Cisco 10720 Internet Router Installation and Configuration Guide

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: DOC-7813062=
Text Part Number: 78-13062-10

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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Cisco 10720 Internet Router Installation and Configuration Guide

CONTENTS

Preface

Document Revison History

The revision history of this document is provided below beginning with version 78-13062-09.

Version	Date	Notes
78-13062-09	June 3, 2005	Adding warning statement numbers. cross-referenced to the *Regulatory Compliance and Safety Information for the Cisco 10720 Router* document.
78-13062-10	January, 2006	Adding two NEBS notes .

The following sections are in this Preface:

Audience

The *Cisco 10720 Internet Router Installation and Configuration Guide* is designed for the person who will install, configure, and maintain a Cisco 10720 Internet Router. This person typically will have substantial experience configuring router- or switch-based IP networks, but might or might not have experience with Cisco products and Cisco-supported protocols.

The user must be familiar with electronic circuitry and wiring practices and have experience as an electronic or electromechanical technician.

Purpose

This guide presents hardware installation and basic configuration procedures for the Cisco 10720 Internet Router and includes information on:

- Installing the hardware
- Starting up the router
- Configuring basic functionality

Organization

The *Cisco 10720 Internet Router Installation and Configuration Guide* is organized as follows:

Chapter/Appendix Number	Title	Description
	Preface	The Preface contains contact information, related documentation to assist in advanced configuration tasks, and a subset of translated safety warnings that can be found in the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication, and other useful information.
Chapter 1	Product Overview	Contains a high-level system overview, physical description of the major components of a Cisco 10720 Internet Router, and functional overview.
Chapter 2	Preparing for Installation	Contains information on safety, site requirements for power, environmental safety, cabling, rack-mounting, electrostatic discharge (ESD), unpacking, and the site log.
Chapter 3	Installing the Cisco 10720 Internet Router	Contains the procedures for verifying the Cisco 10720 Internet Router installation, grounding, cable connection, powering up the router, and basic configuration.
Chapter 4	Troubleshooting	Contains procedures for identifying and solving problems that may occur during installation.
Chapter 5	Maintaining the Cisco 10720 Internet Router	Contains information on safety at the field-replaceable unit (FRU) level, removal and replacement procedures for field-replaceable units and assemblies, and associated procedures to troubleshoot and verify the FRUs.
Appendix A	Technical Specifications	Contains Cisco 10720 Internet Router specifications.

Conventions

This publication uses the following conventions:

- The symbol ^ represents the key labeled *Control*. For example, the key combination ^**z** means hold down the **Control** key while you press the **z** key.

Command descriptions use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating the commands that you should enter at the prompt. The system prompt indicates the current level of the EXEC command interpreter. For example, the prompt `router>` indicates the *user* level, and the prompt `router#` indicates the *privileged* level. Access to the privileged level usually requires a password.
- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternative but required keywords are grouped in braces ({ }) and separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and sample console screen displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([ ]).
- Exclamation points (!) at the beginning of a line indicate a comment line.

Warning Definition

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

For a complete list of translated safety warnings, read the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* document (Document Number 78-13077-xx) that accompanies your Cisco 10720 Internet Router. Cisco recommends you read and understand the safety warnings and guidelines before installing, configuring, or maintaining the router.

Related Documentation

This section provides some reference material out of the Cisco.com library that may be useful for configuring and maintaining the Cisco 10720 Internet Router.

DPT and SRP

A variety of technical information on Dynamic Packet Transport (DPT) and Spatial Reuse Protocol (SRP) is at the following URL:
http://www.cisco.com/en/US/tech/tk482/tk611/tsd_technology_support_protocol_home.html

Cisco IOS Software Releases

- *Release Notes for Cisco IOS Release 12.0S*
- *Release Notes for Cisco IOS Release 12.0 ST*

Modular QoS

- *Modular QoS CLI Overview section in the Cisco IOS Software Configuration for the Cisco 10720 Internet Router* document
- *Quality of Service Overview section in the Cisco IOS Software Configuration for the Cisco 10720 Internet Router* document

Field-Replaceable Units (FRUs)

- *Cisco 10720 Internet Router AC and DC Power Supply Replacement Instructions*, document number 78-13100-xx
- *Cisco 10720 Internet Router Access Card Installation and Configuration*, document number 78-13082-xx
- *Cisco 10720 Internet Router Chassis Replacement Instructions*, document number 78-13098-xx
- *Cisco 10720 Internet Router Fan Assembly Replacement Instructions*, document number 78-13099-xx
- *Cisco 10720 Internet Router Memory Replacement Instructions*, document number 78-16166-xx
- *Cisco 10720 Internet Router Cable Management and Rack Mount Installation Instructions*, document number 78-13101-xx
- *Cisco 10720 Internet Router Uplink Cards Installation and Configuration*, document number 78-13113-xx

Other

- *Cisco 10720 Internet Router Unpacking Instructions*, document number 78-13855-xx
- *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router*, document number 78-13077-xx
- *Compressed Air Cleaning Issues for Fiber-Optic Connections*
- *Inspection and Cleaning Procedures for Fiber-Optic Connections*

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

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

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

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

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

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

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

- For Emergencies only—security-alert@cisco.com

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

- For Nonemergencies—psirt@cisco.com

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

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

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

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

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

CHAPTER 1

Product Overview

The Cisco 10720 Internet Router provides IP services to users at optical speeds at the edge of their networks. The Cisco 10720 Internet Router provides network access using Ethernet and Dynamic Packet Transport (DPT), Packet over SONET (POS), or IEEE 802.17 RPR technology for optical connectivity. Each router is equipped with one uplink card and one Ethernet access card.

The Cisco 10720 Internet Router overview is presented in the following sections:

- Product Description, page 1-1
- Physical and Functional Overview, page 1-2
- Design Specifications, page 1-9

Product Description

The Cisco 10720 Internet Router provides Ethernet and OC-48c/STM-16c Internet access. Ethernet connections are provided by means of copper or optical cables. OC-48c/STM-16c connections are provided by means of optical cables. The router can interoperate with synchronous optical network (SONET) transport infrastructure, but it is not required.

The Cisco 10720 Internet Router has one card cage with two card slots. The upper slot supports one uplink card and the lower slot supports one access card. Network interface connectors are located on the front of the uplink and access cards.

The built-in Flash memory contains a total of 64 MB, with 16 MB dedicated to a read-only partition that contains the Cisco IOS software image that shipped with the router. There are 48 MB dedicated to a read-write partition. The read-write partition contains downloaded Cisco IOS software images and is used to boot up the router.

Additional features of the Cisco 10720 Internet Router are as follows:

- Configuration and administration features, including Telnet and (Cisco Discovery Protocol) CDP
- Serial (AUX) and console ports for local and remote administration
- Remote software download via Trivial File Transfer Protocol (TFTP) and Remote copy.A UNIX utility (RCP)
- IP over DCC (data communications channel) for remote management of the Cisco 15104 OC-48/STM16 Optical Regenerator, where applicable
- Optical receive power monitoring support on the OC-48 interface

Physical and Functional Overview

The Cisco 10720 Internet Router physical and functional overview is presented in the following sections, and shown in Figure 1-1 and Table 1-1:

- Cisco 10720 Internet Router Hardware Features, page 1-3
- Hardware Field Replaceable Units, page 1-4
- Software Features, page 1-8

Figure 1-1 Cisco 10720 Internet Router: AC (Top) and DC (Bottom) Power Supplies

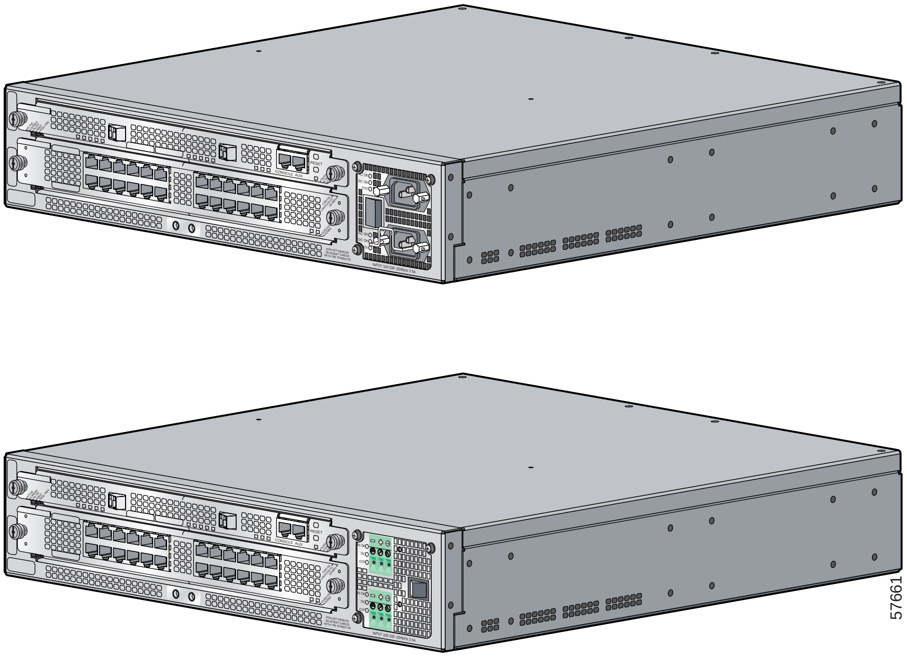


Table 1-1 Cisco 10720 Internet Router Description

Physical Description	
Dimensions	17.25 x 18.25 x 3.5 inches (2 RU) (43.81 cm x 46.36 cm x 8.89 cm) W x D x H
Input Power	Option 1: AC-input • 100/240 VAC • 50/60 Hz • 300W (Dual) Option 2: DC-input • –48/–60 VDC • 300W (Dual)

Cisco 10720 Internet Router Hardware Features

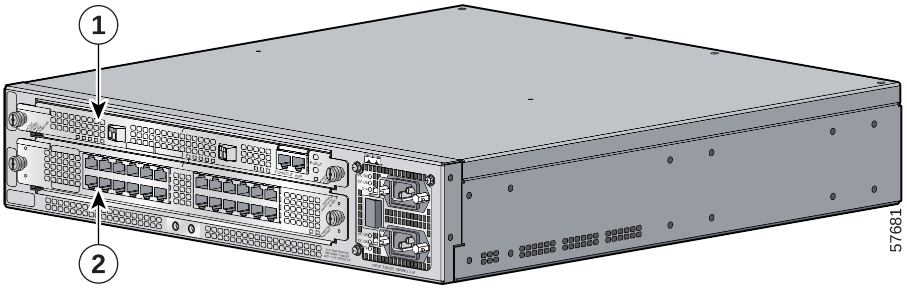
The Cisco 10720 Internet Router provides two dedicated card slots that are not interchangeable or hot swappable. (See Figure 1-2.) The upper slot contains an uplink card. The lower slot contains an Ethernet access card.

- The uplink card slot provides the following options:
  - DPT or POS/DPT uplink card: one OC-48c/STM-16c DPT port or two POS optical ports with an aggregate bandwidth of approximately 5 Gbps
  - RPR/SRP uplink card: two OC-48 RPR/SRP (Resilient Packet Ring/Spatial Reuse Protocol) ports that support small form-factor pluggable (SFP) modules, with an aggregate bandwidth of approximately 5 Gbps
  - Console/auxiliary card: console and serial ports only

  For more information about the uplink card, refer to the *Cisco 10720 Internet Router Uplink Cards Installation and Configuration* publication.
- The Ethernet access card provides either Fast Ethernet or combined Fast Ethernet and Gigabit Ethernet connectivity. For more information about the access card, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.

The uplink card with only console and serial ports can be used with one of the Ethernet access cards to customize the Cisco 10720 Internet Router as an Ethernet-only router.

Figure 1-2 Uplink Card and Access Card



1	Uplink card	2	Access card

The main processing board contains a central processing engine that consists of two sets of processors that manage the control plane traffic and the data plane traffic.

- The Parallel eXpress Forwarding (PXF) network processors manage the data plane and support IP forwarding as well as advanced QoS features.
- The multiple processors in the PXF process packets simultaneously at the rate of approximately 2 Mpps.

The Cisco 10720 Internet Router can be deployed directly over fiber, thus allowing service providers to offer IP plus optical access without the need for extensive SONET/Synchronous Digital Hierarchy (SDH) optical transport infrastructure.

Additional overview information about the router can be located in the *Cisco 10720 Internet Router Overview*, which accompanies other marketing materials related to the Cisco 10720 Internet Router.

Hardware Field Replaceable Units

The Cisco 10720 Internet Router provides dedicated slots for the uplink card and the access card. The card cage is integrated into a rigid metal frame. The Cisco 10720 Internet Router field replaceable units are presented in the following sections:

- Uplink Cards, page 1-4
- Access Card, page 1-6
- Redundant Power Supply, page 1-6
- Fan Assembly, page 1-7
- Mounts, page 1-7
- Cable Management, page 1-8

Uplink Cards

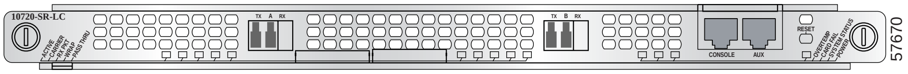
The uplink cards are available with one of the following:

- One OC-48c/STM16c DPT uplink fiber-optic port or two POS uplink fiber-optic ports
- Two RPR/SRP uplink fiber-optic ports supporting SFP modules
- Console and serial (AUX) ports only

There is one slot for an uplink card in the chassis. The cards fit the upper slot of the router chassis. See Figure 1-3 for an example of a typical DPT uplink card.

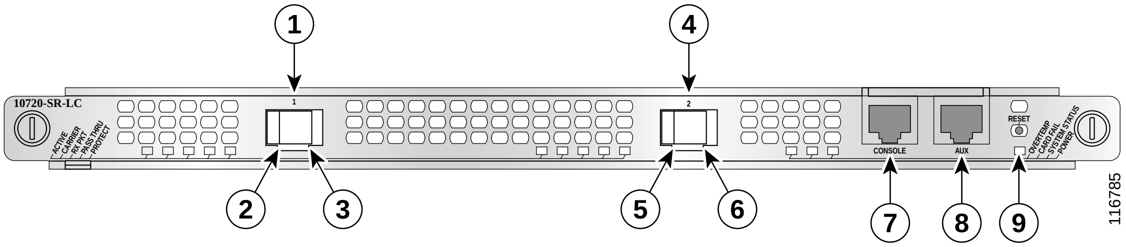
For more information about the uplink cards, versions of the uplink cards, and uplink card cabling, refer to the *Cisco 10720 Internet Router Uplink Cards Installation and Configuration* publication.

Figure 1-3 DPT Uplink Card (Front View)



The cable connector is a special LC optical connector. When using the card for DPT connections, the left port is the spatial reuse protocol (SRP) side A and the right port is SRP side B. When POS connections are made, the two ports are independent of each other. Each port consists of transmit (TX) and receive (RX). For additional information, see the "SONET Distance Limitations" section on page 3-11. The console/auxiliary card has console and serial (AUX) ports only.

Figure 1-4 RPR/SRP Uplink Card (Front View)



1	Span West for RPR mode Side A for SRP mode	**6**	Span East/Side B RX
2	Span West/Side A TX	**7**	Console port
3	Span West/Side A RX	**8**	Auxiliary port
4	Span East for RPR mode Side B for SRP mode	**9**	Reset switch
5	Span East/Side B TX		

The cable connector is a special LC optical connector. The RPR/SRP card uses SFP modules. When connecting to DPT networks in Resilient Pack Rings (IEEE 802.17 RPR) mode, the left port is span West, and the right port is span East. When in the Spatial Reuse Protocol (SRP) mode, the left port is side A, and the right port is side B. Each port consists of transmit (TX) and receive (RX). For additional information, see the "SONET Distance Limitations" section on page 3-11

Key features supported by the DPT and POS uplink card are listed below. For a more extensive list of features, consult your Cisco sales representative.

- Optical power monitoring and 4.6-ppm clock accuracy
- SONET OC-48/SDH-16c compliance
- IP over DCC management interface
- SRP

Key features supported by the RPR/SRP uplink card are listed below. For a more extensive list of features, consult your Cisco sales representative.

- Optical power monitoring and 4.6-ppm clock accuracy
- SONET OC-48/SDH-16c compliance
- IP over DCC management interface
- SRP
- IEEE 802.17 RPR features
- Small Form Factor pluggable (SFP) modules

Access Card

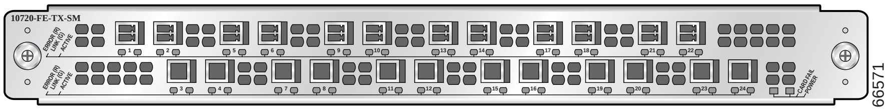
The access card is available in either of the following versions:

- Fast Ethernet with support for copper and fiber-optic cabling
- Combined Fast Ethernet and Gigabit Ethernet. The Fast Ethernet ports support copper or fiber-optic cabling and the Gigabit Ethernet ports use small form-factor pluggable (SFP) optical and copper modules.

There is a slot for one access card in the chassis. The card fits the lower slot of the router chassis. See Figure 1-5 for an example of a typical access card.

For more information about the access card, versions of the access card, and access card cabling, refer to the *Cisco 10720 Internet Router Access Cards Installation and Configuration* publication.

Figure 1-5 Typical Access Card (Front View)



Key features supported by the access card are listed below. For a more extensive list of features, consult your Cisco sales representative.

- Fast Ethernet and Gigabit Ethernet connectivity
- Ethernet Advanced Research Projects Agency (ARPA) MAC encapsulation
- Time Domain Reflectometry (TDR) on 10/100BASE-TX
- Autonegotiation for speed and duplex
- 2000 MAC addresses per port for Address Resolution Protocol (ARP)
- 1000 MAC addresses per Fast Ethernet port
- Cisco IOS software configuration of Ethernet features

Redundant Power Supply

The Cisco 10720 Internet Router comes with either dual AC or dual DC power supplies for redundancy.

Figure 1-6 shows the AC power supply and Figure 1-7 shows the DC power supply for the Cisco 10720 Internet Router.

Figure 1-6 Cisco 10720 Internet Router AC Power Supply

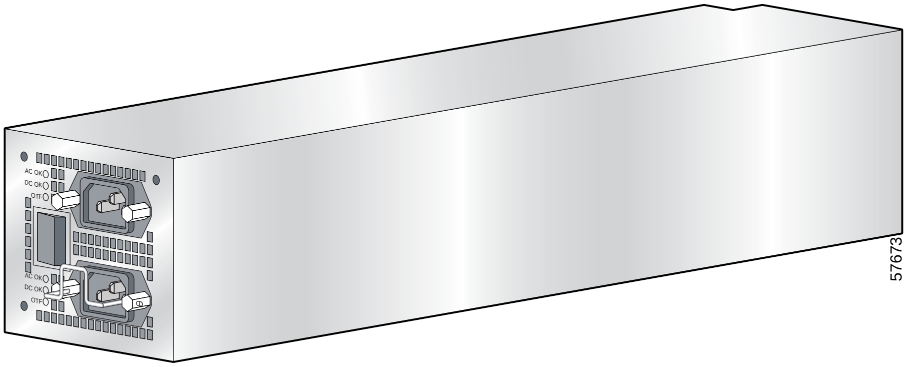
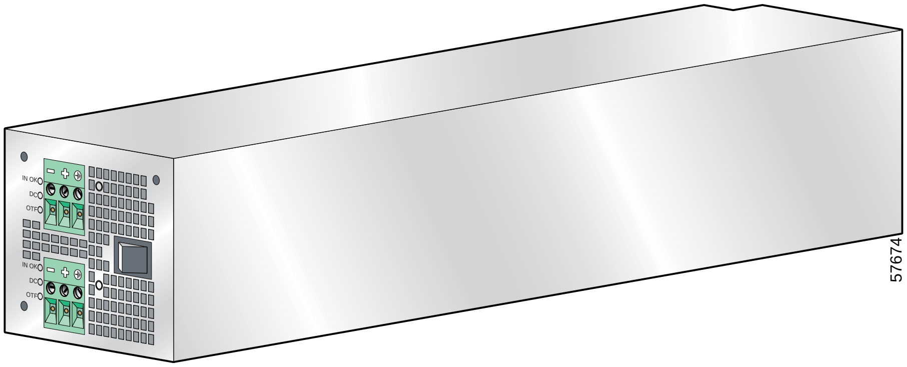


Figure 1-7 Cisco 10720 Internet Router DC Power Supply



Fan Assembly

The router is equipped with a four-fan assembly located on the inside of the back of the chassis. The fan assembly offers redundancy; therefore, the router can continue to operate if one of the fans fails.

Note Replace the fan assembly when a failure occurs. (See the "Removing and Installing the Router Fan Assembly" section on page 5-16.)

Mounts

The Cisco 10720 Internet Router can be mounted in the following ways:

- Front, mid-, or rear rack mounting in any of the following standard mounting bracket sizes:
  - 19-inch EIA (Electronics Industry Association)
  - 23/24-inch EIA
  - ETSI (European Telecommunications Standards Institute)
- Wall mounting
- Desk mounting

Cable Management

The cable-management system organizes the interface cables that lead into and away from the router. Keep the interface cables out of the way of other cables and free of sharp bends.

The cable-management system consists of the following components:

- Cable-management tray for managing the cables
- Cable-management cover to keep the cables from being accidentally stressed

Software Features

A list of software features for the Cisco 10720 Internet Router follows. For more information about advanced and other software features, refer to the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication.

- Cisco IOS Release 12.0 SP and Cisco IOS Release 12.0(29)S
- IP routing protocols, including Intermediate Standard- Intermediate System (IS-IS), Open Shortest Path First (OSPF), Border Gateway Protocol-4 (BGP-4)
- Ethernet features
  - Media dependent interface (MDI) and media dependent interface crossed (MDI-X) mode. (MDI mode is supported on revision B of the combined Fast Ethernet and Gigabit Ethernet access card, and in Japan on all access cards.)
  - 10/100 speed auto-negotiation
  - Half-duplex/full-duplex (HDX-FDX) negotiation
  - Time Domain Reflectometry (TDR)
- Spatial Reuse Protocol (SRP) features
  - SRP intelligent protection switching (IPS)
  - IPS wrap-time < 50 ms
  - SRP rate-limiting for TX traffic (high/low-priority queue)
  - SRP priority slicing for TX traffic
  - SRP fairness algorithm (SRP-fa)
  - 9,000 maximum transmission unit (MTU)
  - SRP hold-off timer for protected SONET
- Resilient Packet Ring (RPR) features
  - Intelligent Protection Switching (IPS): Steering mode or Wrapping mode
  - RPR Fairness: Per Station Fairness, weighted fairness, Conservative mode or aggressive mode
  - Topology: Advanced topology discovery combined with protection events
  - RPR classes: Support for classes A, B, and C in transit and Class A and B for transmit and receive
  - RPR keepalive timer and L1 Holdoff timer

For the physical specifications of the Cisco 10720 Internet Router, see Appendix A, "Technical Specifications."

Design Specifications

The Cisco 10720 Internet Router includes the following design specifications:

- Network Equipment Building Systems, page 1-9
- Electromagnetic Compatibility, page 1-9
- Bonding and Grounding, page 1-9
- Environmental Monitoring, page 1-9
- Shock and Vibration, page 1-9

Network Equipment Building Systems

The Cisco 10720 Internet Router is built to comply with Network Equipment Building Systems (NEBS) (Level 3 per SR-3580) in flammability, structural, and electronics compliance. For more information, see the *Regulatory Compliance and Safety Information for the Cisco 10720* document.

Electromagnetic Compatibility

Electromagnetic Compatibility (EMC)—Emissions, Immunity, Electrostatic Discharge (ESD) for product and packaging. For more information, see the "Maintaining Safety with Electricity" section on page 2-3 and the *Regulatory Compliance and Safety Information for the Cisco 10720* document.

Bonding and Grounding

You should bond and ground the router for safety, circuit protection, noise currents, reliability, and operations compliance. For more information, see the "Grounding the Cisco 10720 Internet Router" section on page 3-9.

Environmental Monitoring

The Cisco 10720 Internet router provides environmental monitoring to assist the user in tracking router operating temperature and humidity. Heat dissipation is not monitored.

Shock and Vibration

Shock and vibration tests are performed on the Cisco 10720 Internet Router. The router is tested to meet the Corporate Mechanical Design Validation and Test (MDVT) specification. Tests verify that the router operating ranges meet handling and earthquake standards. This router was built to comply with Network Equipment Building Systems (NEBS) (Zone 4 per GR-63-Core) in the following areas:

- Earthquake environment and criteria
- Office vibration and criteria
- Transportation vibration and criteria

CHAPTER 2

Preparing for Installation

Installation preparation is presented in the following sections:

- Regulatory Compliance and Safety Information, page 2-1
- Warnings and Cautions, page 2-1
- Required Tools and Equipment, page 2-5
- Environmental Safety Guidelines, page 2-8
- Cisco IOS Software Configuration, page 2-11
- Required Tools and Equipment, page 2-5
- Verifying the Contents in the Box, page 2-11
- Site Log Preparation, page 2-12

Regulatory Compliance and Safety Information

See the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication, Document Number 78-13077-xx, for complete regulatory compliance and safety information. We recommend you read and understand the safety warnings and guidelines before installing, configuring, or maintaining the router.

Warnings and Cautions

The following sections concern warnings and cautions that accompany the Cisco 10720 Internet router:

- Safety Guidelines, page 2-2
- Maintaining Safety with Electricity, page 2-3
- Electrostatic Discharge, page 2-3
- Laser Safety, page 2-4
- Ventilation Guidelines, page 2-5

Safety Guidelines

Before you perform any procedures in this publication, review the safety guidelines in this section to avoid injuring yourself or damaging the equipment.

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

Note Review the safety warnings listed in the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication (Document Number 78-13077-xx) that accompanied your Cisco 10720 Internet Router before installing, configuring, or maintaining the router.

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

- Never attempt to lift an object that might be too heavy for you to lift by yourself.
- Always disconnect the power source and unplug all power cables before lifting, moving, or working on the router.
- Keep the work area clear and dust free during and after installation.
- Keep tools and router components away from walk areas.
- Do not wear loose clothing, jewelry (including rings and chains), or other items that could get caught in the router.
- Fasten your tie or scarf and sleeves.
- Use and operate the router in accordance with its electrical ratings and product usage instructions.
- Do not work alone if potentially hazardous conditions exist.
- Always unplug the power cables when performing maintenance or working on the router

Review the following safety compliance guidelines to avoid injuring yourself or damaging the equipment:

- Your Cisco 10720 Internet Router should be installed in compliance with national and local electrical codes: in the United States, National Fire Protection Association (NFPA) 70, United States National Electrical Code; in Canada, Canadian Electrical Code, part I, CSA C22.1; in other countries, International Electrotechnical Commission (IEC) 364, part 1 through part 7.
- A Cisco 10720 Internet Router configured with an AC-input power supply ships with a three-wire electrical grounding-type plug that will only fit into a grounding-type power outlet. This is a safety feature. The equipment grounding should be in accordance with local and national electrical codes.
- A Cisco 10720 Internet Router configured with a dual DC-input power supply requires an external circuit breaker for the DC-input power source. This circuit breaker should protect against short-circuit and overcurrent faults in accordance with United States National Electrical Code NFPA 70 (United States), Canadian Electrical Code, part I, CSA C22.1 (Canada), or IEC 364 (other countries).
- A Cisco 10720 Internet Router configured with an AC-input power supply must have the socket-outlet combination installed near the router, and it must be easily accessible at all times. The socket-outlet combination serves as the main disconnecting device.
- A Cisco 10720 Internet Router configured with a DC-input power supply must have a readily accessible disconnect device incorporated in the fixed wiring.

Maintaining Safety with Electricity

For information on maintaining safety with electricity, see the "Safety Guidelines" section on page 2-2.

Electrostatic Discharge

Electrostatic discharge (ESD) can damage circuit boards if they are handled improperly. Such mishandling can result in intermittent or complete failures of the board.

When handling circuit boards, observe the following guidelines to prevent ESD damage:

- Always use an antistatic wrist strap and ensure that the strap makes adequate contact with your skin.
- Attach an ESD-preventive strap to your wrist, and to the chassis or to a bare metal surface. (See Figure 2-1.)
- The wrist strap protects equipment from ESD voltages on the body only; ESD voltages on clothing can still cause damage to electronic components.

⚠ **Caution** For safety, periodically check the resistance value of the ESD-preventive wrist strap. The resistance measurement should be between 1 and 10 megohms (Mohms).

Preventing Electrostatic Discharge

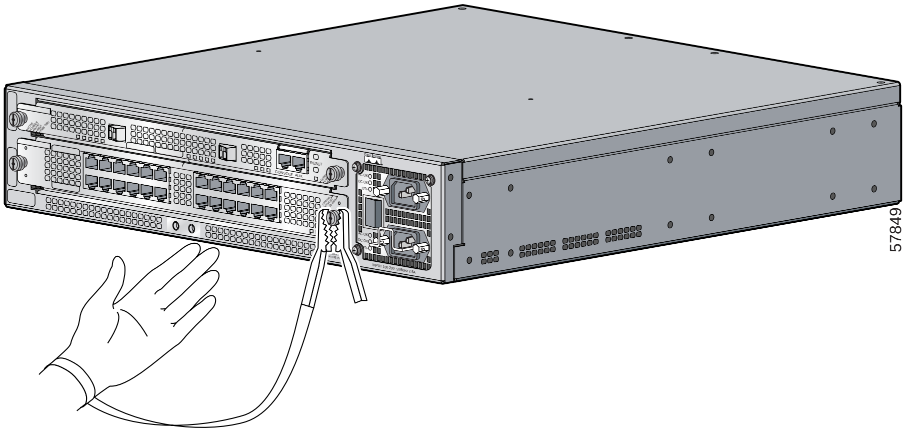
Electrostatic discharge (ESD) damage can occur when electronic cards or components are improperly handled. ESD can cause complete or intermittent failures. We recommend using an antistatic strap when you handle a router or one of its components.

Electromagnetic interference (EMI) shielding is an integral component of the router.

Following are guidelines for preventing ESD damage:

- Always use an ESD-preventive wrist or ankle strap and ensure that it makes good skin contact. Connect the equipment end of the connection cord to bare metal on the router chassis. (See Figure 2-1.)

Figure 2-1 Attaching an ESD-Preventive Strap



- When installing an uplink or access card, confirm that the card is fully seated in the midplane and tighten the spring-loaded screws. These screws prevent accidental removal, provide proper grounding for the system, and help ensure that the connectors are seated in the midplane.

  See the "Removing and Installing an Uplink Card" section on page 5-49 and "Removing and Installing an Access Card" section on page 5-58.
- When removing an uplink or access card, use the spring-loaded screws to unseat the card connector from the midplane.

  See the "Removing and Installing an Uplink Card" section on page 5-49 and "Removing and Installing an Access Card" section on page 5-58.
- Handle cards by the spring-loaded screws only; avoid touching the board or connector pins.
- Place a removed card board-side-up on an antistatic surface or in a static shielding bag. If you plan to return the component to the factory, immediately place it in a static shielding bag.
- Avoid contact between the card and clothing. The wrist strap protects the board only from ESD voltages on the body; ESD voltages on clothing can still cause damage.

Laser Safety

The uplink card is equipped with a Class 1 laser that emits invisible radiation. Do not stare into open line card ports. The following laser warnings apply to the Cisco 10720 Internet Router:

Class 1 Laser Product Warning

Warning **Class 1 laser product.** Statement 1008

General Laser Warning

Warning **Avoid exposure to laser radiation. Do not stare into an open aperture, because invisible laser radiation may be emitted from the aperture when a cable is not inserted in the port.** Statement 125

For translated Class 1 laser warnings, refer to the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication.

Class 1 LED Product Warning

Warning **Class 1 LED product.** Statement 1027

Required Tools and Equipment

The following tools and equipment are required to install the Cisco 10720 Internet Router:

- ESD-preventive wrist strap
- Number 1 Phillips screwdriver
- 1/8-inch flat-blade screwdriver
- Antistatic mat (optional)
- Antistatic bag
- Cable ties
- Wire stripper

Rack-Mounting Guidelines

Before installing the Cisco 10720 Internet Router in a 19-inch EIA, 23- or 24-inch EIA, or ETSI equipment rack, consider the general rack-mounting guidelines presented in the following sections:

- Ventilation Guidelines, page 2-5
- Rack-Mounting Clearance Guidelines, page 2-6
- Maintenance Guidelines for Multiple Routers in a Rack, page 2-6

Ventilation Guidelines

Caution The fan assembly is located in the back of the router chassis. Air flow in the front and back of the router should not be blocked.

Use these guidelines to provide adequate ventilation for the Cisco 10720 Internet Router:

- Install the chassis in an enclosed rack only if the rack has adequate ventilation or an exhaust fan; use an open rack when possible.
- A ventilation system that is too powerful in an enclosed rack can also prevent cooling by creating negative air pressure around the router and redirecting the air away from the air intake vent. If necessary, operate the router with the rack door open or in an open rack.
- Make sure that the air baffle located between the fan assembly and power supply is properly seated to assist in cooling the router.
- Check equipment located near the bottom of the rack, because it can generate excessive heat that is drawn upward and into the intake ports of equipment above, possibly leading to overheating.

Rack-Mounting Clearance Guidelines

The rack-mounting hardware included with the Cisco 10720 Internet Router is suitable for most 19-inch EIA, 23- or 24-inch EIA, or ETSI equipment racks or Telco-style racks.

The following are rack-mounting guidelines for the Cisco 10720 Internet Router:

- If you use a Telco-style rack, be sure that the rack is bolted to the floor, the router mounts to the two rack posts, and the rest of the router is cantilevered off the posts.
- Some Telco-style racks are secured to ceiling brackets, if necessary, because of the weight of the equipment in the rack. Make sure that the rack on which you are installing the Cisco 10720 Internet Router is secured.

Note Warm air exhausts out the back side of the router by drawing cool air in through vents located on the front of the router chassis. Allow sufficient airflow by maintaining 6 inches (15.24 cm) of clearance at both the inlet and exhaust openings on the router and 0.75 inch (1.9 cm) on each side of the router chassis.

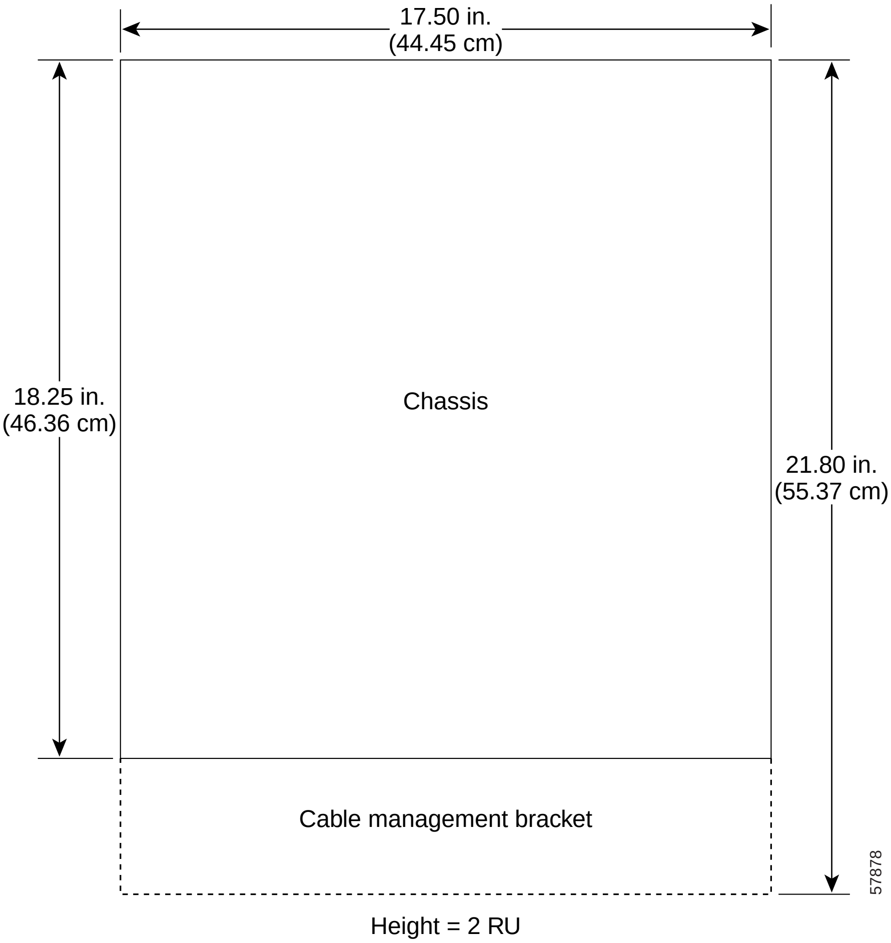
Maintenance Guidelines for Multiple Routers in a Rack

The Cisco 10720 Internet Router is 17.50 inches (44.45 cm) wide by 3.45 inches (8.76 cm) high by 18.25 inches (46.36 cm) deep. The height is equivalent to two rack units (RU). The router is 21.80 inches (55.37 cm) deep when the cable-management tray is installed. When placing multiple routers in a rack, ensure that there is sufficient ventilation to accommodate the routers.

The heated exhaust air from other equipment can enter the inlet air vents and cause overheating inside the router. To avoid this, follow these guidelines:

- Install and use the cable-management system included with the router to keep cables organized and out of the way of the cards and power supply.
- Ensure that cables from other equipment do not interfere with access to the cards and LEDs located in the front of the router.
- When mounting the router in a rack, be sure to use all the screws provided to secure the router to the rack posts.

Figure 2-2 Cisco 10720 Internet Router Outer Dimensions (Top View)



Environmental Safety Guidelines

This section offers guidelines for operating your Cisco 10720 Internet Router in various environments:

- Airflow Guidelines, page 2-8
- Temperature and Humidity Guidelines, page 2-8
- Power Guidelines, page 2-9
- Site Wiring Distance and Interference Guidelines, page 2-10
- Cable Management, page 2-11
- Mounting the Router, page 2-11

Airflow Guidelines

The Cisco 10720 Internet Router air circulation system consists of four fans installed in the back of the router chassis. The fan assembly maintains acceptable operating temperatures for the internal components by drawing cooling air in through vents located on the front of the router chassis, circulating the air through the router, and exhausting the air out of the back of the router chassis.

Observe the following guidelines when selecting a site at which to install the Cisco 10720 Internet Router:

Note Warm air exhausts out the back side of the router by drawing cool air in through vents located on the front of the router chassis. Allow sufficient air flow by maintaining 6 inches (15.24 cm) of clearance at both the inlet and exhaust openings on the router and 0.75 inch (19.1 mm) on each side of the router chassis.

- The site should be as dust-free as possible.
- Under extreme environment conditions, the environmental monitoring system will shut down the power to protect the system components.

Temperature and Humidity Guidelines

The operating environmental site requirements are located in Appendix A, “Technical Specifications.” The temperature and humidity ranges listed are those within which the router will continue to operate. You can maintain normal operation by anticipating and correcting environmental irregularities before they approach critical values.

The environmental monitoring functionality built into the router protects the system and its components from potential damage from overvoltage and overtemperature conditions.

To assure normal operation and avoid maintenance difficulty, plan and prepare your site before installing the router.

Power Guidelines

Caution Read the installation instructions before you connect the router to its power source.

The Cisco 10720 Internet Router requires a 120/220 VAC or –48 VDC dual power supply. Site requirements differ depending on the type of source voltage. We recommend you follow these precautions and recommendations when planning power connections to your router:

- Check the power at your site before installation and periodically after installation to ensure that you are receiving clean power. Install a power conditioner if necessary.
- Install proper grounding, or use the proper grounding receptacle to avoid damage from lightning and power surges.
- Read the safety warnings before you connect the AC or DC power supply to the electrical power at the local or remote site.

AC-Powered Router

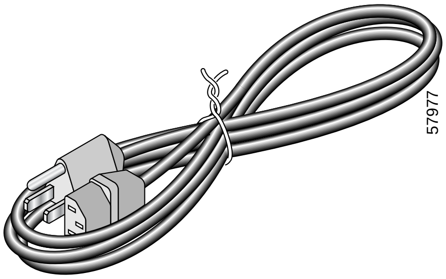
The AC dual power supply includes two terminal blocks for power redundancy. (See Figure 1-6.) The grounding screw is located in the terminal block.

The following guidelines will help to ensure your safety and protect the equipment. This list does not include every potentially hazardous situation, so be alert.

- Install an uninterruptable power source where possible.
- Install proper grounding to avoid damage from lightning and power surges.

See the “Safety Guidelines” section on page 2-2 for additional information. See Figure 2-3 for an example of a typical AC power cord.

Figure 2-3 AC Power Cord



DC-Powered Router

The DC dual power supply includes two terminal blocks for power redundancy. (See Figure 1-7.)

The minimum wire gauge size supported on the DC dual power supply is 17 American Wire Gauge (AWG), which has a 1.5mm wire diameter. The maximum wire gauge size supported on the DC dual power supply is 10 AWG, which has a 6mm wire diameter.

Wires that are installed in the router power source come from two other external DC power sources. If the DC power source on Bus B fails, Bus A will continue to power the generator.

The following guidelines will help to ensure safety and protect the equipment. This list does not include every potentially hazardous situation, so be alert.

A Cisco 10720 Internet Router configured with the dual DC-input power supply should have a readily accessible disconnect device incorporated for fixed wiring.

See the "Safety Guidelines" section on page 2-2 for additional information.

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

Warning **A readily accessible two-pole disconnect device must be incorporated in the fixed wiring.** Statement 91

Site Wiring Distance and Interference Guidelines

This section offers site wiring guidelines for setting up the site plant wiring and cabling. When planning the location of the new system, consider the following:

- Electromagnetic Interference, page 2-10
- Distance Limitations for Signaling and Unshielded Conductors, page 2-10

Electromagnetic Interference

Electromagnetic interference (EMI) can occur between the field and the signals on the wires when the wires are run for any significant distance. This fact has two implications for the construction of plant wiring:

- Poor wiring practice can result in radio interference emanating from the plant wiring.
- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy and/or cause interference with the signal drivers and receivers in the router, and can create an electrical hazard by conducting power surges through lines and into equipment.

Note To predict and remedy strong EMI, consult experts in radio frequency interference (RFI).

A good quality twisted pair cable or shielded twisted pair cable helps limit radiation and noise induced into the cable, minimizing the potential for the following:

- Radio interference
- Interference with the data transmission

Distance Limitations for Signaling and Unshielded Conductors

You must give special consideration to the effect of a lightning strike in the site vicinity if wires exceed recommended distances, or if wires pass between buildings. The electromagnetic pulse (EMP) caused by lightning or other high-energy phenomena can easily couple enough energy into unshielded conductors to destroy electronic devices.

You must provide a properly grounded and shielded environment. Consider electrical surge suppression issues by addressing the following items:

- Potential surge sources
- Distance

Caution Splicing can degrade cable performance.

Cable Management

The cable-management system, located on the front of the router, organizes the interface cables. The cable-management system consists of the following components:

- Cable-management tray for managing cables
- Cable-management cover to keep cables from being accidentally stressed

Before mounting the router or connecting the ports on an uplink card or access card, install the cable-management tray. For more information, see the "Installing the Cable-Management System" section on page 5-70.

