lab testing centers worldwide. This certification gives you an excellent opportunity to demonstrate your technical expertise, and can serve as an alternative to other CCIE designations toward fulfilling Cisco partner requirements.

CDMA Code Division Multiple Access. An access technology that combines each phone call with a code that only one cellular phone extracts from the air.

CLI Command Line Interface. An interface that uses commands entered on a command line to configure and maintain network elements. You use the CLI to access the Cisco IOS software.

E

ECC Error-Correcting Code. Memory that corrects errors on the fly.

ETSI European Telecommunications Standards Institute. The European Telecommunications Standards Institute (ETSI) is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future. ETSI is officially responsible for standardization of Information and Communication Technologies (*ICT*) within Europe. These technologies include telecommunications, broadcasting, and related areas, such as intelligent transportation and medical electronics.

F

FUR Field-Upgradeable ROMMON.

G

GGSN Gateway *GPRS* Support Node. A wireless gateway that allows mobile cell phone users to access the public data network.

GPRS General Packet Radio Service. A service designed for GSM networks. GPRS is standardized by the European Telecommunications Standards Institute (*ETSI*). Cisco Systems' GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet data services. A GPRS network has two essential elements: Serving GPRS Support Node (*SGSN*) and Gateway GPRS Support Node (*GGSN*).

H

HA Home Agent. The Home Agent maintains mobile user registrations and tunnels packets destined for the mobile to the PDSN/FA (Packet Data Serving Node/Foreign Agent). It supports reverse tunneling, and can securely tunnel packets to the *PDSN* using *IPSec*. Broadcast packets are not tunneled. Additionally, the HA performs dynamic home address assignment for the mobile. Home address assignment can be from address pools configured locally, through either DHCP server access, or from the *AAA* (Authentication, Authorization, and Accounting) server

HSRP Hot Standby Router Protocol. A Cisco routing protocol for fault-tolerant IP routing that enables a set of routers to work together to present the appearance of a single virtual router to the hosts on a LAN; used in environments where critical applications are running and fault-tolerant networks have been designed.

I

ICMP Internet Control Message Protocol. A protocol that supports packets containing error, control, and informational messages.

ICT Information and Communication Technologies. Through its core activities, working groups, and regional nodes, successfully served as a multi-stakeholder mechanism to facilitate and promote collaborative initiatives at the regional, subregional, and national levels and to mobilize new public and private resources to support information and communication technologies-for-development programs and projects. The ICT Task Force facilitated the pooling of relevant experience of both developed and developing countries and the sharing of lessons learned in introducing and promoting ICT.

IOS or Cisco IOS Cisco Internet Operating System. Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms.

IPSec Internet Protocol Security. IPSec is the network layer crypto platform for Cisco's security platforms (Cisco IOS Software, PIX, and so on). Originally described in RFCs 1825-1829, which are now obsolete, IPSec is currently discussed in a number of documents presented by the IETF IP Security Working Group. IPSec currently supports IP version 4 unicast packets. IPv6 and multicast support is coming later.

IPSec has the following strengths over current Cisco crypto offerings:

Multivendor: Since the IPSec framework is standardized, customers are not locked into any specific vendor's product. You will find IPSec on routers, firewalls, and client desktops (Windows, Mac, and so on).

Scalability: IPSec was designed with large enterprises in mind and therefore, it has "built-in" key management.

M

MSFC2 Multilayer Switch Feature Card 2. The Multilayer Switch Feature Card 2 quadruples the control plane and software forwarding performance of a Multilayer Switch Feature Card. It combines the benefits of Cisco IOS Software with the performance of the Catalyst 6000/6500 to support a broad array of features. The Multilayer Switch Feature Card 2 adds the following enhancements to the features already offered by the Multilayer Switch Feature Card:

- Four times the control plane and forwarding performance of the MSFC
- Support for Error-Correcting Code (*ECC*) DRAM with option to upgrade to 256 or 512 MB
- Full Internet routing-table support
- Support for 1000 terminated virtual LANs (VLANs)
- Field-replaceable unit for Supervisor Engine 1A already equipped with MSFC
- Enhanced Web Cache Control Protocol Version 2 (WCCPv2) and Cisco IOS server load balancing (SLB) performance
- Enhanced multicast performance

N

NE Network Element. A single piece of telecommunications equipment used to perform a function or service integral to the underlying network.