Mounting the Router

Rack mount brackets are available for 19-inch EIA, 23-inch EIA, or 24-inch EIA, and ETSI racks. Wall-mount brackets and desktop mounts are also available options. For more information about mounting the Cisco 10720 Internet Router, see the "Rack-Mounting the Router" section on page 3-2.

Cisco IOS Software Configuration

The Cisco IOS software that runs on your router contains extensive features and functionality.

For Cisco IOS software configuration information and support, refer to the configuration and command reference publications in the Cisco IOS software configuration documentation set that corresponds to the Cisco IOS software release installed on your Cisco hardware. You can also refer to the Cisco IOS software release notes for the version of Cisco IOS software you are using on your router.

For a list of these documents, see "Related Documentation" section on page xix.

Verifying the Contents in the Box

Check the contents of the shipping packaging and verify that the following are included with your shipment:

- One Cisco 10720 Internet Router fully assembled that includes the following:
  - 1 uplink card
  - 1 access card
  - 1 AC or DC dual power supply
  - 1 main board

  - 1 midplane board
  - 1 fan assembly containing 4 fans
  - 1 air baffle located between power supply and fan number 4
- One accessory kit that includes the following:
  - 19-inch EIA rack-mount brackets (quantity 2)
  - 23- to 24-inch EIA rack-mount brackets (quantity 2)
  - ETSI rack-mount brackets (quantity 2)
  - Wall-mount brackets (quantity 2)
  - Rubber foot pads for desk mounting (quantity 4)
  - Cable-management system (quantity 1 cable-management tray and 1 cable-management cover)
  - AC power cable (quantity 2)
  - Metal AC bracket clips (quantity 2)
  - Screws (quantity 22)
  - Ground lug (quantity 1)
  - Lug-mounting 6.3 mm (M5) screws (quantity 2)
- *Cisco 10720 Internet Router Unpacking Instructions*
- *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router*
- *Obtaining Documentation for the Cisco 10720 Internet Router*

If you do not receive everything you ordered, contact a customer service representative for assistance.

Site Log Preparation

Table 2-1 shows a sample site log. Make copies of the sample or design your own site log. The site log lets you record operation and maintenance activity. Keep the site log in an accessible place near the router.

Site log entries might include the following:

- Installation progress—Make entries in the site log to record installation progress. Log any difficulties encountered and remedies during the installation process for future reference.
- Upgrades and removal/replacement procedures—Use the site log as a record of system maintenance and expansion history.

Each time a procedure is performed on the system, update the site log to record the following:

- Field-replaceable hardware installed, removed, or replaced
- Router configuration changes
- Software upgrades
- Corrective or preventive maintenance procedures performed
- Intermittent problems
- Your comments

Table 2-1 Site Log for the Cisco 10720 Internet Router

Device Identification:		
Date	**Description of Action Performed or Symptom Observed**	**Initials**

CHAPTER 3

Installing the Cisco 10720 Internet Router

Instructions for installing the Cisco 10720 Internet Router and its basic components are presented in the following sections:

Setting up the Cisco 10720 Internet Router

Verify the following before you install the router:

- Fan assembly exhaust vents are not blocked.
- The front of the router is not blocked. The airflow intake is located on the front of the router.
- 24 inches (61 cm) of clearance in front of the router may be needed for working with line cards, power supplies, attaching network interface cards (NICs), or other components.
- Location is temperature-controlled, air-conditioned, and dust-free.
- Power cables and power supplies have been checked for compatibility with your power service.
- Labels on the equipment have been checked to ensure that the power service at your site is suitable for the router.
- AC- or DC-power source voltage receptacles are easy to reach.

Note For information about environmental considerations and requirements, see the "Environmental Safety Guidelines" section on page 2-8.

Cable Management

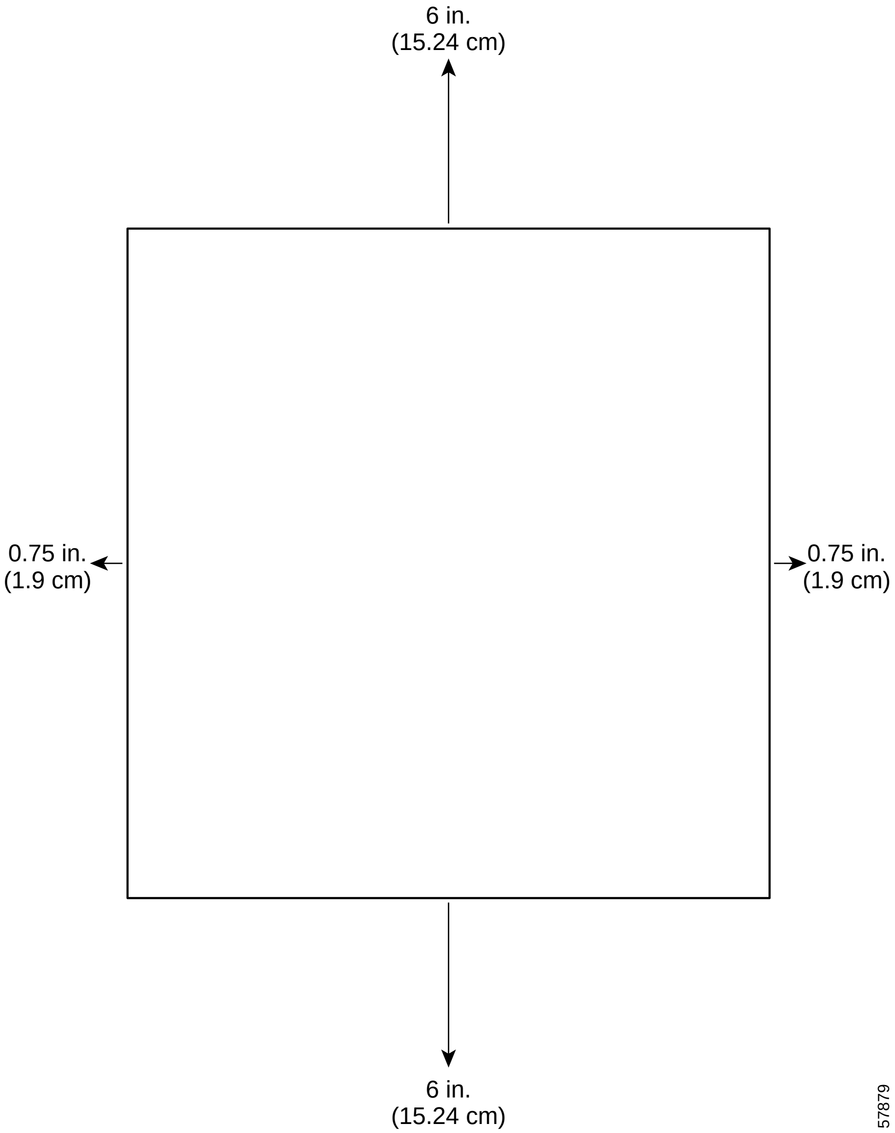
Install the cable-management tray, which is part of the cable-management system, onto the router before mounting the router on a rack, wall, or desktop. For instructions on installing the cable-management system, see the "Removing and Installing the Cable-Management System" section on page 5-68.

Rack-Mounting the Router

This section describes how to mount the router on an equipment rack, wall, or desktop. The router comes with three sets of brackets for rack-mounting, one set of brackets for wall-mounting, and four rubber foot pads for desk-mounting.

Check the clearance around the router before you install the router. See the "Required Tools and Equipment" section on page 2-5 for detailed dimension requirements.

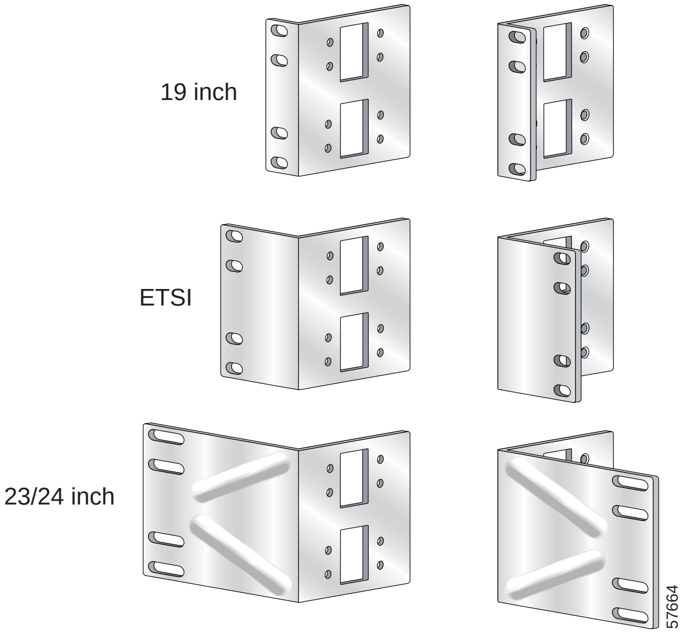
Figure 3-1 Ventilation Requirements for Rack Mounting



Note Warm air exhausts out the back end of the router by drawing cool air in through vents located on the front of the router chassis. Allow sufficient airflow by maintaining 6 inches (15.24 cm) of clearance at both the inlet and exhaust openings on the router and 0.75 inch (19.1 mm) on each side of the router chassis. (See Figure 3-1.)

The following steps describe how to mount the router on a 19-inch EIA, 23-inch, or 24-inch EIA, or ETSI rack:

Figure 3-2 Rack-Mounting Brackets

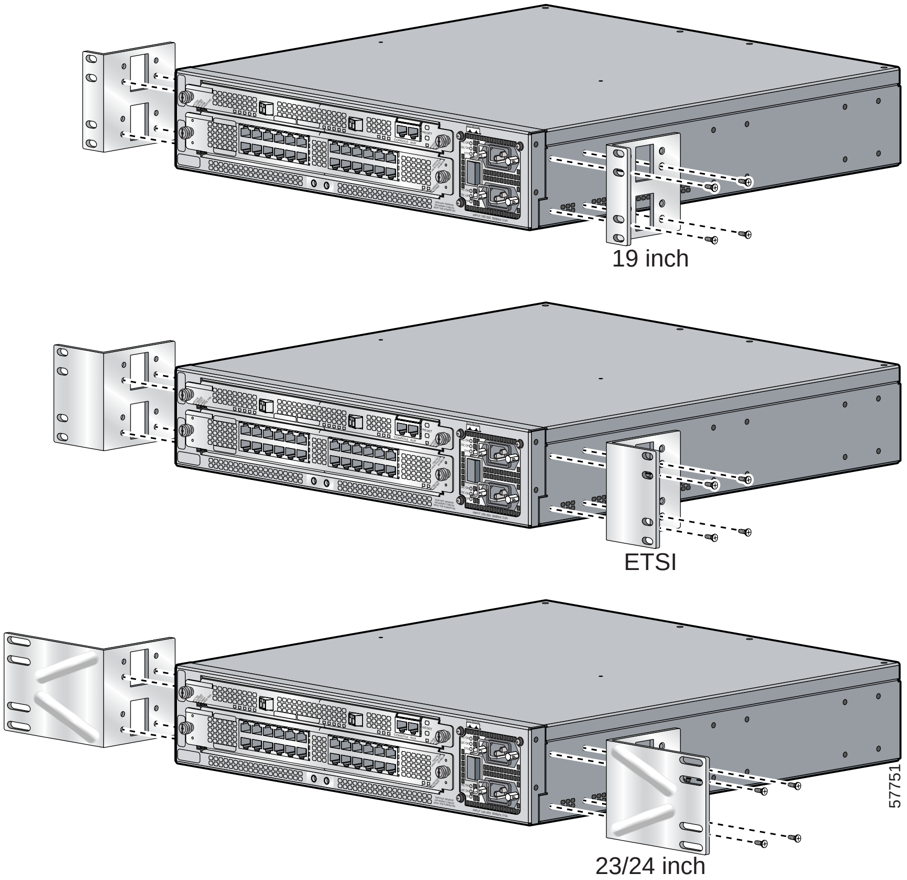


Step 1 Choose the appropriate rack-mounting brackets to fit your rack. (See Figure 3-2.)

Step 2 Attach an ESD-preventive wrist strap to your wrist, and to the router chassis or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 3 Turn the router so that the front panel is facing you. The fans are in the back of the router.

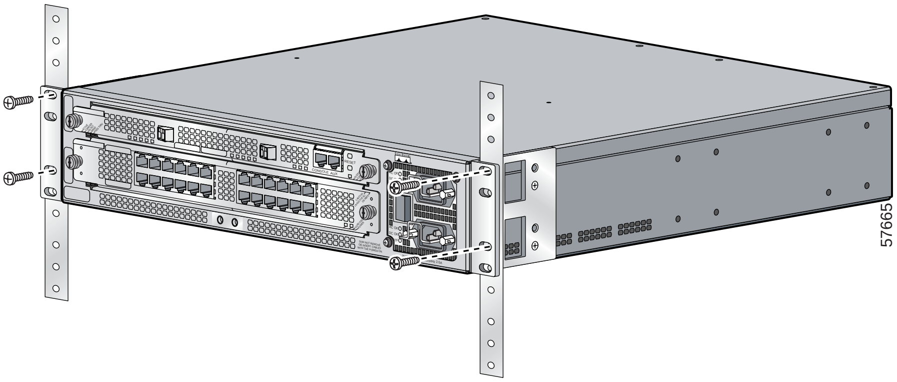
Figure 3-3 *Installing Rack Mounting Brackets*



Step 4 Align the brackets to the right and left sides of the router. Use the Number 1 Phillips screwdriver with the screws that are supplied in the accessory kit to attach the brackets to the router. (See Figure 3-3.)

Step 5 Install the router in a rack with the front panel forward.

Figure 3-4 *Attaching the Router to the 19-Inch Rack (Front Panel Forward)*



Step 6 Align the mounting brackets on the router with the holes in the rack.

Use a Number 1 Phillips screwdriver to attach the four screws that are supplied in the cable accessory kit to attach each side of the router chassis to the rack. (See Figure 3-4.)

Wall-Mounting the Router

The wall-mounting brackets must be mounted on a minimum 5/8-inch (15.9 mm) gypsum wallboard or equivalent with 12 1-1/4-inch Number 10 screws or equivalent (M5 x 31.8 mm).

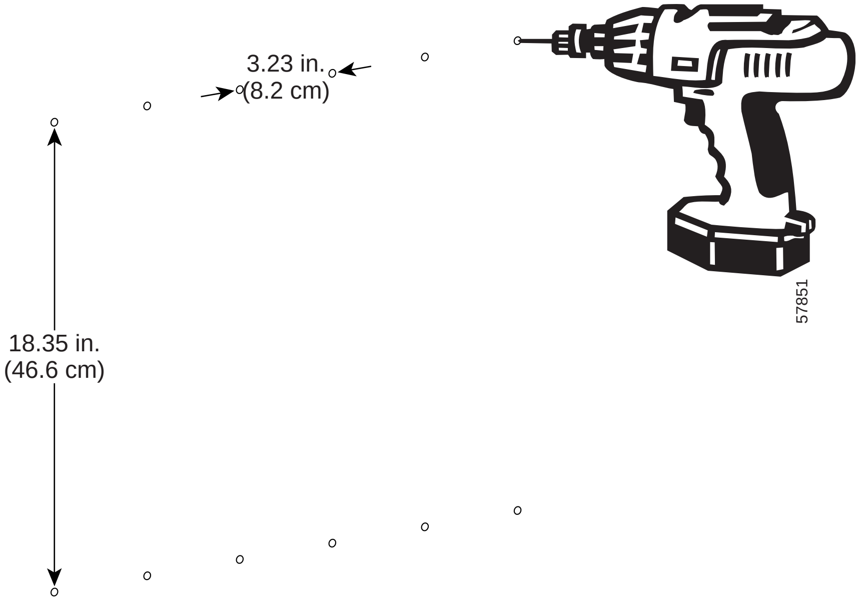
Caution The front and back panels of the router require at least 6 inches of clearance away from the wall or other items that can block the airflow. The side panel requires 1 inch of clearance away from the wall or other items that can block the airflow. The top and bottom of the router chassis do not require any specific clearance.

Perform the following steps to set up a proper and secure wall mount for the router. These steps ensure that adequate ventilation is available at all times. A Number 1 Phillips screwdriver is required to perform the following procedure:

Step 1 Locate the two 17.25-inch (43.82 cm) long metal mounts, 12 1-1/4-inch Number 10 (3.18 cm) screws, and 10 screws for attaching the mount to the router chassis, included in the accessories kit.

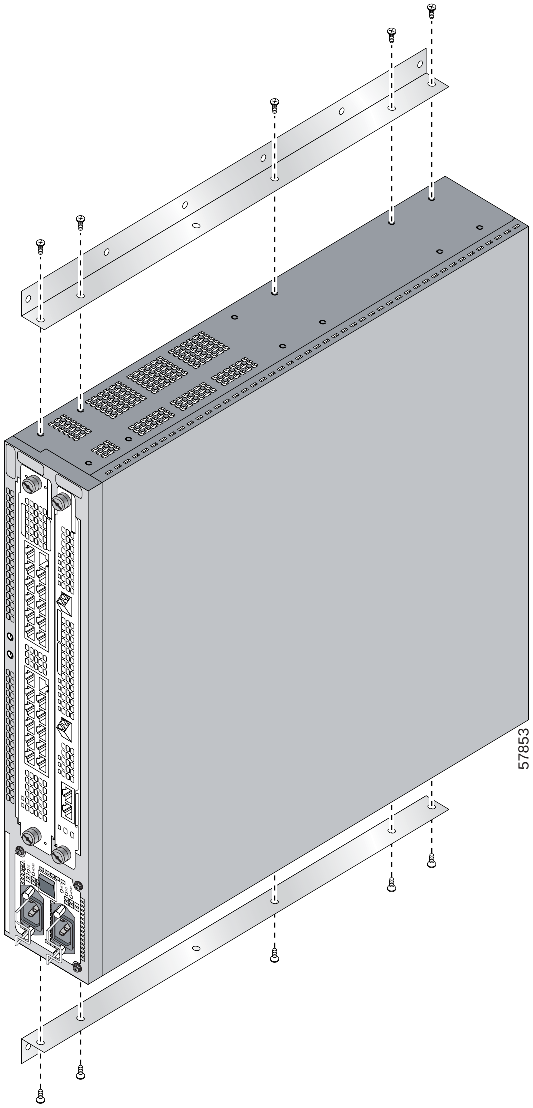
Note Verify that no electrical, heating, or plumbing apparatus is located behind the drilling location.

Figure 3-5 Predrilled Holes on a Mounting Surface



Step 2 Predrill 12 holes on the mounting surface. The holes on the side of the router chassis are 3.23 inches (8.2 cm) apart. The side-to-side distance is 18.35 inches (46.6 cm). (See Figure 3-5.)

Figure 3-6 Attaching Wall-Mounting Brackets to the Router Chassis

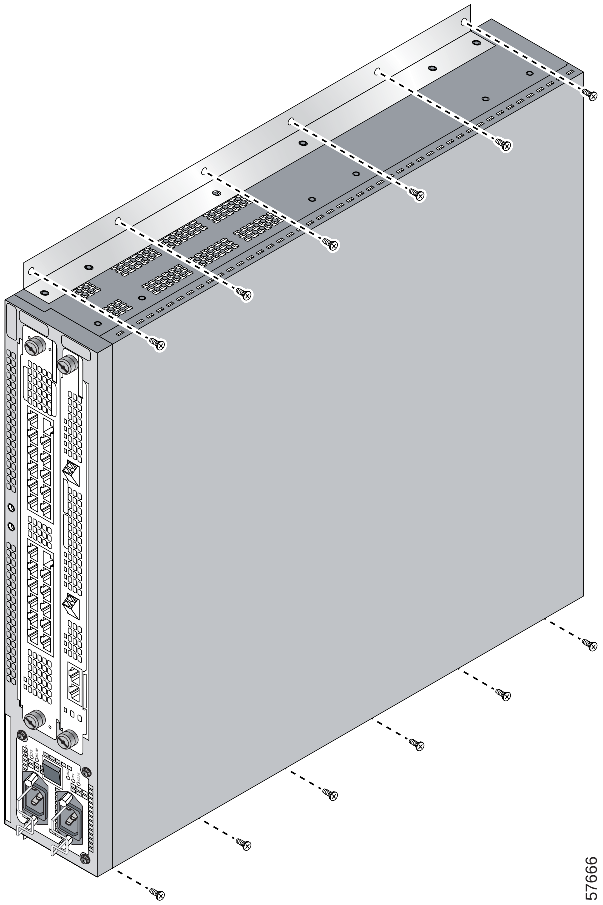


Note When the rack is mounted on the wall, make sure that the power receptacles are at the bottom of the router, as shown in Figure 3-6.

Step 3 Attach an ESD-preventive strap to your wrist, and to the router chassis or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 4 Attach the wall-mounting brackets to the side of each chassis using five screws on each side. (See Figure 3-6.)

Figure 3-7 *Wall-Mount Rack*



Step 5 Match the holes in the wall-mounting brackets to the predrilled holes on the mounting surface. Mount the brackets to the wall using the 12 1-1/4-inch screws. (See Figure 3-7.)

Setting up the Router on a Desktop

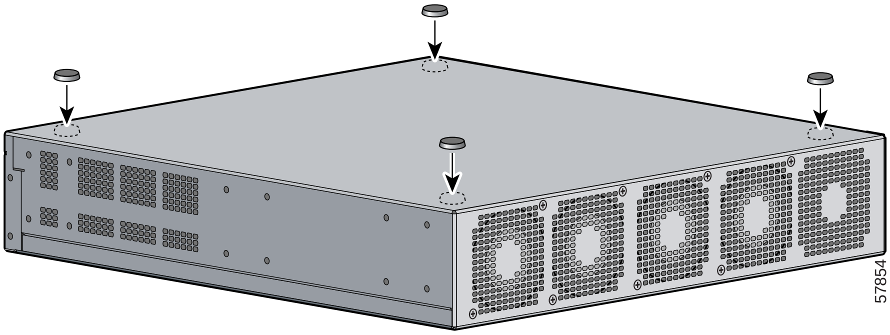
Use the four rubber feet included with the accessory kit to prepare the Cisco 10720 Internet Router for desktop setup. To set up the router on a desktop, perform the following steps:

Step 1 Locate the rubber feet that came with the router.

Step 2 Attach an ESD-preventive wrist strap to your wrist, and to the router chassis or to a bare metal surface. (See the “Preventing Electrostatic Discharge” section on page 2-3 for additional information.)

Step 3 Turn the router upside down to expose the bottom panel.

Figure 3-8 Applying Rubber Feet to the Bottom of the Router Chassis



Step 4 Pull the adhesive paper off the rubber feet and apply them to the bottom of the router. (See Figure 3-8.)

Caution The front and back panels of the router require at least 6 inches clearance away from the wall or other items that can block proper airflow. The side panel requires 1 inch of clearance away from the wall or other items that can block proper airflow. The top and bottom of the router chassis do not require any specific clearance.

Step 5 Turn the router over and set it on a desktop or other level surface that provides the necessary ventilation clearance.

Grounding the Cisco 10720 Internet Router

If the router is installed in a Network Equipment Building System (NEBS) environment, follow the guidelines in this section. For installations other than in a NEBS environment, you may chose to rely on the safety earth ground connection supplied via the International Electrotechnical Commission (IEC) 320 plugs for the AC power supply and DC power supply.

For additional NEBS information, see the *Regulatory Compliance and Safety Information for the Cisco 10720* document.

Supplemental Unit Bonding and Grounding Guidelines

If the router is not installed in a NEBS environment, you can bypass these guidelines and rely on the safety earth ground connection supplied via the IEC 320 plugs for the AC power supply and DC power supply.

Bonding and grounding receptacles are intended to satisfy the Telcordia NEBS requirements for supplemental bonding and grounding connections. The router requires a safety earth ground connection as part of the power cabling to the AC and DC power supplies.

We strongly recommend that you connect the central office (CO) ground system or interior equipment grounding system to the chassis. Grounding to the CO system or your interior equipment grounding system meets the NEBS bonding and grounding requirement.

Use a dual-hole cable lug to attach it to the chassis. Use two 6.3 mm (M6) screws on the 0.63-inch (16 mm) centers as shown in Figure 3-9, Figure 3-10, and Figure 3-11. The lug can be ordered from Cisco (Part Number 32-0607-01). Grounding connectors shall be NRTL listed; use copper conductors only for grounding and bonding connectors.

Figure 3-9 Cable Lug

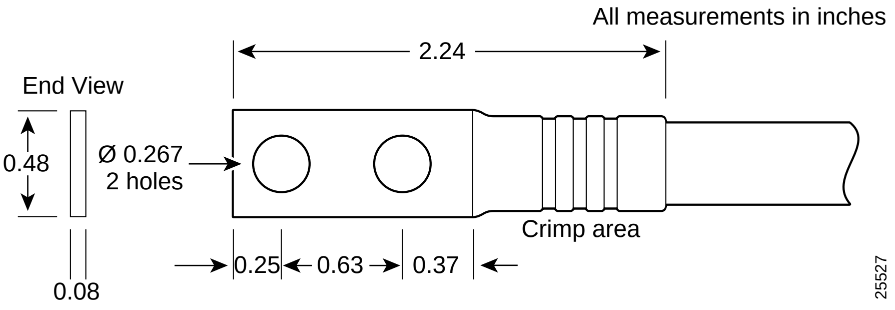
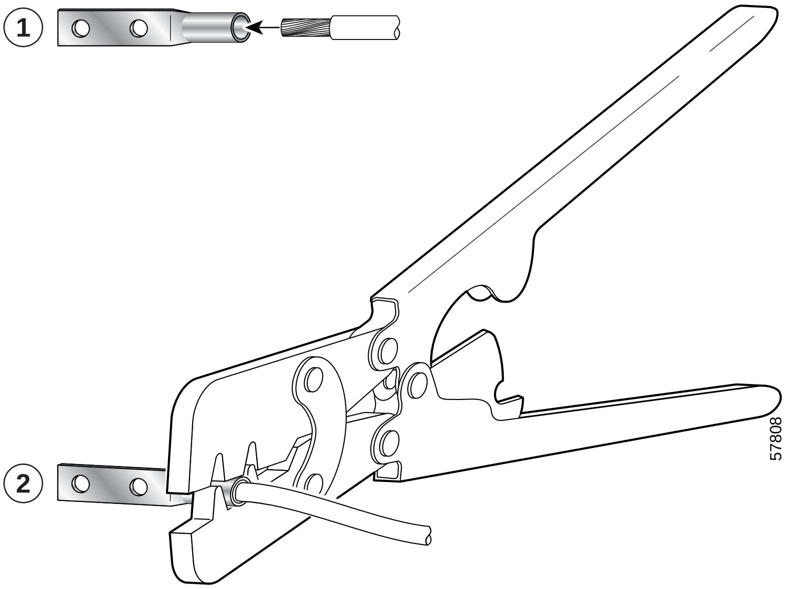
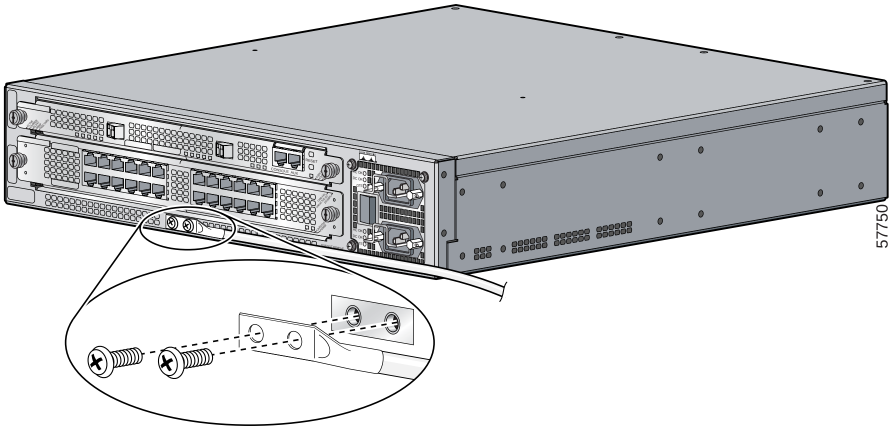


Figure 3-10 Crimping the Lug



1	Place ground wire in the lug	**2**	Crimp the lug

Figure 3-11 Attaching the Grounding Lug to the Router Chassis



SONET Distance Limitations

The maximum distance for single-mode installations is determined by the amount of light loss in the fiber path. Good quality single-mode short-reach optical cable with very few splices can carry an uplink card signal 2 km. A single-mode, intermediate-reach optical cable signal can carry an uplink card signal up to 15 km.

If your environment requires the signal to travel close to the typical maximum distance, use an Optical Time Domain Reflectometer (OTDR) to measure the power loss.

Caution Splicing can degrade cable performance.

Note Single-mode fiber-optic cables are available from a variety of vendors. These cables are not available from Cisco Systems.

Fiber Cables and Connectors

For SONET/SDH single-mode fiber-optic connections, use two simplex optical cables (see Figure 3-12) or one duplex optical cable (see Figure 3-13).

Warning **Class 1 laser product.** Statement 1008

Warning **Class 1 LED product.** Statement 1027

Warning **Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.** Statement 125

Note The fiber-optic connectors must be free of dust, oil, and other contaminants. Carefully clean the fiber-optic connectors using a fiber cleaning kit. See the *Inspection and Cleaning Procedures for Fiber Optic Connections* document for specific information and instructions.

Figure 3-12 Simplex Optical Cable

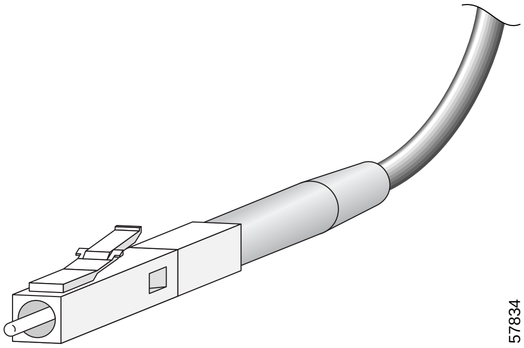
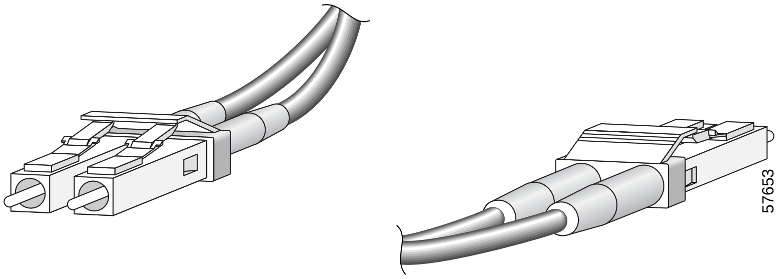


Figure 3-13 Duplex Optical Cable



Attach either one duplex optical cable or two simplex optical cables between the card and the device to which the card is connected. (See Figure 3-16.)

Connecting Ports on the Uplink Cards

Before connecting the ports on an uplink card, install the cable-management tray. For more information, see the "Removing and Installing the Cable-Management System" section on page 5-68.

For cable and connection specifications, refer to the *Cisco 10720 Internet Router Uplink Cards Installation and Configuration* publication.

To connect the ports on the DPT or POS uplink card, or the RPR/SRP uplink card, follow these instructions:

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Verify that the router is turned off and disconnected from its power source.

Installing the OC48 SFP Modules in the RPR/SRP Uplink Card

Use the information in this section to install OC48 SFP modules in the RPR/SRP uplink card.

Note Use only OC48 SFP modules purchased from Cisco Systems.

To install a bale clasp OC48 SFP module in the uplink card, perform the following steps:

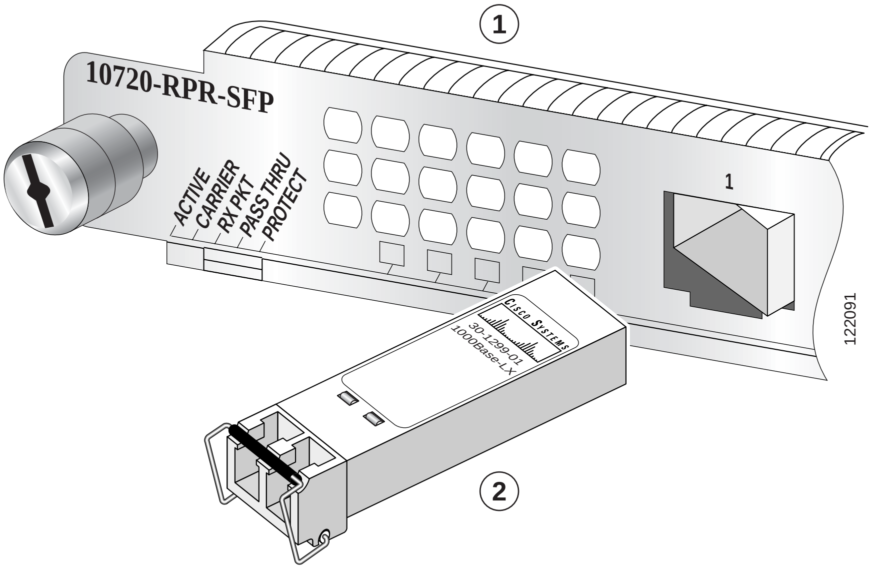
Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Pull the SFP cage cover from the SFP cage.

Step 3 Hold the SFP module with the hardware label facing up, as illustrated in Figure 3-14.

Caution The SFP module must be inserted with the hardware label facing up to avoid damaging the SFP module or uplink card.

Figure 3-14 Installing the Bale Clasp SFP Module in the RPR/SRP Uplink Card



1	RPR/SRP uplink card	2	OC48 SFP module

Step 4 Close the bale clasp on the SFP module by pushing the clasp in the upward direction before inserting the SFP module.

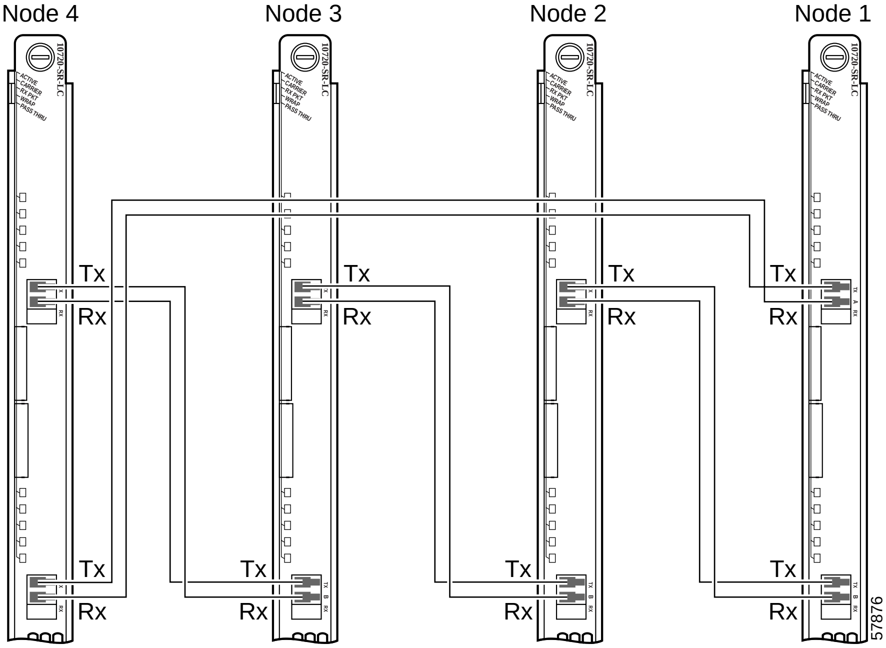
Step 5 Insert the SFP into the appropriate OC48 port and gently push on it until the SFP module snaps into the slot. (See Figure 3-14.)

For some basic troubleshooting tips, see the "Basic Troubleshooting SRP for the Uplink Card" section on page 4-7.

Creating a Four-Node DPT Ring

Create a four-node DPT ring by connecting the fiber-optic cables to DPT uplink cards that are installed in routers on the network. To create a four-node DPT ring, perform the following steps:

Figure 3-15 Creating a DPT Ring Using Uplink Line Cards



Step 1 Install a DPT uplink card in a Cisco 10720 Internet Router on the network.

Step 2 Choose a router with an uplink card to become Node 1 in the four-node DPT ring.

Note The TX side B port on Node 1 goes to the RX side A port on the next router, which will become Node 2. The labels above the fiber connectors identify side A (left port) TX and RX, and side B (right port) TX and RX. (See Figure 3-15.)

Step 3 Add other nodes to the ring by connecting the receive (RX) and transmit (TX) cables. The RX port on one uplink card must be connected to a TX port on the next uplink card. (See Figure 3-15.)

Use Figure 3-15 and Table 3-1 to help organize the cable connections for a four-node DPT ring. Figure 3-16 provides a view of the network when a four-node DPT ring is created.

Figure 3-16 Four-node DPT Ring

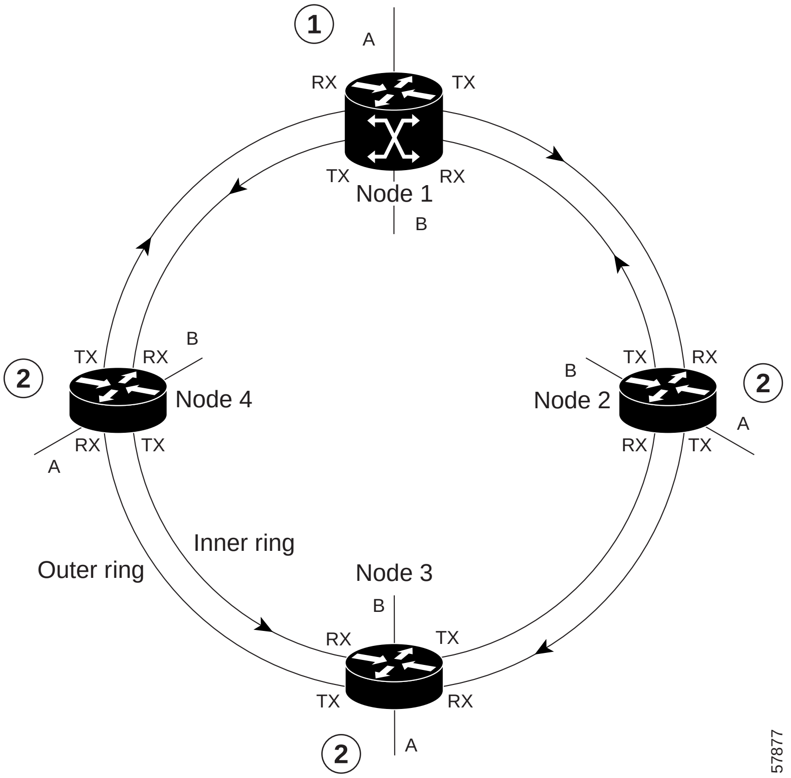


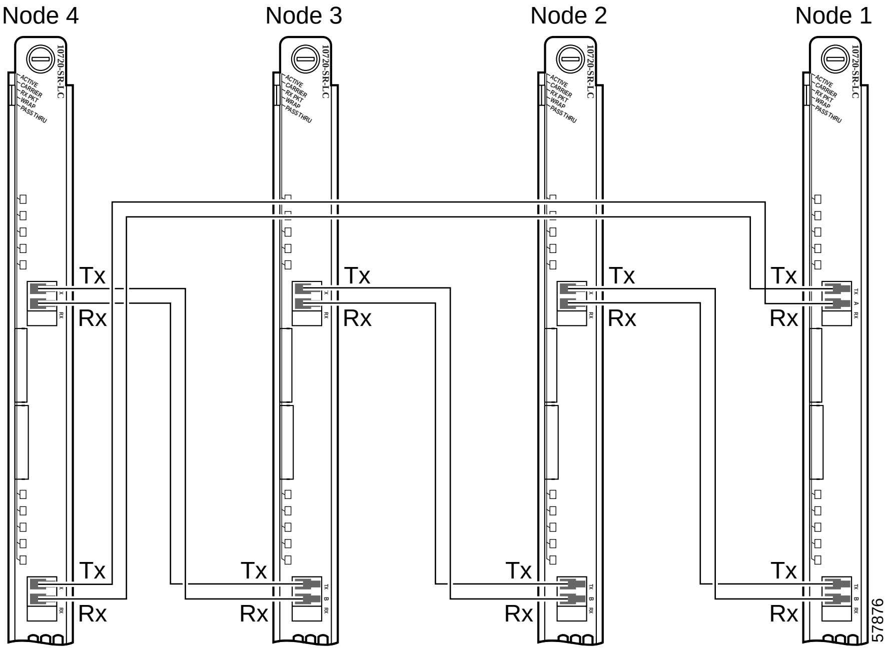
Table 3-1 Cable Connections for a Four-Node DPT Ring

Cable Connections	
From Node / Connector	**To Node / Connector**
Node 1 / TX side B	Node 2 / RX side A
Node 2 / TX side B	Node 3 / RX side A
Node 3 / TX side B	Node 4 / RX side A
Node 4 / TX side B	Node 1 / RX side A
Node 1 / TX side A	Node 4 / RX side B
Node 4 / TX side A	Node 3 / RX side B
Node 3 / TX side A	Node 2 / RX side B
Node 2 / TX side A	Node 1 / RX side B

Creating a Four-Node IEEE 802.17 RPR Mode Ring

Use Figure 3-17 and Table 3-2 to help organize the cable connections for a four-node IEEE 802.17 RPR mode ring.

Figure 3-17 Creating an IEEE 802.17 RPR Mode Ring Using RPR/SRP Uplink Cards



The TX span East port on Node 1 goes to the RX span West port on the next router, which will become Node 2. The labels above the fiber connectors identify span West (left port) TX and RX, and span East (right port) TX and RX. (See Figure 3-17.)

Create a four-node IEEE 802.17 RPR mode ring by connecting the fiber-optic cables to RPR/SRP uplink cards that are installed in routers on the network. To create a four-node IEEE 802.17 RPR mode ring, perform the following steps:

Step 1 Install an RPR/SRP uplink card in a Cisco 10720 Internet Router on the network.

Step 2 Choose a router with an RPR/SRP uplink card to become Node 1 in the four-node IEEE 802.17 RPR mode ring.

Step 3 Add nodes to the ring by connecting the receive (RX) and transmit (TX) cables. The RX port on one RPR/SRP uplink card must be connected to a TX port on the next RPR/SRP uplink card.

Table 3-2 Cable Connections for a Four-Node IEEE 802.17 RPR Mode Ring

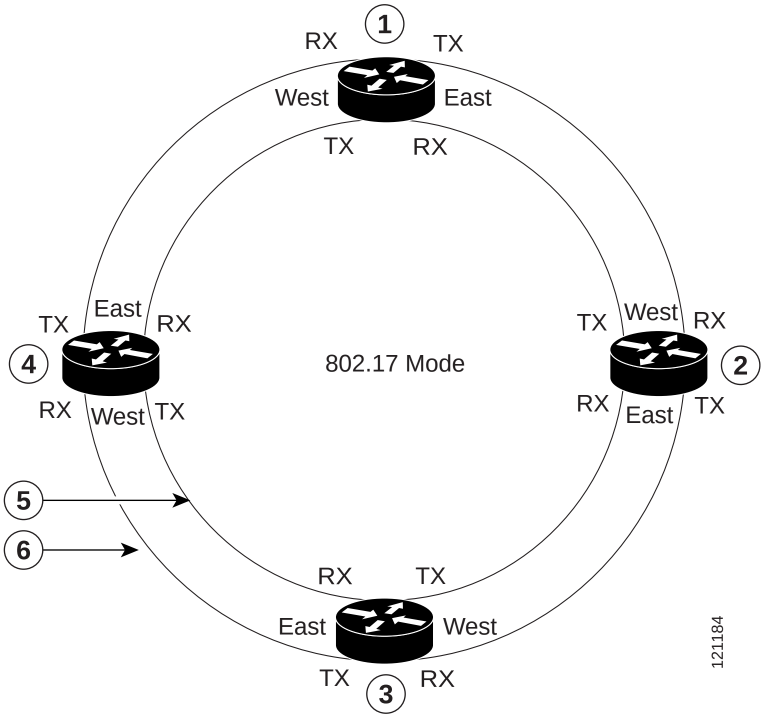
Cable Connections	
From Node / Connector	**To Node / Connector**
Node 1 / TX span East	Node 2 / RX span West
Node 2 / TX span East	Node 3 / RX span West

Table 3-2 Cable Connections for a Four-Node IEEE 802.17 RPR Mode Ring (continued)

Cable Connections	
Node 3 / TX span East	Node 4 / RX span West
Node 4 / TX span East	Node 1 / RX span West
Node 1 / TX span West	Node 4 / RX span East
Node 4 / TX span West	Node 3 / RX span East
Node 3 / TX span West	Node 2 / RX span East
Node 2 / TX span West	Node 1 / RX span East

Figure 3-18 provides a view of the network when a four-node IEEE 802.17 RPR mode ring is created.

Figure 3-18 Four Node IEEE 802.17 RPR Mode Ring



1	Node 1	**4**	Node 4
2	Node 2	**5**	Inner Ring—Ringlet 1
3	Node 3	**6**	Outer Ring—Ringlet 0

Additional Ports on the Uplink Cards

You can connect the console or serial (AUX) port on the uplink cards to any of the following:

- Terminal server
- Access server
- Modem
- Desktop computer
- Laptop
- Terminal

The console and AUX ports are located on the right side of the uplink card.

Note Cisco Systems does not provide AUX port cables. Cables are available from commercial cable vendors.

Attaching a Terminal Server or Access Server to the Console or AUX Port

To connect a terminal server or access server to the AUX port of the router, do the following:

Note Attaching a terminal server or access server to the AUX port is a default setting.

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Verify that the terminal server is turned off and disconnected from its power source.

Step 3 Attach the terminal server end of the RJ-45 cable to the interface port on the terminal server.

Step 4 Attach the other end of the RJ-45 cable to the router console or AUX port.

Step 5 Configure the terminal server for reverse Telnet.

Step 6 Use the default configuration value on the console port or AUX port to configure the terminal router.

Step 7 Use the following configuration on the asynchronous port:

```
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
  no ip directed-broadcast
!
line 8 <=the c10720 console or AUX port is connected to line 8
exec-timeout 0 0 <==(Optional) make the telnet connection over this line not to timeout
forever
transport input all <==allow reverse telnet
```

Step 8 To reverse Telnet to the router from the terminal server, use the following command on a PC in the network:

```
C:> telnet 10.1.1.1 2008
```

Attaching a Modem to the Console or AUX Port

To connect a modem to the AUX port on the router, do the following:

Note Attaching a modem to the AUX port is a default setting.

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Verify that the modem is turned off and disconnected from its power source.

Step 3 Attach an adapter marked "MODEM" (Part Number CAB-25AS-MMOD) to the modem end of the RJ-45-to-RJ-45 cable.

Step 4 Connect the interface port to the modem.

Step 5 Attach the other end of the RJ-45 cable to the router AUX port.

Step 6 Configure the router for modem dial-in by using the **interface asychronous 1** and **line aux 0** commands in the following configuration example:

```
!
hostname Esop
!
enable password Sherman
!
username Peabody password 0 Sherman <= user name and password for dial-in PPP
authentication
!
interface asynchronous 1
 ip address 145.168.1.1 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer in-band <= Allow asynchronous dial-in
 async mode interactive
 peer default ip address 150.168.1.100 <= assign a ip address to the remote PC
 ppp authentication chap <= PPP authentication with CHAP
!
!
line aux 0
 password cisco
 login
 modem InOut <=allow modem dial in and dial out
 modem autoconfigure type usr_sportster <=specify the modem type
 autoselect during-login
 autoselect ppp <=Launch PPP when dial-in is successful.
 transport input all <=allow all types of terminal sessions, such as telnet
 stopbits 1
 speed 19200
 flowcontrol hardware
!
end
```

Connecting a Desktop Computer, Laptop, or Terminal to the Console or AUX Port

When a desktop computer, laptop, or terminal is connected directly to the console port, you can always access the router at any privilege level without an **enable** password or **enable secret** global configuration command configured on the router. (See the "Assigning Passwords" section on page 3-33.)

The AUX port requires an **enable** password or **enable secret** password configured on the router; otherwise, the desktop computer, laptop, or terminal cannot access the enable mode of the router.

The asynchronous interface (interface async 1) can be configured for line 1, which is the AUX port. The AUX port can be connected to a modem. However, no asynchronous interface can be configured for the console port; therefore, the console port cannot connect to a modem.

The console and AUX ports support different baud rates:

- Console—9600 (non-configurable)
- AUX—4800 to 115200 (configurable)

To connect the router to a desktop computer, laptop, or terminal via the console or AUX port, perform the following:

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Verify that the desktop computer, laptop, or terminal is turned off and disconnected from its power source.

Step 3 Attach the desktop computer, laptop, or terminal end of the RJ-45-to-DB9 female connector cable to the computer or terminal serial port on the router.

Step 4 Attach the other end of the RJ-45 cable to the router console or AUX port.

Note For more information, refer to the *Cabling Guide for Console and AUX Ports* guidelines at http://www.cisco.com/warp/public/701/14.html.

Step 5 Configure the router and the desktop computer, laptop, or terminal using the default configuration values for the console port or AUX port. (See Table 3-3.)

Table 3-3 Cisco 10720 Internet Router Default Port Configurations

Function	Default Settings
Speed	9600
Data bit	8
Stop bit	2
Parity	–
Flow control	–

Step 6 Configure the desktop computer, laptop, or terminal serial port with the same port configuration values required by the router. (See Table 3-3.)

Connecting Ethernet Ports on the Access Card

Install the cable-management tray before you connect the copper or optical fiber cable to a Fast Ethernet port or to an SFP module on the Gigabit Ethernet port on the access card. For more information, see the "Removing the Cable-Management System" section on page 5-68.

For cable and connection specifications, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication. See Figure 3-21 for an example of a typical cable used for the access card.

To connect the interface cables to the access card ports, perform the following:

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. See the "Preventing Electrostatic Discharge" section on page 2-3.

Step 2 Verify that the router is turned off and disconnected from its power source

Installing a small form-factor pluggable Gigabit Ethernet (GE) (SFP) module in the access card GE port is described in the following sections:

- Installing a Bale Clasp SFP, page 3-22
- Installing a Latch SFP, page 3-23

Note You do not need to power down the router before you install an SFP. The router may remain powered up during this procedure.

Note The Fast Ethernet ports are suitable for connection to intra-building wiring only, as per GR-1089, Issue 3.

Installing a Bale Clasp SFP

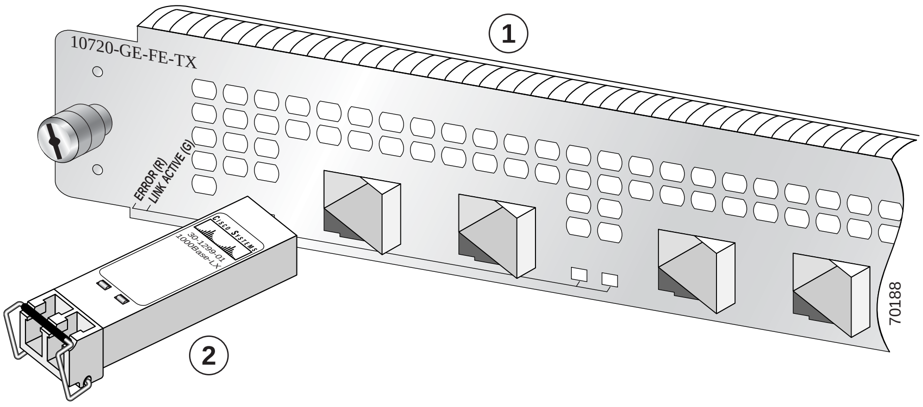
To install a bale clasp GE SFP module in the access card, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Hold the SFP module with the hardware label facing up, as illustrated in Figure 19.

Caution The SFP module must be inserted with the hardware label facing up to avoiding damaging the SFP module or the access card.

Figure 19 Installing the Bale Clasp SFP Module in the Access Card



1	4-Port Gigabit Ethernet 8-Port 10/100BASE-TX access card	**2**	SFP module

⚠ **Caution** Close the bale lever on the SFP module prior to inserting the SFP module into the port cage to ensure proper engagement. The bale lever is considered closed when it is in the upright position. See Figure 3-14. If the bale lever is left open during insertion, there is a possibility that the SFP module may become stuck in the port cage. To remove the SFP module, use a small flathead screwdriver to gently lift the cage tongue (located underneath the SFP module) away from the SFP module body, thus disengaging the SFP module. The SFP module is not damaged by this operation.

Step 3 Close the bale clasp in the upward direction before inserting the SFP module.

Step 4 Insert the SFP into the appropriate Gigabit Ethernet slot and gently push on it until the module snaps into the slot tightly. (See Figure 19.)

Installing a Latch SFP

To install a latch SFP module in the access card, perform the following steps:

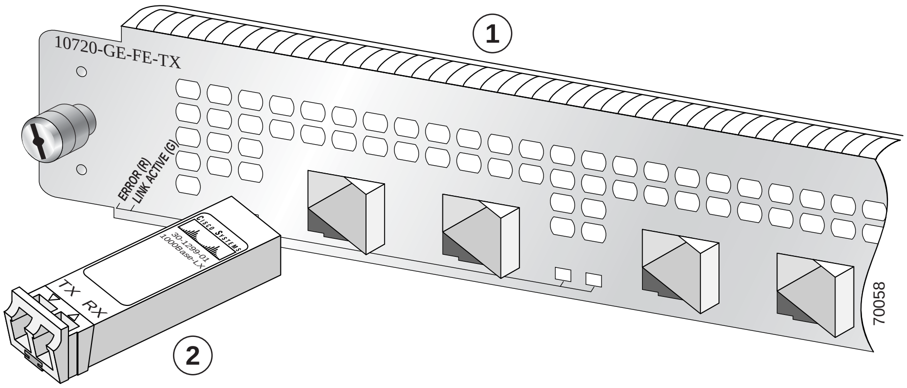
Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Hold the SFP module with the hardware label facing up, as illustrated in Figure 20.

⚠ **Caution** The SFP module must be inserted with the hardware label facing up to avoiding damaging the SFP module or the access card.

Step 3 Insert the SFP into the appropriate Gigabit Ethernet slot and gently push on it until the module snaps into the slot tightly. (See Figure 20.)

Figure 20 Installing the Latch SFP Module in the Access Card



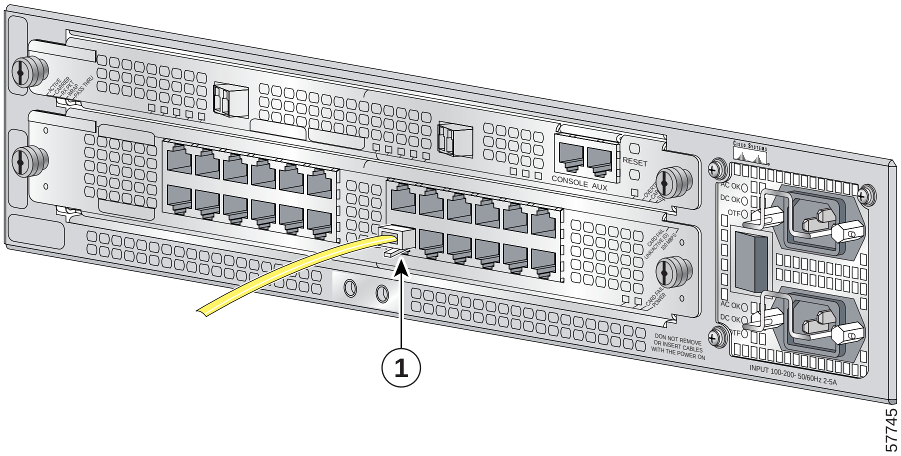
1	4-Port Gigabit Ethernet 8-Port10/100BASE-TX access card	**2**	SFP module

Note Before installing optical fiber cables, clean the optical fiber cable connection. See the *Inspection and Cleaning Procedures for Fiber-Optic Connections* document.

Step 4 Connect the appropriate interface cable to the access card. (See Figure 3-21 for an example.)

Note For specific cabling specifications, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.

Figure 3-21 Connecting the Interface Cable (Typical)


CONSOLE AUX
RESET
CISCO SYSTEMS
AC OK
DC OK
OTF
DO NOT REMOVE OR INSERT CABLES WITH THE POWER ON
INPUT 100-200- 50/60Hz 2-5A
1
57745

1	Ethernet interface cable		

In-Band Ethernet Port

In-band Ethernet is connected to the hub by using one of the Fast Ethernet or Gigabit Ethernet ports on the access card. Out-of-band Ethernet is not available on the Cisco 10720 Internet Router.

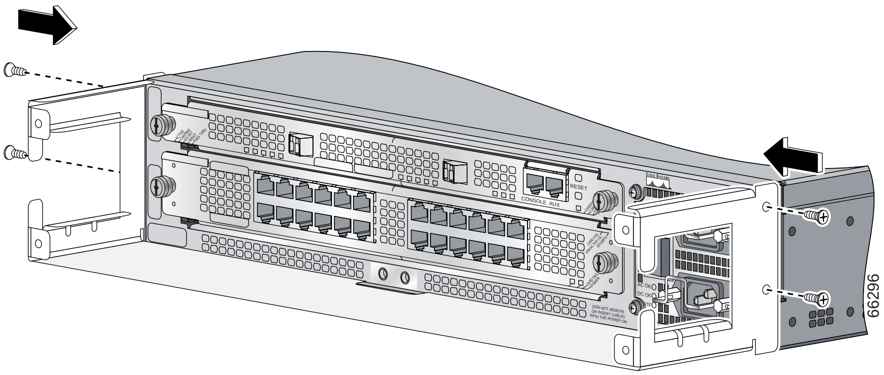
Installing the Cable-Management System

The cable-management system, located on the front of the router, organizes the interface cables. To keep the cables free of sharp bends, extend the cables from the center out both sides of the cable-management system. Excessive bending of an interface cable can degrade performance and possibly harm the cable.

Perform the following steps to install the cable-management system:

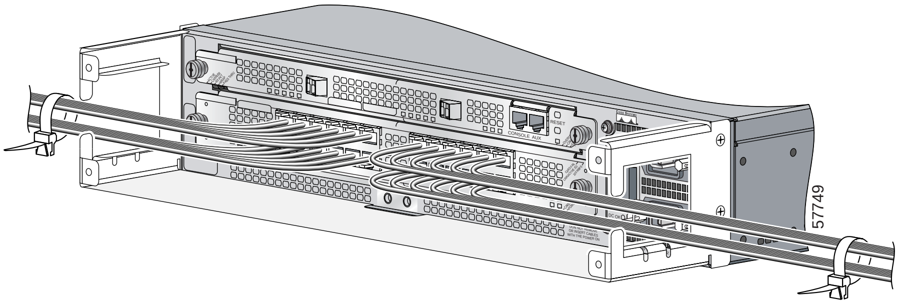
Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Figure 3-22 Attaching the Cable-Management Tray



Step 2 Attach the cable-management tray to the router using four of the 3.5-mm x 6-mm screws that are shipped with the router. Secure the tray with two screws on each side of the router chassis using a Number 1 Phillips screwdriver. (See Figure 3-22.)

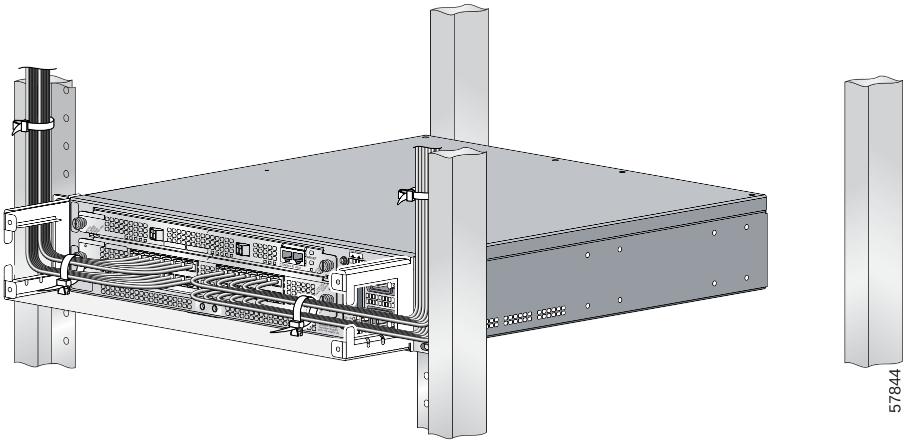
Figure 3-23 Managing Router Cables with the Cable-Management Tray



Step 3 Separate cables and lead them out the sides of the cable-management tray. Use a cable tie to keep the cables together. (See Figure 3-23.)

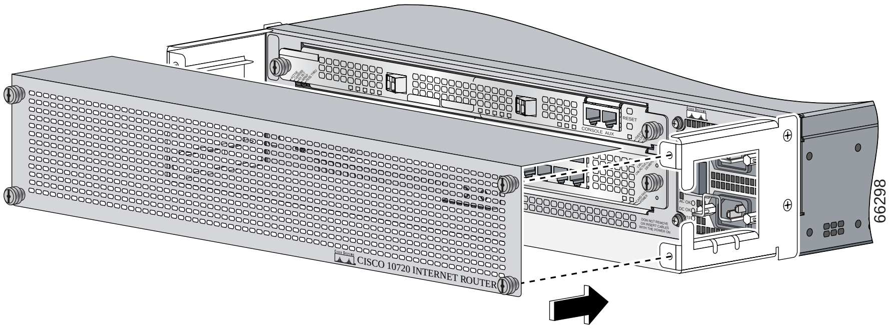
Caution To avoid damage to the cables, avoid excessive bending.

Figure 3-24 Cable-Management Tray and Router Installed in a Rack



Step 4 Use cable ties to secure the cables to the equipment mounting rack to keep the wires from accidental bends or breaks. (See Figure 3-24.)

Figure 3-25 Installing the Cable-Management Cover



Step 5 Using a Number 1 Phillips screwdriver, attach the cable-management cover to the cable-management tray. (See Figure 3-25.)

Go to the "Turning On Power to the Router" section on page 3-26 for information on powering on the router.

Turning On Power to the Router

Perform the following steps to restore power to the router:

- Connecting the AC Power Supply, page 3-27
- Connecting the DC Power Supply, page 3-29

Connecting the AC Power Supply

Warning **Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication. This publication contains important safety information you should know before working with the system.**

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

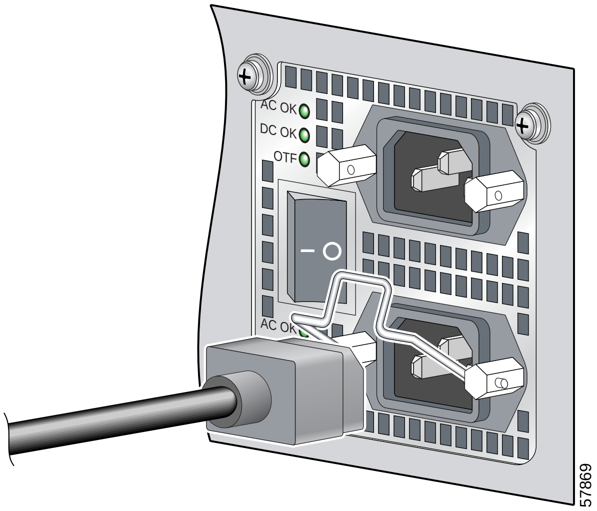
Note For additional information, refer to the *Cisco 10720 Internet Router AC and DC Power Supply Replacement Instructions*. This configuration note is available on Cisco.com or ordered as a printed document. Field replacement documentation is available electronically, by default. If you prefer printed documentation, order it online.

Note We recommend that you attach each AC-input power supply to a dedicated power source for redundancy and use an uninterruptable power supply (UPS) to protect against power failures. Each AC power supply operating between 100 and 240 VAC requires a dedicated 15 A electrical power service for North America, 10 A electrical power service for international specifications.

Perform the following steps to connect the AC power supply:

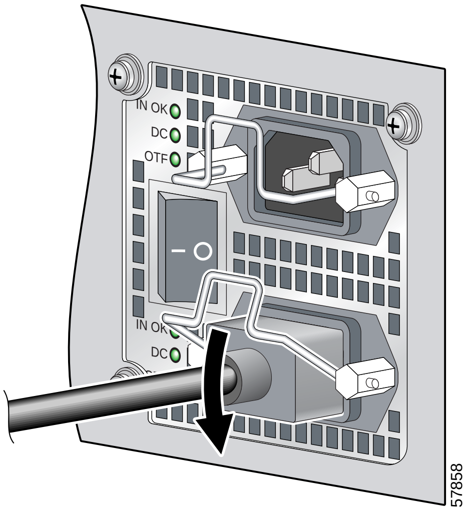
Step 1 Confirm that the power switch on the router is in the off (O) position. (See Figure 3-26.)

Figure 3-26 AC Power Cord Connected to the Router



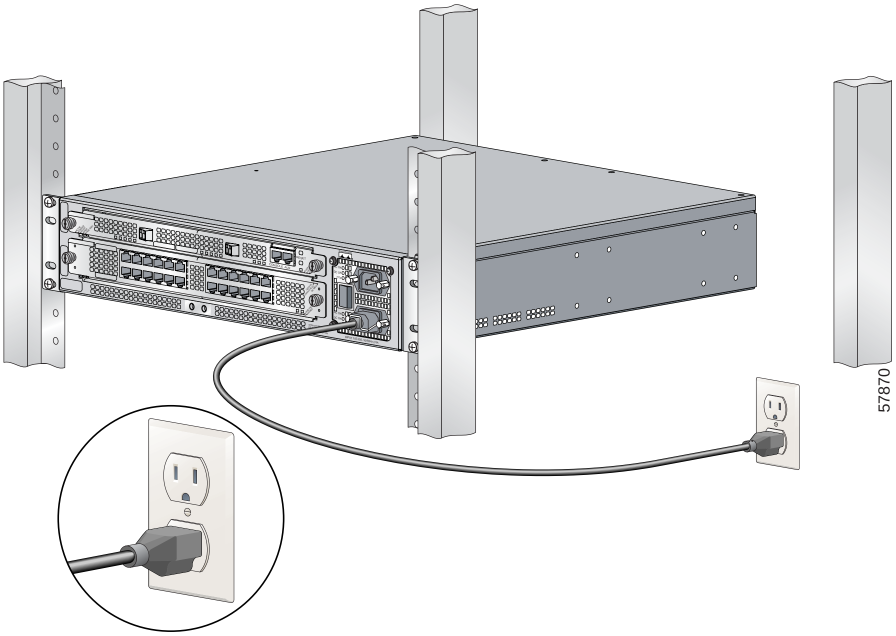
Step 2 Connect the AC power cord to the AC power supply receptacle on the router. (See Figure 3-26.)

Figure 3-27 *Power Cord Secured with a Wire Bracket*



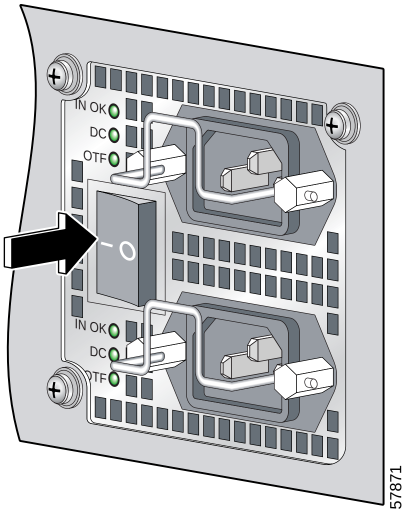
Step 3 Close the wire bracket over the power cord plug. (See Figure 3-27.)

Figure 3-28 *Router Connected to the Power Source*



Step 4 Connect the other end of the AC power cord to the AC power source outlet. (See Figure 3-28.)

Figure 3-29 Power Switch in the On Position



Step 5 Press the power switch to on the (–) position. (See Figure 3-29.)

Connecting the DC Power Supply

Warning **When you install the unit, the ground connection must always be made first and disconnected last.** Statement 42

Warning **Before performing any of the following procedures, ensure that the power is removed from the DC circuit. Ensure that power is removed from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit. Switch the circuit breaker to the off (O) position, and tape the switch handle of the circuit breaker in the off (O) position.** Statement 140

Note The battery return connection is to be treated as an isolated DC return (i.e. DC-I), as defined in GR-1089-CORE, Issue 3.

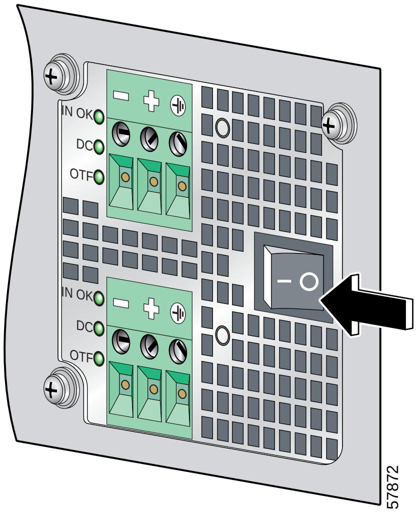
Note The minimum wire gauge size supported on the DC dual power supply is 17 American Wire Gauge (AWG), which has a 1.5mm wire diameter. The maximum wire gauge size supported on the DC dual power supply is 10 AWG, which has a 6mm wire diameter.

Connect the DC power supply by performing the following steps:

Step 1 Verify that the –48V and +48V leads are disconnected from the power source.

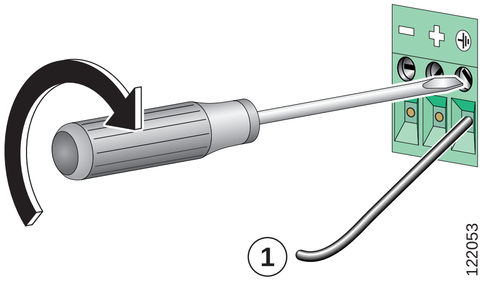
Step 2 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Figure 3-30 Power Switch in the Off Position



Step 3 Verify that the power switch located on the front of the power supply is in the off (O) position. (See Figure 3-30.)

Figure 3-31 Tightening the DC Lead Receptacle

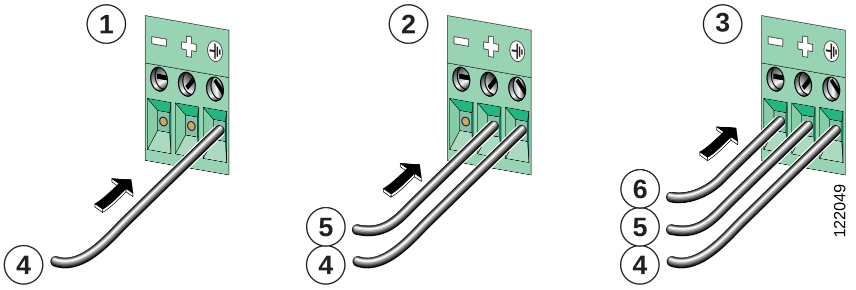


1	Ground lead		

Step 4 Insert the stripped end of the ground lead all the way into the ground lead receptacle on the DC-input power supply and tighten the receptacle screw using a 1/8-inch flat-blade screwdriver. (See Figure 3-31.)

Note Make sure the entire stripped end of each lead is inserted all the way into its receptacle. If any exposed wire at the stripped end of a lead is visible after inserting the lead into its receptacle, remove the lead from the receptacle. Use a wire cutter to cut the stripped end of the lead to fit the receptacle.

Figure 3-32 Connecting the DC Power Leads



1	Ground lead connected	**4**	Ground lead
2	Positive lead connected	**5**	Positive lead
3	Negative lead connected	**6**	Negative lead

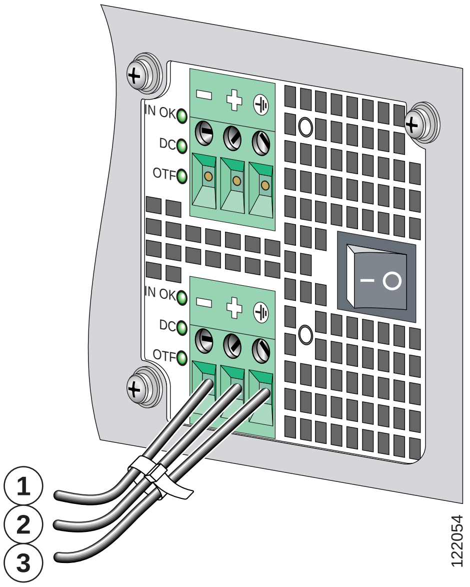
Step 5 Connect the power leads in the following order:

a. Ground (green wire) (See 4 in Figure 3-32.)

b. Positive (white wire) (See 5 in Figure 3-32.)

c. Negative (black wire) (See 6 in Figure 3-32.)

Figure 3-33 DC Power Leads Secured with a Cable Tie



1	Negative lead	**3**	Ground lead
2	Positivelead		

Step 6 After tightening the receptacle screw for the ground, +48V, and –48V DC-input leads, use cable ties to secure the three leads. (See Figure 3-33.)

Note Leave a small service loop in the ground lead to ensure that the ground lead is the last lead to disconnect from the power supply if a great deal of strain is placed on the DC-input leads. It is important that the ground power lead is the last to disconnect from the power supply terminal.

Note Allow sufficient slack in the power cable leads for strain relief. The power cable leads should be adequately secured to prevent the power supply terminal connections from being subjected to strain.

Step 7 After wiring the DC power supply, remove the tape from the circuit breaker switch handle and turn on power by moving the handle of the circuit breaker to the on position.

If you are installing the cable-management system, go to the "Verifying the Router Power Is Turned On" section on page 3-32. If not, install the cables, and then power up the router.

Verifying the Router Power Is Turned On

Check the following to ensure the router is properly powered on:

- LED lights are on.
- Fans are running.
- Power switch indicates router is turned on.

Initial Setup Configuration

The initial setup configuration for the router is presented in the following sections:

- Configuring the Router, page 3-32
- Configuring Global Parameters Using the Setup Facility, page 3-33

Configuring the Router

Perform a basic configuration for the router by using either of the following methods:

- Method 1—Using the setup facility or the **setup** command.

  During the startup of an unconfigured router, the system automatically starts the setup facility. The setup facility enables manual configuration of the router. The setup facility provides a structured, interactive script to set up the router.

- Method 2—Using the global configuration mode through the command line user interface.

You will need the following information before you set up the router:

- Router interfaces
- Router protocols
- Network addresses for the protocols being configured
- Password scheme

Configuring Global Parameters Using the Setup Facility

When using the setup facility or the **setup** command, the system prompts the user to configure global parameters for the router. Global parameters are used for controlling system-wide settings, including the following:

- Host name for the router
- Passwords for the enable secret, enable, and virtual terminal security parameters
- Protocols used by the router

Host Name

The name assigned to the router must follow the rules for ARPANET host names. It must start with a letter, end with a letter or digit, and have only letters, digits, and hyphens. The name must consist of 63 or fewer characters. For more information, refer to *RFC 1035, Domain Names—Implementation and Specifications*.

Do not expect case to be preserved. Conventions dictate that computer names appear all lowercase. For more information, refer to *RFC 1178, Choosing a Name for Your Computer.*

Assigning Passwords

The commands available at the user EXEC level are a subset of those available at the privileged EXEC level. Many privileged EXEC commands are used to set system parameters. You should password-protect these commands to prevent their unauthorized use. For information on how to establish password protection or configure privilege levels, refer to the "Configuring Passwords and Privileges" chapter in the *Security Configuration Guide*. The publication is located in the Cisco IOS software configuration documentation set that corresponds to the Cisco IOS software release installed on your Cisco hardware.

The **enable secret** password functionality is available for the Cisco 10720 Internet Router. Enter the correct password to gain access to privileged-level commands. When ROM monitor is active, the **enable** password can be used, depending on the boot ROM level.

For maximum security, the **enable secret** and the **enable** passwords should be different. If the same password is used for both the **enable secret** and the **enable** functions during the setup process, the system accepts it, but issues a warning indicating that two distinct passwords should be entered.

An **enable secret** password can contain from 1 to 25 uppercase and lowercase alphanumeric characters. An **enable** password can contain any number of uppercase and lowercase alphanumeric characters.

Verifying the Cisco 10720 Internet Router LEDs

The router LEDs are included on the access and uplink cards. The access and uplink cards each contain two sets of LEDs:

- System LEDs
- Status LEDs

The system LEDs inform the user of the condition of the router, while the uplink or access card status LEDs inform the user of the condition or status of the card itself.

The following sections provide information about the uplink card system, uplink card status, access card system, and access card status LEDs:

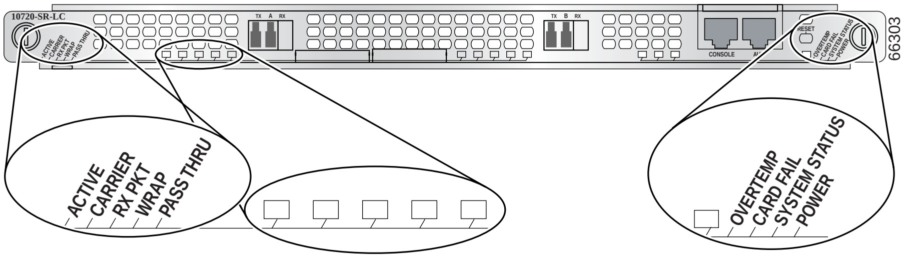
- Uplink Card System LEDs, page 3-34
- Uplink Card Status LEDs, page 3-36
- Access Card System LEDs, page 3-38
- Access Card Status LEDs, page 3-39

Uplink Card System LEDs

Warning **Avoid exposure to laser radiation. Do not stare into an open aperture, because invisible laser radiation may be emitted from the aperture when a cable is not inserted in the port.** Statement 125

The uplink card system LEDs provide information on the functionality of the uplink card in the router. The system LEDs are located on the right side of the uplink card. See Figure 3-34 LEDs on the DPT and POS/DPT uplink cards.

Figure 3-34 DPT and POS/DPT Uplink Card LEDs (Left) and System LEDs (Right)



The configuration of the router will affect the uplink LEDs. Possible variations include optical cable connections and temperature.

Table 3-4 provides a description of the system LEDs on a DPT or POS/DPT uplink card. Table 3-5 provides a description of the LEDs on an RPR/SRP uplink card.

Note The color of the LEDs is green/red on the DPT and POS/DPT uplink cards, and green/amber on the RPR/SRP uplink card.

Note Table 3-4 and Table 3-5 also indicate the system status of the uplink card as it initializes.

Table 3-4 DPT and POS/DPT Uplink Card System LEDs

LED	Activity	Description
OVERTEMP	Green (default status when initialized)	System is operating within the proper temperature range. (inlet <104^{o}F [40^{o}C]; outlet <109^{o}F [43^{o}C])
	Red/Green	Both LEDs are on, appearing *orange*. Systems working on warning temperature range. (104^{o}F [40^{o}C] <= inlet < 122^{o}F [50^{o}C], 109^{o}F [43^{o}C] <= outlet< 127^{o}F [53^{o}C])
	Red	System is working on critical temperature state. (122^{o}F [50^{o}C] <= inlet < 149^{o}F [65^{o}C], 127^{o}F [53^{o}C] <= outlet < 167^{o}F [75^{o}C])
CARD FAIL	Red	A hardware failure is being detected on the uplink card. During power up, the LED will be red, even when the uplink card is powered down.
	Off (default status when initialized)	Card is operational. The LED is turned off after hardware initialization.
SYSTEM STATUS	Red	Not applicable.
	Red/Green	Both LEDs are on, appears orange. This is the normal configuration during power up. Once the software loads successfully, the red LED will turn off.
	Green (default status when initialized)	System is operational.
POWER	Green (default status when initialized)	The uplink card is receiving power from the system[1].
	Off	Uplink card is not receiving power from the system.

[1] System power up is not an indication that the uplink card is powered up. Check the card status LEDs to ensure the card is functional properly and is receiving power form the system.

Figure 3-35 RPR/SRP Uplink System LEDs

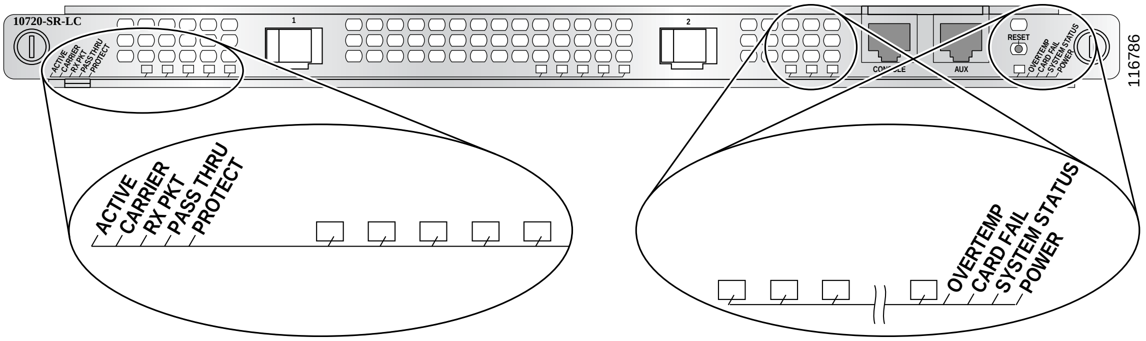


Table 3-5 RPR/SRP Uplink Card System LEDs

LED	Activity	Description
OVERTEMP	Green (default status when initialized)	System is operating within the proper temperature range. (inlet <104^{o}F [40^{o}C]; outlet <109^{o}F [43^{o}C])
	Amber/green	Both LEDs are on (appears orange*)*. System is working on warning temperature range. (104^{o}F [40^{o}C] <= inlet < 122^{o}F [50^{o}C], 109^{o}F [43^{o}C] <= outlet < 127^{o}F [53^{o}C])
	Amber	System is working on critical temperature state. (122^{o}F [50^{o}C] <= inlet < 149^{o}F [65^{o}C], 127^{o}F [53^{o}C] <= outlet < 167^{o}F [75^{o}C])
CARD FAIL	Amber	A hardware failure is detected on the uplink card. During power up, the LED will be amber even when the uplink card is powered down.
	Off (default status when initialized)	Card is operational. The LED is turned off after hardware initialization.
SYSTEM STATUS	Amber	Not applicable.
	Amber/green	Both LEDs are on (appears orange). This is the normal configuration during power up. Once the software loads successfully, the amber LED will turn off.
	Green (default status when initialized)	System is operational.
POWER	Green (default status when initialized)	Uplink card is receiving power from the system.[1]
	Off	Uplink card is not receiving power from the system.

[1] System power up is not an indication that the uplink card is powered up. Check the card status LEDs to ensure the card is functioning properly and is receiving power from the system.

For more specific information on these and other uplink card LEDs, refer to the *Cisco 10720 Internet Router Uplink Cards Installation and Configuration* publication.

Uplink Card Status LEDs

Warning **Avoid exposure to laser radiation. Do not stare into an open aperture, because invisible laser radiation may be emitted from the aperture when a cable is not inserted in the port.** Statement 125

The DPT/POS uplink card status LEDs provide information on the operational status of the DPT or POS uplink card. The status LEDs are located on the left side of the DPT and POS uplink cards. See Figure 3-34 for an example of a typical DPT uplink card.

Table 3-6 provides a description of status LED activity on the DPT uplink card. Table 3-7 provides a description of status LED activity on the POS/DPT uplink card. Table 3-8 provides a description of status LED activity on the RPR/SRP uplink card.

Note The color of the LEDs is green/red on the DPT and POS/DPT uplink cards, and green/amber on the RPR/SRP uplink card.

Table 3-6 DPT Uplink Card Status LEDs

LED	Activity	Description
ACTIVE	Green	The port is active.
	Blinking red	Fiber misconnect is detected (that is, side A connected to neighbor side A).
	Off	The port is not active.
CARRIER	Green	Framer has locked onto the SONET frames.
	Off	Framer has not achieved lock.
RX PACKET	Green	Packets are being received on the port.[1,2]
	Off	No packets are being received on the port.
WRAP	Red	Port is in local wrap.
	Green	Wrap in system (for example, another port on the ring is wrapped).
	Off	No wrap (i.e., the port is operating normally).
PASS THRU	Green	Port is in Pass-thru mode.
	Off	Port is operating normally.

[1] Note that due to the SRP IP packets, this LED will remain permanently lit during normal SRP operation.

[2] After you shut down the port interface on the uplink card, the RX PKT LED remains on if SRP packets (including transit SRP packets) are still being received in Pass-thru mode. The RX PKT LED turns off if no SRP packets are received.

Table 3-7 POS/DPT Uplink Card Status LEDs

LED	Activity	Description
ACTIVE	Green	Port is active.
	Off	Port is not active.
CARRIER	Green	Framer has locked onto the SONET frames.
	Off	Framer has not achieved lock.
RX PACKET	Green	Packets are being received on the port.
	Off	No packets are being received on the port.
SRP WRAP	Off	Not applicable to POS.
SRP PASS THRU	Off	Not applicable to POS.

Note Note that the RPR/SRP uplink card uses the label "PROTECT" instead of "WRAP," and the positions of these two LEDs are different from that on the DPT or POS/DPT uplink card.

Table 3-8 RPR/SRP Uplink Status LEDs

LED	Activity	Description
ACTIVE	Green	Port is enabled by software. There is no side mismatch or loopback.
	Amber	Loopback is on.
	Blinking amber	Port is enabled by software and there is a side mismatch. There is no loopback.
	Off	Port is not enabled by software
CARRIER	Green	Port is up and there is a valid SONET signal without any alarms.
	Amber	Port is up and there is at least one alarm (LOS, LOF, RDI, and so on.)
	Off	Off.
RX PKT	Green	Framer is receiving packets.
	Off	Framer is not receiving packets.
PASSTHRU	Green	Port is in Pass-thru mode.
	Off	Port is operating normally.
PROTECT	Green	Remote wrap.
	Off	No wrap.
	Amber	Local wrap.
	Blinking green	Remote steer.
	Blinking amber	Local steer.