NTP Network Time Protocol. NTP is a utility for synchronizing system clocks over the network, providing a precise time base for networked workstations and servers. In the NTP model, a hierarchy of primary and secondary servers pass timekeeping information by way of the Internet to cross-check and correct errors arising from equipment or propagation failures.

P

PDSN Packet Data Serving Node. A node that provides the primary wireless mobile data access to the Internet and intranets using the CDMA2000 Radio Access Network environment.

Q

QoS Quality of Service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

R

ROMMON ROM-monitor. The ROM-monitor is a ROM-based program that is involved at power-up or reset, or when a fatal exception error occurs. The switch enters ROMMON mode if the switch does not find a valid software image, if the NVRAM configuration is corrupted, or if the configuration register is set to enter ROMMON mode. From the ROMMON mode, you can load a software image manually from Flash memory, from a network server file, or from bootflash. You can also enter ROMMON mode by restarting the switch and pressing Ctrl-C during the first five seconds of startup. When you enter ROMMON mode, the prompt changes to `rommon 1>`. Use the **?** command to see the available ROMMON commands.

RPR+ Route Processor Redundancy Plus. A redundant processor module that contains the CPU, system software, and most of the memory components that are used in a router. Sometimes called a *supervisory processor*. The RPR+ has the following additional benefits over an RPR: reduced switchover time, installed module are not reloaded, allows OIR (On-line Insertion and Removal) for maintenance, synchronization of OIR events, and manual user-initiated switchover using the **redundancy force-switchover** command.

S

SSG Service Selection Gateway. A Cisco product that provides flexible service selection, connectivity to multiple networks, and RADIUS proxy capability.

SLB Server Load Balancing. The Server Load Balancing feature is a Cisco IOS-based solution that provides server load balancing. This feature allows you to define a virtual server that represents a cluster of real servers, known as a server farm. When a client initiates a connection to the virtual server, the IOS SLB load balances the connection to a chosen real server, depending on the configured load balance algorithm or predictor.

SNMP Simple Network Management Protocol. A common method by which network management applications can query a management agent using a supported management information base.

T

TCB Transmission Control Block or Transaction Control Block. It remembers incoming and outgoing requests, providing reliable retransmission of proxied requests and returning the best final response or responses back upstream. One transaction encompasses the received request, the request or requests (if forked) forwarded downstream, responses received from downstream hosts, and the best response returned upstream.

U

UDP User Datagram Protocol. A layer 4 IP protocol that provides for exchange of datagrams without acknowledgements or guaranteed delivery.

W

WCCPv2 Web Cache Control Protocol Version 2. The Web Cache Communication Protocol (WCCP) feature allows you to use a Cisco Cache Engine to handle web traffic, reducing transmission costs and downloading time. This traffic includes user requests to view pages and graphics on World Wide Web servers, whether internal or external to your network, and the replies to those requests. When you request a page from a web server (located in the Internet), the router sends the request to a cache engine. If the cache engine has a copy of the requested page in storage, the cache engine sends you that page. Otherwise, the cache engine retrieves the requested page and the objects on that page from the web server, stores a copy of the page and its objects, and forwards the page and objects to you.

WCCP transparently redirects Hypertext Transfer Protocol (HTTP) requests from the intended server to a cache engine. You do not know that the page came from the cache engine rather than the originally requested web server.

WCCP v2 now contains the following new features:

- Multiple router support
- Improved security
- Faster throughput
- Redirection of multiple TCP port-destined traffic
- Load distributing applications capability
- Client IP addressing transparency

INDEX

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W