For more specific information on these and other uplink card LEDs, refer to the *Cisco 10720 Internet Router Uplink Cards Installation and Configuration* publication.

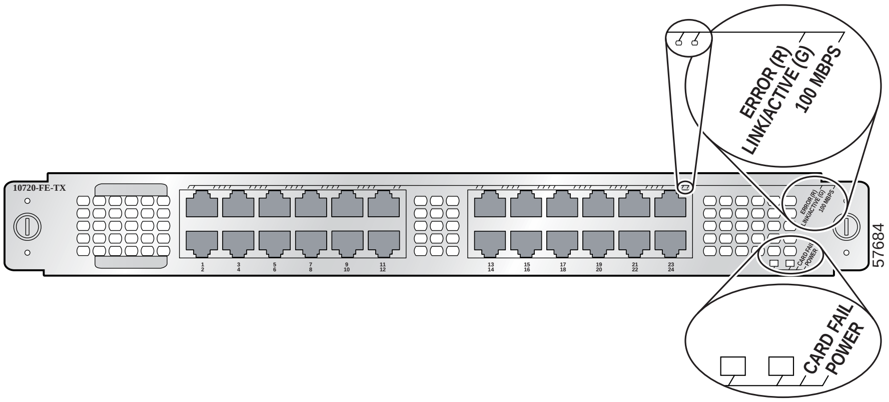
For additional information about laser safety requirements, see the "Laser Safety" section on page 2-4.

Access Card System LEDs

Warning **Avoid exposure to laser radiation. Do not stare into an open aperture, because invisible laser radiation may be emitted from the aperture when a cable is not inserted in the port.** Statement 125

The access card system LEDs provide information on the functionality of the access card in the router. The system LEDs are located on the bottom right side of the access card. (See Figure 3-36.)

Figure 3-36 Access Card Status LEDs (Top) and System LEDs (Bottom)



The configuration of the router will affect the access LEDs. Possible variations include optical cable connections and temperature.

Table 3-9 describes the system LEDs on the access card, and indicates the system status of the access card as it initializes.

Table 3-9 System LEDs for Access Card

LED	Activity	Description
CARD FAIL	Red	A hardware failure is being detected on the access card. During power up, the LED will be red, even when the access card is powered down.
	Off (default status when initialized)	Card is operational. The LED is turned off after hardware initialization.
POWER	Green (default status when initialized)	The access card is receiving power from the system.[1]
	Off	The access card does not receive power from the system.

[1] System power up is not an indication that the access card is powered up.

Access Card Status LEDs

Warning **Avoid exposure to laser radiation. Do not stare into an open aperture, because invisible laser radiation may be emitted from the aperture when a cable is not inserted in the port.** Statement 125

The access card status LEDs provide information on the operational status of the access card. The status LEDs are located on the top right side of the access card. See Figure 3-36 for an example of typical access card status LEDs.

Table 3-10 Access Card Status LEDs

Port Type	LED	Activity	Description
Gigabit Ethernet	**ERROR (R)/LINK (G)**	Red	Error detected on this port. It is turned on at reset and turned off during hardware initialization.
		Solid Green	A link is established on this port.
		Off	No link detected on this port.
	ACTIVE	Blinking Green	Packets are being received or transmitted on this port.
		Off	The port is not active.
Fast Ethernet 10/100BASE-TX	**ERROR (R)/LINK ACTIVE (G)**	Red	Error detected on this port. It is turned on at reset and turned off during hardware initialization.
		Solid green	A link is established on this port, but no activity is detected.
		Blinking green	Packets are being received or transmitted on this port.
		Off	No link detected on this port.
	100 MBPS	Amber	This port is set at 100 MB/s. This LED reflects the status of the Ethernet PHY chip. Even after the link is removed, it will remain in the previous state.
		Off	Port is set at 10 MB/s.

Table 3-10 Access Card Status LEDs (continued)

Port Type	LED	Activity	Description
Fast Ethernet 100BASE-FX	ERROR (R)/LINK (G)	Red	Error detected on this port. It is turned on at reset and turned off during H/W initialization.
		Solid Green	A link is established on this port.
		Off	No link detected on this port.
	ACTIVE	Blinking Amber	Packets are being received or transmitted on this port.
		Off	The port is not active.

For a complete description of the access card LEDs, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.

For additional information about laser safety requirements, see the "Laser Safety" section on page 2-4.

Additional Configuration Features

The following sections provide information on additional router configuration and monitoring procedures:

- Saving the Configuration to NVRAM, page 3-42
- Using the show Commands, page 3-42
- Monitoring Optical Power, page 3-45
- Configuring Basic SRP Functionality, page 3-46
- Configuring POS Functionality, page 3-46
- Configuring Fast Ethernet, page 3-47
- Configuring Gigabit Ethernet, page 3-47
- Configuring TDR on TX Access Card, page 3-47
- Assigning IP Information, page 3-47
- Enabling Write Permission to Bootflash, page 3-47
- Upgrading the Cisco IOS Software Image, page 3-47
- Upgrading ROM Monitor, page 3-48

Saving the Configuration to NVRAM

To save your configuration to NVRAM, use the **copy running-config startup-config** command.

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

Using the show Commands

You can display router information using the **show** commands described in the following sections:

- Using the show running configuration Command, page 3-42
- Using the show version Command, page 3-44
- Using the show environment all Command, page 3-45

Using the show running configuration Command

Use the **show running-configuration** command to verify the router's configuration.

```
router# show running-configuration
Building configuration...

Current configuration : 3791 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Router
!
boot system flash:c10700-p-mz.120-18.ST
!
ip subnet-zero
!
!
interface SRP1/1
ip address 48.1.1.10 255.255.255.0
no ip directed-broadcast
!
interface FastEthernet2/1
ip address 190.10.1.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
media-type mdix
!
interface FastEthernet2/2
ip address 190.10.2.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
media-type mdix
!
interface FastEthernet2/3
ip address 190.10.3.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
media-type mdix
!
```

(Repetitive information removed for FastEthernet2/4 to FastEthernet2/22.)

```
!
interface FastEthernet2/23
ip address 190.10.20.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
media-type mdix
!
interface FastEthernet2/24
ip address 194.16.24.1 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
media-type mdix
!
ip classless
!
snmp-server engineID local 000000090200000164FF2B00
no snmp-server ifindex persist
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
```

Using the show version Command

Use the **show version** command to view the currently running version of Cisco IOS software.

In the following example of the **show version** command, the running system software is Cisco IOS Release 12.0(19)SP:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 10700 Software (C10700-P-M), Version 12.0(19)SP, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
TAC Support:http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 28-Sep-01 11:44 by srani
Image text-base:0x50010960, data-base:0x50660000

ROM:System Bootstrap, Version 12.0(20010529:144545) [yuwang-rommon1 149], DEVELOPMENT
SOFTWARE
BOOTLDR:10700 Software (C10700-P-M), Version 12.0(19)SP, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)

Router uptime is 10 minutes
System returned to ROM by power-on
Running default software

cisco C10720 (R5000) processor (revision 0xFF) with 256000K/6144K bytes of memory.
R527x CPU at 200Mhz, Implementation 40, Rev 10.0
Last reset from power-on
Toaster processor tmc0 is running.
Toaster processor tmc1 is running.
1 one-port OC48 SONET based SRP controller.
1 24 Port 100 Mbps Fast Ethernet TX controller.
24 FastEthernet/IEEE 802.3 interface(s)
```

```
1 SRP network interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512KB).
49152K bytes of Flash internal SIMM (Sector size 512KB).
Configuration register is 0x2102
```

Using the show environment all Command

Use the **show environment all** command to display temperature readings, voltage readings, and fan status.

```
router# show environment all
Power Supplies:
Power Supply is ok.

Temperature readings:
chassis inlet measured at 27C/80F
chassis outlet0 measured at 33C/91F
chassis outlet1 measured at 32C/89F

Voltage readings:
Main Board :Voltage Ok
Access Card :Voltage Ok
Uplink Card :Voltage Ok

Fans:
Fan 1 status is believed to be ok.
Fan 2 status is believed to be ok.
Fan 3 status is believed to be ok.
Fan 4 status is believed to be ok.
Power Supply Fan status is believed to be ok.
Envm stats saved 1 time(s) since reload
Router#
```

Monitoring Optical Power

Optical power monitoring is used to monitor the SRP uplink interface. Use the **show controllers srp** command.

```
Router# show controllers srp
Interface SRP1/1
Hardware is OC48 SRP

SRP1/1 - Side A (Outer RX, Inner TX)

OPTICS
RX readout values: -12 dBm - Within specifications   <==== HERE

SECTION
LOF = 0 LOS = 0 BIP(B1) = 0
LINE
AIS = 0 RDI = 0 FEBE = 0 BIP(B2) = 0
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 0
LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None
```

```
Alarm reporting enabled for: SLOS SLOF PLOP

Framing : SONET
Rx SONET/SDH bytes: (K1/K2) = 0/0 S1S0 = 0 C2 = 0x16
Tx SONET/SDH bytes: (K1/K2) = 0/0 S1S0 = 0 C2 = 0x16 J0 = 0x1
Clock source : Internal
Framer loopback : None
Path trace buffer : Stable
Remote hostname : M0415B
Remote interface: SRP2/0
Remote IP addr : 48.1.1.2
Remote side id : B

BER thresholds: SF = 10e-3 SD = 10e-6
IPS BER thresholds(B3): SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6

SRP1/1 - Side B (Inner RX, Outer TX)

OPTICS
RX readout values: -15 dBm - Within specifications  <==== HERE

SECTION
LOF = 0 LOS = 0 BIP(B1) = 0
LINE
AIS = 0 RDI = 0 FEBE = 0 BIP(B2) = 0
PATH
AIS = 0 RDI = 0 FEBE = 0 BIP(B3) = 0
LOP = 0 NEWPTR = 0 PSE = 0 NSE = 0

Active Defects: None
Active Alarms: None
Alarm reporting enabled for: SLOS SLOF PLOP

Framing : SONET
Rx SONET/SDH bytes: (K1/K2) = 0/0 S1S0 = 0 C2 = 0x16
Tx SONET/SDH bytes: (K1/K2) = 0/0 S1S0 = 0 C2 = 0x16 J0 = 0x1
Clock source : Internal
Framer loopback : None
Path trace buffer : Stable
Remote hostname : M0415B
Remote interface: SRP2/0
Remote IP addr : 48.1.1.2
Remote side id : A

BER thresholds: SF = 10e-3 SD = 10e-6
IPS BER thresholds(B3): SF = 10e-3 SD = 10e-6
TCA thresholds: B1 = 10e-6 B2 = 10e-6 B3 = 10e-6
```

Configuring Basic SRP Functionality

The basic SRP configuration task for the router is located in the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication under “Configuring SRP.”

Configuring POS Functionality

The basic SRP configuration task for the router is located in the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication under “Configuring POS.”

Configuring Fast Ethernet

The basic Fast Ethernet configuration task for the router is located in the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication under “Configuring a Fast Ethernet Interface.”

Configuring Gigabit Ethernet

The basic Gigabit Ethernet configuration task for the router is located in the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication under “Configuring a Gigabit Ethernet Interface.”

Configuring TDR on TX Access Card

The Time Domain Reflectometer (TDR) sends a signal from one end of a cable and measures the time for the signal to reflect back. To detect shorts and breaks, to measure the length of the cable, and to find other physical-layer network problems, use the TDR.

The TDR is used for Fast Ethernet ports on 10/100BASE-TX and 4-Port Gigabit Ethernet 8-Port 10/100 Ethernet TX access cards. For information about how to use the TDR, refer to “Testing for a Cable Problem on a Fast Ethernet Interface” in the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication.

Assigning IP Information

To assign IP addresses to interfaces, refer to “Configuring a Fast Ethernet Connection” in the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication.

Enabling Write Permission to Bootflash

The router provides 64 MB of Flash memory. There are 16 MB dedicated to the bootflash, a read-only partition containing the Cisco IOS software image that shipped with the router. There are 48 MB dedicated to the Flash, a read-write partition containing downloaded Cisco IOS software images.

To enable the write permission to the bootflash, use the **bootflash-write enable** command.

```
router(config)# bootflash-write enable
```

Caution Writing to bootflash memory is not recommended.

Upgrading the Cisco IOS Software Image

You can upgrade the Cisco IOS software image on the router by copying the image to Flash memory and then restarting the router using the updated image.

Note The router does not have an available Ethernet Out of Bound Controller (EOBC) management interface. Cisco IOS software images cannot be downloaded from the ROM monitor or while the system is booting up.

Perform the following steps to update the Cisco IOS software image:

Step 1 Enter the **enable** command.

```
Router> enable
```

Step 2 Copy the Cisco IOS software image from the TFTP server to the router Flash memory using the **copy tftp flash** command.

```
Router# copy tftp flash
Address or name of remote host []? tftp_server
Source filename []? /tftpboot/ image name
Destination filename [file name]?
Accessing tftp://tftp_server//tftpboot/ image name
!!!!!!!
```

Step 3 Specify the new Flash memory image using the **config terminal** command.

```
Router# config terminal
Router(config)# boot system flash:image name
Router(config)# config-register 0x2102
```

Step 4 Restart the router using the **reload** command.

```
Router# reload
Proceed with reload? [confirm]
03:36:32: %SYS-5-RELOAD: Reload requested
```

Note The following commands are presently not supported on a Cisco 10720 Internet Router:
boot system tftp <file> <tftp_server>,
rommon 1>boot <file> <tftp_server>, rommon 1>tftpdnld <file>

Verifying the Image Is Upgraded

Enter the **show version** command to confirm the correct image is loaded on the router. (See the "Using the show Commands" section on page 3-42.)

Upgrading ROM Monitor

The following section provides information for upgrading the ROM monitor (ROMmon) image. For additional information about ROMmon features, refer to the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication.

The following steps are an example ROMmon update procedure:

Step 1 View ROMmon information using the **show rom-monitor** command.

```
Router(boot)# show rom-monitor
Region region1:INVALID
Region region2:INVALID
Currently running ROMMON from S (Gold) region
```

Step 2 Copy the new ROMmon record file onto the router Flash memory using the **copy tftp flash** command.

```
Router(boot)# copy tftp flash
```

Step 3 Program the new ROMmon into the router ROMmon Flash memory using the **upgrade rom-monitor file flash**:*name*.

```
Router(boot)# upgrade rom-monitor file flash:name
ROMMON image upgrade in progress
Erasing flash
Programming flash
Verifying new image
ROMMON image upgrade complete, router must be reloaded.
```

Step 4 View ROMmon information again using the **show rom-monitor** command.

```
Router# show rom-monitor
Region region1:APPROVED, preferred
Region region2:INVALID
Currently running ROMMON from region1 region
```

Verifying ROM Monitor Is Upgraded

To verify the upgraded ROM monitor, use the **show rom-monitor** command to verify that the new ROMmon is approved.

```
Router# show rom-monitor
Region F1: APPROVED, preferred
Region F2: INVALID
Currently running ROMMON from F1 region
```

CHAPTER 4

Troubleshooting

This section contains basic troubleshooting guidance for the Cisco 10720 Internet Router and components.

Basic Troubleshooting RPR-IEEE for the Uplink Card

This section provides basic troubleshooting guidelines for RPR-IEEE on the RPR/SRP uplink card. For additional information about RPR-IEEE configurations, refer to the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication. For additional Cisco IEEE 802.17 related documentation, see the "Related Documentation" section on page xix.

The following sections present information on show commands, verification steps, and alarm messages:

Using the show controller rpr-ieee Command

Verify the following using the **show controller rpr-ieee** command:

- RX optics readout values are within specifications. For example: RX readout values: -11 dBm - Within specifications, RX readout values: -15 dBm - Within specifications
- Error counters are not incrementing.
- There are no active defects or alarms. For example, Active Alarms: None

- Proper clocking configuration for each span (East and West). For example,
  Clock source: Internal
- Proper hosts are on the proper side. For example, Remote span id: East, Remote span id: West

The following example shows sample output from this command:

```
Router# show controllers rpr-ieee 1/1
Interface RPR-IEEE1/1
Hardware is OC48 RPR-IEEE
RPR-IEEE1/1 - West Span (Ringlet0 RX, Ringlet1 TX)
SFP Module West is VALID
OPTICS
TX power -4 (+/- 3) dBm
RX power -5 (+/- 3) dBm
No Active Alarms
No Active Warnings
SECTION
  LOF = 0          LOS    = 0                           BIP(B1) = 0
LINE
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
PATH
   AIS = 0          RDI    = 0          FEBE = 0          BIP(B3) = 0
   LOP = 0          NEWPTR = 0          PSE  = 0          NSE     = 0
Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SLOS SLOF PLOP

Framing            : SONET
Rx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16
Tx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16  J0 = 0x1
Clock source      : Internal
Framer loopback   : None
Path trace buffer : Stable
  Remote hostname : EAST-D
 Remote interface: RPR-IEEE1/1
  Remote IP addr  : 1.1.1.1
  Remote side id  : EAST
BER thresholds:           SF = 10e-3  SD = 10e-6
IPS BER thresholds(B3):   SF = 10e-3  SD = 10e-6
TCA thresholds:           B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
biff (6:57:52 PM):  RPR-IEEE1/1 - East Span (Ringlet1 RX, Ringlet0 TX)
SFP Module East is VALID
OPTICS
TX power -4 (+/- 3) dBm
RX power -5 (+/- 3) dBm
No Active Alarms
No Active Warnings
SECTION
  LOF = 0          LOS    = 0                           BIP(B1) = 0
LINE
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
PATH
  AIS = 0          RDI    = 0          FEBE = 0          BIP(B3) = 0
  LOP = 0          NEWPTR = 0          PSE  = 0          NSE     = 0
Active Defects: None
Active Alarms:  None
Alarm reporting enabled for: SLOS SLOF PLOP
Framing            : SONET
Rx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16
Tx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16  J0 = 0x1
Clock source      : Internal
Framer loopback   : None
Path trace buffer : Stable
```

```
 Remote hostname : WEST-D
 Remote interface: RPR-IEEE1/1
 Remote IP addr  : 1.1.1.3
 Remote side id  : WEST
BER thresholds:           SF = 10e-3  SD = 10e-6
IPS BER thresholds(B3):   SF = 10e-3  SD = 10e-6
TCA thresholds:           B1 = 10e-6  B2 = 10e-6  B3 = 10e-6
```

Using the show controllers rpr-ieee 1/1 transceiver Command

Use the transceiver keyword to display additional information about the status of the small form-factor pluggable (SFP) module used in an RPR port.

```
Router# show controllers rpr-ieee 1/1 transceiver

Show Transceiver: West Span
Static information
    ID: SFP transceiver
    Extended ID: 4
    Connector: LC
    SONET compliance: OC48SR
    Gigabit Ethernet compliance: unspecified
    Fibre Channel link length: unspecified
    Fibre Channel transmitter technology: unspecified
    Fibre Channel transmission media: unspecified
    Fibre Channel speed: unspecified
    Encoding: reserved
    Bit Rate: 2500 Mbps
    Single mode fiber supported length: 2 km
    Upper bit rate limit: unspecified
    Lower bit rate limit: unspecified
    Date code (yyyy/mm/dd): 2004/04/21
    Vendor PN: SCP6828-C5-BNE
    Vendor revision number: D
    Vendor serial number: ECL0817001L
Transceiver status information
Diagnostics calibration is external
Temperature 39 (+/-3 Celsius)
Voltage in transceiver 3232600 uV (+/- 10 mV)
TX bias 8940 uA (+/- 100uA)
TX power 316000 nW / -5 dBm (+/- 3dBm)RX power 300200 nW / -5 dBm (+/- 3dBm)
No Active Alarms
No Active Warnings

Alarm Thresholds:
                       high                     low
Temperature              96 C                  -44 C
Voltage             4000000 uV                   0 uV
TX bias               70000 uA                   0 uA
TX power            1000000 nW / 0   dBm      50100 nW / -13 dBm
RX power            1008300 nW / 0   dBm   unspecified


Warning Thresholds:
                        high                     low
Temperature              91 C                  - 9 C
Voltage             3600000 uV             3000000 uV
TX bias               60000 uA                   0 uA
TX power             630900 nW / -2  dBm      79400 nW / -11 dBm
RX power            1008300 nW / 0   dBm   unspecified
Show Transceiver: East Span
```

```
Static information
    ID: SFP transceiver
    Extended ID: 4
    Connector: LC
    SONET compliance: OC48SR
    Gigabit Ethernet compliance: unspecified
    Fibre Channel link length: unspecified
    Fibre Channel transmitter technology: unspecified
    Fibre Channel transmission media: unspecified
    Fibre Channel speed: unspecified
    Encoding: reserved
    Bit Rate: 2500 Mbps
    Single mode fiber supported length: 2 km
    Upper bit rate limit: unspecified
    Lower bit rate limit: unspecified
    Date code (yyyy/mm/dd): 2004/04/21
    Vendor PN: SCP6828-C5-BNE
    Vendor revision number: D
    Vendor serial number: ECL0817001M
Transceiver status information
Diagnostics calibration is external
Temperature 38 (+/-3 Celsius)
    Voltage in transceiver 3230800 uV (+/- 10 mV)
    TX bias 8724 uA (+/- 100uA)
    TX power 285600 nW / -5 dBm (+/- 3dBm)
    RX power 309900 nW / -5 dBm (+/- 3dBm)
No Active Alarms
No Active Warnings

Alarm Thresholds:
                        high                     low
Temperature               96 C                   -44 C
Voltage              4000000 uV                    0 uV
TX bias                70000 uA                    0 uA
TX power             1000000 nW / 0   dBm      50100 nW / -13 dBm
RX power             1008300 nW / 0   dBm   unspecified

Warning Thresholds:
                        high                     low
Temperature               91 C                   - 9 C
Voltage              3600000 uV              3000000 uV
TX bias                60000 uA                    0 uA
TX power              630900 nW / -2  dBm      79400 nW / -11 dBm
RX power             1008300 nW / 0   dBm   unspecified
```

Using the show arp Command

Use the **show arp** command to verify that the correct Address Resolution Protocol (ARP) table is loaded.

The following example shows sample output from this command:

```
Router# show arp
Protocol Address      Age (min)   Hardware            Addr Type      Interface
Internet 1.1.1.1           154    0001.0001.0001      RPR-IEEE-W     RPR-IEEE1/1
Internet 1.1.1.3           155    0003.0003.0003      RPR-IEEE-E     RPR-IEEE1/1
Internet 1.1.1.2             -    0002.0002.0002      RPR-IEEE       RPR-IEEE1/1
Internet 200.1.1.1           -    0001.64ff.0601      ARPA           GigabitEthernet2/1
Router#
```

Verifying Clocking

There are two modes of clocking for the rpr-ieee interface, LINE and INTERNAL. Clocking works over dark fiber.

- INTERNAL means that the rpr-ieee interface uses its internal 20ppm or Stratum-3 clock. LINE means it takes timing from the other span of the line.
- Having both spans with clocking set to INTERNAL is the default configuration and results in normal operation.
- Having both spans with clocking set to LINE is not advised and will result in bit interleaved parity (BIP) errors over time.
- Pairing opposite spans of a connection with one spans INTERNAL and one span LINE is acceptable, but not necessary.

Ideal clocking is achieved when all interfaces have the clocking set to INTERNAL. The following example shows this configuration:

```
router(config)# interface rpr-ieee 1/1
router(config-if)# rpr-ieee clock-source internal East
router(config-if)# rpr-ieee clock-source internal West
```

PASS-THRU Mode

The rpr-ieee line card acts as an optical regenerator when it is operating in PASS-THRU mode. PASS-THRU mode isolates the node. This mode is activated when the interface is placed in shutdown mode, or the node is not receiving layer 2 keepalives on span East or span West.

Use the **shutdown** interface configuration command to place the router rpr-ieee interface in PASS-THRU mode.

PASS-THRU mode is a useful troubleshooting tool for isolating which node on the ring is faulty.

The following example shows sample output from this command:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface RPR-IEEE 1/1
Router(config-if)#shutdown
Router(config-if)#end
Router#
3d06h: %SYS-5-CONFIG_I: Configured from console by tty1
3d06h: %LINK-5-CHANGED: Interface RPR-IEEE1/1, changed state to administratively down
3d06h: %LINEPROTO-5-UPDOWN: Line protocol on Interface RPR-IEEE1/1, changed state to down
```

Verifying the PASS-THRU Mode

Use the **show rpr-ieee ips** EXEC command to verify that the rpr-ieee node is in PASS-THRU mode, which occurs when the interface is administratively down.

The following example shows sample output from this command:

```
Router# show rpr-ieee protection

RPR-IEEE1/1 is administratively down
Router#
```

Using the show rpr-ieee topology Command

Use the **show rpr-ieee topology** EXEC command to verify that topology is valid.

The following example shows sample output from this command:

```
Router# show rpr-ieee topology
Ring Topology: CLOSED (STABLE)
  Configured protection mode: WRAPPING
  Jumbo preference: SET (ring supports JUMBOS)
  Number of nodes on
      ringlet0: 3       ringlet1: 3
  Checksum: 0x001800D6
  Index (Ri 0)       MAC        IP Address       Edge W/E    Request W/E
       1        0001.0001.0001    1.1.1.1          NO/NO      IDLE/IDLE
       2        0003.0003.0003    1.1.1.3          NO/NO      IDLE/IDLE
       3        0002.0002.0002    1.1.1.2          NO/NO      IDLE/IDLE
  Index (Ri 1)       MAC        IP Address       Edge W/E    Request W/E
       1        0003.0003.0003    1.1.1.3          NO/NO      IDLE/IDLE
       2        0001.0001.0001    1.1.1.1          NO/NO      IDLE/IDLE
       3        0002.0002.0002    1.1.1.2          NO/NO      IDLE/IDLE
```

Using the show rpr-ieee protection Command

The **show rpr-ieee protection** command displays the status of the 802.17 topology-protection. It contains information such as the neighbors found on each ringlet, the protection mode/status and the topology checksum values/status.

The following example shows sample output from this command:

```
Router# show rpr-ieee protection
Protection Information for Interface RPR-IEEE1/1
 MAC Addresses
   West Span (Ringlet 0 RX) neighbor 0001.0001.0001
   East Span (Ringlet 1 RX) neighbor 0003.0003.0003
   Station MAC address 0002.0002.0002
 TP frame sending timers:
     fast timer: 10 msec
     slow timer: 1x100 msec (100 msec)
 Protection holdoff timers:
     L1 Holdoff                         Keepalive Detection
     West Span  0x10 msec (  0 msec)    West Span   3 msec
     East Span  0x10 msec (  0 msec)    East Span   3 msec
  Configured protection mode: WRAPPING
 Protection Status
   Ring is IDLE
   Protection WTR period is 10 sec. (timer is inactive)
     Self Detected Requests                Remote Requests
     West Span IDLE                        West Span IDLE
     East Span IDLE                        East Span IDLE
     Distant Requests
     East Span IDLE                        West Span IDLE

   West Span Failures: none East Span Failures: none
```

If the ring reports an "OPEN" state in the topology, there is a link failure in the ring, the details in the ringlet indices will pinpoint the failure location by indicating the Edge location and the Request (reason) for the Edge.

Fiber Misconnection

Use the **show rpr-ieee EXEC** command to check for misconnected fiber cables, for example, span East to span East or TX to TX. The message, “Misconnection Alarm” shows at the top of the **show rpr-ieee** command output when there is a fiber misconnection.

- One alarm—the problem is with another node on the ring. For example, span East connected to span East.
- Two alarms—the problem is your node. For example, span East to span East and span West to span West.

Basic Troubleshooting SRP for the Uplink Card

This section provides basic troubleshooting guidelines for SRP on the DPT, POS/DPT, and RPR/SRP uplink cards. For additional information about SRP configurations, refer to the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication. For additional Cisco SRP-related documentation, see the “Related Documentation” section on page xix.

The following sections present information on show commands, verification steps, and alarm messages:

Using the show controller srp Command

Verify the following using the **show controller srp** command:

- RX optics readout values are within specifications. For example: RX readout values: -11 dBm - Within specifications, RX readout values: -15 dBm - Within specifications
- Error counters are not incrementing.
- There are no active defects or alarms. For example, Active Alarms: None
- Proper clocking configuration for each side (A and B). For example,
  Clock source : Internal
- Proper hosts are on the proper side. For example, Remote side id : A,
  Remote side id : B

```
Router# show controllers srp

Interface SRP1/1
Hardware is OC48 SRP

SRP1/1 - Side A (Outer RX, Inner TX)
```

```
   OPTICS
➔  RX readout values: -11 dBm    - Within specifications

   SECTION
     LOF = 0          LOS    = 0                            BIP(B1) = 0
   LINE
     AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
   PATH
     AIS = 0          RDI    = 0          FEBE = 0          BIP(B3) = 0
     LOP = 0          NEWPTR = 0          PSE  = 0          NSE     = 0

   Active Defects: None
➔  Active Alarms:  None
   Alarm reporting enabled for: SLOS SLOF PLOP

   Framing           : SONET
   Rx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16
   Tx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16  J0 = 0x1
➔  Clock source      : Internal
   Framer loopback   : None
   Path trace buffer : Stable
     Remote hostname : M0415B
     Remote interface: SRP2/0
     Remote IP addr  : 48.1.1.2
➔    Remote side id  : B

   BER thresholds:           SF = 10e-3  SD = 10e-6
   IPS BER thresholds(B3):   SF = 10e-3  SD = 10e-6
   TCA thresholds:           B1 = 10e-6  B2 = 10e-6  B3 = 10e-6

   SRP1/1 - Side B (Inner RX, Outer TX)

   OPTICS
➔  RX readout values: -15 dBm    - Within specifications

   SECTION
     LOF = 0          LOS    = 0                            BIP(B1) = 0
   LINE
     AIS = 0          RDI    = 0          FEBE = 0          BIP(B2) = 0
   PATH
     AIS = 0          RDI    = 0          FEBE = 0          BIP(B3) = 0
     LOP = 0          NEWPTR = 0          PSE  = 0          NSE     = 0

➔  Active Defects: None
➔  Active Alarms:  None
   Alarm reporting enabled for: SLOS SLOF PLOP

   Framing           : SONET
   Rx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16
   Tx SONET/SDH bytes: (K1/K2) = 0/0        S1S0 = 0  C2 = 0x16  J0 = 0x1
➔  Clock source      : Internal
   Framer loopback   : None
   Path trace buffer : Stable
     Remote hostname : M0415B
     Remote interface: SRP2/0
     Remote IP addr  : 48.1.1.2
➔    Remote side id  : A

   BER thresholds:           SF = 10e-3  SD = 10e-6
   IPS BER thresholds(B3):   SF = 10e-3  SD = 10e-6
   TCA thresholds:           B1 = 10e-6  B2 = 10e-6  B3 = 10e-6

   Router#
```

Using the show arp Command

Use the **show arp** command to verify that the correct Address Resolution Protocol (ARP) table is loaded.

```
Router# show arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  48.1.1.2              181   0001.6340.9100  SRP-B  SRP1/1
Internet  48.1.1.10               -   0001.64ff.3100  SRP2   SRP1/1
Internet  194.16.3.1             68   0001.64ff.3103  ARPA   FastEthernet2/3
Internet  194.16.2.1              123   0001.64ff.3102  ARPA   FastEthernet2/2
Internet  194.16.1.1              -   0001.64ff.3101  ARPA   FastEthernet2/1
repetitive output removed
Router#
```

Verifying Clocking

There are two modes of clocking for the SRP interface, LINE and INTERNAL. Clocking works over dark fiber.

- INTERNAL means that the SRP interface uses its internal 20ppm or Stratum-3 clock. LINE means it takes timing from the other side of the line.
- Having both sides with clocking set to INTERNAL is the default configuration and results in normal operation.
- Having both sides with clocking set to LINE is not advised and will result in bit interleaved parity (BIP) errors over time.
- Pairing opposite sides of a connection with one side INTERNAL and one side LINE is acceptable, but not necessary.

Ideal clocking is achieved when all interfaces have the clocking set to INTERNAL. The following example shows this configuration:

```
router(config)# interface srp 1/1
router(config-if)# srp clock-source internal A
router(config-if)# srp clock-source internal B
```

PASS-THRU Mode

The SRP line card acts as an optical regenerator when it is operating in PASS-THRU mode. PASS-THRU mode isolates the node. This mode is activated when the interface is placed in shutdown mode, or the node is not receiving layer 2 keepalives on side A or side B.

Use the **shutdown** interface configuration command to place the router SRP interface in PASS-THRU mode.

PASS-THRU mode is a useful troubleshooting tool for isolating which node on the ring is faulty.

```
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface srp 1/1
Router(config-if)# shutdown
Router(config-if)# end
Router#
23:42:25: %SYS-5-CONFIG_I: Configured from console by console
23:42:27: %LINK-5-CHANGED: Interface SRP1/1, changed state to administratively down
23:42:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface SRP1/1, changed state to down
```

Verify the PASS-THRU Mode

Use the **show srp ips** EXEC command to verify that the SRP node is in PASS-THRU mode, which occurs when the interface is administratively down.

```
Router# show srp ips

SRP1/1 is administratively down
Router#
```

Using the show srp topology Command

Use the **show srp topology** EXEC command to verify that the topology packets are being sent and received.

```
router# show srp topology

Topology Map for Interface SRP1/1
Topology pkt. sent every 5 sec. (next pkt. after 0 sec.)
Last received topology pkt. 00:00:04
Nodes on the ring: 3
Hops (outer ring)      MAC       IP Address     Wrapped Name
      0             0001.64ff.1580 48.1.1.3       No    M0426C
      1             0001.6347.9700 48.1.1.2       No    M0426B
      2             00b0.c280.cf00 48.1.1.1       No    M0426A
```

By default, the maximum acceptable time for the last topology packet to be received is 5 seconds. If the last received packet value is higher than 5 seconds, topology packets are being lost on the ring.

Using the show srp ips Command

The **show srp ips** command displays the status of the IPS protocol. It contains information such as the direct neighbors' address, the wrap state, the failures state and the latest transmitted and received IPS packets of the SRP node. It also indicates that the interface is administratively up and not in PASS-THRU mode. (See the "PASS-THRU Mode" section on page 4-9.)

```
router# show srp ips

IPS Information for Interface SRP1/1
 MAC Addresses
   Side A (Outer ring RX) neighbor 00b0.c280.cf00
   Side B (Inner ring RX) neighbor 0001.6347.9700
   Node MAC address 0001.64ff.1580
 IPS State
➔  Side A not wrapped
➔  Side B not wrapped
   Side A (Inner ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   Side B (Outer ring TX) IPS pkt. sent every 1 sec. (next pkt. after 1 sec.)
   inter card bus enabled
   IPS WTR period is 60 sec. (timer is inactive)
   Node IPS State: idle

IPS Self Detected Requests           IPS Remote Requests
   Side A IDLE                          Side A IDLE
   Side B IDLE                          Side B IDLE
 IPS messages received
   Side A (Outer ring RX) {00b0.c280.cf00,IDLE,SHORT}, TTL 128
   Side B (Inner ring RX) {0001.6347.9700,IDLE,SHORT}, TTL 128
 IPS messages transmitted
   Side A (Outer ring RX) {0001.64ff.1580,IDLE,SHORT}, TTL 128
   Side B (Inner ring RX) {0001.64ff.1580,IDLE,SHORT}, TTL 128
```

Any status other than IDLE, SHORT indicates that errors are present.

If the value “none” is present in IPS packets received, there is a problem on the ring.

Fiber Misconnection

Use the **show srp EXEC** command to check for misconnected fiber cables, for example, side A to side A or TX to TX. The message, “Misconnection Alarm” shows at the top of the **show srp** command output when there is a fiber misconnection.

- One alarm—the problem is with another ring on the node. For example, side A connected to side A.
- Two alarms—the problem is your node. For example, side A to side A and side B to side B.

Alarm Messages

The following alarm messages display on the console. The suggested solutions cover the most commonly observed errors.

See the following tables for specific alarms and solutions.

Alarm Messages

The following alarm messages report to the console. See Table 4-1 through Table 4-8 for specific alarms and solutions.

The suggested solutions listed below are to the most commonly observed errors:

- Keepalive Alarm Messages for All Uplink Cards, Table 4-1 on page 4-11
- IEEE 802.17 RPR Wrap Messages, Table 4-2 on page 4-13
- IEEE 802.17 RPR Unwap Messages, Table 4-3 on page 4-14
- Other IEEE 802.17 RPR Alarm Messages, Table 4-6 on page 4-16
- SRP Wrap Messages, Table 4-7 on page 4-17
- SRP Unwrap Message, Table 4-8 on page 4-18

Table 4-1 Keepalive Alarm Messages for All Uplink Cards

Alarm	Description	Solution
SRP1/1 Side A Keepalive Failure (MAC)	MAC failure is detected	Check transport span for problems. Typically SRP ring traverses a SONET layer connection, creating this error.
SRP1/1 Side A Keepalive Failure (SLOS)	SONET section loss of signal	Check fiber for breaks, power level, and connectivity. This is a SONET layer 1 issue with fiber.
SRP1/1 Side A Keepalive Failure (SLOF)	SONET section loss of frame	Check the fiber for degradation in (power level) or clocking (internal versus line).

Table 4-1 Keepalive Alarm Messages for All Uplink Cards (continued)

Alarm	Description	Solution
SRP1/1 Side A Keepalive Failure (LSD)	SONET line signal degrade	Check the affected fiber, transmit and receive ports. Check power level. This is a SONET layer 1 issue with signal degrade.
SRP1/1 Side A Keepalive Failure (LSD)	SONET line signal degrade	Check the neighbor node/transport/regenerator for SONET layer 1 issues (LOS, LSF). This is a SONET layer 1 issue with an intermediate unit (usually transport connection or regenerator) forwarding an AIS.
SRP1/1 Side A Keepalive OK	Keepalive failure removed; Layer 2 Keepalive receiving correctly	None.
RPR-IEEE1/1 span WEST Keepalive Failure (MAC)	MAC failure is detected	Check transport span for problems. Typically RPR ring traverses a SONET layer connection, creating this error.
RPR-IEEE1/1 span WEST Keepalive Failure (SLOS)	SONET section loss of signal	Check fiber for breaks, power level, and connectivity. This is a SONET Layer 1 issue with fiber.
RPR-IEEE1/1 span WEST Keepalive Failure (SLOF)	SONET section loss of frame	Check the fiber for degredation in (power level) or clocking (interval versus line).
RPR-IEEE1/1 span WEST Keepalive Failure (LSD)	SONET line signal degrade	Check the affected fiber transmit (TX) and receive (RX) ports. Check the power level. This is a SONET Layer 1 issue with signal degradation.
RPR-IEEE1/1 span WEST Keepalive Failure (LSF)	SONET line signal failure	Check the neighboring node/transport/regenerator for SONET layer 1 issues (LOS, LSF). This is a SONET Layer 1 issue with an intermediate unit (usually transport connection or regenerator) forwarding an AIS.
RPR-IEEE1/1 span WEST Keepalive Failure OK	Keepalive signal removed, Layer 2 Keepalive receiving correctly	None.

Table 4-2 IEEE 802.17 RPR Wrap Messages

Alarm	Description	Solution
RPR-IEEE1/1 wrapped on span East (span WEST User Request Forced Switch)	User initiated forced switch on span WEST on node	User initiated, none.
RPR-IEEE1/1 wrapped on span EAST (span WEST User Request Manual Switch)	User initiated manual switch on span WEST on node	User initiated, none.
RPR-IEEE1/1 wrapped on span EAST (span WEST Self Detect Signal Fail)	SONET Layer 1 signal fail detected	Investigate Keepalive failure. Wrap occurred. Keepalive failure—SLOS, SLOF, LSF, or LAIS.
RPR-IEEE1/1 wrapped on span EAST (span WEST Span Neighbor Signal Degrade)	SONET Layer 1 signal fail detected	Investigate Keepalive failure. Wrap occurred. Keepalive failure—LSD.
RPR-IEEE1/1 wrapped on span EAST (span WEST Self Detect Wait to Restore [WTR])	Wrap cleared, node initiated; Wait to Restore (WTR) state	WTR period is 10 to 360 seconds (user configured), node will unwrap at end of WTR. None.
RPR-IEEE1/1 wrapped on span EAST (span WEST Span Neighbor Forced Switch)	Neighbor node Forced Switch initiated by user. Node wrap to protect failed span	User initiated, none.
RPR-IEEE1/1 wrapped on span EAST (span WEST Span Neighbor Manual Switch)	Neighbor node Manual Switch initiated by user. Node wrap	User initiated, none.
RPR-IEEE1/1 wrapped on span EAST (span WEST Span Neighbor Signal Fail)	Neighbor node wrapped due to signal fail	Investigate the signal degrade on neighbor node.
RPR-IEEE1/1 wrapped on span EAST (span WEST Span Neighbor Signal Degrade)	Neighbor node wrapped due to signal degrade	Investigate the signal degrade on neighbor node.
RPR-IEEE1/1 wrapped on span EAST (span WEST Span Neighbor WTR)	Wrap cleared, node initiated; Wait to Restore state	WTR period is 0 to 1440, or never (user configured), node will unwrap at end of WTR. None. Setting WTR to never will prevent the node from unwrapping.
RPR-IEEE1/1 wrapped on span EAST (span WEST Long Request Forced Switch)	Neighbor node Forced Switch initiated by user; Node wrap to protect failed span; Secondary problem on the short path	Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.

Table 4-2 IEEE 802.17 RPR Wrap Messages (continued)

Alarm	Description	Solution
RPR-IEEE1/1 wrapped on span EAST (span WEST Long Request Manual Switch)	Neighbor node Manual Switch initiated by user; Node wrap to protect failed span; Secondary problem on the short path	Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
RPR-IEEE1/1 wrapped on span EAST (span WEST Long Request Signal Fail)	Neighbor node wrapped due to signal fail	Investigate signal fail on neighbor node. Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
RPR-IEEE1/1 wrapped on span EAST (span WEST Long Request Signal Degrade)	Neighbor node wrapped due to signal degrade	Investigate signal degrade on neighbor node. Investigate why short path request was not received. Check other problems on the short span as indicated on the neighbor node.
RPR-IEEE1/1 wrapped on span EAST (span WEST Long Request WTR)	Wrap cleared; Wait to Restore timer expired	None.

Table 4-3 IEEE 802.17 RPR Unwap Messages

Alarm	Description	Solution
RPR-IEEE1/1 unwrapped on span EAST (wrap cause cleared)	Wrap cleared; Wait to Restore timer expired.	None.

Table 4-4 IEEE 802.17 RPR Steer Messages

Alarm	Description	Solution
RPR-IEEE1/1 protected on span East (span WEST User Request Forced Switch)	User initiated forced switch on span WEST on node	User initiated, none.
RPR-IEEE1/1 protected on span EAST (span WEST User Request Manual Switch)	User initiated manual switch on span WEST on node	User initiated, none.
RPR-IEEE1/1 protected on span EAST (span WEST Self Detect Signal Fail)	SONET Layer 1 signal fail detected	Investigate Keepalive failure. Wrap occurred. Keepalive failure—SLOS, SLOF, LSF, or LAIS.
RPR-IEEE1/1 protected on span EAST (span WEST Span Neighbor Signal Degrade)	SONET Layer 1 signal fail detected	Investigate Keepalive failure. Wrap occurred. Keepalive failure—LSD.

Table 4-4 IEEE 802.17 RPR Steer Messages (continued)

Alarm	Description	Solution
RPR-IEEE1/1 protected on span EAST (span WEST Self Detect Wait to Restore [WTR])	Wrap cleared, node initiated; Wait to Restore (WTR) state	WTR period is 10 to 360 seconds (user configured), node will unwrap at end of WTR. None.
RPR-IEEE1/1 protected on span EAST (span WEST Span Neighbor Forced Switch)	Neighbor node Forced Switch initiated by user. Node wrap to protect failed span	User initiated, none.
RPR-IEEE1/1 protected on span EAST (span WEST Span Neighbor Manual Switch)	Neighbor node Manual Switch initiated by user. Node wrap	User initiated, none.
RPR-IEEE1/1 protected on span EAST (span WEST Span Neighbor Signal Fail)	Neighbor node protected due to signal fail	Investigate the signal degrade on neighbor node.
RPR-IEEE1/1 protected on span EAST (span WEST Span Neighbor Signal Degrade)	Neighbor node protected due to signal degrade	Investigate the signal degrade on neighbor node.
RPR-IEEE1/1 protected on span EAST (span WEST Span Neighbor WTR)	Wrap cleared, node initiated; Wait to Restore state	WTR period is 0 to 1440, or never (user configured), node will unwrap at end of WTR. None. Setting WTR to never will prevent the node from unwrapping.
RPR-IEEE1/1 protected on span EAST (span WEST Long Request Forced Switch)	Neighbor node Forced Switch initiated by user; Node wrap to protect failed span; Secondary problem on the short path	Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
RPR-IEEE1/1 protected on span EAST (span WEST Long Request Manual Switch)	Neighbor node Manual Switch initiated by user; Node wrap to protect failed span; Secondary problem on the short path	Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.

Table 4-4 IEEE 802.17 RPR Steer Messages (continued)

Alarm	Description	Solution
RPR-IEEE1/1 protected on span EAST (span WEST Long Request Signal Fail)	Neighbor node protected due to signal fail	Investigate signal fail on neighbor node. Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
RPR-IEEE1/1 protected on span EAST (span WEST Long Request Signal Degrade)	Neighbor node protected due to signal degrade	Investigate signal degrade on neighbor node. Investigate why short path request was not received. Check other problems on the short span as indicated on the neighbor node.

Table 4-5 IEEE 802.17 RPR Un-Steer Messages

Alarm	Description
RPR-IEEE1/1 unprotected on span EAST (protection cause cleared)	Protection cleared; Wait to Restore timer expired.

Table 4-6 Other IEEE 802.17 RPR Alarm Messages

Alarm	Description	Solution
RPR-IEEE1/1 Ringlet1 reserved A0 bandwidth has exceeded line rate	The amount of total A0 bandwidth on Ringlet1 reserved by all nodes on the ring exceeds the line rate	Check current A0 allocations on each station using the **show rpr-ieee rate-limit** command. Change the A0 allocation on the ring by using the **rpr-ieee tx-traffic reserved** CLI command.
RPR-IEEE1/1 Ringtlet0 reserved A0 bandwidth has exceeded line rate	The amount of total A0 bandwidth on Ringlet0 reserved by all nodes on the ring exceeds the line rate	Check current A0 allocation on each station using the **show rpr-ieee rate-limit** command. Change the A0 allocation on the ring by using the **rpr-ieee tx-traffic reserved** CLI command.
RPR-IEEE1/1 MAX Stations Exceeded	Too many stations have been discovered in the topology (maximum number of ring stations is 255)	Execute the **show rpr-ieee topology** commandto verify stations. Reduce the numer of stations in the ring.
RPR-IEEE1/1 Effective jumbo pref on ring is set for jumbo frames	All stations on the ring now support jumbo frame preference, MTU for the ring has been changed to JUMBO MTU (9100 bytes).	None. Remove jumbo preference on stations to revert to REGULAR MTU (1500 bytes)

Table 4-6 Other IEEE 802.17 RPR Alarm Messages (continued)

Alarm	Description	Solution
RPR-IEEE1/1 Effective jumbo pref on ring is set for regular frame	At least one station on the ring does not support jumbo frame preference, MTU for the ring has been changed to REGULAR MTU (1500 bytes).	None. Configure jumbo preference on all stations to change support to JUMBO MTU (9100 bytes).
RPR-IEEE1/1 Effective protection mode on station is now steering	Protection preference has been changed. Protection mode for this station is now steering.	None.
RPR-IEEE1/1 Effective protection mode on station is now wrapping	Protection preference has been changed. Protection mode for this station is now wrapping.	None.
Configured protection mode is inconsistent with other stations on ring	Not all stations in the ring support the same protection preference (wrapping or steering). This inconsistency will create failures in a protection event.	Change all stations to support the same protection preference, all stations must support wrapping or steering. Use the **show rpr-iee topology** command to verify protection preference. Use the **rpr protection preference wrap** or **no rpr protection preference wrap** configuration command to change the preference.

Table 4-7 SRP Wrap Messages

Alarm	Description	Solution
SRP1/1 wrapped on side B (side A User Request Forced Switch)	User-initiated forced switch on side A on node	User initiated, none.
SRP1/1 wrapped on side B (side A User Request Manual Switch)	User-initiated manual switch on side A on node	User initiated, none.
SRP1/1 wrapped on side B (side A Self Detect Signal Fail)	SONET layer 1 signal fail detected	Investigate Keepalive failure. Wrap occurred. Keepalive failure—SLOS, SLOF, LSF, or LAIS.
SRP1/1 wrapped on side B (side A Span Neighbor Signal Degrade)	SONET layer 1 signal fail detected	Investigate Keepalive failure. Wrap occurred. Keepalive failure—LSD.
SRP1/1 wrapped on side B (side A Self Detect Wait to Restore [WTR])	Wrap cleared, node initiated Wait to Restore (WTR) state	WTR period is 10 to 360 seconds (user configured), node will unwrap at end of WTR. None.

Table 4-7 SRP Wrap Messages (continued)

Alarm	Description	Solution
SRP1/1 wrapped on side B (side A Span Neighbor Forced Switch)	Neighbor node Forced Switch initiated by user; Node wrap to protect failed span	User initiated, none.
SRP1/1 wrapped on side B (side A Span Neighbor Manual Switch)	Neighbor node Manual Switch initiated by user; Node wrap	User initiated, none.
SRP1/1 wrapped on side B (side A Span Neighbor Signal Fail)	Neighbor node wrapped due to signal fail	Investigate the signal fail on neighbor node.
SRP1/1 wrapped on side B (side A Span Neighbor Signal Degrade)	Neighbor node wrapped due to signal degrade	Investigate the signal degrade on neighbor node.
SRP1/1 wrapped on side B (side A Span Neighbor WTR)	Wrap cleared, node initiated Wait to Restore state	WTR period is 10 to 360 seconds (user configured), node will unwrap at end of WTR. None.
SRP1/1 wrapped on side B (side A Long Request Forced Switch)	Neighbor node Forced Switch initiated by user; Node wrap to protect failed span; Secondary problem on the short path	Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
SRP1/1 wrapped on side B (side A Long Request Manual Switch)	Neighbor node Manual Switch initiated by user; Node wrap to protect failed span; Secondary problem on the short path	Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
SRP1/1 wrapped on side B (side A Long Request Signal Fail)	Neighbor node wrapped due to signal fail	Investigate signal fail on neighbor node. Investigate why the short path request was not received. Check other problems on the short span as indicated on the neighbor node.
SRP1/1 wrapped on side B (side A Long Request Signal Degrade)	Neighbor node wrapped due to signal degrade	Investigate signal degrade on neighbor node. Investigate why short path request was not received. Check other problems on the short span as indicated on the neighbor node.
SRP1/1 wrapped on side B (side A Long Request WTR)	Wrap cleared, Wait to Restore timer expired	None.

Table 4-8 SRP Unwrap Message

Alarm	Description	Solution
SRP1/1 unwrapped on side B (side A Wrap cause cleared)	Wrap cleared, Wait to Restore timer expired	None.

Note The solutions provided do not cover all possible problems related to specific alarms.

Basic Troubleshooting Ethernet for the Access Card

This section provides some basic troubleshooting guidelines for Fast Ethernet and Gigabit Ethernet interfaces on the access card. For additional information about troubleshooting Ethernet configurations, refer to the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* publication. For additional Cisco Ethernet-related documentation, refer to "Related Documentation" section on page xix.

The following sections present basic troubleshooting tips for hardware and simple software tasks.

- Verifying Interface Configuration, page 4-19
- FastEthernet/GigabitEthernet Is up, page 4-20
- Line Protocol Is up, page 4-20
- Duplex Mode Setting, page 4-21
- Speed Mode, page 4-21
- Output Hang, page 4-21
- CRC Field Counters, page 4-21
- Late Collision, page 4-21
- Carrier Signal, page 4-22

Verifying Interface Configuration

Use the **show interfaces FastEthernet** *slot/port* command to verify the configuration of a Fast Ethernet interface.

```
Router# show interfaces FastEthernet 2/1

FastEthernet2/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0001.64ff.3101 (bia0001.64ff.3101)
  Internet address is 194.16.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255,
load 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:04, output hang never
  Last clearing of "show interface" counters 00:00:13
  Queueing strategy: PXF First-In-First-Out
  Output queue 0/8192, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     1 packets output, 64 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Use the **show interfaces GigabitEthernet** *slot/port* command to verify the configuration of a Gigabit Ethernet interface.

```
Router# show interfaces GigabitEthernet 2/1

GigabitEthernet2/1 is up, line protocol is up
Internet address is 195.16.1.1/16
MTU 9100 bytes, BW 1000000 Kbit, DLY 10 usec, rely 255/255, load 0/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex mode, link type is autonegotiation, media type is SX
output flow-control is off, input flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:02, output 00:00:00, output hang never
Last clearing of "show interface" counters 03:41:33
Queueing strategy: PXF First-In-First-Out
Output queue 0/8192, 0 drops; input queue 0/75, 0 drops
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 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 watchdog, 0 multicast, 0 pause input
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
Router#
```

FastEthernet/GigabitEthernet Is up

If the interface is down, check the following conditions:

- The cable is fully connected.
- The cable is bent or damaged. If the cable is bent or damaged, the signal will be degraded.
- A hardware failure has not occurred. Observe the LEDs or use the **show** commands to determine if a failure has occurred. If the hardware has failed, replace the card or cable.
- If the interface is administratively down, use the **no shutdown** command to enable the interface.

See the "Verifying Interface Configuration" section on page 4-19 for an example output that shows interface status.

Line Protocol Is up

Check to see if the status is *line protocol is up*, in the first line of the output; see the "Verifying Interface Configuration" section on page 4-19. The status of the interface follows the slot/port configuration:

- The line protocol software processes determine that the line is unusable. Swap the cable.
- Check local or remote interface for misconfiguration.
- Swap interface module when there is a hardware failure.

Duplex Mode Setting

The local interface duplex mode configuration should match the remote interface configuration. See the "Verifying Interface Configuration" section on page 4-19 for an example output that shows duplex settings. Confirm that duplex settings are the same on both ends of the connection.

Speed Mode

The local interface speed mode field should match the remote interface configuration. See the "Verifying Interface Configuration" section on page 4-19 for an example output that shows speed settings. Speed setting display is shown in the following line:

```
10/100/auto
```

Output Hang

The output hang provides the number of hours, minutes, and seconds since the last reset caused by a lengthy transmission. For example, the output hang data is located on line 9 of the **show interfaces GigabitEthernet 2/1** router output:

```
Last input never, output 00:00:04, output hang never
```

See the "Verifying Interface Configuration" section on page 4-19 for a complete example output that shows output hang data.

CRC Field Counters

Excessive noise will cause high CRC errors accompanied by a low number of collisions. Perform the following checks if you encounter high CRC errors:

- Check the cables for damage.
- Verify that the correct cables are being used for the appropriate access card. For cabling specifications, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.

Late Collision

The console will display the following message when late collisions are detected:

```
Port 2/X - Late collision detected. Possible duplex mismatch.
```

Late collisions result from either of the following conditions:

- Ethernet cables are too long.
- Duplex mode does not match the remote interface.

For example, the late collisions data is located on line 22 of the **show interfaces FastEthernet 2/1** router output:

```
0 babbles, 0 late collision, 0 deferred
```

See the "Verifying Interface Configuration" section on page 4-19 for a complete example of the output that identifies late collisions.

Carrier Signal

The lost carrier, no carrier numbers track the number of lost carrier detect signals that have occurred.

- If the transmit clock signal is not active, check the interface for malfunction.
- Check for a cable problem.
- Carrier signal resets can occur when an interface is in one of the following states:
  - Looped back.
  - Shut down.

Cleaning the Fiber-Optic Connections

For information about cleaning fiber-optic cable connectors and receptacles, see the *Inspection and Cleaning Procedures for Fiber-Optic Connections* document. It provides detailed illustrations and photos of procedures and equipment required to properly clean fiber-optic connections.

CHAPTER 5

Maintaining the Cisco 10720 Internet Router

Overview

This chapter contains information for maintaining the Cisco 10720 Internet Router. The router is built to order and is ready for installation and startup when it leaves the factory.

After you install and configure the router, you might need to perform specific maintenance procedures or replace field-replaceable units (FRUs) to ensure that the router continues to operate properly.

⚠ **Caution** You must power down the router prior to any procedure. Failure to do so can result in harm to you or damage to your router.

Each of the following sections provide necessary information for successful removal and installation of FRUs in your router:

Safety Recommendations

Basic safety information is provided at the beginning of any procedure where safety can be an issue.

Read and understand the safety information provided in the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication before attempting any maintenance procedure that involves manipulation to the router hardware that is shipped with your router.

Required Tools and Equipment

This section presents the following topics:

- Tools, page 5-2
- Field-Replaceable Units, page 5-2

Tools

The following tools are required for maintaining the router:

- ESD-preventive strap
- Number 1 Phillips screwdriver
- 1/8-inch flat blade screwdriver
- Antistatic bag (or similar ESD-preventive container)
- Cable ties (optional)
- Wire stripper

Field-Replaceable Units

The following list presents field-replaceable units (FRUs) for the router:

- Replacement accessory rack mount (10720-ACCKIT=)
- Replacement AC router (CISCO10720-AC-A=)
  - Top assembly
  - AC dual power supply
  - Fan
- Replacement AC dual power supply (10720-AC-RPS=)
- Replacement access card (For access card versions and product numbers, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.)
- Replacement cable-management system and rack mount brackets
- Replacement DC router (CISCO10720-DC-A=)
- Top assembly
  - DC dual power supply
  - Fan
- Replacement DC dual power supply (10720-DC-RPS=)
- Replacement fan assembly (10720-FAN=)
- Replacement memory
- Replacement uplink card (For uplink card versions and product numbers, refer to the *Cisco 10720 Internet Router Uplink Cards Installation and Configuration* publication.)

Disconnecting Power from the Router

You must power down your router before maintaining any field-replaceable unit. The following sections present procedures to power down the router:

Overview

The following information demonstrates how to safely power down the router and disconnect site power for a router with AC or DC dual power supplies.

Caution The router must be used with the power supply type that originally shipped with the router from the factory and within in its marked electrical ratings. The AC power supply must be exchanged for AC; the DC power supply must be exchanged for DC. Cisco will not support this product if the power supply is exchanged for a non-factory power supply.

Cisco does not support the router if the power supply is changed from AC power supply to a DC power supply, or vice versa.

Note The power switch is part of the power supply.

Disconnect Device Safety Warning

The router power source must be disconnected before performing any maintenance task on the hardware modules.

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

Warning **The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.** Statement 66

Warning **This unit might have more than one power cord. To reduce the risk of electric shock, disconnect the two power supply cords before servicing the unit.** Statement 14

Warning **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.** Statement 91

Warning **An ON or OFF switch or a disconnect device is not provided on this product with direct current (DC) power. A readily accessible disconnect device, such as a circuit breaker, shall be incorporated into the fixed wiring.** Statement 232

Tools and Equipment Required

You will need the following tools:

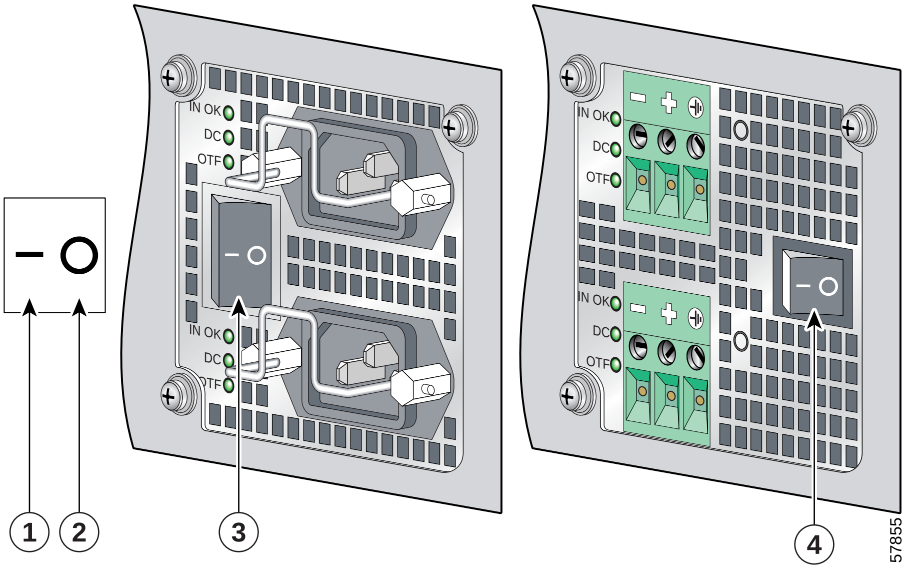
- ESD-preventive strap
- Wire stripper
- Cable ties

Powering Down the Router

To power down the router, perform the following steps:

If the cable-management cover is installed on the router, it must be removed in order to access the power switch. (See the "Removing and Installing the Cable-Management System" section on page 5-68.)

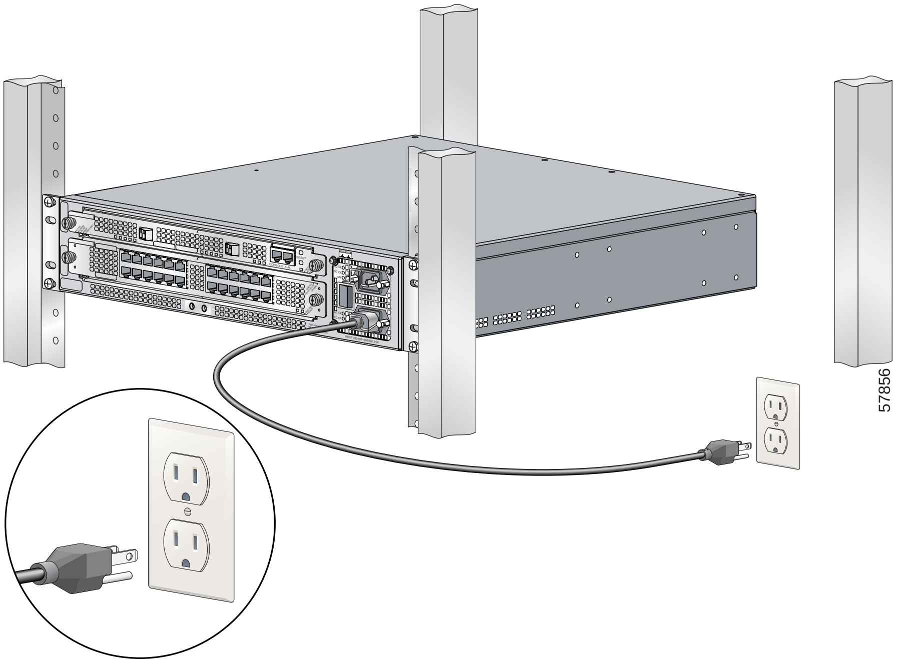
Figure 5-1 cPower Supply Switch Positions



1	– indicates power is on	**3**	AC power switch
2	O indicates power is off	**4**	DC power switch

Step 1 Press the power switch on the router to the off position (O). (See Figure 5-1.)

Figure 5-2 Removing the Router from the Power Source



Step 2 Disconnect the power source from the router as described below for each power input type:

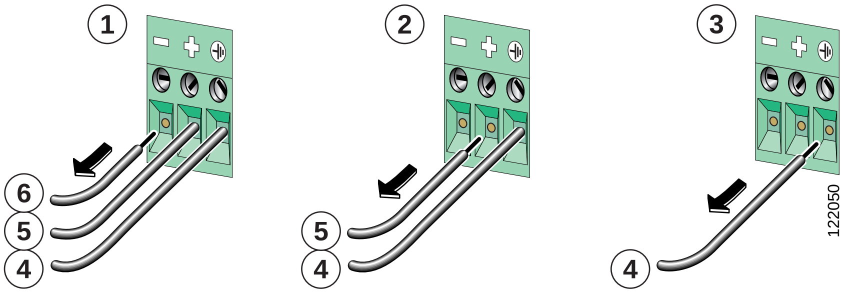
- AC—Disconnect the wall plug. (See Figure 5-2.)

Note Ensure that the power is removed from the DC circuit to ensure proper safety is maintained.

Warning **Before performing any of the following procedures, ensure that the power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit. Switch the circuit breaker to the OFF (O) position, and tape the switch handle of the circuit breaker in the OFF (O) position.** Statement 140

Caution Use an ESD-preventive strap when disconnecting power leads on the router. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Figure 5-3 Removing the DC Power Leads from the Terminal Block



1	Negative lead disconnected	**4**	Ground lead
2	Positive lead disconnected	**5**	Positive lead
3	Ground lead disconnected	**6**	Negative lead

- DC—Disconnect the power source to the router, then disconnect the DC power leads on the router. (See Figure 5-3.)

Step 3 For the DC-input power supply, loosen the three locking screws for the negative, positive, and ground screw connectors on the DC power supply terminal block. (See Figure 5-3.)

d. Remove the –48 VDC lead (black wire) from the terminal block negative connector (–).

e. Remove the +48 VDC lead (white lead) from the terminal block positive connector (+).

f. Remove the safety ground (green lead wire) from the terminal block ground connector.

Note Always remove the safety ground last.

Verifying the Router Is Powered Down

To ensure that your router is properly powered down, check the following:

- LED lights are off.
- Fans are not running.
- Power switch is pressed to the off position (O).
- Power is disconnected at the source.

Connecting Power to the Router

Before connecting the router power supply, read the information provided in the following sections:

- Safety, page 5-7
- Tools and Equipment Required, page 5-7
- Connecting the AC Power Supply, page 5-7
- Connecting the DC Power Supply, page 5-9

Safety

Warning **When installing the unit, always make the ground connection first and disconnect it last.** Statement 42

Warning **Before performing any of the following procedures, ensure that the power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit. Switch the circuit breaker to the OFF (O) position, and tape the switch handle of the circuit breaker in the OFF (O) position.** Statement 140

Tools and Equipment Required

You will need the following tools and equipment to power up the router:

- ESD-preventive strap
- Wire stripper
- Cable ties

Connecting the AC Power Supply

Caution Before you install, operate, or service the system, read the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication. This publication contains important safety information you should know before working with the system.

Note We recommend that you attach each AC-input power supply to a dedicated power source for redundancy and use an uninterruptable power supply (UPS) to protect against power failures. Each AC power supply operating between 100 and 240 VAC requires a dedicated 15A electrical power service for North America or a 10A electrical power service for international specifications.

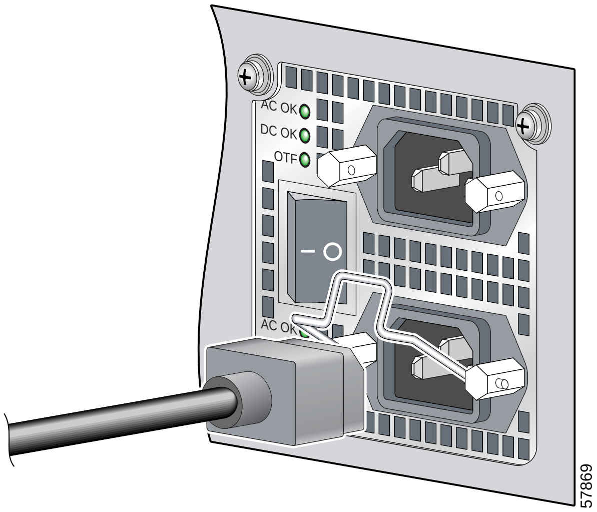
To connect the AC power supply, perform the following steps:

Step 1 Verify that the power switch on the router is off (O). (See Figure 5-1.)

Step 2 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the “Preventing Electrostatic Discharge” section on page 2-3.)

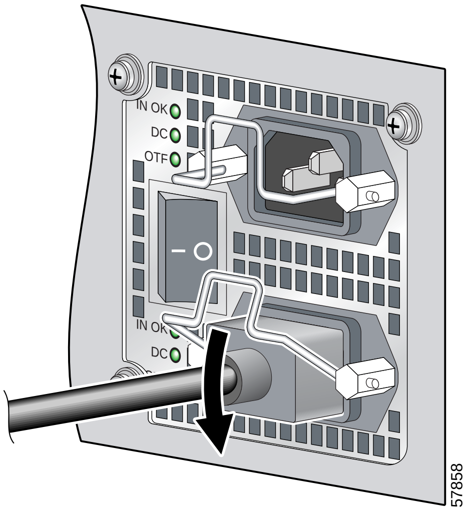
Step 3 Connect the AC power cord to the AC power supply receptacle on the router. (See Figure 5-4.)

Figure 5-4 Connecting the AC Power Cord to the Router



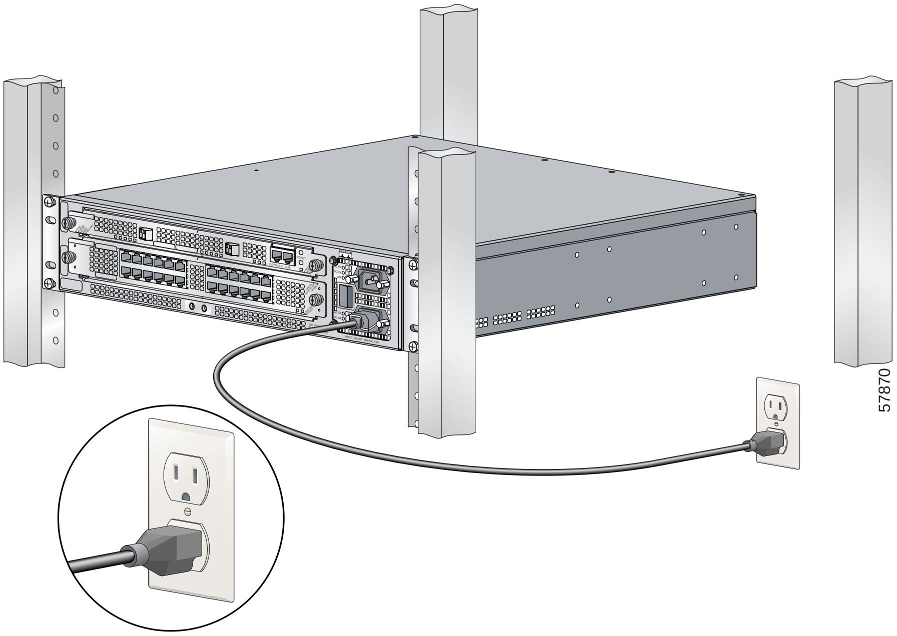
Step 4 Close the wire bracket over the power cord plug. (See Figure 5-5.)

Figure 5-5 Securing the Power Cord with the Wire Bracket



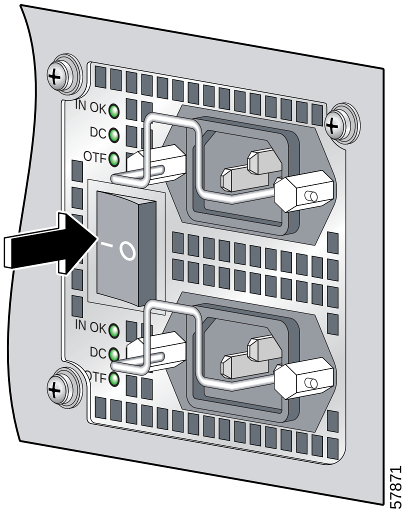
Step 5 Connect the other end of the AC power cord to the AC source receptacle. (See Figure 5-6.)

Figure 5-6 Connecting the Router to the AC Receptacle



Step 6 Press the power switch on (–). (See Figure 5-7.)

Figure 5-7 Power Switch in the On (—) Position



Connecting the DC Power Supply

Note The minimum wire gauge size supported on the DC dual power supply is 17 American Wire Gauge (AWG), which has a 1.5mm wire diameter. The maximum wire gauge size supported on the DC dual power supply is 10 AWG, which has a 6mm wire diameter.

To connect the DC power supply, perform the following steps:

Step 1 Ensure that the –48V and +48V leads are disconnected from the power source.

Step 2 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 3 Using a wire stripper, strip approximately 0.55 inch (14 mm) from the –48V, +48V, and ground leads. (See Figure 5-8 and Figure 5-9.)

Figure 5-8 Stripping the DC-Input Leads

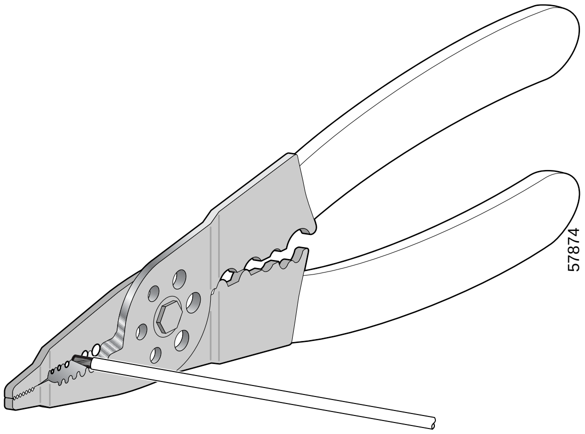
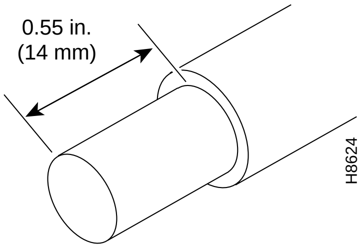
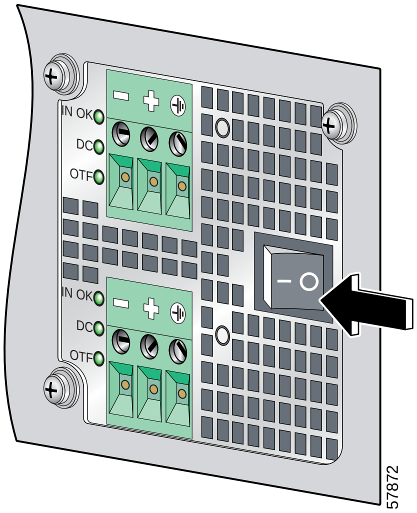


Figure 5-9 DC Lead Stripped 0.55 inch (14 mm)



Step 4 Confirm that the power switch located on the front of the power supply is in the off position (O). (See Figure 5-10.)

Figure 5-10 Power Switch in the Off (O) Position



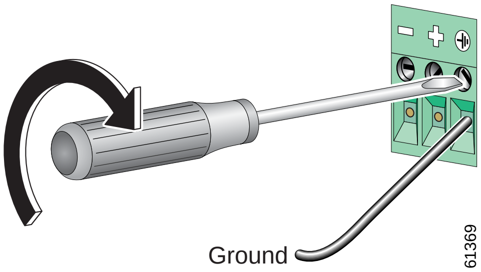
Step 5 Locate the ground, positive, and negative terminals. (See Figure 5-10.)

Caution Leave a small service loop in the ground lead. If a strain is placed on the ground, the +48V, or the –48V DC input leads causing them to pull out of the power supply, the ground power lead must be the last to disconnect from the power supply terminal.

Step 6 Insert the stripped end of the ground lead all the way into the ground lead receptacle. Tighten the receptacle screw using a 1/8-inch flat blade screwdriver. (See Figure 5-11.)

Note Make sure the entire stripped end of each lead is inserted all the way into its receptacle. If any exposed wire at the stripped end of a lead is visible after inserting the lead into its receptacle, remove the lead from the receptacle, use the wire stripper to cut the stripped end of the lead, and repeat Step 2 through Step 6.

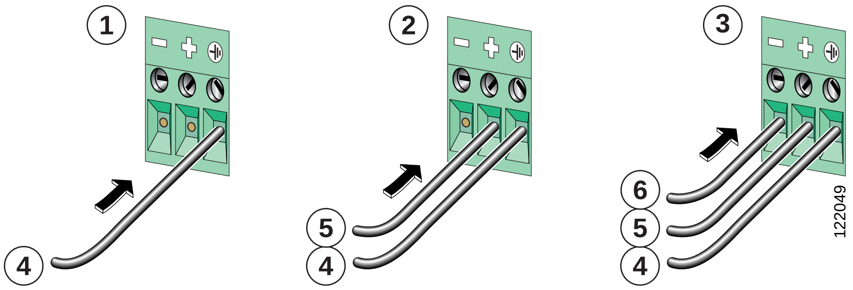
Figure 5-11 Tightening the DC Lead Receptacle



Step 7 Connect the leads in the following order: (See Figure 5-12.)

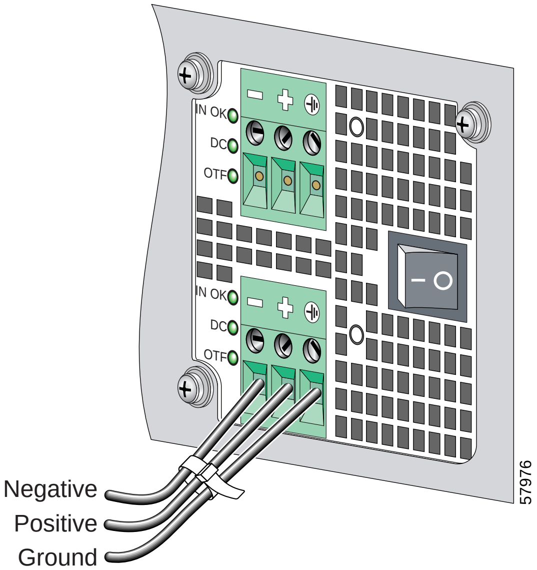
1. Ground (green wire)
2. Positive (white wire)
3. Negative (black wire)

Figure 5-12 Connecting the DC Power Leads



1	Ground lead connected	**4**	Ground lead
2	Positive lead connected	**5**	Positive lead
3	Negative lead connected	**6**	Negative lead

Figure 5-13 Power Leads Secured with Cable Tie



Step 8 After tightening the receptacle screw for the +48V, and –48V DC-input leads, use a cable tie to secure the three leads. (See Figure 5-13.)

Caution Allow sufficient slack in the power cable leads for strain relief. The power cable leads should be adequately secured to prevent the power supply terminal connections from being subjected to strain.

Step 9 After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the on position.

Step 10 Press the power switch on (—). (See Figure 5-1.)

Removing and Installing the Router Chassis Cover

The following sections provide information on how to remove and replace the router cover:

- Safety, page 5-13
- Required Tools and Equipment, page 5-13
- Removing the Router Cover, page 5-13
- Installing the Router Cover, page 5-15

Safety

The cover must replaced and securely fastened as soon as possible after removing it to prevent damage to the router components.

Caution Power down the router before working on it and secure the router cover completely before remounting the router.

For more information on powering down your system, refer to the "Disconnecting Power from the Router" section on page 5-3.

Required Tools and Equipment

You will need the following tools:

- ESD-preventive strap
- Number 1 Phillips screwdriver

Removing the Router Cover

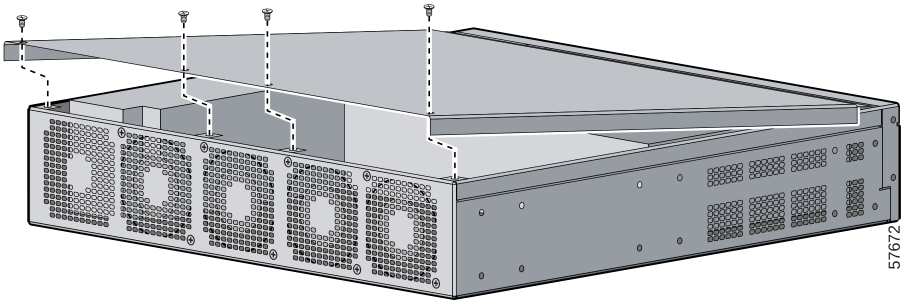
To remove the router cover, perform the following steps:

Step 1 If the cable-management cover is installed on the router, it must be removed in order to access the power switch. (See the "Removing and Installing the Cable-Management System" section on page 5-68.)

Caution Do not remove the cable-management tray until all cables are removed from the cards and power supply.

Step 2 Power down the router. (See the "Disconnecting Power from the Router" section on page 5-3.)

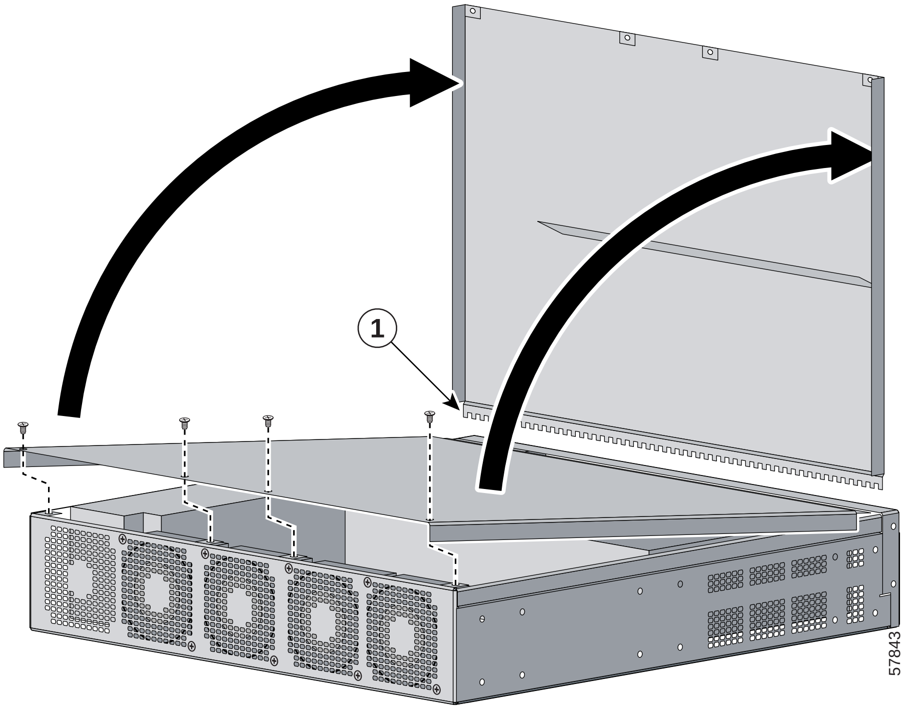
Figure 5-14 Screws on the Router Cover



Step 3 Arrange the router so that you face a side panel. (See Figure 5-14.)

Step 4 Using a Number 1 Phillips screwdriver, remove the four screws that secure the cover to the router chassis. (See Figure 5-14.) Place the screws in a safe place for use later.

Figure 5-15 Removing the Router Chassis Cover



1	Router chassis cover		

Step 5 Slide the cover back toward the fan assembly until the cover disengages from the front of the router chassis. Lift the cover up and away from the router chassis and store it in a safe place until it is installed back on the router chassis. (See Figure 5-15.)

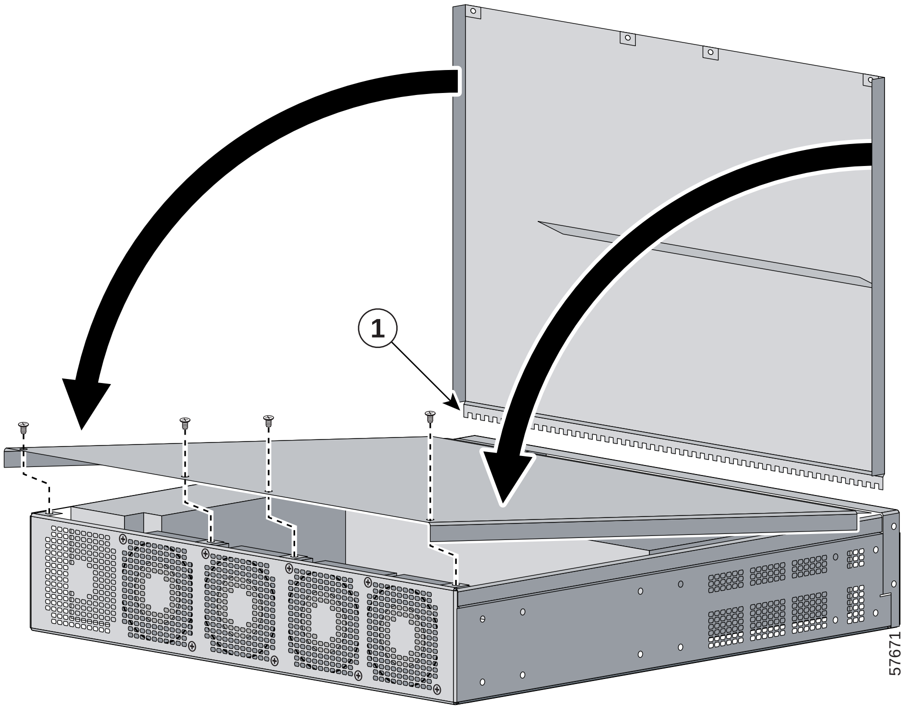
Caution Replace the cover after completing any maintenance task on the router. This reduces the chance of damage to the router components while the router is not in service.

Installing the Router Cover

To replace the router cover, perform the following steps:

Tip If you are right-handed, face the router so the front is on your left and the back is on your right side. This position lets you align the cover and the router chassis more easily. Reverse the position of the router if you are left-handed.

Figure 5-16 Positioning the Cover in the Router

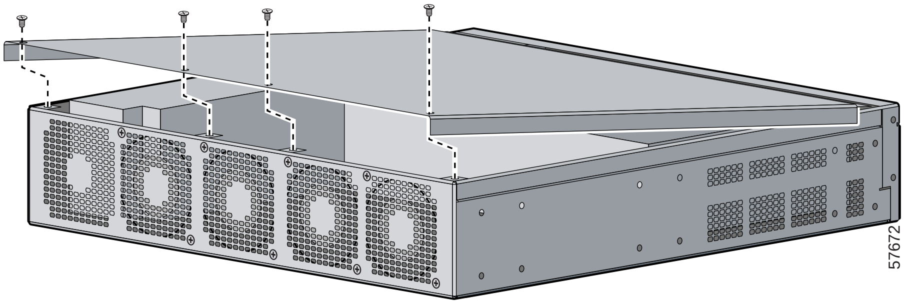


1	Router chassis cover		

Step 1 Arrange the router so that you face a side panel. (See Figure 5-17.)

Step 2 Place the router cover over the router and align the front edge of the router cover with the front lip of the router chassis. Slide the cover down and forward until the router cover is firmly seated under the front lip of the router chassis. Lower the back of the cover to close the router. (See Figure 5-16.)

Figure 5-17 Securing the Router Cover



Step 3 Using a Number 1 Phillips screwdriver, secure the router cover with four screws. (See Figure 5-17.)

Step 4 Reinstall the router on a rack, wall, or desktop.

Step 5 Reinstall all interface cables.

Step 6 Reconnect the AC power cord or rewire the DC power supply. (See the "Connecting the AC Power Supply" section on page 5-7 and "Connecting the DC Power Supply" section on page 5-9.)

Step 7 After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the on position.

Step 8 Power up –) the router. The internal power supply fan should also power up.

Removing and Installing the Router Fan Assembly

The following sections provide information for removing, installing, and troubleshooting the router fan assembly:

- Safety, page 5-16
- Required Tools and Equipment, page 5-17
- Removing the Fan Assembly, page 5-17
- Installing the Fan Assembly, page 5-21
- Verifying Fan Assembly Functionality, page 5-26
- Troubleshooting the Fan Assembly, page 5-26

Safety

Before performing this procedure, read the following caution:

Caution Power down the router before working on it and secure the router cover completely before remounting the router.

Required Tools and Equipment

You will need the following tools and equipment:

- ESD-preventive strap
- Number 1 Phillips screwdriver
- Replacement fan assembly
- Antistatic bag (optional)

Removing the Fan Assembly

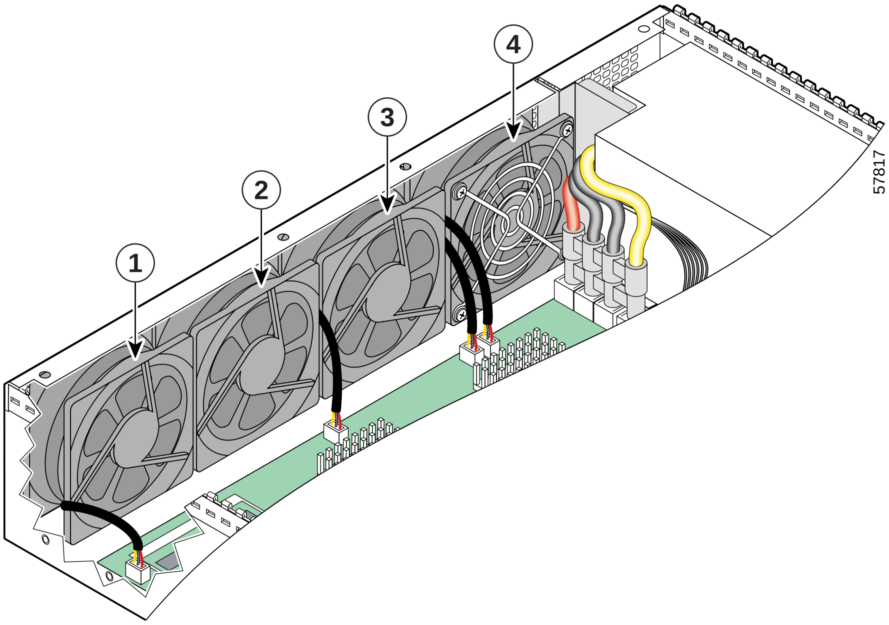
Perform the following steps to remove the fan assembly:

Step 1 If the cable-management system is installed on the router, remove it to access the power switch. (See the "Removing and Installing the Cable-Management System" section on page 5-68.)

Step 2 Power down your router as described in the "Disconnecting Power from the Router" section on page 5-3.

Step 3 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

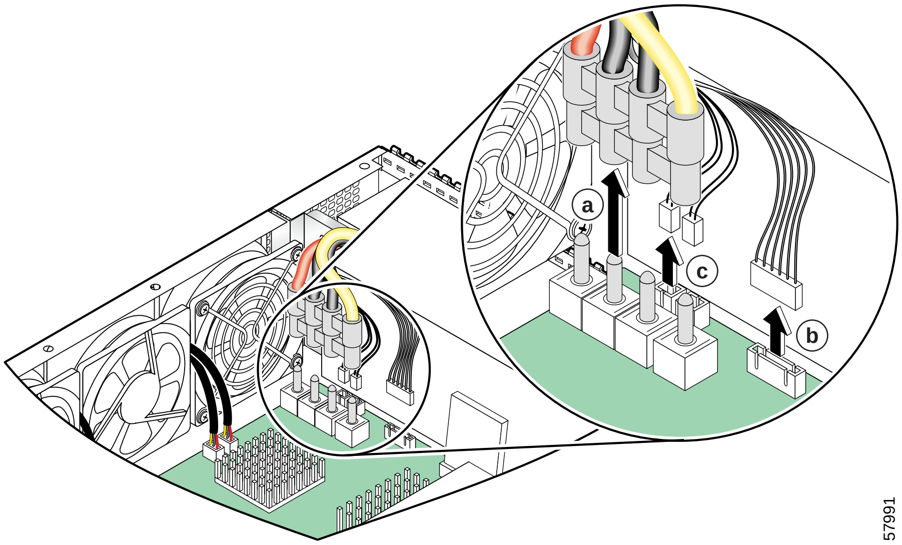
Figure 5-18 Fan Locations at the Back of the Router



1	Fan Number 1	**3**	Fan Number 3
2	Fan Number 2	**4**	Fan Number 4

There are four fans and four separate connectors on the main board. Fan Number 1 is located farthest away from the power supply. Fan Number 4 is located closest to the power supply and must have a guard attached at all times. (See Figure 5-18.)

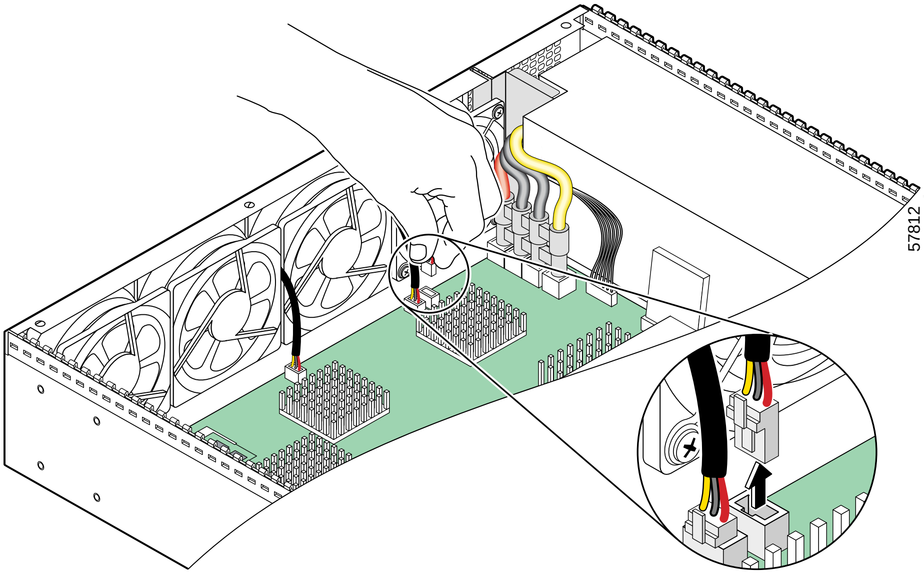
Figure 5-19 Disconnecting the Power Supply Unit From the Main Board



a	4-jack harness	**c**	2-pin +/–12V connector
b	6-pin connector		

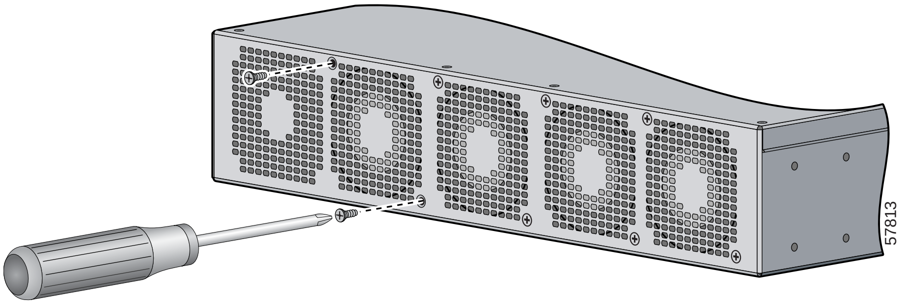
Step 4 Disconnect the 4-jack harness (main power supply unit output cable) from the main board and move it behind the power supply unit in order to access Fan Number 4. (See Figure 5-19.)

Figure 5-20 Removing Power Connection from the Main Board



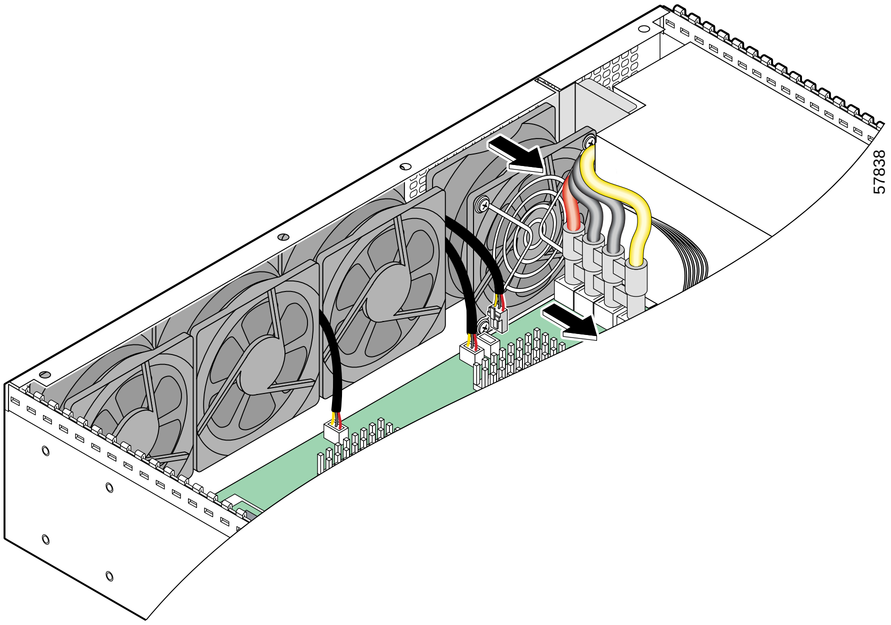
Step 5 Remove the power connection for the fan from the main board. (See Figure 5-20.)

Figure 5-21 Removing Fan Assembly Mounting Screws



Step 6 Using a Number 1 Phillips screwdriver, unscrew the two screws located behind the fan on the back end of the router. (See Figure 5-21.)

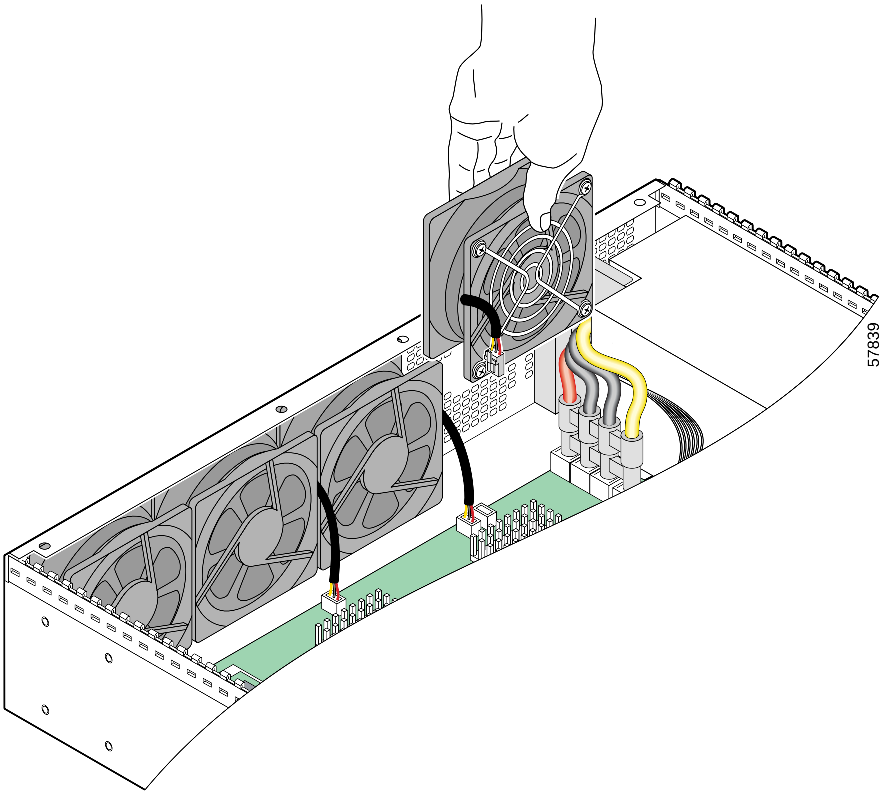
Figure 5-22 Sliding Fan Out from the Router Chassis



Note Fan Number 4 has a guard mounted on it and should remain that way at all times when installed in the router.

Step 7 After the fan has been fully unsecured from the router, slide the fan forward and lift it out of the router chassis. (See Figure 5-22 and Figure 5-23.)

Figure 5-23 Lifting the Fan Out of the Router Chassis



Installing the Fan Assembly

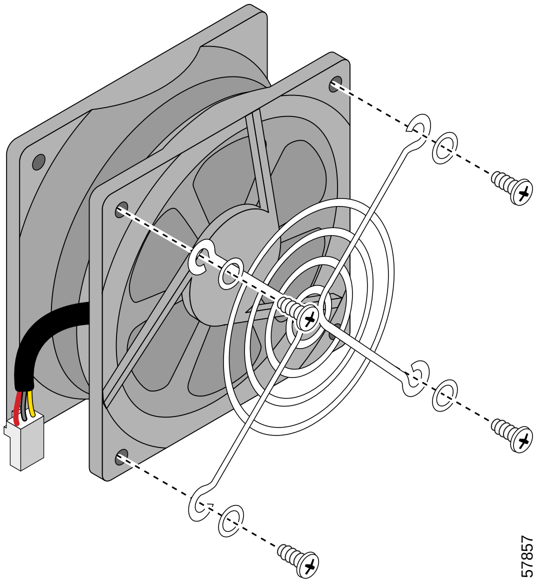
To install the fan assembly, perform the following steps:

Step 1 Verify that the router is powered down. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 2 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Note Step 3 is only required when installing Fan Number 4. To install Fan Numbers 1, 2, and 3, proceed to Step 4.

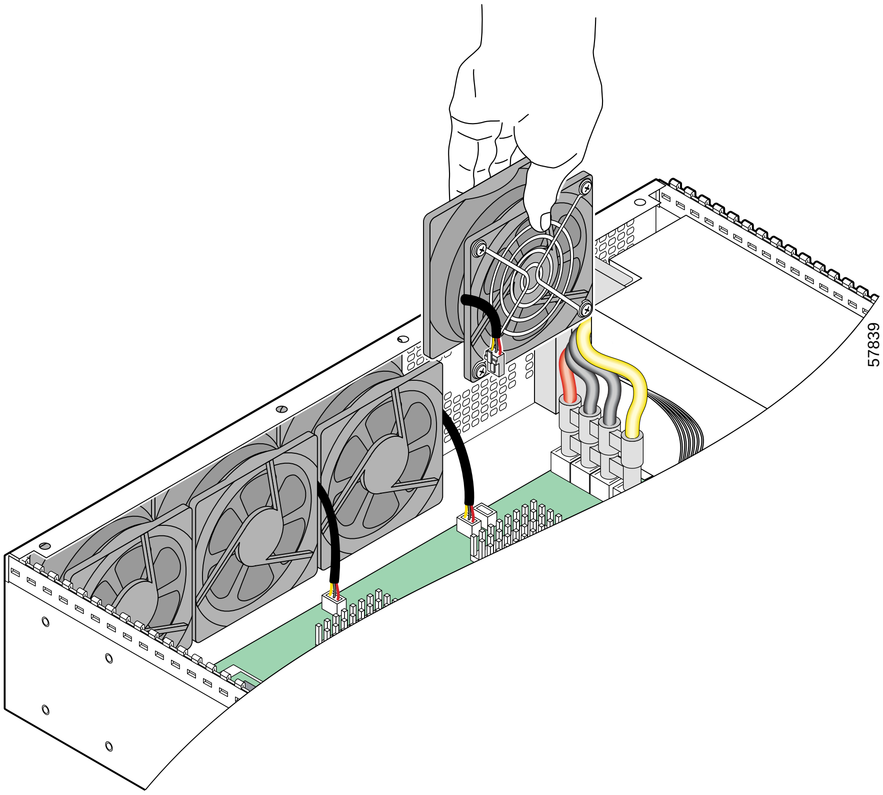
Figure 5-24 Installing the Fan Guard (Required on Fan Number 4)



Step 3 Install the fan guard on Fan Number 4 before securing the fan to the router chassis or operating the router. To install the fan guard, perform the following:

1. Place the fan guard onto the back of the fan. (See Figure 5-24.)
2. Using four washers, place one on each corner of the fan guard. (See Figure 5-24.)
3. Using a Number 1 Phillips screwdriver, secure the fan guard and washers to the fan with four screws. (See Figure 5-24.)

Figure 5-25 Placing Fan in the Router Chassis



Step 4 Carefully place the fan between the main board and the back of the router chassis and slide the fan into position. (See Figure 5-25 and Figure 5-26.)

Figure 5-26 Positioning Fan Inside Router Chassis

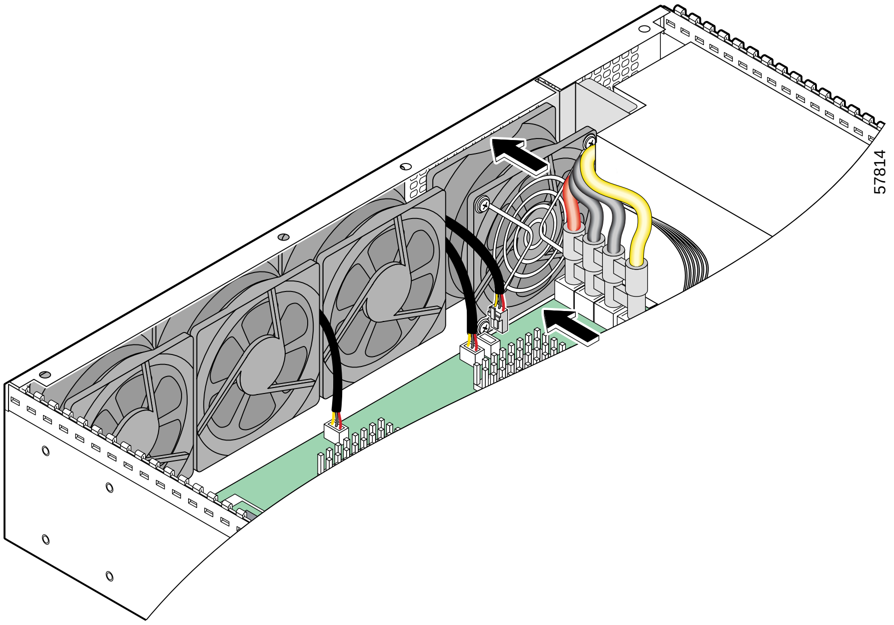
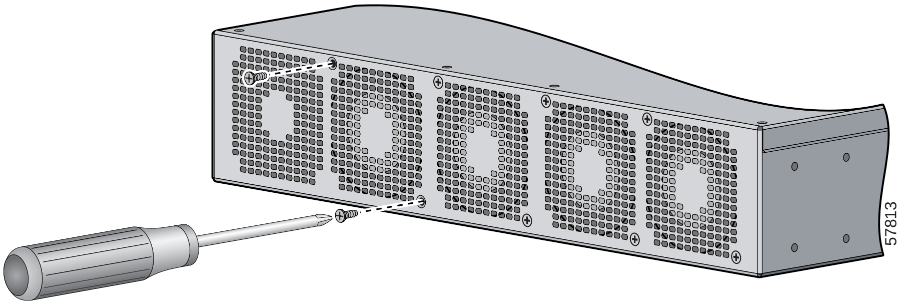
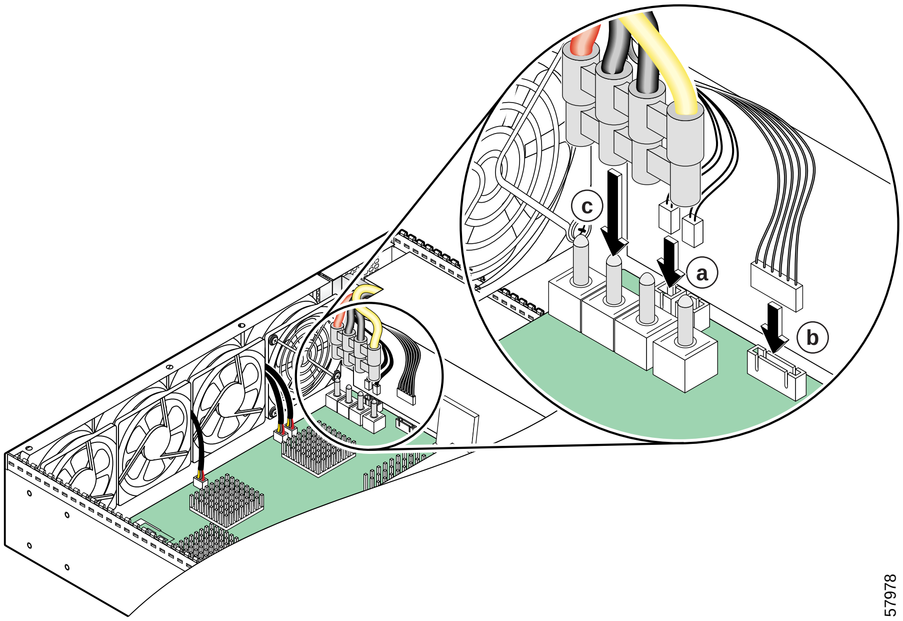


Figure 5-27 Securing the Fan Assembly to the Router Chassis



Step 5 Using a Number 1 Phillips screwdriver, secure the fan to the router chassis with two screws. (See Figure 5-27.) The fan assembly is now installed in the back of the router.

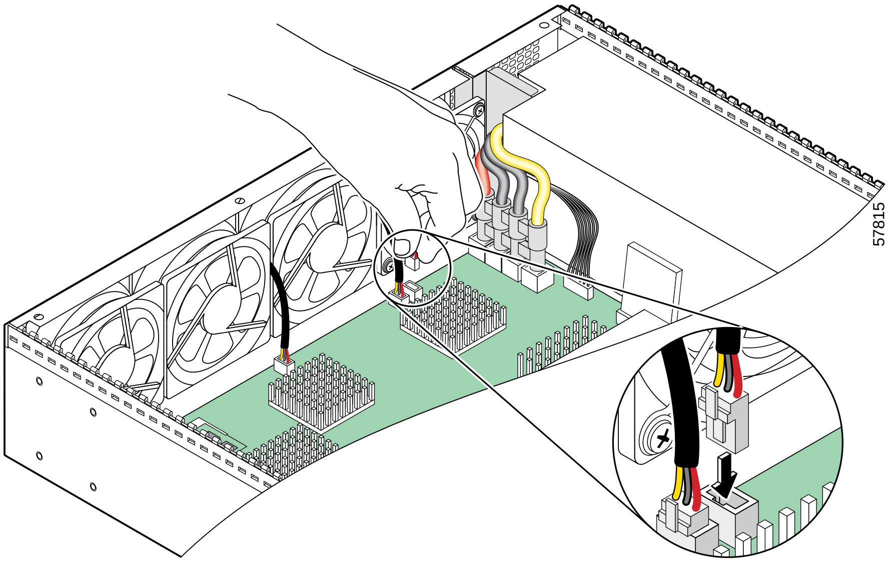
Figure 5-28 Connecting the Power Supply Unit to the Main Board



a	2-pin +/–12V connector	c	4-jack harness
b	6-pin connector		

Step 6 Move the 4-jack harness (main power supply unit output cable) out from behind the power supply unit and reconnect it to the main board. (See Figure 5-28.)

Figure 5-29 Connecting the Fan Power Cable to the Main Board



Step 7 Connect the fan power connection to the main board. (See Figure 5-29.)

Step 8 Reinstall the chassis cover. (See the "Removing and Installing the Router Chassis Cover" section on page 5-13.)

Step 9 Reconnect all interface cables to the uplink card and access card.

Step 10 Power up the router. (See the "Connecting Power to the Router" section on page 5-7.)

Verifying Fan Assembly Functionality

Use the **show environment** command to display router environment information. Overtemperature conditions can signal problems with the fan assembly. (See the "Using the show environment all Command" section on page 3-45.)

Troubleshooting the Fan Assembly

Verify the following when troubleshooting the fan assembly installation:

- Check for proper seating of the fan connection on the main board.
- Ensure that all power connections are securely connected.
- Ensure that adequate ventilation is available.

Removing and Installing the Route Processor Memory

To upgrade and verify the Route Processor (RP) memory in the Cisco 10720 Internet Router, the following procedures must be completed in the specified order.

Caution To prevent upgrade failure, complete the upgrade using the following procedure sequence. Ensure that each procedure is complete before starting the next procedure.

1. Check that the Cisco 10720 Internet Router has Cisco IOS Release 12.0(27)S or later installed and running. See the "Upgrading and Verifying the Cisco IOS Release" section on page 5-27 for procedures.
2. Upgrade the ROM monitor (ROMmon) image on the Cisco 10720 Internet Router, then verify the version. See the "Upgrading and Verifying the ROMmon Image" section on page 5-27 for procedures.

   Refer to the *Cisco IOS Release 12.0 Configuration Fundamentals Configuration Guide* for information on ROMmon.
3. Replace the 256-MB RP memory with 512-MB RP memory.

Upgrading and Verifying the Cisco IOS Release

Ensure that the Cisco IOS Release 12.0(27)S or later is installed and running on the Cisco 10720 Internet Router. Refer to the “File Management” chapter of the *Cisco IOS Release 12.0 Configuration Fundamentals Configuration Guide* for procedures.

Once the upgrade is completed, use the **show version** command to check that the Cisco 10720 Internet Router has the Cisco IOS Release 12.0(27)S or later installed and running.

Upgrading and Verifying the ROMmon Image

The following sections provide procedures for upgrading both the golden ROM monitor (ROMmon) image (the original image that you receive with the router) and the alternate ROMmon image. For additional information about ROMmon features, refer to the *Cisco IOS Software Configuration for the Cisco 10720 Internet Router* document.

The following procedures are provided:

- Upgrading the Golden ROMmon Image with FPGA Version 3, page 5-27
- Upgrading the Golden ROMmon Image with FPGA Version 4, page 5-28
- Upgrading the ROMmon Image, page 5-28
- Verifying the ROMmon Image, page 5-29

Upgrading the Golden ROMmon Image with FPGA Version 3

To upgrade the golden ROMmon (S ROMmon) image on the Cisco 10720 Internet Router with FPGA version 3, follow these steps:

Step 1 Determine the version of the FPGA by using the **show diag** command. The last line in the sample output below provides the information on the FPGA version.

```
C10720# show diag
Mainboard:
  MAIN:type 0x0001, 800-08427-01 rev 255 (decimal) - Warning:Pre-FCS
revision. dev none
        SW key:00-00-00  S/N CAT0502000L
        Test hist:0x00(no failure) RMA#:000000
        RMA hist:0 upgrades 0 field failures
  PCA: 73-5349-02 rev 255 (decimal) - Warning:Pre-FCS revision. fab
ver 2
  DIAG:Test count:0x00000000 Test results:0x00000000
  Van Allen Memory Size:64 MB
  Toaster Memory Size - Column 1:32 MB
  Toaster Memory Size - Column 2:128 MB
  Toaster Memory Size - Column 3:32 MB
  Toaster Memory Size - Column 4:32 MB
  Toaster Memory Size - Column 5:32 MB
  Toaster Memory Size - Column 6:32 MB
  Toaster Memory Size - Column 7:32 MB
  Toaster Memory Size - Column 8:32 MB
  Main FPGA ver:0x0003
```

With a FPGA version 3, you will need to upgrade the FPGA to version 4 before you can upgrade the golden ROMmon. Only FPGA version 4 supports the golden ROMmon upgrade.

Step 2 Download Cisco IOS Release 12.0(28)S or later releases of 12.0 S.

Step 3 Use the **upgrade hw-mnodule slot 0** command to upgrade the main FPGA.

```
C10720# upgrade hw-module slot 0
```

The upgrade process takes about one minute. Do not power off the router when you finish the upgrade.

Step 4 Complete the FPGA programming. When finished, power off and power on the router to have the upgrade take effect.

Step 5 Use the **show diag** command to verify that you have successfully upgraded to FPGA version 4.

Upgrading the Golden ROMmon Image with FPGA Version 4

To upgrade the golden ROMmon image with FPGA version 4, follow these steps:

Step 1 Make sure you are at the ROMmon F1 or F2 region. You cannot upgrade the golden ROMmon from the golden ROMmon region. To run ROMmon from the F1 or F2 region, see the "Upgrading the ROMmon Image" section on page 5-28 and the '"“Verifying the ROMmon Image” section on page 5-29.

Step 2 Copy the ROMmon file to Flash memory.

Step 3 Use the **upgrade rom-monitor file** command to upgrade the golden ROMmon.

```
C10720# upgrade rom-monitor file C10700_ROMMON_FILE_NAME gold
Upgrading ROMMON gold region...
Erasing flash
Programming flash
Verifying new image
Gold region upgrade complete, C10720 must be reloaded.
C10720#
```

Step 4 Power off and power on the router to complete the golden ROMmon upgrade procedure.

Upgrading the ROMmon Image

To upgrade the ROMmon image on the Cisco 10720 Internet Router, perform the following steps:

Step 1 From the IOS prompt, view ROMmon information using the **show rom-monitor** command.

```
Router# show rom-monitor
Region region1:INVALID
Region region2:INVALID
Currently running ROMMON from S (Gold) region
```

Step 2 Copy the new ROMmon record file on to the router Flash memory using the **copy tftp flash** command.

```
Router# copy tftp flash
```

Step 3 Program the new ROMmon into the router ROMmon Flash memory using the **upgrade rom-monitor file flash:***name* command.

```
Router# upgrade rom-monitor file flash:name
ROMMON image upgrade in progress
Erasing flash
Programming flash
```

```
Verifying new image
ROMMON image upgrade complete, router must be reloaded.
```

Step 4 Proceed to the "Verifying the ROMmon Image" section on page 5-29.

Verifying the ROMmon Image

To verify the ROMmon image upgrade on the Cisco 10720 Internet Router, use the **show rom-monitor** command.

```
Router# show rom-monitor
Region F1: APPROVED, preferred
Region F2: INVALID
Currently running ROMMON from F1 region
```

Removing the 256-MB Route Processor Memory

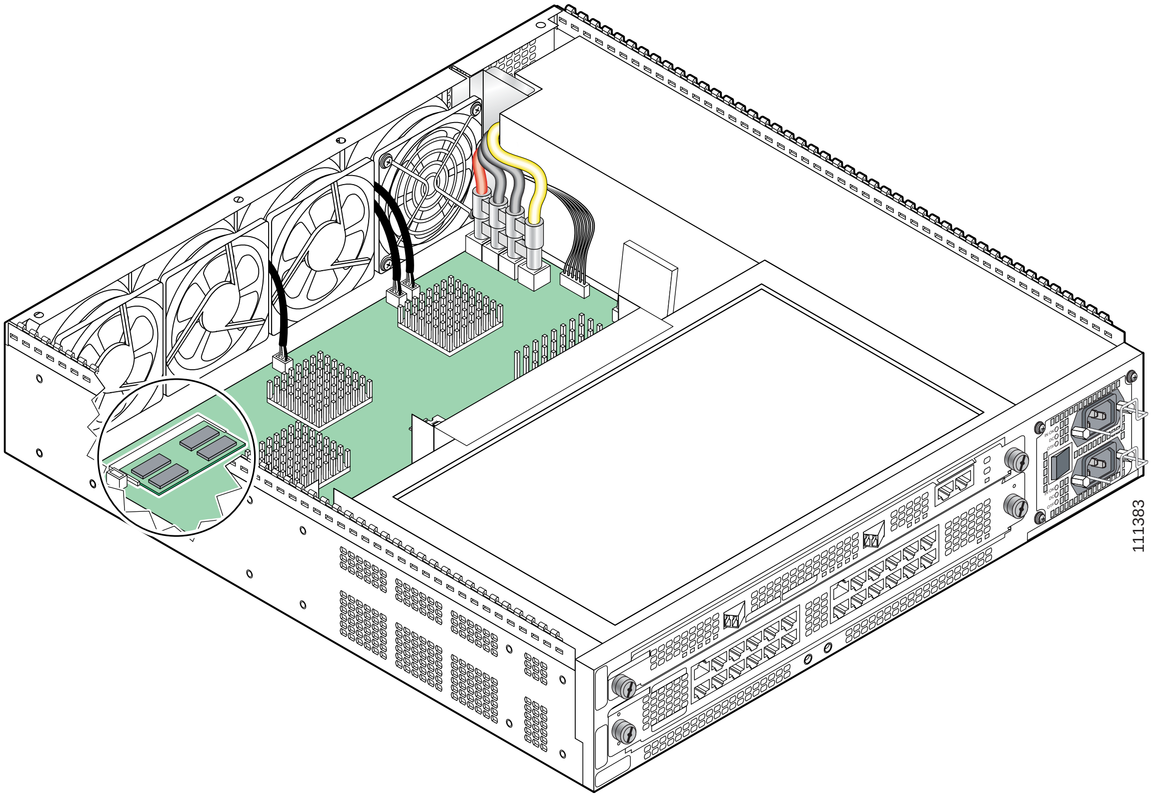
To remove the RP memory module, perform the following steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Place the router on an antistatic mat so that the front of the router is facing you.

Step 3 Locate the RP memory module on the router motherboard. (See Figure 5-30 for the location of the RP memory module on the motherboard.

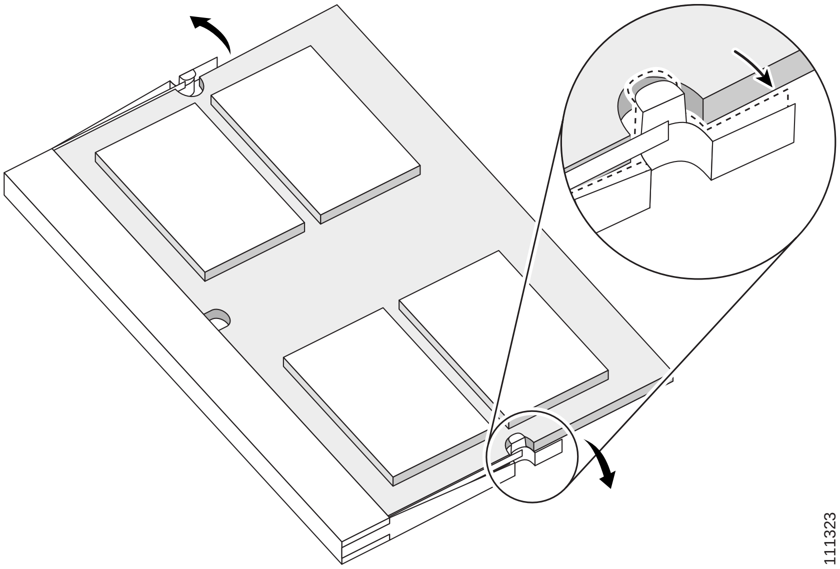
Figure 5-30 RP Memory Module on the Router Motherboard



Step 4 Remove the RP memory module by gently moving the latches in an outward direction, parallel to and away from the memory module until it releases and rotates to a 45-degree angle. (See Figure 5-31.)

⚠ **Caution** The latch on the RP memory socket is enclosed by the metal strain relief latch. The latch should never be moved past the metal strain relief latch.

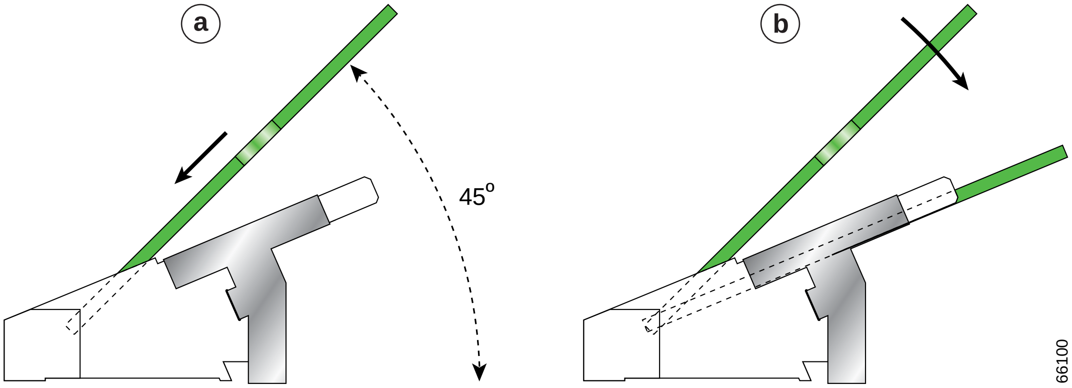
Figure 5-31 Moving the Latches Away from the RP Memory Module



Caution Handle the edges of the RP memory module only. Do not touch the integrated circuit devices on the RP memory module, the metal traces (or *fingers*) along the edge of the RP memory module, or the pins in the RP memory socket.

Step 5 As the RP memory module is released, the module is positioned at a 45-degree angle. Gently pull the RP memory module out of the socket. Continue to keep the module in a 45-degree angle until it is completely removed from the socket guides. (See Figure 5-32.)

Figure 5-32 Removing the RP Memory Module



a	Inserting the RP memory module	b	Locking the RP memory module

Step 6 Immediately place the RP memory module in an antistatic bag to protect it from ESD damage.

Installing the 512-MB Route Processor Memory

To install the RP memory module, perform the following steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Place the router on an antistatic mat so that the front of the router is facing you.

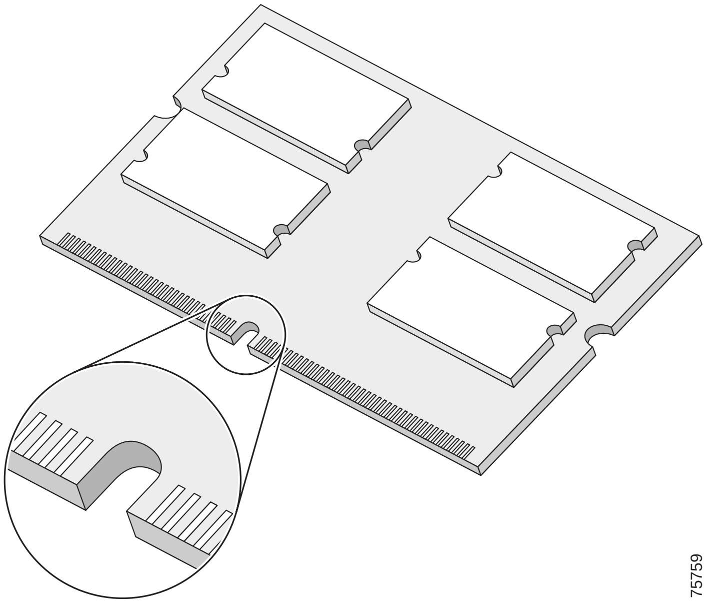
Step 3 Locate the RP memory socket on the router motherboard. (See Figure 5-30.)

Step 4 Remove the new 512-MB RP memory module from the protective antistatic bag.

Caution Grasp the edges of the RP memory module only. Do not touch the integrated circuit devices on the RP memory module, the metal traces (or *fingers*) along the edge of the memory, or the pins in the memory socket.

Step 5 Line up the RP memory module key with the key in the motherboard socket. (See Figure 5-33.)

Figure 5-33 RP Memory Module with Key in Face-Up Position



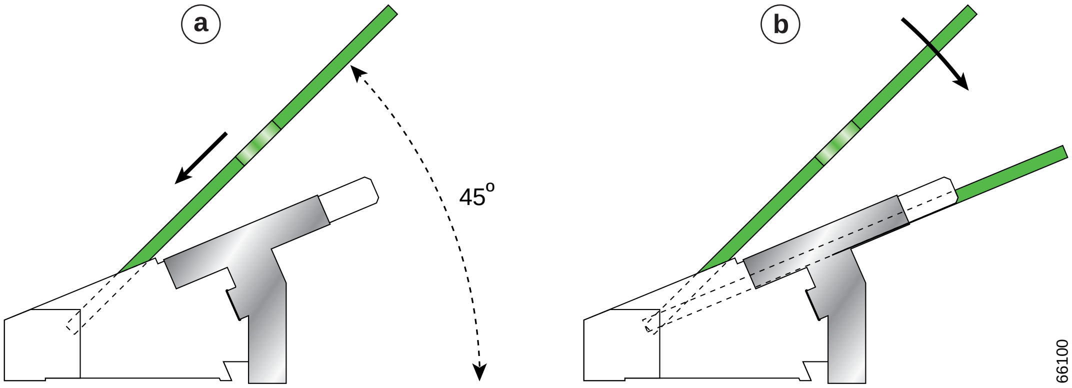
Step 6 Line up the RP memory module at a 45-degree angle. (See Figure 5-34a.)

Note With the key is in the face-up position, the metal traces on the left side of the key measure 0.9 inch (23.20 mm). The metal traces on the right side of the key measure 1.29 inches (32.80 mm). The RP memory cannot be inserted until the keys are lined up properly.

Step 7 Place both thumbs at the end of the socket and use your index fingers to guide the memory module in to the socket until it is fully seated.

Ensure that your index fingers are located on the outer corners of the RP memory module to maintain even pressure when the module is seating in the socket.

Figure 5-34 Installing the RP Memory Module



a	Inserting the RP memory module	b	Locking the RP memory module

Step 8 Gently press the RP memory module down using your index fingers, distributing even pressure across the module until it locks into the tabs. (See Figure 5-34b.)

Caution Excessive pressure can damage an RP socket.

Step 9 Verify that the release levers are flush against the side of the socket. If they are not, the RP memory module might not be seated properly.

Step 10 If the module appears misaligned, carefully remove it and reseat it, ensuring that the release lever is flush against the side of the RP memory socket.

Checking the 512-MB Route Processor Installation

When you power up the router, the router reinitializes and detects the memory change as part of the reinitialization cycle. The time required for the router to initialize can vary with different router configurations and memory configurations.

If the router does not initialize properly after you replace the memory, or if the console terminal displays a checksum or memory error, verify that you have installed the correct RP memory and that it is installed correctly in the router.

If the router fails to restart properly after several attempts and you are unable to resolve the problem, access Cisco.com or contact your Cisco service representative for assistance. Before calling, make note of any console error messages, unusual LED states, or other router indications or behaviors that might help to resolve the problem. Under certain highly improbable scenarios (for example, battery failure), the router may fail to boot after the 512-MB upgrade. In such cases, see the "Obtaining Technical Assistance" section on page xxii for information on contacting Cisco.

To check the installation of the RP memory, use the **show version** command and check that the upgraded RP memory is 512 MB.

See the following **show version** command example to locate the RP memory. Line 17 of the example is in italic print to indicate where the RP memory is listed.

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 10700 Software (C10700-P-M), Version 12.0(27)S
TAC Support:http://www.cisco.com/tac
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 28-Sep-01 11:44 by user_1
Image text-base:0x50010960, data-base:0x50660000

ROM:System Bootstrap, Version 12.0(20010529:144545) [rommon1 149], DEVELOPMENT SOFTWARE
BOOTLDR:10700 Software (C10700-P-M), Version 12.0(27)S)

Router uptime is 10 minutes
System returned to ROM by power-on
Running default software

cisco C10720 (R5000) processor (revision 0xFF) with 507904K/16384K bytes of memory.
R527x CPU at 200Mhz, Implementation 40, Rev 10.0
Last reset from power-on
Toaster processor tmc0 is running.
Toaster processor tmc1 is running.
1 one-port OC48 SONET based SRP controller.
1 24 Port 100 Mbps Fast Ethernet TX controller.
24 FastEthernet/IEEE 802.3 interface(s)
1 SRP network interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512KB).
49152K bytes of Flash internal SIMM (Sector size 512KB).
Configuration register is 0x2102
```

Removing and Installing the AC or Dual DC Power Supply

The following sections provide information for removing, installing, and troubleshooting the AC or DC dual power supply:

- Safety, page 5-34
- Required Tools and Equipment, page 5-35
- Removing an AC or Dual DC Power Supply, page 5-35
- Installing an AC or Dual DC Power Supply, page 5-42
- Verifying AC or Dual DC Power Supply Functionality, page 5-46

Safety

Before replacing the power supply, refer to the "Safety Recommendations" section in the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication.

The router must be used with the power supply originally shipped with the router from the factory and within its marked electrical ratings.

Caution This router is equipped with a dual power supply. Ensure that both power supply connections are disconnected before beginning any procedure.

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

Warning **Before working on a system that has an on/off switch, switch OFF the power and unplug the power cord.** Statement 1

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

Required Tools and Equipment

You will need the following tools and equipment to replace an AC or DC power supply:

- ESD-preventive strap
- Number 1 Phillips screwdriver
- Antistatic bag (optional)
- Replacement AC or DC dual power supply (See Figure 1-6 and Figure 1-7.)

Removing an AC or Dual DC Power Supply

To remove the power supply, perform the following steps:

Step 1 Remove the cable-management cover if it is installed on the router to access the power switch. (See the "Removing and Installing the Cable-Management System" section on page 5-68.)

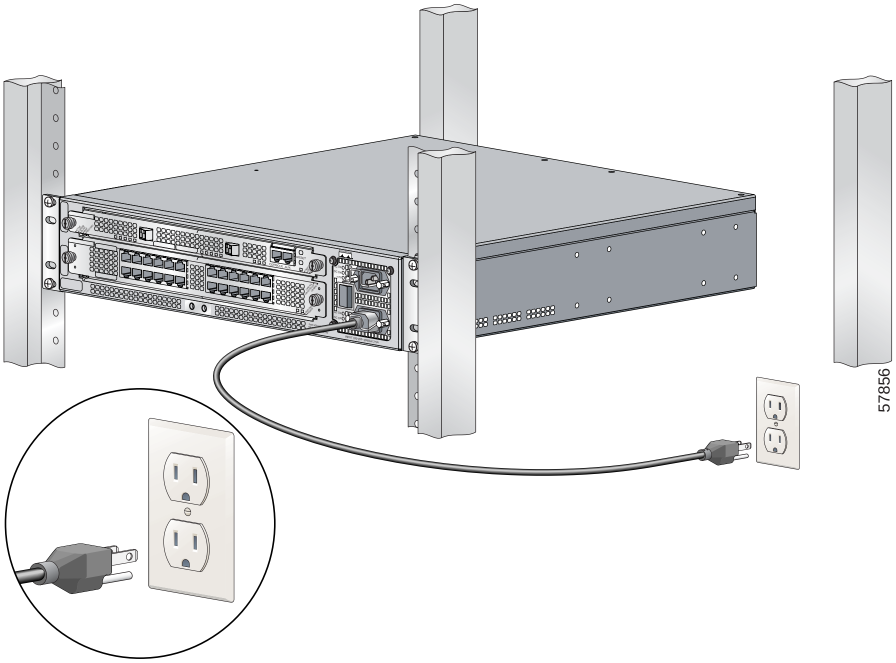
Step 2 Power down the router. (See the "Disconnecting Power from the Router" section on page 5-3.)

Warning **Before performing any maintenance on this router or its components, unplug the power cord on AC units.** Statement 246

Step 3 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Note To disconnect a DC power supply, proceed to Step 5.

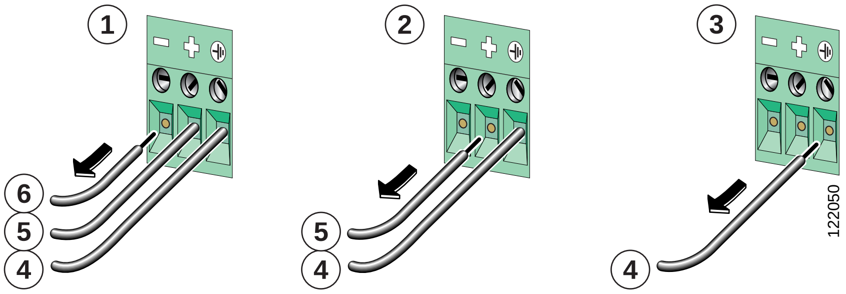
Figure 5-35 Removing Router from the Power Source



Step 4 For an AC power supply, disconnect the power source by removing the AC power cord from the wall plug. (See Figure 5-35.)

Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.** Statement 140

Figure 5-36 Removing the Dual DC Power Leads from the Terminal Block



1	Negative lead disconnected	**4**	Ground lead
2	Positive lead disconnected	**5**	Positive lead
3	Ground lead disconnected	**6**	Negative lead

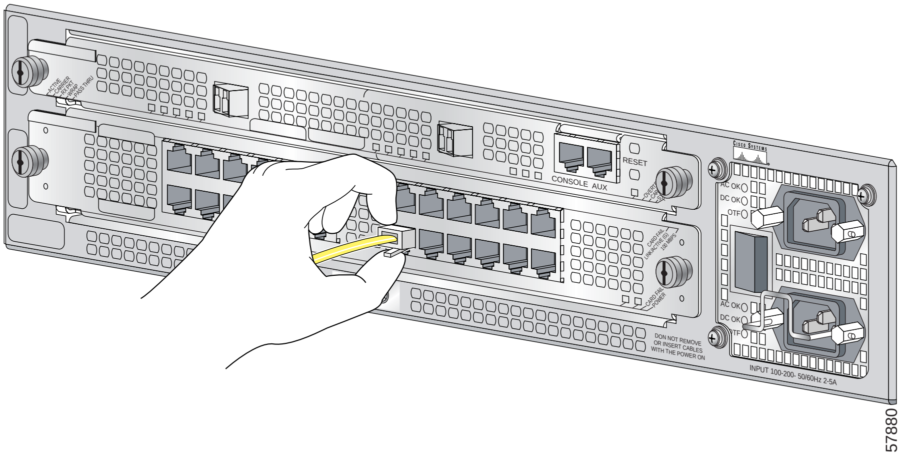
Step 5 Loosen the three locking screws for the negative, positive, and ground connectors on the DC power supply terminal block. (See Figure 5-36.)

a. Remove the –48 VDC wire (black wire) from the terminal block negative connector (–).

b. Remove the +48 VDC wire (white wire) from the terminal block positive connector (+).

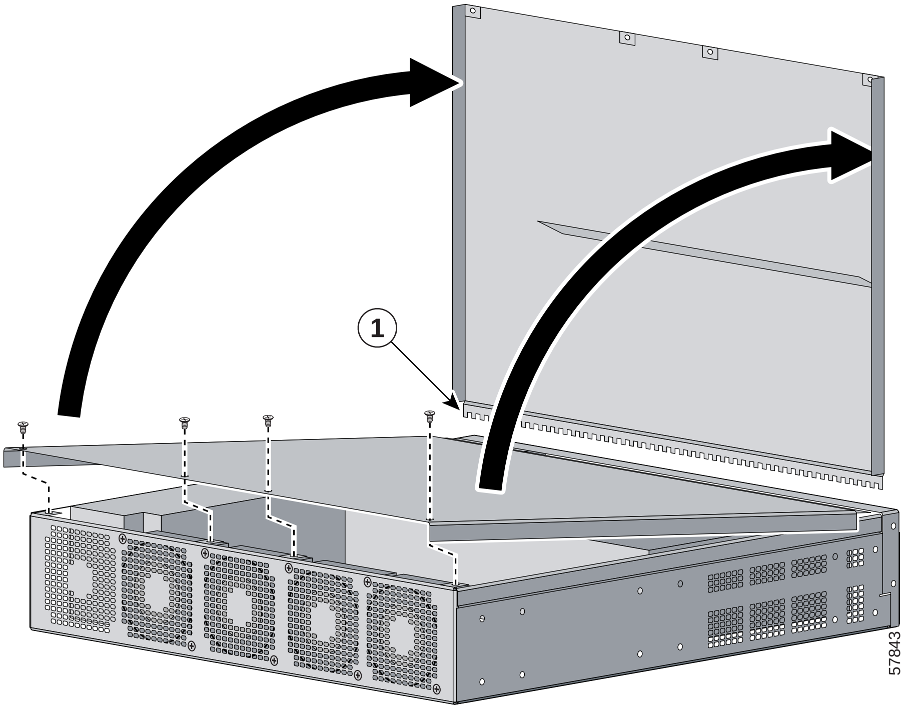
c. Remove the safety ground (green wire) from the terminal block ground connector.

Figure 5-37 Removing the Interface Cables



Step 6 Remove all interface cables from the uplink and access cards. (See Figure 5-37.)

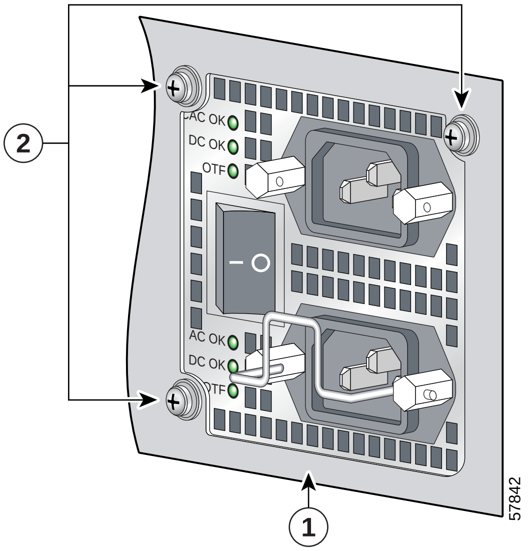
Figure 5-38 Opening the Cover



Step 7 Place the router so that the back panel is in front of you. (See Figure 5-38.)

Step 8 Unscrew the four screws that secure the cover to the router using a Number 1 Phillips screwdriver and remove the chassis cover.

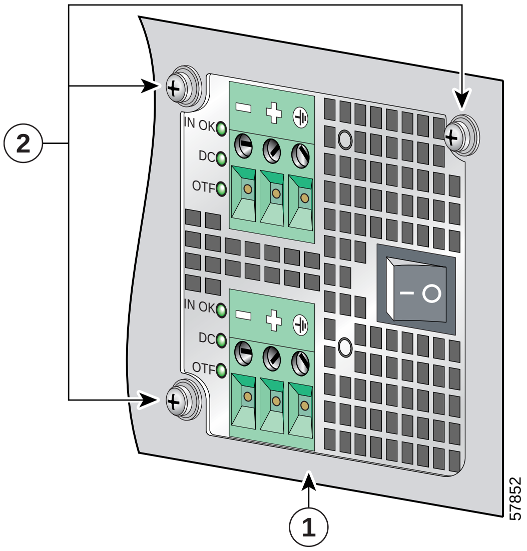
Figure 5-39 AC Power Supply Mounting Screws



1	AC power supply unit	**2**	Power supply mounting screws

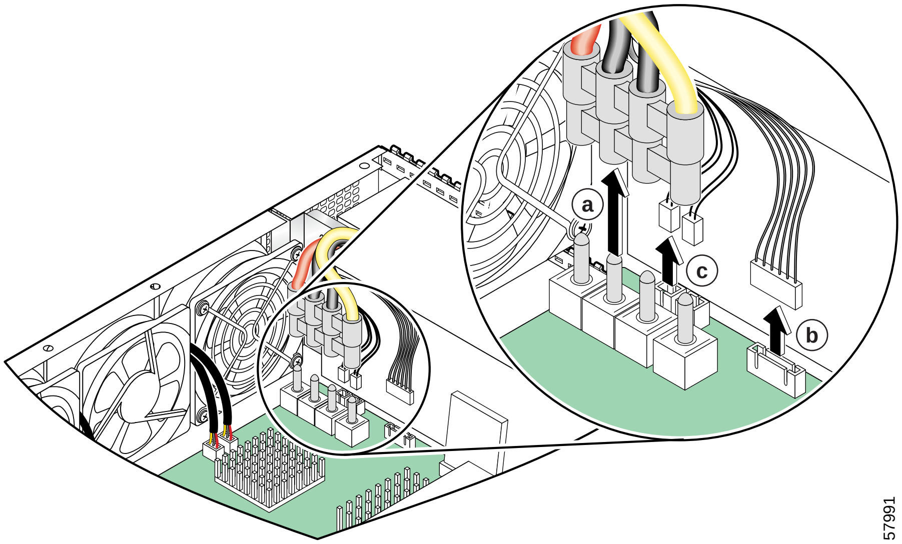
Step 9 Using a Number 1 Phillips screwdriver, remove the three mounting screws that secure the power supply to the router. (See Figure 5-39 for the AC power supply and Figure 5-40 for the Dual DC power supply.)

Figure 5-40 Dual DC Power Supply Mounting Screws



1	DC power supply unit	2	Power supply mounting screws

Figure 5-41 Disconnecting the Power Connectors from the Main Board



a	4-jack harness	c	2-pin +/–12V connector
b	6-pin connector		

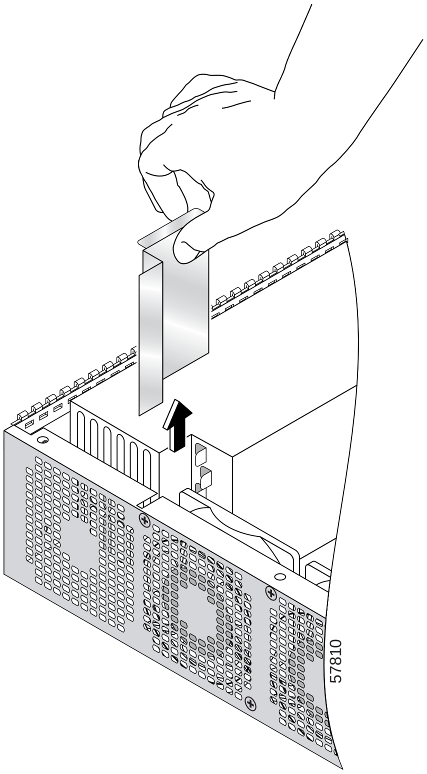
Step 10 Disconnect the following power connectors from the main board: (See Figure 5-41.)

a. 4-jack harness

b. 6-pin connector

c. 2-pin +/–12V connector

Figure 5-42 Removing the Air Baffle Separator

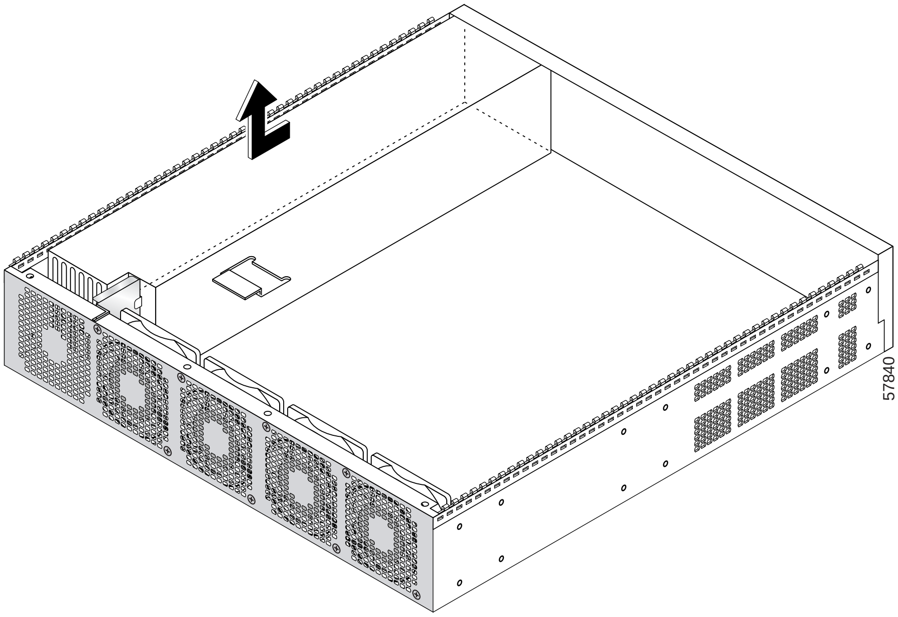


Step 11 Lift the air baffle separator out of the chassis. (See Figure 5-42.)

Step 12 Place the 4-jack harness behind the power supply before lifting it out.

Note Avoid disturbing the fan assembly by placing the 4-jack harness behind the power supply after it is removed from the main board. Do this before lifting the power supply from the router chassis.

Figure 5-43 Lifting the Power Supply Out of the Router



Step 13 Slide the power supply away from the front panel to disengage the power supply hook from the router hook and remove the power supply from the router. (See Figure 5-43.)

Step 14 After removing the power supply, replace the cover until you are ready to install a new power supply. This will prevent damage to the main board and other components while the router is out of service. (See the "Removing and Installing the Router Chassis Cover" section on page 5-13.)

Installing an AC or Dual DC Power Supply

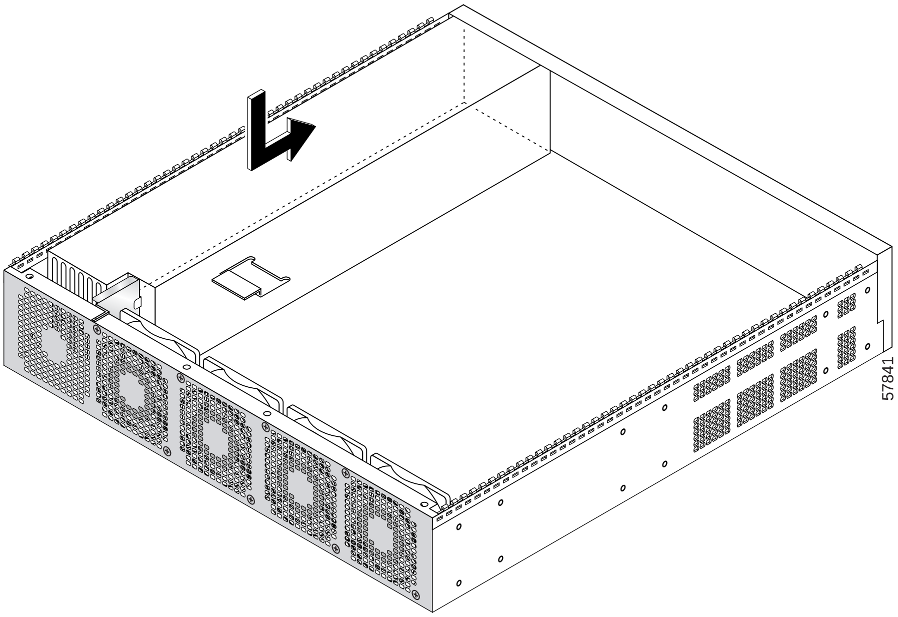
Caution Only install the same type of AC or DC power supply that was originally installed in the Cisco 10720 Internet Router that was shipped to you from Cisco. Installing a different type of power supply (AC or DC) than was originally installed in the router is not supported.

Note The minimum wire gauge size supported on the DC dual power supply is 17 American Wire Gauge (AWG), which has a 1.5mm wire diameter. The maximum wire gauge size supported on the DC dual power supply is 10 AWG, which has a 6mm wire diameter.

Perform the following steps to install an AC or DC dual power supply:

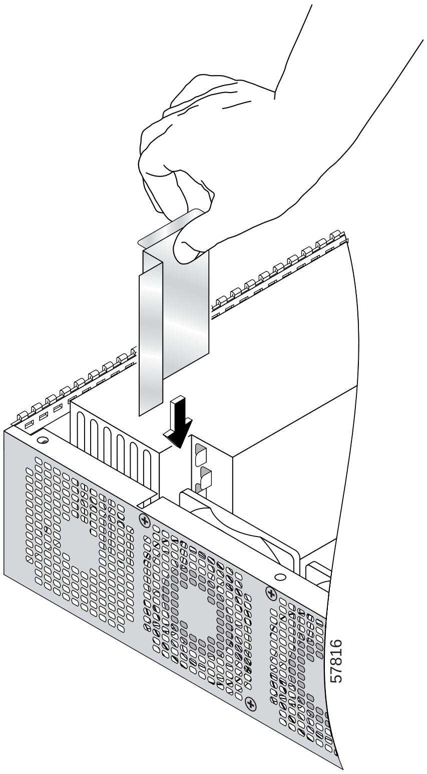
Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. See the "Preventing Electrostatic Discharge" section on page 2-3.

Figure 5-44 Inserting the Power Supply in the Router



Step 2 Place the power supply into the router and slide it toward the front panel. (See Figure 5-44.) You should feel the hook engage.

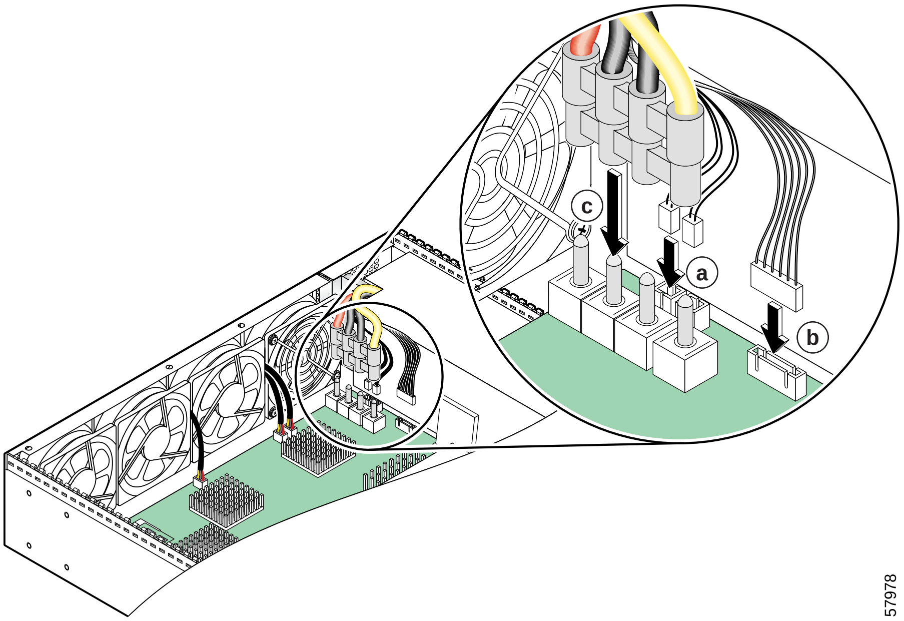
Figure 5-45 Installing the Air Baffle Separator



Step 3 Replace the air baffle separator in the router. (See Figure 5-45.)

Caution Observe the proper keying of the DC output connector to the back panel connector. Exerting force on the connector can damage the router.

Figure 5-46 Connecting the Power Connectors to the Main Board



a	2-pin +/–12V connector	**c**	4-jack harness
b	6-pin connector		

Step 4 Reconnect the following power connectors to the main board: (See Figure 5-46.)

a. 2-pin +/–12V connectors

b. 6-pin connector

c. 4-jack harness

Step 5 Turn the router so that you face the rear panel, and then reinstall the three mounting screws. (See Figure 5-39 for the AC power supply and Figure 5-40 for the DC power supply.)

Step 6 Replace the router cover. (See the "Removing and Installing the Router Chassis Cover" section on page 5-13.)

To connect the AC power supply, go to Step 8. To connect the DC power supply, go to Step 7.

Step 7 Connect the DC power supply in the following order:

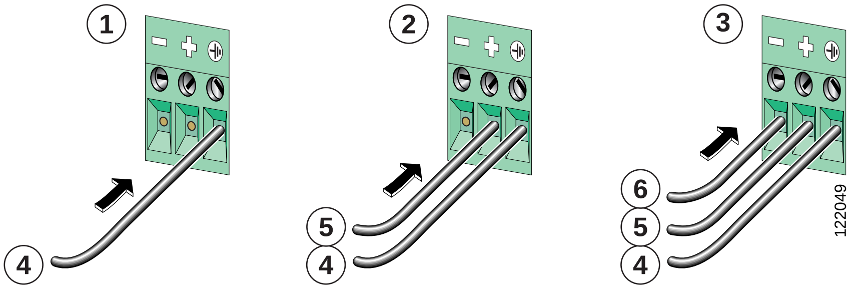
a. Insert the safety ground (green wire) into the terminal block ground connector and tighten the locking screw. Ensure that no bare wire is exposed. (See Figure 5-47.)

b. Insert the +48 VDC wire (white wire) into the terminal block positive connector (+) and tighten the locking screw. Ensure that no bare wire is exposed. (See Figure 5-47.)

c. Insert the –48 VDC wire (black wire) into the terminal block negative connector (–) and tighten the locking screw. Ensure that no bare wire is exposed. (See Figure 5-47.)

Note Verify that the power supply leads are secured with a cable tie on the DC power supply.

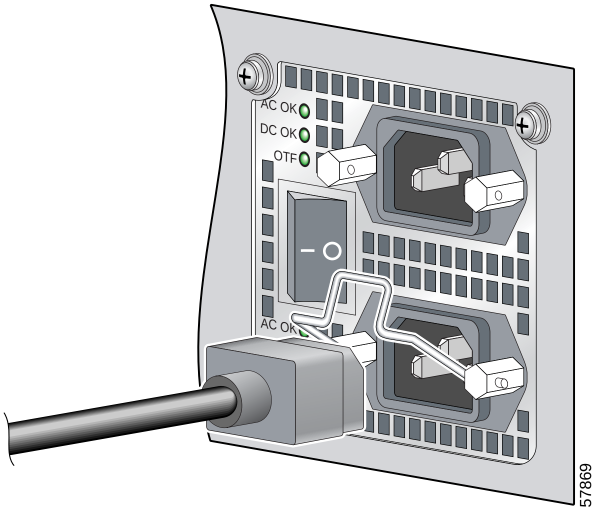
Figure 5-47 Connecting the DC Power Leads to the Terminal Block



1	Ground lead connected	**4**	Ground lead
2	Positive lead connected	**5**	Positive lead
3	Negative lead connected	**6**	Negative lead

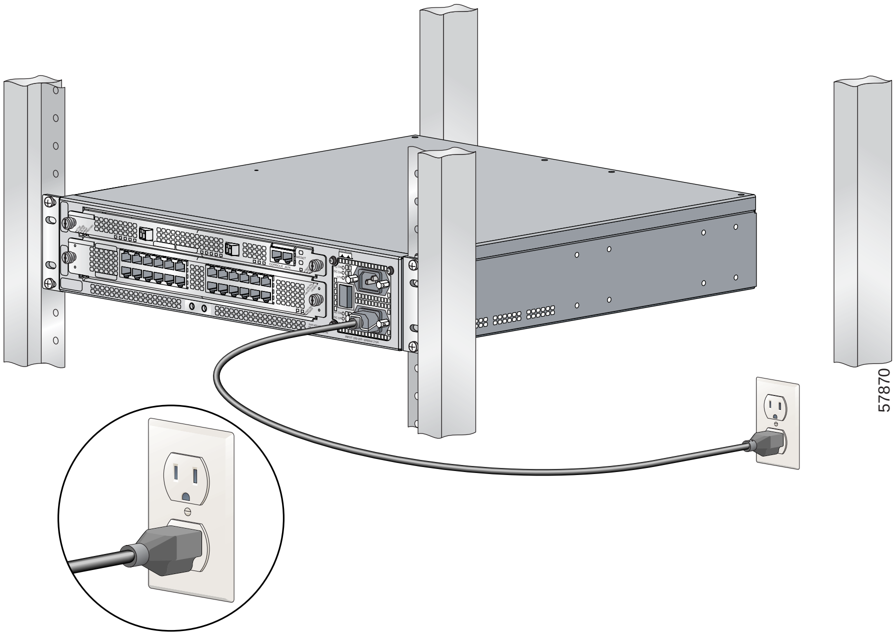
Warning **After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.** Statement 8

Figure 5-48 Attaching the AC Power Cord to the Router



Step 8 Connect the AC power supply by connecting the AC power cord. (See Figure 5-48.)

Figure 5-49 Connecting the Router to the Power Source



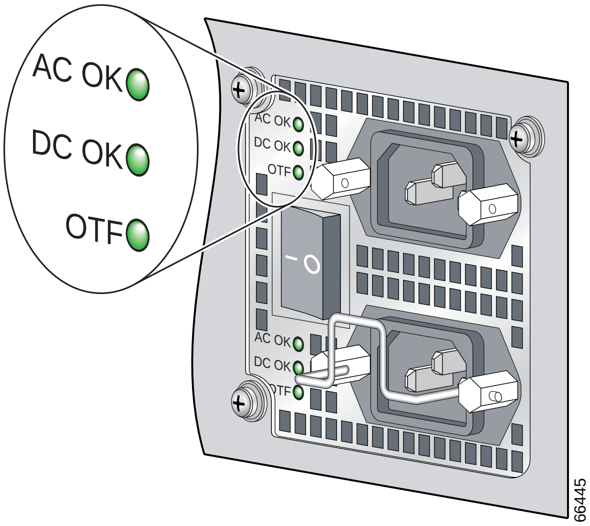
Step 9 Connect the router to the main power source. (See Figure 5-49.)

Step 10 Power up (–) the router. (See the "Connecting Power to the Router" section on page 5-7.)

Verifying AC or Dual DC Power Supply Functionality

The internal power supply fan should power on when power is restored to the router. Six green LEDs on the front of the power supply should be active. If one LED is not actively lit, consult the appropriate redundant power supply LED status messages in Table 5-1 for AC power supply status LEDs and Table 5-2 for DC power supply status LEDs . (See Figure 5-50 for AC power supply status LEDs and Figure 5-51 for DC power supply status LEDs.)

Figure 5-50 AC Power Supply LEDs

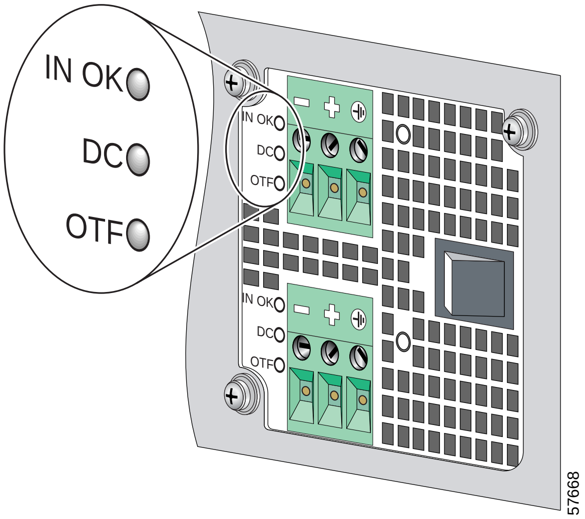


The AC power supply LEDS provide status information. (See Table 5-1.)

Table 5-1 AC Power Supply Status LEDs

LED	Activity	Description
AC OK	Solid Green	The AC input voltages to both individual power supplies are within acceptable limits.
	Off	Power is off.
DC OK	Solid Green	Both individual power supplies are functioning normally.
	Off	Power is off.
OTF (Over Temp Failure)	Amber/Red	As a lamp test at power up, this LED comes up amber/red for approximately half a second. OR The power system overheated or one of the internal fans failed.
	Solid Green	The temperature of the corresponding individual power supply is within acceptable limits. (That is, the temperature is normal.)
	Off	Power is off.

Figure 5-51 Dual DC Power Supply LEDs



The dual DC power supply status LEDs provide status information. (See Table 5-2.)

Table 5-2 Dual DC Power Supply Status LEDs

LED	Activity	Description
IN OK	Green	The DC input voltages to both individual power supplies are within acceptable limits.
	Off	Power is off.
DC	Green	Both individual power supplies are functioning normally.
	Off	Power is off.
OTF (Over Temp Failure)	Amber/Red	As a lamp test at power up, this LED comes up amber/red for approximately half a second. OR The power system overheated or one of the internal fans failed.
	Green	The temperature of the corresponding individual power supply is within acceptable limits. (That is, the temperature is normal.)
	Off	Power is off.

Removing and Installing an Uplink Card

The following sections present information and procedures for removing and installing an uplink card in the Cisco 10720 Internet Router:

- Safety, page 5-49
- Required Tools and Equipment, page 5-49
- Removing an Uplink Card, page 5-50
- Installing an Uplink Card, page 5-55
- Verifying Uplink Card Functionality, page 5-57
- Troubleshooting the Uplink Card Functionality, page 5-57

Safety

Confirm that your ESD-preventive strap is properly set up before handling the uplink card. You must use your hands to remove this card by grasping the spring-loaded screws. For more information, see the "Preventing Electrostatic Discharge" section on page 2-3.

⚠ **Caution** Any attempt to remove the card from its slot by any other method than described in these procedures can damage the uplink card, access card, midplane card, or router chassis.

⚠ **Warning** **Class 1 laser product.** Statement 1008

⚠ **Warning** **Class 1 LED product.** Statement 1027

Required Tools and Equipment

You will need the following tools and equipment:

- ESD-preventive strap
- Number 1 Phillips screwdriver
- Cable ties
- 1/8-inch flat-blade screwdriver
- Replacement uplink card

Removing an Uplink Card

To remove the uplink card from the router, perform the following steps:

Step 1 If the cable-management cover is installed on the router, it must be removed in order to access the power switch and uplink card. (See the "Removing and Installing the Cable-Management System" section on page 5-68.)

Step 2 Power down the router. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 3 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Removing an SFP

The RPR/SRP uplink card uses SFP modules. If your uplink card does not use SFP modules, follow Step 1 and Step 2, and then go to Step 6.

Warning **Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.** Statement 125

Warning **Class 1 laser product.** Statement 1008

Warning **Class 1 LED product.** Statement 1027

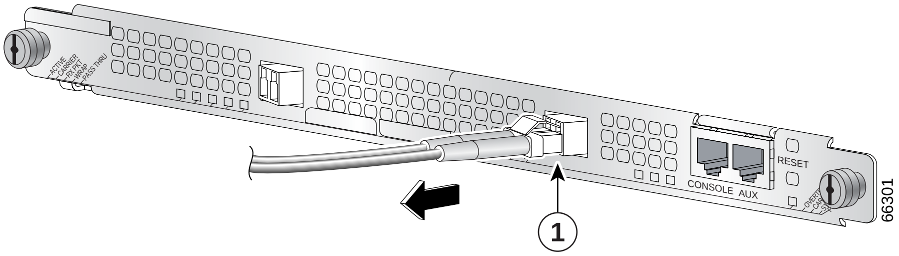
Note You do not need to power down the router before you remove an SFP module. The router may remain powered up during this procedure.

Removing a Bale Clasp SFP

To remove a bale clasp SFP module from the access card, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

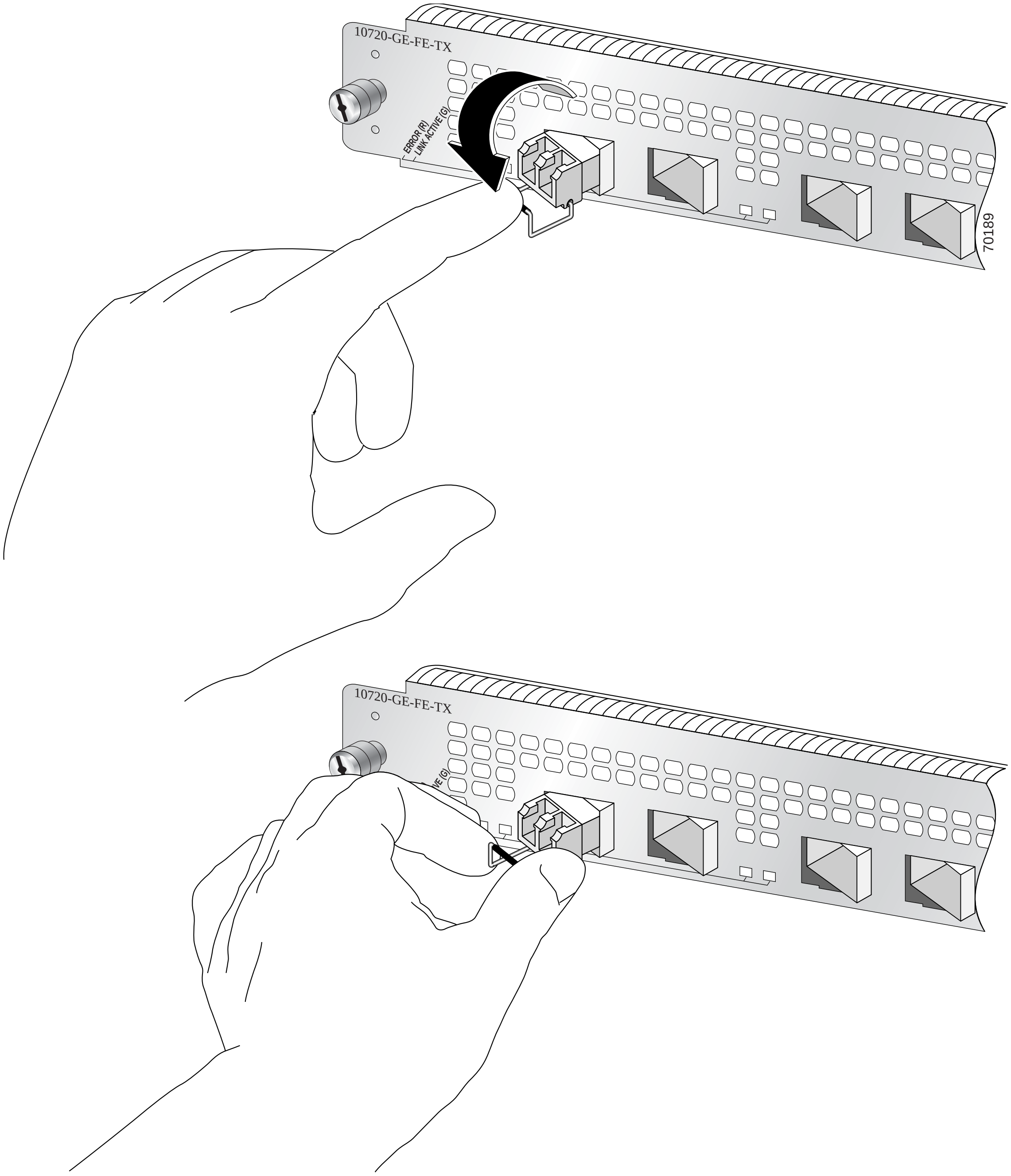
Figure 5-52 Optical Interface Cable



1	Optical interface cable connector		

Step 2 Remove all optical interface cables from the card if the card has optical interface ports. (See Figure 5-52.)

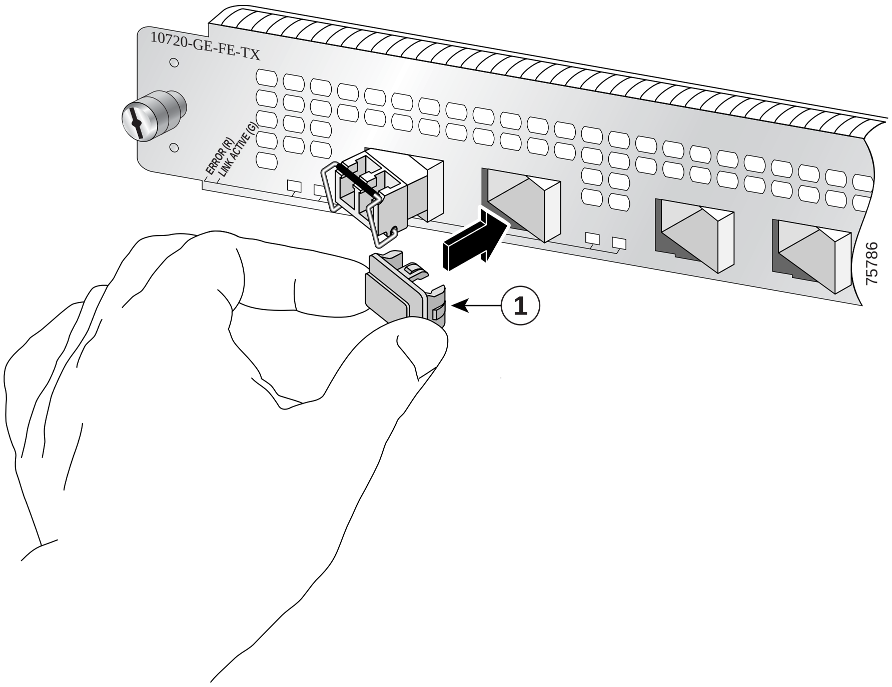
Figure 5-53 Removing a Bale Clasp SFP Module



Step 3 Open the bale clasp on the SFP module by pressing the clasp downward until it is in a horizontal position as shown in Figure 5-53.

Step 4 Grasp the SFP module by the bale clasp and gently pull it out of the Gigabit Ethernet slot as shown in Figure 5-53.

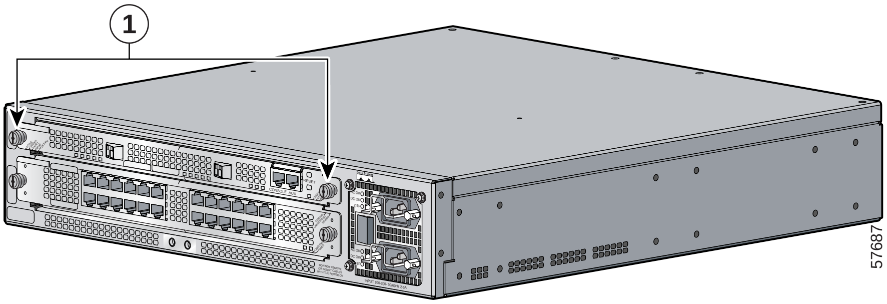
Figure 5-54 Installing an SFP Cage Cover



1	SFP cage cover		

Step 5 Protect your uplink card by inserting clean SFP cage covers into the SFP cage when there is no SFP installed, as shown in Figure 5-54.

Figure 5-55 Spring-Loaded Screws on the Uplink Card



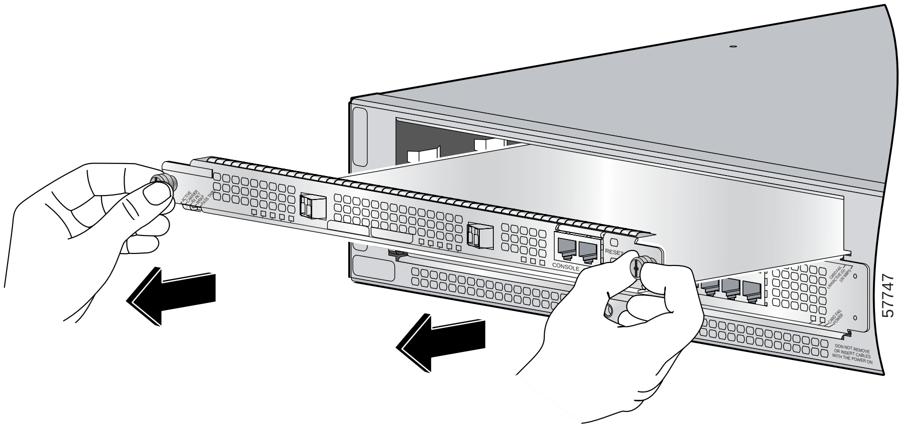
1	Uplink card spring-loaded screws		

Step 6 Locate the spring-loaded screws on the front of the uplink card (card located in the upper card slot). (See Figure 5-55.)

Step 7 Using the Number 1 Phillips screwdriver, unfasten the spring-loaded screws by turning them counterclockwise.

Step 8 Grasp the spring-loaded screws and using your hold on the screws, gently move the card back and forth until it disengages from the midplane.

Figure 5-56 Removing Uplink Card from the Router Chassis



Step 9 When the uplink card disengages from the midplane, pull the card straight out of the router. (See Figure 5-56.)

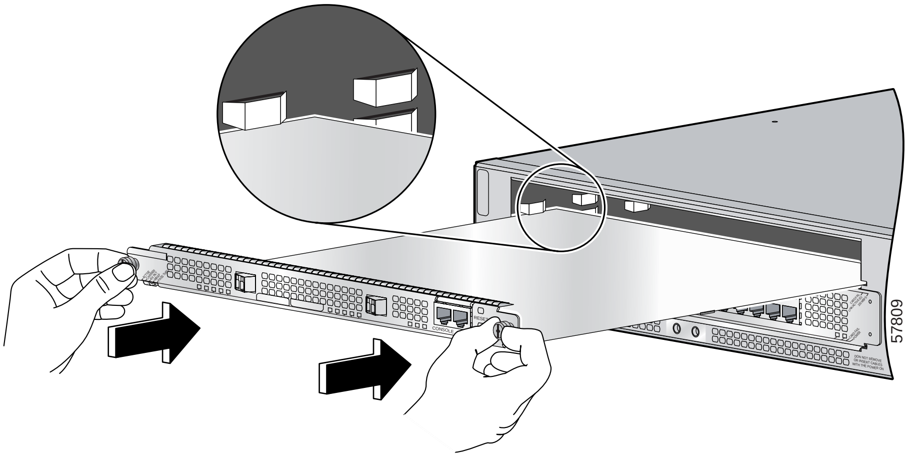
Installing an Uplink Card

To install an uplink card, perform the following steps:

Step 1 Confirm that the router is powered down before installing the uplink card. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 2 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Figure 5-57 Sliding Uplink Card into Router Chassis



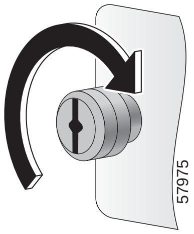
Step 3 Grasp the card and use the uplink card slot guides to insert the card into the router.

Step 4 Using your hold on the spring-loaded screws located on the front of the uplink card, insert the card into the upper card slot of the router chassis. (See Figure 5-57.)

Caution Do not force the card into the slot. Exerting too much force on the card can damage the card or the router.

Step 5 Gently slide the card into the router chassis until the card seats into the midplane.

Figure 5-58 Turning Spring-Loaded Screws Clockwise



Step 6 Using a 1/8-inch flat-blade screwdriver, tighten the spring-loaded screws by turning them clockwise until the card is completely secure. (See Figure 5-58.)

Installing the OC48 SFP Modules in the RPR/SRP Uplink Card

Use the information in this section to install OC48 SFP modules in the RPR/SRP uplink card.

Note Use only OC48 SFP modules purchased from Cisco Systems.

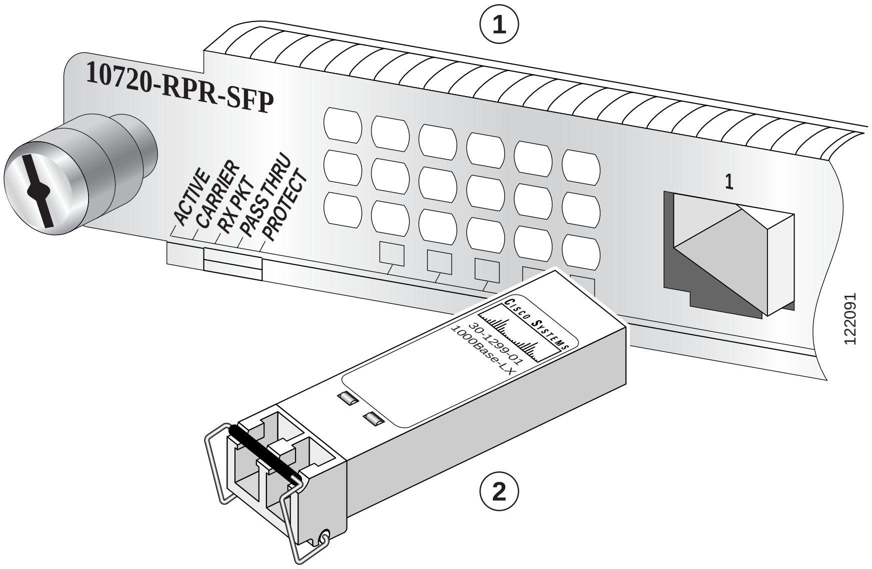
To install a bale clasp OC48 SFP module in the uplink card, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Hold the SFP module with the hardware label facing up, as illustrated in Figure 5-1.

Caution The SFP module must be inserted with the hardware label facing up to avoid damaging the SFP module or uplink card.

Figure 5-59 Installing the Bale Clasp SFP Module in the RPR/SRP Uplink Card



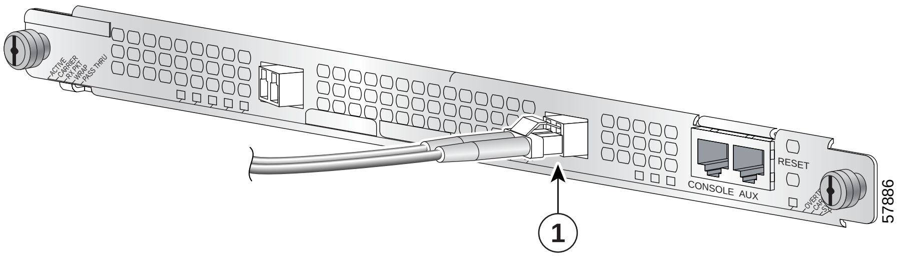
1	RPR/SRP uplink card	2	OC48 SFP module

Step 3 Close the bale clasp on the SFP module by pushing the clasp in the upward direction before inserting the SFP module.

Step 4 Insert the SFP into the appropriate OC48 port and gently push on it until the SFP module snaps into the slot. (See Figure 5-59.)

Connecting the Optical Cables

Figure 5-60 Connecting the Optical Cable to the Router



1	Optical cable connector		

Step 1 Before connecting the optical fiber cables, clean the cable connection as well as the optical connection in the router. See the *Inspection and Cleaning Procedures for Fiber-Optic Connections* document.

Step 2 Connect the optical interface cables to the uplink card if the card has optical interface ports. (See Figure 5-60.)

Verifying Uplink Card Functionality

You can verify that the uplink card is functioning by checking the LEDs located on the front panel of the uplink card. For a complete description of the uplink card LEDs, see the "Verifying the Cisco 10720 Internet Router LEDs" section on page 3-33. Also, refer to the *Cisco 10720 Internet Router Uplink Card Installation and Configuration* publication.

Troubleshooting the Uplink Card Functionality

The following tips will help you troubleshoot the functionality of the uplink card:

- Verify the LED status.
- Ensure that the card is fully seated against the midplane.
- Verify that all cables are connected properly.
- Check that the power switch is turned to the on position.
- Confirm that the power supply connection is secure.

Removing and Installing an Access Card

The following sections present information and procedures for removing and installing an access card in the Cisco 10720 Internet Router:

- Safety, page 5-58
- Required Tools and Equipment, page 5-58
- Removing an SFP, page 5-58
- Installing an Access Card, page 5-64
- Verifying Access Card Functionality, page 5-67
- Troubleshooting the Access Card Functionality, page 5-67

Safety

Confirm that your ESD-preventive strap is properly set up before handling the access card. You must use your hands to remove this card by grasping the spring-loaded screws. For more information, see the "Preventing Electrostatic Discharge" section on page 2-3.

Caution Any attempt to remove the card from its slot by any other method than described in these procedures can damage the access card, midplane card, or router chassis.

Required Tools and Equipment

You will need the following tools and equipment:

- ESD-preventive strap
- Number 1 Phillips screwdriver
- Cable ties
- 1/8-inch flat-blade screwdriver
- Replacement access card

Removing an SFP

To remove SFPs, perform the following steps:

Step 1 Remove the cable-management cover if it is installed on the router, to access the power switch and access card. (See the "Removing and Installing the Cable-Management System" section on page 5-68.)

Step 2 Power down the router. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 3 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 4 Remove all Ethernet interface cables from the access card. (See Figure 5-37.)

Warning **Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.** Statement 125

Warning **Class 1 laser product.** Statement 1008

Warning **Class 1 LED product.** Statement 1027

The procedure for removing a small form-factor pluggable (SFP) module is described in the following sections:

- Removing a Bale Clasp SFP, page 5-51
- Removing a Latch SFP, page 5-61

Note You do not need to power down the router before you remove an SFP module. The router may remain powered up during this procedure.

Removing a Bale Clasp SFP

To remove a bale clasp SFP module from the access card, perform the following steps:

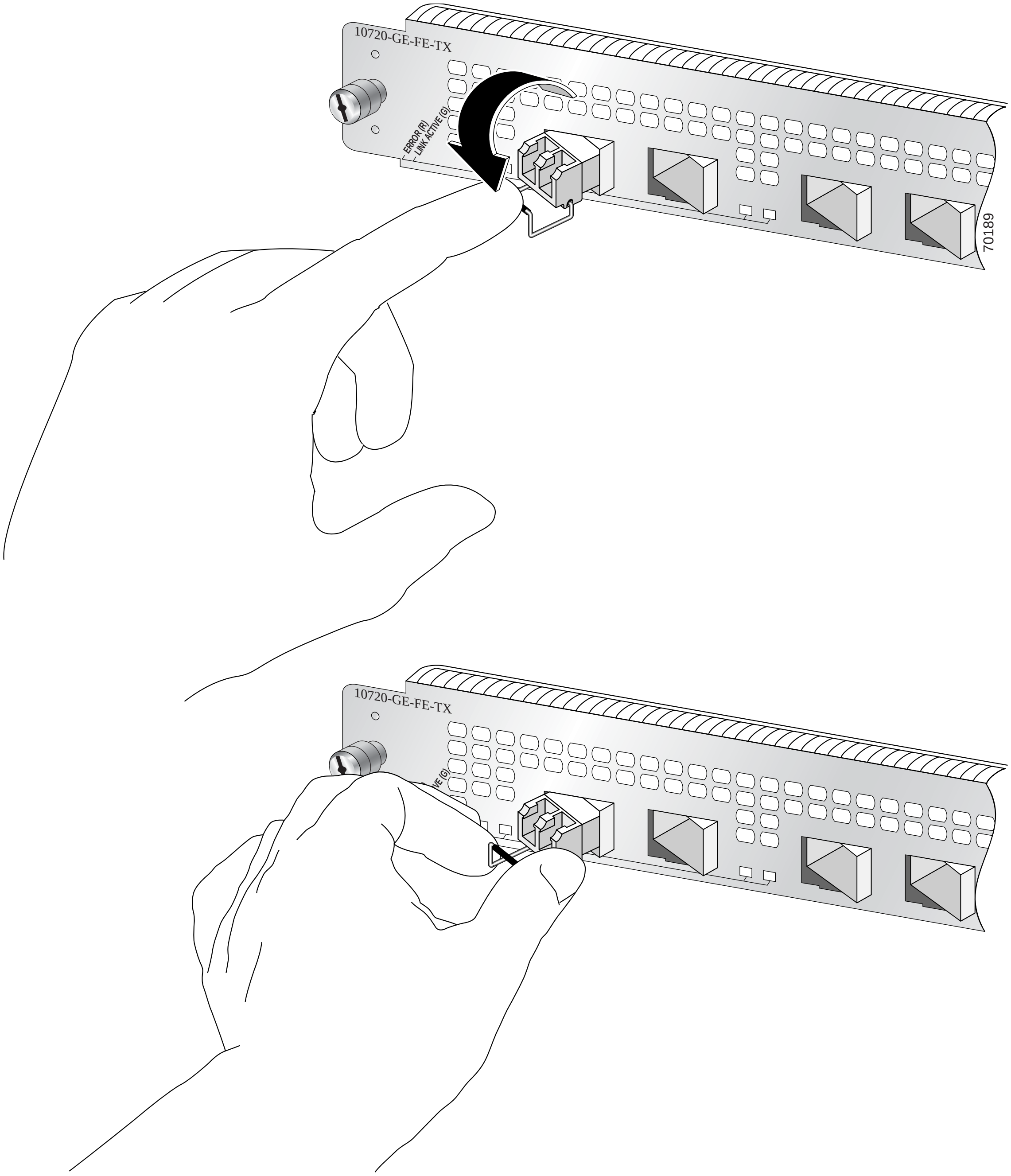
Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Remove all optical interface cables from the SFP Gigabit Ethernet port. (See Figure 5-52.)

Step 3 Open the bale clasp on the SFP module by pressing the clasp downward until it is in a horizontal position as shown in Figure 5-53.

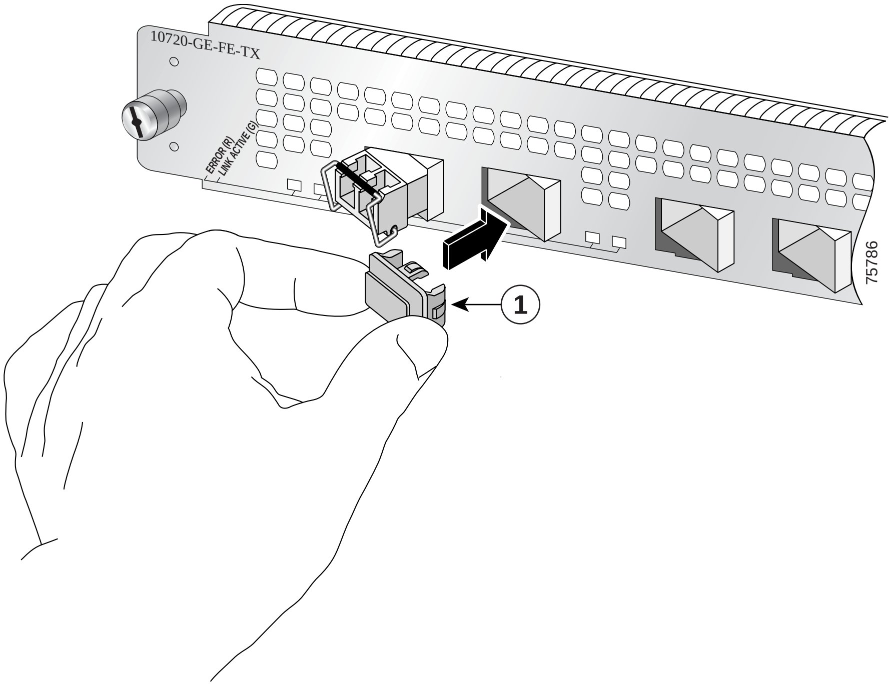
Step 4 Grasp the SFP module by the bale clasp and gently pull it out of the Gigabit Ethernet slot as shown in Figure 5-53.

Figure 61 Removing a Bale Clasp SFP Module



Step 5 Protect your access card by inserting clean SFP cage covers into the SFP cage when there is no SFP installed, as shown in Chapter 5, “Maintaining the Cisco 10720 Internet Router,” Figure 5-54.

Figure 62 Installing an SFP Cage Cover



1	SFP cage cover

Removing a Latch SFP

To remove a latch SFP module from the access card, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the “Preventing Electrostatic Discharge” section on page 2-3.)

Step 2 Remove all optical interface cables from the SFP Gigabit Ethernet port. (See Figure 5-52.)

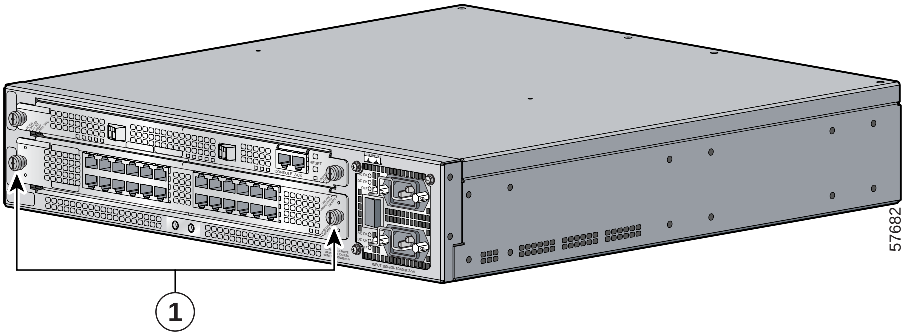
Step 3 Push the small latch on the bottom front of the SFP to release the module from the connector in the Gigabit Ethernet slot.

Step 4 Grasp the SFP module by the sides and gently pull it out of the Gigabit Ethernet slot.

Step 5 Protect your access card by inserting clean SFP cage covers into the SFP cage when there is no SFP installed, as shown in Chapter 5, “Maintaining the Cisco 10720 Internet Router,” Figure 5-54.

Removing the Access Card

Figure 5-63 Spring-Loaded Screws on the Access Card



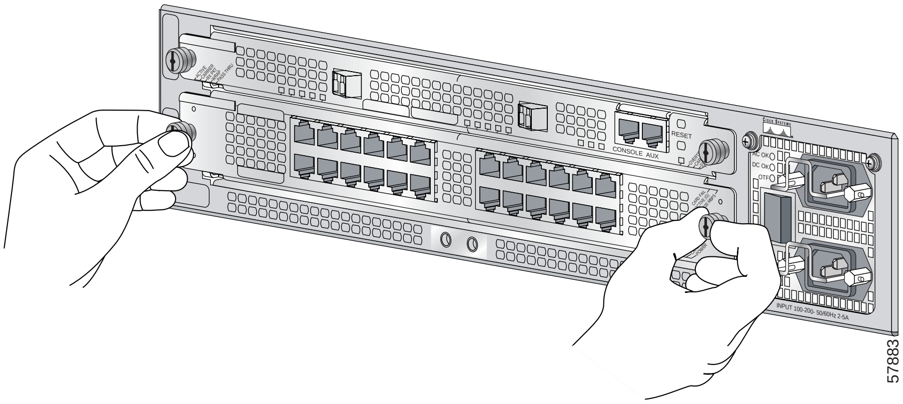
1	Access card spring-loaded screws		

Step 1 If you have not already done so, see the "Removing an SFP" section on page 5-58 and follow the instructions for removing the cable-management system, powering down the router, attaching an anti-static wriststrap, removing optical cables, and removing the SFPs.

Step 2 Locate the spring-loaded screws on the front of the access card (card located in the lower card slot). (See Figure 5-63.)

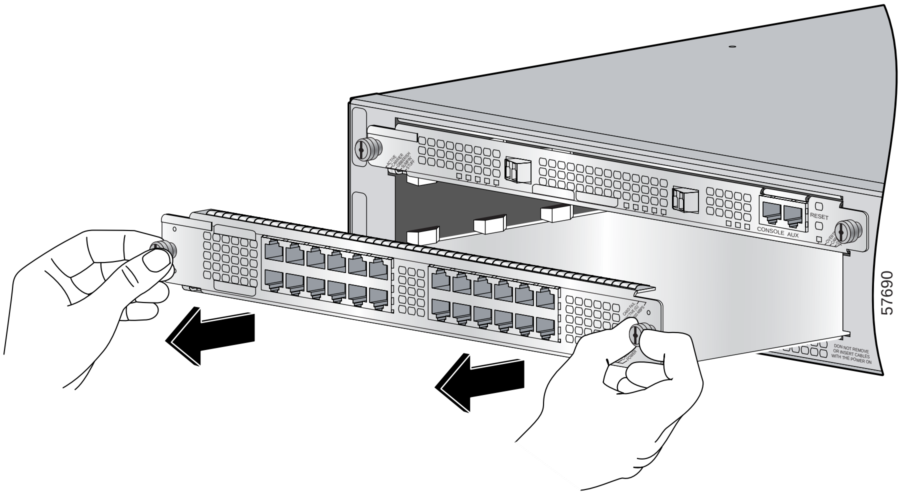
Step 3 Using a Number 1 Phillips screwdriver, unfasten the spring-loaded screws by turning them counterclockwise.

Figure 5-64 Grasping the Access Card Spring-Loaded Screws



Step 4 Remove the access card from the router by grasping the spring-loaded screws. Using your hold on the screws, gently move the access card back and forth until the card disengages from the midplane. (See Figure 5-64.)

Figure 5-65 Removing Access Card from the Router Chassis



Step 5 When the access card disengages from the midplane, pull the card straight out. (See Figure 5-65.)

Note For instructions on removing small form-factor pluggable (SFP) optical interface modules from the access card, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.

Installing an Access Card

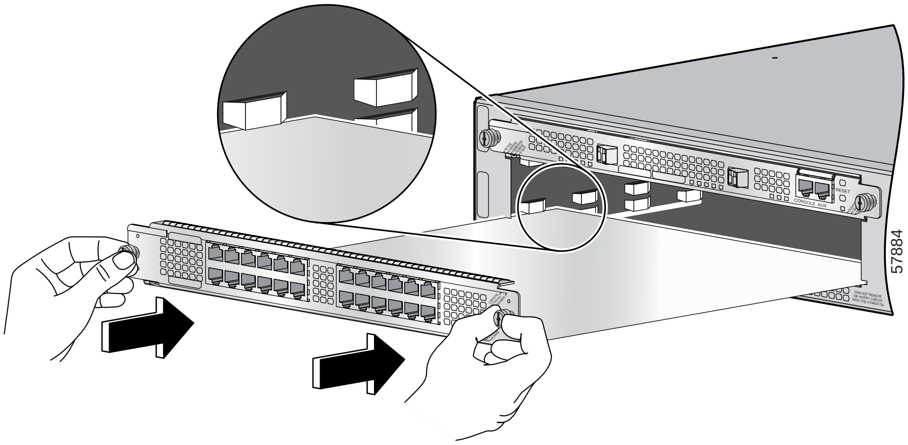
To install an access card in the router, perform the following steps:

Step 1 Verify that the router is powered down. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 2 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 3 Grasp the card and use slot guides inside the router as a guide to insert the card into the router.

Figure 5-66 Sliding Access Card into Router Chassis

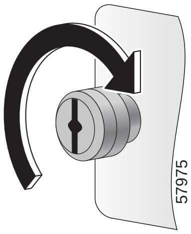


Step 4 Using your hold on the spring-loaded screws located on the front of the access card, insert the card into the lower card slot of the router chassis. (See Figure 5-66.)

⚠ **Caution** Do not force the card into the slot. Exerting too much force on the card can damage the card or the router.

Step 5 Gently slide the access card into the router chassis until the card seats into the midplane.

Figure 5-67 Turning the Spring-Loaded Captive Installation Screws Clockwise



Step 6 Using a 1/8-inch flat-blade screwdriver, tighten the spring-loaded screws by turning them clockwise until the card is completely secure.

Installing the SFP Modules on the Access Card

Use the information in this section to install Gigabit Ethernet (GE) SFP modules in the access card.

Note Use only SFP modules purchased from Cisco Systems.

Note The Cisco 10720 is a Class A product when using copper the SFP-GE-T= module in the Cisco 10720 GE-FE-TX-B= access card. The Cisco 10720 is a Class B product when using optical SFP modules in the Cisco 10720 GE-FE-TX-B= access card.

Installing a Bale Clasp GE SFP Module

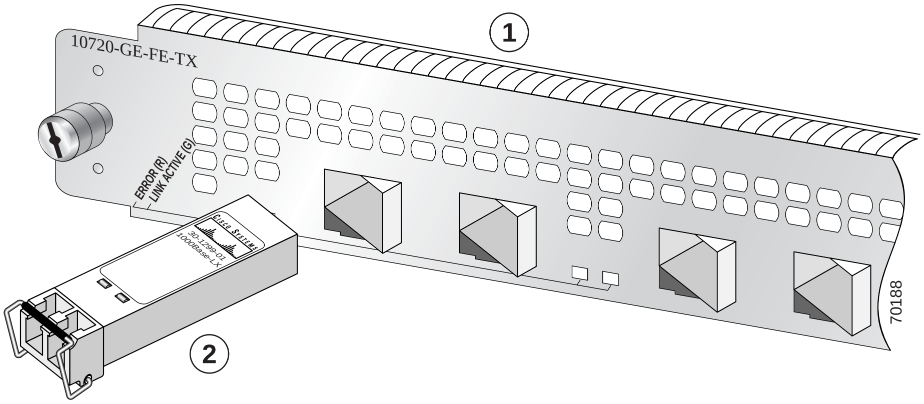
To install a bale clasp GE SFP module in the access card, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Step 2 Hold the SFP module with the hardware label facing up, as illustrated in Figure 5-1.

Caution The SFP module must be inserted with the hardware label facing up to avoid damaging the SFP module or access card.

Figure 5-68 Installing the Bale Clasp SFP Module in the Access Card



1	Access card	2	GE SFP module

Step 3 Close the bale clasp on the SFP module by pushing the clasp in the upward direction before inserting the SFP module.

Caution Close the bale lever on the SFP module prior to inserting the SFP module into the port cage to ensure proper engagement. The bale lever is considered closed when it is in the upright position. See Figure 5-59. If the bale lever is left open during insertion, there is a possibility that the SFP module may become stuck in the port cage. To remove the SFP module, use a small flathead screwdriver to gently lift the cage tongue (located underneath the SFP module) away from the SFP module body, thus disengaging the SFP module. The SFP module is not damaged by this operation.

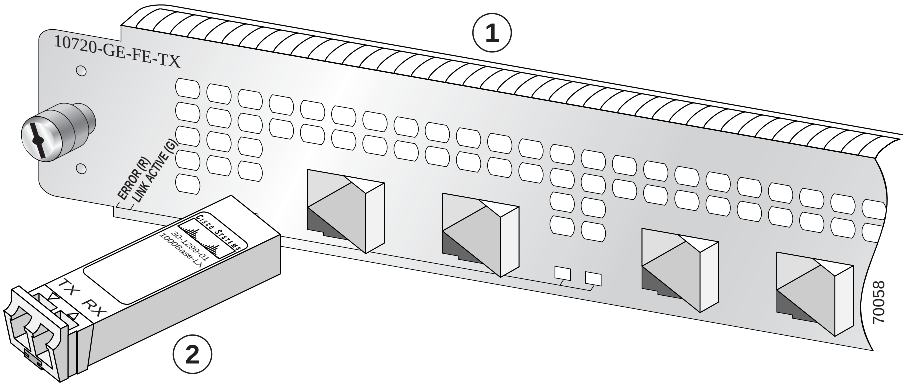
Step 4 Insert the SFP into the appropriate GE port and gently push on it until the SFP module snaps into the slot. (See Figure 5-59.)

Installing a Latch GE SFP Module

To install a latch GE SFP module in the access card, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Figure 5-69 Installing the Latch SFP Module in the Access Card



1	Access card	2	GE SFP module with latch

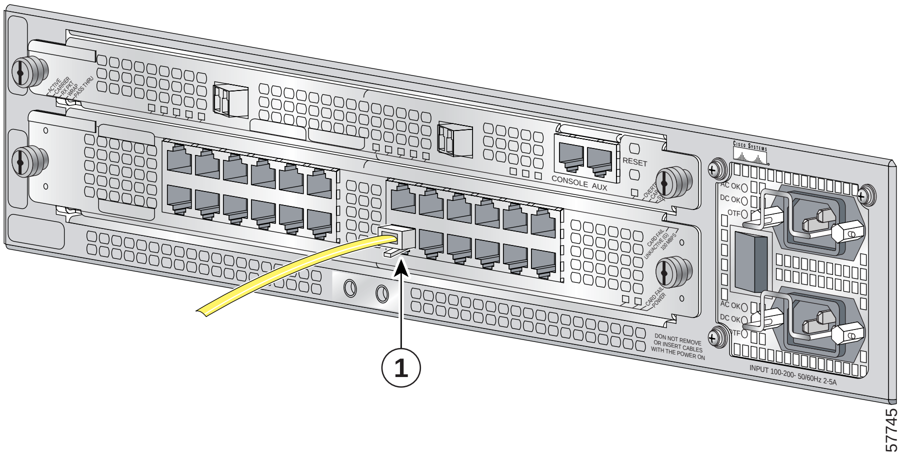
Step 2 Hold the SFP module with the hardware label facing up, as illustrated in Figure 5-69.

Caution The SFP module must be inserted with the hardware label facing up to avoid damaging the SFP module or the uplink card.

Step 3 Insert the SFP into the appropriate RPR/SRP uplink card slot and gently push on it until the module snaps into the slot tightly. (See Figure 5-69.)

Step 4 Close the latch to lock the SFP module into the slot.

Figure 5-70 Attaching the Interface Cable to the Access Card


CONSOLE
AUX
RESET
AC OK
DC OK
OTF
DON NOT REMOVE OR INSERT CABLES WITH THE POWER ON
INPUT 100-200- 50/60Hz 2-5A
1
57745

1	Interface cable connector		

Step 5 Before connecting the optical fiber cables, clean the cable connection as well as the optical connection in the router. See the *Inspection and Cleaning Procedures for Fiber-Optic Connections* document.

Step 6 Attach the appropriate interface cables to the access card. (See Figure 5-70.)

Note For additional information about SFP optical interface modules in the access card, refer to the *Cisco 10720 Access Card Installation and Configuration Guide*.

Verifying Access Card Functionality

You can verify that the access card is functioning by checking the LEDs located on the front panel of the access card. For a complete description of the access card LEDs, see the "Verifying the Cisco 10720 Internet Router LEDs" section on page 3-33. Also, refer to the *Cisco 10720 Internet Router Access Card Installation and Configuration* publication.

Troubleshooting the Access Card Functionality

The following tips will help you troubleshoot the functionality of the access card:

- Verify LED status.
- Ensure that the card is fully seated against the midplane.
- Verify that all cables are connected properly.
- Check that the power switch is turned to the on position.
- Confirm that the power supply connection is secure.

Removing and Installing the Cable-Management System

The following section provides information and procedures for removing and installing the Cisco 10720 Internet Router cable-management system:

- Safety, page 5-68
- Required Tools and Equipment, page 5-68
- Removing the Cable-Management System, page 5-68
- Installing the Cable-Management System, page 5-70

Safety

Power down the router before performing any maintenance procedure and read the following safety warnings and cautions:

⚠ **Warning** **Before working on a system that has an ON/OFF switch, switch OFF the power and unplug the power cord.** Statement 1

⚠ **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

⚠ **Caution** Excessive bending in an interface cable can degrade performance.

Required Tools and Equipment

You need the following tools and equipment:

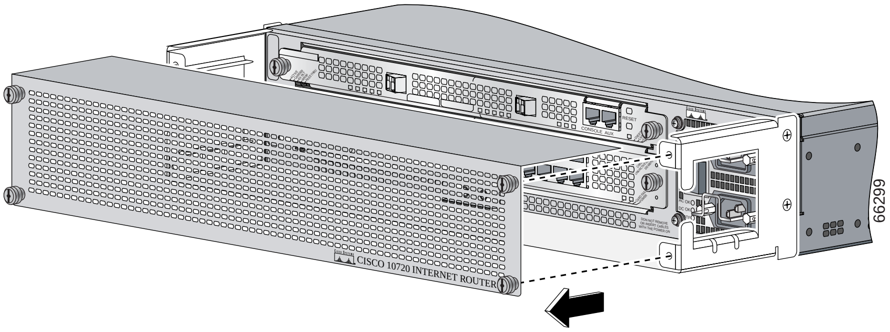
- ESD-preventive strap
- Number 1 Phillips screwdriver
- Cable ties

Removing the Cable-Management System

To remove the cable-management system, perform the following steps:

Step 1 Attach an ESD-preventive strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

Figure 5-71 Removing the Cable-Management Cover



Step 2 Verify that all cables are safely secured before detaching the cable-management cover. If the cable-management cover is not installed, go to Step 4.

Caution To avoid accidental damage to router cables or card ports, remove all cables before removing the cable-management tray.

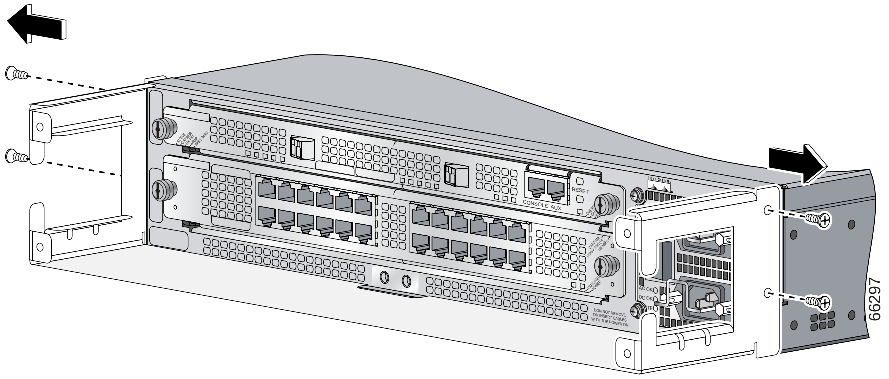
Step 3 Remove the cable-management cover from the router by removing the four screws that secure the cover to the router. (See Figure 5-72.)

Step 4 Power down the router. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 5 Remove cable ties and separate the interface cables if needed to lead the cables into the inside of the cable-management tray. (See Figure 5-75.)

Step 6 Remove all interface cables from their respective ports.

Figure 5-72 Removing the Cable-Management Tray



Step 7 Detach the cable-management tray from the router by removing the two 3.5 mm x 6 mm screws on each side of the router. (See Figure 5-72.)

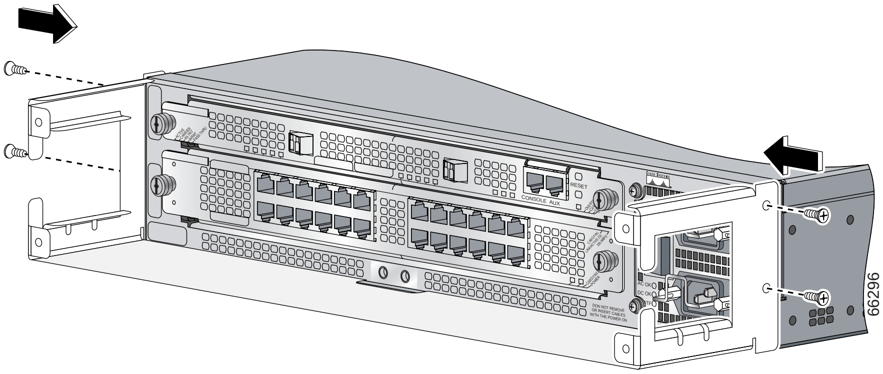
Installing the Cable-Management System

Perform the following steps to install the cable-management system:

Step 1 Power down your router. (See the "Disconnecting Power from the Router" section on page 5-3.)

Step 2 Attach an ESD-preventive wrist strap to your wrist, and to the router or to a bare metal surface. (See the "Preventing Electrostatic Discharge" section on page 2-3.)

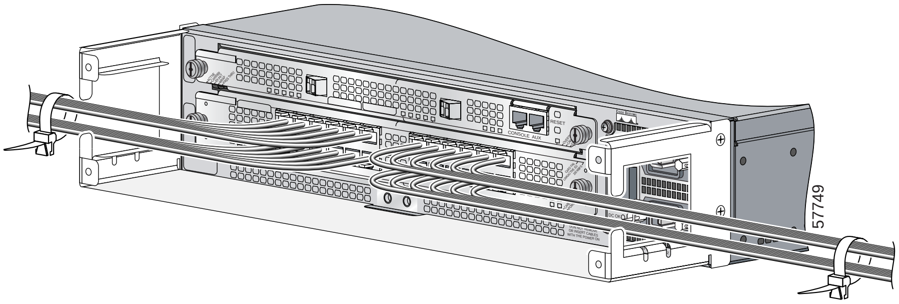
Figure 5-73 Attaching the Cable-Management Tray



Step 3 Attach the cable-management tray to the router using four of the 3.5 mm x 6 mm screws that ship with the router. Secure the tray with two screws on each side of the router chassis. (See Figure 5-73.)

Step 4 Connect all interface cables to their respective ports if necessary.

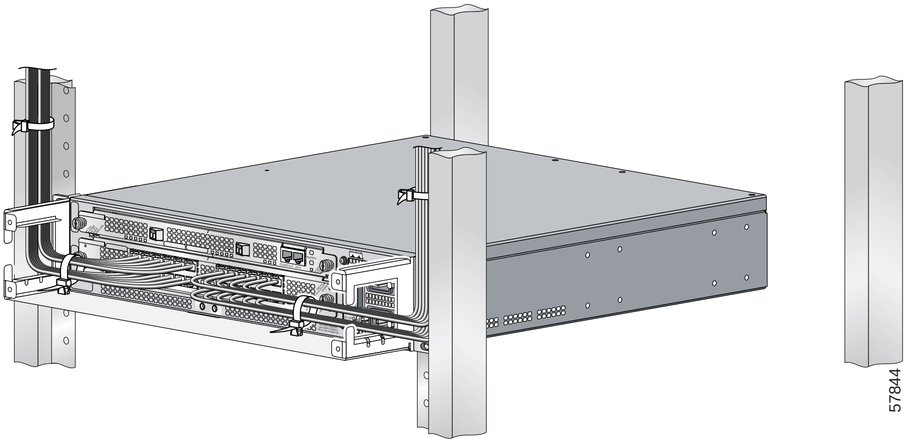
Figure 5-74 Managing Interface Cables with the Cable-Management Tray



Step 5 Separate the cables and lead them out the sides of the cable-management system. Use a cable tie to keep the cables together. (See Figure 5-74.)

Note To avoid damage to the cables, avoid excessive bending.

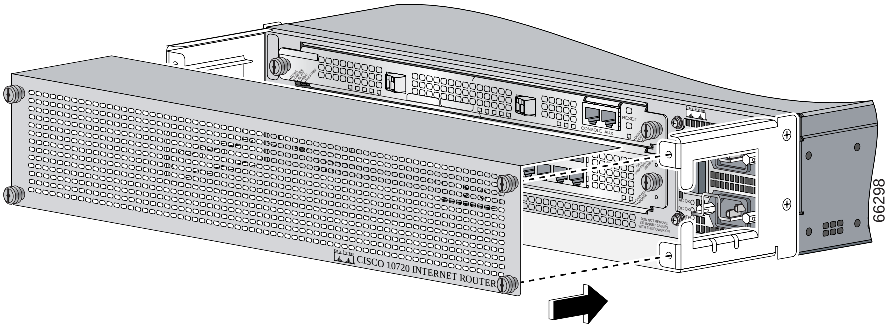
Figure 5-75 Cable-Management System Installed in a Rack



Step 6 Use cable ties to secure the cables to the rack to keep the wires from accidental bends or breaks. (See Figure 5-75.)

Step 7 Power up the router. (See the "Connecting Power to the Router" section on page 5-7.)

Figure 5-76 Installing the Cable-Management Cover



Step 8 (Optional) Using a Number 1 Phillips screwdriver, attach the cable-management cover with four screws to secure the cable-management cover to the router. (See Figure 5-76.)

APPENDIX A

Technical Specifications

This appendix contains physical and environmental specification information. For regulatory compliance and safety information, see the *Regulatory Compliance and Safety Information for the Cisco 10720 Internet Router* publication.

Physical and Environmental Specifications

Table A-1 Cisco 10720 Internet Router Specifications

Physical Router Chassis
Weight—34 lb (15.3 kg)
Dimensions—3.5 in. x 17.50 in. x 18.25 in. (8.9 cm x 44.45 cm x 46.35cm) H x W x D
Mounting options—19-, 23-/24-in. EIA, ETSI, front, mid-, or rear rack mounting, wall mounting, table mounting
Environmental
Temperature— Operating Temperature: 32^o to 104^{o}F (0^o to 40^{o}C) Non-operating: –4^o to 149^{o}F (–20^o to 65^{o}C)
Relative humidity— Operating relative humidity: 10 to 85% noncondensing Non-operating: 5 to 95% noncondensing
Altitude— Operating: 0 to 10,000 ft (0 to 3000 m) Non-operating: 0 to 15,000 ft (0 to 4570 m)
Total AC and DC Input Power— Maximum: 500W (1708 BTU/hr) Measured maximum: 200–300W (683–1025 BTU/hr)
AC and DC Heat Dissipation— Maximum: 500W
Acoustic noise—Maximum 60 dBa
Shock— Operating (half sine)—21 in./sec (0.53 m/sec) Non-operating (trapezoidal pulse)—20 G[1], 52 in./sec (1.32 m/sec)

Table A-1 Cisco 10720 Internet Router Specifications (continued)

Vibration— Operating: 0.35 Grms[2] from 3 to 500 Hz Non-operating: 1.0 Grms from 3 to 500 Hz
Software
Cisco IOS Software 12.0(19)SP or later
Router Processor (RP) Memory
256 MB—Routers shipped before November 2003 512 MB—Routers shipped after November 2003[3]

[1] G is a value of acceleration, where 1 G equals 32.17 ft/sec (9.81 m sec).

[2] Grms is the root mean square value of acceleration.

[3] The minimum Cisco IOS software required to use the 512 MB of RP memory on a Cisco 10720 Internet Router is Cisco IOS Release 12.0(27)S.

Power Specifications

Table A-2 Dual AC Power Supply

Description	Value
Total AC Input Power	Maximum: 500W (1708 BTU/hr) Measured maximum 200–300W (683–1025 BTU/hr)
Heat Dissipation	500W
Input Voltage	100 to 240 VAC
Input Line Frequency	50/60 Hz
Typical Input Current	2.5 to 5A

Table A-3 Dual DC Power Supply

Description	Value
Total DC Input Power	Maximum 500W (1708 BTU/hr) Measured maximum 200–300W (683–1025 BTU/hr)
Heat Dissipation	500W
Input Voltage	–48/–60 VDC
Maximum Input Current	9.0A
Typical Input Current	3.0 to 4.0A

INDEX